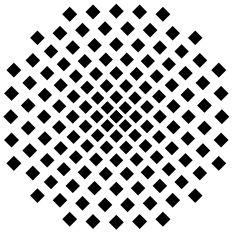


Universität Stuttgart

Institut für Nachrichtenvermittlung und Datenverarbeitung

Prof. Dr.-Ing. habil. Dr. h. c. mult. P. J. Kühn

76. Bericht über verkehrstheoretische Arbeiten

Sicherheitsarchitektur für mehrseitig sichere Kommunikationsdienste am Beispiel ISDN

von

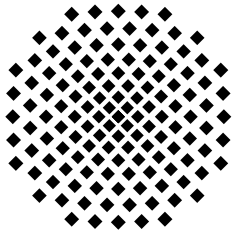
Reiner Sailer

1999

D 93

Druck: E. Kurz & Co., Druckerei + Reprografie GmbH., Stuttgart

ISBN 3-922403-86-7



University of Stuttgart

Institute of Communication Networks and Computer Engineering

Prof. Dr.-Ing. habil. Dr. h. c. mult. P. J. Kühn

76th Report on Studies in Congestion Theory

A security architecture for multilaterally secure telecommunication services and its implementation for ISDN

by

Reiner Sailer

1999

Summary

Telecommunication services are gaining more and more importance in everyone's life. Facing the present transition into an Information Society, we increasingly depend on reliable and secure telecommunication services to exchange information.

To comply with security requirements – like anonymity, data confidentiality, data integrity, availability, or authenticity – and to maintain or even improve the users' control of information processed by telecommunication services represent major challenges for existing and future telecommunication infrastructure.

Security issues are not considered sufficiently in present telecommunication environments. One of the reasons for that is that security requirements are not static but develop with applications. Hence, it seems unlikely that future telecommunication infrastructure – irrespective of the network technology: fixed or mobile – will inherently offer appropriate security for any user, service, and situation.

Therefore, the main objective of this thesis is to develop a *security architecture* that enables the upgrade of existing telecommunication infrastructure and supports supplementary security services that are user controlled and activated on demand to enhance basic telecommunication services, thus forming secure telecommunication services. In doing so, an *add-on approach* is taken in order to both save the huge investment into existing telecommunication infrastructure and enable this architecture to keep track with changing and evolving security requirements. The trend to heterogeneous network environments and telecommunication services spanning different types of networks additionally demands for *open and universal security services* that support security interworking at network boundaries.

Chapter 1 – Introduction

The *relationships* between users, telecommunication functions, and security functions are briefly analysed in this chapter. These relationships serve as a basis both to constitute the scope of this thesis and to define and elaborate the security architecture in chapter 3. The relationships between security functions – emerging from the need to *synchronize coupled security processes* representing security services – and between security and telecommunication functions – emerging from the need to *link security and telecommunication services* – are designated to be supported by the considered security architecture.

Chapter 2 – Networking Basics

This chapter introduces the Integrated Services Digital Network (ISDN) and its basic architecture. The security architecture developed throughout chapter 4 will be applied to the ISDN architecture in chapter 5. Signalling protocols, including Intelligent Network extensions, are described in detail as security services will benefit from conventional infrastructure, too.

Chapter 3 – Security Basics

Basic mechanisms of network security and concepts of *multilateral security* are introduced and depicted. Above all, the understanding of security as being derived by a fair negotiation of security requirements among all parties involved in a service is presented and justified.

The security architecture and its responsibilities to support multilaterally secure services are defined and major building blocks are derived. This chapter concludes with a brief overview of related security standards considering various standardization bodies.

Chapter 4 – Mechanisms for Multilaterally Secure Telecommunication Services

Major building blocks of the proposed security architecture are refined in this chapter. As a foundation, particularly the *add-on approach* and the *placement of security functions* in telecommunications are reconsidered and refined for their employment in telecommunication networks.

The *security supplementary services control* block presented here is independent of the given telecommunication environment. It is responsible for negotiating and coordinating security supplementary services and acts as a control application basing on an open service access point for security services (SAP^{Sec}).

The *security adaptation layer* adapts the SAP^{Sec} to the respective telecommunication environment. It is introduced both to implement this SAP^{Sec} interface by enhancing the actually given network interface and to compose secure telecommunication services by linking security and telecommunication control functions.

Chapter 5 – Architecture for User Controlled and Secure ISDN Services

The building blocks of the security architecture are used to implement an environment for multilaterally secure ISDN services. The implementation basing on the Linux operating system and its ISDN networking functions is described and various placement options for the security functions are discussed. Chapter 5 closes with the comparison of work presented in this thesis with previously existing work in related security areas.

Chapter 6 – Summary of Results and Outlook

Throughout this thesis, a security architecture that supports multilaterally secure services has been designed. It supports the negotiation of security services and the activation of security services on demand.

The security architecture has been implemented by adding infrastructure or functions and requires only minor if any changes of designated existing ISDN infrastructure. It exploits existing protocol mechanisms of the ISDN to exchange security protocol data units between terminals (user-to-user information) or between terminals and local exchanges (facility information). This thesis shows that there is need for more efficient support to exchange security control information between terminals (end-to-end) and between terminals and network servers (e. g. Intelligent Network Service Control Points). The ISDN protocol mechanisms that indicate required terminal capabilities to serve an incoming call (High Layer Capabilities) are exploited to address dedicated security enhanced ISDN terminals, i.e. to avoid responses of conventional ISDN terminals to connection requests that demand security enhancements.

Furthermore, by implementing the architecture for ISDN it has been demonstrated that it is feasible to link security and telecommunication services in selective infrastructure only (terminals, servers, or local exchanges). Thus, additional investment and changes are needed only at locations where additional benefits (i.e. security enhancements) need to be obtained.

Finally, the building blocks of the architecture can be easily adapted to other network technologies based on common channel signalling networks, e. g. GSM or B-ISDN/ATM. The adaptation of the depicted security architecture to IP-based networks is for further study.

Appendix

The appendix provides detailed information about the specification of the security architecture for ISDN. There are given SDL block interaction diagrams, process interaction diagrams, commented signalling time diagrams, and security specific codings of ISDN information elements as well as protocol traces of real exchanges of security protocol data units embedded in user-to-user information elements.

Inhaltsverzeichnis

1 Einführung ... 1

1.1 Ziele und Abgrenzung der Arbeit ... 1

1.2 Übersicht über die Arbeit ... 2

2 Netztechnische Grundlagen ... 5

2.1 Dienstekonzept im ISDN ... 6

2.2 Konfigurationen am ISDN-Teilnehmeranschluß ... 8

2.3 Referenzmodell und Protokollstruktur im ISDN ... 11

2.4 Steuerungs-Ebene im ISDN ... 12

2.4.1 Zeichengabesystem Nr. 1 an der Benutzer-Netzschnittstelle ... 14

2.4.2 Zentrales Zeichengabesystem Nr. 7 ... 21

2.4.3 Komponenten und Zeichengabeschnittstellen des Intelligenten Netzes ... 25

3 Sicherheitstechnische Grundlagen ... 29

3.1 Definitionen und Begriffe ... 29

3.2 Blickwinkel der Netzsicherheit ... 31

3.2.1 Duale Sicherheit und die Beziehung Mensch-Maschine ... 31

3.2.2 Mehrseitige Sicherheit in der Kommunikationstechnik ... 33

3.2.3 Schutzziele mehrseitig sicherer Kommunikationsdienste ... 35

3.3 Modelle für die Bewertung der Sicherheit von Systemen ... 37

3.3.1 Angreifermodelle – Sicht der Angreifer ... 37

3.3.2 Vertrauensbereiche – Sicht der Betroffenen ... 38

3.3.3 Bedrohungsmodelle – Systemsicht ... 39

3.4 Sicherheitsarchitekturen als Basis der Netzsicherheit ... 41

3.4.1 Definition und Einordnung der Sicherheitsarchitektur ... 42

3.4.2 Technische Bausteine einer Sicherheitsarchitektur ... 43

3.5 Stand der Standardisierung von Sicherheitsdiensten ... 53

3.5.1 Sicherheitsstandards der ITU und der ISO ... 53

3.5.2 Sicherheitsstandards der IETF ... 56

3.5.3 Weitere Standardisierungsaktivitäten ... 57

4 Mechanismen für mehrseitig sichere Telekommunikationsdienste ... 59

4.1 Additiver Ansatz ... 60

4.1.1 Integration und Kooperation von Sicherheitsfunktionen ... 60

4.1.2 Sichere Laufzeitumgebungen für Sicherheitsfunktionen ... 61

4.2 Plazierung und Wirkungsbereich von Sicherheitsfunktionen ... 62

4.2.1 Allgemeine Integrationsmöglichkeiten für Sicherheitsfunktionen ... 62

4.2.2 Klassifizierung von Sicherheitsfunktionen ... 65
4.2.3 Wirkungsbereich von Sicherheitsfunktionen ... 68
4.2.4 Auslagerung von Sicherheitsfunktionen ... 74
4.2.5 Benutzerorientierte Sicht auf Sicherheitsfunktionen – EzE-Sicherheit ... 76
4.3 Schnittstellenanforderungen exemplarischer Sicherheitsdienste ... 77
4.3.1 Authentisierungsdienste ... 77
4.3.2 Schutz von Nutzdaten und Steuerungsdaten durch Zwischenschichten ... 81
4.3.3 Schutz der Kommunikationsbeziehung ... 84
4.4 Sicherheitsarchitektur für mehrseitig sichere TK-Dienste – Anforderungen und Bausteine ... 86
4.4.1 Sicherheitsdienstesteuerung ... 88
4.4.2 Sicherheitsadaptionsschicht ... 91
4.5 Zusammenfassung ... 98

5 Architektur für benutzerkontrollierbare, sichere Dienste im ISDN ... 101
5.1 Universelle offene Sicherheitsdienste ... 101
5.2 Sicherheitsarchitektur am ISDN-Teilnehmeranschluß ... 103
5.2.1 Zielsetzung ... 103
5.2.2 Integration der Sicherheitsarchitektur in die Protokollarchitektur ... 104
5.2.3 Beispiel: Authentisierung zwischen Endgerät und TVSt ... 112
5.2.4 Implementierung der Sicherheitsarchitektur in einer Linux-Umgebung ... 114
5.2.5 Netztechnische Bewertung des Ansatzes ... 115
5.2.6 Sicherheitstechnische Bewertung des Ansatzes ... 119
5.3 Auslagerung von Sicherheitsfunktionen ... 121
5.3.1 Zusätzliche Geräte im Teilnehmerbereich ... 121
5.3.2 Auslagerung in spezielle Netzknoten ... 122
5.4 Einordnung und Abgrenzung existierender Ansätze ... 126

6 Zusammenfassung und Ausblick ... 129
6.1 Zusammenfassung der Ergebnisse ... 129
6.2 Ausblick ... 130

Literatur ... 133

Abbildungsverzeichnis ... 143

Anhang ... 145

Abkürzungsverzeichnis

Ack . . . . . Acknowledge (Empfangsbestätigung)
API . . . . . Application Programming Interface
ASE . . . . . Application Service Element
ATM . . . . . Asynchronous Transfer Mode
B-ISDN. . . . . Broadband-ISDN (Breitband-ISDN)
BMBF . . . . . Bundesministerium für Bildung, Wissenschaft, Forschung und Technologie
BSI . . . . . Bundesamt für Sicherheit in der Informationstechnik
CC . . . . . Call Control (Rufsteuerung)
CCF . . . . . Call Control Function
Cnf . . . . . Confirmation (Dienstprimitiv-Bestätigung)
Comp . . . . . Complete (Dienstprimitiv-Bestätigung)
CR . . . . . Call Reference
CRC . . . . . Cyclic Redundancy Check
DEA . . . . . Data Encryption Algorithm
DES . . . . . Data Encryption Standard
DEV . . . . . Device
DL . . . . . Data Link
DM . . . . . Dienstmerkmal
DMUX . . . . . Demultiplexer
DP . . . . . Detection Point
DSA . . . . . Digital Signature Algorithm
DSS . . . . . Digital Signature Standard
DSS1 . . . . . Digital Subscriber Signalling System No. 1
ECMA. . . . . European Computer Manufacturers Association
ET . . . . . Funktionsgruppe Exchange Termination
ETSI . . . . . European Telecommunications Standards Institute
EzE . . . . . Ende-zu-Ende
FAC . . . . . Facility
FCS . . . . . Frame Check Sequence (Rahmenprüfsumme)
FSM . . . . . Finite State Machine (Endlicher Automat)
GSM. . . . . Global System for Mobile Communications
HDLC . . . . . High-level Data Link Control
HLC . . . . . High Layer Compatibility
HLC^{Sec}. . . . . HLC-Kodierung für Übermittlungsdienst für Sicherheitssteuerungsdaten
HLC^{Sp} . . . . . HLC-Kodierung für Sprachdienste (0x01)
HLC^{SpSec} . . . . HLC-Kodierung für um Sicherheitsdienste erweiterte Sprachdienste
HLC^{TF} . . . . . HLC-Kodierung für Telefaxdienste (0x04)
HMAC. . . . . Message Authentication Code based on cryptographic hash functions
HW . . . . . Hardware

IDEA. . . . . International Data Encryption Algorithm
IE . . . . . Informationselement (Information Element)
IEC . . . . . International Electrotechnical Commission
IEEE. . . . . Institute of Electrical and Electronics Engineers
IETF . . . . . Internet Engineering Task Force
IN . . . . . Intelligent Network
INAP. . . . . Intelligent Network Application Protocol / Part
Ind . . . . . Indication (Dienstprimitiv-Anzeige)
IP . . . . . Intelligent Peripheral
IP . . . . . Internet Protocol
IPsec . . . . . IP Security (Sicherheitsprotokolle für das Internet Protocol)
IPv6 . . . . . Internet Protocol Version 6
ISDN . . . . . Integrated Services Digital Network (Diensteintegrierendes Digitalnetz)
ISO. . . . . International Organization for Standardization
ISP . . . . . Intermediate Service Part
ISS . . . . . ISDN Supplementary Services
ISUP. . . . . ISDN User Part (Anwenderteil für die ISDN-Zwischenamtssignalisierung)
IT-System . . . . Informationstechnisches System
ITU . . . . . International Telecommunication Union
IuKDG . . . . . Informations- und Kommunikationsdienste-Gesetz
K_d . . . . . Schlüssel zur Entschlüsselung (Decryption Key)
K_e . . . . . Schlüssel zur Verschlüsselung (Encryption Key)
$K_öX$. . . . . öffentlicher Schlüssel, der der Identität X zugeordnet ist
K_gX. . . . . geheimer Schlüssel des Trägers der Identität X
LI . . . . . Linklevel
LAPD . . . . . Link Access Procedure on the D-Channel
LT . . . . . Line Termination (netzseitiger übertragungstechnischer Abschluß der Anschlußleitung)
MAC . . . . . Message Authentication Code
MAP . . . . . Mobile Application Part
MTP . . . . . Message Transfer Part
MUX . . . . . Multiplexer
N-ISDN. . . . . Narrowband-ISDN (Schmalband-ISDN)
NIST. . . . . National Institute of Standards and Technology
NLSP . . . . . Network Layer Security Protocol
NNI. . . . . Network Node Interface (netzinterne Schnittstelle)
NT . . . . . Network Termination (teilnehmerseitige Netzabschlußeinheit)
NT1 . . . . . Funktionsgruppe Network Termination 1
NT2 . . . . . Funktionsgruppe Network Termination 2
OSI. . . . . Open Systems Interconnection
PCI . . . . . Protocol Control Information
PDU . . . . . Protocol Data Unit (Protokolldateneinheit)
PI . . . . . Partnerinstanz (Peer Entity)
PKI . . . . . Public Key Infrastructure
PzP . . . . . Punkt-zu-Punkt
Rej . . . . . Reject (Dienstprimitiv-Ablehnung)
Req . . . . . Request (Dienstprimitiv-Anforderung)

Res. . . . . Response (Dienstprimitiv-Antwort)
RM . . . . . Referenzmodell
RSA . . . . . Asymmetrisches Kryptosystem
(benannt nach seinen Erfindern: Rivest, Shamir, Adleman)
SA . . . . . Security Association
SA-ID . . . . . Security Association Identifier
SAL . . . . . Security Adaptation Layer (Sicherheitsadaptionsschicht)
SAP . . . . . Service Access Point (Dienstzugangspunkt)
SAPI. . . . . Service Access Point Identifier
SC . . . . . Smart Card
SCCP . . . . . Signalling Connection Control Part
(Steuerteil für Ende-zu-Ende-Zeichengabenachrichten im Zeichengabesystem Nr. 7)
SCEF . . . . . Service Creation Environment Function
SCF . . . . . Service Control Function
SCP . . . . . Service Control Point
SDF . . . . . Service Data Function
SDL . . . . . Specification and Description Language
SDP . . . . . Service Data Point
SDT . . . . . SDL Development Toolkit
SDU . . . . . Service Data Unit
SEP . . . . . Signalling End Point (Zeichengabe-Endpunkt)
SF . . . . . Sicherheitsfunktion (Teilfunktion eines Sicherheitsdienstes)
SFC . . . . . Supplementary Functional Component
SHA . . . . . Secure Hash Algorithm
SI . . . . . Service Indicator
SIG. . . . . Signatur
SMF . . . . . Service Management Function
SP . . . . . Signalling Point (Zeichengabeknoten)
SRF . . . . . Specialized Resource Function
SSF . . . . . Service Switching Function
SSL . . . . . Secure Socket Layer
SSP . . . . . Service Switching Point
SSN . . . . . Subsystem Number
SSS . . . . . Security Supplementary Services
SSS-Control . . Sicherheitsdienstesteuerung
SSSC . . . . . Security Supplementary Services Component
STP . . . . . Signalling Transfer Point (Zeichengabe-Transferpunkt)
TA. . . . . Terminal Adapter, Endgeräte-Anpassung
TC . . . . . Transaction Capabilities
TCAP . . . . . Transaction Capabilities Application Part
(Transaktionsunterstützung für verteilte Prozesse)
TCP . . . . . Transmission Control Protocol
TE . . . . . Terminal Equipment (Endeinrichtung)
TE1 . . . . . TE Typ 1 (Endeinrichtung mit ISDN-konformen Dienst-Schnittstellen)
TE2 . . . . . TE Typ 2 (Endeinrichtung ohne ISDN-konforme Dienst-Schnittstellen)
TEI . . . . . Terminal Equipment Identifier

TF . . . . . Telekommunikationsfunktion (Teilfunktion eines Telekommunikationsdienstes)
TLSP . . . . . Transport Layer Security Protocol
TK . . . . . Telekommunikation
TTP . . . . . Trusted Third Party (Vertraute Dritte Instanz)
TVSt . . . . . Teilnehmervermittlungsstelle
UNI . . . . . User Network Interface (Benutzer-Netzschnittstelle)
UUS . . . . . User-to-User Signalling
VI . . . . . Vertraute Instanz
VSt . . . . . Vermittlungsstelle
ZGS Nr. 7 . . . . Zentrales Zeichengabesystem Nr. 7
ZS . . . . . Zwischenschicht

Und dies ist ein allgemeines Gesetz;
jedes Lebendige kann nur innerhalb eines Horizontes
gesund, stark und fruchtbar werden
F. Nietzsche

Kapitel 1

Einführung

Kommunikationsdienste sind heute wesentlicher Bestandteil praktisch aller Lebensbereiche. Die Abhängigkeit von Telekommunikationsdiensten steigt dabei, obwohl die Kontrolle über deren Ablauf und die durch diese Dienste verarbeiteten Informationen vom Benutzer nur sehr eingeschränkt wahrgenommen werden kann. Damit steigt auch die Verletzlichkeit der Informationsgesellschaft [49] insgesamt.

Um dieser Verletzlichkeit entgegenzuwirken, müssen Telekommunikationsdienste den steigenden Anforderungen an die Sicherheitsaspekte gerecht werden. Die sich daraus entwickelnden Sicherheitsanforderungen können oftmals bei der Einführung neuer Systeme und Dienste noch nicht konkretisiert werden und finden deshalb derzeit nur unzulänglich Berücksichtigung. Da darüberhinaus die Investitionen in die Kommunikationsinfrastruktur enorm sind, müssen die Ressourcen als Basis bestehender und neuer Dienste auch weiterhin nutzbar sein.

Diese Arbeit soll die Grundlage für benutzerkontrollierbare Sicherheitsdienste schaffen, gleichzeitig jedoch auch die Interessen der Netzbetreiber und Dienstanbieter im Hinblick auf den Schutz ihrer Investitionen berücksichtigen.

1.1 Ziele und Abgrenzung der Arbeit

Die vorliegende Arbeit verfolgt das Ziel, die Einführung benutzerkontrollierbarer Sicherheitsdienste zu fördern. Diese Sicherheitsdienste sollen möglichst unabhängig vom jeweils genutzten Kommunikationsnetz sein und so netzübergreifend Sicherheitsanforderungen ihrer Benutzer unterstützen.

Sicherheit wird durch die Integration zusätzlicher Sicherheitsfunktionen und geschützter Laufzeitumgebungen angestrebt. Diese werden soweit möglich additiv und evolutionär – und damit investitionserhaltend – in die bestehende Kommunikationsinfrastruktur eingebracht. Die in dieser Arbeit beschriebene Sicherheitsarchitektur schafft die Grundlage für diesen Ansatz. Sie behandelt die in Bild 1-1 hervorgehobenen Beziehungen zwischen neuen Sicherheitsfunktionen (SF) und bestehenden Telekommunikationsfunktionen (TF):

- die Auswahl und Aktivierung von Sicherheitsfunktionen (z. B. in Endgeräten)
- die Unterstützung der Synchronisierung von verteilten, kooperierenden Sicherheitsfunktionen (z. B. Verschlüsselung beim Sender, Entschlüsselung beim Empfänger einer Nachricht)
- die sogenannte Kopplung von aktivierten Sicherheitsfunktionen und herkömmlichen Telekommunikationsfunktionen

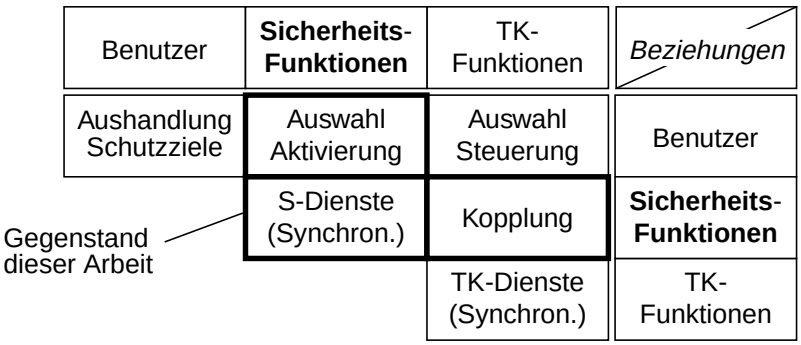


Bild 1-1: Beziehungen zwischen TK- und Sicherheitsfunktionen und Benutzern

Zur Erbringung dieser Unterstützung werden zwei wesentliche Komponenten der Sicherheitsarchitektur eingeführt:

- Eine transparente Zwischenschicht (*Sicherheitsadaptionsschicht*) dient zur Unterstützung der Synchronisierung (Beziehung: SF-SF) und Kopplung (Beziehung: SF-TF). Die Plazierung dieser Zwischenschicht wird aus der Protokollarchitektur des zugrundeliegenden Netzes abgeleitet.
- Ein Anwendungsprozeß dient als Kontrollstruktur (*Sicherheitsdienstesteuerung*) dieser Zwischenschicht. Diese Kontrollstruktur aktiviert optional zuschaltbare und netzübergreifende Sicherheitsdienstmerkmale (Beziehung: Benutzer-SF).

Das Ziel der Arbeit ist die Strukturierung einer Sicherheitsarchitektur zur optionalen Zuschaltung benutzerkontrollierter Sicherheitsdienste. Ihre praktische Anwendbarkeit wird durch eine exemplarische Implementierung für das ISDN gezeigt. Die Sicherheitsarchitektur soll auch die Synchronisierung und den Betrieb neuer Sicherheitsdienste basierend auf existierenden Netzdiensten ermöglichen. Die Ausgestaltung der Sicherheitsdienste selbst soll dabei nicht eingeschränkt werden.

1.2 Übersicht über die Arbeit

In Kapitel 2 werden die Grundlagen des ISDN vorgestellt. Zunächst werden das Dienstkonzept des ISDN und die Komponenten und Schnittstellen am ISDN-Teilnehmeranschluß erläutert.

Danach wird die Steuerung von ISDN-Diensten näher beschrieben. Das ISDN stellt das Anwendungsfeld für die Sicherheitsarchitektur dar.

Kapitel 3 führt in die Grundlagen der Netzsicherheit ein. Es werden die für diese Arbeit wesentlichen Sichtweisen dualer und mehrseitiger Sicherheit erläutert. Anschließend wird der Begriff der Sicherheitsarchitektur definiert. Ein Überblick über die Standardisierung von Sicherheitsdiensten schließt diesen Grundlagenteil ab.

Kapitel 4 bildet den Kern der Arbeit. Hier wird zunächst der additive Ansatz zur Erweiterung bestehender Telekommunikationsdienste um Sicherheitsdienste erläutert. Danach wird formal gezeigt, wie die Plazierung von Sicherheitsfunktionen und deren Wirkung gegen Angreifer zusammenhängen. Die Darstellung einiger exemplarischer Sicherheitsdienste veranschaulicht deren Anforderungen an die Ablaufumgebung. Die im Anschluß daran entwickelte Sicherheitsarchitektur und ihre Komponenten dienen als Basis sowohl für die Integration neuer Sicherheitsdienste als auch für deren Synchronisierung und Betrieb.

Die technische Umsetzung der Sicherheitsarchitektur für das ISDN ist Gegenstand von Kapitel 5. Der Schwerpunkt der Arbeit liegt auf der Integration der Sicherheitsarchitektur in die ISDN-Protokolle am Teilnehmeranschlußbereich. Es werden jedoch auch Ansätze für sinnvolle Erweiterungen der Protokolle im Zwischenamtsbereich aufgezeigt. Unterschiedliche Varianten der Implementierung der Sicherheitsarchitektur werden bezüglich ihrer Auswirkungen auf das Kommunikationsnetz und bezüglich ihrer Unterstützung von Sicherheitsdiensten bewertet. Die Abgrenzung der vorliegenden Arbeit zu bereits bestehenden Arbeiten zur Sicherheit im ISDN schließt dieses Kapitel ab.

Kapitel 6 faßt die wichtigsten Ergebnisse der Arbeit zusammen und soll den Blick für mögliche zukünftige Entwicklungen öffnen.

Kapitel 2

Netztechnische Grundlagen

Moderne Kommunikationsnetze entsprechen dem steigenden Bedarf an unterschiedlichen Netzdiensten durch ein universelles diensteintegrierendes Netzkonzept. Das im öffentlichen Bereich eingeführte diensteintegrierende Digitalnetz – heute als Schmalband-ISDN (Narrowband-ISDN, N-ISDN) bezeichnet – ist als Folge dieser Anforderungen entstanden. Es läßt sich zusammenfassend durch folgende technische Merkmale beschreiben:

- Digitale Übertragung über Kanäle mit einer Datentransferrate von je 64 kbit/s
- Durchschaltevermittlung im Zeitmultiplex
- Rechnersteuerung der Vermittlung
- Zentralkanalsignalisierung im Kernnetz
- Digitaler Teilnehmeranschluß mit zwei B-Kanälen (Basisanschluß) oder Vielfachen von 30 B-Kanälen (Primärmultiplexanschluß)
- Zentrale Signalisierung im Anschlußbereich über einen separaten D-Kanal mit 16 bzw. 64 kbit/s (Primärmultiplexanschluß)

Nutzdaten werden im Rahmen der Diensterbringung bittransparent zwischen Endeinrichtungen übermittelt. Dadurch kann ein solches Kommunikationsnetz einem breiten Spektrum von Anwendungen als Kommunikationsplattform dienen. Daraus resultierende Anforderungen werden von digitalen Übertragungssystemen erfüllt. Die Basis für eine schnelle Integration neuer Dienste und die Erweiterung bestehender Dienste bildet die programmierbare Rechnersteuerung innerhalb der Vermittlungsknoten.

Die Nachteile hinsichtlich hoher Bandbreitenanforderungen neuer Anwendungen (Multimedia-Dienste z. B. im Gesundheitswesen, Videokonferenzen, Internetdienste) haben zur momentan ausgeprägten Koexistenz von Rechner- und Datennetzen geführt, die in Zukunft zusammenwachsen werden. Das bestehende ISDN liefert die Voraussetzungen, eine im Prinzip universelle Telekommunikations-Infrastruktur aufzubauen. Aufbauend auf diesem heute als N-ISDN bezeichneten Netz erfolgt eine Weiterentwicklung innerhalb der ITU zur breitbandigen, ATM-basierten Variante B-ISDN. Alternativ dazu entwickelt sich aus dem paketorientierten Internet ein diensteintegrierendes Universalnetz, welches für eine Reihe neuer Dienste von Vorteil ist, aber hinsichtlich der Dienstgüte noch viele Fragen offen läßt.

Die Einführung des ISDN wurde durch die Deutsche Telekom AG in Deutschland aus technischer Sicht mit der Digitalisierung des Kernnetzes in 1997 abgeschlossen. Die Analoganschlüsse dominieren zwar noch im Teilnehmerbereich von Privatkunden, doch existiert die

Analogtechnik nur noch im Anschlußnetz. Innerhalb des Netzes werden auch analoge Sprachdienste digital realisiert. Das ISDN ist seit 1993 als EURO-ISDN europaweit standardisiert. Es gelten die Empfehlungen der I-Serie der International Telecommunication Union (ITU).

Diese Arbeit stützt sich auf die Empfehlungen der I-Serie (Integrated Services Digital Networks – ISDN) der ITU und auf damit in Beziehung stehende Empfehlungen der Q-Serie (Switching and Signalling), der G-Serie (Transmission Systems and Media, Digital Systems and Networks) und der X-Serie (Data Networks and Open System Interconnection). Bild 2-1 gibt einen Überblick über die Strukturierung der Empfehlungen der I-Serie und den darin referenzierten Empfehlungen.

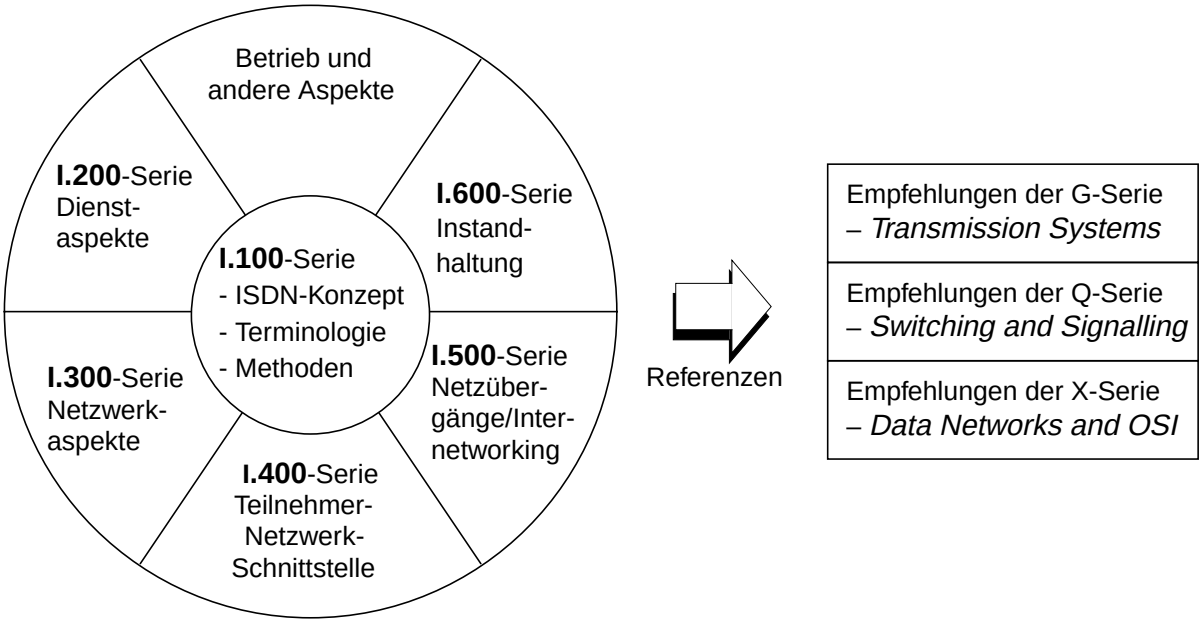


Bild 2-1: Strukturierung der Empfehlungen der ITU zum ISDN

Für diese Arbeit sind im Bezug auf das ISDN neben der I-Serie die Empfehlungen der Q-Serie für Zeichengabeprotokolle und zusätzliche Dienstmerkmale im ISDN sowie das Basisreferenzmodell für offene Systeme (OSI-Referenzmodell, siehe ITU-T Empfehlung X.200 [115] bzw. ISO-Standard 7498 [86]) von besonderer Bedeutung.

2.1 Dienstekonzept im ISDN

Ein *Kommunikationsdienst* (Dienst) umfaßt alle funktionalen Eigenschaften eines Kommunikationsnetzes, welche eine bestimmte Kommunikationsform zwischen Endgeräten unterstützen. Ein Dienst wird im ISDN durch die Gesamtheit seiner Dienstmerkmale beschrieben, von denen bestimmte zur Etablierung einer Kommunikationsform zwischen Endgeräten unverzichtbar sind. Neben dieser Grundausstattung eines Dienstes (Basisdienst) wird eine Vielzahl zusätzlicher Funktionen (zusätzliche Dienstmerkmale, Supplementary Services) bereitgestellt, welche entweder dem Benutzer des Dienstes oder dem Netzbetreiber dienen [46]. Als zusätzliche Dienstmerkmale sind beispielsweise die Entgeltinformationen während und nach der Dienstnutzung, das Identifizieren oder Anrufbeantworter-Dienste im ISDN verfügbar.

Basisdienste lassen sich in Übermittlungsdienste und Teledienste untergliedern. Bild 2-2 veranschaulicht die Einordnung und den Wirkungsbereich der unterschiedlichen Dienstformen.

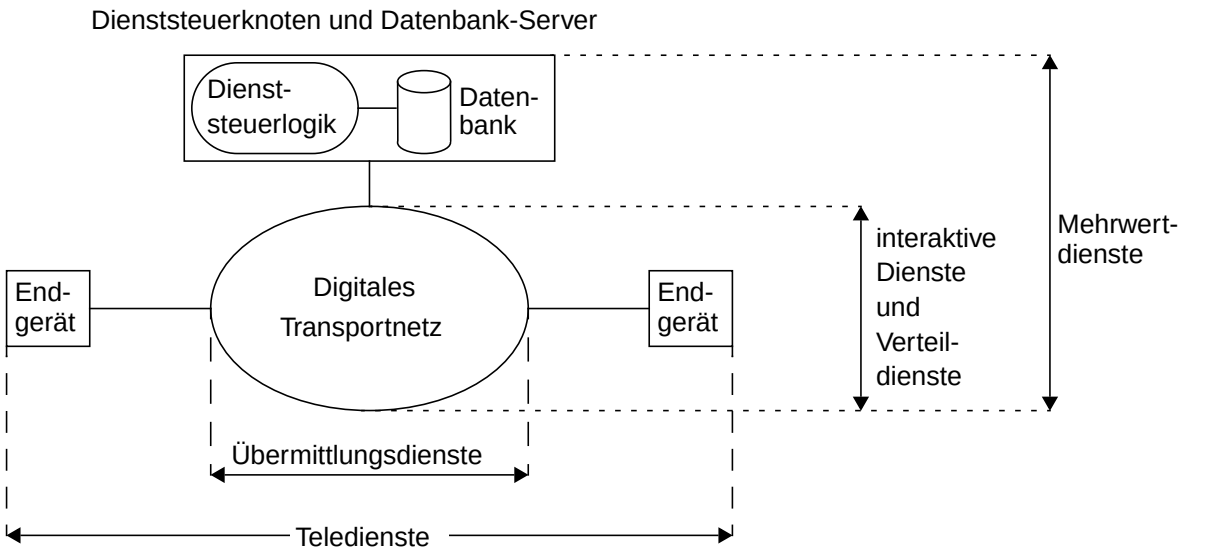


Bild 2-2: Wirkungsbereich von Übermittlungsdiensten und Telediensten [46]

Übermittlungsdienste (Bearer Services) umfassen die code- und anwendungsunabhängige Nachrichtenübermittlung ohne Berücksichtigung der Kommunikationsfunktionen innerhalb der Endgeräte und zentraler Dienste- und Datenserver (ITU-T Empfehlungen I.230 [92] ff.). Im ISDN finden meist Übermittlungsdienste zur Datenübermittlung (Unrestricted Digital Information) und zur Übermittlung von Sprachinformation (Speech) Anwendung. Übermittlungsdienste lassen sich im Hinblick auf die Art der Vermittlung (Paket- bzw. Leitungsvermittlung) und die Datenrate weiter spezifizieren. Diese Untergliederung hat sich in der Standardisierung eines speziellen Beschreibungselementes für den Übermittlungsdienst (Bearer Capability) niedergeschlagen.

Teledienste umfassen zusätzlich die Benutzer-Benutzer-Kommunikation einschließlich der Steuerung des Dialogs durch Endeinrichtungen und durch zentrale Diensteserver innerhalb des Kommunikationsnetzes. Teledienste lassen sich weiter untergliedern in interaktive Dienste (Telefon, File-Transfer, Elektronische Post, Abruf von gespeicherten Daten) und Verteildienste (Rundfunk, interaktives Fernsehen). Teledienste sind in den Empfehlungen I.240 [93] und I.241 definiert.

Zur flexiblen Realisierung und zur schnellen Einführung neuer Dienste finden zentrale Dienststeuerknoten- und Datenbank-Server Anwendung. Diese sind über standardisierte Schnittstellen an das ISDN angebunden. Die Dienststeuerlogik des Dienststeuerknotens erweitert bestehende Dienste und ermöglicht eine dynamische Tarifierung unterschiedlicher Rufphasen (Verbindungsaufbau mit Ansage, Verbindung, Verbindungsabbau). Daraus resultieren sogenannte Mehrwertdienste, wie beispielsweise die ursprungs- oder tageszeitabhängige Zielansteuerung, bei der die Zielrufnummer als Bestandteil der Diensterbringung (Ruf) innerhalb des Netzes vom zentralen Dienstserver bestimmt wird. Die Einbindung von zentralen Dienste- und Datenservern wird in Abschnitt 2.4.3 bei der Behandlung des Intelligenten Netzes näher erläutert. Mehrwertdienste werden ebenfalls unter den Begriff Teledienste gefaßt[1].

1 In der Empfehlung I.210, Abschnitt 3.5.1 werden Endgeräte- und Netzfunktionen sowie *Funktionen spezieller zentraler Einrichtungen* unter Teledienste gefaßt.

2.2 Konfigurationen am ISDN-Teilnehmeranschluß

Die in Bild 2-2 vereinfacht als Endgerät dargestellte Teilnehmerinfrastruktur kann sich am ISDN-Anschluß je nach Anforderungen aus sehr unterschiedlichen Bausteinen zusammensetzen, welche flexibel miteinander verbunden werden müssen. Beispiele ergänzender Teilnehmerinfrastruktur stellen Geräte zum Anschluß analoger Telefax-, Telefon- oder Datenendgeräte sowie Telekommunikationsanlagen mit Internvermittlungs- und Multiplexer-Funktionen dar. Moderne Anwendungen im Teilnehmerbereich, wie z. B. Computer Integrated Telephony oder Call Center-Lösungen führen neue Einrichtungen ein, welche zunehmend komplexe Konfigurationen auch im Teilnehmerbereich bedingen.

Zur Strukturierung des Teilnehmerbereiches im ISDN sind in der Empfehlung I.411 [96] *Referenz-Konfigurationen* vorgegeben, die unterschiedliche Anforderungen eines breiten Spektrums von Anwendungen abdecken. Diese Konfigurationen beschreiben mögliche Zusammenschaltungen physischer Geräte im Teilnehmerbereich und definieren einheitliche Referenzpunkte (Bezugspunkte), an denen unterschiedliche Geräte-Konfigurationen möglich sind. Die technische Auslegung der Referenzpunkte in Form physikalischer Schnittstellen ist schließlich sowohl von der Art des ISDN-Anschlusses (Basisanschluß, Primärmultiplexanschluß) als auch von der Art des Übertragungsmediums (Glasfaser, Koaxialkabel, Zweidraht- oder Vierdraht-Kupferleitung) abhängig.

Zur Strukturierung der Referenz-Konfigurationen werden in der ITU-T Empfehlung I.411 zwei Beschreibungskonzepte eingeführt:

- *Funktionsgruppen* fassen Funktionen zusammen, welche jeweils unterschiedlichen Typen von Geräten im Teilnehmer- und Netzbereich zugeordnet werden können (z. B. Endgerät, Telekommunikationsanlage, Vermittlungsstelle).

- *Referenzpunkte* (oder Bezugspunkte) dienen zur Abgrenzung verschiedener Funktionsgruppen. Sie beschreiben logische Schnittstellen zwischen unterschiedlichen Funktionsgruppen und können – müssen aber nicht – mit einer physikalischen Schnittstelle korrespondieren. Im ISDN werden die Referenzpunkte R, S, T, U und V unterschieden.

Diese Strukturierung soll die flexible Implementierung von Funktionsgruppen in unterschiedlichen Geräten und die flexible Zusammenschaltung von Geräten im Teilnehmerbereich erleichtern. Darauf basierend kann neuen Anforderungen im Teilnehmerbereich durch Zuschalten ergänzender Geräte oder durch Austausch von Geräten Rechnung getragen werden. Es werden folgende Funktionsgruppen unterschieden (vgl. Bild 2-3):

- Die Funktionsgruppe *NT1* (Network Termination) beinhaltet Funktionen gemäß der Schicht 1 des OSI-Referenzmodelles [86] zum übertragungstechnischen Abschluß der Anschlußleitung im Teilnehmerbereich. Sie umfaßt Funktionen zur Synchronisierung, zur Notspeisung von Endgeräten und zur Koordinierung des konkurrierenden Zugriffes mehrerer Endgeräte auf der Teilnehmerseite.

- Die Funktionsgruppe *NT2* umfaßt neben Funktionen der Schicht 1 auch Multiplexer-, Protokollabwicklungs-, Vermittlungs- und Konzentrationsfunktionen höherer Schichten.

- Die Funktionsgruppe *TE* (Terminal Equipment) umfaßt Endeinrichtungsfunktionen, wie z. B. Protokollbehandlungs- und Unterhaltungsfunktionen, sowie Schnittstellen- und Anschaltungsfunktionen zu anderen Geräten oder Systemen.

- Die Funktionsgruppe *TE1* umfaßt Funktionen der Funktionsgruppe TE und zusätzlich Funktionen zum ISDN-Dienstzugang (ISDN-Endgerätefunktion).
- Die Funktionsgruppe *TE2* umfaßt Funktionen der Funktionsgruppe TE und Funktionen zum Dienstzugang, welche nicht mit der ISDN-Teilnehmerschnittstelle korrespondieren (z. B. Funktionen analoger Endgeräte).

■ Die Funktionsgruppe *TA* (Terminal Adapter) umfaßt Funktionen der Terminalanpassung zur Anschaltung von Nicht-ISDN-Geräten an das ISDN, genauer an den Referenzpunkt S. Je nach technischer Realisierung der Funktionen werden am R-Bezugspunkt physikalische Schnittstellen der V-Serie (Anschaltung von Datenendgeräten an das Fernsprechnetz) oder der X-Serie (Anschaltung von Datenendgeräten an das Datennetz) realisiert. Die häufigste Anwendung stellt noch immer die Schaffung einer analogen Schnittstelle am R-Referenzpunkt zur Anschaltung und Weiterverwendung herkömmlicher analoger Telefon- oder Telefaxgeräte dar.

■ Die Funktionsgruppe *LT* (Line Termination)[2] ist die zur Funktionsgruppe NT1 duale Funktionsgruppe auf der Seite der Teilnehmervermittlungsstelle (TVSt). Sie bildet den netzseitigen übertragungstechnischen Abschluß der Teilnehmeranschlußleitung und kann innerhalb der Vermittlungsstelle oder aber in Vorfeldeinrichtungen (Multiplexer, Konzentratoren) enthalten sein. Sie übernimmt Aufgaben der Stromversorgung, Fehlererkennung, Signalregeneration und Codierung bzw. Decodierung.

■ Die Funktionsgruppe *ET* (Exchange Termination) umfaßt Funktionen bis zur Schicht 3 des OSI-Referenzmodelles. Sie trennt Zeichengabedaten (D-Kanal-Daten) von Nutzdaten und schließt die Übertragungsstrecke zwischen Teilnehmervermittlungsstelle und Endgerät bzw. NT ab.

Die genannten Referenzpunkte und Funktionsgruppen werden in Bild 2-3 in Beziehung gesetzt. Die Referenzpunkte R, S und T werden in der Empfehlung I.411 definiert und bieten mit den zugehörigen – ebenfalls standardisierten – technischen Umsetzungen[3] offene physikalische Schnittstellen im Teilnehmerbereich.

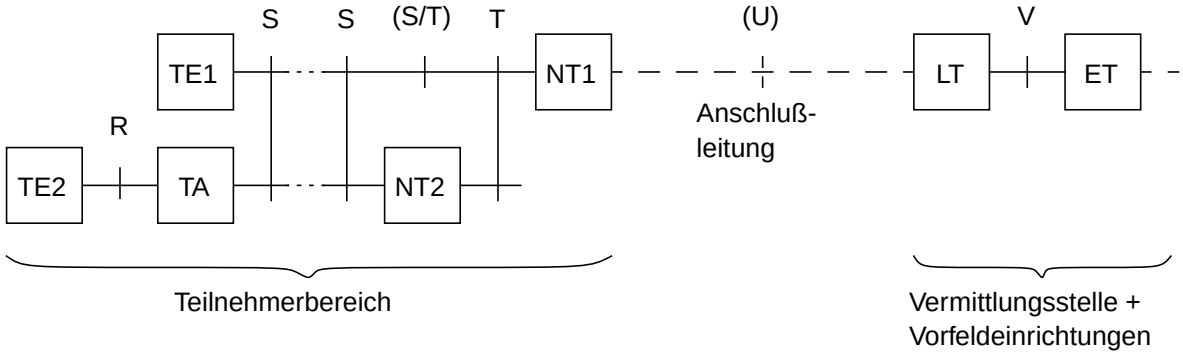


Bild 2-3: Funktionsgruppen und Referenzpunkte am ISDN-Basisanschluß

2 Die Funktionsgruppen LT und ET sind in I.411 nicht explizit definiert. Die Empfehlungen I.430/Annex E [97] aus dem Jahre 1988 und Q.512 [100] grenzen jedoch den Umfang dieser Funktionsgruppen ein.

3 Die technischen Umsetzungen der Referenzpunkte (physikalische Schnittstellen) und Anforderungen an Übertragungssysteme für die Teilnehmeranschlußleitung sind in den ITU-T Empfehlungen G.9xx festgelegt.

Am Basisanschluß wird die physikalische Auslegung der Referenzpunkte S und T als S_0-Schnittstelle bezeichnet. Sie ist meist als Bussystem ausgelegt und erlaubt den parallelen Anschluß von bis zu 8 ISDN-Endgeräten. Am Primärmultiplexanschluß wird die physikalische Auslegung am Referenzpunkt S als S_{2M}-Schnittstelle bezeichnet. Die Funktionen und Parameter an dieser Schnittstelle entsprechen der 2-Mbit/s-Schnittstelle der digitalen Übertragungssysteme PCM30. Sie ist zunächst für den Punkt-zu-Punkt-Betrieb zum Anschluß von Telekommunikationsanlagen vorgesehen.

Für die Anschlußleitung wurde kein Referenzpunkt standardisiert, da dort keine Benutzer-Netz Schnittstelle vorgesehen ist. Die physikalische Auslegung der Teilnehmeranschlußleitung zwischen dem Netzabschluß (NT) und dem übertragungstechnischen Abschluß (LT) innerhalb des ISDN ist betreiberspezifisch. Der zugehörige Bezugspunkt wird im allgemeinen in Anlehnung an die standardisierten Referenzpunkte mit U bezeichnet. Die lokalen Randbedingungen (bestehende Infrastruktur) und strategische Entscheidungen (Kosten) haben dazu geführt, daß für den Basisanschluß in Deutschland ein Zeitgleichlageverfahren mit Echokompensation auf der bestehenden Kupferdoppelader (U_{k0}-Schnittstelle[4]) eingeführt wurde, während in den USA ein Zeit-Getrenntlageverfahren auf der Teilnehmeranschlußleitung eingesetzt wird (U_{P0}-Schnittstelle).

Die Empfehlung Q.512 definiert den Referenzpunkt V. Die zum Bezugspunkt V korrespondierenden physikalischen Schnittstellen werden mit V_x bezeichnet[5]. Die V_1-Schnittstelle wird für Basisanschlüsse (Basic Rate Access) verwendet. Die V_3-Schnittstelle kennzeichnet den Primärmultiplexanschluß (Primary Rate Access). Weitere V-Referenzpunkte sind für analoge Anschlußleitungen und Vorfeldeinrichtungen wie Multiplexer oder Konzentratoren definiert.

Bild 2-4 zeigt einige Referenz-Konfigurationen für den ISDN-Teilnehmerbereich. In den Konfigurationen (1) und (2) fallen die Referenzpunkte S und T zusammen, die Funktionsgruppe NT2 ist leer. In Konfiguration (4) existiert keine zum Referenzpunkt T korrespondierende physikalische Schnittstelle, da die Funktionen von NT2 und NT1 innerhalb eines Gerätes implementiert sind.

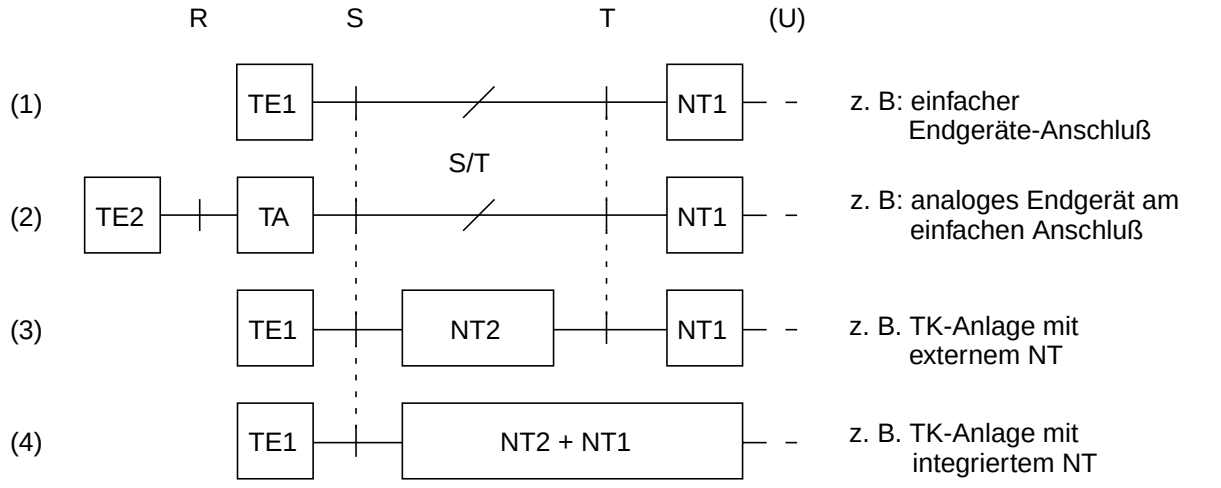


Bild 2-4: Referenz-Konfigurationen am ISDN-Teilnehmeranschluß

4 Nationale Festlegungen für die U_{k0}-Schnittstelle im Netz der Deutsche Telekom AG sind in den Technischen Richtlinien 1 TR 210, 1 TR 211 und 1 TR 220 [81] gegeben.

5 Nicht zu verwechseln mit den Empfehlungen V.x der V-Serie für Datendienste über das Fernsprechnetz.

Referenz-Konfigurationen beschreiben folglich Verteilungsmöglichkeiten von Funktionen auf unterschiedliche Geräte und Bezugspunkte für die Zusammenschaltung verschiedener Geräte zum Erhalt einer gewünschten Gesamtfunktionalität an der Benutzer-Netzschnittstelle im ISDN. Das Konzept der Referenz-Konfiguration definiert somit eine *orthogonale Sicht* zu der durch das OSI-Referenzmodell vorgegebenen Strukturierung von Funktionen innerhalb eines Kommunikationssystems.

2.3 Referenzmodell und Protokollstruktur im ISDN

Im folgenden werden durchschaltevermittelnde Dienste zur Verbindung von Endgeräten über das ISDN betrachtet. Die darüber hinaus im ISDN angebotenen paketvermittelnden Dienste – die sowohl über einen Nutzkanal, als auch über den Signalisierkanal (D-Kanal) angesprochen werden können – werden nicht gesondert behandelt. Einzelheiten dazu sind in [47] und in der Empfehlung Q.72 [98] enthalten.

Die Daten, welche durch die Funktionen eines Knotens verarbeitet werden müssen, lassen sich in drei Kategorien einteilen:

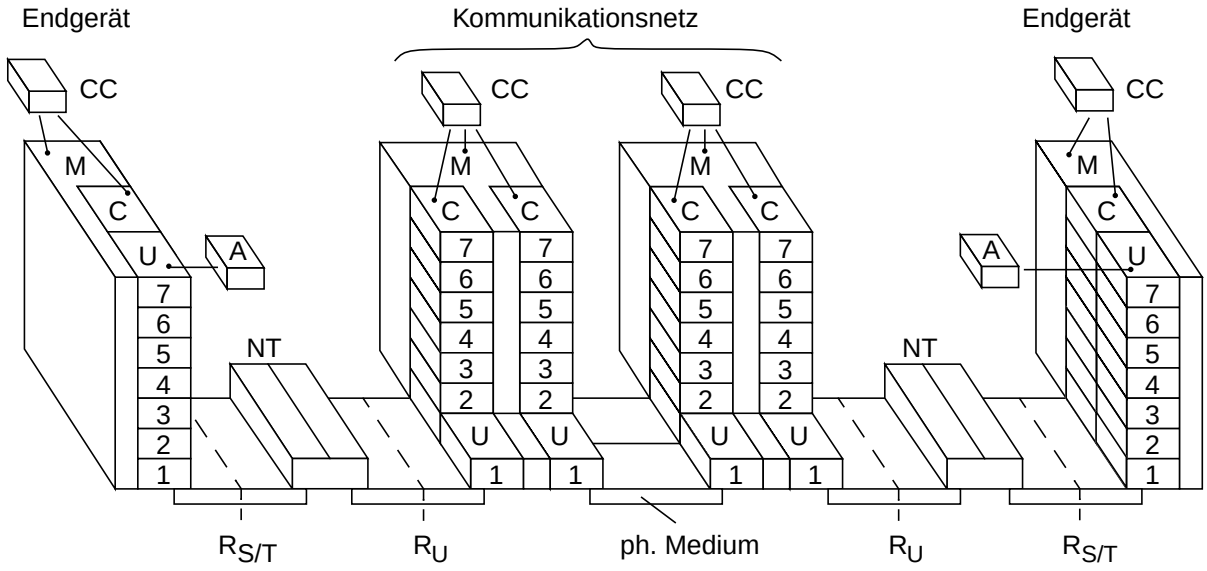
- Benutzer-zu-Benutzer-Daten (Nutzdaten, User Data)
- Steuerungsdaten (Dienste-Steuerungsdaten, Control Data)
- Managementdaten (Management Data)

Die Funktionen innerhalb eines Knotens werden im Hinblick auf die Art der durch sie verarbeiteten Daten – und damit der Art der durch sie bearbeiteten Aufgabe – in sogenannte Ebenen untergliedert. Die Steuerungs-Ebene (Control Plane) umfaßt Funktionen zur Steuerung von Kommunikationsvorgängen und bildet die Basis für ISDN-Dienste. Die Management-Ebene umfaßt jene Funktionen, die für das Management eines Kommunikationssystems notwendig sind (Management Plane). Der Nutzer-Ebene (User Plane) werden die Funktionen zur Behandlung von Nutzdaten zugeordnet (siehe Bild 2-5).

Eine *Funktionsschicht* (auch Schicht genannt) ist definiert als eine Teilmenge von Funktionen entsprechend der Gliederung dieser Funktionen nach den im OSI-Referenzmodell festgelegten Kriterien. Es werden die Funktionsschichten Bitübertragungsschicht (Physical Layer, Schicht 1), Datensicherungsschicht (Data Link Layer, Schicht 2), Vermittlungsschicht (Network Layer, Schicht 3), Transportschicht (Transport Layer, Schicht 4), Kommunikationssteuerungsschicht (Session Layer, Schicht 5), Darstellungsschicht (Presentation Layer, Schicht 6) und Verarbeitungsschicht (Application Layer, Schicht 7) innerhalb der Steuerungs- und Nutzer-Ebene unterschieden.

Bei leitungsvermittelnden Diensten beschränkt sich die Behandlung von Nutzdaten innerhalb des Netzes auf Codierungs- und Decodierungsfunktionen (Bitübertragungsschicht U-1 in Bild 2-5). Funktionen zur Fehlererkennung sind für die Übertragung von Nutzdaten innerhalb des Netzes nicht vorgesehen. Diese müssen bei Bedarf innerhalb der Endgeräte als zusätzliche Datensicherungsfunktionen implementiert werden. Datensicherungsfunktionen sind in die Funktionsschicht U-2 einzuordnen. Gewöhnlich wird zur Datensicherung ein auf dem HDLC-Standard (High-Level Data Link Control Procedures, siehe [84], [85]) basierendes Verfahren verwendet.

Die Funktionen zur Steuerung von ISDN-Diensten werden in der *Steuerungs-Ebene* zusammengefaßt. Die *Rufsteuerung* (Call Control) ist als Anwendung der Dienste der Steuerungs-



U	Nutzer-Ebene (User Plane)	CC	Rufsteuerung (Call Control)
C	Steuerungs-Ebene (Control Plane)	A	Anwendung (Application)
M	Management-Ebene (Management Plane)	NT	Netzabschluß (Network Termination)
R_x	Referenzpunkt X		

Bild 2-5: ISDN-Referenzmodell – Ebenen und Funktionsschichten [95]

Ebene für den Auf- und Abbau von Verbindungen, für die Verwaltung von Ressourcen (B-Kanäle, etc.) und die Realisierung zusätzlicher Dienstmerkmale zuständig. Die Rufsteuerungen der an einem Telekommunikationsdienst beteiligten Knoten handeln beim Verbindungsaufbau die variablen Dienstparameter (z. B. den zu verwendenden B-Kanal) aus und steuern die Ressourcen-Belegung. Zum Austausch von Steuerinformation zwischen Endgeräten und der Teilnehmervermittlungsstelle bzw. zwischen Vermittlungsstellen greifen die jeweiligen Prozesse zur Rufsteuerung auf Basisdienste der Steuerungs-Ebene zurück.

Die Managementfunktionen eines Knotens verwalten im Gegensatz zu den Steuerfunktionen die von einer Verbindung unabhängige Ressourcen. Dazu gehören beispielsweise die Adressen, welche von den unterschiedlichen Funktionsschichten benutzt werden, oder Einstellungen zu Fenstergrößen von Datensicherungsprotokollen, die langfristig gültig sind. Managementfunktionen sind auch für die Erkennung und Behandlung von Fehlern zuständig, die schichtenübergreifend bedeutsam sind. Innerhalb der Management-Ebene werden Funktionen zum Management der verschiedenen Ebenen (Layer Management) und Funktionen zum übergreifenden Management eines Knotens (Node Management) unterscheiden [117].

Die im Hauptteil dargelegten Untersuchungen beziehen sich vor allem auf die Steuerungs-Ebene sowie die Dienstesteuerung im ISDN. Deshalb werden die Funktionsschichten dieser Ebene im folgenden näher beschrieben.

2.4 Steuerungs-Ebene im ISDN

Die Funktionen der Steuerungs-Ebene dienen zum Austausch von Steuerungsinformation und zur koordinierten Steuerung der Endeinrichtungen und der Netzknoten zur Realisierung von Kommunikationsdiensten.

Der Austausch von Steuerungsinformation zwischen Endeinrichtungen und Netz bzw. zwischen Steuerungseinrichtungen innerhalb des Netzes wird in der Vermittlungstechnik als *Zeichengabe* oder *Signalisierung* bezeichnet. Die Zeichengabe dient zum Auf- und Abbau von Verbindungen, zur Inanspruchnahme von weiteren Leistungsmerkmalen sowie zum Netzbetrieb und zur Administration [46]. Im ISDN wird die *Zentralkanal-Signalisierung* angewendet, d. h. es werden grundsätzlich separate, digitale Kanäle zur Übertragung von Steuerungsdaten bereitgestellt, welche von mehreren Zeichengabeeinrichtungen gemeinsam genutzt werden. Das ISDN enthält also ein eigenständiges paketvermittelndes Netz zum Austausch von Steuerungsdaten.

Es wird zwischen dem *Zentralen Zeichengabesystem Nr. 7* (ZGS Nr. 7) zum Austausch von Steuerungsinformation zwischen Netzknoten und dem *Digitalen Zeichengabesystem Nr. 1* (DSS 1) zum Austausch von Steuerungsinformation an der Benutzer-Netzschnittstelle unterschieden. Bild 2-6 veranschaulicht sowohl die logische Trennung von Zeichengabe- und Nutzkanalnetz, als auch den Wirkungsbereich des ZGS Nr. 7 innerhalb des Netzes und die Anwendung des DSS 1 an der Benutzer-Netzschnittstelle. Die Umsetzung der Zeichengabe an der Benutzer-Netzschnittstelle ist in der Abbildung nicht ausgeführt.

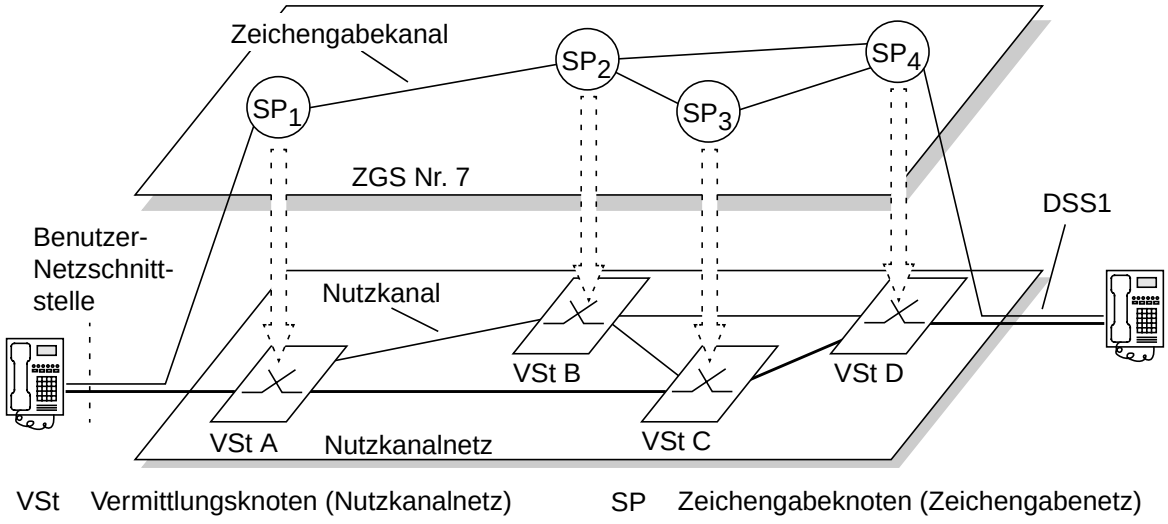


Bild 2-6: Zeichengabe- und Nutzkanal-Netz im ISDN

Bei der Knoten-übergreifenden Steuerung von Kommunikationsdiensten steht – neben den lokal innerhalb einer Funktionsschicht ausgeführten Aufgaben – die Interaktion verschiedener, an einem Dienst beteiligter Knoten beziehungsweise ihrer für die Steuerung zuständigen Instanzen im Vordergrund. Zum Aufbau einer Nutzkanalverbindung zwischen den in Bild 2-6 dargestellten Endgeräten müssen beispielsweise die Steuerprozesse der Zeichengabeknoten SP_1, SP_3 und SP_4 koordiniert zusammenwirken, um die Nutzkanalverbindung abschnittsweise durchzuschalten. Deshalb wird nachfolgend zum Begriff der Funktionsschicht der Begriff des Protokolles eingeführt.

Ein *Protokoll* bezeichnet die Gesamtheit aller Vereinbarungen zur Zusammenarbeit zwischen Instanzen der gleichen Funktionsschicht in unterschiedlichen Kommunikationssystemen (Knoten). Es beinhaltet insbesondere die Regeln zur *Interpretation von Nachrichten* und zur *Koordinierung des Nachrichtenaustausches*. Protokolle, welche sich auf Funktionsschichten der Steuerungs-Ebene beziehen, werden als Zeichengabeprotokolle oder Signalisierprotokolle

bezeichnet. Sie definieren im Zusammenspiel die Dienste eines Zeichengabesystems im Sinne der Dienstedefinition im OSI-Referenzmodell. Dem Protokoll kommt folglich die Aufgabe zu, über die Festlegungen zur Codierung und zur Interpretation von Steuerungsdaten den notwendige Steuerungsinformationsfluß zwischen verschiedenen Teilnehmer- und Netzknoten zu ermöglichen.

Da die Anforderungen an die Codierung und Interpretation von Steuerungsdaten von den jeweils zu koordinierenden Steuerungsfunktionen abhängen, sind Protokolle und Funktionsschichten fest miteinander verbunden. Protokolle besitzen – im Gegensatz zu ausschließlich lokale Bedeutung besitzenden Funktionen – eine weitreichende Bedeutung für die Kompatibilität innerhalb eines Verbundes von Zeichengabe-Einrichtungen. Sie sind deshalb international standardisiert und besitzen einen fest vorgegebenen Satz an Interpretations- und Koordinierungs-Regeln. Optionale Erweiterungen, z. B. die Einführung nationaler Steuerungsparameter und Steuerungsnachrichten, besitzen deshalb nur innerhalb eines Netzes Bedeutung und können ohne besondere Maßnahmen nicht zur netzübergreifenden Steuerung von Kommunikationssystemen genutzt werden.

Aufgrund der unterschiedlichen Aufgaben, die an der Benutzer-Netzschnittstelle und an netzinternen Schnittstellen über die Steuerungs-Ebene abgewickelt werden müssen, unterscheiden sich auch die Funktionen der jeweiligen Steuerungs-Ebene und die ihnen zugeordneten Zeichengabeprotokolle. Zunächst werden die Funktionsschichten und Protokolle an der Benutzer-Netzschnittstelle besprochen. Anschließend wird auf die netzinternen Funktionsschichten und Protokolle der (Dienste-) Steuerungs-Ebene eingegangen.

2.4.1 Zeichengabesystem Nr. 1 an der Benutzer-Netzschnittstelle

Bei der offiziellen Einführung des ISDN in Deutschland im Jahre 1989 waren noch keine europaweiten Standards für die Signalisierung an der Benutzer-Netzschnittstelle verfügbar. Deshalb wurde mit der Technischen Richtlinie 1 TR 6 [80] zunächst ein nationaler Standard eingeführt, welcher nun schrittweise verschwindet und durch den 1993 eingeführten europäischen Standard ersetzt wird. Maßgeblich sind heute die ITU-T Empfehlungen Q.930 [108] und Q.931 [109] für die Netzwerkschicht (Schicht 3, OSI-RM) der Steuerungs-Ebene. Für den gesicherten Austausch von Steuerungsdaten (Schicht 2, OSI-RM) sind die Empfehlungen Q.920 [106] und Q.921 [107] bestimmend. Die Protokolle der Schichten 2 und 3 werden zusammenfassend auch als ISDN-D-Kanal-Protokolle bezeichnet.

Bild 2-7 ordnet die an der Benutzer-Netzschnittstelle angewendeten Zeichengabeprotokolle am ISDN-Basisanschluß in das ISDN-Referenzmodell ein.

Die Implementierung der Bitübertragungsschicht ist abhängig von der Anschlußart (Basisanschluß, Primärmultiplexanschluß). Die folgende Beschreibung bezieht sich auf den Basisanschluß, also auf die Auslegung des S-Bezugspunktes als S_0-Schnittstelle und des national festgelegten U-Referenzpunktes als U_{k0}-Schnittstelle über eine Kupferdoppelader. Die darüberliegenden Schichten sind von der Auslegung des Anschlusses weitgehend unabhängig.

Schicht 1 – Die Bitübertragungsschicht im ISDN

Die Aufgabe der *Schicht 1* stellt die Adaption eines Kommunikationssystems (Knotens) an das zur Übertragung von Daten genutzte Medium dar. Der Netzabschluß (Network Termination, NT, vgl. Bild 2-7) setzt die Signale der S-Schnittstelle am Basisanschluß (S_0-Bus) in Signale für die Anschlußleitung (U_{k0}-Schnittstelle) um und umgekehrt. Die Bitübertragungsrate beträgt am S_0-Bus 192 kbit/s. Darin sind die B-Kanäle (2 x 64 kbit/s), der D-Kanal (16 kbit/s)

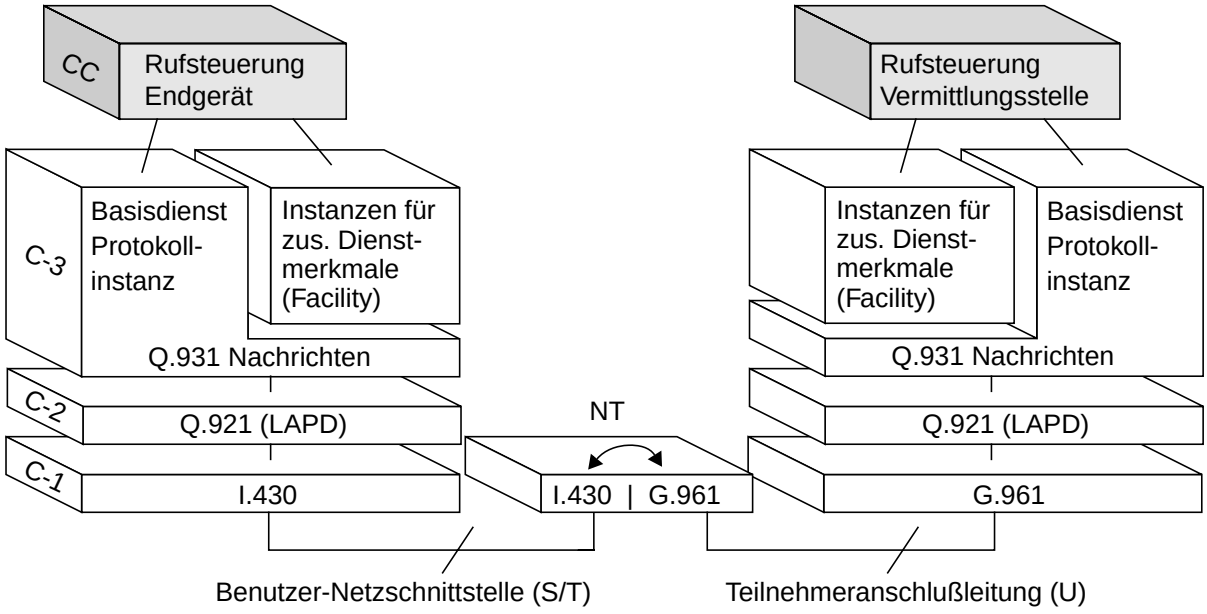


Bild 2-7: Zeichengabeprotokolle am Teilnehmeranschluß im ISDN

sowie weitere Kanäle für die Synchronisation und die Steuerung des Buszugriffes enthalten. Auf der Teilnehmeranschlußleitung (U_{k0}-Schnittstelle) werden 160 kbit/s bei einer Schrittgeschwindigkeit von 120 kbaud übertragen.

Die Funktionen der Schicht 1 ermöglichen den Austausch binärer Signale zwischen direkt verbundenen Kommunikationssystemen. Die Ausprägung dieser Schicht ist an das jeweilige Übertragungsverfahren angepaßt und unterscheidet sich folglich an den Schnittstellen der Referenzpunkte S/T und an der Teilnehmeranschlußleitung (Referenzpunkt U). Die Aktivierung und Deaktivierung des ISDN-Anschlusses wird ebenfalls durch Funktionen und Protokolle der Schicht 1 realisiert.

Schicht 2 - Datensicherungsschicht im ISDN

Die *Schicht 2* beinhaltet Funktionen und Protokolle zum Medienzugriff und bietet darüberliegenden Schichten gesicherte Übertragungsdienste für binäre Daten an. Die Funktionen der Schicht 2 wirken jeweils auf einen Übertragungsabschnitt und beziehen sich deshalb immer auf direkt benachbarte (verbundene) Kommunikationssysteme. Sie dient zur Abgrenzung und Transparenz von Daten und realisiert einen gegen Übertragungsfehler gesicherten Austausch von Steuerungsdaten. Zur Erkennung und Begrenzung der Übertragungsrahmen werden feste Rahmenbegrenzer benutzt (Binär: 01111110). Zur Erhaltung der Transparenz der innerhalb von Rahmen übertragenen Daten wird das sogenannte „Bit-Stopfen“ verwendet[6]. Damit wird das Vorkommen von Rahmenbegrenzern innerhalb eines Rahmens verhindert. Zur Fehlersicherung dienen eine Prüfsumme (Frame Check Sequence, FCS), Reihenfolgezähler und Zeitüberwachungs-Mechanismen. Der Aufbau der zwischen Schicht 2-Instanzen verschiedener Kommunikationssysteme ausgetauschten Übertragungsrahmen (Schicht 2-Protokolldateneinheiten) ist in Bild 2-8 dargestellt.

6 Beim „Bit-Stopfen“ wird vor dem Absenden innerhalb eines Rahmens nach jeweils 5 aufeinanderfolgenden 1-Bits ein 0-Bit eingefügt. Beim Empfänger wird ein nach 5 aufeinanderfolgenden 1-Bits auftretendes 0-Bit einfach entfernt. Damit kennzeichnet das Auftreten von 6 aufeinanderfolgenden 1-Bits beim Empfänger sicher das Rahmenende. Gleichzeitig kennzeichnen mehr als 6 aufeinanderfolgende 1-Bits einen freien Übertragungskanal.

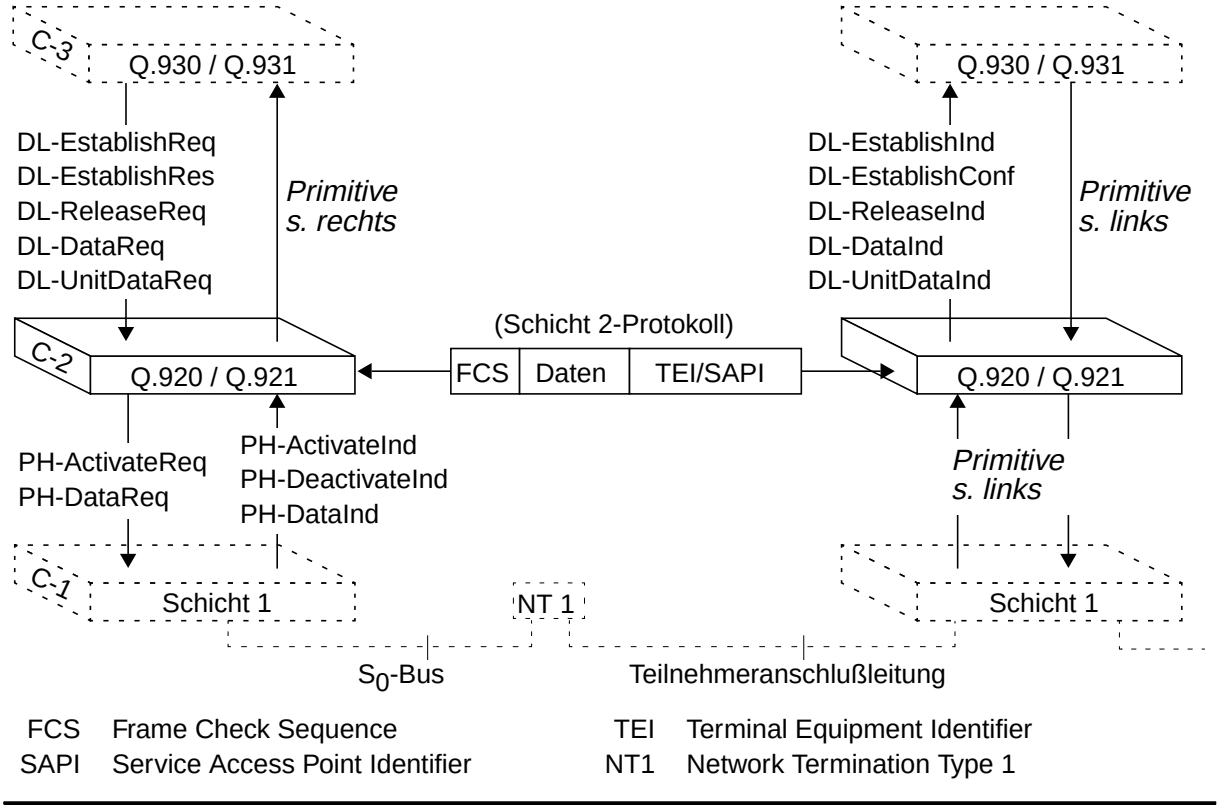


Bild 2-8: Dienste und Dienstprimitive der Schicht 2 des ISDN-D-Kanals nach Q.921

Im Bild sind auch die Dienstprimitive für den Auf- und Abbau von Schicht 2-Verbindungen (DL-Establish, DL-Release) sowie für den Datenaustausch (DL-Data, DL-UnitData) angegeben. Die Dienstprimitive für Management-Aufgaben (TEI-Management, etc.) sind nicht dargestellt. Die Schicht 2 der Steuerungs-Ebene bietet ihren Nutzern zwei unterschiedliche Ausprägungen von Datendiensten an:

- Der *unbestätigte Datendienst* (DL-UnitData) wird unabhängig vom Aufbau einer Schicht 2-Verbindung angeboten. Eine Reihenfolgesicherung bzw. Empfangsbestätigung findet nicht statt.

- Der *bestätigte Datendienst* (DL-Data) setzt eine Schicht 2-Verbindung voraus. Die mit diesem Dienst übertragenen Datenblöcke sind reihenfolgegesichert und werden vom Empfänger bestätigt.

Das Protokoll der Schicht 2 ist aus dem standardisierten Protokoll HDLC (High-Level Data Link Control) abgeleitet und wird mit *LAPD* (Link Access Procedure on the D-Channel) bezeichnet. Am Basisanschluß wird die Fenstergröße für bestätigte Datendienste fest auf 1 gesetzt. Empfangene Schicht 2-Rahmen werden beim Dienst DL-Data innerhalb der Schicht 2 sofort quittiert. Die Adressierung von Schicht 2-Rahmen wird über die für einen Anschluß eindeutig vergebene Endgeräte-Kennung (Terminal Equipment Identifier) und den Dienstzugangspunkt (Signalisierung, Management, Paketdaten, etc.) durchgeführt. Damit ist je Endgerät genau eine Schicht 2-Verbindung für Zeichengabezwecke adressierbar.

Die Protokolle zur Schicht 2 an der ISDN-Benutzer-Netzschnittstelle sind in den Empfehlungen Q.920 und Q.921 vorgegeben. Diese stützen sich auf die allgemeinen Vereinbarungen HDLC-basierter Protokolle. Die entsprechenden Empfehlungen I.440 und I.441 der I-Serie

verweisen auf diese Empfehlungen der Q-Serie. Für die maximale Länge des Informationsfeldes zur Übertragung von Schicht 3-PDUs ist für Schicht 2-PDUs auf 260 Oktetts festgelegt.

Schicht 3 – Vermittlungsschicht

Die Dienste der Schicht 2 ermöglichen den verbindungsorientierten, gesicherten Austausch von Zeichengabenachrichten zwischen Endeinrichtungen (Endgeräte, TK-Anlagen, etc.) und dem netzseitigen Abschluß (Funktionsgruppe ET) im ISDN. Die Schicht 3 baut auf diesen Diensten auf und ermöglicht durch die Definition eigener Protokolldateneinheiten die Synchronisation von Schicht 3-Instanzen in Endeinrichtungen und in der Teilnehmervermittlungsstelle zur Auswahl von Kommunikationsdiensten (Telediensten), zum Auf- und Abbau zugehöriger Verbindungen und zur Behandlung zusätzlicher Dienstmerkmale.

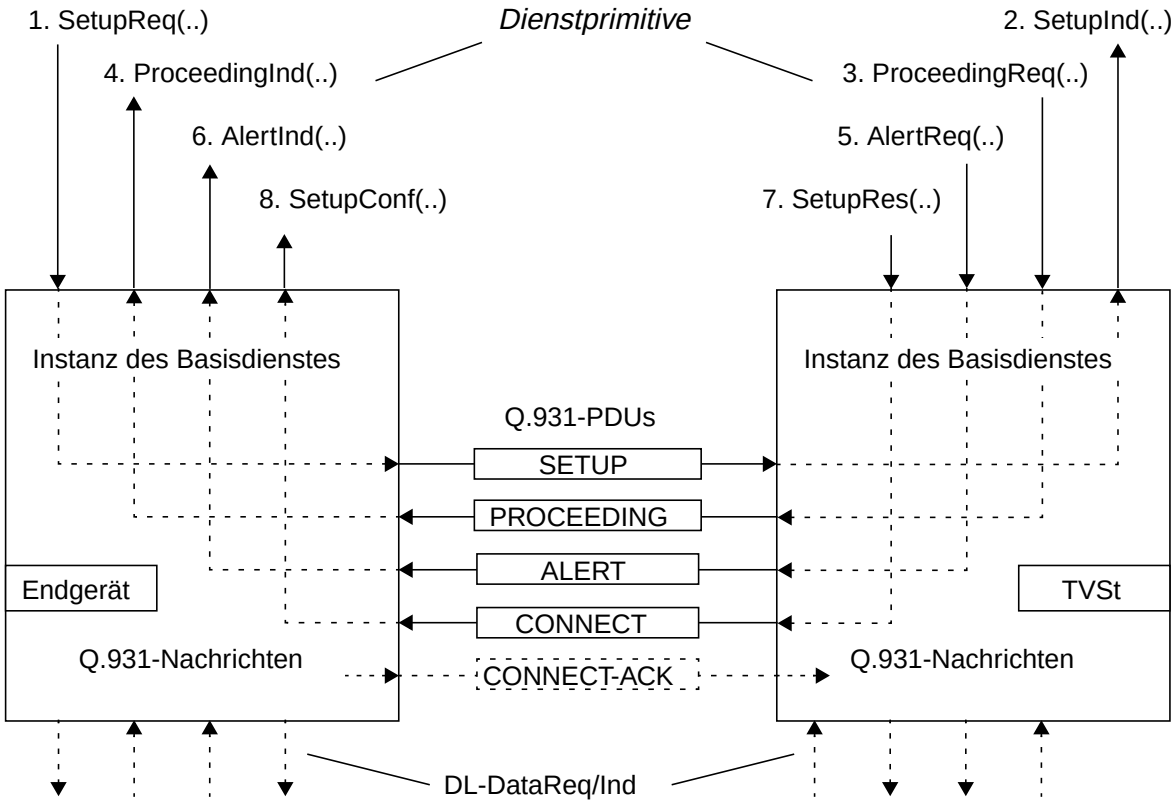


Bild 2-9: Dienstprimitive und PDUs zum Verbindungsaufbau nach Q.931

Zur Verwaltung mehrerer Schicht 3-Verbindungen und zur Steuerung von verbindungsunabhängigen Dienstmerkmalen dient die sogenannte Call Reference. Sie ermöglicht logische Verbindungen über eine einzelne Schicht 2-Verbindung. Die Rufsteuerungen innerhalb des Endgerätes und der Teilnehmervermittlungsstelle sprechen die Dienste der Schicht 3 über Dienstprimitive an. Diese sind in der Empfehlung Q.931 in Annex A definiert.

Protokolle zur Schicht 3 an der ISDN-Benutzer-Netzschnittstelle sind in den Empfehlungen Q.930 und Q.931 festgelegt. Die Empfehlungen I.450 und I.451 verweisen auf diese Empfehlungen. Sie definieren Dienstprimitive, Protokolldateneinheiten und darin enthaltene Informationselemente (Datentypen) zum Austausch von dienstespezifischen Parametern zwischen Schicht 3-Instanzen in Endeinrichtungen und der Teilnehmervermittlungsstelle. Die Einordnung der Schicht 3 in die Steuerungs-Ebene des ISDN-Referenzmodelles ist in Bild 2-5 und

Bild 2-7 dargestellt. Den Zusammenhang zwischen Dienstprimitiven und übermittelten Protokolldateneinheiten beim einfachen Verbindungsaufbau zeigt Bild 2-9 für den rufenden Anschluß.

Der Verbindungsaufbau wird mit Hilfe des Dienstprimitives SetupReq angefordert und innerhalb der Schicht 3 durch Senden einer *Setup*-Nachricht eingeleitet. Sofern genügend Wahlinformation in dieser Nachricht enthalten ist, um das Rufziel zu adressieren, wird von der Vermittlungsstelle mit einer *Proceeding*-Nachricht geantwortet. Sonst wird mit der *Setup-Acknowledge*-Nachricht weitere Wahlinformation vom Endgerät angefordert. Ist am Ziel-Anschluß ein kompatibles und freies Endgerät gefunden, so wird dies durch die Vermittlungsstelle mit einer *Alert*-Nachricht angezeigt. Das Durchschalten der Verbindung wird mit einer *Connect*-Nachricht bestätigt. Bei automatischen Diensten – ohne Benutzer-Interaktion bei der Rufannahme – kann das gerufene Endgerät direkt mit einer Connect-Nachricht antworten. Eine Alert-Nachricht entfällt dann. Das Senden der *Connect-Acknowledge*-Nachricht ist optional. Einzelheiten über den Protokollablauf können der Protokollspezifikation der Empfehlung Q.931 entnommen werden.

Den allgemeinen Aufbau von Schicht 3-Protokolldateneinheiten zum Austausch von Zeichengabeinformation zwischen Schicht 3-Instanzen in Endeinrichtungen und der Teilnehmervermittlungsstelle zeigt Bild 2-10.

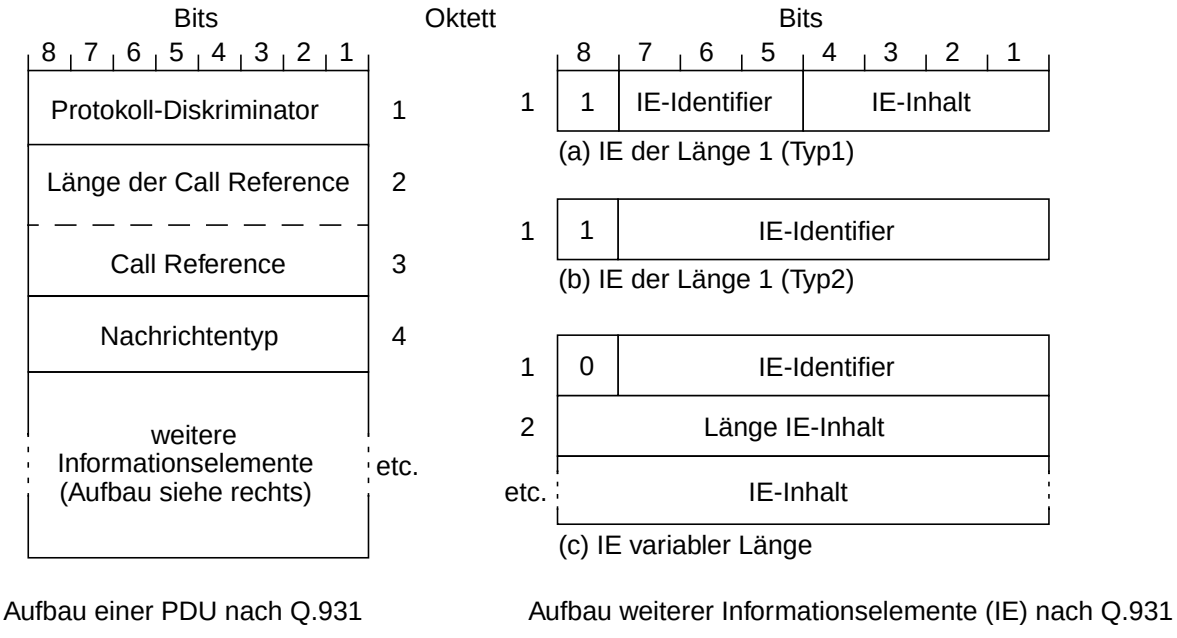


Bild 2-10: Aufbau von Protokolldateneinheiten nach Q.931

Anhand des Protokoll-Diskriminators lassen sich unterschiedliche Schicht 3-Protokolle unterscheiden. Im EURO-ISDN gilt für das Protokoll nach Q.931 bzw. I.451 die Kennung 0x08, für das ältere nationale Protokoll nach 1TR6 sind aufgabenspezifisch die Kennungen N1 (0x41) oder N0 (0x40) zu verwenden. Für proprietäre oder proprietär erweiterte Protokolle, beispielsweise zwischen Telekommunikationsanlagen und System-Telefonen, werden reservierte Protokoll-Diskriminatoren verwendet. Damit ist beim Empfang einer Schicht 3-PDU ihre protokollspezifische Interpretation bzw. die Prüfung der Kompatibilität assoziierter Funktionsschichten möglich.

Zusätzliche Informationen werden innerhalb der Zeichengabenachrichten in sogenannten Informationselementen (Bild 2-10 rechts) übermittelt. Es stehen dafür verschiedene Typen von Informationselementen (IE) zur Verfügung. Für diese Arbeit werden insbesondere Informationselemente mit variabler Länge von Bedeutung sein. Zusätzlich zum Nachrichtentyp können hier z. B. die Nummer des zu nutzenden B-Kanals, Wahlinformation oder Anzeigen für im Nutzkanal verfügbare Inband-Signale (z. B. Wählton, Freiton) zwischen der Rufsteuerung im Endgerät und der Vermittlungsstelle ausgetauscht werden. Die Länge von Schicht3-PDUs wird augenblicklich durch die maximale Länge von Informationsfeldern in Schicht2-PDUs (260 Oktetts) begrenzt, da eine Segmentierung von Schicht3-PDUs noch nicht vorgesehen bzw. implementiert ist.

Die Empfehlung Q.931 beschreibt jedoch in Anhang H [110] optionale Prozeduren zur Segmentierung von Schicht 3-PDUs vor ihrer Weitergabe zur Übertragung an Schicht 2. Die Implementierung erfolgt in einer transparenten Zwischenschicht, die zwischen Schicht 2 und Schicht 3 eingefügt wird. Diese Zwischenschicht übernimmt die Aufgaben zur Segmentierung und Reassemblierung von Schicht 3-PDUs. Es sind maximal 8 Segmente vorgesehen, so daß sich unter Beachtung des durch die Segmentierung eingeführten Mehraufwandes die maximale Gesamtlänge einer Schicht 3-PDU vor ihrer Segmentierung zu 2020 Oktetts berechnet.

Steuerung von zusätzlichen Dienstmerkmalen im ISDN

Es sind gegenwärtig drei verschiedene Schicht 3-Protokolle für die Steuerung von Dienstmerkmalen (Supplementary Services) im ISDN vorgesehen (siehe ITU-T Empfehlung Q.932 [111]). Diese werden aufgrund ihrer Bedeutung im weiteren Verlauf der Arbeit kurz erläutert:

- Das *Keypad Protocol* ist ein stimulus-orientiertes Protokoll. Das Endgerät besitzt keine Kenntnis über die darüber gesteuerten Dienstmerkmale, sondern transportiert lediglich Tasten-Eingaben des Benutzers durch sogenannte *Keypad*-Informationselemente innerhalb von Information-Nachrichten zum Netz. Das Netz kann mit Hilfe von *Display*-Informationselementen zusätzliche Anweisungen für den Benutzer zum jeweiligen Endgerät übertragen. Keypad-Protokolle sind netzspezifisch realisiert.

- Das *Feature Key Management Protocol* basiert auf dem Austausch von *Feature Activation*- und *Feature Indication*-Informationselementen. Diese Informationselemente können in Nachrichten zum Verbindungsaufbau (vgl. Bild 2-9) oder in separaten Information-Nachrichten übertragen werden. Das Dienstmerkmal, das durch den jeweiligen Feature-Indikator aufgerufen wird, ist mit dem Netzbetreiber separat zu vereinbaren und in einem sogenannten Dienste-Profil festgelegt. Das Endgerät muß keine Kenntnis über die zu steuernden Dienstmerkmale besitzen.

- Das *Functional Protocol* (funktionales Protokoll) setzt Dienstmerkmal-spezifische Funktionen innerhalb des Endgerätes voraus. Damit sind einige Dienstmerkmale auch ohne Interaktion durch den Benutzer realisierbar. Die Steuerung basiert auf *Facility*-Informationselementen, welche in *Facility*- oder *Register*-Nachrichten oder in Nachrichten des ISDN-Basisdienstes übertragen werden können. Für einige Dienstmerkmale sind spezielle Nachrichten für das funktionale Protokoll definiert (z. B. Hold- und Retrieve-Nachrichten), mit denen spezifische Informationen übertragen werden können.

Das Keypad- und das Feature Key Management-Protokoll besitzen lediglich lokale Bedeutung. Das funktionale Protokoll hingegen kann auch weiterreichende Bedeutung besitzen und bildet deshalb die Grundlage für zukünftige, netzübergreifend wirksame Dienstmerkmale. Die

innerhalb der ITU-T-Empfehlungen spezifizierten zusätzlichen Dienstmerkmale basieren auf dem funktionalen Protokoll.

Zusätzliche Dienstmerkmale sind innerhalb der ITU-T-Empfehlungen in drei unterschiedlichen Stufen (Abstraktionsebenen) beschrieben. Allgemeine Beschreibungen und einen Überblick über standardisierte zusätzliche Dienstmerkmale und ihre Interaktion mit den Benutzern geben die Empfehlungen I.250 [94] bis I.259 (Stage 1 Description). Die Empfehlungen Q.80 [99] bis Q.87 liefern eine funktionale Beschreibung der Dienste und ihre Verteilung innerhalb des Netzes (Stage 2 Description). Die ausführliche Beschreibung der Codierung der Steuerinformation in Facility-Informationselementen und die Spezifikation der Abläufe basierend auf dem funktionalen Protokoll liefern die Empfehlungen Q.950 [112] bis Q.957 (Stage 3 Description).

Rufsteuerung

Die *Rufsteuerung* umfaßt die Gesamtheit der Steuervorgänge zum Auf- und Abbau sowie zur Verwaltung von Verbindungen, die zu einem Ruf gehören. Die Rufsteuerung kann sich zum Auf- und Abbau und zum Unterhalt von Verbindungen der sogenannten *Verbindungssteuerung* bedienen. Ein Ruf stellt in diesem Zusammenhang eine Kommunikationsbeziehung zwischen Benutzern des ISDN dar beziehungsweise zwischen Benutzern und Dienste- oder Daten-Servern innerhalb des Netzes (siehe auch Bild 2-2).

Gleichzeitig interagiert die Rufsteuerung im Endgerät auch mit den peripheren Einrichtungen der Endeinrichtung, um beispielsweise auf Ereignisse (Hörer abnehmen, Wahltasten betätigen) entsprechend der Erwartung des Benutzers reagieren zu können oder Anzeigen des Netzes an den Benutzer weiterzuleiten (Anzeige von Entgelt- oder Dienstmerkmal-Information am Display, etc.).

Bei der Steuerung eines ISDN-Sprachdienstes kommen der Rufsteuerung innerhalb der Teilnehmervermittlungsstelle u. a. folgende Aufgaben zu:

- Steuerung von ISDN-Verbindungen
- Verwaltung von Netzressourcen (z. B. Tongeneratoren, B-Kanäle, netzinterne Nutzkanäle, Zeichengabekanäle)
- Identifikation des Teilnehmers
- Prüfung der Freischaltung und Berechtigung des rufenden Anschlusses
- Prüfung der Rufnummer des rufenden Teilnehmers (z. B. bei Rufnummernanzeige)
- Umsetzung von Teilnehmer- und Zwischenamts-Zeichengabe (Interworking)
- Anstoß, Steuerung und Abschluß der Entgeltdatenerfassung bzw. Online-Abbuchung
- Überwachung des Verbindungszustandes während einer Verbindung
- Steuerung von zusätzlichen ISDN-Dienstmerkmalen (ISDN Supplementary Services)

Die Rufsteuerung innerhalb der Endgeräte ist weniger umfangreich, da die Verwaltung von netzinternen Ressourcen entfällt. Innerhalb von Transit-Vermittlungsstellen entfallen die Teilnehmer-spezifischen Aufgaben (z. B. Identifizieren, Interworking, Rufnummernprüfung).

Auffällig ist die Asymmetrie bei sicherheitsrelevanten Funktionen, wie beispielsweise der Entgeltdatenerfassung und der Identifikation. Diese Asymmetrie resultiert aus der ehemaligen Monopolstellung der Deutsche Telekom AG – eine Identifikation des Dienstanbieters durch den Benutzer war implizit gegeben – und aus der Rechtslage bei Streitigkeiten bezüglich der erfaßten Entgeltdaten und der folgenden Rechnungsstellung. Die durch den Netzbetreiber erfaßten Daten galten bis zum Gegenbeweis durch den Kunden grundsätzlich als korrekt und als maßgeblich für die Rechnungserstellung. Schließlich war die Teilnehmermobilität im ISDN nicht sehr ausgeprägt, so daß eine anschlußbasierte Identifikation und Entgeltdatenzuordnung ausreichend erschien.

2.4.2 Zentrales Zeichengabesystem Nr. 7

Die Funktionen der Steuerungs-Ebene innerhalb von Netzknoten im ISDN dienen zum Auf- und Abbau von 64-kbit/s-Nutzkanalverbindungen zwischen Teilnehmeranschlüssen und zur Realisierung von ISDN-Diensten und zusätzlichen Dienstmerkmalen. Um diese verteilten Steuerungsaufgaben zu lösen, müssen die beteiligten ISDN-Vermittlungsstellen Steuerungsinformation austauschen, welche eine Koordination zwischen den unterschiedlichen Steuerprozessen ermöglicht.

Die Steuerungsfunktionen innerhalb der einzelnen Netzknoten sowie die zugehörigen Protokolle zur Koordination der Zusammenarbeit von Steuerungsfunktionen unterschiedlicher Netzknoten werden zusammenfassend als Zwischenamts-Zeichengabesystem (oder Zwischenamts-Signalisiersystem) bezeichnet. Das Zwischenamts-Zeichengabesystem im ISDN zeichnet sich gegenüber herkömmlichen Zeichengabesystemen dadurch aus, daß die Zeichengabenachrichten unabhängig von den *Nutzkanälen*, die damit gesteuert werden sollen, in separaten *Zeichengabekanälen* übermittelt werden. So lassen sich bis ca. 2000 Nutzkanäle über einen einzigen 64 kbit/s-Zeichengabekanal steuern. Die resultierende nutzkanalunabhängige Zeichengabe ermöglicht Dienste, welche losgelöst von der Nutzung einer durchgeschalteten Verbindung realisiert werden. Dieses vom Nutzkanalnetz unabhängige Zeichengabenetz folgt dem Standard des *Zentrales Zeichengabesystems Nr. 7* (ZGS Nr. 7). Einen Überblick über die Strukturierung der Steuerungsfunktionen und die verwendeten Protokolle bietet die ITU-Empfehlung Q.700 [101].

Das zentrale Zeichengabesystem Nr. 7 bildet die Grundlage für die unterschiedlichsten Steuerungsaufgaben. Neben der Steuerung von ISDN-Diensten wird auch die Steuerung von Verbindungen in Mobilfunknetzen und die Steuerung von zentralen Dienste- und Daten-Servern unterstützt.

Komponenten des ZGS Nr. 7

Beim ZGS Nr. 7 handelt es sich um ein eigenständiges logisches Netz, das vom Nutzkanalnetz streng getrennt ist. Auch die Verarbeitung der Zeichengabenachrichten innerhalb von Vermittlungsknoten – bis hin zur Ablaufumgebung der Steuerprozesse – ist streng von der Behandlung der Nutzdaten getrennt. Das Zusammenwirken des Nutzkanal-Netzes und des Zeichengabenetzes wurde bereits in Bild 2-6 veranschaulicht. Die Komponenten des Zwischenamts-Zeichengabesystems lassen sich wie folgt kurz zusammenfassen:

- *Zeichengabepunkte* (Signalling Point, SP) stellen die Knoten des Zeichengabenetzes dar. Es kann sich dabei um Vermittlungsstellen (VSt) oder andere Netzknoten (z. B. spezielle zentrale Datenbanken oder Diensteserver) handeln. Jedem Zeichengabepunkt ist eine

netzweit eindeutige Adresse (Signalling Point Code, SPC) zugeordnet. Es werden zwei Arten von Zeichengabepunkten unterschieden:

- *Zeichengabe-Endpunkte* (Signalling End Point, SEP) erzeugen oder interpretieren und verarbeiten anwendungsabhängige Steuerungsdaten z. B. zum Auf- und Abbau von Nutzkanalverbindungen. Zeichengabebeziehungen bestehen immer zwischen Zeichengabe-Endpunkten.
- *Zeichengabe-Transferpunkte* (Signalling Transfer Point, STP) dienen zur reinen Vermittlung von Zeichengabenachrichten zwischen verschiedenen Zeichengabestrecken ohne Auswertung anwendungsabhängiger Zeichengabeinformation. STPs können sowohl in SEPs integriert sein als auch in Form eines leistungsfähigen Zeichengabevermittlungssystems auf einer eigenständigen Plattform basieren. STPs realisieren Funktionen bis zur Schicht 3 des OSI-Referenzmodelles (Vermittlungsschicht).

- *Zeichengabestrecken* oder Zeichengabekanäle verbinden benachbarte Zeichengabepunkte. Sie belegen meist einen oder mehrere Zeitkanäle eines Übertragungssystems, welche exklusiv für die Zeichengabe reserviert und über Management-Funktionen innerhalb der Netzknoten eingestellt werden. Die Einrichtung von Zeichengabekanälen orientiert sich am Bedarf. Die Topologie des Zeichengabenetzes kann, bedingt durch die nutzkanalunabhängige Zeichengabe, von der des Nutzkanalnetzes abweichen.

- *Zeichengabenachrichten* dienen als Transportbehältnisse für Zeichengabeinformation von Steuerungsanwendungen und werden transparent zwischen entfernten Zeichengabepunkten vermittelt. Zeichengabenachrichten sind vergleichbar mit Protokolldateneinheiten des OSI-Referenzmodells.

Die Funktionen innerhalb von Zeichengabepunkten und zugehörige Protokolle zur Koordination verschiedener Zeichengabepunkte zur verteilten Realisierung der Steuerungsdienste des ZGS Nr. 7 werden im nächsten Abschnitt näher vorgestellt.

Funktionsschichten und Protokolle des ZGS Nr. 7

Die Funktionen innerhalb von Zeichengabeknoten lassen sich nach dem Vorbild des OSI-Referenzmodelles funktional untergliedern. Die Grundlage des ZGS Nr. 7 bildet ein einheitliches Nachrichtentransfersubsystem (Message Transfer Part, MTP), das seinen Anwendern (MTP-Dienst-Nutzern) den gesicherten Austausch von Zeichengabenachrichten zwischen Zeichengabeknoten ermöglicht (vgl. Bild 2-11).

Der *MTP* bietet seinen Anwendern (SCCP, ISDN User Part, etc.) den Transport von Zeichengabenachrichten über das Zeichengabesystem Nr. 7 zu einem Ziel-Zeichengabeknoten und dort zu einem Anwender des MTP an. Das Nachrichtentransfersubsystem umfaßt Zugangsfunktionen zu einem physikalischen Zeichengabekanal (*Signalling Link Functions*), Funktionen zur gesicherten Übertragung von Zeichengabenachrichten über eine Zeichengabestrecke (*Signalling Link Functions*) sowie Funktionen zur Nachrichtenlenkung und zur Verteilung von Nachrichten an die verschiedenen Anwenderteile im Zielknoten (*Signalling Network Functions*). Die Nachrichtenlenkung basiert auf der Adresse des Zielknotens (Destination Point Code, DPC). Die Verteilung von Nachrichten an die Anwenderteile basiert auf dem sogenannten Diensteindikator (Service Indicator, SI). Es sind codierungsbedingt 16 Anwender des MTP unterscheidbar. Im Rahmen dieser Arbeit sind als Anwender des MTP insbesondere der ISDN-User Part und der Signalling Connection Control Part interessant. Diese sind mit Hilfe der Dienstindikatoren SI_{ISUP} (Code 5) und SI_{SCCP} (Code 3) durch den MTP adressierbar [102].

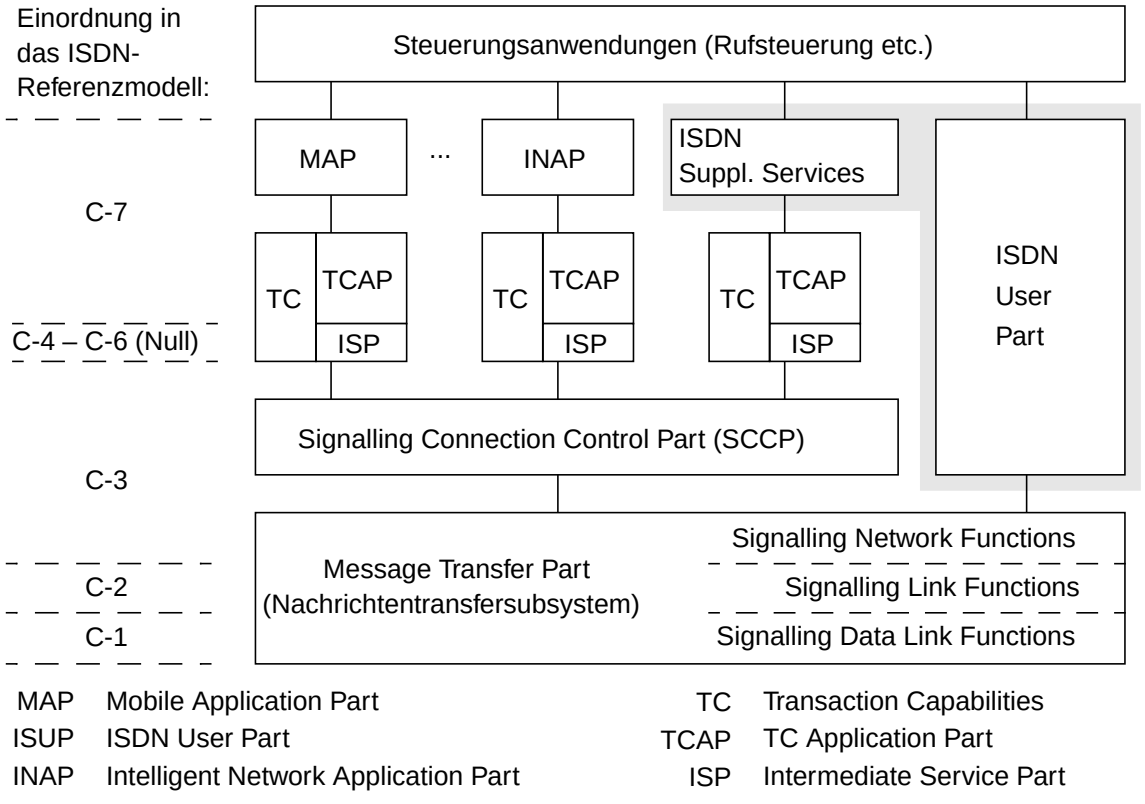


Bild 2-11: Funktionsschichten und Protokolle des ZGS Nr. 7

Auch die betriebs- und sicherheitstechnische Steuerung des Zeichengabenetzes wird durch den MTP gesteuert. Dazu zählen u. a. das Herstellen von Ersatzschaltungen bei Ausfall von Zeichengabestrecken und das Management von Zeichengabepunkten und -strecken. Die Zeichengabeprotokolle und die Funktionen des MTP sind in den Empfehlungen Q.701 bis Q.710 festgelegt.

Der für die Steuerung im ISDN wichtigste Anwender des MTP ist der *ISDN User Part* (ISUP, siehe Empfehlungen Q.761 [105] ff.). Er dient zum abschnittsweisen Auf- und Abbau von Nutzkanalverbindungen. Dabei werden Zeichengabenachrichten zwischen ISDN User Parts benachbarter Vermittlungsstellen ausgetauscht, um einen Nutzkanal zwischen diesen Knoten zu schalten beziehungsweise auszulösen. Der ISUP nutzt zum Austausch von Zeichengabenachrichten den Datendienst des MTP. Er kann, bedingt durch die Art der Auswertung von Zielrufnummern, nur benachbarte Zeichengabeknoten adressieren. Sollen mit dem ISUP Zeichengabeinformationen zwischen entfernten Zeichengabepunkten (z. B. Teilnehmervermittlungsstellen) ausgetauscht werden, so müssen diese in allen zwischenliegenden Zeichengabepunkten auf Anwendungsebene (ISUP und Rufsteuerung) interpretiert und behandelt werden. Die Behandlung von Zeichengabenachrichten innerhalb von Zeichengabeknoten ist jedoch aufwendig.

Deshalb wurde eine Funktionsschicht definiert, welche die Dienste des MTP ergänzt und seinen Anwendern zusätzliche Dienste zum verbindungslosen und verbindungsorientierten Austausch von Zeichengabenachrichten zwischen beliebigen Zeichengabepunkten anbietet. Diese Funktionsschicht – *Signalling Connection Control Part* (SCCP) genannt – ermöglicht insbesondere die direkte Adressierung entfernter Zeichengabepunkte, ohne die Einbeziehung von Anwenderteilen zwischenliegender Zeichengabepunkte. Somit werden vor allem die zwischen

Ursprungs- und Ziel-Zeichengabepunkt liegenden Zeichengabepunkte entlastet; von ihnen werden lediglich Funktionen eines Zeichengabe-Transferpunktes benötigt.

Zusammen mit dem MTP bietet der SCCP die Dienste der OSI-Schicht 3 (Netzwerkschicht) an. Der SCCP adressiert seine Anwender über sogenannte Subsystem-Nummern (Subsystem Number, SSN). Für die in Bild 2-11 dargestellten SCCP-Anwender sind beispielsweise die Subsystem-Nummern SSN_{ISS} (Code 11), SSN_{MAP} (Code 5) und SSN_{INAP}[7] definiert [103]. Entfernte Anwenderteile können über einen sogenannten Global-Title adressiert werden. Eine Global-Title-Adresse muß innerhalb des SCCP aufgelöst und in eine vom MTP verwendbare Adresse umgewandelt werden. Gegebenenfalls kann die Global-Title-Adresse nur teilweise innerhalb des SCCP des Ursprungs-Zeichengabepunktes aufgelöst werden. In diesem Fall muß auf dem Weg zum Ziel-Zeichengabepunkt mindestens ein weiterer SCCP durchlaufen werden, der die Global-Title-Adresse (teilweise) weiter auflöst. Die (teilweise) Umsetzung von Global-Title-Adressen in MTP-Adressen erfolgt durch den SCCP innerhalb der Zeichengabeknoten mit Hilfe von Datenbanken. Die Protokolle und Funktionen des SCCP sind in den Empfehlungen Q.711 bis Q.714 näher beschrieben.

Der sogenannte *Transaktions-Anwendungsteil (TCAP)* enthält Funktionen und Prozeduren zur Übermittlung von anwendungsunabhängigen, nicht nutzkanalbezogenen Steuerinformationen zwischen verschiedenen Zeichengabepunkten. Der TCAP arbeitet auf der Basis von Operationen, welche auf entfernten Netzknoten angestoßen werden können und Rückmeldungen von Ergebnissen dieser Operationen an den Initiator. Die Übermittlung von Daten zwischen Anwendungsteilen in unterschiedlichen Zeichengabepunkten basiert auf dem verbindungslosen Datenübermittlungsdienst des SCCP.

Die Funktionen des TCAP sind auf der Anwendungsschicht (Schicht 7 des OSI-Referenzmodells) einzuordnen und in Form von Anwendungsdienstfunktionen (Application Service Element, ASE) strukturiert. Der TCAP läßt sich weiter strukturieren in Funktionen

- zur Behandlung von Komponenten und Dialogen (*Component Sublayer*). Die *Dialogsteuerung* ermöglicht es, bei parallel ablaufenden Operationen (z. B. Datenbank-Abfragen) die entsprechenden Ergebnisse eindeutig einer Operation zuzuordnen. In den sogenannten *Komponenten* werden Operationen (und zugehörige Parameter) zur Ausführung auf entfernten Zeichengabepunkten codiert.

- zur Transaktionssteuerung (*Transaction Sublayer*). Diese enthält Funktionen zum Austausch von Nachrichten, mit denen Komponenten (Operationen, Parameter) transportiert bzw. Dialoge gesteuert werden können.

Eine dritte Unterschicht, der sogenannte *Intermediate Service Part (ISP)*, umfaßt Funktionen der Schichten 4 bis 6 des OSI-RM, welche durch den MTP, SCCP und TCAP nicht abgedeckt sind. Der ISP wurde bisher nicht näher spezifiziert, da bestehende TCAP-Anwender mit verbindungslosen Netzdiensten (SCCP, MTP) auskommen. Sollte in Zukunft verstärkt Bedarf nach der Übertragung großer Datenmengen über den TCAP entstehen, so können verbindungsorientierte Protokolle innerhalb des ISP spezifiziert werden.

7 Die Subsystem-Nummer(n) zur Adressierung des INAP sind Netzbetreiber-spezifisch. Das INAP ist folglich netzübergreifend ausschließlich über die Global-Title-Adressierung des SCCP ansprechbar. Am Netzübergang zum Zielnetz müssen die Zieladresse des Zeichengabe-Endpunktes sowie die jeweilige Subsystem-Nummer aus der Global-Title-Adresse bestimmt werden. Im Netz der Deutsche Telekom AG wird gegenwärtig für das INAP die Subsystemnummer 0xF1 verwendet [82].

Die Funktionen zum Austausch von Zeichengabenachrichten über mehrere Zwischenknoten, z. B. zur Nutzkanal-unabhängigen Steuerung von Dienstmerkmalen zwischen Teilnehmervermittlungsstellen, sind im Anwendungsteil *ISDN Supplementary Services* (ISS) [104] zusammengefaßt. Die ISS greifen zum Austausch von Zeichengabenachrichten auf die Dialogsteuerung des TCAP zurück. Sie enthalten beispielsweise das Nutzkanal-unabhängige Dienstmerkmal „Rückruf Bei Besetzt“. Zu dessen Steuerung werden Zeichengabenachrichten direkt zwischen Ursprungs- und Zielvermittlungsstelle – ohne Einbeziehung von ISDN-Anwenderteilen zwischenliegender Vermittlungsstellen – ausgetauscht. Die ISS greifen zur Adressierung entfernter Zeichengabe-Knoten auf die Global-Title-Adressierung des SCCP zurück. Die Rufsteuerung im ISDN bedient sich sowohl der Dienste des ISUP zum Auf- und Abbau von ISDN-Verbindungen, als auch der Dienste der ISS zur Steuerung von ISDN-Dienstmerkmalen.

Das *Intelligent Network Application Protocol* (INAP[8]) dient zur Integration von Dienstefunktionen zentraler Dienste-Server in die Dienstesteuerung im ISDN. Die zugehörigen Komponenten und Schnittstellen werden im nächsten Abschnitt näher beleuchtet, da sie zentrale Bedeutung bei der Einführung neuer Dienstefunktionen (z. B. zur Realisierung oder Unterstützung von Sicherheitsdiensten) besitzen.

Der *Mobile Application Part* (MAP) unterstützt die Dienste-Steuerung mit Funktionen zur Mobilitätsverwaltung in digitalen Mobilfunknetzen. Er unterstützt die Ermittlung des Aufenthaltsortes eines mobilen Teilnehmers und den Austausch von Daten zur Identifikation eines mobilen Teilnehmers und zur Zugriffskontrolle.

2.4.3 Komponenten und Zeichengabeschnittstellen des Intelligenten Netzes

Zur schnellen und kostengünstigen Einführung neuer Dienste, zur flexiblen Steuerung und zum einfachen Management von Diensten werden zugehörige Steuerungsfunktionen auf zentralen Zeichengabe-Knoten implementiert und bei Bedarf über spezielle Zeichengabeschnittstellen in die Dienstesteuerung im ISDN einbezogen (Dienststeuerknoten siehe Bild 2-2).

Zukünftig sollen Dienstesteuerungsfunktionen und Vermittlungsfunktionen streng getrennt werden. Die Vermittlungsfunktionen werden innerhalb der Vermittlungsstellen verbleiben. Diese Funktionen ändern sich, wenn von der Fehlerbeseitigung abgesehen wird, nicht häufig und müssen schnell verfügbar sein.

Über die einfache Verbindungssteuerung hinausgehende Dienstefunktionen (Rufnummernumwertung, zielabhängige Rufansteuerung etc.) sollen in zentralen Dienste-Servern als sogenannte Dienststeuerlogik realisiert werden, damit sie von zentraler Stelle aus gepflegt sowie schnell und flächendeckend eingeführt und weiterentwickelt bzw. deaktiviert werden können.

Zur Einbeziehung zentraler Dienststeuerlogik (Service Control Functions, SCF) wird die Rufsteuerung innerhalb der Vermittlungsstellen an bestimmten Stellen unterbrochen. Das dafür gegenüber herkömmlichen Rufmodellen erweiterte Rufmodell, welches die Unterbrechung eines ISDN-Rufes und die Einbeziehung der Dienststeuerlogik ermöglicht, wird *Basic Call State Model* (BCSM) genannt und bildet die Grundlage des Intelligenten Netzes. Die Abarbeitungspunkte innerhalb eines Rufes, an denen Unterbrechungen stattfinden können, werden

8 In der Literatur wird sowohl die Bezeichnung Intelligent Network Application Part als auch Intelligent Network Application Protocol verwendet. Hier wird der Begriff Application Part (bzw. Anwenderteil) im Zusammenhang mit den Funktionsschichten des ZGS Nr. 7 verwendet. Steht die Interaktion von Komponenten des IN im Mittelpunkt, so wird der Begriff Application Protocol (bzw. Protokoll) verwendet.

Detection Points (DP) genannt. Bild 2-12 zeigt das ISDN und die zusätzliche Infrastruktur des Intelligenten Netzes sowie die Zeichengabeschnittstellen zur Einbeziehung zugehöriger Dienststeuerlogik in die Dienstesteuerung des ISDN.

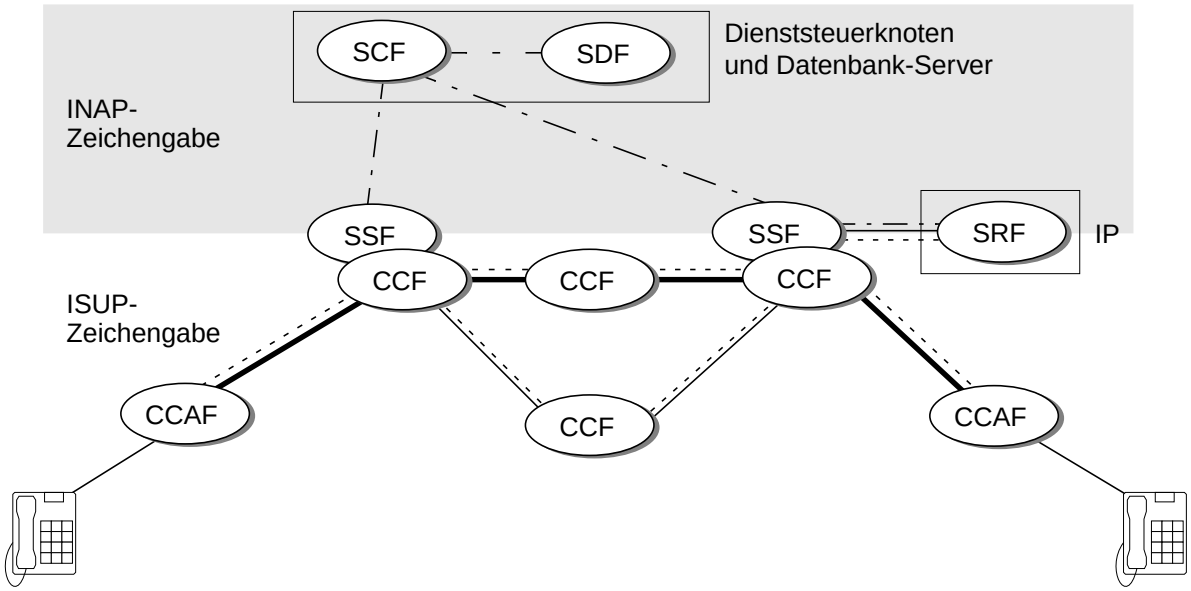


Bild 2-12: Funktionsgruppen und Zeichengabe-Schnittstellen des Intelligenten Netzes

Die *Call Control Function* (CCF) stellt die herkömmliche Rufsteuerung innerhalb der Vermittlungsstellen dar. Die *Call Control Agent Function* (CCAF) beinhaltet zusätzlich die Steuerung der Benutzer-Netzschnittstelle und entspricht der Rufsteuerung einer ISDN-Teilnehmervermittlungsstelle (TVSt). Nachfolgend werden die mit dem IN neu eingeführten Funktionsgruppen der Steuerungs-Ebene kurz dargestellt:

Die Unterbrechung der Rufsteuerung innerhalb der Vermittlungsstellen und die zeitweise Übergabe der Dienstesteuerung an den Dienststeuerknoten werden durch die *Service Switching Function* (SSF) gesteuert. Die SSF muß in jenen Zeichengabepunkten integriert sein, von denen ausgehend IN-Dienstefunktionen in die Rufsteuerung einbezogen werden sollen.

Die *Service Control Function* (SCF) bezeichnet die eigentliche zentrale Dienststeuerlogik, die in die gewöhnliche Rufsteuerung einbezogen werden soll. Gegenwärtig sind beispielsweise Funktionen zur zeit- oder ursprungsabhängigen Bestimmung einer Zielrufnummer sowie Ansagedienste verfügbar. Die Zielrufnummer wird dabei nicht mehr vom rufenden Teilnehmer, sondern während des Verbindungsaufbaus von der SCF bestimmt. Dazu wird der Ruf nach Erhalt der gewählten Rufnummer unterbrochen und, falls die Rufnummer einem IN-Dienst entspricht, diese Rufnummer durch die SSF an die zentrale SCF übergeben. Die zentrale SCF bestimmt daraufhin die Zielrufnummer und übergibt sie als Grundlage der Vervollständigung des Verbindungsaufbaus an die SSF.

Zur Abarbeitung der Dienststeuerlogik greift die SCF auf eine Datenbank zurück. Diese Datenbank ist über die *Service Data Function* (SDF) ansprechbar. In zentralen Datenbanken können beispielsweise Benutzer-Einstellungen zur Realisierung persönlicher Dienste gespeichert werden, auf die während der Diensterbringung zurückgegriffen werden muß.

Zusätzliche Komponenten, *Intelligent Peripherals* (IP) genannt, ermöglichen eine Interaktion des Benutzers mit der SCF während der Dienste-Ausführung. Die SCF kann dem Benutzer

während dem Verbindungsaufbau eine IP-Einheit zuschalten. Dabei wird der Nutzkanal benutzt, der abschnittsweise bis zu der Vermittlungsstelle aufgebaut wurde, die den Ruf unterbrochen und die Steuerung an die zentrale Dienstefunktion (SCF) übergeben hat. Über die sogenannte *Specialized Resource Function* (SRF) kann die zentrale Dienstefunktion das Einspielen von Ansagen für den Benutzer und den Empfang von Benutzereingaben (über Tonwahl) steuern. Die SRF kann von der SSF oder SCF je nach Ausprägung über den ISUP, die D-Kanal-Protokolle oder direkt über das INAP angesprochen werden.

Weitere definierte Funktionsgruppen, z. B. zum Management von IN-Diensten (Service Management Function, SMF) oder zur Erzeugung von IN-Diensten (Service Creation Environment Function, SCEF), haben keinen direkten Einfluß auf die Dienstesteuerung.

Das INAP definiert die Operationen, die von den dargestellten Funktionsgruppen implementiert werden sowie zugehörige Übergabe- und Ergebnis-Parameter. Es wird festgelegt, welche Funktionsgruppe welche Operation von welcher Funktionsgruppe anfordern kann. Dabei werden die Beziehungen SSF $\leftrightarrow$ SCF, SCF $\leftrightarrow$ SDF, SCF $\leftrightarrow$ SRF unterschieden.

Für das IN der Deutsche Telekom AG sind die in realen Netzkomponenten implementierten Ausschnitte der IN-Funktionalität zusammen mit den betreiberspezifischen Anforderungen in der Technischen Richtlinie 163 TR 78 [83] festgelegt. Diese Richtlinie wird, schritthaltend mit der Weiterentwicklung der Komponenten und neuen Anforderungen moderner Dienste, stetig fortgeschrieben. Die Rahmenwerke für gegenwärtige Implementierungen bilden die IN-Standards der ITU (Q.12xx-Serie [114]) und des ETSI [78]. Darin sind unterschiedlichste Architekturen für die Lokalisierung der IN-Funktionsgruppen SSF, SRF, SCF und SDF und zugehörige Protokolle zum Austausch von Steuerinformation festgelegt.

Kapitel 3

Sicherheitstechnische Grundlagen

Der Schwerpunkt dieses Kapitels liegt auf der Einführung von Grundlagen der Netzsicherheit. Nach der Definition wesentlicher Begriffe in Abschnitt 3.1 werden in Abschnitt 3.2 die Sichtweisen *dualer* und *mehrseitiger* Sicherheit auf die Sicherheitsaspekte eingeführt. Diese unterstützen die Einordnung und Bewertung von Kommunikationssystemen.

Abschnitt 3.3 beschreibt Grundlagen zur Modellierung von Systemen im Hinblick auf eine sicherheitstechnische Bewertung von Telekommunikationssystemen. Abschnitt 3.4 führt den Begriff der Sicherheitsarchitektur ein. Die Sicherheitsarchitektur wird anschließend strukturiert und mit den Sichtweisen dualer und mehrseitiger Sicherheit in Beziehung gesetzt.

Den aktuellen Stand der Standardisierung innerhalb der ITU, ISO und der Internet Engineering Task Force (IETF) zeigt Abschnitt 3.5. Da die Dokumente der IETF für IP-basierte Netze an die fortlaufenden Entwicklungen angepaßt werden, wird ausschließlich auf jene Standards eingegangen, die als stabil bezeichnet werden können und die einen Bezug zu einer Sicherheitsarchitektur aufweisen.

Die Kenntnis der Grundlagen und die Anwendung der vorgestellten Methoden fördern Schutzmechanismen, die Anforderungen an Sicherheitsaspekte nachprüfbar gegen zufällige Fehler und auch gegen intelligente Angreifer erfüllen.

3.1 Definitionen und Begriffe

Anforderungen an IT-Systeme mit Bezug zur Netzsicherheit umfassen die Vertraulichkeit, Verfügbarkeit, Integrität, Zurechenbarkeit und Rechtsverbindlichkeit. Obwohl die Definition dieser sogenannten *Sicherheitsanforderungen* intuitiv klar scheint, werden die Begriffe in der Literatur häufig inkonsistent verwendet. Die Festlegung auf diese fünf Basisanforderungen, aus denen sich alle weiteren Sicherheitsanforderungen zusammensetzen lassen, wird in der Fachwelt kontrovers diskutiert. Eine anwendungsnahe Definition der Begriffe erfolgt in Abschnitt 3.2.

Sicherheitsanforderungen können nicht alleine stehen, sondern müssen – um sinnvoll interpretiert werden zu können – mit einem Wert in Beziehung gesetzt werden. Ein *Wert* (schützenswertes Gut) bezeichnet im folgenden einen Aspekt eines Systems, der für dessen korrekte Funktion von besonderer Bedeutung ist. Werte umfassen bei Telekommunikationssystemen z. B. Art und Dauer eines Kommunikationsereignisses (z. B. Telefonanruf) und Kommunikationsinhalt (übermittelte Information), Ort eines Kommunikationsereignisses sowie Identitäten der Beteiligten.

Die Kombination aus Sicherheitsanforderung und Wert wird *Schutzziel* genannt. Der Schutz vor unautorisierter Kenntnisnahme von Gesprächsinhalten stellt beispielsweise ein Schutzziel dar (Vertraulichkeit × Gesprächsinhalt). Ein *Angriff* bezeichnet eine unautorisierte Handlung einer Person mit möglicher Auswirkungen auf Sicherheitsaspekte des Systems. Ein *erfolgreicher Angriff* führt zur Verletzung eines Schutzziels innerhalb des betrachteten Systems. Ein *Angreifermodell* beschreibt die maximal (unterstellte) Stärke angenommener Angreifer, bei der die Schutzziele (bei gegebenen Schutzmaßnahmen) noch garantiert sind.

Das durch ein System garantierbare Maß an *Sicherheit* wird durch die Menge von Schutzzielen festgelegt, welche durch das System auch gegen angenommene Angreifer erreicht werden. Ein System wird bezüglich eines Betroffenen als *sicher* bezeichnet, wenn es alle Schutzziele dieses Betroffenen erfüllt. Das Attribut sicher ist folglich abhängig vom jeweiligen Bezugspunkt. Ein Kommunikationsnetz kann aus Sicht des Netzbetreibers durchaus sicher sein, obwohl es aus Sicht eines Benutzers einige Schutzziele nicht erfüllt, d. h. *nicht sicher*[1] ist.

Der *Datenschutz* befaßt sich mit dem Schutz des Persönlichkeitsrechts. Besonders wichtig ist hierbei das Grundrecht auf freie Entfaltung der Persönlichkeit und daraus abgeleitet das informationelle Selbstbestimmungsrecht: „Der einzelne soll – ohne Beschränkung auf seine Privatsphäre – grundsätzlich selbst entscheiden können, wie er sich Dritten oder der Öffentlichkeit gegenüber darstellen will, ob und inwieweit von Dritten über seine Persönlichkeit verfügt werden kann“ [56]. Das *Bundesdatenschutzgesetz* regelt den Umgang mit personenbezogenen Daten: „Zweck des Gesetzes ist es, den einzelnen davor zu schützen, daß er durch den Umgang mit seinen personenbezogenen Daten in seinem Persönlichkeitsrecht beeinträchtigt wird“ [57]. Spezielle Anforderungen an den Datenschutz aus Sicht von Multimedia und Telekommunikation werden in [58] diskutiert.

Der Begriff *Datensicherheit* wird verwendet, wenn die technische und organisatorische Umsetzung von Schutzzielen im Vordergrund stehen. Datensicherheit dient als Überbegriff für Verfahren mit dem Ziel der Erfüllung von Schutzzielen mit Bezug auf Informationsträger (z. B. Benutzer-zu-Benutzer Daten).

Netzsicherheit bezeichnet die Eigenschaft, daß ein Kommunikationsnetz und damit in Verbindung stehende Systeme wohldefinierte Schutzziele erreichen.

Zur Garantie von Schutzzielen sind neben allgemeinen technischen und organisatorischen Maßnahmen auch auf spezielle Schutzziele zugeschnittene Schutzmechanismen entwickelt worden. Diese sogenannten *Sicherheitsmechanismen* beschreiben technische und organisatorische Verfahren, die auf Werte angewendet werden, um bestimmte Schutzziele zu garantieren. Die organisatorische Einbettung von Sicherheitsmechanismen mündete beispielsweise bei der Einführung der digitalen Signatur in einem Signaturgesetz und einer zugehörigen Verordnung. Diese regeln die Rechtsverbindlichkeit von und den Umgang mit digitalen Signaturen [59]. Die technische Umsetzung dieser Verfahren resultiert in *Sicherheitsfunktionen*. Ein Beispiel stellt die Verschlüsselung von Nutzdaten vor ihrer Übermittlung über Kommunikationsnetze dar.

Der Begriff des Sicherheitsdienstes wird aus der Definition des Kommunikationsdienstes abgeleitet: Ein *Sicherheitsdienst* umfaßt alle funktionalen Eigenschaften eines Kommunikationsnetzes (inklusive Endgeräte und zentrale Server), welche zur Garantie von Schutzzielen

1 Die Attribute *sicher* und *unsicher* sind vorsichtig zu verwenden, da sie ein komplementäres Bild vorspiegeln. Eine in dieser Art komplementäre Interpretation des Sicherheitsbegriffes ist nicht angebracht, da seine Interpretation von den jeweiligen Schutzzielen der Bezugspersonen abhängig ist.

beitragen[2]. Er ist also nach den Definitionen in Kapitel 2.1 den Telediensten bzw. Mehrwertdiensten zugeordnet.

3.2 Blickwinkel der Netzsicherheit

In diesem Abschnitt werden unterschiedliche Blickwinkel der Netzsicherheit eingeführt, um eine Begriffswelt zu schaffen, anhand derer die später vorgestellten Methoden eingeordnet und bewertet werden können. Die Einführung der Sichtweisen dualer und mehrseitiger Sicherheit ([1], [3]) erfolgte in der Literatur allgemein für informationstechnische Systeme (IT-Systeme) und wird im folgenden auf Kommunikationssysteme bzw. Kommunikationsdiensteumgebungen übertragen. Die beiden gewählten Sichtweisen orientieren sich an den Bedürfnissen *aller* an einem Dienst Beteiligten. Sie bieten deshalb eine sinnvolle Perspektive im Hinblick auf eine Informationsgesellschaft, deren Bürger sich mit einer zunehmenden Substitution der herkömmlichen Kommunikationsformen (Briefe, direkte Kommunikation etc.) durch auf automatisierte IT- Systeme basierende Kommunikationsformen konfrontiert sehen.

3.2.1 Duale Sicherheit und die Beziehung Mensch-Maschine

Aus dem Blickwinkel der dualen Sicherheit werden sowohl das maschinelle IT-System mit seinen Randbedingungen als auch die Benutzer mit ihren Unzulänglichkeiten in die Sicherheitsbetrachtungen miteinbezogen. Der Begriff *duale Sicherheit* wurde von Dierstein in [1] umfassend definiert und wird im folgenden auf das Umfeld der dieser Arbeit zugrundeliegenden Kommunikationsdiensteumgebung angewendet.

Die komplementären Sichten der dualen Sicherheit – *Sicherheit vor dem System* und *Sicherheit des Systems* – dienen zur Einordnung von Sicherheitsanforderungen in solche, die durch die Interaktion mit einem informationstechnischen System entstehen (Sicherheit vor dem System) und jene, die durch die Substitution ehemals nicht maschinell erledigter Aufgaben durch automatisierte IT-Systeme, speziell durch Kommunikationsdienste entstehen (Sicherheit des Systems). Die „duale“ Sichtweise dient hier hauptsächlich als Brücke zwischen den menschlichen Benutzern (und deren Sicherheitssicht) und der innerhalb der technischen Kommunikationsdiensteumgebung diskutierten Sicherheitsdienste.

Aus Sicht der Betroffenen wird die Sicherheit vor dem System als *Beherrschbarkeit* bezeichnet. Ein Kommunikationsdienst gilt als beherrschbar, wenn die Rechte oder schutzwürdigen Belange der Betroffenen durch das Vorhandensein oder die Benutzung des Dienstes nicht unzulässig beeinträchtigt werden. Die Forderungen an einen Kommunikationsdienst und die zugrundeliegende Kommunikationsinfrastruktur lassen sich im Bezug auf den Umgang von Menschen mit diesen Diensten und Systemen wie folgt definieren:

- *Zurechenbarkeit* (Accountability) verlangt die Fähigkeit der eindeutigen Zuordnung von Ereignissen infolge der Benutzung eines Kommunikationsdienstes zu dem jeweiligen Verantwortungsträger (Initiator).

- *Rechtsverbindlichkeit* (Legal Liability) bzw. Verbindlichkeit (Liability) verlangt, daß für die Nutzung von Kommunikationsdiensten und den aus der Nutzung resultierenden Ergeb-

2 Ein Sicherheitsdienst wird i. a. aus verteilten Sicherheitsfunktionen bestehen, welche z. B. innerhalb der Endgeräte installiert werden und sich – entsprechend den herkömmlichen verteilten Dienstefunktionen – über den Austausch von Steuerinformation synchronisieren.

nissen die verantwortlichen Instanzen gegenüber Dritten beweiskräftig nachweisbar sein können müssen[3].

Verläßlichkeit beschreibt die Sicherheit, die das System während der Diensterbringung bietet. Ein IT-System gilt als verläßlich, wenn weder die Daten noch die Datenverarbeitung in ihrem Bestand, ihrer Nutzung oder ihrer Verfügbarkeit beeinträchtigt werden [1]. Forderungen an die Verläßlichkeit von Kommunikationsdiensten lassen sich wie folgt definieren:

- *Vertraulichkeit* (Confidentiality) beschreibt die Forderung nach Schutz von Information vor unautorisierter Kenntnisnahme.
- *Integrität* (Integrity) beschreibt die Forderung nach Schutz von Information vor unautorisierter und unerkannter Veränderung. Dieser Schutz kann sich auch auf Kommunikationsdienste bzw. deren Funktionalität oder auf Kommunikationsinfrastruktur allgemein beziehen.
- *Verfügbarkeit* (Availability) beschreibt die Forderung, daß Kommunikationsdienste oder damit in Verbindung stehende Netzfunktionen für den autorisierten Benutzer bei Bedarf wie vereinbart (z. B. Qualität) zur Verfügung stehen.

Die Forderungen nach dualer Sicherheit erhalten insbesondere dort Bedeutung, wo maschinelle Systeme vorhandene menschliche Tätigkeiten übernehmen oder ersetzen. Dies trifft zweifellos im hier diskutierten Falle der Kommunikationstechnik zu. Bild 3-1 veranschaulicht die komplementären Sichten der dualen Sicherheit.

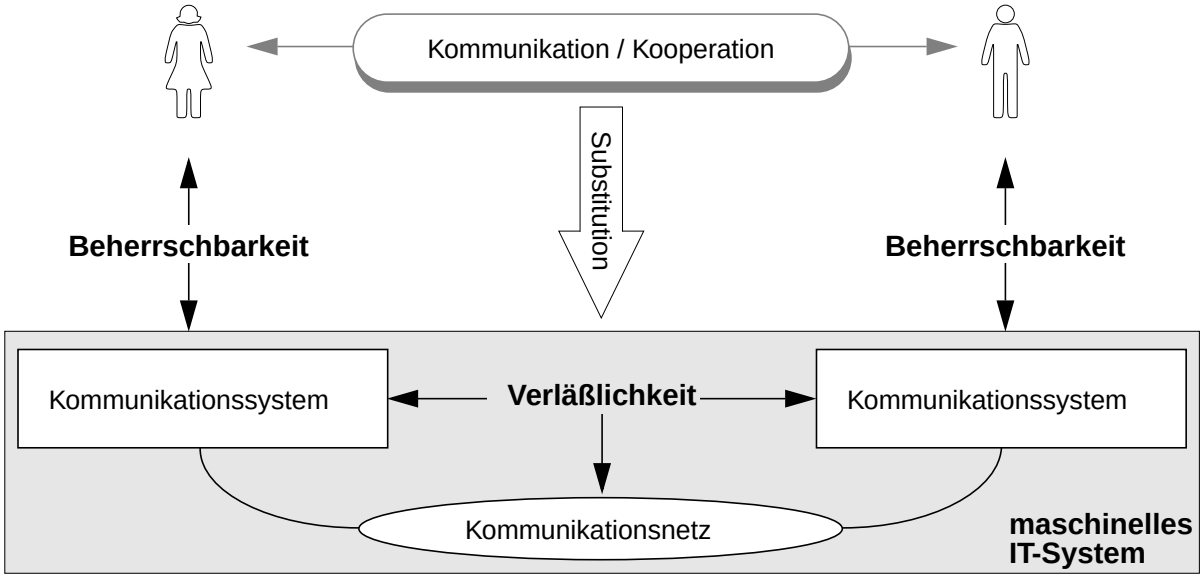


Bild 3-1: Substitutionseffekt aus dem Blickwinkel dualer Sicherheit

Eine „sichere“ Substitution ehemals menschlicher Tätigkeiten durch Benutzung maschineller Systeme setzt voraus, daß sowohl das substituierende System eine der bisherigen Tätigkeit

3 Die Rechtsverbindlichkeit von elektronischen Transaktionen wird durch das im IuKDG in Artikel 3 beschlossene Signaturgesetz (trat zum 1. August 1997 in Kraft) und die zugehörige Verordnung der Bundesregierung zur digitalen Signatur (trat zum 1. November 1997 in Kraft) unterstützt. Sich entwickelnde Infrastrukturen und organisatorische sowie rechtliche Handhabungsweisen werden diesen Aspekt der Beherrschbarkeit entscheidend prägen [6],[123],[139].

vergleichbare inhärente Sicherheit bietet und daß das substituierende System von den Benutzern beherrscht wird.

Durch diese Transformation ehemals rein menschlicher Tätigkeiten auf Kommunikationssysteme entstehen folgende Problemfelder, welche im Sinne der Beherrschbarkeit durch entsprechende Gestaltung der Technik kompensiert werden müssen, in den heutigen Systemen jedoch großteils nur unzureichend Beachtung finden:

- Die Interpretation von Benutzereingaben zur Verarbeitung durch das Kommunikationssystem ist für die Benutzer nicht notwendigerweise klar. Unter Interpretation verstehen wir die Zuweisung einer Bedeutung zu Benutzereingaben durch das Kommunikationssystem. Umgekehrt gilt selbiges für die Interpretation von Anzeigen des Kommunikationssystems durch die Benutzer.

- Verantwortung kann nicht an ein maschinelles IT-System delegiert werden. Lediglich Aufgaben können dem System übertragen werden. Folglich verbleibt die Verantwortung z. B. für die sichere Übertragung von Daten oder die vorschriftsgemäße Nutzung von Kommunikationsdiensten beim Benutzer.

- Die durch das Kommunikationssystem verarbeiteten Nutzdaten und Dienstesteuerungsdaten sowie die damit erarbeiteten Ergebnisse müssen stets für den Benutzer nachvollziehbar sein. Die Funktion von Kommunikationsdiensten muß folglich während und nach der Benutzung kontrollierbar und durch den Benutzer gegebenenfalls beeinflußbar sein.

Ein Kommunikationsdienst wird bezüglich der dualen Sicht als sicher bezeichnet, falls damit ausgeführte Aufgaben zurechenbar und rechtsverbindlich gestaltet werden können und der Dienst die an ihn gestellten Leistungsaspekte, wie z. B. geforderte Schutzziele aus den Bereichen Vertraulichkeit, Verfügbarkeit und Integrität, erfüllt. Der Kommunikationsdienst muß also im obigen Sinne beherrschbar und verläßlich sein.

Sowohl die Beherrschbarkeit als auch die Verläßlichkeit eines Kommunikationssystems sind meist nicht durch einen einzelnen Benutzer bestimmbar, da oft mehrere unabhängige Beteiligte zu einem Kommunikationsdienst beitragen (z. B. Benutzer, Dienstanbieter, Netzbetreiber). Einzig durch die Beachtung der Anforderungen aller betroffenen Personen ist eine ausgewogene Berücksichtigung ihrer Schutzziele möglich. Der nächste Abschnitt befaßt sich deshalb mit Gestaltungsaspekten von Diensten zur Berücksichtigung der Schutzinteressen aller Betroffenen und mit Voraussetzungen für eine Konsensfindung im Falle widersprüchlicher Schutzziele.

3.2.2 Mehrseitige Sicherheit in der Kommunikationstechnik

In der Kommunikationstechnik bedeutet *mehrseitige Sicherheit* die Einbeziehung der Sicherheitsanforderungen aller Beteiligten sowie das faire Austragen daraus resultierender Schutzkonflikte beim Benutzen von Kommunikationsdiensten [3].

Ein Merkmal mehrseitiger Sicherheit ist das Vorgehen zur Auflösung von Schutzkonflikten gegensätzlicher Sicherheitsanforderungen von verschiedenen Beteiligten. Es ist eine ausgewogene Berücksichtigung der Schutzinteressen aller Beteiligter anzustreben. Das Ergebnis der Aushandlung und Konfliktauflösung muß für alle Beteiligten ersichtlich und akzeptabel sein. Das Beispiel in Bild 3-2 zeigt ein Szenario für einen Datenbankzugriff über ein Kommunikationsnetz. Als Betroffene, zugleich Beteiligte, sind der Benutzer, der Netzbetreiber und der Datenbank-Dienstanbieter zu unterscheiden.

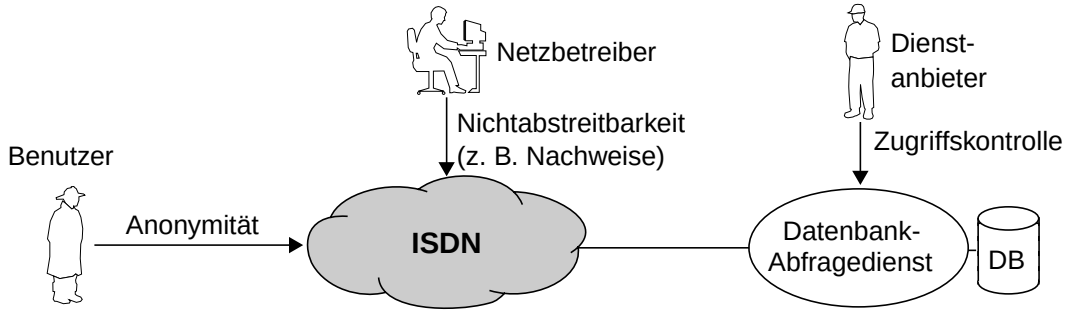


Bild 3-2: Szenario eines Datenbankzugriffes mit unterschiedlichen Schutzzielen

Im Beispiel sind vor der Dienstnutzung gemeinsame Schutzziele auszuhandeln. Der Benutzer fordert die Vertraulichkeit seiner Identität (Anonymität) gegenüber Netzbetreiber und Dienstanbieter. Der Netzbetreiber möchte das ihm zustehende Verbindungsentgelt vom Benutzer sicher erhalten, während der Dienstanbieter den Zugriff auf seine Datenbank kontrollieren muß.

Der Konflikt besteht darin, daß gängige Verfahren zur Entgeltdatenerfassung und zur Zugriffskontrolle auf der Identität des Benutzers beruhen. Das Aushandlungsergebnis könnte folgendermaßen aussehen:

- Der Benutzer greift auf das Kommunikationsnetz durch *Barzahlung oder Debitkarte* zu, somit entfällt die Notwendigkeit der Erfassung von Entgeltdaten. Die Nichtabstreitbarkeitsforderung wird deshalb aus der Menge der geforderten Schutzziele gestrichen.

- Gegenüber dem Datenbank-Dienstanbieter weist sich der Benutzer mit Hilfe eines *Pseudonyms* (eines Decknamens) aus, das er von einer ihm vertrauten Instanz erhält. Die Zugriffskontrolle kann dann auf Basis des Decknamens und der vertrauten Instanz realisiert werden. Die Spannungen zwischen Anonymität und Zugriffskontrolle werden dadurch aufgelöst, wobei die Anonymität gegenüber einer dem Benutzer und dem Dienstanbieter vertrauten Instanz vom Benutzer *bewußt* aufgegeben wird.

- Der Dienstanbieter akzeptiert, daß eine ihm nicht bekannte Person auf seine Datenbank zugreift, solange sie beweisen kann, daß die vertraute Instanz sie dazu ermächtigt hat.

Diese Art der Aushandlung und Kompromißlösung ist typisch für mehrseitig sichere Dienste und erfordert gegebenenfalls die Einbeziehung der Betroffenen. Die Aufgabe bzw. Nichtberücksichtigung von Schutzzielen muß für die Betroffenen ersichtlich und akzeptiert sein.

Die Sicherheitsanforderungen sind letztlich einzelnen Menschen und Organisationen zugeordnet, die sich zur Bewältigung ihres privaten und beruflichen Alltags moderner Telekommunikationstechnik bedienen. Sicherheit dient aber nicht nur den Kommunikationspartnern selbst, sondern auch all jenen, die mit den Partnern oder mit dem jeweiligen Kommunikationsinhalt in Beziehung stehen oder mit der Bereitstellung der Kommunikationsmittel zu tun haben [2].

Bei der Interaktion mehrerer Benutzer über Kommunikationsnetze bestehen unterschiedliche Anforderungen an die Sicherheit zugrundeliegender Kommunikationsdienste. Diese Anforderungen sind im Bereich der Verläßlichkeit und der Beherrschbarkeit des Systems angesiedelt und beziehen sich auf Werte, welche durch den Dienst geschaffen oder transferiert werden. Somit entsteht neben der Dimension der unterschiedlichen Sicherheitsanforderungen eine weitere Dimension: die Dimension der Schutzziele verschiedener Betroffener an einen Kommuni-

kationsdienst. Die an einem Kommunikationsdienst beteiligten Personen[4] lassen sich allgemein einordnen in:

- *Benutzer*: Eine Person, welche Kommunikationsdienste im betrachteten Einzelfalle nutzt.
- *Kunde*: Eine Person, welche eine vertragliche Bindung mit einem Dienstanbieter oder Netzbetreiber eingeht. Dem Kunden wird das Entgelt für die Dienstnutzung zugeordnet. Kunde und Benutzer können, müssen aber nicht identisch sein.
- *Netzbetreiber*: Eine Person, welche die Netztechnik zur Verfügung stellt, betreibt und wartet, auf der Kommunikationsdienste angeboten werden.
- *Dienstanbieter*: Eine Person, welche Kommunikationsdienste anbietet und dazu u. a. Infrastruktur des Netzbetreibers nutzt.
- *Hersteller*: Eine Person, welche Kommunikationsinfrastruktur herstellt.

Der Begriff des *Betroffenen* umfaßt sowohl Personen, die aktiv einen Dienst nutzen als auch Personen, die durch den Dienst beeinflußt werden. Dabei kann es sich beispielsweise um Dritte handeln, deren Daten mit Hilfe von Kommunikationsdiensten übertragen werden.

Ein *mehrseitig sicherer Kommunikationsdienst* berücksichtigt die Schutzziele aller Betroffenen in ausgewogener Weise. Dazu muß jeder Betroffene beteiligt werden können, um gegebenenfalls aktiv am Aushandlungsprozeß teilzunehmen.

3.2.3 Schutzziele mehrseitig sicherer Kommunikationsdienste

Im folgenden werden einige wichtige Schutzziele dargelegt, die im Sinne der mehrseitigen Sicherheit von Kommunikationsdiensten erfüllt werden müssen. Sie entstammen Ergebnissen langer Diskussionen [3] und stellen den aktuellen Stand einer fortdauernden Entwicklung dar. Somit werden sich die Schutzziele und zugeordnete Schutzmechanismen mit den Anwendungen weiterentwickeln. Diesem Umstand ist durch Gestaltungsmaßnahmen bei der Integration von Sicherheitsfunktionen in Kommunikationsnetze, z. B. durch Anbieten von Optionen, Rechnung zu tragen.

I. Schutzziele bezüglich der *Verläßlichkeit* von Kommunikationsdiensten und zugehöriger Kommunikationsinfrastruktur:

- Schutzziele zur Vertraulichkeit (Confidentiality)

  C1: *Nutzdaten* (Kommunikationsinhalte) sollen vor allen Instanzen außer dem (oder den) Kommunikationspartner(n) vertraulich bleiben können.

  C2: *Dienstesteuerungsdaten* sollen vor allen Instanzen, außer den jeweils verarbeitenden Dienstefunktionen, vertraulich bleiben können. Bei Dienstesteuerungsdaten kann es sich beispielsweise um Rufnummern der Benutzer oder Aufenthaltsorte bei mobilitätsunterstützenden Netzen handeln.

  C3: *Zustandsdaten der Kommunikationsinfrastruktur*, aus denen schützenswerte Daten abgeleitet werden können (z. B. ein Verbindungsweg oder die Tatsache, daß eine Kommunikation stattfindet), sollen vermieden werden können oder auf den Teil der

4 Der Begriff „Person“ umfaßt sowohl natürliche als auch juristische Personen. Es können mehrere Personen derselben Kategorie an einem Kommunikationsdienst beteiligt sein, z. B. mehrere Benutzer oder Netzbetreiber.

Infrastruktur beschränkt werden, der die Schutzziele der jeweils betroffenen Personen garantieren kann.

C4: *Benutzer von Kommunikationsdiensten* sollen voreinander anonym bleiben können, und Unbeteiligte (inklusive Netzbetreiber und Dienstanbieter) sollen dann nicht in der Lage sein, sie zu beobachten.

- Schutzziele zur Integrität (Integrity)

  I1: Fälschungen von Daten (inklusive des Absenders) sollen erkannt werden können. Dies betrifft sowohl *Dienstesteuerungsdaten* zur Aushandlung einer Verbindung (z. B. Rufnummern) oder zur Steuerung von Mehrwertdiensten als auch *Nutzdaten*.

  I2: Fälschungen von *Kommunikationsdiensten* (Manipulationen) dürfen gegenüber Betroffenen nicht unerkannt bleiben.

  I3: Die *Identitäten* der an einem Kommunikationsdienst beteiligten Personen müssen für alle Betroffenen prüfbar sein. Unter Beteiligten werden Personen verstanden, die als Benutzer direkt oder in ihrer Verantwortung für Netzinfrastruktur indirekt an einem Kommunikationsdienst teilnehmen.

  I4: *Kommunikationsinfrastruktur* und *Kommunikationsdienste* müssen vor Mißbrauch geschützt sein.

- Schutzziele zur Verfügbarkeit (Availability)

  A1: *Kommunikationsdienste* und mit ihrer Benutzung verknüpfte *Informationen* müssen allen Partnern, die dies wünschen und denen die Kommunikation nicht verboten ist, in vereinbarter Qualität zur Verfügung stehen.

  A2: *Kommunikationsdienste* müssen gegen Fehler robust sein. Bei zusammengeschalteten Kommunikationsnetzen sollen die einzelnen *Kommunikationsnetze* autonom sein.

II. Schutzziele bezüglich der *Beherrschbarkeit* von Kommunikationsdiensten und zugehöriger Kommunikationsinfrastruktur:

- Schutzziele zur Zurechenbarkeit (Accountability)

  Z1: Die Nutzung eines Kommunikationsdienstes muß den Benutzern zurechenbar sein können. Ebenso muß die Kommunikation bestimmter Inhalte einem Sender und den Empfängern zuordenbar sein können.

  Z2: Niemand darf dem Netzbetreiber bzw. Dienstanbieter *Entgelte* für erbrachte Dienstleistungen vorenthalten – zumindest erhält der Netzbetreiber bei der Inanspruchnahme von Kommunikationsdiensten entsprechende *Beweismittel*, sofern das Entgelt später eingefordert werden muß.

- Schutzziele zur Rechtsverbindlichkeit (Legal Liability)

  R1: *Kommunikationsumstände* (z.B. ausgehandelte Schutzziele, beteiligte Personen) und *Kommunikationsinhalte* müssen gegenüber Dritten rechtskräftig nachgewiesen werden können. Die Tatsache, daß ein Kommunikationsdienst rechtsverbindlich in Anspruch genommen wird, ist selbst Teil des Kommunikationsumstandes. Die Rechtsverbindlichkeit muß deshalb in die Aushandlung der durch einen Kommunikationsdienst garantierten Schutzziele miteinbezogen werden und kann nicht für zurückliegende Kommunikationsereignisse hergestellt werden[5].

Jeder Betroffene kann weitere Schutzziele mit der Inanspruchnahme oder Unterstützung eines Kommunikationsdienstes verbinden. Die zugrundeliegenden zusätzlichen Schutzmechanismen sollten für jeden Kommunikationsvorgang optional einforderbar bzw. aushandelbar sein oder durch Voreinstellung festgelegt werden können.

3.3 Modelle für die Bewertung der Sicherheit von Systemen

Während die Bewertung eines Kommunikationsnetzes oder eines Kommunikationsdienstes aus netztechnischer Sicht (Leistungsfähigkeit, Dienstqualität, Ressourcenbelegung, etc.) seit langem beherrscht und praktiziert wird, sind die Grundlagen für eine sicherheitstechnische Bewertung von Kommunikationsnetzen oder Kommunikationsdiensten noch nicht einheitlich festgelegt. Deshalb werden in diesem Abschnitt jene Begriffe eingeführt und veranschaulicht, die für die sicherheitstechnische Bewertung im weiteren Verlauf der Arbeit notwendig sind.

3.3.1 Angreifermodelle – Sicht der Angreifer

Ein *Angreifer* beschreibt eine Instanz (i. a. eine Person), welche eine unautorisierte Handlung, d. h. einen *Angriff*, gegen ein System durchführt, die im Erfolgsfall zur Verletzung eines Schutzzieles führt.

Ein *Angreifermodell* (oder Angriffsmodell) beschreibt die Attribute angenommener Angreifer, die bei der Sicherung eines Systems berücksichtigt werden. Es bildet die Grundlage für die Sicherheitsbewertung eines zugrundeliegenden Systems. Wesentliche Charakteristiken eines Angreifers umfassen:

- Die **Motivation** eines Angreifers läßt Rückschlüsse darauf zu, ob ein Angreifer vorhandenes Angriffspotential nutzen wird oder nicht. Motivationsfaktoren umfassen:
  - *Gewinnerwartung* für den Angreifer im Erfolgsfalle bzw. *Aufwand-Nutzen-Verhältnis*; das Aufwand-Nutzen-Verhältnis kann durch künstliche Angreifer bestimmt werden, die vom Verantwortlichen für Systemsicherheit beauftragt werden[6]
  - *Selbstdarstellung* durch herausragende Erfolge innerhalb einer Gemeinschaft
  - Befriedigung von *Rachegelüsten*, z. B. bei vor der Entlassung stehenden oder unzufriedenen Mitarbeitern
  - Befriedigung des *Spieltriebs* eines Angreifers
- Das **Systemwissen** eines Angreifers entscheidet letztlich, ob dieser einen Zugriffspunkt am System identifizieren kann, an dem ein erfolgversprechender Angriff möglich ist. Auch die Durchführung eines Angriffs verlangt meist einen aktiven Eingriff in das System und ist stark vom Systemwissen des Angreifers abhängig. Systemwissen kann beispielsweise durch praktische Erfahrungen oder mit Hilfe von Fachliteratur erworben werden.
- Die **technische Angreiferstärke** entscheidet darüber, ob ein Angreifer eine im System vorhandene Schwachstelle ausnutzen kann. Die Durchführbarkeit eines erfolgversprechenden Angriffes hängt u. a. von folgenden Gegebenheiten ab:
  - Zugangsmöglichkeiten des Angreifers zum angegriffenen System,

5 Die Betroffenen müssen in diesen Fällen über die Rechtsverbindlichkeit informiert und sich der dabei entstehenden Verbindlichkeiten bewußt sein. Dieses ist u. a. durch entsprechende Mechanismen an der Mensch-Maschine-Schnittstelle zu garantieren [4].

6 siehe IBM/Tigerteams, Sicherheitsberater, Penetration-Tests bei Firewalls

- Verfügbarkeit technischer Geräte und Erfahrungen mit deren Bedienung,
- Zeit zur Vorbereitung und Durchführung von Angriffen,
- Verfügbarkeit finanzieller Mittel zur Durchführung von Angriffen bzw. zur Beschaffung von Angriffsgeräten oder Systeminformationen.

In dieser Arbeit wird vor allem die technische Angreiferstärke als Maß für die Angreiferstärke genutzt, die zur Durchführung eines erfolgreichen Angriffes notwendig ist. Die anderen Faktoren (auch „weiche“ Faktoren genannt) sind aus technischer Sicht nicht greifbar und müssen von Fall zu Fall neu bestimmt werden.

Abgeleitete Anforderungen an eine Sicherheitsarchitektur: Eine Sicherheitsarchitektur für offene Kommunikationsdiensteumgebungen muß flexibel genug sein, um sehr unterschiedliche Anwendungen mit individuellen Schutzzielen unterstützen zu können. Insbesondere sollte die Architektur keine Annahmen über die „weichen“ Faktoren treffen. Dienste einer Sicherheitsarchitektur können z. B. durch optional schaltbare Schutzmechanismen und abgestufte Mechanismenausprägungen unterschiedlicher Stärke (z. B. unterschiedliche Schlüssellängen oder Kryptographie-Algorithmen) der jeweiligen Situation angepaßt werden.

3.3.2 Vertrauensbereiche – Sicht der Betroffenen

Vertraut ein Benutzer einem technischen Gerät, so beschreibt dies, daß dieser von dessen erwartungsgemäßer Funktion ausgeht, obwohl er nicht genügend Informationen besitzt, um dieses nachvollziehbar und sicher vorhersagen zu können.

Innerhalb eines *Vertrauensbereiches* werden keine Angreifer angenommen. Ein Vertrauensbereich beschreibt einen – bezüglich der Sicherheitsaspekte atomaren – Bereich, dem von einer Person vertraut wird im Hinblick darauf, daß die Schutzziele dieser Person darin erfüllt sind. Die Bestimmung und Abgrenzung von Vertrauensbereichen beruht auf Annahmen, die für die Bewertung eines Systems getroffen werden und von den einzelnen Betroffenen abhängen. Vertrauensbereiche sind insbesondere in hochkomplexen Umgebungen (z. B. Kommunikationsdiensteumgebungen) essentiell, da nicht davon ausgegangen werden kann, daß jeder Teilnehmer die Vorgänge im gesamten System nachvollziehen kann.

Da kein technisches System gegen allmächtige Angreifer gesichert werden kann, spielen Vertrauensbereiche auch eine wichtige Rolle bei der Lokalisierung von Sicherheitsfunktionen. Sie bilden einen wichtigen Ausgangspunkt für Sicherheitsbewertungen. Bei der sicherheitstechnischen Bewertung von Systemen wird davon ausgegangen, daß Sicherheitsfunktionen innerhalb von Vertrauensbereichen vor Manipulationen und Ausspähung geschützt sind. Innerhalb von Vertrauensbereichen wird die Wirksamkeit installierter Sicherheitsfunktionen angenommen. Ausgehend von dieser Annahme sind weitere Sicherheitseigenschaften des Systems über Angreifermodelle und Wirkungen von Schutzfunktionen ableitbar.

Um ein solches Vertrauen zu rechtfertigen, werden augenblicklich größte Anstrengungen von Hardware- und Software-Herstellern unternommen. Beispielsweise werden Chipkarten gebaut, die gegen Ausspähung und Manipulation schützen sollen und deren Entwicklungsprozeß hohen Sicherheitsanforderungen genügt [67]. Gleichzeitig machen sich Forschergruppen in aller Welt auf, diesen angeblichen Manipulationsschutz auf die Probe zu stellen.

Aufgrund der Abhängigkeit heutiger Chipkarten von externer Spannungs-, Strom- oder Systemtakt-Versorgung werden auch autonome Module entworfen (z. B. integriert in Armbanduhren), deren Sicherheitsmechanismen weitgehend unabhängig von ihrer Umgebung sind.

Beispiele für Vertrauensbereiche in Form mobiler sicherer Module (z. B. zur Speicherung und Nutzung geheimer Signaturschlüssel) werden in [15] diskutiert.

In einer Kommunikationsdiensteumgebung muß folglich eine flexible, benutzerorientierte Definition von Vertrauensbereichen unterstützt werden. Es muß aushandelbar sein, welche Schutzfunktionen in welchen Systemen in Konsequenz ausgehandelter Schutzziele aktiviert werden. Insbesondere bei der Benutzung von komplexen Endgeräten müssen Schutzfunktionen außerhalb des Endgerätes (z. B. in Chipkarten) sinnvoll in den Kommunikationsdienst einbezogen werden können.

3.3.3 Bedrohungsmodelle – Systemsicht

Eine *Bedrohung* beschreibt Schwachstellen eines Systems, an denen ein erfolgreicher Angriff auf Schutzziele angesetzt werden kann. Ein Bedrohungsmodell liefert Kriterien zur Klassifizierung von Bedrohungen und zur Analyse von Systemen im Hinblick auf bestehende Bedrohungen.

Bedrohungen werden auch als Angriffspotential bezeichnet. Sie bilden den Ausgangspunkt für erfolgreiche Angriffe. Die Eintrittswahrscheinlichkeit für das Ausnutzen einer Systemschwäche multipliziert mit dem erwarteten Schaden durch den erfolgreichen Angriff werden als Risiko bezeichnet. Risikoanalysen versuchen, dieses Risiko zu minimieren. Es sind einige Vorgehensweisen bei der Risikobewertung eines Systems erprobt, beispielsweise jene des Bundesamtes für Sicherheit in der Informationstechnik (BSI) [75] oder der ETSI [79].

In dieser Arbeit werden jedoch die Bedrohungen im Mittelpunkt der sicherheitstechnischen Untersuchungen stehen. Der Grund dafür liegt in der allgemeinen Verwendbarkeit der Aussagen über Bedrohungen. Risiken sind durch die Abschätzung einer Eintrittswahrscheinlichkeit für erfolgreiche Angriffe und die meist vereinfachte Abschätzung eines Schadens nicht formal greifbar.

Bild 3-3 zeigt Klassifizierungskriterien für Bedrohungen und den Umgang mit den unterschiedlichen Bedrohungsklassen. Das Bedrohungsmodell unterstützt die Strukturierung von Sicherheitsuntersuchungen. Zu Beginn werden systemtechnische Randbedingungen erarbeitet und unter Zuhilfenahme angenommener Angreifermodelle zu Aussagen über bestehende Bedrohungen verarbeitet. Schließlich werden die Bedrohungen bewertet, wozu sehr viel Kontextwissen einbezogen werden muß.

Das Bild zeigt in der linken Hälfte ein System aus Angreifersicht. Der äußere Ring beschreibt die systemtechnischen Randbedingungen, die Angriffsmöglichkeiten einschränken und damit Bedrohungen beschränken. Die Durchlaßstellen im äußeren Ring beschreiben Schwachstellen des Systems, welche beim Vorhandensein von Angreifern systemtechnisch nicht ausschließbare Bedrohungen bedingen. Die Lücken dieses Rings hängen vom zugrundeliegenden Angreifermodell ab, da kein noch so gut geschütztes System absolute Sicherheit[7] garantieren kann. Die Wahl dieses Angreifermodelles, auf dem basierend die Sicherheitsbewertung durchgeführt wird, hat starke Auswirkungen auf den Nutzen der Untersuchung.

Der mittlere Schutzring stellt die Angriffshöhe, d. h. den für erfolgreiche Angriffe notwendigen Aufwand dar. Ob Bedrohungen tatsächlich ausnutzbar sind, hängt sowohl von den ange-

7 Da bisher alle Systeme von Menschen entwickelt bzw. durch Hilfsmittel, die durch Menschen direkt oder indirekt entwickelt wurden, gebaut und geschützt werden, sind Fehler bei diesen Systemen inhärent. Nichtangreifbar sind deshalb ausschließlich Schutzziele, welche sich auf nicht vorhandene Werte beziehen.

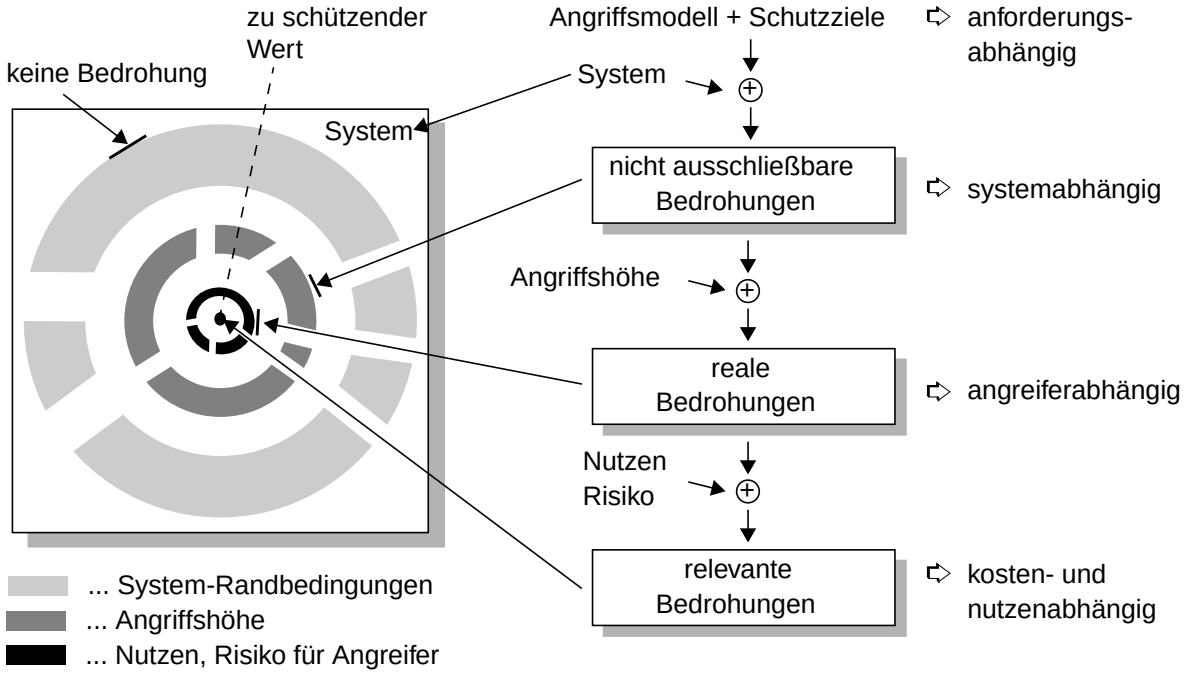


Bild 3-3: Systemzentrierte Klassifizierung von Bedrohungen – Bedrohungsmodell

nommenen Angreifern und deren Stärke als auch von systemtechnischen Randbedingungen ab. Schwachstellen im System, welche durch Angreifer des zugrundeliegenden Angreifermodelles ausnutzbar sind, bedingen reale Bedrohungen.

Der innere Ring stellt einen letzten Schutz vor erfolgreichen Angriffen dar. Reale Bedrohungen werden nur dann von einem Angreifer tatsächlich ausgenutzt, wenn dieser entsprechend motiviert ist. Dazu gehören das Verhältnis von Aufwand und Gewinn (Nutzen) sowie Risiken, die als Folge eines Angriffsversuches für den Angreifer entstehen können.

Die Sicherheitsbewertung eines komplexen Systems ist deshalb sehr schwierig, weil sich die zugrundeliegenden Randbedingungen meist im Laufe der Zeit mehr oder weniger stark verändern. Veränderungen im System (Betrieb, Management, Infrastruktur von Kommunikationsnetzen) führen dazu, daß sich die systemtechnischen Randbedingungen für Angreifer verändern, d. h. neue Schwachstellen entstehen oder bestehende Schwachstellen verschwinden. Neue Geräte bzw. der Preisverfall ehemals teurer technischer Geräte (z. B. Protokoll-Analysatoren) können die Angreifermodelle wesentlich beeinflussen. Nicht zuletzt wird die Motivation eines Angreifers von den Anwendungen beeinflußt, welche durch das System unterstützt werden und die Wertschöpfung des Systems bestimmen.

Da sich die Randbedingungen des Systems, die Angriffshöhe und das Kosten/Nutzen-Verhältnis gegenseitig beeinflussen, ist das Modell in ständiger Bewegung. Diese Abhängigkeiten wirken sich im Modell in Bild 3-3 dadurch aus, daß die Positionen der durchlässigen Stellen der dargestellten Ringe zeitlich variabel sind. Diese durchlässigen Stellen bezüglich relevanter Bedrohungen werden dadurch ständig verändert und sind schwer vorherzusehen. Zwar werden durch gezielte Veränderung des Systems bekannte Angriffslücken oft geschlossen, ebenso oft werden durch eine Veränderung des Systems jedoch auch neue und unvorhergesehene Angriffsmöglichkeiten geschaffen.

Die *sicherheitstechnische Bewertung* von Systemen bezieht Aussagen über Anreiferstärke (Angriffsmodelle) und Randbedingungen des Systems (Aufwandsabschätzungen für erfolgrei-

che Angriffe, möglicher Schaden am System) ein und liefert Aussagen über bestehende relevante Bedrohungen. Auf diese relevanten Bedrohungen kann unterschiedlich reagiert werden:

- Durch Erweiterung des Systems um Schutzmechanismen kann Bedrohungen *aktiv entgegengewirkt* werden. Beispiele für Schutzmechanismen, die systembedingte Randbedingungen zuungunsten des Angreifers verändern:
  - Zugangskontroll- und Zugriffskontrollmechanismen erschweren Angreifern den Zugang zum System oder den Zugriff auf schutzwürdige Systembestandteile. Die Vermeidung von schutzwürdigen Daten nimmt einem Angreifer von vornherein das Angriffsziel (Datensparsamkeit). In Bild 3-3 führen solche Schutzmechanismen zur Schließung von Lücken im äußeren Ring.
  - Durch Verschlüsselung nach leistungsfähigen Algorithmen und mit großzügiger Schlüssellänge läßt sich der Aufwand für Angriffe auf die Vertraulichkeit verschlüsselter Daten stark erhöhen. Damit können Lücken geschlossen werden, die einem starken Angreifer durch Wahl einer zu geringen Schlüssellänge Angriffsmöglichkeiten geboten haben (mittlerer Ring in Bild 3-3).
  - Protokollierung von Systemvorgängen (Audit), in Verbindung mit der Zuordenbarkeit von Systemvorgängen zu Personen, erhöht das Entdeckungsrisiko für Angreifer.

  Da neue Schutzmechanismen nie gegen alle denkbaren Angreifer völlig sicher gestaltet werden können, bedingen *Anreicherungen* meist Veränderungen der Angriffshöhe (mittlerer Ring) an den Stellen, an denen der äußere Ring nicht genügend Schutz bietet. Das *Eliminieren von Angriffszielen*, z. B. durch Weglassen von Funktionen oder Daten, ist aber in der Lage, auch Lücken im äußeren Ring zu schließen, d. h. Angriffsmöglichkeiten grundsätzlich auszuschließen.

- Relevante Bedrohungen können *versichert* werden, d. h. der mögliche Schaden eines erfolgreichen Angriffes (basierend auf einer relevanten Bedrohung) kann versichert werden. Dazu muß jedoch eine Abschätzung des Schadens möglich und die Reparation des möglichen Schadens finanziell ausgleichbar sein.

- Schließlich können verbleibende Bedrohungen auch *als Restrisiko akzeptiert* werden. Dazu ist jedoch eine obere Abschätzung des möglichen Schadens unabdingbar.

In einem idealen System (aus Sicht der sicherheitstechnischen Bewertung) sind die für Sicherheitsaspekte wesentlichen Parameter ersichtlich. Sicherheitsrelevante Parameter können damit bewußt verändert werden. Auswirkungen von Änderungen sind im voraus abschätzbar, so daß gegebenenfalls das durch die Veränderung von Systemparametern entstehende Angriffspotential proaktiv durch entsprechende Schutzmechanismen ausgeglichen werden kann. Es muß ein Bewußtsein dafür geschaffen werden, daß das Eliminieren von Angriffszielen dem Einsatz zusätzlicher Schutzmechanismen vorzuziehen ist, da neue Schutzmechanismen erfahrungsgemäß auch neue Bedrohungen mit sich bringen.

3.4 Sicherheitsarchitekturen als Basis der Netzsicherheit

Ein Kommunikationsdienst besteht aus einer Menge von Funktionselementen und Beziehungen zwischen diesen Funktionselementen. Funktionselemente umfassen sowohl Funktionen in Endgeräten und Netzknoten, als auch Funktionen in zentralen Dienste-Servern innerhalb des Kommunikationsnetzes.

Kommunikationsdienste erfüllen heute vor allem die Anforderungen seiner Benutzer an Dienstqualität und Schutzziele des Netzbetreibers oder Dienstanbieters. Die verfügbaren Kommunikationsdienste sind jedoch nicht in der Lage, jene Schutzziele zu erfüllen, die sich auf Benutzerseite entwickeln.

Damit ein Kommunikationsdienst zukünftig variierende und sich weiterentwickelnde Schutzziele garantieren kann, müssen zu den eigentlichen Dienste-Funktionen weitere Funktionselemente in geeigneter Weise hinzugefügt werden, welche die Durchsetzung dieser Schutzziele gegen angenommene Angreifer garantieren. Zunächst wird das allgemeine Architekturkonzept beschrieben, mit dem Sicherheitsdienste eingeordnet und in Beziehung zueinander gesetzt werden. Anschließend werden die grundlegenden technischen Bausteine der Sicherheitsarchitektur eingeführt.

3.4.1 Definition und Einordnung der Sicherheitsarchitektur

Sicherheitsdienste werden durch eine Sicherheitsarchitektur in ihr Wirkungsumfeld (z. B. Telekommunikationsnetze) eingeordnet und in ihren Wechselwirkungen beschrieben. Zur Hinführung auf den Begriff und die Bedeutung der Sicherheitsarchitektur dient folgendes Zitat aus dem Bereich der Betriebssysteme [48]:

„Besteht ein System aus zahlreichen einzelnen Komponenten, dann erfährt deren Zusammenwirken eine besondere, eigenständige Bedeutung. Deshalb wird neben den Komponenten selbst die Entwicklung und der Umgang mit Beziehungen zwischen den Komponenten eine Rolle spielen müssen.

Mit der Vielzahl von Komponenten, Aktivitäten, Beziehungen und Betriebsmitteln entstehen zahlreiche organisatorische Aufgaben, die bei einelementigen Systemen nicht gegeben sind. So sind etwa Vorgänge der Koordination, des Wettbewerbs oder der gegenseitigen Abgrenzung zu regeln. Fragen der Korrektheit, der Leistung, aber auch der Verstehbarkeit und Erklärbarkeit erfahren eine zunehmende Wichtigkeit. Die Struktur des ganzen darf nicht wild wuchern, sondern muß sich in vorgezeichneten Bahnen entfalten. Es entsteht eine Systemarchitektur.“

Eine *Sicherheitsarchitektur* wird folglich jene Systembestandteile – Komponenten und Beziehungen zwischen Komponenten – umfassen, welche Einfluß auf die Sicherheit eines Systems besitzen. Dabei sind neben jenen Beziehungen zwischen den Komponenten einer Sicherheitsarchitektur insbesondere auch jene zwischen Komponenten der Sicherheitsarchitektur und anderen Systemkomponenten zu berücksichtigen. Eben diese sogenannten *äußeren Beziehungen* bestimmen die Integrierbarkeit, die Skalierbarkeit und Realisierbarkeit, d.h. die Umsetzbarkeit einer Sicherheitsarchitektur in großem Maße. Sie stellen die Schnittstelle der Sicherheitsarchitektur zu ihrem Umfeld oder Anwendungsfeld dar.

Bei der Betrachtung von Kommunikationsdiensten sind vor allem die äußeren Beziehungen der Sicherheitsfunktionen zum Netzmanagement, zum Netzbetrieb, zur Entgeltdatenerfassung und zur Verarbeitung von Benutzerdaten innerhalb von Kommunikationsdiensten (z. B. Rufnummern zur Verkehrslenkung) von Bedeutung. Zusätzlich müssen die Benutzer mit den aktiven Elementen der Sicherheitsarchitektur interagieren können, um Optionen auszuwählen und im Rahmen einer Aushandlung zur Auflösung von Schutzziel-Konflikten beitragen zu können.

Bild 3-4 zeigt eine Gliederung von Bausteinen einer Sicherheitsarchitektur in unterschiedlichen Abstraktionsebenen. In der obersten Ebene unterscheiden wir zwischen den komplementären Sichten dualer Sicherheit: der Verläßlichkeit und der Beherrschbarkeit des zugrundelie-

genden Kommunikationsdienstes. Über die Schutzziele der durch den Kommunikationsdienst betroffenen Personen wirkt sich die mehrseitige Sicherheit auf die Sicherheitsarchitektur aus.

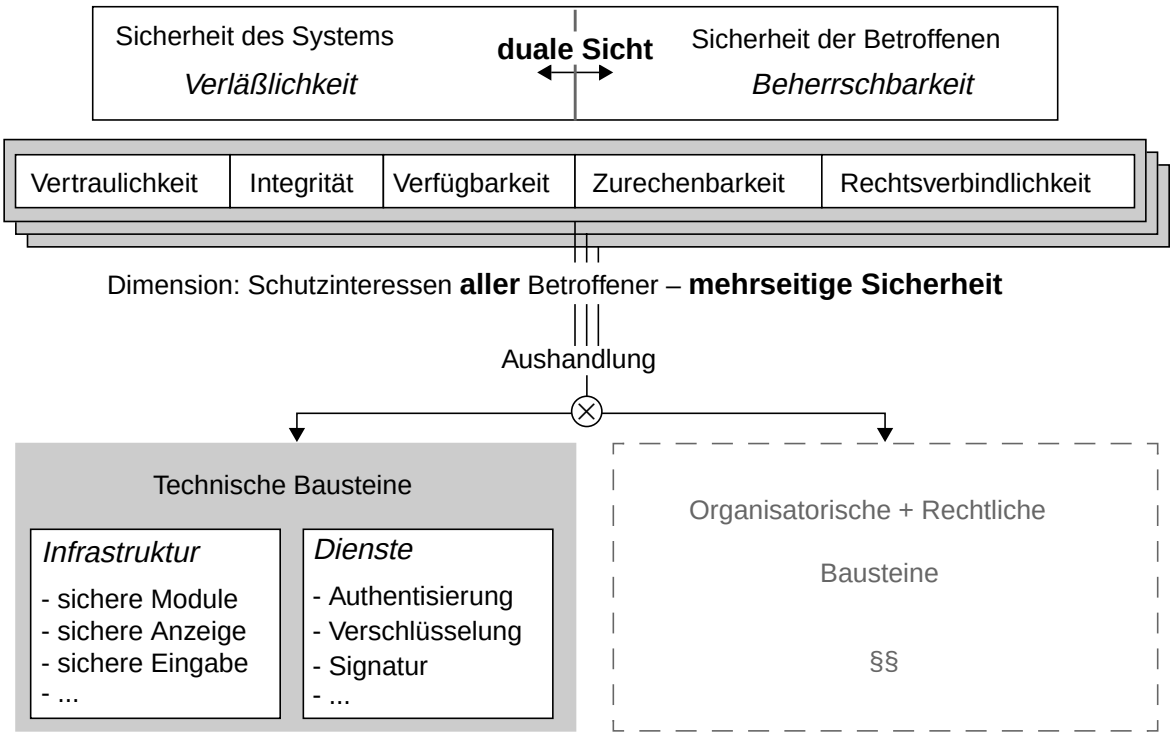


Bild 3-4: Bausteine einer Sicherheitsarchitektur

Dazu stehen technische Sicherheitsbausteine zur Garantie von Schutzzielen zur Verfügung. Diese Bausteine stehen in Beziehung mit den damit durchsetzbaren Schutzzielen zur Vertraulichkeit, Integrität, Verfügbarkeit, Zurechenbarkeit und Rechtsverbindlichkeit. Auf unterster Ebene sind einige technische Bausteine angegeben (Infrastruktur und darauf ablaufende Dienste). Organisatorische und rechtliche Bausteine sind z. B. in [50] dargestellt. Sie werden dort explizit angesprochen, wo sie Schnittstellen zur vorliegenden Arbeit aufweisen.

3.4.2 Technische Bausteine einer Sicherheitsarchitektur

Beschreibungen weiterer technischer Sicherheitsmechanismen sind in der allgemeinen Literatur enthalten (z. B. [52], [54], [55], [73], [74]). Im weiteren Verlauf des Kapitels werden die Beziehungen zwischen den in Kapitel 3.2.3 dargestellten Schutzzielen mehrseitig sicherer Kommunikationsdienste und letztendlich der realen Implementierung der Schutzmechanismen untersucht. Die vorgestellten Verfahren werden bei ihrer Einführung auch im Hinblick auf die nachfolgend vorgestellten Randbedingungen beim Einsatz in Kommunikationsnetzen bewertet.

3.4.2.1 Kryptographiesysteme

Der Begriff *Kryptographie* bezeichnet die Wissenschaft und das Studium der Geheimschrift [60]. Die klassische Kryptographie diente zum Schutz von Informationen, die mit Hilfe von Informationsträgern über Kanäle (z. B. repräsentiert durch Kuriere) übertragen wurden, an denen das Ablauschen und Abfangen bzw. Einspielen von Daten möglich war.

Moderne Kryptographie schützt Daten, die über Hochgeschwindigkeitsnetze übertragen oder in Rechnern gespeichert werden. Als Ziele der Kryptographie sind heute besonders die Vertraulichkeit und die Authentizität von Bedeutung. Wie wir im Abschnitt 3.4.2.3 zu digitalen Signaturen sehen werden, ist durch Verknüpfung kryptographischer Verfahren mit organisatorischen Verfahren und rechtlichen Regelungen auch der rechtskräftige Urheberschaftsnachweis für Nachrichten gegenüber Dritten realisierbar.

Die Kryptographie liefert heute die wichtigsten Verfahren zum aktiven Schutz von Informationen innerhalb von Rechner- bzw. Kommunikationssystemen. Sie bildet die Grundlage für die Sicherheitsmechanismen, die in dieser Arbeit angesprochen werden. Ein Kryptographiesystem (kurz: Kryptosystem) bezeichnet einen Raum, in dem Verfahren der Kryptographie anwendbar sind. Ein Kryptosystem besteht aus fünf Bestandteilen [61]:

- Dem Raum der *Klartextnachrichten*. Er beinhaltet jene Nachrichten, welche durch Anwendung von Kryptographie geschützt werden sollen.

- Dem Raum der *Schlüsseltextnachrichten*. Er beinhaltet jene Nachrichten, die durch Anwendung von Geheimschrift aus den Klartextnachrichten entstehen.

- Dem Raum aller *Schlüssel* (Schlüsselraum), mit denen Klartextnachrichten in Schlüsseltextnachrichten umgeschrieben werden können und umgekehrt.

- Einer Familie von *Verschlüsselungstransformationen* zur Umwandlung von Klartext- in Schlüsseltextnachrichten (parametrisiert durch Elemente des Schlüsselraumes).

- Einer Familie von *Entschlüsselungstransformationen* zur Rückwandlung von Schlüsseltextnachrichten in Klartextnachrichten (parametrisiert durch Elemente des Schlüsselraumes).

Wir bezeichnen ein Kryptosystem als *symmetrisch*, wenn der Schlüssel für zusammengehörige Verschlüsselungs- und Entschlüsselungstransformationen identisch ist. Sonst wird das Kryptosystem *asymmetrisch* genannt.

Kryptosysteme sind nicht inhärent sicher, d. h. die Qualität eines Kryptosystems hängt entscheidend von seinen Bestandteilen ab. Bewertungen von konkreten Kryptosystemen beziehen die Größe des Schlüsselraumes, des Raumes der Klartext- und Schlüsseltextnachrichten und die speziellen Transformationen zur Ver- und Entschlüsselung sowie unterschiedlich mächtige Angriffsmethoden in die Untersuchung mit ein. Diese Bewertungen werden als Kryptoanalyse bezeichnet und begleiten die Forschungen im Bereich der Kryptographie. Beispiele von Untersuchungen spezieller Kryptosysteme sind in [10], [12], [51], [61] zu finden.

Der praktische Nutzen der Kryptographie besteht – so wie sie hier angewandt wird – darin, daß Nachrichten vor ihrem Versenden über unsichere Kanäle vor unbefugter Kenntnisnahme geschützt bzw. über unsichere Kanäle empfangene Nachrichten auf Verfälschung und Echtheit geprüft werden können.

In den nachfolgenden Abschnitten werden jene Anwendungen von Kryptosystemen näher vorgestellt, die zur Erreichung der in Kapitel 3.2.3 genannten Schutzziele an Kommunikationsdienste von besonderer Bedeutung sind und praktisch eingesetzt werden können.

3.4.2.2 Verschlüsselungssysteme

Verschlüsselungssysteme dienen dazu, Information innerhalb unsicherer Kommunikationssysteme und auf unsicheren Übertragungsstrecken vor unbefugter Kenntnisnahme zu schützen (Schutzziele C1, C2).

Ein Verschlüsselungssystem besteht aus einem Algorithmus (*Verschlüsselungsalgorithmus*), mit dessen Hilfe Daten (*Klartextnachrichten*) so transformiert (verschlüsselt) werden, daß sie nicht mehr interpretierbar sind. Die Rücktransformation erfolgt durch einen *Entschlüsselungsalgorithmus*, der die transformierten Daten (*Schlüsseltextnachrichten*) wieder eindeutig auf die ursprünglichen Daten abbildet (entschlüsselt).

Ein Verschlüsselungssystem läßt sich eindeutig beschreiben durch:

- Schlüssel zur Verschlüsselung K_e (Encryption Key)
- Schlüssel zur Entschlüsselung K_d (Decryption Key)
- Verschlüsselungsalgorithmus (Encryption) E: $K_e \times$ Klartext $\rightarrow$ Schlüsseltext
- Entschlüsselungsalgorithmus (Decryption) D: $K_d \times$ Schlüsseltext $\rightarrow$ Klartext

Die Abbildungen E und D müssen dabei der Bedingung $D(K_d, E(K_e, X)) = X$ für alle X aus dem Raum der Klartextnachrichten genügen.

Gebräuchlich ist folgende Klassifizierung in *symmetrische* und *asymmetrische* Verschlüsselungssysteme:

- Bei *symmetrischen Verschlüsselungssystemen* sind die Schlüssel zur Ver- und Entschlüsselung gleich ($K_e = K_d$). Die bekanntesten Vertreter sind durch den Data Encryption Standard (DES) und den International Data Encryption Algorithm (IDEA) definiert (siehe [52], [53]).
- Bei *asymmetrischen Verschlüsselungssystemen* sind die Schlüssel zur Ver- und Entschlüsselung nicht identisch. Asymmetrische Verschlüsselungssysteme werden zusätzlich nach der Schwierigkeit bewertet, mit der einer der beiden Schlüssel aus dem anderen Schlüssel abgeleitet werden kann. Der bekannteste Vertreter ist RSA [5]. Bei der asymmetrischen Verschlüsselung muß der Schlüssel zur Entschlüsselung (K_d) geheimgehalten werden. Der Schlüssel zur Verschlüsselung (K_e) kann öffentlich bekannt sein und muß dem jeweiligen Empfänger, der den Schlüsseltext mit K_d entschlüsseln kann, eindeutig zuordenbar sein.

Die Sicherheit der Verfahren, d. h. die Erfüllung der Anforderung, daß nur der Besitzer des Schlüssels K_d die mit K_e verschlüsselten Daten wiederherstellen kann, hängt von den verwendeten Algorithmen E und D, deren Implementierung, der Wahl der Schlüssel K_e und K_d sowie von der Größe des Schlüsselraumes ab.

Konkrete Anwendungen von Verschlüsselungsverfahren zum Schutz von Datenströmen sind beispielsweise in [14] und [62] dargestellt.

3.4.2.3 Signatursysteme

Signatursysteme ermöglichen den eindeutigen Nachweis der Urheberschaft einer Nachricht bzw. des zugehörigen Nachrichteninhaltes. Sie basieren auf asymmetrischen Kryptosystemen. Dabei wird jedem Identitätsträger (Person, Prozeß, etc.) ein Schlüsselpaar (K_g, $K_ö$) zugeordnet. Der geheime Schlüssel K_g ist ausschließlich dem jeweiligen Identitätsträger bekannt. Der

öffentliche Schlüssel $K_ö$ ist allgemein verfügbar und muß eindeutig dem jeweiligen Identitätsträger zuordenbar sein. K_g darf aus $K_ö$ nicht – bzw. nicht innerhalb des Gültigkeitszeitraumes einer Signatur – ableitbar sein.

Der Erzeuger einer Nachricht kann diese signieren, indem er eine für die Nachricht geltende Signatur mit dem nur ihm bekannten geheimen Schlüssel K_g (Signierschlüssel) erzeugt[8]. Der Empfänger einer Nachricht kann deren Signatur prüfen, indem er sie mit dem öffentlichen Schlüssel ($K_ö$) des angeblichen Urhebers testet und damit prüft.

Oft wird anstatt der gesamten Nachricht lediglich ein Hashwert signiert. Dem Prüfer einer Nachricht muß dann der entsprechende Algorithmus zur Erzeugung des Hashwertes bekannt sein und zur Verfügung stehen. Die Prüfung erfolgt in diesem Fall durch Entschlüsselung der Signatur mit dem öffentlichen Schlüssel des angeblichen Urhebers und Vergleich mit dem selbstberechneten Hashwert der empfangenen Nachricht. Nachrichten, die zum selben Hashwert führen (Kollision), sind anhand ihrer Signatur nicht unterscheidbar.

Ein Signatursystem läßt sich beschreiben durch:

- Schlüssel K_g zur (Erzeugung einer) Signatur von Nachrichten
- Schlüssel $K_ö$ zur Prüfung einer Signatur
- Signieralgorithmus E: $K_g \times \text{Nachricht} \rightarrow \text{Signatur}$
- Prüfalgorithmus D: $K_ö \times \text{Signatur} \rightarrow \text{Testergebnis}$

$K_ö$ ist dabei öffentlich bekannt und eindeutig einer Identität zuordenbar. K_g ist nur dem Identitätsträger bekannt, dem der zugehörige öffentliche Schlüssel $K_ö$ zugeordnet ist. K_g läßt sich (innerhalb der Gültigkeitsdauer des Signatursystems) nicht aus $K_ö$ ableiten.

Die bekanntesten Verfahren zur Bildung von Signatursystemen sind das 1989 veröffentlichte RSA-Verfahren [5], das gleichzeitig als asymmetrisches Verschlüsselungssystem Anwendung findet. Eine zunehmend interessante Alternative bietet der Digital Signature Algorithm (DSA), der 1991 im Digital Signature Standard (DSS) des National Institute of Standards and Technology (NIST, USA) veröffentlicht wurde [52].

Sofern das zu einem Signatursystem gehörige Schlüsselpaar rechtskräftig und eindeutig einer Person zugeordnet werden kann, ist mit solchen Systemen ein Urhebernachweis möglich. Der Beweiswert gegenüber Dritten hängt entscheidend von der Sicherheit der Generierung des Schlüsselpaares, der Verwaltung des geheimen und öffentlichen Schlüssels (K_g und $K_ö$) zur Generierung und Prüfung einer Signatur, von der sicheren Zuordnung öffentlicher Schlüssel zu einer Identität sowie der Sicherheit der zugrundeliegenden Signier- und Prüfalgorithmen ab.

Der Beweiswert von digitalen Signaturen wird durch das Signaturgesetz ([123] Artikel 3) und die durch die Bundesregierung veröffentlichte Verordnung zur digitalen Signatur [139] geregelt. Im Bereich der Kommunikationsdienste sind damit im Hinblick auf die in Abschnitt 3.2.3 genannten Schutzziele mehrseitig sicherer Dienste u. a. folgende Anwendungsmöglichkeiten gegeben:

8 Während bei asymmetrischen Verschlüsselungssystemen zum Schutz der Vertraulichkeit der öffentlich bekannte Schlüssel ($K_ö$) zur Verschlüsselung angewendet wird, wird zur Generierung von Urhebernachweisen der geheime Schlüssel (K_g) verwendet.

- Durch Signieren von Kommunikationsdienst-Anforderungen kann die Teilnahme an Kommunikationsdiensten nachweisbar gemacht werden. Durch Signaturen können die Urheber den Kommunikationsinhalten zugeordnet werden. Das Signieren von Empfangsbestätigungen schafft eine Zuordnung von Teilnehmern zu Empfängern von Kommunikationsinhalten (Schutzziel Z1).

- Durch Signieren von Kommunikationsdienst-Anforderungen und Qualitätszusicherungen können Benutzer, Netzbetreiber und Dienstanbieter während der Diensterbringung Beweise erhalten, wenn dies durch Forderungen (Nutzungsverhalten, Entgelt) gerechtfertigt und gegenseitig abgestimmt ist (Schutzziele I4 und Z2).

- Eine Rechtsverbindlichkeit wird erreicht, wenn zur Signatur solche Signatursysteme eingesetzt werden, die den Anforderungen des Signaturgesetzes und der Signaturverordnung genügen und wenn die Betroffenen sich der Rechtskraft ihrer Signatur und der dadurch entstehenden Verbindlichkeiten bewußt sind (Schutzziel R1).

Eine Grundlage für viele Verfahren stellt die für den Benutzer vertrauenswürdige Zuordnung von öffentlichen Schlüsseln und den damit prüfbaren Identitäten von Personen dar. Dazu werden Zertifizierungsstellen aufgebaut, die die Zuordnung von öffentlichen Prüfschlüsseln zu Identitäten von Personen beglaubigen. Es werden augenblicklich in Deutschland sowohl staatliche Zertifizierungsstellen (durch das Bundesamt für Sicherheit in der Informationstechnik) als auch private Zertifizierungsstellen (z. B. durch die Deutsche Telekom AG und die DaimlerChrysler AG) aufgebaut, die durch die Regulierungsbehörde für Telekommunikation geprüft und zugelassen werden. Öffentliche Schlüssel müssen bei Bedarf zum Schutz vor kompromittierten Schlüsseln geprüft werden können.

3.4.2.4 Echtheitsnachweisverfahren

Authentisierungsverfahren dienen zur Prüfung der Echtheit[9] von Informationsträgern. Im Zusammenhang mit Kommunikationsdiensten sind die Identitäten von Sender und Empfänger(n), die Kommunikationsinhalte (Nutzdaten), die Interpretationsregeln für Daten, und gegebenenfalls auch der Aufenthaltsort von Sender bzw. Empfänger von Bedeutung. Die entsprechenden Informationsträger müssen bei Bedarf vom Empfänger auf Authentizität (Echtheit) geprüft werden können.

Authentisieren heißt „glaubwürdig machen“. Dies ist deutlich schwächer als „rechtskräftig nachweisbar gestalten“ und dient i. a. eher zur persönlichen Echtheitsprüfung, als zum Nachweis gegenüber Dritten.

Symmetrische Verfahren sind meist innerhalb einer Kommunikationsbeziehung wirksam, d. h. außerhalb der Kommunikation kann die Echtheit nicht mehr geprüft oder gegenüber Dritten nachgewiesen werden. Asymmetrische Verfahren dagegen erlauben auch den Nachweis gegenüber Dritten und werden als digitale Signaturverfahren bezeichnet.

Bei der Betrachtung von Kommunikationsdiensten sind die Interpretationsregeln für Dienstesteuerungsdaten weitgehend durch das Kommunikationsprotokoll vorgegeben. Der Aufenthaltsort ist im Augenblick i. a. noch kein Prüfkriterium. Neue Verfahren erlauben jedoch auch die Einbeziehung des Aufenthaltsortes [45]. In der Zukunft ist es wahrscheinlich, daß der Zugriff auf sensitive Daten auch von autorisierten Personen nur von bestimmten, als sehr

9 Unter Echtheit einer Nachricht oder ihres Inhaltes verstehen wir sowohl die Unverfälschtheit des Inhaltes als auch die Aktualität, d. h. die enge zeitliche Korrelation zum betrachteten Kommunikationsereignis.

sicher eingestuften Umgebungen heraus abgerufen werden darf (z. B. vom Heimarbeitsplatz aus, aber nicht im Internet-Cafe). In den folgenden Betrachtungen erhalten vor allem die Prüfung der Echtheit der Identität des Senders (Wer sendet die Nachricht?), des Empfängers bzw. der Empfänger (Wer empfängt die Nachricht?) und des Nachrichteninhaltes (Ist die Nachricht unverfälscht angekommen?) besondere Bedeutung.

Der Empfänger der Nachricht kann auf der Basis der geprüften Identität eine Zugriffskontrolle durchführen bzw. unverfälscht angekommene Daten verarbeiten.

Als Echtheitsmerkmal für Nachrichten(-teile) dient im allgemeinen verschlüsselte Redundanz. Diese Redundanz muß (möglichst) eindeutig aus der Nachricht gewonnen werden. Eindeutige Redundanz ist z. B. ein Duplikat der Nachricht. Da dies aber die Übertragungsmenge verdoppelt, wird meist ein guter Hashwert als Redundanz benutzt. Ein Angreifer darf nicht in der Lage sein, die (Klartext-)Nachricht zu verändern und die Redundanz an die Änderung anzupassen. Deshalb wird die Redundanz i. a. mit einem gegenüber unautorisierten Personen geheimen Schlüssel verschlüsselt. Eine mit einem guten Kryptosystem verschlüsselte Redundanz kann (ohne Kenntnis des Schlüssels) von einem Angreifer nicht gezielt geändert werden.

Um die zeitliche Korrelation einer Nachricht mit dem aktuellen Kommunikationsereignis prüfen zu können, werden zusätzlich Zeitstempel, Transaktionsnummern etc. verwendet, welche die Gültigkeit der Echtheitsmerkmale beschränken und so auf die Aktualität der Nachricht hinweisen[10]. Werden Sender und Empfänger in die Redundanzbildung miteinbezogen, so sind auch diese Informationen gegen Verfälschung während der Übertragung geschützt.

Sollen Sender durch den Empfänger unterscheidbar sein, so muß für jeden Sender ein eigener geheimer Schlüssel für die Verschlüsselung der Redundanz (Bildung der Echtheitsmerkmale) installiert werden. Sollen Empfänger in der Lage sein, die Echtheit einer Nachricht zu prüfen, jedoch nicht in der Lage sein, eine Nachricht zu fälschen, so müssen unterschiedliche Schlüssel zur Generierung und zur Prüfung eines Echtheitsmerkmales verwendet werden. Hierzu werden asymmetrische Verschlüsselungssysteme eingesetzt.

Echtheitsnachweis basierend auf symmetrischen Kryptosystemen

Der Echtheitsnachweis kann basierend auf symmetrischen Kryptosystemen erfolgen. Das Echtheitsmerkmal einer Nachricht muß so beschaffen sein, daß es nur von einer Person erstellt werden kann, die den geheimen Schlüssel ($K_e = K_d = K$) kennt und daß ein nachträgliches Verändern der Nachricht über das Echtheitsmerkmal erkennbar wird.

Bei diesem Verfahren besitzen Sender und Empfänger einer Nachricht einen gemeinsamen, gegenüber anderen geheimgehaltenen Schlüssel K[11]. Aus der Nachricht wird ein Hashwert gebildet. Dieser wird mit K verschlüsselt und der Nachricht vor dem Versenden beigefügt. Die verschiedenen Varianten und Möglichkeiten der effizienten Zusammenführung von Hashwert-Berechnung und Verschlüsselung – z. B. durch Parametrisierung des Hash-Algorithmus mit dem geheimen Schlüssel – sind in [7], [13] und in der allgemeinen Literatur zu finden.

10 Dies dient u. a. zur Erkennung von eingespielten Nachrichten, die an anderer Stelle oder aus anderen Transaktionen abgelauscht wurden.

11 Der Schlüssel alleine beschreibt das symmetrische Verschlüsselungssystem natürlich nicht eindeutig. Hier und im folgenden wird davon ausgegangen, daß die weiteren Parameter des zugrundeliegenden Verschlüsselungssystems – mit Ausnahme des Schlüssels – aus dem Kontext hervorgehen bzw. durch die technisch verfügbaren Implementierungen bestimmt sind.

Der verschlüsselte Hashwert (Echtheitsmerkmal) wird *Message Authentication Code* (MAC) genannt. Der Empfänger benutzt den einem bestimmten Sender zugeordneten Schlüssel zur Entschlüsselung des MAC und prüft, ob das Ergebnis mit dem berechneten Hashwert der Nachricht übereinstimmt (Korrektheit). Darüberhinaus prüft der Empfänger, ob Zeitstempel und Transaktionsnummer die zeitliche Korrelation und die Zuordenbarkeit zur vorliegenden Transaktion nahelegen. Bild 3-5 veranschaulicht die Erzeugung und Prüfung von Echtheitsmerkmalen basierend auf symmetrischen Kryptosystemen[12].

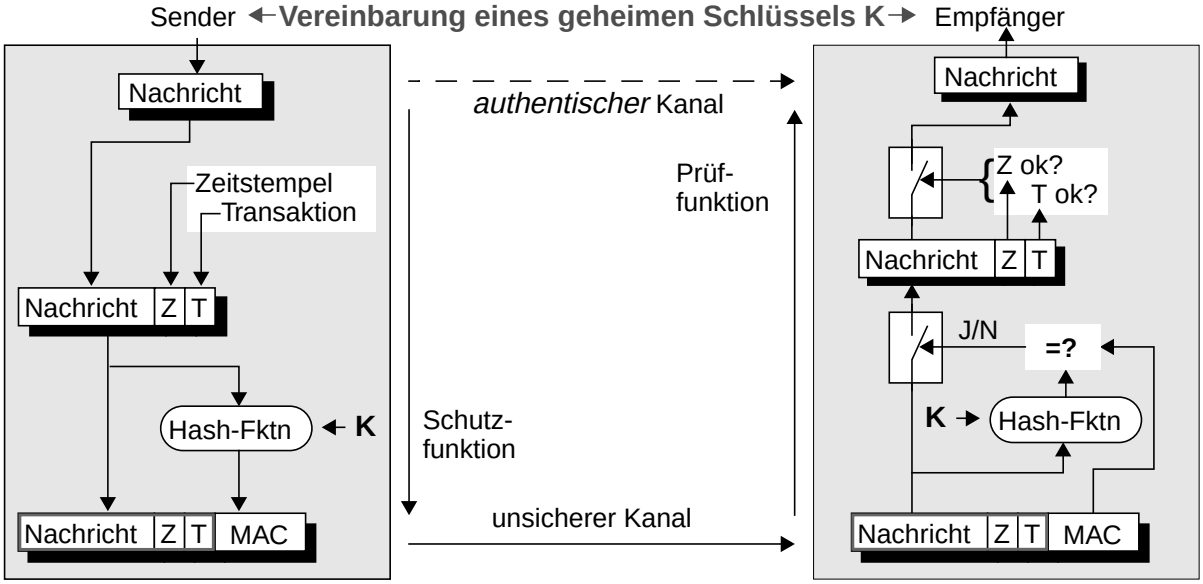


Bild 3-5: Echtheitsnachweis mit Hilfe symmetrischer Kryptosysteme

Bild 3-5 veranschaulicht, wie auf einem Kanal, in den gefälschte Nachrichten eingespielt oder verändernde Angriffe nicht ausgeschlossen werden können, ein authentischer Kanal zwischen Sender und Empfänger etabliert werden kann. Dazu müssen die Nachrichten vor ihrem Versenden über den unsicheren Kanal mit Hilfe von Schutzfunktionen (z. B. basierend auf Zeitstempel, Transaktionsnummer, Echtheitsmerkmal) geschützt werden. Nachrichten, die auf einem unsicheren Kanal empfangen werden, müssen auf Authentizität (Echtheit) geprüft werden. Nur Nachrichten, die die Authentizitätskriterien erfüllen, dürfen zur Weiterverarbeitung an den Empfänger durchgereicht werden. Zur Realisierung von Schutz- und Prüffunktion müssen Sender und Empfänger einen gemeinsamen, gegenüber allen angenommenen Angreifern geheimen Schlüssel K vereinbart haben.

Der Beweiswert gegenüber Dritten ist dadurch eingeschränkt, daß derselbe Schlüssel zur Generierung und zur Prüfung des Echtheitsmerkmales benutzt wird. Somit ist eine Urheberschaft gegenüber Dritten nicht nachweisbar. Jeder der in der Lage ist, das Echtheitsmerkmal zu prüfen, kann dieses auch fälschen bzw. an eine gefälschte Nachricht anpassen.

Ist ein geheimer Schlüssel nur für eine einzige Transaktion gültig, so kann schon die Generierung des MAC mit diesem Schlüssel den Bezug der Nachricht zu einer Transaktion garantieren. Zeitstempel und Transaktionsnummer können in diesem Fall durch einen einfachen Zähler zur Reihenfolgesicherung und Duplikatserkennung ersetzt werden. Zu einer Transaktion können beispielsweise alle Verbindungssteuernachrichten zusammengefaßt werden, die dieselbe

12 Transaktionsnummer und Zeitstempel können auch vor der Prüfung des MAC geprüft werden.

Verbindung betreffen. Ebenso könnten alle Steuernachrichten eines Dienstmerkmales (siehe Abschnitt 2.4.1) als eigenständige Transaktion aufgefaßt werden.

Echtheitsnachweis basierend auf asymmetrischen Kryptosystemen

Ein Echtheitsnachweis auf der Basis asymmetrischer Verschlüsselungsverfahren hat gegenüber den eben besprochenen Verfahren den Vorteil, daß die Schlüssel zur Bildung des Echtheitsmerkmales (geheimer Schlüssel K_g) und zur Prüfung des Echtheitsmerkmales (öffentlicher Schlüssel $K_ö$) unterschiedlich sind. Damit kann – sofern K_g nicht aus $K_ö$ ableitbar ist – der Prüfer der Echtheit einer Nachricht das Echtheitsmerkmal nicht fälschen bzw. an eine gefälschte Nachricht anpassen.

Die zum Nachweis der Echtheit benutzten technischen Verfahren entsprechen jenen, welche auch zur Erzeugung einer digitalen Signatur benutzt werden. Im Gegensatz zur digitalen Signatur, deren Zweck die rechtskräftige Nachweisbarkeit der Urheberschaft von Nachrichteninhalten gegenüber Dritten darstellt, dient der Authentizitätsnachweis dazu, den *Sender* (und gegebenenfalls die adressierten Empfänger) einer Nachricht, die Zugehörigkeit zum *Kontext* (Zeit und Transaktion), in dem diese Nachricht verarbeitet wird, sowie deren *Unverfälschtheit* zu prüfen. Bild 3-6 veranschaulicht die Erzeugung und Prüfung von Echtheitsmerkmalen basierend auf asymmetrischen Kryptosystemen durch Verschlüsselung bzw. Entschlüsselung von Redundanz mit asymmetrischen Verschlüsselungsverfahren.

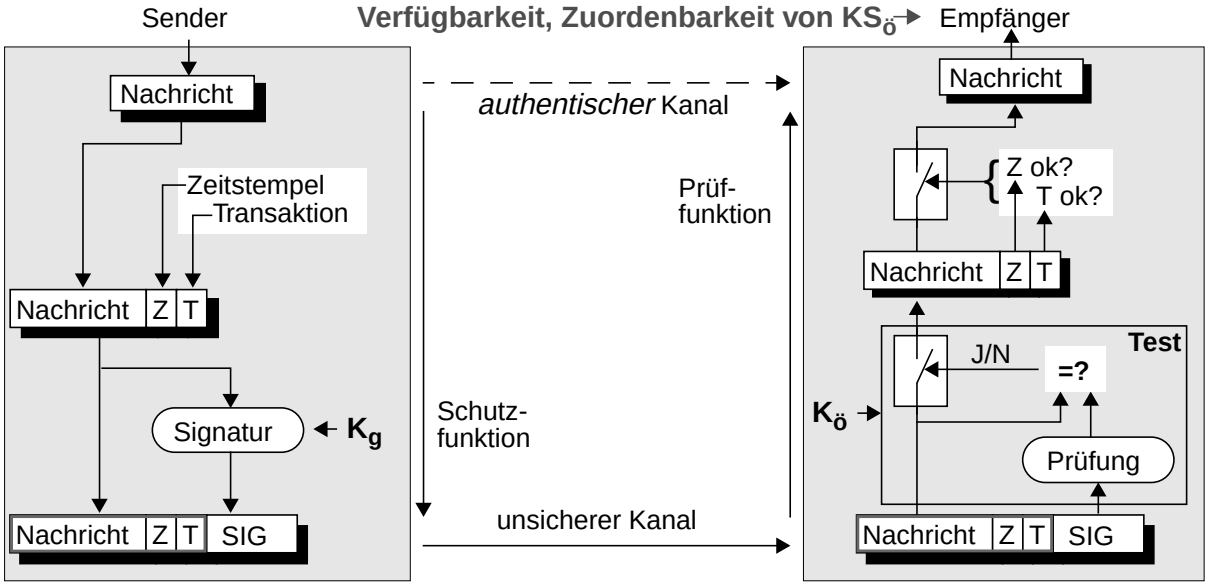


Bild 3-6: Echtheitsnachweis mit Hilfe asymmetrischer Kryptosysteme

Die Nachricht wird vor ihrer Übermittlung durch Redundanz ergänzt, die während ihrer Übermittlung über den unsicheren Kanal ohne Kenntnis von K_g nicht unbemerkt verändert werden kann. Beim Empfänger wird die in der Signatur SIG enthaltene geschützte Redundanz mit der in der Nachricht enthaltenen Redundanz verglichen. In Bild 3-6 wird als Echtheitsmerkmal ein Duplikat der Nachricht mit K_g verschlüsselt und als Signatur angehängt. Ähnlich dem in Bild 3-5 dargestellten Verfahren könnte lediglich ein Hashwert der Nachricht (inklusive Zeitstempel und Transaktionskennung) mit K_g verschlüsselt als Signatur dienen[13].

Sofern die Echtheit von Nachrichten ausschließlich innerhalb einer geschlossenen Nutzergruppe von Bedeutung ist, können private Schlüsselverzeichnisse benutzt werden, deren Verwaltung unabhängig von Signaturgesetzen und Verordnungen einfach realisiert werden kann.

Echtheitsnachweis bei spontaner Kommunikation

In offenen Kommunikationsnetzen sollte auch bei der spontanen Kommunikation mit bisher unbekannten Personen sichere Kommunikation möglich sein. Zusätzlich stellen die geschützt zu übermittelnden Daten, abhängig vom jeweiligen Dienst, hohe Anforderungen an die Verarbeitungseinheiten. Für offene Sicherheitsdienste sind deshalb folgende Randbedingungen gegeben:

- Die Sicherheitsdienste müssen ohne vorherige Vereinbarung gemeinsamer geheimer Schlüssel auskommen.
- Die Sicherheitsfunktionen müssen für große Datenmengen und für hohe Übertragungsgeschwindigkeiten geeignet sein.

Zum Schutz von großen Datenmengen unter hohen zeitlichen Anforderungen bieten sich heute vor allem symmetrische Kryptoverfahren an. Diese benötigen jedoch einen geheimen Schlüssel, der zwischen den Kommunikationspartnern zuvor vereinbart sein muß (siehe Bild 3-5).

Zur Vereinbarung dieses geheimen Schlüssels werden asymmetrische Kryptosysteme benutzt. Vor dieser Schlüsselvereinbarung muß die Identität der Kommunikationspartner geprüft werden, damit klar ist, zwischen welchen Partnern der Echtheitsnachweis etabliert wird. Dazu wird jedem potentiellen Kommunikationspartner ein Schlüsselpaar eines asymmetrischen Kryptosystems (K_g, $K_ö$) zugewiesen, siehe Kapitel 3.4.2.2. Der einem Kommunikationspartner zugeordnete öffentliche Schlüssel wird veröffentlicht und zur Prüfung der Identität benutzt. Der geheime Schlüssel (K_g) ist ausschließlich dem Kommunikationspartner bekannt, dem der zugehörige öffentliche Schlüssel ($K_ö$) zugeordnet ist.

Beim Aufbau einer Kommunikationsbeziehung (z. B. Verbindungsaufbau) beweisen sich die Kommunikationspartner gegenseitig ihre Identität. Dies tun sie durch Verschlüsseln von Nachrichten mit dem nur ihnen bekannten geheimen Schlüssel (K_g). Der Empfänger der Nachricht prüft diese Nachricht mit dem öffentlichen Schlüssel, der dem erwarteten Kommunikationspartner zugeordnet ist, siehe Kapitel 3.4.2.3. Um Angriffe wie z. B. das Wiedereinspielen von abgehörten (verschlüsselten oder signierten) Nachrichten oder das Fälschen öffentlicher Schlüssel zu verhindern, müssen die Prüfnachrichten entsprechend aufgebaut und die öffentlichen Schlüssel gültig und sicher zuordenbar sein. In [25] wird ein Protokoll zum Identitätsnachweis auf seine Robustheit bezüglich verschiedener Angriffe untersucht.

Innerhalb der Nachrichten zur Prüfung der Identität des Kommunikationspartners können Schlüsselteile (KE bzw. KS) ausgetauscht werden, die zur Vereinbarung eines geheimen Schlüssels (K) führen. Diese Schlüsselteile KE bzw. KS können durch Verschlüsselung mit

13 Die im Bild veranschaulichte Transformation der Nachricht durch die Schutzfunktion ist in diesem Fall jedoch nicht mehr bijektiv. Dies führt dazu, daß Nachrichten, deren Hashwerte gleich sind, bei der Prüfung nicht unterschieden werden können. Ein Angreifer könnte also unbemerkt eine Nachricht innerhalb einer solchen Klasse (Nachrichten mit gleichem Hashwert) in eine andere Nachricht derselben Klasse ändern, ohne daß dies beim Empfänger erkennbar wäre. Der Kanal ist dann noch authentisch bezüglich der Klassen von Nachrichten mit gleichem Hashwert. Sinnvoll nutzbar sind Hash-Verfahren zum Echtheitsnachweis, wenn a) ein Angreifer keine weiteren Nachrichten zu einem gegebenen Hashwert finden kann (Aufwand) oder wenn b) höchstens eine einzige „sinnvolle“ Nachricht in jeder solchen Klasse vorhanden ist (inhärente Redundanz).

dem öffentlichen Schlüssel des Empfängers geheim übermittelt werden. Der Schlüssel K kann anschließend zum Betrieb eines symmetrischen Kryptoverfahrens zwischen Sender und Empfänger genutzt werden. Nach der Prüfung der Identität können alle ausgetauschten Nachrichten mit Hilfe symmetrischer Kryptosysteme (basierend auf dem geheimen Schlüssels K) vom Sender gesichert bzw. vom Empfänger geprüft werden.

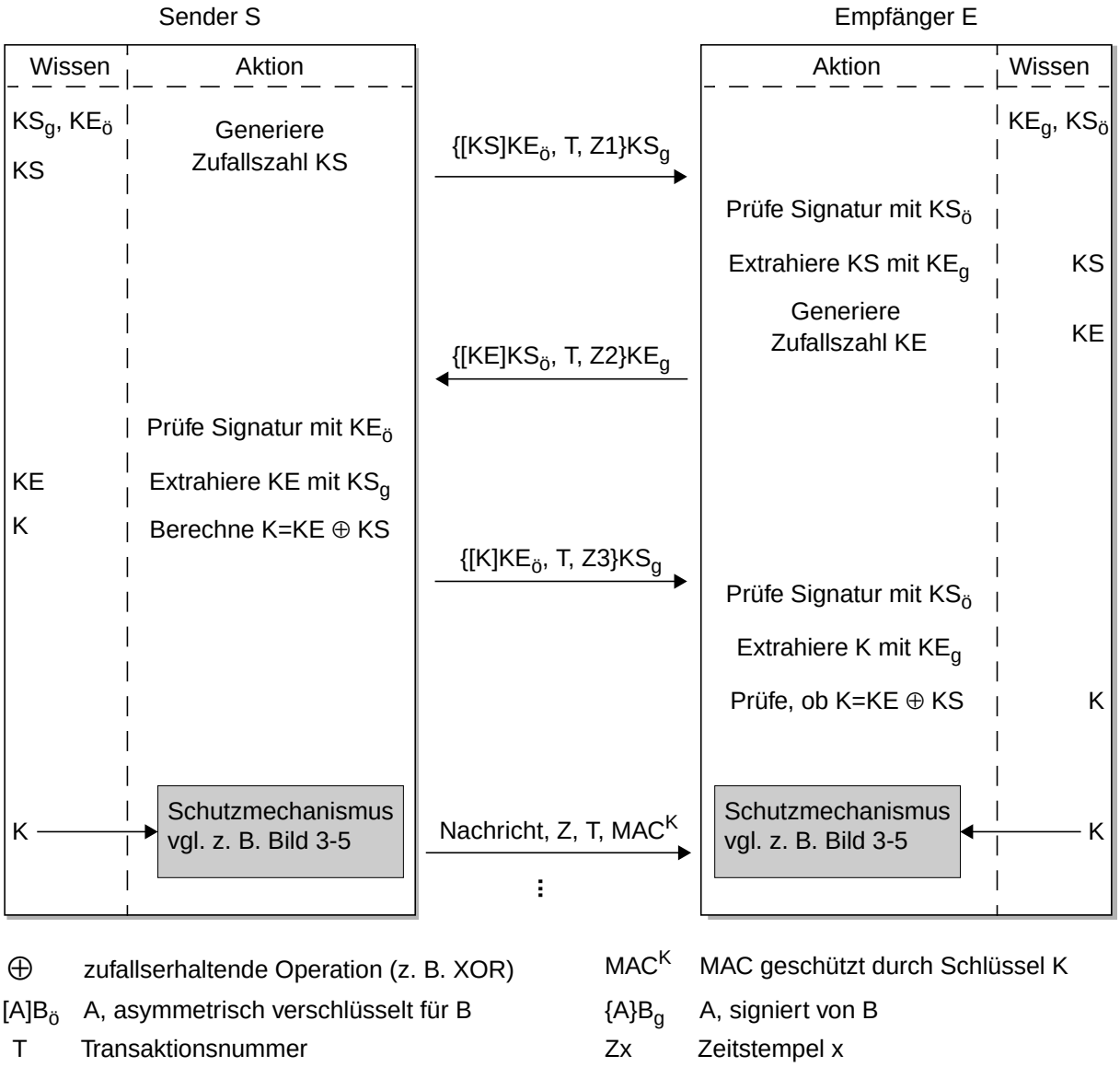


Bild 3-7: Echtheitsnachweis mit Hilfe hybrider Verfahren

Sei (KS_g, $KS_ö$) das asymmetrische Schlüsselpaar des Senders S und (KE_g, $KE_ö$) das asymmetrische Schlüsselpaar des Empfängers E und seien $KS_ö$ und $KE_ö$ gegenseitig bekannt und den jeweiligen Identitätsträgern S und E eindeutig zuordenbar. Dann lassen sich aus obiger Diskussion resultierende Anforderungen an zugrundeliegende asymmetrische Kryptosysteme zur Unterstützung authentischer spontaner Kommunikation wie folgt zusammenfassen:

- Signatur / Signaturprüfung zur Authentizitätsprüfung der Nachricht bzw. Identität des Senders: *Nachricht = E($KS_ö$,D(KS_g,Nachricht))*

- Verschlüsselung / Entschlüsselung zur Vereinbarung eines Geheimnisses:
  $Geheimnis = D(KE_g,E(KE_ö,Geheimnis)$

Die einfachste Lösung bietet ein asymmetrisches Kryptosystem, mit welchem sowohl verschlüsselt als auch signiert werden kann. Das bekannte, stark verbreitete RSA-Verfahren ist ein Beispiel für ein solches asymmetrisches Kryptosystem [5].

Den zeitlichen Ablauf des hybriden Verfahrens zeigt Bild 3-7. Die Identitäten von Sender und Empfänger sind nicht explizit als Nachrichtenbestandteile aufgeführt, lassen sich aber leicht aus den Pfeilrichtungen ableiten. Die ersten drei Nachrichten in Bild 3-7 dienen zur gegenseitigen Prüfung der Identität des Kommunikationspartners und zur Vereinbarung eines gemeinsamen geheimen Schlüssels K. Dieser wird anschließend zur schnellen Generierung und Prüfung der Echtheit von Nachrichten verwendet. Dazu kann beispielsweise das Verfahren aus Bild 3-5 verwendet werden. Sowohl Sender als auch Empfänger tragen zu dem vereinbarten gemeinsamen Schlüssel K bei. Für die unterschiedlichen Richtungen können gegebenenfalls unterschiedliche gemeinsame Schlüssel (z. B. zum Echtheitsnachweis) vereinbart werden.

3.5 Stand der Standardisierung von Sicherheitsdiensten

Die Standardisierung von Sicherheitsdiensten liefert einen wichtigen Beitrag zur Kompatibilität unterschiedlicher Implementierungen. Im folgenden wird ein kurzer Überblick über die Standardisierungsaktivitäten der International Telecommunication Union (ITU) bzw. International Organization for Standardization (ISO) und der Internet Engineering Task Force (IETF) gegeben. Es wird ausschließlich auf jene Standards näher eingegangen, die Bezug zur hier diskutierten Sicherheitsarchitektur für das ISDN aufweisen.

3.5.1 Sicherheitsstandards der ITU und der ISO

Die für die vorliegende Arbeit relevanten Aktivitäten der ITU bzw. ISO beschränken sich auf die abstrakte Sicht (Rahmenwerke) für unterschiedliche Sicherheitsdienste. Die vorliegenden ITU-Standards werden referenziert; die jeweils inhaltsgleichen ISO-Standards sind in der Literatur angegeben.

Der ISO-Standard ISO/IEC 7498-2 [87] und die ITU-Empfehlung X.800 [118] beschreiben die übergeordneten Aspekte einer Sicherheitsarchitektur für offene Systeme. Es werden folgende Sicherheitsdienste unterschieden:

- Authentisierungsdienste umfassen sowohl Dienste zur Authentisierung von Partnerinstanzen (*Peer Entity Authentication*), als auch zur Authentisierung des Senders bzw. des Ursprungs von Daten (*Data Origin Authentication*).

- Zugriffskontrolldienste (*Access Control*) dienen zum Schutz vor unautorisierter Nutzung von Ressourcen. Für diese Arbeit ist vor allem der Schutz von über Telekommunikationsdienste angesprochenen Ressourcen von Bedeutung.

- Vertraulichkeitsdienste lassen sich bezüglich der zu schützenden Werte gliedern:
  - Zum Schutz von Nutzdaten werden Sicherheitsdienste für die verbindungsorientierte (*Connection Confidentiality*) und verbindungslose (*Connectionless Confidentiality*) Übermittlung unterschieden. Es werden auch Dienste definiert, die lediglich bestimmte Felder von Nachrichten schützen (*Selective Field Confidentiality*). Dies ist sinnvoll, falls der Schutz der gesamten Nachricht zu aufwendig wäre oder falls bestimmte Teile von Nachrichten von Zwischensystemen gelesen werden müssen.

- Zur Schutz von Kommunikationsereignissen sind lediglich Dienste definiert, welche die Ableitung von Informationen aus der Beobachtung von Netzverkehr verhindern (*Traffic Flow Confidentiality*). Dienste zum gezielten Schutz von Steuerungsdaten werden nicht explizit angesprochen, können aber aus den Diensten zum Schutz verbindungsloser Nutzdaten abgeleitet werden.

- Integritätsdienste gliedern sich entsprechend der Art der geschützten Nutzdaten (*Connection Integrity, Connectionless Integrity*). Es werden Dienste definiert, die lediglich bestimmte Felder von Nachrichten gegen unautorisierte und unbemerkte Veränderung schützen (*Selective Field Integrity*). Diese Dienste sind sinnvoll, wenn bestimmte Teile einer Nachricht während ihrer Übermittlung zwischen Sender- und Empfängerinstanz (z. B. in Zwischensystemen) verändert werden müssen.

- Nichtabstreitbarkeitsdienste gliedern sich in Dienste zum Nachweis der Urheberschaft von Nachrichten (*Proof of Origin*) und zum Nachweis des Erhalts von Nachrichten (*Proof of Delivery*). Sie müssen entsprechende Nachweise generieren, welche im Falle des Abstreitens der Urheberschaft bzw. des Erhaltes von Nachrichten zur Beweisführung herangezogen werden können. Der Beweiswert der Nachweise hängt vom jeweiligen Anwendungsfall, vom rechtlichen Umfeld und von der Realisierung des Dienstes ab.

Die genannten Dienste stellen Basisdienste dar. Diese können in der Praxis in unterschiedlichen Schichten implementiert werden. Auch die Kombination unterschiedlicher Sicherheitsdienste ist möglich. Neben allgemeinen Sicherheitsbegriffen und Sicherheitsdiensten beschreiben die Standards eine Zuordnung von Sicherheitsmechanismen zu den unterschiedlichen Sicherheitsdiensten. Außerdem werden die unterschiedlichen Sicherheitsdienste mit den 7 Schichten des OSI-Referenzmodells in Beziehung gesetzt. Bild 3-8 zeigt die Sicherheitsstandards der ITU im Überblick.

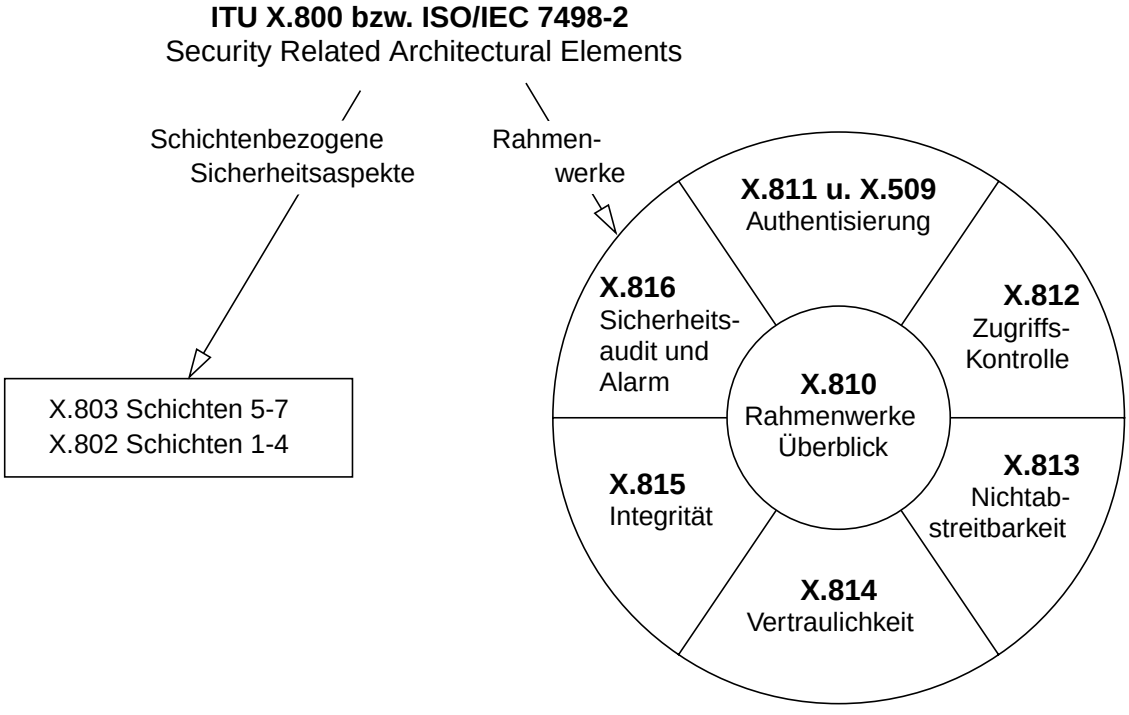


Bild 3-8: Sicherheitsstandards der ITU

Die Beziehung von Sicherheitsdiensten und Schichten des OSI-Referenzmodelles wird durch die beiden Empfehlungen X.802 [119] und X.803 [120] verfeinert dargestellt. Die ITU-Empfehlung X.802 beschreibt schichtenübergreifende Aspekte von Sicherheitsdiensten für die Transport-, Vermittlungs-, Datensicherungs- und Bitübertragungsschicht (Lower Layers). Es werden der Aufbau einer Sicherheitsassoziation zur Vereinbarung von gemeinsamen Schlüsseln, Algorithmen und Protokollen sowie ein allgemeines Austauschformat für Sicherheits-PDUs beschrieben. Die Empfehlung schließt mit Plazierungsmöglichkeiten für spezielle OSI-Sicherheitsdienste (Transport Layer Security Protocol, TLSP [89], Network Layer Security Protocol, NLSP [90]).

Aspekte von Sicherheitsdiensten für die höheren Schichten (Kommunikationssteuerungs-, Datendarstellungs- und Verarbeitungsschicht, Upper Layers) werden in X.803 zusammengefaßt. Diese Empfehlung definiert ein Basismodell

- zur Entwicklung anwendungsunabhängiger Sicherheitsdienste und Protokolle.
- zur Nutzung dieser Dienste und Protokolle zur Erfüllung von Sicherheitsanforderungen eines breiten Spektrums von Anwendungen.

Dieses zielt darauf ab, die Anzahl anwendungsabhängiger Anwendungsdiensteinheiten (Application Service Entities, ASEs) zu minimieren.

Diese Empfehlung wird durch weitere Empfehlungen X.83x ergänzt, welche Sicherheitsdienste für diese höheren Schichten näher spezifizieren. Die höheren Schichten des OSI-Referenzmodelles sind jedoch selten standardgemäß implementiert, so daß diese Empfehlungen bislang keine große Relevanz erlangen und Weiterentwicklung erfahren. Innerhalb der Steuerungs-Ebene des ISDN an der Benutzer-Netzschnittstelle (vgl. Bild 2-7) werden keine höheren OSI-Schichten implementiert. Dies gilt für IP-basierte Netze generell. Sicherheitsdienste höherer Schichten werden hier deshalb nicht explizit adressiert, weil ihr Vorhandensein bei der Definition einer Sicherheitsarchitektur nicht vorausgesetzt werden kann.

Die *Rahmenwerke* für Sicherheitsdienste sind in den Empfehlungen X.81x der ITU definiert und beschreiben die Anwendung von Sicherheitsdiensten in offenen Diensteumgebungen. Sie definieren Hilfsmittel zum Schutz von Systemen und Objekten innerhalb von Systemen und, was für diese Arbeit von besonderer Bedeutung ist, zwischen Systemen. Sie befassen sich jedoch nicht mit der Konstruktion sicherer Systeme oder mit technischen Sicherheitsmechanismen. Die Rahmenwerke geben auch keine Protokolle für Sicherheitsdienste vor. Zu jedem der X.81x Empfehlungen existiert ein inhaltlich identischer Standard der ISO, der in der Literaturreferenz angegeben ist. Die Rahmenwerke für die einzelnen Dienste (siehe Bild 3-8) werden zusammen mit den Sicherheitsdiensten in Abschnitt 4.3 eingeführt. Einen Überblick über die Rahmenwerke und übergeordnete Konzepte (z. B. Vertrauen, Sicherheitskennzeichen, Wechselwirkungen zwischen Sicherheitsdiensten) gibt die ITU-Empfehlung X.810 [121].

Darüberhinaus erweitert die ITU-Empfehlung H.235 [91] die Architektur der H3.xx-Serie über audiovisuelle und Multimedia-Systeme um Authentisierungs- und Datensicherheitsdienste. Diese Empfehlung befindet sich in der Entwicklung. Sie könnte mit den damit in Verbindung stehenden Empfehlungen zur H.323 (paketbasierte Multimedia-Kommunikationssysteme) und H.245 (Steuerungsprotokoll für Multimedia-Kommunikation) im Zuge der Weiterentwicklung der paketbasierten Netze steigende Bedeutung erlangen. Dem Anspruch, eine Sicherheitsarchitektur zu definieren, wird die Empfehlung in der Version von 1998 nur in sehr eingeschränktem Maße gerecht. In dieser Version werden vor allem Definitionen gegeben und Sicherheits-

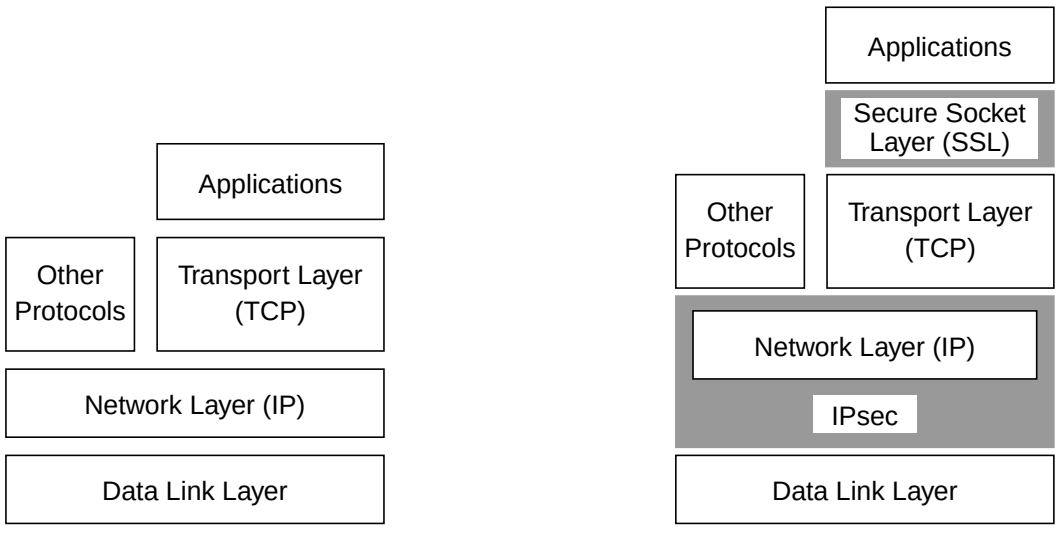
bausteine beschrieben. Die Beziehungen zwischen den bestehenden und den neu definierten Komponenten sind nicht ausgeprägt.

3.5.2 Sicherheitsstandards der IETF

Aufgrund der hohen Verbreitung von IP-basierten Netzen und ihrem Zusammenwachsen mit öffentlichen Netzen (ISDN, B-ISDN, GSM), werden IP-basierte Sicherheitslösungen in diese Arbeit miteinbezogen. Eine sinnvolle und benutzerfreundliche Sicherheitsarchitektur muß letztendlich unterschiedliche Netztechniken integrieren und netzübergreifende Sicherheitsdienste unterstützen.

Die IETF kümmert sich vor allem um die praktische Anwendung von Protokollen und Diensten in IP-basierten Netzen. Dort werden unterschiedliche Sicherheitsdienste spezifiziert und im Detail beschrieben. Diese Dokumente (Request For Comments, RFCs) sind von besonderer praktischer Bedeutung für kompatible Sicherheitsdienste in sich entwickelnden IP-basierten Netzen. Implementierungen der von der IETF vorgeschlagenen Dienste sind weit verbreitet und werden speziell im Hinblick auf die praktische Anwendung entwickelt. Die folgende Beschreibung beschränkt sich auf die bereits angedachten und teilweise implementierten Sicherheitsprotokolle und Sicherheitsarchitekturen. Auf die zugrundeliegenden Kommunikationsprotokolle IP-basierter Netze wird durch Referenzen verwiesen. Die Dokumente der IETF sind im Internet frei zugänglich. Die Struktur der IETF und die Handhabung ihrer Dokumente ist in einem eigenen Dokument [134] beschrieben.

Für diese Arbeit sind besonders der Secure Socket Layer (SSL [129]) und Sicherheitsdienste für das Internet Protocol (IPsec [138]) interessant. Sie stellen zwar keine Sicherheitsarchitektur mit Benutzerbezug dar, sind aber aufgrund der verwendeten Mechanismen und Protokolle auch für die vorliegende Arbeit interessant. Bild 3-9 zeigt links den ursprünglichen Protokollturm IP-basierter Netze. Rechts sind die Erweiterungen durch Sicherheitsfunktionen des SSL und von IPsec eingezeichnet.



(a) Protokoll-Turm IP-basierter Netze (b) Protokoll-Turm mit Sicherheitsfunktionen

Bild 3-9: SSL und IPsec in IP-basierten Netzen

Der *Secure Socket Layer* implementiert Sicherheitsfunktionen in einer Zwischenschicht, die direkt auf dem Transmission Control Protocol (TCP [132]) der Transportschicht aufsetzt. Da

die Schichten 5-7 in IP-basierten Netzen nicht implementiert sind, kann die SSL-Funktionalität auch direkt in die Anwendung integriert werden. Dies ist z. B. beim Netscape Navigator geschehen. SSL beinhaltet eine einfache Aushandlung von Sicherheitsparametern, die gegenseitige Authentisierung von Kommunikationspartnern (hier: Client und Server) mit Verfahren der symmetrischen und asymmetrischen Kryptographie, sowie den Schutz von übermittelten Nutzdaten vor unautorisierter Kenntnisnahme und vor unerkannter unautorisierter Veränderung.

Die *Sicherheitsdienste für das Internet Protocol* (IP [133]) sind der Vermittlungsschicht zuzurechnen. Sie werden im allgemeinen unter dem Begriff IPsec [138] zusammengefaßt. IPsec umfaßt Protokollerweiterungen des IP zur Authentisierung und zur Verschlüsselung von IP-Paketen. In der neuen Version des Internet Protocols (IP Version 6, IPv6 [136]) sind diese Mechanismen bereits integraler Bestandteil der Vermittlungsschicht. Die Sicherheitsmechanismen von IPsec lassen sich sowohl auf die PDUs der jeweiligen Transportprotokolle (TCP, etc.) als auch auf IP-Datagramme abbilden. Im ersten Fall sind die Sicherheitsfunktionen oberhalb der herkömmlichen IP-Funktionalität, im zweiten Fall an der unteren Grenze der IP-Schicht integriert. Werden IP-PDUs (Datagramme) verschlüsselt, so wird dem verschlüsselten Datagramm ein neuer Paketkopf im Klartext vorangestellt. Basierend auf diesem Paketkopf wird das Paket zu dem Knoten vermittelt, der die inverse Sicherheitsfunktion (hier: Entschlüsselung) vornimmt. Damit ist die Kompatibilität von durch Sicherheitsfunktionen erweiterten mit herkömmlichen IP-Knoten gewährleistet.

Das Zusammenwachsen von IP-basierten Netzen (Internet) und öffentlichen Telefonnetzen (Public Switched Telephone Network, PSTN) dokumentiert sich u. a. in der *PINT-Arbeitsgruppe (PSTN/Internet Inter-Networking Working Group)*. Sie untersucht Technologien und Architekturen, die es Internet-Anwendungen ermöglichen, Dienste im PSTN zu nutzen und zu erweitern (siehe RFC 2458 [137]). Die zugehörigen Dokumente beschränken sich im Bezug auf Sicherheitsaspekte in ihrer derzeitigen Form auf die Nennung von Sicherheitsanforderungen an Infrastruktur und Dienste.

3.5.3 Weitere Standardisierungsaktivitäten

Das European Telecommunications Standards Institute (ETSI) befaßt sich im Projekt *TIPHON* (Telecommunications and Internet Protocol Harmonization Over Networks) vor allem mit Sprachkommunikation und verwandten Kommunikationsdiensten (z. B. Telefax). Primäres Ziel ist die Schaffung globaler Standards unter Einbeziehung von IETF und ITU zur Verbesserung der Zusammenarbeit von paketvermittelnden Netzen (Internet) und leitungsvermittelnden Netzen (ISDN, Analoges Fernsprechnetz) zur Erbringung dieser Dienste. Die TIPHON-Arbeitsgruppe befaßt sich u. a. mit der Spezifikation von Protokollen und zugehörigen Parametern und Sicherheitsmechanismen für die Internet-Telefonie [77]. Eine umfassende Sicherheitsarchitektur für netzübergreifende Dienste (z. B. ISDN / Internet) wird augenblicklich noch nicht angesprochen.

Das Institute of Electrical and Electronics Engineers (IEEE) hat mit dem Standard IEEE 802.10 eine Zwischenschicht (Secure Data Exchange, SDE [130]) vorgeschlagen, die die Datensicherungsschicht in Lokalen Netzen um Sicherheitsfunktionen erweitert. Benutzerkontrollierbare Sicherheitsdienste oder eine entsprechende Sicherheitsarchitektur sind darin nicht enthalten. Die vorgeschlagenen Sicherheitsfunktionen dienen vor allem als Basisschutz gegen Angreifer an Übertragungsstrecken.

Ein kurzer Überblick über weitere Sicherheitsstandards der ISO, der ITU, des IEEE und der European Computer Manufacturers Association (ECMA) befindet sich im Anhang A der NIST Veröffentlichung 800-7 [124].

Kapitel 4

Mechanismen für mehrseitig sichere Telekommunikationsdienste

Dieses Kapitel behandelt Sicherheitsdienste, mit Hilfe derer Sicherheitsfunktionalität in Kommunikationsabläufe eingebunden werden kann. Ein *Sicherheitsdienst* umfaßt alle funktionalen Eigenschaften eines Kommunikationsnetzes und aufsetzender Anwendungen, welche zur nachvollziehbaren Erfüllung bestimmter Schutzziele in einer Kommunikationsbeziehung beitragen. Ein Telekommunikationsdienst wird als *sicher* bezeichnet, wenn er neben den Anforderungen an die Kommunikationsaspekte auch alle Anforderungen an die Sicherheitsaspekte (Schutzziele) erfüllt. Spiegeln sich in den für einen Dienst spezifizierten Schutzzielen die Sicherheitsinteressen aller Beteiligten in einem fairen Verhältnis wider, so wird der Dienst *mehrseitig sicher* genannt.

Zur Aushandlung und zur nachvollziehbaren Erfüllung von Schutzzielen im ISDN müssen dort neue Funktionen eingebracht werden. Ein Telekommunikationsdienst, der die Sicherheitsanforderungen nicht inhärent erfüllt, kann somit durch Zuschalten von Sicherheitsfunktionen zu einem sicheren Telekommunikationsdienst erweitert werden. Die Integration von Sicherheitsdiensten in Form additiver Sicherheitsfunktionen wird in Abschnitt 4.1 vorgestellt. Der additive Ansatz bildet die Grundlage für die in dieser Arbeit vorgeschlagene Sicherheitsarchitektur.

Wo diese neuen Sicherheitsfunktionen integriert werden können und welche Auswirkungen die Plazierung von Sicherheitsfunktionen auf ihre Wirkung gegen verschiedene Angriffe und Angreifer besitzt, wird in Abschnitt 4.2 untersucht.

In Abschnitt 4.3 werden Dienstzugangspunkte exemplarischer Sicherheitsdienste (kooperierende, verteilte Sicherheitsfunktionen) vorgestellt und ihre Anforderungen an die Diensteumgebung hergeleitet. Über diese Dienstzugangspunkte sind die Beziehungen von Sicherheitsdiensten zu ihrer Umgebung definiert.

Schließlich stehen in Abschnitt 4.4 die Beziehungen zwischen Sicherheitskomponenten untereinander und mit ihrer Umgebung (Telekommunikationskomponenten, Benutzer etc.) im Vordergrund. Es werden *Komponenten* vorgestellt, die diese *Beziehungen* (z. B. Kopplung von Sicherheits- und TK-Dienst) unterstützen. Die in diesem Kapitel eingeführte allgemeine Sicherheitsarchitektur unterstützt den additiven Ansatz und ermöglicht die Erweiterung bestehender Kommunikationsnetze um Sicherheitsdienste. Sie schafft durch die Unterstützung von flexibel definierbaren Beziehungen zwischen Telekommunikations- und Sicherheitsdiensten die Basis für mehrseitig sichere Telekommunikationsdienste.

4.1 Additiver Ansatz

Da die Investitionskosten für Kommunikationsinfrastruktur enorm sind, müssen diese Ressourcen als Basis bestehender und neuer Dienste langfristig genutzt werden. Gleichzeitig steigen die Anforderungen an die Sicherheitsaspekte, welche oftmals bei der Einführung neuer Systeme und Dienste noch nicht konkretisiert werden können und deshalb nur unzulänglich Berücksichtigung finden.

Deshalb wird hier der Ansatz verfolgt, durch Hinzufügen von Funktionalität und Infrastruktur die bestehenden Dienste so anzureichern, daß bei der bisherigen Entwicklung unzureichend berücksichtigte und sich neu entwickelnde Schutzziele erfüllt werden können. Das Prinzip des additiven Ansatzes zur Integration von Sicherheitsfunktionen ist in Bild 4-1 dargestellt.

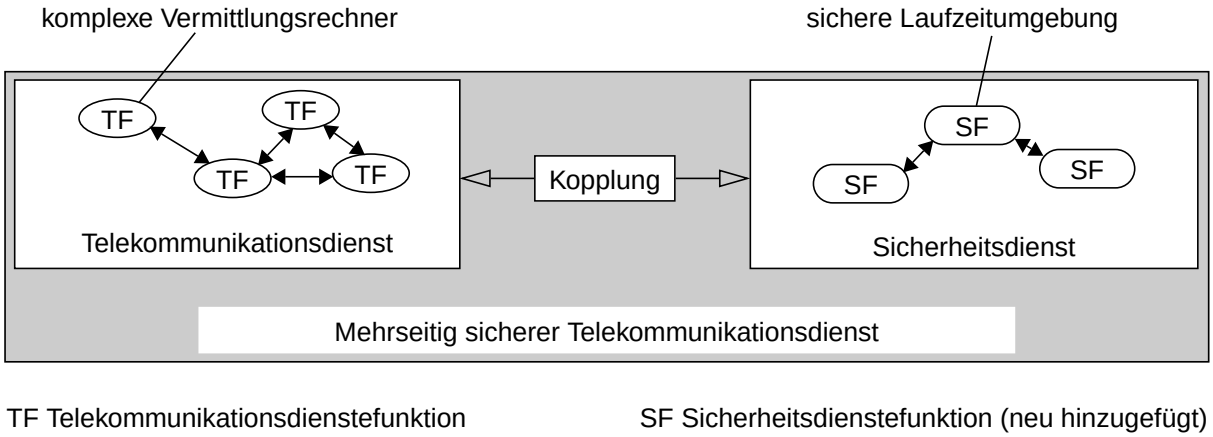


Bild 4-1: Additiver Ansatz zur Realisierung von Sicherheitsdiensten

Mehrseitig sichere Telekommunikationsdienste lassen sich aus bestehenden Telekommunikationsdiensten (verteilten, kooperierenden Funktionen) ableiten, indem Sicherheitsfunktionen hinzugefügt und mit den bestehenden Dienstefunktionen geeignet verknüpft werden.

Der additive Ansatz wurde in [25] und [30] zur Anreicherung der Verbindungssteuerung im ISDN um Funktionen zur Authentisierung eingesetzt. Er wird hier zur Integration allgemeiner Sicherheitsdienste erweitert. Additiv bedeutet hier, daß die hinzugefügten Sicherheitsdienstefunktionen das Zusammenspiel der bestehenden Dienstefunktionen nicht beeinträchtigen. Durch Kopplung von Sicherheitsfunktionen und bestehenden Dienstefunktionen entstehen neue Telekommunikationsdienste, die bestimmte Schutzziele nachvollziehbar erfüllen.

4.1.1 Integration und Kooperation von Sicherheitsfunktionen

Die Kombination von Sicherheitsmechanismen – z. B. Verschlüsselung und Entschlüsselung – dient als Grundlage zukünftiger Sicherheitsdienste. Sicherheitsdienste werden in Kommunikationssystemen in Form verteilter Funktionalität (z. B. Verschlüsselung beim Sender, Entschlüsselung beim Empfänger) implementiert. Die kooperierenden Funktionen laufen i. a. in unterschiedlichen Prozessen auf unterschiedlichen Kommunikationssystemen ab. Daraus entstehen folgende allgemeine Anforderungen an das zugrundeliegende verteilte System – in diesem Falle das Kommunikationsnetz bzw. die Kommunikationssysteme:

- Die an der Erbringung der Gesamtfunktionalität eines Sicherheitsdienstes beteiligten Prozesse müssen *identifiziert* werden können (Auswahl, Adressierung).

- Zur Erbringung der Gesamtfunktionalität eines Sicherheitsdienstes müssen sich die beteiligten Prozesse über den Austausch von (eindeutig interpretierbaren) Nachrichten *synchronisieren* können.

- Zur Garantie der Kompatibilität muß *aushandelbar* sein, welche Funktionen innerhalb der Prozesse verwendet werden.

Die Integration von Sicherheitsdiensten in Kommunikationsnetze orientiert sich stark an der Implementierung von Kommunikationsdiensten. Zusätzliche Freiheitsgrade (z. B. Algorithmen, Betriebsweisen) führen dabei zu unterschiedlichen Implementierungen desselben Dienstes (z. B. Verschlüsselungsverfahren nach IDEA oder DES). Während im ISDN die nutzbaren Mechanismen (z. B. Fehlersicherung) festgelegt sind, ist dies für Sicherheitsmechanismen aus vielerlei Gründen nicht wünschenswert[1]. Dies macht eine dynamische Aushandlung verwendeter Sicherheitsdienste und daraus resultierender Sicherheitsmechanismen erforderlich.

4.1.2 Sichere Laufzeitumgebungen für Sicherheitsfunktionen

Sicherheitsfunktionen müssen vor Manipulation und Ausspähung geschützt sein, d. h. in einer bezüglich des gültigen Angreifermodelles sicheren Umgebung ablaufen. Sonst arbeiten die Sicherheitsfunktionen – selbst bei korrekter Implementierung – nicht nachvollziehbar bzw. die geheimen Schlüssel können ausgespäht werden [16]. Damit sind diese Sicherheitsfunktionen im Sinne nachvollziehbar sicherer Dienste nutzlos.

Eine Laufzeitumgebung wird als sicher bezeichnet, wenn sie gegen relevante Bedrohungen (siehe Bild 3-3) geschützt ist[2]. Sichere Laufzeitumgebungen sind sowohl für die Vertrauenswürdigkeit, als auch für die Effektivität von Sicherheitsdiensten notwendig. Anforderungen an sichere und portable Laufzeitumgebungen werden in [15] diskutiert.

Beispiele heute bereits verfügbarer, nachvollziehbar sicherer Laufzeitumgebungen sind Smartcards [67] oder der an einen PCI-Prozessorbus anschließbare IBM Cryptographic Coprocessor [31],[32]. Durch eine unabhängige Evaluation und den evaluierungsfreundlichen Entwurf von Laufzeitumgebungen wird auch die Nachvollziehbarkeit eines nicht in allen Einzelheiten offengelegten oder verstehbaren Produktes begünstigt.

Die heute im Einsatz befindlichen Kommunikationsendgeräte, insbesondere Rechner, sind aufgrund ihrer Komplexität nicht umfassend prüfbar und weisen eine Vielzahl von Sicherheitslükken auf. Sie sind i. a. bei hohem Schutzbedarf als sichere Laufzeitumgebung völlig ungeeignet. Die Ursachen dafür sind vielfältig, aber alleine die hochkomplexe Software ist nicht befriedigend prüfbar und gegen Manipulation zu schützen. Sicherheitsrelevante Funktionen sollten deshalb modular sein und möglichst wenige funktionale Abhängigkeiten zu nicht sicherheitsrelevanten Funktionen aufweisen. Dieses erleichtert die Auslagerung sicherheitsrelevanter Funktionen auf separate, möglicherweise teure, aber dafür nachvollziehbar sichere Laufzeitumgebungen.

---

1 Ein Verschlüsselungsverfahren könnte beispielsweise aufgrund einer Schwäche des zugrundeliegenden Algorithmus gebrochen werden. In diesem Fall muß ohne Änderung des Netzes oder der Kommunikationssysteme ein Wechsel auf ein anderes Verfahren möglich sein. Dies gilt entsprechend für die Implementierung eines Sicherheitsmechanismus (z. B. im Falle von Implementierungsfehlern). Es werden folglich nicht nur Implementierungen unterschiedlicher Verfahren sondern auch verschiedene Implementierungen desselben Verfahrens unterschieden.

2 Die Menge der relevanten Bedrohungen hängt nach Abschnitt 3.3.3 u. a. von der Stärke der Angreifer ab, gegen die ein System oder Dienst schützen soll.

Die Integration von sicheren Laufzeitumgebungen zur Einbeziehung darin ausgelagerter Sicherheitsfunktionen muß durch die Diensteumgebung unterstützt werden. Darüber hinaus müssen Benutzer die Möglichkeit besitzen, Laufzeitumgebungen vor ihrer Benutzung auf ihre Sicherheit hin zu prüfen. Dies kann durch Abruf von digital signierten Nachweisen realisiert werden (ähnlich der TÜV-Plakette, die die Verkehrssicherheit von Fahrzeugen auch gegenüber Laien bestätigt).

4.2 Plazierung und Wirkungsbereich von Sicherheitsfunktionen

In diesem Abschnitt wird vorrangig untersucht, wo Sicherheitsfunktionen plaziert werden können und wie sich die Plazierung auf die erreichbare Sicherheit auswirkt.

Die Plazierung von Sicherheitsfunktionen entscheidet darüber, welche Art von Daten gegenüber welchen Angreifern geschützt werden können. Dadurch sind auch die Schutzziele festgelegt, die durch diese Funktionen höchstens garantiert werden können. Zunächst werden die prinzipiellen Freiheitsgrade bei der Plazierung von Sicherheitsfunktionen besprochen. Es werden Randbedingungen aufgezeigt, die aus der Transparenz von hinzugefügten Sicherheitsfunktionen bezüglich bestehender Kommunikationsdienste resultieren. Danach wird die Wirksamkeit von Sicherheitsfunktionen – im Hinblick auf die zu garantierenden Schutzziele – in Abhängigkeit von der Plazierung der Sicherheitsfunktionen und angenommener Angriffsmöglichkeiten untersucht. Die Grundlagen dieses sogenannten Allokationskonzeptes sind in [44] ausführlich erläutert und werden hier erweitert und auf das ISDN angewendet.

4.2.1 Allgemeine Integrationsmöglichkeiten für Sicherheitsfunktionen

Zur Integration von Sicherheitsfunktionen in Kommunikationssysteme bestehen grundsätzlich zwei Freiheitsgrade (vgl. Bild 4-2):

- Der *horizontale Freiheitsgrad* bezeichnet die Auswahl einer Komponente. Komponenten im Teilnehmerbereich umfassen i. a. ISDN-Terminals, zusätzliche Infrastruktur oder den Netzwerkabschluß bzw. die Telekommunikationsanlage. Zusätzliche Infrastruktur stellt beispielsweise ein in die Anschlußleitung oder die Hausverkabelung (Referenzpunkte S,T bzw. U vgl. Bild 2-3) eingeschleiftes Verschlüsselungsgerät dar.
- Der *vertikale Freiheitsgrad* bezeichnet die innerhalb einer Komponente vorhandenen Plazierungsmöglichkeiten. Hier können Zwischenschichten innerhalb der Schichtenarchitektur integriert werden oder Sicherheitsfunktionen direkt in die Anwendungen selbst eingebracht werden.

Die verschiedenen Ebenen (Steuerungs-, Nutzer- und Management-Ebene) innerhalb eines Kommunikationssystems stellen i. a. keinen Freiheitsgrad dar. Die Ebene ist meist durch die Art der zu schützenden Daten festgelegt.

Aufgrund der hohen Investitionskosten existierender ISDN-Netzinfrastruktur müssen Erweiterungen kompatibel gestaltet werden. Dies bedeutet, daß additiv hinzugefügte Sicherheitsdienste die bestehenden Dienste nicht stören dürfen. Darüber hinaus sollen erweiterte und herkömmliche Endgeräte und Netzinfrastrukturbestandteile weiterhin zusammenarbeiten können.

Grundsätzlich können Kommunikationssysteme durch Integration von Sicherheitsfunktionen in die Anwendung oder in die Schichtenfunktionen erweitert werden. Bild 4-3 zeigt im Fall (a) die Erweiterung einer Anwendung um Sicherheitsfunktionen. Dazu muß jede Anwendung erweitert werden, die sicherheitsrelevante Daten erzeugt oder verarbeiten möchte. Dies ermög-

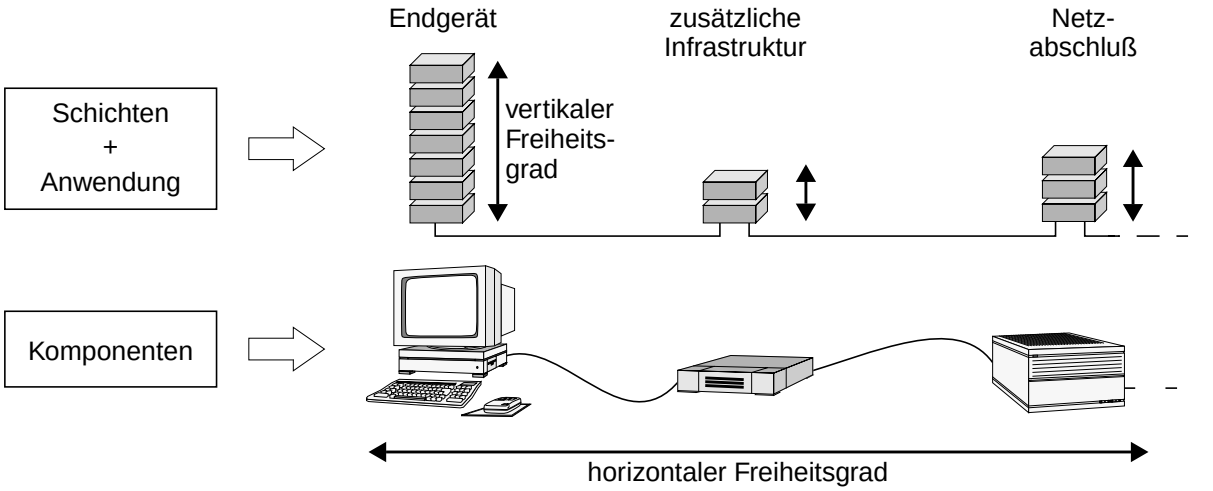


Bild 4-2: Freiheitsgrade bei der Plazierung von Funktionen im Teilnehmerbereich

licht einerseits maßgeschneiderte Sicherheitsfunktionalität für unterschiedliche Anwendungsdaten, bedingt andererseits jedoch erheblichen Aufwand zur Installation und zur Wartung bzw. Weiterentwicklung von Sicherheitsfunktionen. Dieser anwendungsorientierte Ansatz kann weitgehend unabhängig vom zugrundeliegenden Kommunikationsnetz gestaltet werden.

Beim zweiten Ansatz werden Sicherheitsfunktionen – transparent für Anwendungen – in Kommunikationsschichten integriert (siehe Bild 4-3, Fall b). Dabei können bestehende Schichtenimplementierungen ergänzt, oder es kann eine neue Zwischenschicht integriert werden. Dieser Ansatz ist anwendungsunabhängig und wirkt für alle Anwendungen, die über diese Zwischenschicht kommunizieren. Im folgenden wird der Ansatz der transparenten Zwischenschicht gegenüber der Erweiterung bestehender Schichtenfunktionen bevorzugt. Durch dieses Vorgehen werden Protokolle für Sicherheitsdienste klar von Protokollen für Telekommunikationsdienste getrennt. Dies begünstigt die Kompatibilität unterschiedlicher Implementierungen erweiterter Systeme und deren Kompatibilität zu herkömmlichen (nicht erweiterten) Systemen.

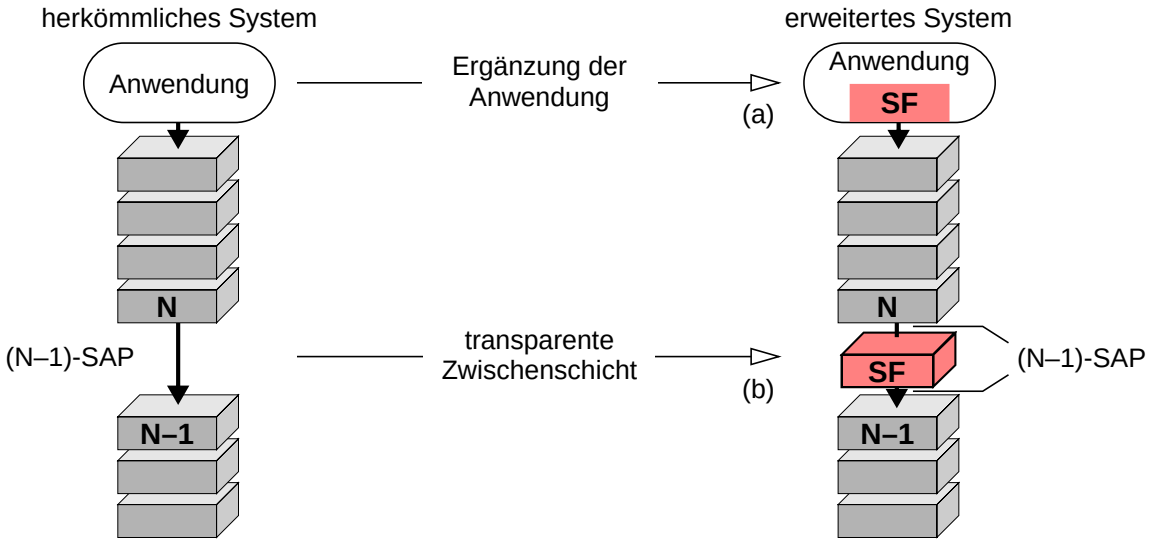


Bild 4-3: Integration von Sicherheitsfunktionen in Kommunikationssysteme

Sicherheitsfunktionen werden bezüglich bestehender Telekommunikationsfunktionen als transparent bezeichnet, wenn sie deren Zusammenwirken nicht stören. Der additive Ansatz verlangt die Transparenz neu hinzugefügter Sicherheitsfunktionen. Die sich daraus ableitenden Randbedingungen für Sicherheitsfunktionen in Form einer Zwischenschicht werden in den folgenden Unterabschnitten strukturiert.

Transparenz bezüglich existierender Dienstefunktionen

Bei der Integration von Sicherheitsfunktionen in Kommunikationssysteme lassen sich Transparenzanforderungen mit Hilfe der Schichtenarchitektur des OSI-Referenzmodelles [115] veranschaulichen. Im folgenden werden die im Standard zum OSI-Referenzmodell definierten Begriffe verwendet.

Additiv eingebrachte Sicherheitsfunktionen dürfen weder die Dienstschnittstellen zwischen existierenden Schichten verändern noch den Nachrichtenaustausch zwischen Partnerinstanzen stören. Die Sicherheitsfunktionen in Bild 4-4 dürfen weder die Instanz PI_1 noch die Instanz PI_2 beim Zugriff auf Dienste darunterliegender Schichten beeinträchtigen.

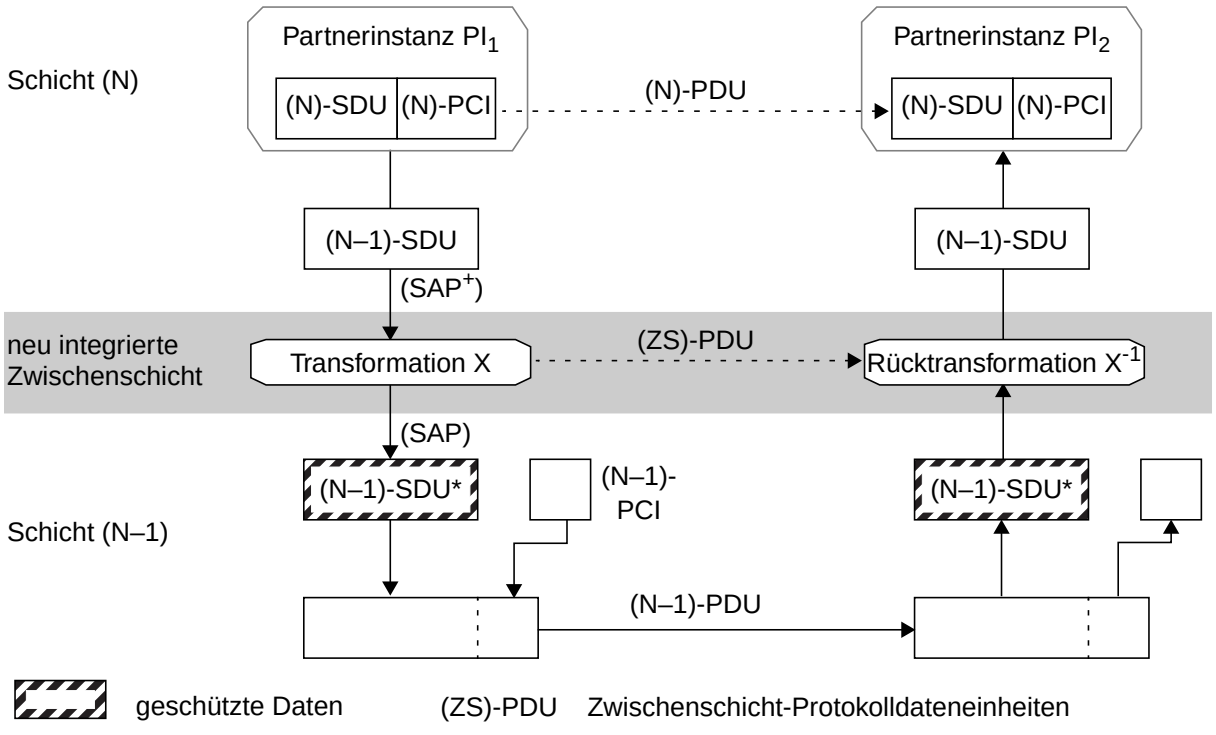


Bild 4-4: Transparenz additiver Sicherheitsfunktionen

Sicherheitsdienste werden als *vertikal transparent* (bezüglich der vertikalen Kommunikation im OSI-RM) bezeichnet, wenn sie bestehende Dienstzugangspunkte beibehalten oder lediglich um optionale Parameter – z. B. zur Steuerung der integrierten Sicherheitsfunktionen – und Primitive erweitern (vgl. SAP^+ in Bild 4-4). Dies bedeutet, daß der Austausch von Dienstdateneinheiten (Service Data Unit, SDU) zwischen der Schicht (N) und der Schicht (N–1) nicht beeinträchtigt wird. Verändern die Sicherheitsfunktionen die Länge der über die Schnittstelle ausgetauschten Dienstdateneinheiten (z. B. beim Hinzufügen von Integritätsprüfsummen), so ist die maximale Länge von Dienstdateneinheiten zu beachten. Vertikale Transparenz kennzeichnet die Transparenz von Sicherheitsfunktionen innerhalb eines einzelnen Telekommuni-

kationssystems. Der neu entstehende Dienstzugangspunkt SAP^+ ist bei gegebener vertikaler Transparenz kompatibel zum ursprünglichen Dienstzugangspunkt *SAP*.

Sicherheitsdienste werden als *horizontal transparent* (bezüglich der horizontalen Kommunikation im RM) bezeichnet, wenn sie den Austausch von Protokolldateneinheiten zwischen Partnerinstanzen nicht beeinträchtigen. Bild 4-4 veranschaulicht den Einfluß von Sicherheitsfunktionen auf den Austausch von Protokolldateneinheiten (Protocol Data Unit, PDU) zwischen Partnerinstanzen. Zur Garantie horizontaler Transparenz dürfen verändernde Sicherheitsfunktionen im Weg der PDUs zwischen Partnerinstanzen nur paarweise (Transformation und Rücktransformation) auftreten. Fehlte beispielsweise die Rücktransformation (X^{-1}) unterhalb der Partnerinstanz PI_2 in Bild 4-4, so könnte diese Instanz die ankommende Dienstdateneinheit (N–1)-SDU* nicht verarbeiten, bzw. die zur Verarbeitung notwendige Protokoll-Kontrollinformation (N)-PCI nicht interpretieren.

Eine zusätzliche Transparenzforderung ergibt sich, wenn Zeitüberwachungsmechanismen oberhalb von eingebrachten Sicherheitsdiensten eingesetzt werden. Dann muß die durch den Sicherheitsdienst eingebrachte Verzögerungszeit innerhalb der Toleranzbereiche der Zeitüberwachungsmaßnahmen gehalten werden. Diese Transparenz ist nicht in allen Fällen garantierbar; in Grenzfällen kann die durch Sicherheitsfunktionen eingebrachte zusätzliche Verzögerung zur Auslösung einer Ausnahmebehandlung führen.

Kompatibilität von erweiterten und herkömmlichen Endgeräten

Aus der Forderung nach horizontaler Transparenz läßt sich auch die Forderung nach Kompatibilität auf Geräte-Ebene ableiten. Telekommunikationssysteme, welche um Sicherheitsfunktionen erweitert sind, sollten weiterhin mit herkömmlichen Telekommunikationssystemen zusammenarbeiten können. Beispielsweise sollten ISDN-Endgeräte mit und ohne Sicherheitserweiterung weiterhin über die herkömmlichen ISDN Dienste zusammenarbeiten. Dies wird durch optionale Sicherheitsfunktionen unterstützt, die je nach Bedarf zu- oder abgeschaltet werden können.

Kompatibilität erfordert auch den Austausch von Informationen über angebotene bzw. angeforderte Sicherheitsdienste zwischen Telekommunikationssystemen (z. B. Endgeräten). Das gerufene Endgerät muß vor der Annahme eines Rufes prüfen, ob es die geforderten Dienste (Telefaxdienst, Telefonsprachdienst, Sicherheitsdienste, etc.) unterstützt. Das rufende Endgerät muß dazu in der Lage sein, den geforderten Dienst mit der Dienstanforderung zu übermitteln. Nur so läßt sich sicherstellen, daß Transformation (beim Sender) und Rücktransformation (beim Empfänger) kompatibel und damit transparent sind.

4.2.2 Klassifizierung von Sicherheitsfunktionen

Sicherheitsfunktionen werden im Hinblick auf ihren Wirkungskreis klassifiziert, um Aussagen über ihre Leistungsfähigkeit zu verallgemeinern. Die hier vorgeschlagene Klassifizierung basiert auf den in [9] beschriebenen Beziehungen zwischen kooperierenden Instanzen, die gemeinsam eine Funktionalität erbringen. Sie dient als Grundlage für die Bewertung von Sicherheitsfunktionen und die mit ihrer Hilfe erreichbaren Schutzziele.

Sicherheitsfunktionalität wird genau dann als *Linklevel-Sicherheitsfunktionalität (Ll)* bezeichnet, wenn die enthaltenen Sicherheitsfunktionen durch benachbarte Knoten erbracht werden und sich auf einen einzelnen Übertragungsabschnitt beziehen. Ein Praxisbeispiel stellt Sicherheitsfunktionalität zum Schutz von Daten auf einer besonders gefährdeten Übertragungsstrecke (z. B. auf einer Richtfunkstrecke) dar.

Sicherheitsfunktionalität wird *Ende-zu-Ende (EzE)* genannt, wenn die beteiligten Sicherheitsfunktionen ausschließlich innerhalb von Endpunkten einer Kommunikationsbeziehung lokalisiert sind. Als Bezugssystem dient die Kommunikationsbeziehung aus Sicht der Kommunikationspartner. Sicherheitsfunktionen innerhalb kommunizierender Endgeräte oder zentraler Server können beispielsweise eine Authentisierung der Kommunikationspartner unterstützen.

Sicherheitsfunktionalität wird *Punkt-zu-Punkt (PzP)* genannt, wenn sich zwischen den erbringenden Knoten weitere Knoten befinden oder sich die Sicherheitsfunktionalität nicht auf eine einzelne physikalische Übertragungsstrecke bezieht. PzP-Sicherheit wird beispielsweise zur Sicherung von virtuellen privaten Netzen eingesetzt. Dort werden Daten vor ihrer Übermittlung zwischen verschiedenen Unternehmensstandorten innerhalb von ISDN-Routern oder sogenannten Firewalls [68] verschlüsselt. Sie sind dadurch während der Übermittlung über Zwischennetze (z. B. ISDN, Internet) vor unautorisierter Kenntnisnahme geschützt.

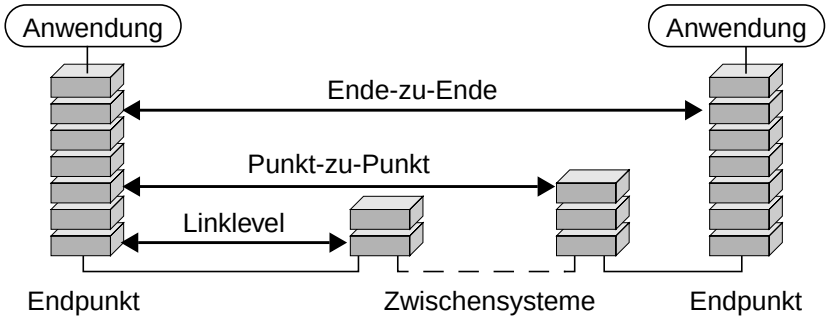


Bild 4-5: Klassifizierung von kooperierenden Sicherheitsfunktionen

Bild 4-5 illustriert die verschiedenen Klassen von Sicherheitsfunktionen. Es zeigt Ende-zu-Ende-, Punkt-zu-Punkt- und Linklevel-Sicherheitsfunktionalität.

Randbedingungen bei der Plazierung von Sicherheitsfunktionen

Als Folge der in Abschnitt 4.2.1 aufgezeigten Transparenzanforderungen lassen sich Grenzen für Ende-zu-Ende- und Punkt-zu-Punkt-Sicherheitsfunktionalität herleiten. Diese bedingen Einschränkungen des vertikalen Freiheitsgrades bei der Plazierung von Sicherheitsfunktionen. Zentral ist dabei die Aussage zur horizontalen Transparenz aus Abschnitt 4.2.1, daß Sicherheitsfunktionen auf dem Kommunikationspfad der PDUs zwischen Partnerinstanzen nur paarweise auftreten dürfen. Sonst wird i. a. die Kommunikation dieser Partnerinstanzen gestört.

Sicherheitsfunktionen höherer Schichten beeinflussen bei Einhaltung der Schichtenprinzipien [115] die Kommunikation von Partnerinstanzen niedrigerer Schichten nicht. Für darunterliegende Instanzen sind die Sicherheitsfunktionen deshalb transparent, weil SDUs höherer Schichten in der Regel nicht interpretiert, sondern transparent behandelt werden, solange Längenbeschränkungen beachtet werden.

Sind die Sicherheitsfunktionen als Zwischenschichten eingezogen, so verbleibt, Partnerinstanzen oberhalb der Sicherheitsfunktionen zu untersuchen. Es wird hier davon ausgegangen, daß die Sicherheitsfunktionen den durch Zeitüberwachungsmaßnahmen höherer Schichten gegebenen Randbedingungen genügen[3].

3 Ist dies nicht der Fall, so können zu den beschriebenen Randbedingungen weitere Einschränkungen bezüglich der Plazierung hinzukommen.

Die Verschlüsselung von (N–1)-SDUs verhindert die Interpretation der darin geschachtelten PDUs und PCIs in zwischen Ver- und Entschlüsselung liegenden (N)-Instanzen. Integritätsdienste fügen im allgemeinen Prüf-Information zu (N)-PDUs hinzu und verändern dadurch die Struktur der PDUs. Partnerinstanzen oberhalb solcher Sicherheitstransformationen dürfen folglich durch paarweise auftretende Sicherheitsfunktionen nicht getrennt werden, da sie sonst die empfangenen PDUs nicht verarbeiten können.

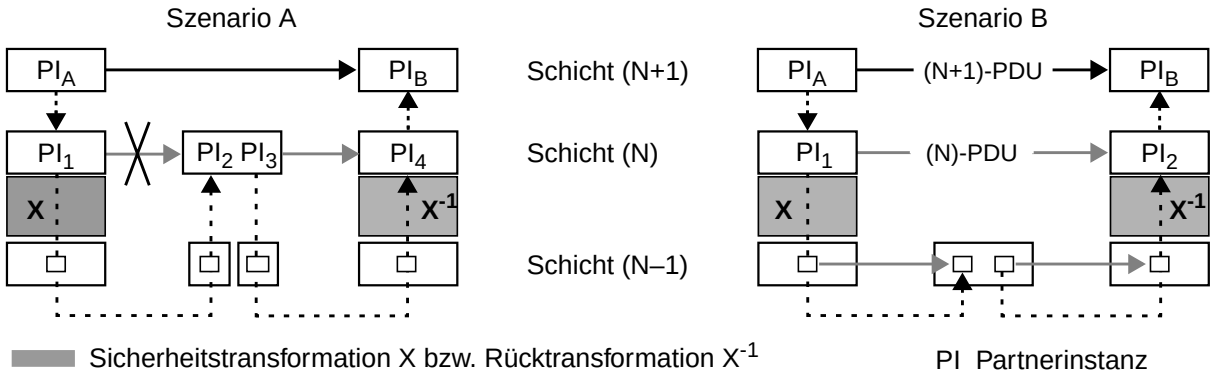


Bild 4-6: Herleitung von Grenzlinien für EzE- und PzP-Sicherheitsfunktionen

Bild 4-6 zeigt die graphische Interpretation der Randbedingungen für paarweise auftretende Sicherheitsfunktionen zum Schutz von zwischen Partnerinstanzen PI_A und PI_B ausgetauschten (N+1)-PDUs. In Szenario A werden diese (N+1)-PDUs mit Hilfe der Partnerinstanzen PI_1 und PI_2 (bzw. PI_3 und PI_4) innerhalb von (N)-PDUs übertragen. Der Austausch dieser (N)-PDUs ist jedoch gestört, da PI_1 und PI_2 durch Sicherheitsfunktionen (Transformation X in Bild 4-6) getrennt sind. Da die Sicherheitsfunktionen zwischen diesen Instanzen nicht paarweise auftreten, empfängt die Partnerinstanz PI_2 geschützte SDUs, die sie i. a. nicht interpretieren kann oder die nicht den Kodierungsvorschriften entsprechen. Auf die Kommunikation darunterliegender Partnerinstanzen im Kommunikationspfad (im Bild 4-6 lediglich durch Kästchen angedeutet) haben die Sicherheitsfunktionen keinen Einfluß.

Der Austausch von PDUs zwischen PI_3 und PI_4 kann entsprechend durch die Rücktransformation X^{-1} gestört sein, die entweder die ungeschützte SDUs transparent an PI_4 weiterleitet, diese verwirft oder aber durch die Anwendung der Rücktransformation so verändert, daß PI_4 diese nicht interpretieren kann. Die Kommunikation zwischen PI_3 und PI_4 wird nicht gestört, falls die Rücktransformation unterhalb von PI_4 selektiv auf zuvor transformierte (geschützte) SDUs angewendet wird.

In Szenario B (vgl. Bild 4-6) stören die Sicherheitsfunktionen keine Partnerinstanzen, da sie zwischen Partnerinstanzen ausschließlich paarweise oder gar nicht auftreten. (N+1)-PDUs können deshalb mit Hilfe geschützter (N)-PDUs der Schicht (N) übertragen werden.

Aus diesen Randbedingungen lassen sich Grenzen für den vertikalen Freiheitsgrad bei der Plazierung von Sicherheitsfunktionen innerhalb von Kommunikationssystemen ableiten. Resultierende Begrenzungen werden in Form sogenannter Grenzlinien für Ende-zu-Ende- und Punkt-zu-Punkt-Sicherheitsfunktionen angegeben.

- Die *Ende-zu-Ende-Grenzlinie* (EzE-Grenzlinie) beschreibt die untere vertikale Grenze für die transparente Implementierung von Sicherheitsfunktionen. Sie ist definiert durch die unterste Kommunikationsschicht, die in keinem Zwischensystem auf dem Kommunikationspfad zwischen den betrachteten Endpunkten durchlaufen wird (vgl. Bild 4-7). Bei Ein-

haltung der vertikalen Transparenz (vgl. Abschnitt 4.2.1) ist gewährleistet, daß Ende-zu-Ende-Sicherheitsfunktionen oberhalb der EzE-Grenzlinie keine Kommunikationsfunktionen in Zwischensystemen beeinflussen.

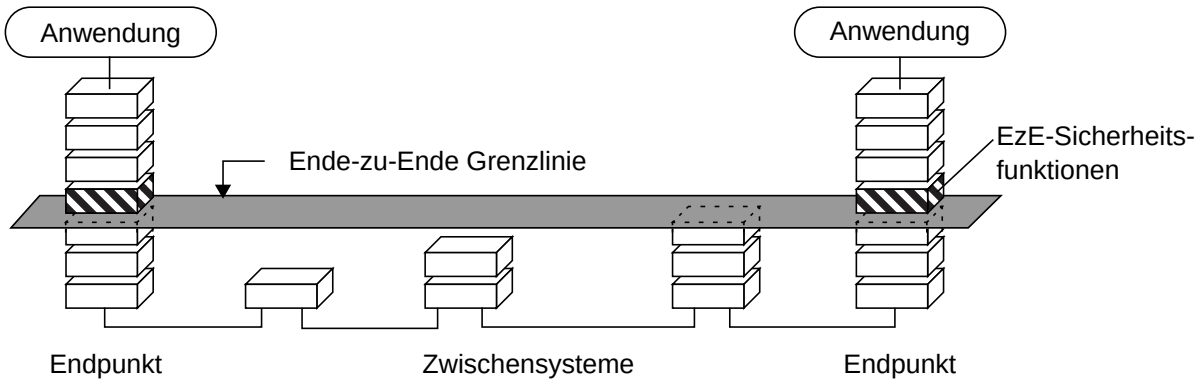


Bild 4-7: EzE-, PzP und Ll-Grenzlinien

In paketvermittelnden Netzen liegt die EzE-Grenzlinie i. a. an der oberen Grenze der Vermittlungsschicht. In leitungsvermittelnden Netzen (z. B. ISDN) liegt die EzE-Grenzlinie für die Steuerungs-Ebene i. a. auf Anwendungsebene, die EzE-Grenzlinie für die Nutzer-Ebene liegt dagegen an der oberen Grenze der Bitübertragungsschicht.

- Die Punkt-zu-Punkt-Grenzlinie (PzP-Grenzlinie) läßt sich aus obiger Definition leicht ableiten. Sie ist definiert durch die unterste Schicht, die in keinem Zwischensystem auf dem Kommunikationspfad zwischen zwei betrachteten Kommunikationssystemen durchlaufen wird. Bedeutung hat diese Grenzlinie zum Beispiel für die Beziehung zwischen Endsystemen und zentralen Servern im Netz (vgl. Bild 2-2), die eine Kommunikation unterstützten, jedoch keinen Endpunkt darstellen.

Aus diesen Zusammenhängen und resultierenden Randbedingungen erwachsen Einschränkungen für die Plazierung von Sicherheitsfunktionen. Nachfolgend wird der Einfluß dieser Randbedingungen auf die durch EzE-, PzP- und Ll-Sicherheitsfunktionen abwehrbaren bzw. nicht abwehrbaren Angriffe untersucht.

4.2.3 Wirkungsbereich von Sicherheitsfunktionen

Dieser Abschnitt stellt den Zusammenhang zwischen der Plazierung von Sicherheitsfunktionen und den damit erreichbaren (und nicht erreichbaren) Schutzzielen dar. Sicherheitsuntersuchungen setzen im allgemeinen ein Angreifermodell voraus. Basierend auf diesem Angreifermodell (vgl. Abschnitt 3.3.1) wird untersucht, ob die vereinbarten Schutzziele erreicht werden oder nicht. Ein Schutzziel gilt als erreicht, wenn keine erfolgreichen (nicht abgewehrten) Angriffe bezüglich des Schutzzieles angenommen werden.

Die Plazierung von Sicherheitsfunktionen entscheidet direkt über abwehrbare bzw. nicht abwehrbare Angriffe, d. h. über ein Schutzpotential. Erst die tatsächliche Implementierung entsprechender Sicherheitsfunktionen und die Beachtung weiterer Randbedingungen für erfolgreiche Angriffe (vgl. Abschnitt 3.3.3 über Bedrohungsmodelle) lassen Schlüsse bezüglich erreichter oder nicht erreichter Schutzziele zu.

In diesem Abschnitt wird untersucht, gegen welche Angriffe die jeweils betrachteten Sicherheitsfunktionen wirksam sind und wo die Grenzen des Wirkungsbereiches von Sicherheits-

funktionen liegen. Es werden Schutzziele mit Bezug zur Integrität und Vertraulichkeit von Daten betrachtet. Für Untersuchungen zur Verfügbarkeit kann die nachfolgende Abstraktion nicht übernommen werden.

4.2.3.1 Angreifermodell

Das nachfolgend eingeführte Angreifermodell ist für kommunizierende Systeme geeignet. Bild 4-8 zeigt das Modell für die Kommunikation zweier Kommunikationssysteme über einen nicht näher spezifizierten Kommunikationspfad und die Angriffspunkte für mögliche Angreifer. Die Sicherheitsfunktionen seien in Form transparenter Zwischenschichten implementiert. Der durch diese Funktionen auf Sender- und Empfängerseite realisierte Sicherheitsdienst werde zum Schutz der von der Quelle zur Senke übermittelten Daten eingesetzt.

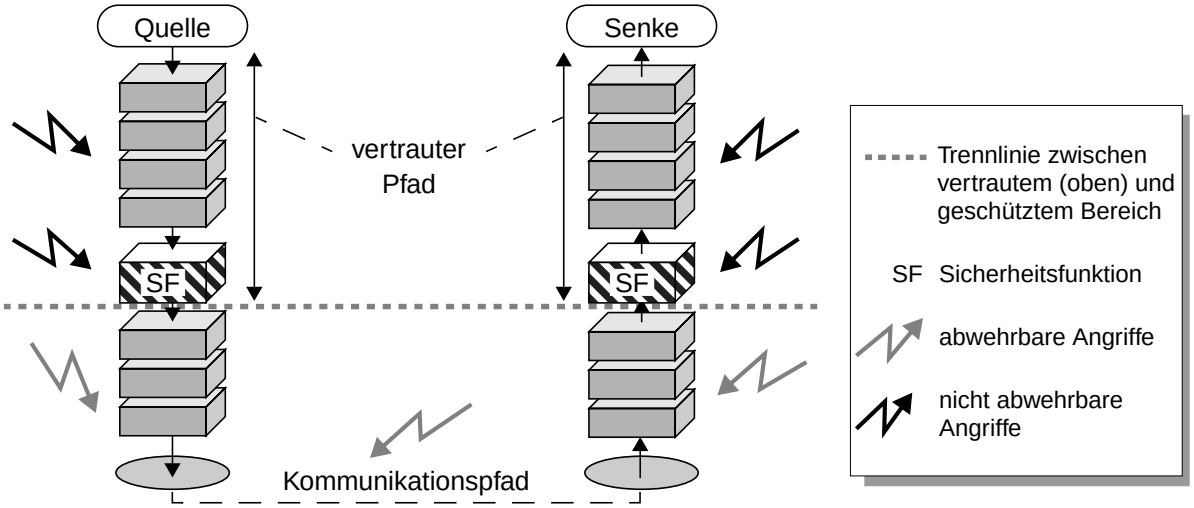


Bild 4-8: Angriffspunkte – erreichbare Sicherheit

Quelle und Senke können Anwendungen oder Instanzen in Kommunikationsschichten repräsentieren. Entsprechend fallen dort schützenswerte Anwendungsdaten oder Protokolldaten an. Im folgenden werden Angriffe auf die *Vertraulichkeit* und *Integrität* von schützenswerten Daten betrachtet. Es werden folgende Angriffspunkte unterschieden [44]:

- *Angriffe zwischen der Quelle schützenswerter Daten und der schützenden Sicherheitsfunktionalität*: Diese Angriffe sind *nicht abwehrbar,* da die Sicherheitsfunktionen dort keine Wirkung besitzen. Die Sicherheitsfunktionen sind entweder noch nicht angewendet (auf der Seite der Quelle) oder die Wirkung der Sicherheitsfunktionen ist bereits durch die inverse Sicherheitsfunktion aufgehoben (auf der Seite der Senke).

- *Angriffe auf die Sicherheitsfunktionen selbst*: Diese Angriffe sind durch die Sicherheitsfunktionen selbst *nicht abwehrbar.* Sie werden i. a. dadurch ausgeschlossen, daß für die Sicherheitsfunktionen ein sicherer Bereich vorausgesetzt wird, in dem keine Angreifer angenommen werden. Ist dies nicht gegeben, so tragen diese manipulierbaren Sicherheitsfunktionen nicht zur nachvollziehbaren Erfüllung von Schutzzielen bei.

- *Angriffe zwischen den verteilten Sicherheitsfunktionen:* Angriffe auf die Daten auf dem Kommunikationspfad zwischen den paarweise auftretenden Sicherheitsfunktionen sind *abwehrbar.* Bei korrekt arbeitenden Sicherheitsfunktionen werden diese Angriffe nicht erfolgreich sein. Dabei wird vorausgesetzt, daß entsprechend der Schutzziele wirksame

Sicherheitsfunktionen gewählt werden. Aus Sicherheitssicht ist der zwischen den Sicherheitsfunktionen liegende Bereich bezüglich der durch die Sicherheitsfunktionen erreichten Schutzziele transparent. Dieses schafft Abstraktionsmöglichkeiten, die insbesondere bei komplexen Telekommunikationsnetzen für eine Sicherheitsbewertung wichtig sind.

Der Teil des Datenpfades, auf dem Angriffe nicht abwehrbar sind wird als *vertrauter Pfad* bezeichnet. Es wird diesem Teil des Datenpfades dahingehend vertraut, daß dort keine erfolgreichen Angriffe angenommen werden. Dies kann durch weitere Sicherheitsfunktionen oder auch durch organisatorische oder technische Gegebenheiten begründet sein, die relevante Bedrohungen ausschließen (siehe Abschnitt 3.3.3).

Das betrachtete Kommunikationsszenario werde von den Sicherheitsfunktionen in zwei disjunkte Bereiche unterteilt:

- Der Bereich oberhalb der Sicherheitsfunktionen wird als *Vertrauensbereich* bezeichnet. Angriffe werden dort (auch in Zwischensystemen) nicht angenommen. Vertrauensbereichen wird in Bezug auf die korrekte und erwartungsgemäße Funktion seiner Komponenten vertraut. Daten die in diesem Bereich anfallen, sind dort nicht gegen Angriffe geschützt.

- Der Bereich unterhalb der Sicherheitsfunktionen wird als *geschützter Bereich* bezeichnet. Dort sind jene Schutzziele bezüglich der oberhalb der Sicherheitsfunktionen anfallenden Daten erreichbar, die durch diese Sicherheitsfunktionen garantiert werden können.

Eine bezüglich Sicherheit *effektive Strategie* zur Plazierung von Sicherheitsfunktionen wird den Vertrauensbereich minimieren. Dieses Vorgehen reduziert einerseits meist die Komplexität des Vertrauensbereiches[4] und erleichtert damit auch dessen Prüfung. Außerdem minimiert es die erfolgversprechenden Angriffspunkte potentieller Angreifer. Zum Schutz von Anwendungsdaten sind deshalb Sicherheitsfunktionen vorzuziehen, die möglichst nahe bei der Anwendung bzw. innerhalb der Anwendung implementiert werden können.

In einem Kommunikationssystem werden auch innerhalb der Kommunikationsschichten schützenswerte Daten erzeugt (z. B. Senderadresse, Empfängeradresse, Dienstkennung). Sicherheitsfunktionen in Zwischenschichten schützen jedoch nur jene Daten, die oberhalb dieser Sicherheitsfunktionen anfallen. Sofern auch Protokolldaten schützenswert sind, können Sicherheitsfunktionen in unterschiedlichen Schichten und in der Anwendung integriert werden; jeweils möglichst nahe am Entstehungsort bzw. Verwertungsort schützenswerter (Protokoll-)Daten.

Eine *effiziente Strategie* zum Schutz von Protokoll- und Anwendungsdaten (z. B. Adressen, Prüfsummen, Kommunikationsinhalte) ist, die zugehörigen Sicherheitsfunktionen möglichst nahe am Übertragungsmedium zu plazieren, da damit alle zwischen Anwendung und Medium erzeugten Daten geschützt werden können. Dem Pfad der Daten von der Anwendung über die Schichten zu den Sicherheitsfunktionen muß dabei vertraut werden. Solange sich der vertraute Pfad vollständig innerhalb eines Kommunikationssystems befindet, kann dieses Vertrauen durch organisatorische und technische Maßnahmen des Benutzers oder des Systembetreibers gerechtfertigt sein.

4 Der Benutzer kann nicht sämtliche Funktionen oberhalb der Trennlinie nachvollziehen und prüfen. Deshalb muß er von der erwartungsgemäßen Funktion dieses Bereiches ausgehen, ohne genügend Information zu besitzen, um dieses sicher vorhersagen zu können – er muß eben vertrauen. Je weniger Funktionalität in diesem Bereich allokiert ist, desto geringer wird der Anteil der für den Benutzer nicht nachvollziehbaren Funktionen, so daß die Basis für ein Vertrauen gestärkt wird.

Strategien zur optimalen Plazierung von Sicherheitsfunktionen innerhalb eines vorgegebenen Allokationsbereiches bezüglich Effizienz und Effektivität hinsichtlich der gegebenen Schutzziele werden in [44] vorgestellt und ausführlich diskutiert.

4.2.3.2 Sicherheits-Gaps – Ursachen nicht abwehrbarer Angriffe

Als Sicherheits-Gap werden Bereiche oder eine Menge von Schichten bezeichnet, bezüglich derer kein Schutz durch EzE-, PzP- oder Ll-Sicherheitsfunktionen möglich ist. Dies kann entweder durch oben genannte Transparenzanforderungen (bzw. daraus abgeleiteten Grenzlinien) oder durch Fehlen sicherer Ablaufumgebungen für Sicherheitsfunktionen bedingt sein. Die EzE-Grenzlinie beschränkt dabei die Daten, die autonom durch die Kommunikationspartner geschützt werden können. Unterhalb der EzE-Grenzlinie erzeugte bzw. verarbeitete Daten können im allgemeinen nicht durch EzE-Sicherheitsfunktionen geschützt werden.

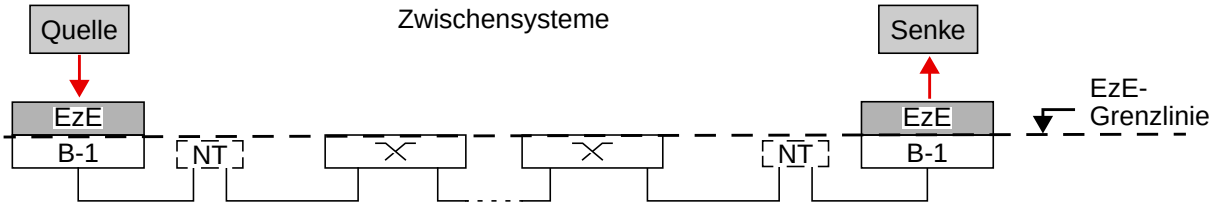


Bild 4-9: Nutzer-Ebene im ISDN

Bild 4-9 zeigt vereinfacht die Nutzer-Ebene im ISDN. Nutzdaten können oberhalb von Schicht 1 an beliebiger Stelle innerhalb der Endgeräte EzE-gesichert werden, da innerhalb des Netzes lediglich Funktionen der Schicht 1 (z. B. Kanalkodierung, -dekodierung) implementiert werden. Sofern auf Schicht 1 keine schützenswerten Daten bzw. Informationen anfallen, existiert hier kein Gap.

Bild 4-10 zeigt am Beispiel der Steuerungs-Ebene im ISDN einen Sicherheits-Gap, der sich aus Benutzersicht (abhängig vom Vertrauen in den Netzbetreiber bzw. Dienstanbieter) bis zur Rufsteuerung hinauf erstreckt. Dies bedeutet, daß keine Rufsteuerungsdaten (z. B. gerufene Teilnehmernummer bzw. rufende Teilnehmernummer, Dienstart, Zeitpunkte und Profil der Dienstnutzung) durch EzE-Funktionen gesichert werden können.

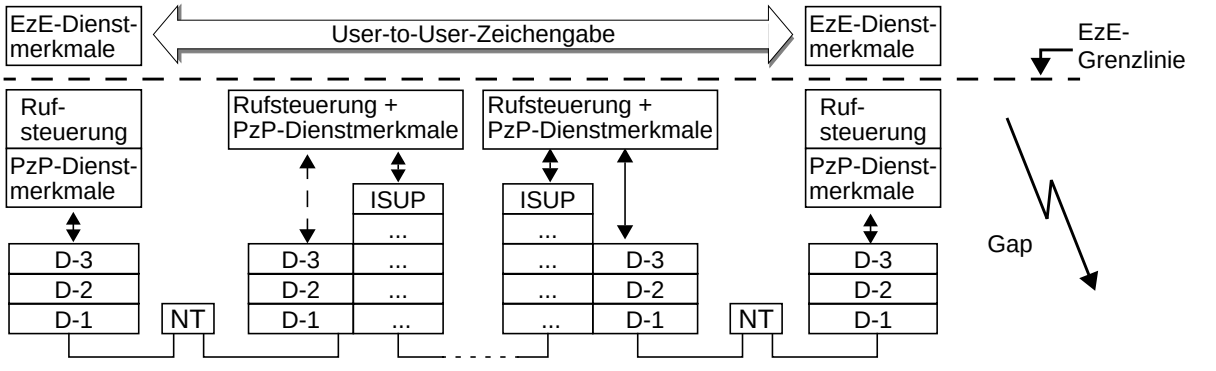


Bild 4-10: Sicherheits-Gaps der Steuerungs-Ebene im ISDN aus Benutzersicht

In der Steuerungs-Ebene des ISDN sind Daten im allgemeinen nicht EzE-sicherbar, da die Schichten 1–3 innerhalb der Teilnehmervermittlungsstelle implementiert sind und die Anwendungssteuerungsdaten meist ebenfalls innerhalb der Teilnehmervermittlungsstelle umgesetzt

und geprüft werden. Lediglich die sogenannten User-To-User-Steuerungsdaten werden vom Netz transparent weitergeleitet. Sie können folglich zum Schutz darauf basierender EzE-Dienstmerkmale EzE-geschützt werden bzw. zur Synchronisierung für EzE-Sicherheitsfunktionen genutzt werden.

In bestehenden Netzen ist oft ein solcher Sicherheits-Gap in der Steuerungs-Ebene zu beobachten. Manche Daten müssen prinzipiell innerhalb von Netzen verarbeitet werden und können somit niemals EzE-geschützt werden. Dies gilt beispielsweise für Netzadressen in vermittelnden Netzen.[5]

EzE-Sicherheitsfunktionen können jedoch durch aneinandergereihte (fortgesetzte) PzP-Sicherheitsfunktionen angenähert werden. Dazu müssen in den Zwischensystemen, in denen PzP-Sicherheitsfunktionen integriert werden, aus Sicht der Kommunikationspartner sichere Ablaufumgebungen vorhanden sein. Ebenso können PzP- bzw. EzE-Sicherheitsfunktionen durch Ll-Sicherheitsfunktionen angenähert werden. Bild 4-11 zeigt ein Beispiel für PzP-angenäherte EzE-Sicherheit.

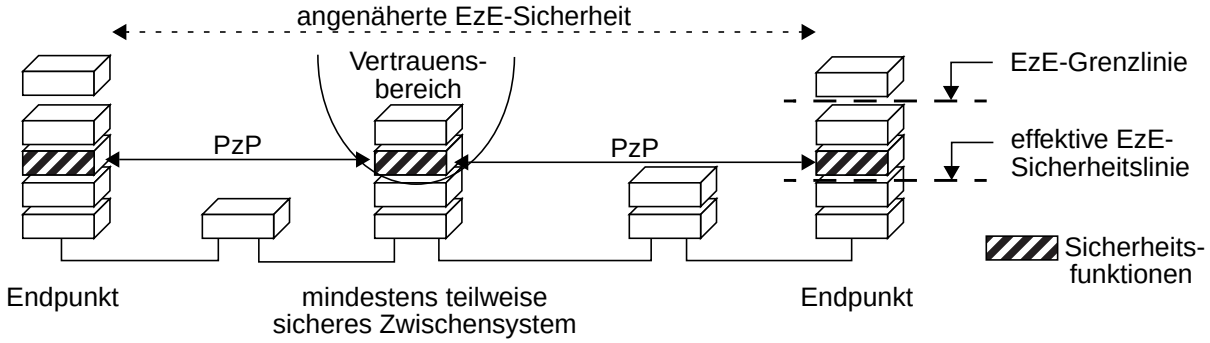


Bild 4-11: PzP-Annäherung von EzE-Sicherheit

Eine Definition für die *effektive EzE-Sicherheitslinie* kann unter Berücksichtigung sicherer Zwischensysteme wie folgt aus der Definition der EzE-Grenzlinie abgeleitet werden: Die effektive EzE-Sicherheitsgrenzlinie beschreibt die untere vertikale Grenze für die transparente Implementierung von Sicherheitsfunktionen aus Sicht der Kommunikationspartner. Sie ist definiert durch die oberste nicht vertrauenswürdige bzw. unsichere Kommunikationsschicht, die in mindestens einem Zwischensystem auf dem Kommunikationspfad zwischen den betrachteten Endpunkten durchlaufen wird. In Bild 4-11 liegt die effektive EzE-Sicherheitslinie oberhalb von Schicht 2, da diese sowohl im teilweise sicheren Zwischensystem, als auch in weiteren Zwischensystemen die oberste unsichere bzw. nicht vertrauenswürdige Schicht darstellt.

Wird in einem Zwischensystem PzP-Sicherheitsfunktionalität zur Annäherung von EzE-Sicherheitsfunktionalität eingebracht, so müssen alle Funktionen oberhalb der PzP-Sicherheitsfunktionen im Vertrauensbereich der Kommunikationspartner liegen, d. h. als sicher angenommen werden. Dies gilt, weil aus Transparenzgründen innerhalb der Zwischensysteme oberhalb der Sicherheitsfunktionen die Daten ungeschützt verarbeitet werden müssen[6]. Deshalb ist in Bild 4-11 der Vertrauensbereich im Zwischensystem nach oben offen gezeichnet.

5 Netzadressen können aber z. B. in Broadcast-Netzen durch sogenannte implizite Adressierung ersetzt werden. Dies kann dadurch realisiert werden, daß z. B. nur ein bestimmter Empfänger (Adressat) eine Nachricht entschlüsseln kann, dies aber möglicherweise für die anderen Empfänger nicht erkennbar ist [51].

Die Endgeräte werden oberhalb der Sicherheitsfunktionen sowieso als vertrauenswürdig angenommen. Zwischensysteme sind für diese effektive EzE-Sicherheitslinie folglich so lange transparent, wie sie aus Sicht der Kommunikationspartner einen sicheren Bereich darstellen und geeignete PzP-Sicherheitsfunktionen anbieten.

Eine Interpretation des Angriffsmodelles aus Bild 4-8 veranschaulicht die Argumentation: Die dort eingeführte Trennlinie zwischen Vertrauensbereich und geschütztem Bereich kann solange nach unten verschoben werden, bis ein nicht vertrauenswürdiger Bereich eines Zwischensystems an den stetig vergrößerten Vertrauensbereich anstößt. Ein weiteres Verschieben der Grenzlinie nach unten (d. h. die Implementierung der Schutzfunktionen in niedrigeren Schichten) führte zur Zerstörung des Vertrauensbereiches. Nachvollziehbare Sicherheit wäre nicht mehr gewährleistet. Bild 4-12 veranschaulicht dies an einem Beispiel.

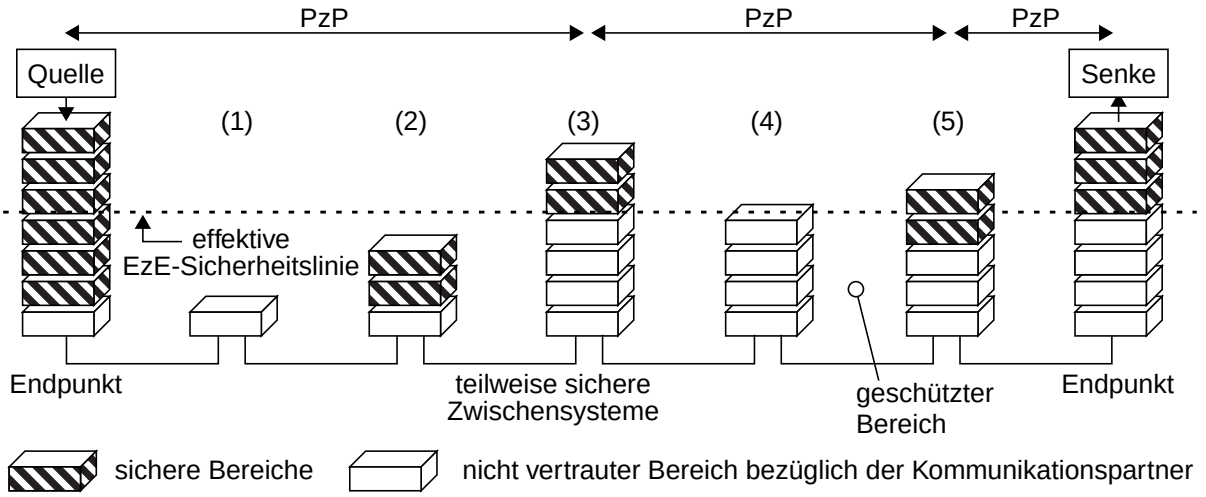


Bild 4-12: Effektive EzE-Grenzlinie unter Berücksichtigung von Zwischensystemen

Die effektive EzE-Sicherheitslinie ist durch die Zwischensysteme (3) und (4) und durch die Senke nach unten begrenzt. Sie kann unter Einbeziehung der vertrauenswürdigen Bereiche in den Zwischensystemen (3) und (5) durch PzP-Sicherheitsfunktionen angenähert werden. Dadurch sind alle oberhalb der effektiven EzE-Sicherheitslinie anfallenden Daten (Protokoll- und Anwendungsinformation) auf Übertragungsstrecken und in Zwischen- und Endsystemen geschützt (im geschützten Bereich). Ähnlich können auch effektive PzP-Sicherheitslinien definiert werden.

PzP-angenäherte EzE-Sicherheit bedingt folglich aus Sicht der Kommunikationspartner eine Auslagerung von Sicherheitsfunktionen in Zwischensysteme. Durch fortgesetzte Ll-Sicherheit angenäherte EzE-Sicherheit stellt den Grenzfall für angenäherte Sicherheit dar. In diesem Fall muß allen Zwischensystemen im Verbindungspfad von der Anwendung bis zur Schicht 2 vertraut werden. Sicherheitsfunktionen sind hier nur noch gegen externe Angreifer an den Übertragungsstrecken sinnvoll, da den Betreibern der Zwischensysteme implizit bezüglich des korrekten Betriebs etc. vertraut wird.

Unterhalb der *effektiven EzE-Sicherheitslinie* können Daten nicht durch Einbringen von Sicherheitsfunktionen EzE-gesichert werden. Durch Datensparsamkeit[7] können schützens-

6 In seltenen Fällen können durch Integration von Sicherheitsfunktionen auf mehreren Schichten unsichere Bereiche in Zwischensystemen kompensiert werden.

werte Daten in diesem Bereich jedoch minimiert werden. Die Verschleierung von Information (z. B. durch Verteilung, vgl. Abschnitt 4.3.3) kann den Aufwand für erfolgreiche Angriffe erhöhen und somit realen Bedrohungen nach Bild 3-3 entgegenwirken.

4.2.4 Auslagerung von Sicherheitsfunktionen

Die Integration von Sicherheitsfunktionen in Endgeräte kann aus vielfältigen Gründen schwierig sein. Nicht frei programmierbare Endgeräte (z. B. Telefonapparate) bieten meist keine Zugangspunkte für die Integration. Gemeinsam genutzte Endgeräte besitzen möglicherweise keine bezüglich der beteiligten Kommunikationspartner vertrauenswürdige Ablaufumgebung zur Integration von Sicherheitsfunktionen. Hinzu kommen Randbedingungen der Transparenz (z. B. EzE-Grenzlinie), die eine Implementierung von Sicherheitsfunktionen im Endgerät ausschließen können.

Aus Gründen fehlender Implementierungsschnittstellen oder sicherer Bereiche, des z. T. hohen Integrationsaufwandes und der durch Transparenz-Forderungen gegebenen Randbedingungen werden nachfolgend Möglichkeiten zur Auslagerung von Sicherheitsfunktionen aus den Endgeräten untersucht.

Bild 4-13a zeigt die Auslagerung von Sicherheitsfunktionen in autonome Zusatzgeräte. Dazu wird die zu implementierende Sicherheitsschicht in einer sogenannten Black-Box realisiert. Im ISDN wird diese Vorgehensweise angewendet, um auch mit nicht frei programmierbaren Endgeräten (z. B. Telefonapparaten) eine sichere Kommunikation zu ermöglichen. Die Black-Box verkörpert einen sicheren Bereich, in dem Sicherheitsfunktionen integriert sind. Werden im unterlegten Bereich keine Angreifer angenommen, so ist diese Black-Box-Lösung sicherheitstechnisch äquivalent[8] zu dem erweiterten Endsystem in Bild 4-3b in Abschnitt 4.2.1. Black-Box-Lösungen haben prinzipbedingt folgende Nachteile:

- Die hier gezeigte Anordnung fügt zusätzliche Verzögerungen in das Gesamtsystem ein, da die Schichten 1 bis N–1 in diesem Falle dreimal anstatt nur einmal durchlaufen werden. Je höher die Zwischenschicht in der Black-Box integriert werden soll (d. h. je größer N), desto aufwendiger wird deren Implementierung.

- Da der unterlegte Bereich als Vertrauensbereich vorausgesetzt wird, müssen Black-Box-Geräte möglichst nahe am eigentlich gewünschen Ort der Sicherheitsfunktionen (hier: Endgerät) installiert werden.

Eine Black-Box kann jedoch klein, handlich und mobil sein und vom Teilnehmer bei Bedarf in die Anschlußleitung eines ISDN-Endgerätes eingeschleift werden. Unterstützen Endgeräte den Einsatz von ausgelagerten Sicherheitsfunktionen, so können die obigen Nachteile entfallen. Chipkarten zur Speicherung und Verarbeitung geheimer Schlüssel können beispielsweise Anwendungen in komplexen oder öffentlichen Endgeräten direkt unterstützen und bei entsprechenden Schnittstellen direkt am gewünschten Ort wirken.

---

7 Datensparsamkeit bezeichnet den sparsamen Umgang mit schützenswerten Daten. Schützenswerte Daten sollten nur dort verarbeitet oder gespeichert werden können, wo dies zur Diensterbringung notwendig ist. Zur Datensparsamkeit können auch veränderte Protokolle beitragen, die mit weniger schützenswerten Daten auskommen als bestehende Protokolle (z. B. Broadcast anstatt Vermittlung). Insbesondere zur Realisierung von Anonymität und Unbeobachtbarkeit sind neue Protokolle zu entwickeln.

8 In diesem Falle kann aus Sicherheitssicht vom unterlegten Bereich abstrahiert werden.

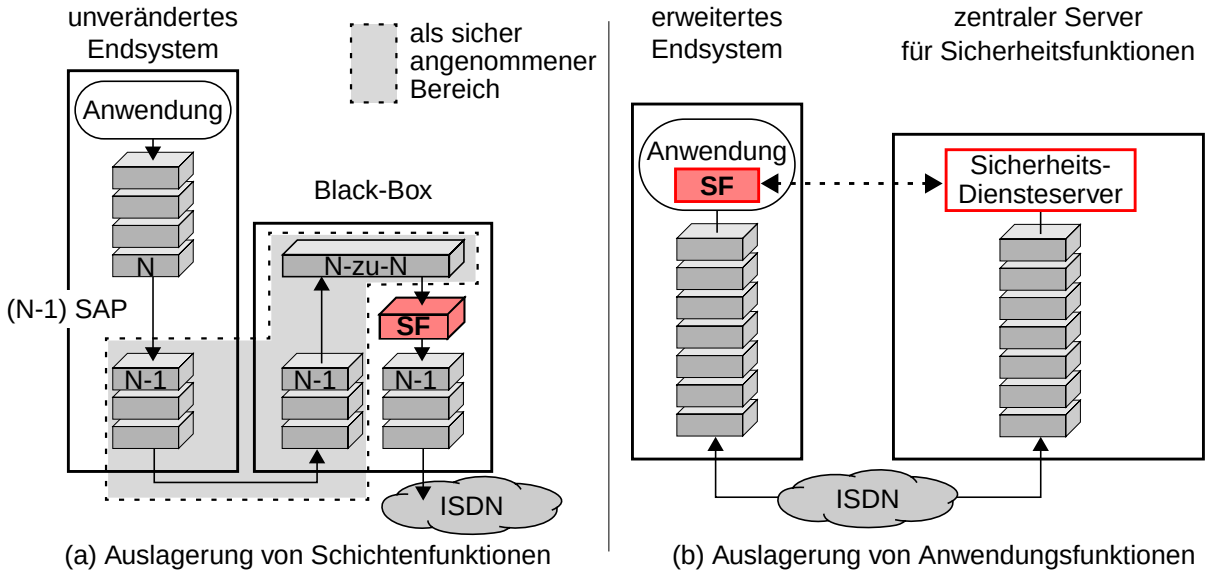


Bild 4-13: Auslagerung von Sicherheitsfunktionen

Im ISDN hat mit der Einführung der Dienste des Intelligenten Netzes eine Bewegung eingesetzt, die die Auslagerung von Dienstesteuerlogik in zentrale Server vorsieht. Dadurch läßt sich ein hoher Bündelungsgewinn, eine einfache Wartbarkeit und Erweiterbarkeit sowie eine schnelle Weiterentwicklung von Diensten erreichen.

Für Sicherheitsdienste auf Anwendungsebene kann ebenfalls eine Auslagerung von Sicherheitsfunktionen in zentrale (über das Kommunikationsnetz angesprochene) Server aus Gründen der Kompatibilität, der Verfügbarkeit, der einfachen Wartbarkeit und des Bündelungsgewinnes sinnvoll sein:

- *Kompatibilität* kann dadurch geschaffen werden, daß Sicherheitsfunktionen nach Bedarf auf zentralen Servern angesprochen bzw. von dort zur Ausführung sicher in die Endgeräte geladen werden können. Weiterentwickelte oder um Fehler bereinigte Funktionen stehen somit unmittelbar für viele Kommunikationspartner bereit.

- Die *Verfügbarkeit* des zentralen Servers kann durch die Erreichbarkeit über unterschiedliche Netze und durch Einsatz von Spiegelservern maximiert werden. Der Zusatzaufwand ist durch den Bündelungsgewinn gerechtfertigt.

- *Kosteneffizienz* ist durch Bündelungsgewinn möglich, da zentrale Server eine hohe Auslastung erreichen können. Die hohen Kosten für sichere Ablaufumgebungen und validierte Software können sich so schneller amortisieren.

Die Auslagerung von Sicherheitsfunktionen auf spezialisierte Sicherheitsinfrastruktur eröffnet Möglichkeiten der gemeinsamen Nutzung dieser Sicherheitsfunktionen. Bild 4-13b zeigt ein Beispiel für ausgelagerte Sicherheitsanwendungen. Ein typisches Beispiel stellen Infrastrukturen zur Verwaltung von öffentlichen Schlüsseln beziehungsweise Schlüsselzertifikaten dar. Damit können der Verwaltungsaufwand zum Führen gültiger und ungültiger Schlüssel zentralisiert und die Kosten unter vielen Benutzern aufgeteilt werden.

Werden ausgelagerte Sicherheitsfunktionen (z. B. Verwaltung von Schlüsselzertifikaten) von mehreren Teilnehmern benutzt, so wird der zugehörigen Infrastruktur und ihren Betreibern von diesen Teilnehmern vertraut. Diese zentrale Instanz wird als *vertrauenswürdige Dritte Instanz*

(Trusted Third Party, TTP) bezeichnet, die die Sicherheitsfunktionen der Kommunikationspartner ergänzt.

4.2.5 Benutzerorientierte Sicht auf Sicherheitsfunktionen – EzE-Sicherheit

Eine Kommunikationsbeziehung zwischen Endgeräten oder zwischen Endgeräten und zentralen Servern wird vom zwischenliegenden Kommunikationsnetz unterstützt. Aus Sicht eines Benutzers ist jedoch zweifellos der Schutz der übergeordneten Kommunikationsbeziehung zwischen Endsystemen und gegebenenfalls zentralen Servern das primäre Ziel.

Nicht gelöst ist damit jedoch die Frage, ob EzE-Sicherheit direkt durch EzE-, oder durch EzE-annähernde PzP- oder Ll-Sicherheitsfunktionen realisiert werden soll. Die Diskussionen der verschiedenen Klassen von Sicherheitsfunktionen und deren Auswirkung auf das Angreifermodell haben gezeigt, daß die geeignete Wahl der Plazierung von Sicherheitsfunktionen von sehr vielen Faktoren abhängt. Unter anderem hängt die Plazierung von folgenden Faktoren ab:

- Angreifermodell und daraus abgeleitet den Vertrauensbereichen,
- Schutzzielen (insbesondere Ort der Erzeugung und Verarbeitung schützenswerter Daten),
- Implementierungsaufwand und Kosten beim Betrieb von Sicherheitsfunktionen (zusätzliche Verzögerung, Variabilität der Verzögerung, Schlüsselmanagement, etc.),
- Randbedingungen der Transparenz und resultierender Grenzlinien.

Da diese Faktoren wiederum von den Beteiligten und den jeweils genutzten Telekommunikationsdiensten abhängen, ist nachvollziehbar, daß die Plazierung und die Auswahl von Sicherheitsfunktionen durch die jeweils Betroffenen bzw. einen vertrauenswürdigen Stellvertreter beeinflußt werden können muß. Dennoch gibt es aus Benutzersicht einige wichtige allgemeine Anmerkungen zu den verschiedenen Sicherheitsfunktionsklassen:

- Die durch *EzE-Sicherheitsfunktionen* garantierten Schutzziele sind – mit Ausnahme der Verfügbarkeit – vom zwischenliegenden Kommunikationsnetz unabhängig. Vertraut werden muß lediglich den Endgeräten, welche mobil sein können und so unter ständiger Aufsicht des Benutzers verbleiben können. Da EzE-Sicherheitsfunktionen innerhalb der Endpunkte einer Kommunikationsbeziehung lokalisiert sind, sind sie den Benutzern am nächsten. Dies unterstützt Kontrollmöglichkeiten für die Benutzer.
- Durch *fortgesetzte PzP-Sicherheitsfunktionen* angenäherte EzE-Sicherheit setzt in jedem an den PzP-Sicherheitsfunktionen beteiligten Zwischensystem zusätzliches Vertrauen der Benutzer in die ausgelagerten Sicherheitsfunktionen selbst und in die Telekommunikationsdienstfunktionen oberhalb der Sicherheitsfunktionen voraus (vgl. Vertrauensbereich in Bild 4-11).
- EzE-Sicherheit kann durch *fortgesetzte Ll-Sicherheitsfunktionen* nur dann angenähert werden, wenn alle Knoten oberhalb und am Ort der Ll-Sicherheitsfunktionen vom Benutzer als sicher angenommen werden. Da Ll-Sicherheitsfunktionen (laut Definition) in benachbarten Knoten im Kommunikationspfad implementiert werden müssen, werden diese Funktionen meist in der Bitübertragungs- oder der Datensicherungs-Schicht realisiert. Nach Bild 4-8 bedingt dies, daß dieser Schutz hauptsächlich gegen Angriffe an den Übertragungsstrecken wirkt.

Ebenso lassen sich PzP-Sicherheitsfunktionen durch fortgesetzte Ll-Sicherheitsfunktionen annähern. Mischformen aus PzP- und Ll-Sicherheitsfunktionen sind leicht aus den hier besprochenen reinen Formen abzuleiten.

Wie diese Diskussion zeigt, gibt es keine allgemeingültige optimale Plazierung von Sicherheitsfunktionen. Die Entscheidung für eine Plazierung hängt sowohl von den Daten ab, die geschützt werden sollen, als auch von dem Vertrauen des jeweils Betroffenen in Teile der Kommunikationsinfrastruktur.

Es müssen an die Bedürfnisse der Benutzer angepaßte Sicherheitsdienste in unterschiedlichen Schichten und in Anwendungen unterstützt werden, um bezüglich unterschiedlicher Angreifermodelle effiziente und effektive Sicherheit realisieren zu können. Dieses impliziert, daß eine Sicherheitsarchitektur für mehrseitig sichere Dienste eine flexible Anordnung und Aktivierung von Sicherheitsfunktionen unterstützen muß.

4.3 Schnittstellenanforderungen exemplarischer Sicherheitsdienste

Die oben untersuchten Sicherheitsfunktionen (z. B. EzE-Sicherheitsfunktionen in kommunizierenden Endgeräten) realisieren im Zusammenspiel Sicherheitsdienste. Der Zugang und die Aktivierung dieser Dienste erfolgt über sogenannte Dienstzugangspunkte. Über diese Dienstzugangspunkte treten die Sicherheitsdienste mit ihrer Umgebung in Beziehung. Sicherheitsdienst-Nutzer und Sicherheitsdienst interagieren durch den Austausch von Dienstdateneinheiten über diesen Dienstzugangspunkt (z. B. zur Aktivierung, Initialisierung, Meldung von Ergebnissen oder Fehlern).

Nachfolgend werden exemplarische Sicherheitsdienste beschrieben, die zur Realisierung von Sicherheitsanforderungen wie Vertraulichkeit, Integrität und Authentizität eingesetzt werden können. Sie dienen als Bausteine, die durch eine Sicherheitsarchitektur mit existierenden Diensten in Beziehung gesetzt werden und gemeinsam mehrseitig sichere Kommunikationsdienste ermöglichen.

Die folgende Darstellung von Sicherheitsdiensten konzentriert sich auf (i) das Ziel des Dienstes aus Sicht der Anwender, (ii) die Beschreibung des Dienstes und seiner Dienstschnittstellen und (iii) die Anforderungen an die Diensteumgebung.

Auf Implementierungen von Mechanismen und Protokollen wird lediglich verwiesen, weil sie für diese Arbeit nicht von primärem Interesse sind und eine Sicherheitsarchitektur von Implementierungen weitestgehend unabhängig sein sollte. Zur Implementierung von Dienstschnittstellen in Form von Programmierschnittstellen (Application Programming Interface, API) existieren mehrere Ansätze, auf die zurückgegriffen werden kann (vgl. z. B. [66]).

Die Rahmenwerke für Authentisierungs-, Integritäts- und Vertraulichkeitsdienste der ITU (X.811, X.814, X.815) beschränken sich auf die Beschreibung von Operationsfolgen und Datenelementen. Spezifikationen und Dienstschnittstellen sind nicht enthalten. Deshalb werden in den nachfolgenden Dienstbeschreibungen generische Dienstschnittstellen definiert, die zur Beschreibung der Steuerung von Sicherheitsdiensten ausreichend sind.

4.3.1 Authentisierungsdienste

Authentisieren bedeutet „glaubwürdig machen“. Das *Ziel* eines Authentisierungsdienstes ist die *Prüfung von Information, hier einer vorgegebenen Identität*. Eine Identität kann durch Wissen (Geheimnis), eine eindeutige Charakteristik (z. B. Fingerabdruck) oder durch Besitz

(z. B. Ausweis, Chipkarte) nachgewiesen werden [24]. Identitäten können juristischen oder natürlichen Personen, Infrastruktur oder Software-Prozessen zugeordnet werden. Einen Überblick über Authentisierungsverfahren bieten beispielsweise [63], [64] und [65].

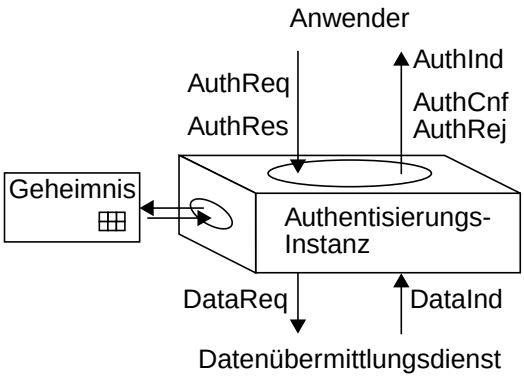
In der Telekommunikation bietet sich vor allem der Nachweis einer Identität durch Wissen an, da dieser durch technische Verfahren (Nachrichtenaustausch) realisierbar ist. Es muß sich dabei um ein Wissen handeln, welches nur dem jeweiligen Identitätsträger bekannt sein kann (d. h. um ein Geheimnis). Dieses Wissen muß durch andere Instanzen prüfbar sein, ohne daß es dadurch bekannt wird.

Die zur Prüfung einer Identität notwendige Prüf-Information muß sicher an diese Identität gebunden sein. Allgemein können Identitäten unterschieden werden, für die unterschiedliche Prüf-Information vorliegt. Je nach Bindung der Identität können Kommunikationspartner, Anwendungen, Endgeräte oder Netzadressen authentisiert werden.

Wird das einer Identität zugeordnete geheime Wissen in einem (mobilen) sicheren Modul (z. B. Chipkarte) gehalten, so wird sich der Teilnehmer i. a. vor der Benutzung gegenüber dem technischen Geheimnisträger authentisieren müssen. Dazu eignen sich besonders biometrische Verfahren, d. h. eindeutige Charakteristiken eines Identitätsträgers [24].

4.3.1.1 Allgemeine Beschreibung eines Authentisierungdienstes

Eine Authentisierungsinstanz bezeichnet eine Instanz, die stellvertretend für den Träger einer Identität das Authentisierungsprotokoll durchführt. Die prüfende Instanz schickt der geprüften Instanz eine Aufforderung zum Wissens-Nachweis (*Challenge*-Nachricht). Diese Aufforderung wird von der geprüften Instanz mit dem Geheimnis bearbeitet und als Nachweis zurückschickt (*Response*-Nachricht). Diese Antwort wird nun von der prüfenden Instanz mit Hilfe der zur geprüften Identität gehörenden Prüf-Information verifiziert. Zum Nachweis des geheimen Wissens können je nach verwendetem Verfahren mehrere solcher Nachweisschritte (Challenge-Response Nachrichtenpaare) notwendig sein. Bild 4-14 zeigt die generische Dienstschnittstelle für Authentisierungsdienste.



Primitiv	*Übergabeparameter*
AuthReq	zu prüfende und eigene Identität Prüf-Information für zu prüfende Id. Authentisierungsprotokoll-Kennung
AuthInd	prüfende und zu prüfende Id. Authentisierungsprotokoll-Kennung
AuthRes	zu prüfende und eigene Identität (Geheimnis für Nachweis der Id.) Authentisierungsprotokoll-Kennung
AuthCnf	eigene und geprüfte Id., Ergebnis OK
AuthRej	negative Rückmeldung (NOK)

Bild 4-14: Generische Dienstschnittstelle für Authentisierungsdienste

Die prüfende Instanz wird durch einen Anwender mit Hilfe des *AuthReq*-Primitives mit der Prüfung einer Identität der Partnerinstanz beauftragt. Dabei werden die zu prüfende Identität, die zur Identität gehörende Prüf-Information und die Kennung des zu verwendenden Authenti-

sierungsprotokolles durch den Anwender vorgegeben. Das Ergebnis der Authentisierung wird dem Anwender über das Primitiv *AuthCnf* mitgeteilt.

Die geprüfte Instanz erhält vom Übermittlungsdienst eine Nachricht, die Informationen über das zu verwendende Authentisierungsprotokoll und die nachzuweisende Identität enthält. Dieses wird dem Anwender der geprüften Instanz mit dem *AuthInd*-Primitiv angezeigt. Der Anwender bestätigt die Authentisierung mit dem *AuthRes*-Primitiv. Dabei kann das Geheimnis zum Nachweis der jeweiligen Identität an die geprüfte Instanz übergeben werden. Meist soll das Geheimnis nicht an die technische Authentisierungsinstanz weitergegeben werden, sondern im sicheren Bereich (z. B. Chipkarte) verbleiben. In diesem Fall werden jene Funktionen, die Zugriff auf das Geheimnis benötigen (z. B. Signatur), aus der Authentisierungsinstanz ausgelagert und innerhalb des sicheren Moduls implementiert. Die geprüfte Instanz erhält über eine Treiberschnittstelle sicheren Zugang zu den erforderlichen Funktionen.

Bei der gegenseitigen Authentisierung (Mutual Authentication) wird das Verfahren nacheinander zur Prüfung der Identitäten beider Kommunikationspartner durchgeführt.

4.3.1.2 Anwendungsbeispiel: Authentisierung zweier Kommunikationspartner nach X.509

Bei Telekommunikationsdiensten ist meist eine gegenseitige Authentisierung der Kommunikationspartner sinnvoll. Bild 4-15 zeigt anhand eines Signalisierungs-Zeitdiagrammes den Ablauf einer 3-Wege Authentisierung nach X.509. Dabei authentisieren sich die Anwender *A* und *B* gegenseitig. Die Nachrichten *Response1* (zum Nachweis der Identität von *B*) und *Challenge2* (zur Anforderung des Nachweises der Identität von *A*) werden in einer Nachricht zusammengefaßt übertragen. Deshalb sind insgesamt 3 Nachrichten auszutauschen, was den Namen 3-Wege-Authentisierung für dieses Protokoll bedingt.

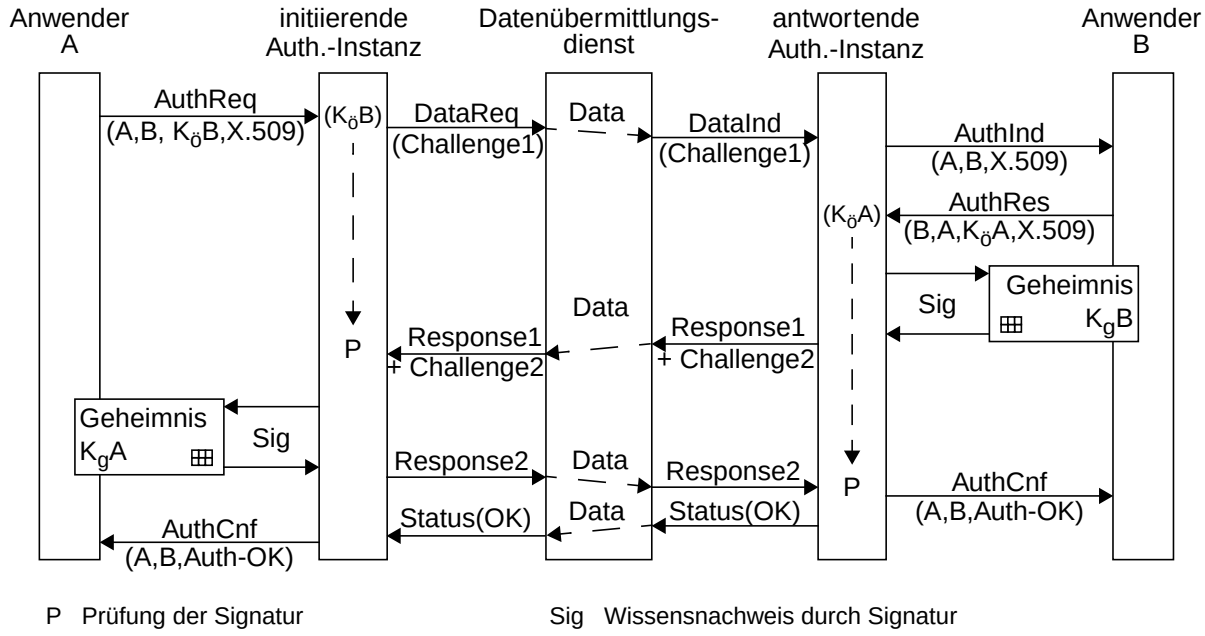


Bild 4-15: Signalisierungs-Zeitdiagramm einer Authentisierung nach X.509

Bei dem Geheimnis handelt es sich um den geheimen Schlüssel eines Schlüsselpaares ($K_{ö}$,K_g) eines asymmetrischen Kryptosystems (z. B. RSA [5]). Der öffentliche (Prüf-) Schlüssel ($K_{ö}A$ bzw. $K_{ö}B$) des Schlüsselpaares ist eindeutig einer Identität (*A* bzw. *B*) zugeordnet. Der Nach-

weis der Kenntnis des geheimen Schlüssels (hier durch Signatur einer Nachricht mit K_gA bzw. K_gB) wird als Identitätsnachweis genutzt. Die *Challenge*-Nachricht wird dazu von der empfangenden (geprüften) Instanz mit dem geheimen Schlüssel signiert (vgl. *Sig* in Bild 4-15). Der geheime Schlüssel muß den Authentisierungsinstanzen nicht übergeben werden. Die Signatur einer *Challenge*-Nachricht kann z. B. über eine Treiberschnittstelle von einer Chipkarte oder einem anderen sicheren Modul angefordert werden.

Die signierte Nachricht (*Response*) wird von der prüfenden Instanz mit dem öffentlichen Schlüssel des Gegenüber geprüft. Die öffentlichen Schlüssel können z. B. bei der Authentisierungs-Anforderung (*AuthReq*) bzw. der Authentisierungs-Bestätigung (*AuthRes*) an die Authentisierungsinstanzen übergeben werden. Ebenso werden die Kennung des zu verwendenden Protokolles und die zu prüfende Identität über die Dienstschnittstelle an die Authentisierungsinstanzen übergeben. Das Ergebnis der Authentisierung wird den Anwendern durch eine *AuthCnf*-Nachricht angezeigt.

Die Inanspruchnahme des Datenübermittlungsdienstes ist in Bild 4-15 verkürzt dargestellt. Die *Challenge*-, *Response*- und *Status*-Nachrichten werden mit Hilfe des *DataReq*-Primitivs an den Datenübermittlungsdienst übergeben und bei der empfangenden Authentisierungsinstanz durch das Primitiv *DataInd* angezeigt. Ist die Adresse der Partnerinstanz nicht durch den Kommunikationskontext festgelegt, so muß diese ebenfalls an den Datenübermittlungsdienst übergeben werden.

Die *Challenge*- und *Response*-Nachrichten müssen so beschaffen sein und verarbeitet werden, daß sie Angriffen während der Übermittlung (z. B. Einfügen, Verändern, Löschen, Aufzeichnen und Wiedereinspielen von Nachrichten) widerstehen. Dem Datenübermittlungsdienst sollte nicht vertraut werden müssen. Deshalb werden i. a. Zeitstempel, Transaktionsnummern, Zufallszahlen und ähnliches mehr zu den eigentlichen Nachrichteninhalten (z. B. geprüfte Identität, Sender, Empfänger etc.) hinzugefügt. In [25] wird u. a. dargelegt, wie die unterschiedlichen Nachrichtenbestandteile und die Abfolge der Nachrichten entsprechend den Authentisierungsprotokollen der ITU-Empfehlung X.509 gegen die oben genannten Angriffe schützen.

4.3.1.3 Automatisierter Zugriff auf Prüf-Information – Public Key Infrastructure

Die Verwaltung von öffentlichen Schlüsseln (Prüf-Information) kann von sogenannten *Verzeichnisdiensten* übernommen werden. Diese liefern auf Anfrage den zu einer Identität gehörigen gültigen öffentlichen Schlüssel. Diese Verzeichnisdienste führen auch eine Liste über gesperrte Schlüssel (Key Revocation List), deren zugehörige geheime Schlüssel bekannt geworden oder auf andere Weise ungültig geworden sind (kompromittierte Schlüssel).

Zertifizierungsdienste stellen die Verbindung einer Identität zu einem öffentlichen Schlüssel her. Diese Verbindung von Identität und öffentlichem Schlüssel wird dadurch geschützt, daß die Zertifizierungsstelle ein sogenanntes Zertifikat ausstellt, das von ihr signiert wird. Ein Schlüsselzertifikat behinhaltet mindestens die Identität, den öffentlichen Prüfschlüssel und den zugehörigen Prüfalgorithmus (z. B. RSA), den Gültigkeitszeitraum des Zertifikates sowie die Identität der Zertifizierungsinstanz. Die Zertifizierungsstelle ist auch für die Prüfung der Identität zuständig (z. B. durch Ausweiskontrolle). Der Empfänger eines Zertifikates muß vor der Benutzung eines öffentlichen Schlüssels die Signatur des zugehörigen Zertifikates prüfen. Er muß dazu im Besitz des öffentlichen Schlüssels der ausstellenden Zertifizierungsinstanz sein.

Die Infrastruktur, die zur Zertifizierung und Verwaltung von öffentlichen Schlüsseln zuständig ist, wird zusammenfassend auch als Public Key Infrastructure (PKI) bezeichnet. Die Vertrau-

enswürdigkeit der Authentisierung hängt direkt von der Authentizität der öffentlichen Schlüssel ab und damit von der Vertrauenswürdigkeit der Zertifizierungsstelle (Verbindung von Identität und Prüf-Information) und des Verzeichnisdienstes (Aktualität, Gültigkeit). Interessante Ansätze und Gestaltungsalternativen für Verzeichnis- und Zertifizierungsdienste werden in [50] angesprochen. In [126] werden konkrete Schnittstellen zur Zusammenarbeit von Verzeichnisdiensten, Zertifizierungsdiensten und Zugriffsfunktionen mit ihren wesentlichen Definitionen für Daten- und Befehlsformate zusammengefaßt.

4.3.1.4 Vereinbarung eines gemeinsamen geheimen Schlüssels

Die Vereinbarung eines gemeinsamen geheimen Schlüssels zur Verwendung für symmetrische Verschlüsselungs- und Integritätsschutz-Verfahren in Zwischenschichten kann in die Authentisierung der Kommunikationspartner integriert werden. Dazu muß innerhalb des Austausches der in Bild 4-15 eingezeichneten Challenge- und Response-Nachrichten ein gemeinsames Geheimnis vereinbart werden. Dies kann z. B. dadurch realisiert werden, daß von *A* ein nur *A* bekannter Schlüsselteil K_A mit dem öffentlichen Schlüssel von *B* verschlüsselt und in die Nachricht *Challenge1* integriert wird. Ebenso wird von *B* ein nur *B* bekannter Schlüsselteil K_B mit dem öffentlichen Schlüssel von *A* verschlüsselt in die Nachricht *Response1+Challenge2* integriert. Gelesen werden können diese Schlüsselteile nur bei Kenntnis[9] des jeweiligen geheimen Schlüssels (vgl. Abschnitt 3.4.2.4).

Die Kommunikationspartner können im Anschluß an eine erfolgreiche Authentisierung aus diesen Schlüsselteilen K_A und K_B mit einem (beiden Seiten) bekannten Algorithmus einen oder mehrere gemeinsame geheime Schlüssel K^i ableiten. Diese Schlüssel können an die zu aktivierenden Zwischenschichten übergeben werden. Der gemeinsame Schlüssel darf nur dann verwendet werden, wenn die Authentisierung erfolgreich verläuft.

Anforderungen an die Diensteumgebung: Die Diensteumgebung muß Möglichkeiten zur Synchronisierung der Authentisierungsinstanzen (z. B. durch Challenge- und Response-Nachrichten) zur Verfügung stellen. Dazu müssen die an der Authentisierung beteiligten Instanzen adressierbar und ein Dienst zur Übermittlung der Synchronisierungsnachrichten verfügbar sein. Eine Sicherheitsarchitektur sollte außerdem Mittel zum Zugriff auf Prüf-Information (z. B. Schlüsselzertifikate) zur Verfügung stellen und Schnittstellen zur Einbindung von sicheren Modulen (Auslagerung der Operationen auf einem Geheimnis) unterstützen.

4.3.2 Schutz von Nutzdaten und Steuerungsdaten durch Zwischenschichten

Das *Ziel* bei der Integration von transparenten Zwischenschichten ist der Schutz von Nutz- und Steuerungsdaten durch Einschleifen von Sicherheitsfunktionen in den Kommunikationspfad. Zum Schutz der Integrität übermittelter Nutzdaten könnte eine Zwischenschicht wie in Bild 3-5 zum Einsatz kommen. Der Dienstzugangspunkt für die Integritäts- und Vertraulichkeitsdienste der Zwischenschicht ist durch den Dienstzugangspunkt der darunterliegenden Schicht festgelegt (vgl. Bild 4-4). Erweiterungen dieses Dienstzugangspunktes betreffen die Initialisierung, Aktivierung und Deaktivierung der paarweise auftretenden Sicherheitsfunktionen. Dadurch ist die Zwischenschicht vertikal transparent für die Anwender, da der Dienstzugangspunkt nicht verändert (sondern höchstens erweitert) wird. Bild 4-16 zeigt die Erweiterung von Dienstzugangspunkten zur Steuerung transparenter Zwischenschichten (hier: ZS-SAP genannt).

9 Die Schlüsselteile müssen genügend zufällige Bits umfassen, um ein Raten des Schlüssels aussichtslos zu gestalten.

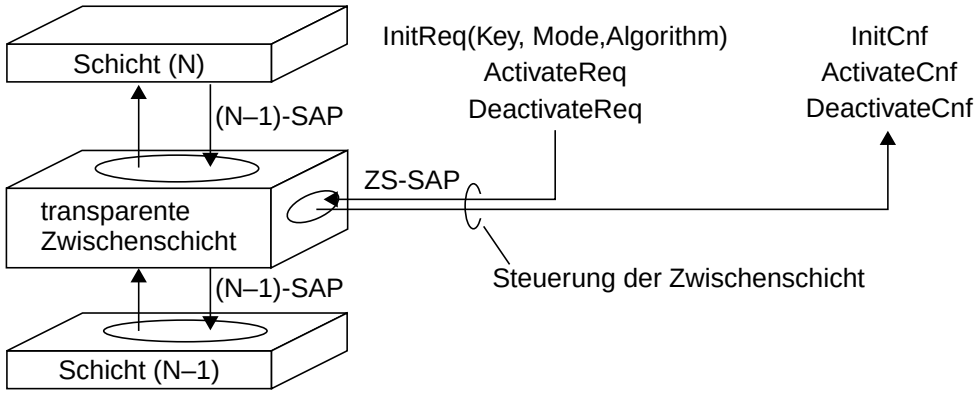


Bild 4-16: Erweiterte Dienstzugangspunkte für transparente Zwischenschichten

Vor der Aktivierung einer Sicherheits-Zwischenschicht muß diese durch das *InitReq*-Primitiv unter Angabe des zu benutzenden Schlüssels, des Algorithmus und des Betriebsmodus initialisiert werden. Die Schlüssel können, wie in Abschnitt 4.3.1 beschrieben, im Verlaufe einer vorausgehenden Authentisierung vereinbart werden.

Müssen sich die Partnerinstanzen vor der Benutzung der Zwischenschicht synchronisieren, so sollten die Zwischenschichten die Synchronisierung transparent für den Benutzer über den bestehenden (N–1)-SAP durchführen. Die erfolgreiche Initialisierung und Synchronisierung der Zwischenschicht wird durch das Primitiv *InitCnf* angezeigt. Dieses Primitiv zeigt die Betriebsbereitschaft der Zwischenschicht an.

Durch das Dienstprimitiv *ActivateReq* wird die Zwischenschicht schließlich aktiviert. Nun werden alle SDUs, die von Schicht (N) an Schicht (N–1) weitergegeben werden, verschlüsselt (bzw. mit Integritätsschutz versehen) und von der Partnerinstanz der Zwischenschicht entschlüsselt (bzw. geprüft). Daten können nacheinander unterschiedliche Sicherheitsfunktionen (z. B. Signatur und Verschlüsselung) durchlaufen. In der Gegenrichtung müssen die entsprechenden inversen Funktionen (z. B. Entschlüsselung und Signaturprüfung) in umgekehrter Weise angewendet werden. Die Partnerinstanzen in Zwischenschichten können sich bei Bedarf über den bestehenden (N–1)-SAP oder über den ZS-SAP resynchronisieren.

Die Zwischenschicht kann durch das Primitiv *DeactivateReq* deaktiviert werden. Wie dabei mit den benutzten geheimen Schlüsseln und den weiteren Parametern verfahren wird (speichern oder vernichten) ist implementierungsabhängig. Eine deaktivierte Zwischenschicht läßt SDUs zwischen den Schichten (N) und (N–1) unverändert passieren. Denkbar sind auch Primitive zum Blockieren des Datenaustausches über die Zwischenschicht (z. B. *BlockReq*, *UnblockReq*).

Beispiel: Zwischenschicht für Integritäts- und Verschlüsselungsdienste

Die in Bild 4-17 dargestellte Zwischenschicht bietet Integritäts- und Verschlüsselungsdienste an. Bei aktiviertem Integritätsschutz wird einer eingehenden (N–1)-SDU vor der Weitergabe an die Schicht N–1 eine kryptographisch mit K^I gesicherte Prüfsumme beigefügt. Bei aktiviertem Verschlüsselungsdienst wird die (N–1)-SDU vor der Weitergabe mit dem Schlüssel K^V verschlüsselt. Das Bild zeigt einen Fall, in dem sowohl Integritäts- als auch Verschlüsselungsdienst aktiviert sind. Die Protokoll-Kontrollinformation einer Sicherheits-Zwischenschicht muß in Form eines Klartext-Kopfes beigefügt werden, anhand dessen die empfangende Instanz die Entschlüsselung und Prüfung der Integrität steuern kann. Der Klartextkopf muß mindestens eine Kennung der Sicherheitsassoziation für den Empfänger beinhalten; die adressierte

Sicherheitsassoziation kennzeichnet in diesem Fall die kryptographischen Schlüssel und Algorithmen, die zum Entschlüsseln und zur Prüfung der Integrität beim Empfänger notwendig sind.

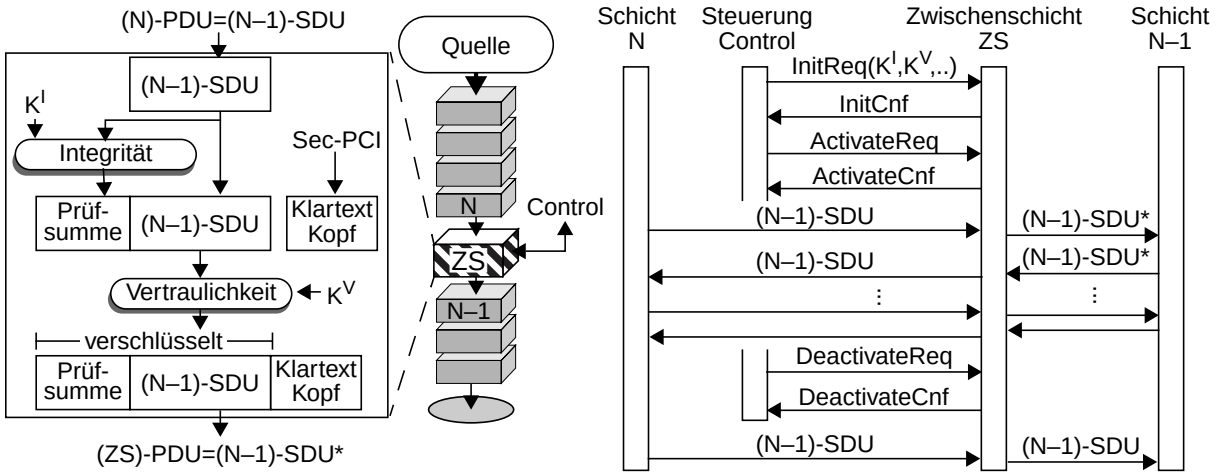


Bild 4-17: Eine Zwischenschicht zur Verschlüsselung und zum Integritätsschutz

Die von Schicht N empfangene (N–1)-SDU wird durch eine Prüfsumme ergänzt, verschlüsselt und anschließend mit einem Klartext-Kopf versehen. Diese hier als Zwischenschicht-PDU bezeichnete Einheit wird als (N–1)-SDU* an die Schicht (N–1) übergeben[10]. Die Partnerinstanz der Zwischenschicht empfängt diese (N–1)-SDU* und benutzt den Klartext-Kopf, um die Sicherheitsassoziation mit den Parametern zur Entschlüsselung und Integritätsprüfung zu adressieren. Dieser Klartext-Kopf bezeichnet die Kontrollinformation des Sicherheitsprotokolles (Security Protocol Control Information, SecPCI in Bild 4-17). Anschließend wird der verschlüsselte Teil der (ZS)-PDU entschlüsselt. Die Integritätsprüfung kann durchgeführt werden wie in Bild 3-5 dargestellt.

Die Steuerung der Zwischenschicht ist in Bild 4-17 auf der rechten Seite veranschaulicht. Bei der Initialisierung durch das *InitReq*-Primitiv werden der Zwischenschicht die zu verwendenden Schlüssel und die Parameter der zu initialisierenden Dienste übergeben. Nach der Aktivierung durch das *ActivateReq*-Primitiv beginnt die Zwischenschicht, eine empfangene (N–1)-SDU vor ihrer Weitergabe in eine (N–1)-SDU* nach oben beschriebenem Verfahren umzuwandeln, d. h. zu schützen. Mit dem *DeactivateReq*-Primitiv wird die Zwischenschicht vollständig transparent geschaltet. Die empfangenen (N–1)-SDUs werden bei inaktiver Sicherheitsfunktionalität unverändert an Schicht (N–1) weitergegeben.

Entsprechend wird in umgekehrter Richtung auf der Empfangsseite verfahren. Die Synchronisierung der Partnerinstanzen der Zwischenschicht sei in diesem Fall durch übergeordnete Mechanismen realisiert. Die empfangende Instanz kann beispielsweise anhand von Redundanz im Klartext-Kopf erkennen, ob und welche Schutzmechanismen auf Senderseite angewendet wurden und die inversen Funktionen anstoßen.

Anforderungen an die Diensteumgebung: Der Zugang zum Dienstzugangspunkt ZS-SAP zur Steuerung der Zwischenschicht durch eine übergeordnete Sicherheitssteuerung muß möglich

10 Die (N–1)-SDU wird bei aktivierter Zwischenschicht mit * versehen, um anzuzeigen, daß sie sich von der (N–1)-SDU bei inaktiver Zwischenschicht unterscheidet und auf Empfängerseite nicht direkt durch die Schicht (N) verarbeitbar ist.

sein. Die Resynchronisierung der Sicherheitsfunktionen innerhalb einer Zwischenschicht sollte über den vorhandenen Dienstzugangspunkt (N–1)-SAP transparent für darunterliegende Schichten realisierbar sein. Eine Resynchronisierung kann z. B. notwendig werden, wenn Datenpakete während der Übermittlung verlorengehen bzw. eingefügt werden. Die Notwendigkeit und der Aufwand einer Resynchronisierung sind vom verwendeten Schutzverfahren abhängig.

4.3.3 Schutz der Kommunikationsbeziehung

Im Informationszeitalter gewinnen Informationsdienste, die sehr spezifische Informationen anbieten, mehr und mehr an Bedeutung. Dadurch kann der bloße Zugriff auf solche Dienste Informationen über Interessen eines Benutzers preisgeben. Ist aus der Netzadresse des Benutzers seine Identität ableitbar (z. B. bei öffentlichen Rufnummern), so können durch Verknüpfung der durch einen Dienst angebotenen Informationen mit der Identität des anfragenden Benutzers schützenswerte Informationen entstehen.

Schutzziel: Die Netzadresse (hier: Rufnummer) des anfragenden Teilnehmers und des gerufenen Informationsdienstes sollen durch die Netzbetreiber oder externe beobachtende Angreifer nicht in Beziehung gesetzt werden können.

Problem: Die Netzadressen des Benutzers und des Informationsdienstes sind durch Endgerät und Informationsdienst *nicht EzE-sicherbar.* Die Adresse des Benutzers kann aus der Dienstanforderung abgeleitet werden; die Adresse des Informationsdienstes muß dem Kommunikationsnetz (im ISDN) zum Verbindungsaufbau zur Verfügung stehen. Die Adressierungs- und Routingfunktionen beim Verbindungsaufbau liegen unterhalb der EzE-Grenzlinie.

Lösung: Die Information über die Beziehung zwischen Benutzer und Informationsdienst wird verteilt, indem die Verbindung über ein Zwischensystem (hier: Proxy-Server) geführt wird. Für einen externen Beobachter ist aus dem Verlauf der Verbindungen ableitbar: (i) Der Benutzer baut eine Verbindung zum Proxy-Server auf und (ii) der Proxy-Server baut eine Verbindung zu einem Informationsdienst auf. Es muß verhindert werden, daß angenommene Angreifer diese Teilverbindungen korrelieren und so die Beziehung Benutzer–Informationsdienst aufdecken können. Der Proxy-Server muß (hier) vertrauenswürdig sein bezüglich der Vertraulichkeit der Kommunikationsbeziehung Benutzer–Informationsdienst.

Bild 4-18 zeigt eine Möglichkeit, die Beziehung zwischen Benutzer und Informationsdienst gegenüber Netzbetreibern und externen Angreifern dadurch zu verschleiern, daß sehr viele Benutzer den Proxy-Server nutzen (d. h. Verbindungen zum Proxy-Server aufbauen) und der Proxy-Server Verbindungen zu einer Vielzahl von Informationsdiensten unterhält.

Dadurch wird eine sogenannte Anonymitätsgruppe erzeugt. Die Benutzer greifen auf Informationsdienste indirekt über einen Proxy-Server zu. Dieser Proxy-Server verteilt die Anfragen auf unterschiedliche Informationsdienste. Die für den Netzbetreiber oder externe Angreifer sichtbaren Verbindungen verlaufen stets vom Benutzer zum Proxy-Server und vom Proxy-Server zum Informationsdienst. Die korrekte Zuordnung der Teilverbindungen ist nur dem Proxy-Server bekannt und darf durch Beobachtung nicht ableitbar sein.

Anhaltspunkte für eine Korrelation der Verbindungsteile *Benutzer→Proxy* und *Proxy→Informationsdienst* müssen gegen angenommene Angreifer geschützt werden:

- *Ziel-Information:* Die Rufnummer des Informationsdienstes wird durch den Benutzer auf dem Verbindungsweg zum Proxy-Server geschützt (i. a. verschlüsselt). Ebenso muß die

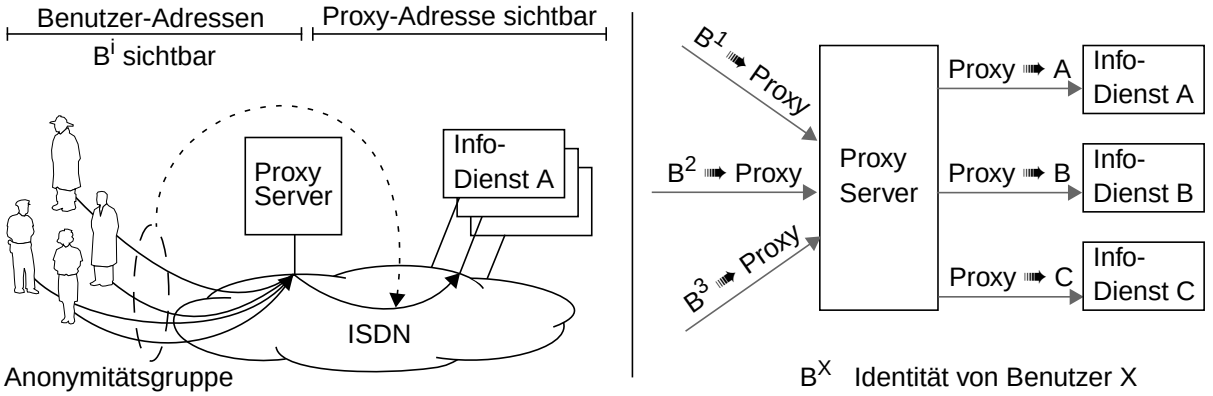


Bild 4-18: Schutz von Kommunikationsbeziehungen durch Anonymitätsgruppen

Identität des Benutzers zwischen Proxy-Server und Diensteserver geschützt werden, falls diese an den Informationsdienst weitergegeben wird.

- *Zeitliche Korrelation von Steuerungsvorgängen ein- und ausgehender Verbindungen am Proxy-Server:* Durch spezielle Vorkehrungen (vgl. [8],[37]) können zeitliche Korrelationen beim Verbindungsauf- oder -abbau über den Proxy-Server verborgen werden. Beispielsweise können Verbindungswünsche im Proxy gesammelt und dann zeitlich zufällig oder gemeinsam in einem Schub zu den entsprechenden Informationsdiensten weitergeleitet werden.

- *Korrelation der am Proxy ein- und ausgehenden Nutzdaten:* Durch Vergleich der am Proxy ein- und ausgehenden Nutzdaten (Kodierung oder Nachrichtenlängen) könnten zueinandergehörige Verbindungsteile identifiziert werden. Dies kann dadurch verhindert werden, daß der Nutzdatenstrom zwischen Benutzer und Proxy-Server bzw. zwischen Proxy-Server und Informationsdienst mit unterschiedlichen (nur den jeweiligen Sendern und Empfängern) bekannten Schlüsseln verschlüsselt werden oder indem nur Nachrichten fester Länge benutzt und diese verschlüsselt werden.

Solange die Anonymitätsgruppe mehr als einen Benutzer und die Dienstgruppe mehr als einen Dienst umfaßt ist nicht eindeutig ableitbar, welcher Benutzer auf welchen Dienst zugreift. Je größer die Anonymitätsgruppe und je vielfältiger die über den Proxy genutzten Informationsdienste, desto weniger Informationen sind den Kommunikationsereignissen zuordenbar. Soll auch dem Proxy-Dienst nicht vertraut werden, so kann auf sogenannte MIXe (vgl. [8], [37]) zurückgegriffen werden. Die dabei verwendeten Verfahren resultieren i. a. in einer Verteilung der Proxy-Funktionalität auf mehrere (mindestens zwei) nacheinander durchlaufene Proxy-Server. Zum Aufdecken der Beziehung von Benutzer und Info-Dienst ist bei optimaler Konfiguration die Zusammenarbeit aller durchlaufener Proxy-Server notwendig. Ein vertrauenswürdiger Proxy-Server reicht in diesem Fall, um die Vertraulichkeit der Beziehung zu garantieren.

Grenzen des Verfahrens: Durch aktives Eingreifen des Netzbetreibers könnte die Anonymitätsgruppe bis auf einen Teilnehmer reduziert werden; damit wäre die Kommunikationsbeziehung aufgedeckt. Außerdem könnte der Netzbetreiber oder ein Informationsanbieter die Datenrate sehr stark absenken und dann beobachten, ob sich ein Benutzer auffällig korreliert zu den Änderungen verhält (z. B. Dienst abbricht etc.).

Anforderungen an die Diensteumgebung: Aufgrund der angestrebten großen Anonymitätsgruppe sollte der Proxy-Server als Netzdienst ansprechbar sein. Dazu muß der Proxy-Server

durch die Benutzer adressierbar sein und seinerseits die Informationsdienste adressieren können. Schützenswerte Daten müssen zwischen Endgerät und Proxy-Server bzw. zwischen Proxy-Server und Dienst geschützt (z. B. verschlüsselt) werden können. Der Proxy sollte unabhängig von den Netzbetreibern und Informationsdiensteanbietern betrieben werden können.

4.4 Sicherheitsarchitektur für mehrseitig sichere TK-Dienste – Anforderungen und Bausteine

Die Zusammenhänge von Plazierung und Zusammenwirken von Sicherheitsfunktionen zur Erbringung von Sicherheitsdiensten sind nun erarbeitet. Nachfolgend werden die aus den Beziehungen zwischen Sicherheits- und TK-Funktionen resultierenden Anforderungen an eine Sicherheitsarchitektur für mehrseitig sichere Telekommunikationsdienste aufgezeigt.

Zur Unterstützung der durch die Hinzunahme von Sicherheitsfunktionen entstehenden Beziehungen (oder auch Interaktionsmuster) werden zwei neue Komponenten eingeführt. Sie stellen die Grundbausteine der vorgeschlagenen Sicherheitsarchitektur dar: Die *Sicherheitsadaptionsschicht (Security Adaptation Layer, SAL)* unterstützt die Kopplung von Sicherheitsdiensten und bestehenden Telekommunikationsdiensten zur Garantie von Schutzzielen während der Diensterbringung. Die Steuerung der Sicherheitsadaptionsschicht durch den Benutzer oder durch Anwendungsprozesse wird durch die sogenannte *Sicherheitsdienstesteuerung (SSS-Steuerung, Security Supplementary Services Control)* unterstützt.

Die Gestaltung der letztendlich durch einen sicheren Dienst garantierten Schutzziele im Sinne der *mehrseitigen Sicherheit* begründet folgende allgemeinen Anforderungen an die Diensteumgebung:

- Integration von Sicherheitsfunktionen in *sichere Ablaufumgebungen* als Basis von Sicherheitsdiensten (siehe Abschnitt 4.1, 4.2)
- Vereinbarungen über das Zusammenwirken von Sicherheitsfunktionen zur Realisierung von *Sicherheitsdiensten* (Sicherheitsmechanismen, Protokolle, siehe Abschnitt 4.3)
- Aushandlung von *Schutzzielen* zwischen Betroffenen und Ableitung zu aktivierender Sicherheitsdienste

Die Art und Weise der Mensch-Maschine-Interaktion nach Maßgabe dualer Sicherheit führt darüberhinaus zu folgenden allgemeinen Anforderungen an die Diensteumgebung:

- Nachvollziehbarkeit von sicheren Telekommunikationsdiensten bedingt, daß den Benutzern klar ist, welche Schutzziele in einer gegebenen Situation garantiert sind. Dies ist durch die Mensch-Maschine-Schnittstelle zu unterstützen.
- Beherrschbarkeit von sicheren Telekommunikationsdiensten bedingt, daß der Benutzer kontrollieren und beeinflussen kann, wie der sichere Telekommunikationsdienst arbeitet. Der neue Aspekt hierbei ist die Kontrolle der Sicherheitsbestandteile eines Kommunikationsdienstes, d. h. die Visualisierung der Vorgänge in einer für den Benutzer verständlichen Art und Weise und Eingriffsmöglichkeiten des Benutzers in den Ablauf der Dienste.
- Zurechenbarkeit von Kommunikationsereignissen wird durch optionale Authentisierungsdienste auf unterschiedlichen Ebenen unterstützt (z. B. Authentisierung von Benutzeridentitäten). Die Rechtsverbindlichkeit wird technisch durch einen evaluierungsfreundlichen

Entwurf der Sicherheitsarchitektur unterstützt. Eine vertrauenswürdige Diensteplattform und (für die Betroffenen) nachvollziehbar ablaufende Sicherheitsdienste sind notwendige Voraussetzung für die Rechtsverbindlichkeit.

Aus diesen Gestaltungszielen lassen sich Anforderungen an eine Sicherheitsarchitektur ableiten. Bild 4-19 zeigt ein Modell für mehrseitig sichere Telekommunikationsdienste basierend auf dem additiven Ansatz, der in Abschnitt 4.1 vorgestellt wurde. Die Aushandlung gemeinsamer Schutzziele wird durch die Benutzer vorgenommen; sie kann durch Technik (hier: Sicherheitsdienstesteuerung) unterstützt werden. Basierend auf den ausgehandelten Schutzzielen werden durch die Benutzer Sicherheitsdienste angefordert. Diese werden vom Telekommunikationssystem durch Aktivierung und Betrieb von Sicherheitsfunktionen umgesetzt.

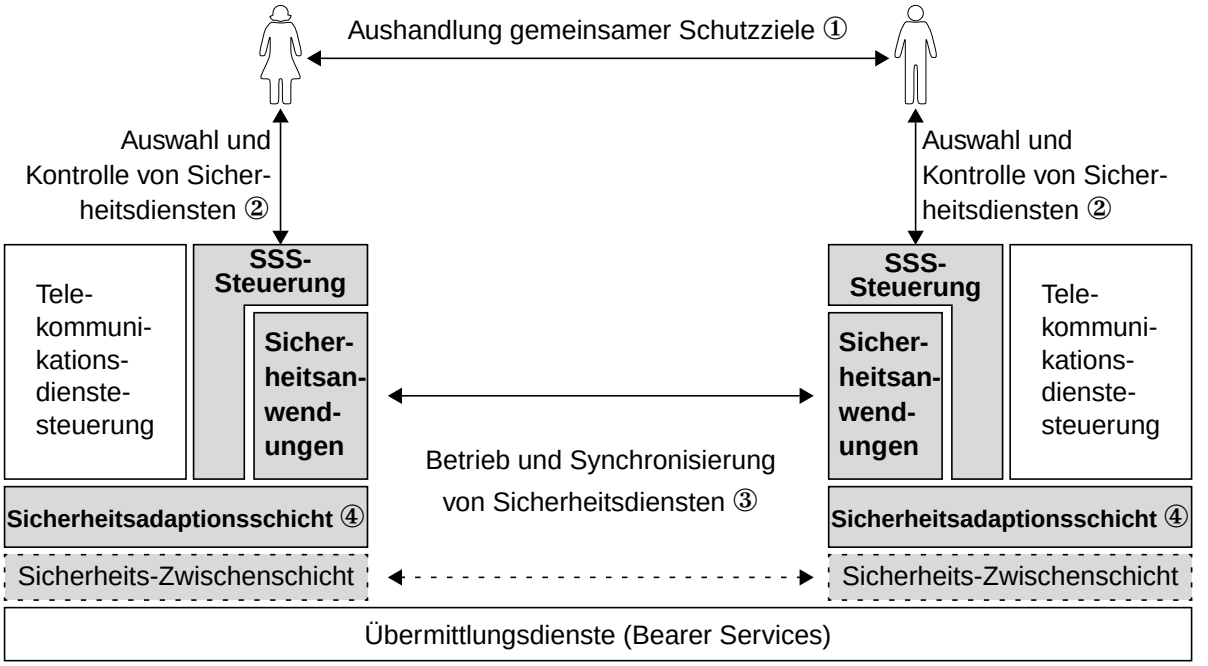


Bild 4-19: Komponenten einer Plattform für mehrseitig sichere Dienste

Sicherheitsanwendungen reichern die bestehenden Teledienste optional an. Sie werden deshalb in Anlehnung an die zusätzlichen Dienstmerkmale im ISDN als *Security Supplementary Services* (SSS) bezeichnet.

Transparente *Sicherheits-Zwischenschichten* enthalten Sicherheitsfunktionen zum Schutz der Integrität oder Vertraulichkeit von Nutz- bzw. Dienstesteuerungsdaten. Die durch sie erbrachten Sicherheitsdienste werden auch als *Security Bearer Services* bezeichnet, da sie Übermittlungsdienste anreichern.

Die *Sicherheitsadaptionsschicht (SAL)* faßt die Funktionen zur Synchronisierung von Sicherheits- und Telekommunikationsdiensten zusammen und ermöglicht so über die Sicherheitsdienstesteuerung optional zuschaltbare Sicherheitsdienste.

Die *Sicherheitsdienstesteuerung (SSS-Steuerung)* stellt das Bindeglied zwischen der Auswahl von Sicherheitsdiensten durch den Benutzer, den im Telekommunikationssystem implementierten *Sicherheitsanwendungen* und der *SAL* dar.

Gemäß der Definition einer Sicherheitsarchitektur spielen vor allem die Beziehungen eine Rolle, an denen Sicherheitskomponenten (SAL, SSS-Steuerung, Sicherheitsanwendungen, Zwischenschichten) und Benutzer beteiligt sind. Diese umfassen Beziehungen (i) zwischen Benutzern, (ii) zwischen Sicherheitskomponenten und Benutzern, (iii) zwischen Sicherheitskomponenten sowie (iv) zwischen Sicherheitskomponenten und existierenden Telekommunikationskomponenten. Die aus diesen Beziehungen folgenden Anforderungen aus Netzsicht müssen durch die Sicherheitsarchitektur erfüllt werden. Dazu werden die Komponenten der Sicherheitsarchitektur, die *Sicherheitsdienstesteuerung* und die *Sicherheitsadaptionsschicht*, im Hinblick auf die Unterstützung dieser Anforderungen verfeinert.

4.4.1 Sicherheitsdienstesteuerung

Die Hauptaufgaben der Sicherheitsdienstesteuerung sind der Aufbau einer Sicherheitsassoziation, d. h. die Unterstützung der Aushandlung von Schutzzielen und die Festlegung der zu verwendenden Sicherheitsdienste, und die Steuerung der Benutzerinteraktion.

4.4.1.1 Aushandlung von Schutzzielen und Steuerung der Benutzerinteraktion

Gemäß der Definition in Abschnitt 3.2.2 müssen *mehrseitig sichere Dienste* die Schutzziele aller Betroffener in angemessenem Maße berücksichtigen. Wie in Abschnitt 3.2.3 beschrieben, muß gegebenenfalls über unverträgliche oder widersprüchliche Schutzziele verhandelt werden (vgl. ① in Bild 4-19). Da die Schutzziele der Betroffenen vom jeweils genutzen Telekommunikationsdienst und den Nutzdatenanwendungen abhängen, müssen sie flexibel ausgehandelt werden können.

Die Aushandlung von Schutzzielen wird in [20] am Beispiel eines Erreichbarkeitsmanagementsystems näher beschrieben. Eine die Aushandlung unterstützende Mensch-Maschine-Schnittstelle wurde in der Praxis getestet. Die Ergebnisse betreffend die Aushandlung und die Gestaltung der Mensch-Maschine-Schnittstelle sind in [21] dargelegt. Sie betreffen vor allem die Ergonomie der Benutzeroberfläche und die korrekte Interpretation von Benutzereingaben durch das Gerät sowie der Geräteanzeigen durch den Benutzer. Die Mensch-Maschine-Schnittstelle muß dafür ausgelegt sein, die Benutzer in der verantwortlichen Nutzung von (mehrseitig sicheren) Telekommunikationsdiensten zu unterstützen.

Die ausgehandelten Schutzziele werden durch den Benutzer oder automatisiert auf Sicherheitsdienste abgebildet. Für jeden Sicherheitsdienst sind die Sicherheitsmechanismen (z. B. Verschlüsselung) und ihre Ausprägung (z. B. Algorithmus, Schlüssellänge, Betriebsweise) zu bestimmen.

Aus Gründen der *Beherrschbarkeit* ist besonders die *Abbildung von Schutzzielen auf letztendlich aktive Sicherheitsdienste* (vgl. ② in Bild 4-19) für den Benutzer von Interesse. Der Benutzer muß sich jederzeit über die aktivierten Dienste informieren und gegebenenfalls korrigierend in die Diensterbringung eingreifen können. Diese vertikale Schnittstelle wird durch die diesbezügliche Implementierung der Mensch-Maschine-Schnittstelle festgelegt. An dieser Stelle werden die Sichten von Benutzer und Maschine zusammengeführt.

Eine solche Mensch-Maschine-Schnittstelle wird im Projekt *Sicherheit und Schutz in offenen Datennetzen* [23], gefördert vom Bundesministerium für Bildung, Wissenschaft, Forschung und Technologie (BMBF) entwickelt. Den Anwendern der modernen Entwicklungen der Telekommunikation soll ermöglicht werden, bei der Nutzung verteilter Anwendungen ihre Sicherheitsinteressen und -bedürfnisse zu formulieren und durchzusetzen. Ausgehend von Schutzzie-

len, wie z. B. Vertraulichkeit des Kommunikationsinhaltes, werden Sicherheitsdienste und Mechanismen bestimmt, die dieses Schutzziel technisch umsetzen.

Aus Netzsicht muß der zur Aushandlung notwendige Datenaustausch durch die Sicherheitsdienstesteuerung unterstützt werden.

4.4.1.2 Aufbau einer Sicherheitsassoziation

Anforderungen an die *Kompatibilität* unterschiedlich erweiterter und herkömmlicher Endgeräte bedingen die *Festlegung von Sicherheitsmechanismen* zur Realisierung von Sicherheitsdiensten (vgl. ③ in Bild 4-19). Die Assoziation zwischen Sicherheitsdiensten und Sicherheitsmechanismen sollte flexibel sein, damit Sicherheitsmechanismen beim Bekanntwerden von Angriffsmöglichkeiten durch bessere Sicherheitsmechanismen ersetzt werden können bzw. unterschiedliche Kommunikationsendgeräte eine gemeinsame Menge von Sicherheitsmechanismen und zugehörige Parameter identifizieren und nutzen können. Zur Problematik der Sicherheit verschiedener kryptographischer Verfahren und ihrer Implementierungen siehe z. B. [10], [12], [62].

Voraussetzung für eine solche Vereinbarung sind eindeutige Identifikatoren für unterschiedliche Mechanismen und Protokollen (z. B. Algorithmen, verwendete Schlüssellängen, Betriebsweisen, Zertifikate etc.). Kodierungen für Algorithmen und Schlüssellängen etc. wurden vom ATM-Forum für die ATM-Sicherheitsspezifikation [72] bereits erarbeitet. Anforderungen für die Interoperabilität von Zertifikaten (z. B. zur sicheren Zuordnung von öffentlichen Schlüsseln zu Identitäten) werden in [126] beschrieben und Kodierungsvorschriften für Zertifikate sind in [116] spezifiziert.

Die *Sicherheitsassoziation* stellt die Zusammenfassung aller zwischen zwei oder mehreren Instanzen vereinbarten Sicherheitsparameter eines Sicherheitsdienstes dar. Es existiert zu jedem aktiven Sicherheitsdienst eine Sicherheitsassoziation. Sie beinhaltet

- die Menge aktiver Sicherheitsmechanismen zur Erbringung eines Sicherheitsdienstes und zugehörige Parameter sowie
- Protokolle, die das Zusammenspiel verteilter Sicherheitsfunktionen zur Erbringung eines Sicherheitsdienstes regeln.

Die *Sicherheitsdienstesteuerung* als übergeordnete Instanz führt eine kumulierte Sicherheitsassoziation, die alle Sicherheitsparameter enthält, die für den Benutzer von Interesse sein können. Diese Sicherheitsassoziation wird bei der Bestimmung der zu aktivierenden Sicherheitsdienste durch den Benutzer vorgegeben oder aus den Benutzereingaben abgeleitet.

Die Sicherheitsdienstesteuerung gibt diese Parameter an die *Sicherheitsadaptionsschicht* weiter (vgl. ④ in Bild 4-19). Die SAL verteilt im Rahmen der Initialisierung und Aktivierung die relevanten Parameter – z. B. Identifikator für Algorithmus und Betriebsweise, Schlüssellänge, Protokoll, vereinbarte Schlüssel etc. – an die entsprechenden Sicherheitsinstanzen. Für jeden aktiven Sicherheitsdienst wird eine Sicherheitsassoziation angelegt und mittels sogenannter Security Association Identifier (SA-ID [119]) verwaltet. Dadurch können Nutzdaten unterschiedlicher (logischer) Verbindungen innerhalb derselben Zwischenschicht unabhängig voneinander geschützt werden.

Bild 4-20 zeigt exemplarisch drei Sicherheitsassoziationen: Die Benutzer-Benutzer-Authentisierung folgt dem ITU-Standard X.509. Es wird als PublicKey-Verfahren beschrieben und benutzt RSA als asymmetrisches Verschlüsselungssystem. Es wird mit einer Schlüssellänge

von 1024 Bit gearbeitet. Die verwendeten Schlüssel umfassen den geheimen Schlüssel, der i. a. nicht innerhalb eines Kommunikationsgerätes, sondern in einer sicheren Umgebung (z. B. Chip-Karte) gehalten wird, Schlüsselzertifikate der Kommunikationspartner und den öffentlichen Prüfschlüssel der Zertifizierungsinstanz zur Prüfung der Zertifikate (siehe Abschnitt 4.3.1). Diese Assoziation wird von der Authentisierungsanwendung genutzt und gepflegt.

Sicherheitsdienst	SA-ID	Mechanismus	Algorithmus	Modus	Protokoll	Schlüssel	
Benutzer-Benutzer-Authentisierung	0001	PublicKey Authentisierung	RSA	3-Way	ITU-X.509 [116]	1024 Bit	..
Integritätsschutz Nutzkanal B1	0003	Shared Secret Key Hashwert	HMAC-SHA1	t=80	RFC 2104 [135]	128 Bit	..
Verschlüsselung Nutzkanal B1	0017	Shared Secret Key Verschlüsselung	DES	CBC	ISO 8372 [88]	64 Bit	..

Bild 4-20: Beispiele für Sicherheitsassoziationen

Analog werden die Sicherheitsfunktionen zur Realisierung der Schutzziele *Integrität und Vertraulichkeit der übermittelten Nutzdaten* beschrieben. Im Beispiel arbeiten die Verfahren mit symmetrischen Kryptosystemen zur Erzeugung geschützter Hashwerte beziehungsweise zur Verschlüsselung von Nutzdaten. Diese Assoziationen werden in den jeweiligen Zwischenschichten genutzt und gepflegt.

Die Sicherheitsanwendungen und die Zwischenschichten, die Sicherheitsdienste anbieten, verwalten ihre Sicherheitsassoziationen nach der Initialisierung autonom. Änderungen von Parametern dürfen nur synchron in allen an einem Sicherheitsdienst beteiligten Kommunikationssystemen (bzw. den beteiligten Instanzen) verändert werden.

4.4.1.3 Verfeinerte Struktur der Sicherheitsdienstesteuerung

Im folgenden wird die Sicherheitsdienstesteuerung verfeinert. Im Mittelpunkt stehen die Beziehungen, die durch sie ermöglicht oder unterstützt werden. Die Sicherheitsdienstesteuerung ist wie in Bild 4-21 dargestellt modular aufgebaut.

Über die Benutzer-Schnittstelle können Teilnehmer ihre Schutzziele spezifizieren und mit Hilfe der *Aushandlungsfunktionen* mit den anderen Teilnehmern abgleichen (Schnittstelle *1* in Bild 4-21). Der zur Aushandlung notwendige Datenaustausch wird über die Schnittstelle *4* von der SAL angefordert (Datenübermittlungsdienst der SAL). Optional können über die Benutzer-Schnittstelle alle Sicherheitsanwendungen durch den Benutzer direkt (unabhängig von der SAL) angesprochen werden.

Die Auswahl von Sicherheitsdiensten und Mechanismen erfolgt über die *Benutzer-Schnittstelle* (*2* in Bild 4-21). Die SAL-Steuerung aktiviert bei Bedarf die geforderten Sicherheitsdienste und integriert sie in die Synchronisierung mit den zu sichernden TK-Diensten. Sicherheitsanwendungen können über die *Schnittstelle für sichere Module* (*3* in Bild 4-21, z. B. Schnittstelle eines Chipkartenlesegerätes [76]) auf ausgelagerte Funktionen (z. B. Signatur mit geheimem Schlüssel) zurückgreifen.

Die *Sicherheitsanwendungen* werden von der Sicherheitsdienstesteuerung lediglich verwaltet. Sie können deshalb einfach ergänzt werden. Den Sicherheitsanwendungen steht der Datenübermittlungsdienst der SAL zum Austausch von Sicherheitssteuerungsinformation (z. B.

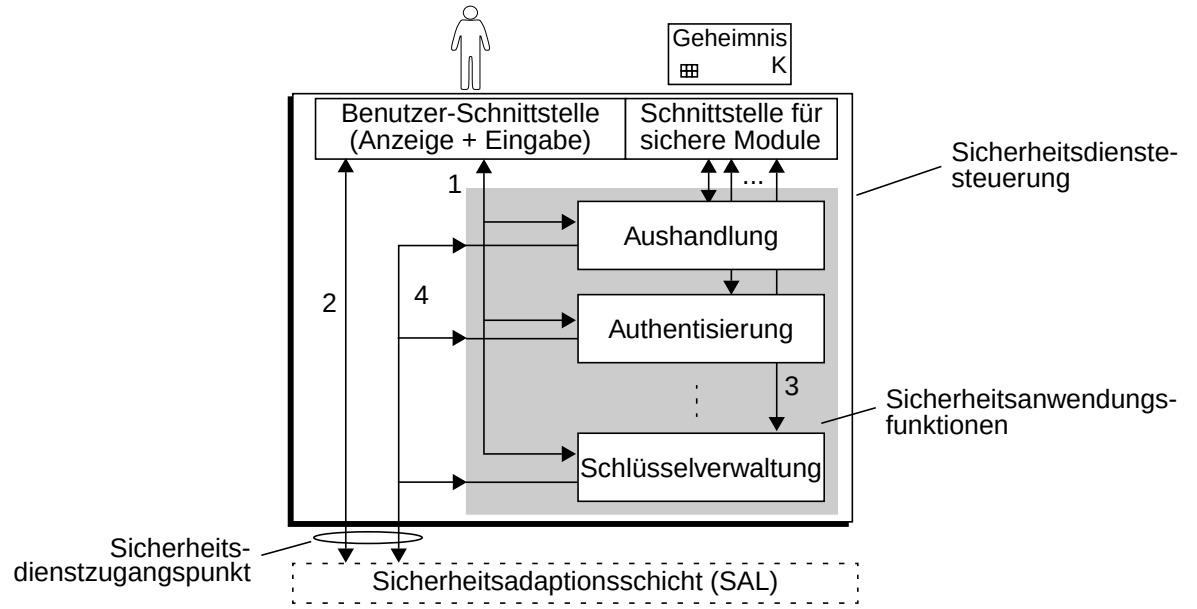


Bild 4-21: Verfeinerte Struktur der Sicherheitsdienstesteuerung

Authentisierungsnachrichten) zur Verfügung. Die Ansteuerung der Sicherheitsdiensteanwendungen durch die SAL erfolgt über die Schnittstelle *4*.

4.4.2 Sicherheitsadaptionsschicht

Ausgehend von einer Menge von vereinbarten Schutzzielen müssen Sicherheitsdienste benutzerkontrolliert aktiviert und mit bestehenden Telekommunikationsdiensten gekoppelt werden. Eine flexible Aushandlung (siehe Abschnitt 4.4.1.1) von Schutzzielen setzt voraus, daß Sicherheitsmechanismen möglichst unabhängig sind vom genutzten Telekommunikationsdienst (z. B. Datendienst) und von den Nutzanwendungen (z. B. File-Transfer, Internet-Zugang).

Die in diesem Abschnitt näher beschriebene *Sicherheitsadaptionsschicht* adaptiert neue Sicherheitsdienste an herkömmliche Telekommunikationsdienste (vgl. Bild 4-19). Sie ist dafür verantwortlich, daß die ausgehandelten Sicherheitsdienste flexibel in die Diensterbringung integriert werden können. Aufgrund der Vielfalt der durch sie unterstützten Beziehungen stellt sie die zentrale Komponente der Sicherheitsarchitektur dar.

4.4.2.1 Prinzipien der Funktionsweise der Sicherheitsadaptionsschicht

Die SAL dient als Bindeglied zwischen neu hinzugefügten Sicherheitsdienstefunktionen und herkömmlichen Telekommunikationsdiensten (vgl. Bild 4-1). Sie sorgt dafür, daß ausgehandelte Sicherheitsmechanismen initialisiert, aktiviert und mit dem Ablauf von Telekommunikationsdiensten synchronisiert werden.

Die primären Anforderungen an die SAL lassen sich wie folgt zusammenfassen:

- Die SAL muß die vollständige *Kontrolle über die Telekommunikationsdienste* besitzen. Diese Kontrolle wird zur Einleitung von Ausnahmebehandlungen genutzt, falls die für einen TK-Dienst geforderten Sicherheitsdienste nicht erfolgreich ablaufen.
- Es muß ein logischer *Synchronisierkanal für hinzugefügte Sicherheitsfunktionen* (inklusive Sicherheitsdienstesteuerung) zur transparenten Übermittlung von Sicherheitssteuerungsdaten zur Verfügung gestellt werden.

- Die SAL muß die *Kommunikation zwischen Sicherheitskomponenten* innerhalb eines Kommunikationssystems koordinieren. Sie initialisiert, aktiviert und deaktiviert Sicherheitsdienste und hält Informationen über deren aktuellen Zustand.

  Beispiel: Anwendungsdaten können in einer transparenten Zwischenschicht in der Nutzdaten-Ebene verschlüsselt werden. Dazu muß der Zwischenschicht mitgeteilt werden ob, nach welchem Algorithmus, mit welchem Schlüssel und in welcher Betriebsweise Nutzdaten verschlüsselt werden sollen. Dies wird der Steuerung der Zwischenschicht durch die SAL mitgeteilt. Rückmeldungen der Zwischenschicht an die SAL-Steuerung umfassen z. B. die Betriebsbereitschaft und Synchronisierungsfehler beim Ver- bzw. Entschlüsseln.

- Die *Kopplung von Sicherheits- und TK-Dienst* muß auf das Notwendigste beschränkt sein. So ist eine weitgehende Unabhängigkeit von Sicherheits- und TK-Dienstablauf garantiert. Die Art der Kopplung muß flexibel auf die Anforderungen der Benutzer abgestimmt werden.

  Beispiel: Eine Benutzer-Benutzer-Authentisierung kann mit dem Verbindungsaufbau synchronisiert werden; der Verbindungsaufbau wird in diesem Fall nur dann vervollständigt, wenn die Authentisierung der Kommunikationspartner erfolgreich abgeschlossen wurde.

Die aus diesen Anforderungen abgeleitete Plazierung der SAL innerhalb eines Kommunikationssystems und ihre Schnittstellen werden im folgenden näher untersucht.

4.4.2.2 Einordnung und Arbeitsweise der Sicherheitsadaptionsschicht

Die *Sicherheitsadaptionsschicht* unterstützt als zentrale Komponente der Sicherheitsarchitektur die Beziehungen zwischen Sicherheits- und TK-Diensten über die in Bild 4-22 bezeichneten Schnittstellen. Das Bild veranschaulicht die Anordnung zur Kopplung herkömmlicher Telekommunikationsdienste und neu integrierter Sicherheitsfunktionen (unterlegt).

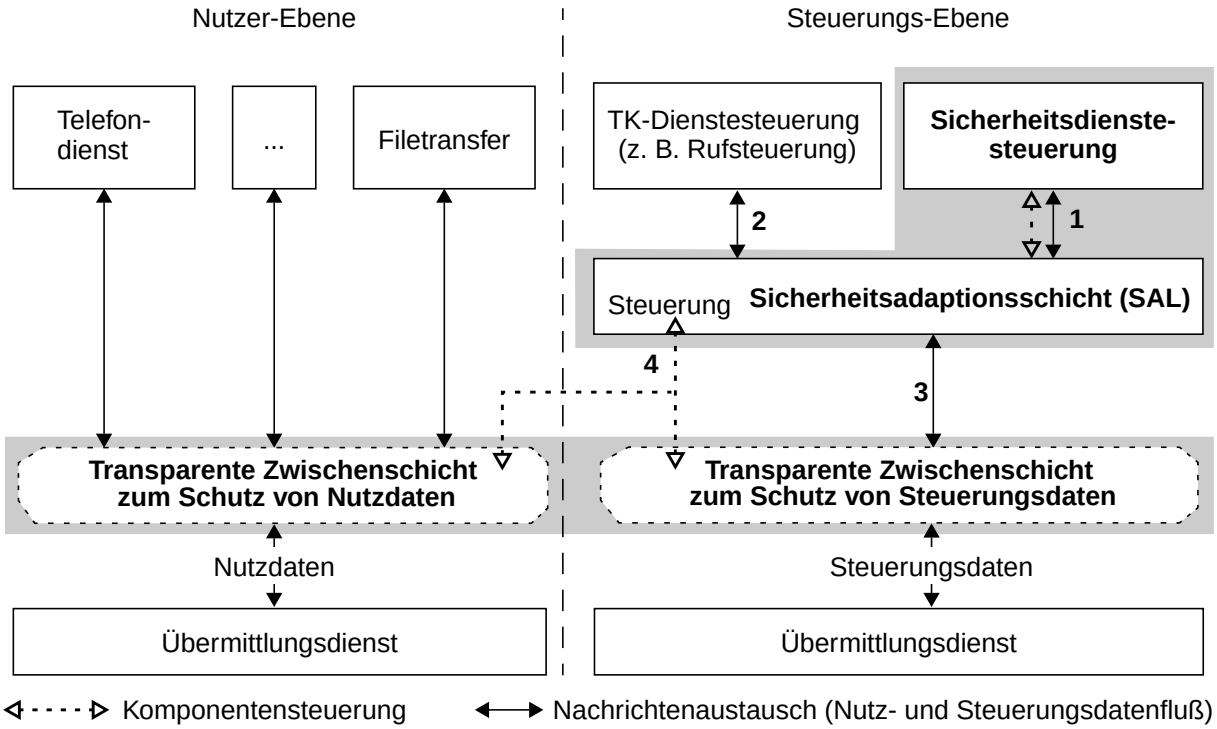


Bild 4-22: Kopplung von Sicherheits- und Telekommunikationsdienst

Steuerung von Sicherheitskomponenten

Die innerhalb der Sicherheitsdienstesteuerung implementierten Sicherheitsanwendungen (z. B. Aushandlung, Authentisierung) können direkt durch die SAL-Steuerung über die Schnittstelle *1* in Bild 4-22 angestoßen werden.

Sicherheitsfunktionen zum Schutz von Nutzdaten und Steuerungsdaten (in Form transparenter Zwischenschichten) werden durch die SAL-Steuerung gemäß des ZS-Dienstzugangspunktes (vgl. ZS-SAP in Bild 4-16) über die Schnittstelle *4* in Bild 4-22 gesteuert. Mit Hilfe von Status-Rückmeldungen (z. B. *ActivateCnf*) pflegt die Sicherheitsadaptionsschicht ihre Sicht auf die innerhalb von Zwischenschichten realisierten Sicherheitsdienste.

Synchronisierung kooperierender Sicherheitsdienstefunktionen

Die Sicherheitsdienstesteuerungen der verschiedenen Teilnehmer tauschen Steuerungsdaten im Rahmen der Aushandlung von Schutzzielen und der Implementierung von Sicherheitsanwendungsdiensten aus. Die SAL unterstützt diesen Datenaustausch durch das Anbieten eines Datenübermittlungsdienstes an der Schnittstelle *1* in Bild 4-22 (z. B. zum Austausch von Authentisierungsnachrichten, vgl. Bild 4-15). Kooperierende Instanzen in *Zwischenschichten* können sich bei Bedarf ebenfalls über den Datenübermittlungsdienst der SAL synchronisieren, hier über die Schnittstelle *4* in Bild 4-22.

Dieser Datenübermittlungsdienst muß durch die Sicherheitsadaptionsschicht auf Transportmechanismen vorhandener Übermittlungsdienste (z. B. Dienste von Zeichengabesystemen) abgebildet werden. Maximale Nachrichtenlängen bestehender Übermittlungsdienste können eine Segmentierung langer Sicherheitsdienstesteuernachrichten vor ihrem Übermitteln innerhalb der SAL notwendig machen.

Synchronisierung von TK- und Sicherheitsdiensten – Schaffung sicherer TK-Dienste

Die SAL muß mit einer systemweiten Sicht auf die aktiven Sicherheitsdienste ausgestattet sein, um die Synchronisierung von TK- und Sicherheitsdiensten durchzuführen. Die *Zwischenschichten* melden Zustandsänderungen über die Schnittstelle *4* direkt an die SAL-Steuerung. Die *Sicherheitsanwendungsdienste* übergeben bei Zustandsänderungen entsprechende Statusinformation über die Sicherheitsdienstesteuerung an die SAL-Steuerung (z. B. Aushandlungsergebnisse, Authentisierungsergebnisse).

Da die Sicherheitsadaptionsschicht als transparente Zwischenschicht in der Steuerungs-Ebene realisiert wird, passieren alle zwischen TK-Dienstesteuerungsprozessen ausgetauschten Steuerinformationen die SAL (über die Schnittstellen *2* und *3* in Bild 4-22). Abhängig von der Sicht auf den Zustand zugeschalteter Sicherheitsdienste entscheidet die Kopplung der SAL, ob TK-Dienstesteuernachrichten passieren dürfen oder wie sie verändert werden müssen, um den Ablauf eines Telekommunikationsdienstes dem jeweils aktuellen Zustand der Sicherheitsdienste anzupassen. Telekommunikationsdienste können durch eingefügte oder veränderte Steuernachrichten weitgehend von der Kopplung der SAL kontrolliert werden. Beispielsweise kann ein Verbindungsaufbau durch Einfügen von Disconnect-Nachrichten abgebrochen werden, falls eine begleitende Benutzer-Benutzer-Authentisierung fehlschlägt.

Zur Erhaltung der Transparenz müssen bei der Bearbeitung von Steuernachrichten innerhalb der SAL die durch Timer vorgegebenen zeitlichen Randbedingungen der jeweiligen TK-Dienstesteuerung (z. B. Rufsteuerung) berücksichtigt werden.

4.4.2.3 Verfeinerung der Struktur der Sicherheitsadaptionsschicht

Um Telekommunikations- und Sicherheitsdienste synchronisieren zu können, muß die SAL über deren Zustand informiert sein. Sicherheitsdienste melden ihre Zustandsänderungen explizit an die SAL weiter (s. o.). Den Zustand der Telekommunikationsdienste erhält die SAL durch Interpretation der Steuernachrichten, die zwischen TK-Dienstesteuerung und Übermittlungsdienst ausgetauscht werden.

Für jeden aktiven Sicherheitsdienst wird in der SAL ein Zustandsautomat eingerichtet und initialisiert (*FSM_Sicherheitsdienst)*. Dieser repräsentiert die Sicht der Sicherheitsadaptionsschicht auf den Zustand des Sicherheitsdienstes. Rückmeldungen der Sicherheitsdienste über Zustandsänderungen (z. B. Ergebnis einer Authentisierung) führen in der SAL zur Aktualisierung des jeweiligen Zustandsautomaten. Somit besitzt die SAL jederzeit eine systemweite Sicht auf die Zustände der zu synchronisierenden Sicherheitsdienste. Bild 4-23 zeigt die verfeinerte Struktur der Sicherheitsadaptionsschicht.

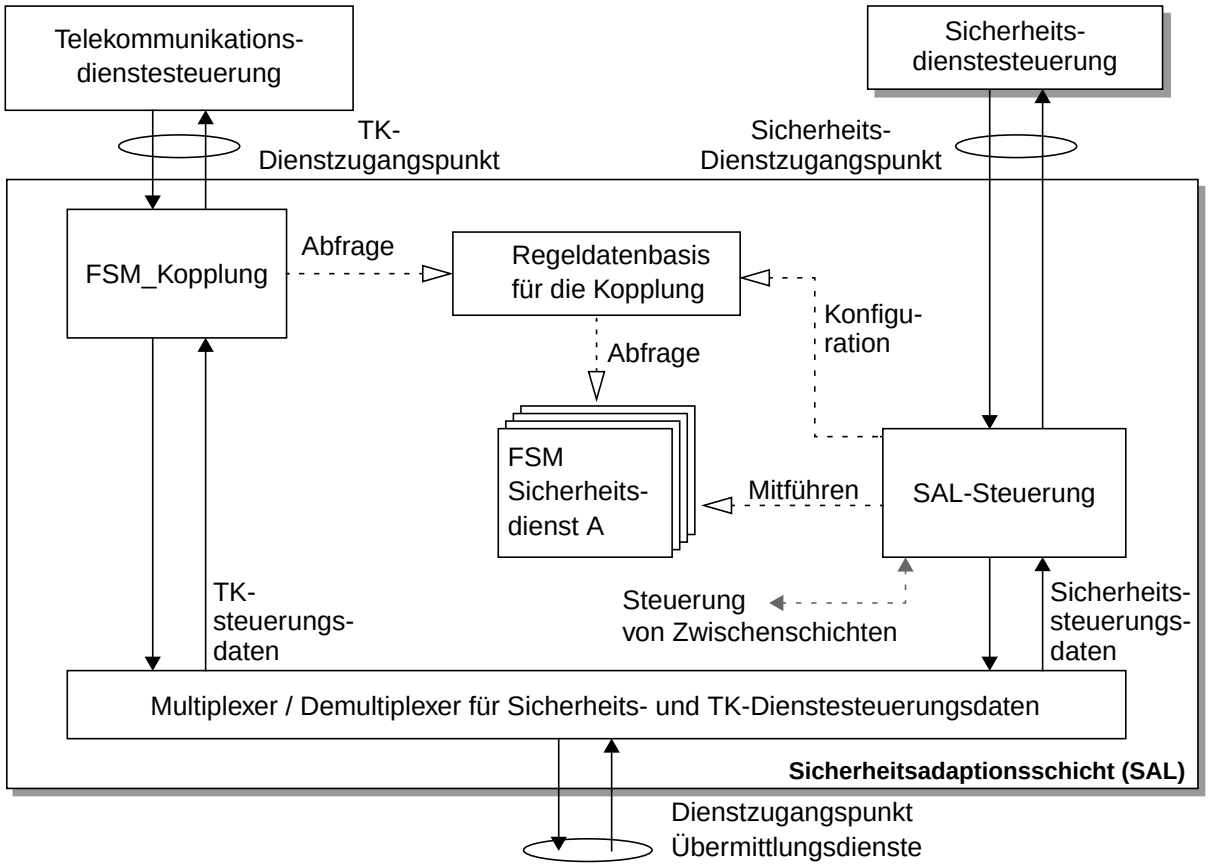


Bild 4-23: Strukturierung der Sicherheitsadaptionsschicht in der Dienstesteuerungsebene

Neben diesen passiven Zustandsautomaten für Sicherheitsdienste beinhaltet die SAL eine zentrale SAL-Steuerung, eine Regeldatenbasis zur Beschreibung der Synchronisierung von TK- und Sicherheitsdiensten, einen Automaten *FSM_Kopplung* zur Verarbeitung der durch die SAL geleiteten TK-Dienstesteuernachrichten sowie einen Multiplexer bzw. Demultiplexer.

Die zentrale *SAL-Steuerung* verarbeitet Informationen über zu aktivierende Sicherheitsdienste, die ihr von der Sicherheitsdienstesteuerung als Ergebnis der Aushandlung übergeben werden. Neben der Initialisierung und Aktivierung der entsprechenden Sicherheitsdienste leitet die

SAL-Steuerung aus den geforderten Sicherheitsdiensten die Regeln für die Regeldatenbasis ab.

Die *Regeldatenbasis* stellt eine Spezifikation der Synchronisierung von Sicherheits- und TK-Dienstesteuerungsfunktionen dar. Sie beschreibt (basierend auf den Zuständen aktiver Sicherheitsdienste) zusätzliche Bedingungen für Zustandsübergänge der TK-Dienstesteuerung.

Die Regel $\rightarrow Z \Leftarrow B$ wird folgendermaßen interpretiert: Ein Übergang in den Zustand *Z* darf nur dann durchgeführt werden, wenn die Bedingung *B* erfüllt ist. Ist diese Bedingung nicht erfüllt, so ist eine Ausnahmebehandlung einzuleiten. Dazu muß die Bedingung *B* innerhalb aller Transitionen geprüft werden, die zu *Z* führen.

Beispiel: Wird für den Übergang in den Zustand ACTIVE (Verbindung aufgebaut) die Regel $\rightarrow$*ACTIVE* $\Leftarrow$ *FSM_Auth.State == OK* in der Regeldatenbasis spezifiziert, so bedeutet dies, daß sich der Zustandsautomat für die Authentisierung im Zustand *OK* (Authentisierung erfolgreich abgeschlossen) befinden muß, wenn die TK-Dienstesteuerung in den Zustand *ACTIVE* (Verbindung aufgebaut) übergeht. Ist die Bedingung nicht erfüllt, so ist eine Ausnahmebehandlung einzuleiten (z. B. Verzögerung oder Abbruch des Dienstes). Ein ausführliches Beispiel wird im Anschluß an die Beschreibung der verfeinerten SAL besprochen.

Der Zustandsautomat *FSM_Kopplung* überwacht die Übergänge der TK-Dienstesteuerung im Hinblick auf die in der Regeldatenbasis vorgegebenen Übergangsbedingungen. Alle zwischen TK-Dienstesteuerung und Übermittlungsdienst ausgetauschten Nachrichten werden gemäß dieses Zustandsautomaten behandelt. Der Empfang einer Nachricht löst einen Zustandsübergang aus. Innerhalb des Überganges kann die Weiterleitung der Nachricht von den Bedingungen in der Regeldatenbasis abhängig gemacht werden (siehe *Abfrage* in Bild 4-23).

Nur wenn alle Bedingungen für einen Übergang erfüllt sind, wird auch die betreffende TK-Dienstesteuernachricht an das Netz beziehungsweise die TK-Dienstesteuerung weitergegeben. Ist für einen Übergang im Zustandsautomat *FSM_Kopplung* eine Regel in der Regeldatenbasis vorhanden, die nicht erfüllt ist, dann muß eine Ausnahmebehandlung entsprechend der Interpretation des jeweiligen Ereignisses vorgesehen werden. Dieses kann z. B. zu einer Verzögerung der Nachricht (z. B. beim Warten auf den Abschluß einer Authentisierung) oder zu einem Dienstabbruch und einer Anzeige an den Benutzer führen (z. B. bei nicht erfolgreicher Authentisierung).

Die Kontrolle über die TK-Dienstesteuerung erhält die Kopplung nur dann, wenn alle Dienstesteuerungsdaten (z. B. Nachrichten zum Verbindungsaufbau) den Kopplungsautomaten *FSM_Kopplung* passieren müssen. Es darf für einen TK-Dienst nicht möglich sein, die Kopplung zu umgehen.

Der *Multiplexer* hat die Aufgabe, die von den Anwendungen der Steuerungsebene erhaltenen Steuerungsdaten für Telekommunikationsdienste und Sicherheitsdienste auf bestehende Datenübermittlungsdienste der Steuerungs-Ebene abzubilden. Dabei wird entsprechend des Zieles (PzP- oder EzE-Sicherheitsdienst) auch die Adressierung der Sicherheitssteuerungsdaten implementiert. Der *Demultiplexer* muß aus empfangenen Nachrichten die Steuerungsdaten für Telekommunikationsdienste und für Sicherheitsdienste extrahieren. Steuerungsdaten für Telekommunikationsdienste dienen als Eingabe für den Zustandsautomaten *FSM_Kopplung* (vgl. Bild 4-23). Steuerungsdaten für Sicherheitsdienste werden zur Verarbeitung an die *SAL-Steuerung* weitergegeben und von dort gegebenenfalls an die *Sicherheitsdienstesteuerung* oder an Sicherheits-Zwischenschichten weitergeleitet. Multiplexer bzw. Demultiplexer sind an die vorhandenen Übermittlungsdienste der Steuerungs-Ebene anzupassen und müssen Unterschei-

dungsmerkmale zur Trennung von Telekommunikations- und Sicherheitsdienstesteuerungsdaten einfügen.

4.4.2.4 Beispiel: Kopplung von Benutzer-Authentisierung und Verbindungsaufbau im ISDN

Das zu realisierende Schutzziel laute Authentizität der Identität der Kommunikationspartner. Es betrifft ausschließlich die Dienstesteuerung und hat keinen Einfluß auf die Nutzdaten. Die Benutzer-Benutzer-Authentisierung sei innerhalb der Sicherheitsdienstesteuerung als Anwendungsdienst implementiert. Betrachtet wird die den Verbindungsaufbau initiierende Seite.

Nachdem die SAL-Steuerung den Anstoß des Telekommunikationsdienstes erkannt hat (*SetupReq*-Primitiv), fordert sie die ausgehandelten Sicherheitsdienste an. Hier fordere sie die Benutzer-Benutzer-Authentisierung bei der Sicherheitsdienstesteuerung an. Die Abarbeitung des Authentisierungsprotokolles läuft transparent für die Sicherheitsadaptionsschicht in den Sicherheitsdienstesteuerungen der beteiligten Endgeräte ab. Die SAL unterstützt lediglich die Übermittlung der Authentisierungsnachrichten (vgl. Bild 4-15). Das positive Ergebnis der Authentisierung wird der SAL-Steuerung mitgeteilt; diese aktualisiert daraufhin ihre Sicht auf den Sicherheitsdienst (*FSM_Auth.State := OK*).

Bild 4-24 zeigt die *Regeldatenbasis* und den vereinfachten Zustandsautomaten *FSM_Kopplung* zur Synchronisierung einer Benutzer-Benutzer-Authentisierung mit dem Verbindungsaufbau im ISDN. Die Rufsteuerung ist der Teil der Dienstesteuerung im ISDN, der für den Verbindungsaufbau und -abbau zuständig ist.

Der Verbindungsaufbau (vgl. Abschnitt 2.4.1, Bild 2-9) und die Prüfung der Identitäten der Gesprächspartner (Authentisierung) werden so mit der auf das Notwendigste beschränkten Verzahnung realisiert. Die Regeldatenbasis wurde durch die SAL-Steuerung so konfiguriert, daß der Verbindungsaufbau nur dann vervollständigt wird (vgl. Bild 4-24, Übergang in den Zustand *ACTIVE*), wenn die Identitäten der Kommunikationspartner nachgewiesen sind. Dies ist aus Sicht der Sicherheitsadaptionsschicht nach einer positiven Rückmeldung über den Authentisierungsverlauf durch die Sicherheitsdienstesteuerung der Fall.

Das Bild zeigt auf der linken Seite den Zustandsautomaten, der die Nachrichten verarbeitet, die zwischen der Q.931-Instanz und der Rufsteuerung des Endgerätes ausgetauscht werden. Der nicht unterlegte Teil des in der Spezifikationssprache SDL beschriebenen Prozesses stellt das transparente Durchreichen der Nachrichten dar. Der unterlegte Teil sorgt für die Kopplung mit parallel ablaufenden Sicherheitsdiensten. Für den überwachten Übergang lassen sich drei Fälle unterscheiden:

- Sofern die vereinbarten Sicherheitsdienste beim Empfang des *SetupConf*-Primitivs (d. h. beim Übergang in den Zustand *ACTIVE*) erfolgreich abgearbeitet bzw. aktiviert sind, verhält sich der Kopplungsautomat völlig transparent (d. h. *FSM_Auth.Stat==OK*).

- Sind die vereinbarten Sicherheitsdienste noch nicht abgeschlossen (z. B. Authentisierung) bzw. noch nicht aktiv oder synchronisiert (z. B. Zwischenschichten zur Verschlüsselung), so wird der Telekommunikationsdienst verzögert. Dies entspricht den Bedingungen *FSM_Auth.Stat<>OK* und *FSM_Auth.Stat<>NOK* in Bild 4-24. Dabei sind zeitliche Randbedingungen von Zeitüberwachungsmaßnahmen der Rufsteuerung und der Q.931-Instanz zu beachten.

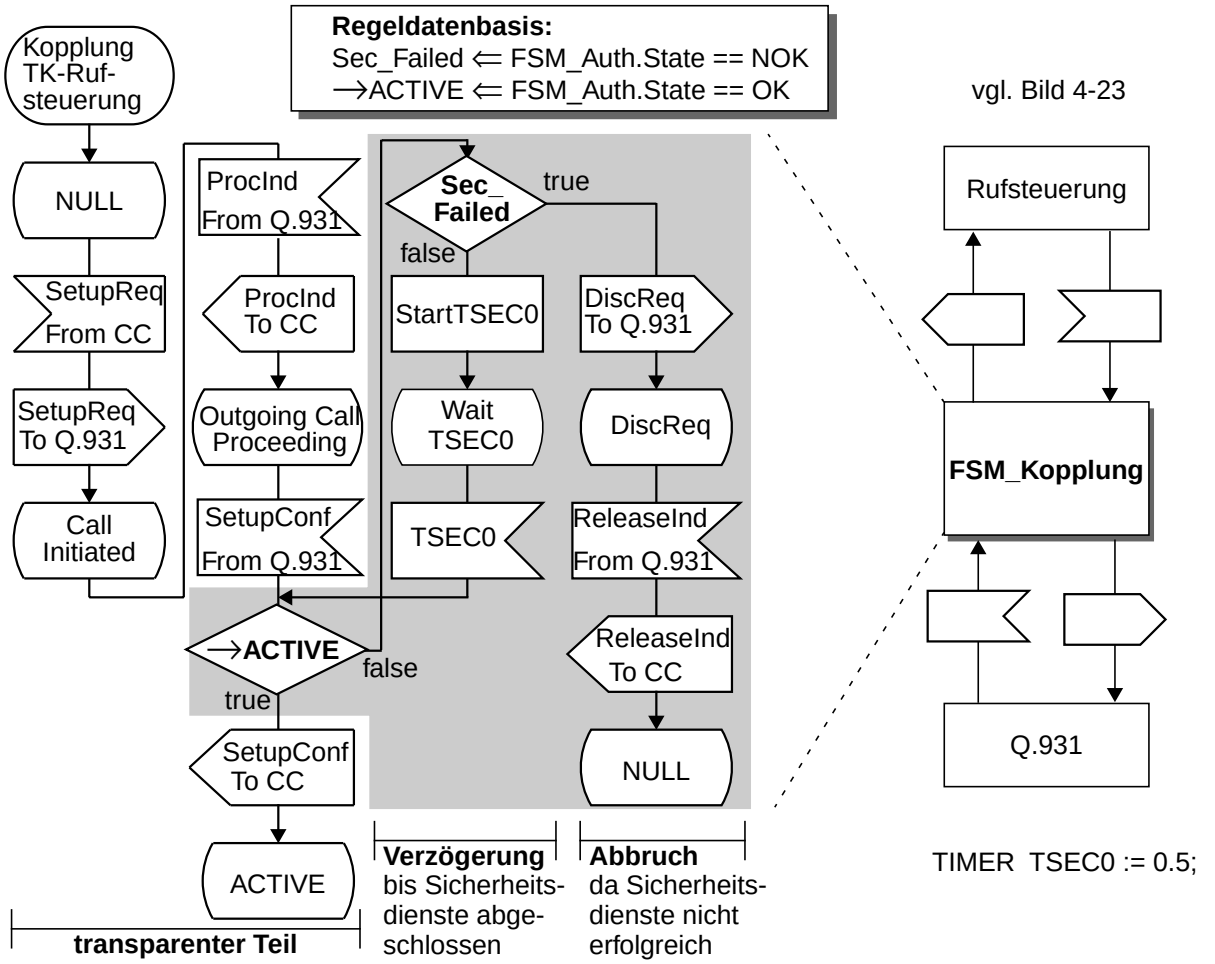


Bild 4-24: Kopplung von Authentisierung und Verbindungsaufbau im ISDN

- Können die vereinbarten Sicherheitsdienste nicht erfolgreich abgeschlossen oder aktiviert werden (vgl. Bedingung *FSM_Auth.Stat==NOK* in Bild 4-24), so wird der Telekommunikationsdienst abgebrochen. Dies kann der Sicherheitsdienstesteuerung über den Sicherheitsdienstzugangspunkt und von dort dem Benutzer angezeigt werden (vgl. Bild 4-23).

Die dargestellte Regeldatenbasis spezifiziert 2 Regeln für die Fälle →*ACTIVE* und *Sec_Failed*. Die Vervollständigung des Verbindungsaufbaus durch Übergang in den Zustand *ACTIVE* wird nur dann erlaubt, wenn die zugehörige Authentisierung erfolgreich abgeschlossen wurde (Verzweigung im SDL-Prozeßdiagramm). Wird eine Übergangsbedingung nicht erfüllt, so wird eine entsprechende Ausnahmebehandlung durch den Kopplungsautomaten eingeleitet. Diese entspricht dem Warten auf den Abschluß der Authentisierung (Verzögerungsteil in Bild 4-24; *TSEC0* kann z. B. 0,5s Laufzeit besitzen) bzw. dem Abbruch der Diensterbringung (Abbruch-Teil in Bild 4-24). In ähnlicher Weise können auch Funktionen zur Verschlüsselung oder zum Integritätsschutz beim Verbindungsaufbau initialisiert und aktiviert werden. Die Synchronisierung mit den Sicherheitsdiensten kann je nach Telekommunikationsdienst an anderer Stelle im Automaten *FSM_Kopplung* der Sicherheitsadaptionsschicht durchgeführt werden.

Beispielsweise könnte verlangt werden, daß vor dem Beginn des Verbindungsaufbaus (Durchreichen der *SetupReq*-Meldung) die Authentisierung erfolgreich abgeschlossen ist (Regel: →*Call_Initiated* ⇐ *FSM_Auth.State == OK*) und vor Weiterleiten der *SetupCnf*-Meldung die Sicherheitsdienste für Nutzdaten aktiv sind (Regel: →*ACTIVE* ⇐ *FSM_UserSec.State ==*

ACTIVE). Diese Art der Kopplung über spezialisierte Zustandsautomaten ermöglicht sowohl eine effektive als auch flexible Zuschaltung von Sicherheitsdiensten bei Bedarf. Nicht aktivierte Sicherheitsdienste werden in den Regeln nicht verwendet. Ein generischer Kopplungsautomat könnte beispielsweise die Regeldatenbasis bei jedem Übergang prüfen. Die Adaptionsschicht muß für jeden anzureichernden Telekommunikationsdienst einen entsprechenden Kopplungsautomaten *FSM_Kopplung* führen.

Durch diese Vorgehensweise werden funktionale Abhängigkeiten zwischen herkömmlichen Kommunikationsdienstefunktionen und Sicherheitsdienstefunktionen minimiert und in der Sicherheitsadaptionsschicht zusammengefaßt. Der hier verfolgte Weg zur Kopplung von sicherheitsrelevanten und existierenden Dienstefunktionen ermöglicht eine hohe Flexibilität beim Einsatz von Sicherheitsdiensten und Sicherheitsmechanismen und begünstigt die Kompatibilität von unterschiedlich erweiterten Endgeräten. Gleichzeitig wird für sicherheitsunkritische Dienste die Kompatibilität mit herkömmlicher Kommunikationsinfrastruktur garantiert.

4.5 Zusammenfassung

Der in diesem Abschnitt beschriebene additive Ansatz zielt auf eine Erweiterung bestehender Kommunikationssysteme um Sicherheitsfunktionen ab. Dabei wird die Kompatibilität und Interoperabilität von erweiterten und herkömmlichen Kommunikationssystemen erhalten.

Die hinzugefügten Sicherheitsfunktionen und ihre Plazierung entscheiden über den durch sie erreichbaren Schutz. Weiterhin fügen Sicherheitsfunktionen zusätzliche Verzögerungen (Delay) und möglicherweise Verzögerungsschwankungen (Jitter) ein. Ihre Synchronisation erfordert zusätzlichen Aufwand für den Datenaustausch. Deshalb unterstützt die hier vorgeschlagene Sicherheitsarchitektur eine flexible Verknüpfung bestehender Telekommunikationsdienste und neu hinzugefügter Sicherheitsdienste.

Die Sicherheitsanwendungen werden als *Security Supplementary Services* bezeichnet. Dies spiegelt wider, daß diese Sicherheitsdienste optional und zusätzlich zum Grunddienst geschaltet werden können und im Teledienst-Bereich angesiedelt sind. Die Sicherheitsdienste, die durch Zwischenschichten realisiert werden, sind hingegen eher im Bereich der Übermittlungsdienste angesiedelt, die durch sie erweitert werden. Sie werden deshalb auch als *Security Bearer Services* bezeichnet.

Die *Sicherheitsdienstesteuerung* bildet das Bindeglied zwischen Benutzer und Sicherheitsadaptionsschicht. Über sie können Benutzer die zuzuschaltenden Sicherheitsdienste in der SAL aktivieren. Darüberhinaus verwaltet sie Sicherheitsanwendungen, die bestehenden Telekommunikationsdiensten bei Bedarf zugeschaltet werden können.

Eine *Sicherheitsadaptionsschicht* (Security Adaptation Layer, SAL) koordiniert sowohl diese Kopplung, als auch den Datenaustausch zwischen Sicherheitskomponenten innerhalb eines Kommunikationssystems (Komponenten-Steuerung). Zusätzlich stellt die Sicherheitsadaptionsschicht einen Datenübermittlungsdienst bereit, über den sich kooperierende Sicherheitsfunktionen zur Realisierung von Sicherheitsdiensten durch den Austausch von Sicherheitssteuerungsdaten synchronisieren können. Diese Funktionen der SAL werden durch einen neuen Sicherheitsdienstzugangspunkt angesprochen.

Die Sicherheitsadaptionsschicht stellt folglich den Teil der Sicherheitsarchitektur dar, der vom zugrundeliegenden Kommunikationssystem und den TK-Diensten abhängig ist. Sie muß die spezifische TK-Dienstesteuerung kontrollieren und mit dem Zustand von zugeschalteten Sicherheitsdiensten synchronisieren. Die Implementierung der Sicherheitsadaptionsschicht für

das ISDN und Beispiele für die Nutzung der Sicherheitsarchitektur werden im nächsten Kapitel erläutert.

Kapitel 5

Architektur für benutzerkontrollierbare, sichere Dienste im ISDN

Die in Kapitel 4 vorgestellte Sicherheitsarchitektur für Kommunikationssysteme wird nun in die Protokollarchitektur des diensteintegrierenden Digitalnetzes ISDN integriert. Abschnitt 5.1 führt zunächst in die Grundidee offener, universeller Sicherheitsdienste ein. Danach werden in Abschnitt 5.2 die Komponenten der Sicherheitsarchitektur und dadurch unterstützte Sicherheitsdienste in die Protokollarchitektur an der Benutzer-Netzschnittstelle (DSS1) eingeordnet.

Die Auslagerung von Sicherheitsfunktionen wird in Abschnitt 5.3 behandelt. Zunächst werden Zusatzgeräte im Teilnehmerbereich diskutiert. Anschließend wird die Einbeziehung von Sicherheitsfunktionen in zentralen Servern im Netz skizziert. Dazu wird die Sicherheitsarchitektur auf die Protokollarchitektur im Zwischenamtsbereich abgebildet.

Schließlich grenzt Abschnitt 5.4 die hier vorliegende Arbeit von bereits existierenden Ansätzen für Sicherheitsdienste im ISDN ab.

5.1 Universelle offene Sicherheitsdienste

Der hier verfolgte additive Ansatz zielt auf eine weitgehend unabhängige Realisierung von Telekommunikations- und Sicherheitsdiensten ab und ermöglicht so einheitliche Sicherheitsdienstschnittstellen für unterschiedliche Telekommunikationsnetze (z. B. N/B-ISDN, Internet, GSM). Davon profitieren vor allem die von der Netztechnik unabhängigen Sicherheitsanwendungen (Aushandlung, Authentisierung, Schlüsselvereinbarung, Schlüsselverwaltung etc.), d. h. die *Security Supplementary Services*. Diese werden durch die Sicherheitsdienstesteuerung verwaltet und finden einen einheitlichen Dienstzugangspunkt zur Aktivierung oder Synchronisierung von Sicherheitsdiensten in erweiterten Endgeräten und Netzknoten vor.

Bild 5-1 veranschaulicht die Grundidee universeller Sicherheitsdienste. Die über Kommunikationsnetze verbundenen Kommunikationssysteme (Endgeräte, Netzknoten, Server, Zusatzgeräte) sollen – unabhängig vom jeweils genutzten Kommunikationsnetz – in der Lage sein, an Sicherheitsdiensten zu partizipieren. Im folgenden werden vor allem Sicherheitsdienste im ISDN betrachtet (in Bild 5-1 hervorgehoben).

Im Bild sind Sicherheitsfunktionen in Endgeräten und zentralen Servern und auch in Teilnehmervermittlungsstellen vorgesehen, die im Zusammenspiel Sicherheitsdienste erbringen können. Unabhängig davon werden auf einer anderen logischen Ebene die Telekommunikationsdienste erbracht. Die Kopplung von Sicherheits- und TK-Dienst erfolgt benutzerkontrolliert

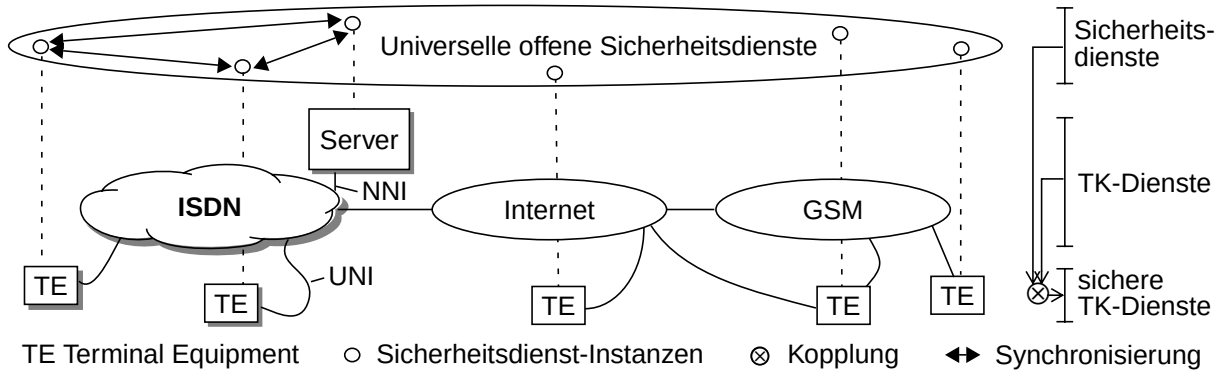


Bild 5-1: Universelle Sicherheitsdienste

innerhalb der Endgeräte. Die jeweilige Plazierung der Sicherheitsfunktionen richtet sich nach dem jeweiligen Schutzziel und dem Angreifermodell (vgl. Abschnitt 4.2) und umgekehrt.

Sicherheitsfunktionen partizipierender Kommunikationssysteme müssen (i) von anderen Sicherheitsfunktionen adressiert werden können bzw. andere Sicherheitsfunktionen adressieren können und (ii) Steuerinformation zur Synchronisierung mit kooperierenden Sicherheitsfunktionen in anderen Kommunikationssystemen austauschen können. Bild 5-2 zeigt das Vorgehen zur Übermittlung von Steuerinformationen zwischen Sicherheitsfunktionen.

Informationen zur Synchronisierung von Sicherheitsfunktionen müssen vor ihrer Übermittlung beim Sender kodiert und beim Empfänger dekodiert werden (vgl. ① in Bild 5-2). Die Vorschriften dazu können z. B. im Rahmen der Aushandlung einer Sicherheitsassoziation festgelegt werden und sich auf gängige Standards stützen. In der ITU-Empfehlung X.509 [116] oder der amerikanischen Empfehlung NIST-SP 800-15 [126] sind beispielsweise Kodierungsvorschriften für Schlüsselzertifikate enthalten. Der zweite Schritt umfaßt die Übermittlung der Sicherheitssteuerungsdaten (kodierte Sicherheitssteuerungsinformationen). Diese sollen auf im ISDN verfügbare Übermittlungsdienste abgebildet werden[1]. Dazu muß der Empfänger adressiert werden können und die Sicherheitssteuerungsdaten müssen in das durch den Übermittlungsdienst geforderte Format gebracht werden (z. B. Länge).

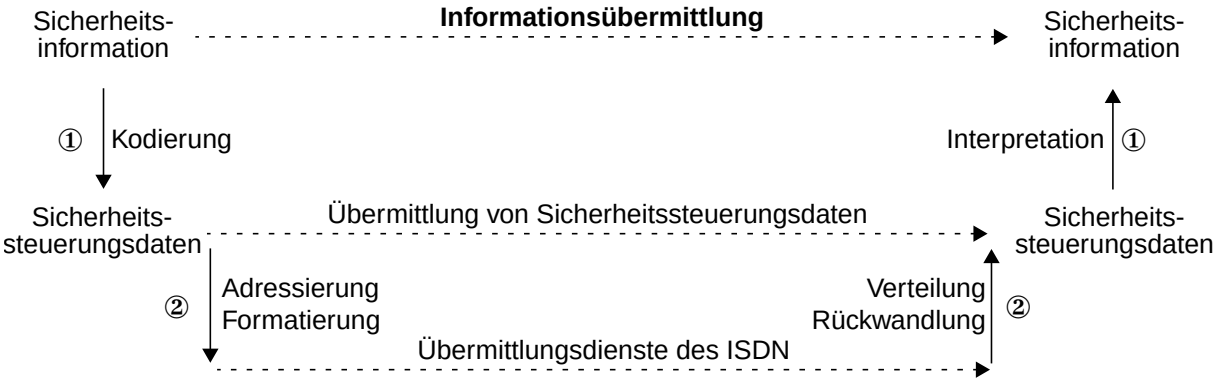


Bild 5-2: Übermittlung von Sicherheitssteuerungsinformation

1 Sofern die kommunizierenden Systeme auch andere Datenübermittlungsdienste unterstützen (z. B. TCP/IP, GSM), so können alternativ auch diese zum Austausch von Sicherheitssteuerungsdaten genutzt werden.

Beim Zugang zu diesen Übermittlungsdiensten interagieren Sicherheitsfunktionen (Sender oder Empfänger) und herkömmliche Telekommunikationsfunktionen. Deshalb wird diese Schnittstelle innerhalb der Sicherheitsadaptionsschicht (vgl. ② Bild 4-22) implementiert. Die tatsächliche Übermittlung der Sicherheitssteuerungsdaten durch ISDN-Dienste liegt nicht mehr im Verantwortungsbereich der Sicherheitsarchitektur (sofern die Verfügbarkeit gewährleistet ist), da hier ausschließlich TK-Funktionen interagieren.

Nachfolgend wird zunächst die Sicherheitsarchitektur am Teilnehmeranschluß im ISDN (DSS1) implementiert. Anschließend wird skizziert, wie auch zentrale Server im Netz über die netzinternen Zeichengabeprotokolle an Sicherheitsdiensten partizipieren können.

5.2 Sicherheitsarchitektur am ISDN-Teilnehmeranschluß

5.2.1 Zielsetzung

Endgeräte sollen durch die Erweiterung um die Sicherheitsarchitektur den Betrieb von Sicherheitsdiensten im ISDN ermöglichen. Bild 5-3 zeigt die Phasen eines verbindungsorientierten ISDN-Dienstes (z. B. File-Transfer, Sprachdienst). Vertikal sind die Signalisiervorgänge für ISDN- (nach oben) und Sicherheitsdienste (nach unten) aufgetragen. In horizontaler Richtung ist die Zeitachse gezeichnet, auf der die Phasen verbindungsloser Zustand, Verbindungsaufbau, Datenaustausch und Verbindungsabbau unterschieden werden.

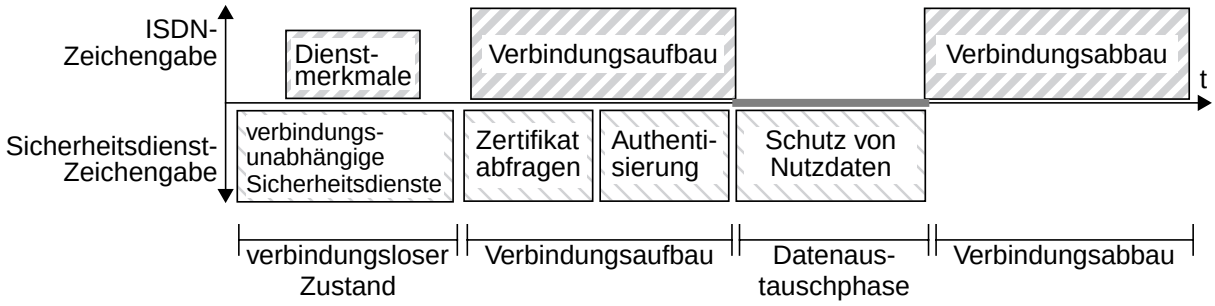


Bild 5-3: Ende-zu-Ende-Sicherheitsdienste zwischen ISDN-Endgeräten

Die Kopplung der Sicherheitsarchitektur soll die optionale Zuschaltung von Sicherheitsdiensten zu ISDN-Diensten ermöglichen. Beispielsweise sollen eine Authentisierung mit dem Verbindungsauf- und Abbau oder der Schutz von Nutzdaten mit dem Datenaustausch verknüpft werden. Dabei darf aus Gründen der Kompatibilität die Zeichengabeschnittstelle an der Benutzer-Netzschnittstelle des ISDN nicht verändert werden. Erweiterte ISDN-Endgeräte sollen weiterhin mit herkömmlichen ISDN-Endgeräten zusammenarbeiten und am selben Anschluß parallel betrieben werden können. Die Verknüpfung von ISDN- und Sicherheitsdiensten soll innerhalb von (bezüglich der Betroffenen) vertrauenswürdigen Bereichen stattfinden[2].

Die Kopplung von Sicherheits- und ISDN-Diensten wird hier für ISDN-Endgeräte besprochen. Innerhalb von Teilnehmervermittlungsstellen sind bereits Überwachungs- und Kontrollmechanismen vorhanden. Dort könnte z. B. die Identifizierung eines Teilnehmers (bisher: Anschlußlage, auf der ein Verbindungswunsch ankommt) durch eine Authentisierung ersetzt werden. Dies ermöglicht Teilnehmermobilität und die Prüfung anschlußunabhängiger Identitäten.

2 Bezüglich der Teilnehmer bieten sich besonders ISDN-Endgeräte oder zentrale, vertrauenswürdige Server im Netz an. Für den Netzbetreiber bieten sich Teilnehmervermittlungsstellen oder zentrale Server im Netz an.

5.2.2 Integration der Sicherheitsarchitektur in die Protokollarchitektur

Die Realisierung der Sicherheitsarchitektur für Endgeräte und Teilnehmervermittlungsstellen unterscheidet sich von der Realisierung für zentrale Server im Netz. Bei erweiterten Endgeräten und Teilnehmervermittlungsstellen spielt die Kompatibilität zu bestehender ISDN-Infrastruktur eine wesentliche Rolle. Diese Kompatibilität wird durch den additiven Ansatz der hier vorgestellten Sicherheitsarchitektur gefördert.

5.2.2.1 Spezifikation der Schnittstellen der Sicherheitsarchitektur

Die ISDN-Protokollarchitektur in Endgeräten (vgl. Bild 2-7) wird um die Sicherheitsadaptionsschicht und die Sicherheitsdienstesteuerung ergänzt. Es werden die Schnittstellen der Sicherheitsadaptionsschicht auf bestehende Schnittstellen innerhalb von ISDN-Endgeräten abgebildet. Bild 5-4 zeigt die Komponenten SSS und SAL und ihre Schnittstellen im ISDN.

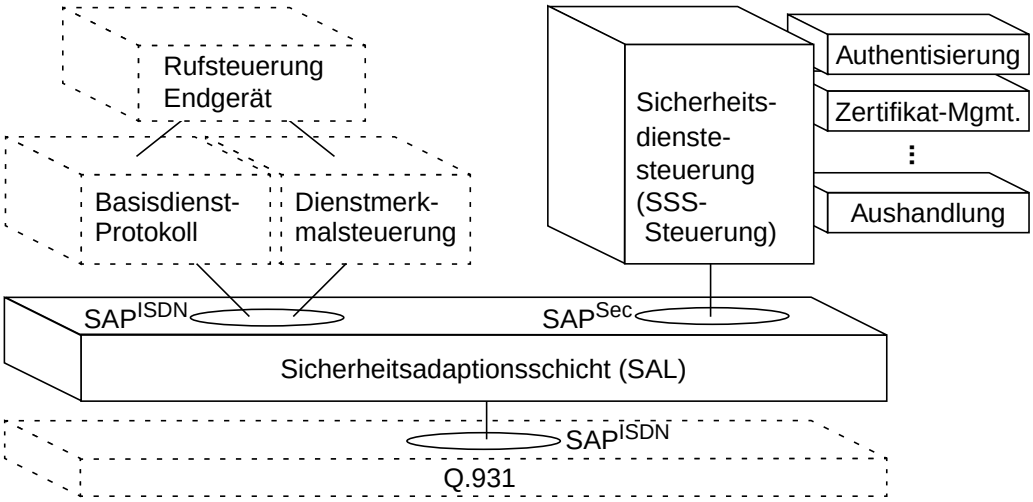


Bild 5-4: Sicherheitsarchitektur für ISDN-Endgeräte

Der Dienstzugangspunkt für ISDN-Dienste (SAP^{ISDN}) ist standardisiert [109]. Die *Sicherheitsadaptionsschicht* trennt die TK-Dienstesteuerung vom Netz und ist so in der Lage, die Steuerung von ISDN-Diensten mit Hilfe des Zugriffs auf ihre Steuernachrichten zu kontrollieren. Der Dienstzugangspunkt wird dabei nicht verändert, so daß die Kompatibilität gegenüber dem Netz und gegenüber herkömmlichen Endgeräten (bei abgeschalteten Sicherheitsdiensten) gewährleistet ist. Die Realisierung dieses Teils der SAL wurde bereits in Abschnitt 4.4.2.4 für die Rufsteuerung im ISDN veranschaulicht. Es verbleibt, den neuen Dienstzugangspunkt für Sicherheitsdienste (SAP^{Sec}) zu definieren und die darüber angebotenen Dienste auf die vorhandenen Dienste im ISDN (hier: SAP^{ISDN}) und die innerhalb der SAL erbrachten Dienste abzubilden. Über den Dienstzugangspunkt SAP^{Sec} (vgl. 5-5) werden folgende Aufgaben abgewikkelt:

- *Lokale Synchronisierung* zwischen der Sicherheitsadaptionsschicht und der Sicherheitsdienstesteuerung: Durch das *SAL_Activate*-Primitiv teilt die Sicherheitsdienstesteuerung der SAL-Steuerung mit, welche Sicherheitsdienste mit welchem ISDN-Dienst (und auf welche Art) zu koppeln sind. Die SAL fordert die entsprechenden Sicherheitsanwendungen dann bei Bedarf bei der SSS-Steuerung an (*SSS_Req*). Die Sicherheitsdienstesteuerung unterrichtet die Sicherheitsadaptionsschicht über das Ergebnis der Durchführung von Sicherheitsdiensten (*SSS_Cnf*, *SSS_Rej*). Mit dem *SAL_Notify*-Primitiv unterrichtet die

SAL die Sicherheitsdienstesteuerung über wichtige Vorgänge im ISDN (z. B. Ende eines erweiterten ISDN-Dienstes) zur Synchronisierung mit den Security Supplementary Services.

- Die Sicherheitsanwendungen bzw. die SSS-Steuerungen unterschiedlicher Endgeräte greifen zum Nachrichtenaustausch auf einen *Datenübermittlungsdienst* der Kopplung zurück (*SAL_DataReq*, *SAL_DataInd*). Die Abbildung dieses Übermittlungsdienstes auf die der Sicherheitsadaptionsschicht zur Verfügung stehenden ISDN-Dienste (SAP^{ISDN}) stellt eine wesentliche Herausforderung für die Integration aus der Sicht offener Systeme dar.

Zwischen Sicherheitsdienstesteuerung und SAL besteht keine hierarchische Schichten-Schnittstelle. Beide Komponenten nutzen Dienste der anderen. Bild 5-5 zeigt ausschnittsweise die Dienstschnittstellen der Sicherheitsarchitektur.

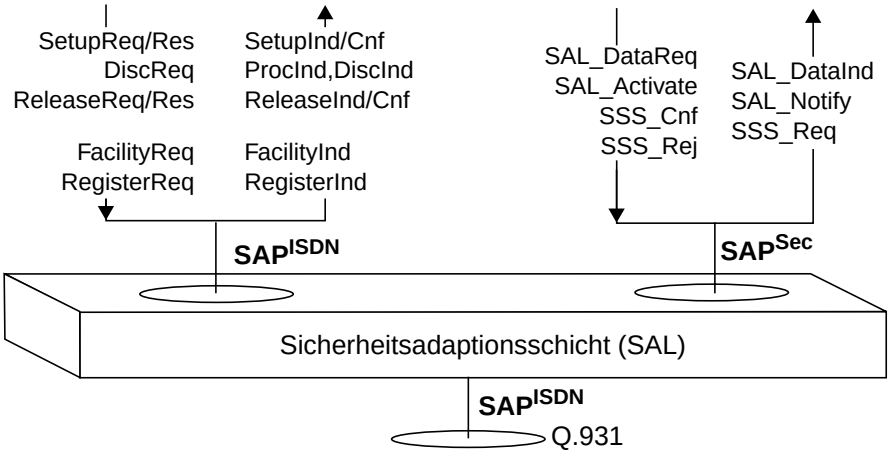


Bild 5-5: Dienstschnittstellen der Sicherheitsarchitektur

Über die im Bild gezeichneten Schnittstellen treten die für Sicherheitsaspekte wesentlichen Komponenten (Sicherheits-, TK-Dienste) eines erweiterten Kommunikationssystems in Beziehung zueinander. Die *Sicherheitsdienstesteuerung* ist durch die Trennung der Schnittstellen SAP^{ISDN} und SAP^{Sec} unabhängig vom zugrundeliegenden Kommunikationsnetz. Die Anpassung an die jeweilige Telekommunikationsumgebung (ISDN, etc.) wird ausschließlich durch die Sicherheitsadaptionsschicht realisiert.

5.2.2.2 Übermittlungsdienste der Sicherheitsadaptionsschicht

Die Abbildung der Übermittlungsdienste auf den ISDN-Dienstzugangspunkt ist dem Multiplexer/Demultiplexer innerhalb der Sicherheitsadaptionsschicht zuzuordnen (vgl. Bild 4-23). Das ISDN bietet der ISDN-Dienstesteuerung und zusätzlichen ISDN-Dienstmerkmalen [47] folgende Übermittlungsdienste an, die auch zur Übermittlung von Sicherheitssteuerungsdaten genutzt werden können:

- *User-to-User-Zeichengabe* zwischen Endgeräten [113]: Die User-to-User-Zeichengabe ermöglicht den Austausch von Steuerinformation zwischen Endgeräten transparent für das Netz. In dieser Arbeit wird der UUS-Service-1 genutzt, der die Integration von Benutzer-zu-Benutzer-Daten in Form von *UUS-Informationselementen* in die Q.931-Nachrichten zur Rufsteuerung ermöglicht (*Setup, Alert, Connect, Disconnect*). Diese *UUS*-Informationselemente werden als Bestandteil der Rufsteuernachrichten transparent durch das Netz

zum gerufenen Endgerät weitergeleitet. Die Adressierung erfolgt implizit anhand der Zeichengabe-Assoziation des Rufes.

- *Dienstmerkmal-Zeichengabe* zwischen Endgerät und Teilnehmervermittlungsstelle [111], [112]: In dieser Arbeit wird das in Abschnitt 2.4.1 beschriebene *Funktionale Protokoll* verwendet. Mit den zugehörigen Nachrichten (*Register, Facility*) können sich kooperierende Sicherheitsfunktionen in Endgerät und Teilnehmervermittlungsstelle synchronisieren.

Weitere Übermittlungsdienste an der Q.931-Schnittstelle, wie z. B. Datendienste über den ISDN-D-Kanal, oder zusätzliche Netzzugänge (z. B. GSM oder Internet) können ebenfalls zur Übermittlung von Sicherheitssteuerungsdaten genutzt werden.

Übermittlungsdienst für EzE-Sicherheitsdienste

Zur Unterstützung von Ende-zu-Ende-Sicherheitsdiensten wird in dieser Arbeit die User-to-User-Zeichengabe verwendet. Da Sicherheitsdienste i. a. unabhängig von einem ISDN-Verbindungsaufbau realisierbar sein sollen (z. B. Abholung von Zertifikaten), wird die Übermittlung von Sicherheitssteuerungsdaten (*SecPDU*) – wie in Bild 5-6 dargestellt – unabhängig von anderen ISDN-Diensten durch User-to-User-Zeichengabe realisiert. Der Übermittlungsdienst wird von den Security Supplementary Services durch das Primitiv *SAL_DataReq* angefordert. Dem Primitiv werden sowohl die Adresse *EzE* (Ende-zu-Ende-Sicherheitsdienst), als auch die Sicherheitssteuerungsdaten (*SecPDU*) mitgegeben. Beim Empfänger werden die Sicherheitssteuerungsdaten durch das Primitiv *SAL_DataInd* angezeigt.

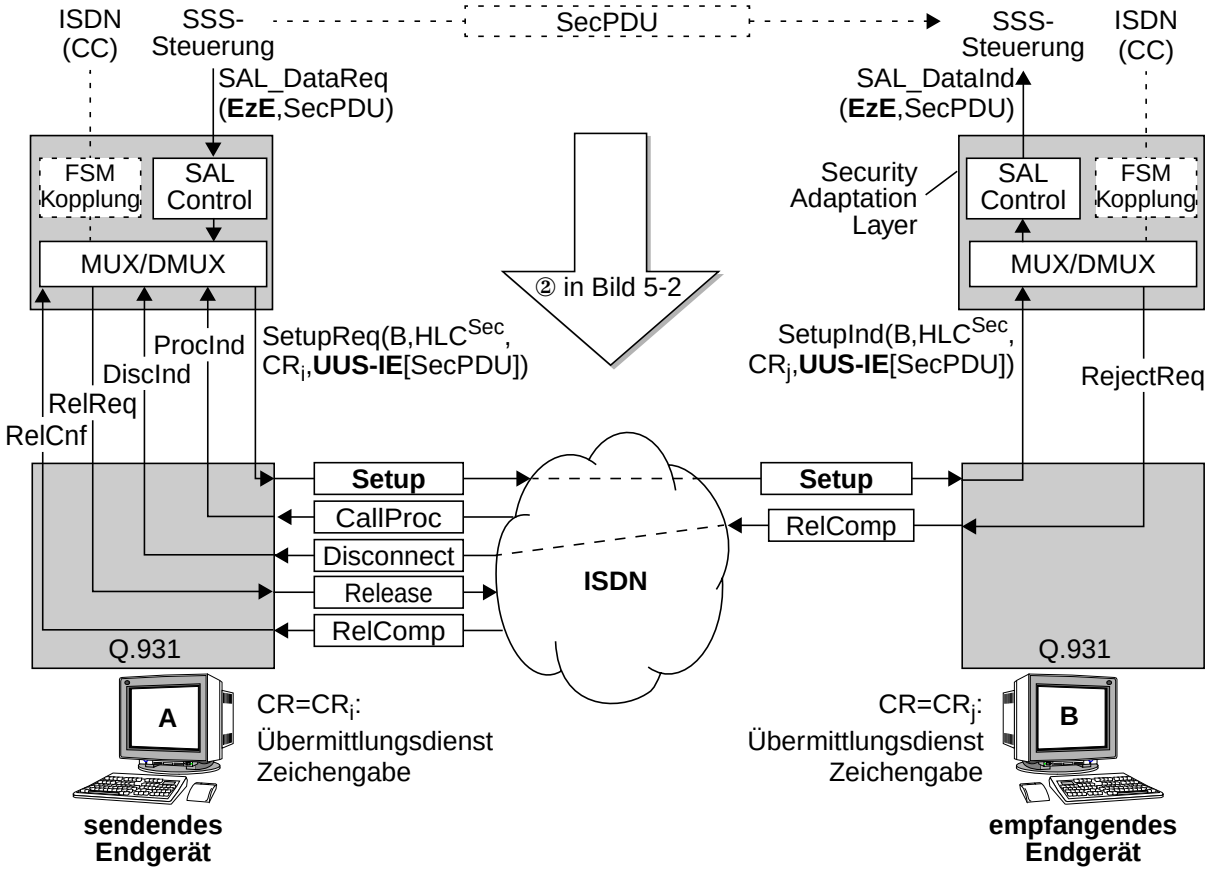


Bild 5-6: Austausch von Steuerinformation für Ende-zu-Ende-Sicherheitsdienste

Zur Übermittlung von Sicherheitssteuerungsdaten von Endgerät A zu Endgerät B wird ein Verbindungswunsch von A nach B übermittelt und vom Ziel abgelehnt. In der *Setup*-Nachricht wird die Sicherheitssteuerinformation in Form eines *UUS-Informationselementes* beigefügt. Die Kopplung des sendenden Endgerätes muß dazu die Rufnummer kennen, zu der die Sicherheitssteuerungsdaten übermittelt werden sollen. Die SAL des empfangenden Endgerätes muß diese *Setup*-Nachricht filtern, das *UUS*-Informationselement extrahieren und die darin enthaltene *SecPDU* an die Sicherheitsdienstesteuerung weiterleiten. Um den Transfer abzuschließen, sendet die empfangende SAL eine *ReleaseComplete*-Nachricht zurück, um die Protokollautomaten der Zwischensysteme (Vermittlungsstellen) wieder zurückzusetzen. Endgerät *B* kann gegebenenfalls eine Bestätigung für die erhaltene *SecPDU* (z. B. deren Hashwert) der *RelComp*-Nachricht als *UUS*-Informationselement beifügen. Dieses UUS-IE wird dem Endgerät A in der *Disconnect*-Nachricht angezeigt. Damit ist ein bestätigter Übermittlungsdienst realisierbar (vgl. Protokollierung dieses Szenarios in Anhang A.6). Diese Art der Übermittlung von *SecPDUs* ist mit erheblichem Steueraufwand innerhalb des Netzes verknüpft. In Abschnitt 5.2.5.3 wird deshalb auf einen verbindungsunabhängigen Übermittlungsdienst für User-to-User-Daten näher eingegangen.

UUS-Informationselemente besitzen eine vom jeweiligen Netz abhängige maximale Länge (meist < 133 Oktetts). Zusätzlich sind sie durch die maximale Länge eines Schicht 2-Rahmens (Q.921, N.201 = 260 Oktetts [107]) begrenzt. Deshalb müssen Sicherheitssteuerungsdaten vom Sender gegebenenfalls segmentiert und beim Empfänger reassembliert werden. Dies kann an unterschiedlichen Stellen realisiert werden:

- *Segmentierung am unteren Rand der Schicht 3*: Nach Q.931 Anhang H [110] wird die *Setup*-Nachricht in diesem Fall mit Hilfe mehrerer (max. 8) *Segment*-Nachrichten übertragen. Der weitere Ablauf des Szenarios bleibt gleich.

- *Segmentierung innerhalb der Sicherheitsadaptionsschicht*: Eine Segmentierung ist hier ungleich aufwendiger, da für jedes Segment einer *SecPDU* das in Bild 5-6 gezeigte Szenario ablaufen würde. Bei Segmentierung von *SecPDUs* sollten auch weitere Verbindungssteuerungsnachrichten (z. B. *Alerting*, *Disconnect*) und zusätzliche Nachrichten (z. B. *Information*-Nachrichten anderer UUS-Dienste [113]) zur Übertragung von *UUS*-Informationselementen genutzt werden, um den zusätzlichen Aufwand in Relation zu den übertragenen Sicherheitssteuerungsdaten zu reduzieren.

- *Segmentierung innerhalb der Sicherheitsdienstesteuerung:* Dieses ist abzulehnen, da Segmentierung bzw. Reassemblierung vom zugrundeliegenden Netz abhängig sind. Die Anwendungskomponenten sollen netzunabhängig bleiben.

Sind die Endgeräte über eine Punkt-zu-Punkt-Verbindung an das ISDN angeschlossen, so führt die Ablehnung der Rufannahme durch die *RelComp*-Nachricht in Bild 5-6 sofort zum Abbau der Verbindung bis zum rufenden (sendenden) Teilnehmer. Sonst wird in der gerufenen Vermittlungsstelle gewartet (hier: Timer T303 = 4 Sekunden [109]), ob andere Endgeräte den Ruf annehmen.

Übermittlungsdienst für UNI-Sicherheitsdienste

Zur Unterstützung von Sicherheitsdiensten zwischen Endgeräten und Teilnehmervermittlungsstellen (UNI) müssen neue zusätzliche Dienstmerkmale vereinbart und implementiert werden. Die ITU-Empfehlung Q.932 benennt das *Funktionale Protokoll* für Dienstmerkmale als das Protokoll, welches für die Definition und einfache Integration neuer Dienstmerkmale gedacht

ist. Die zugehörigen Prozeduren sind unabhängig von der Art des ISDN-Zugangs (Basic Rate / Primary Rate).

Gemäß dem funktionalen Protokoll wird eine Zeichengabe-Assoziation (adressiert durch die Call Reference) zwischen Endgerät und Vermittlungsstelle aufgebaut, über die der Datenaustausch zur Realisierung zusätzlicher Dienstmerkmale erfolgt. Die Korrelation zusammengehöriger Steuerungsdaten wird durch die Call Reference der Nachrichten hergestellt. Eine solche Call Reference CR_i zwischen Endgerät und Teilnehmervermittlungsstelle wird mit Hilfe der *Register*-Nachricht etabliert. Anschließend können alle *SecPDUs* (kodiert in *Facility*-Informationselementen, *FAC-IE*) in *Facility*-Nachrichten ausgetauscht werden; dabei ist die ausgehandelte Call Reference CR_i zu verwenden. Diese Zeichengabe-Assoziation kann über längere Zeit genutzt werden. Der Abbau des logischen Kanals (d. h. die Freigabe der CR) erfolgt durch das Senden der *RelComp*-Nachricht (vgl. Bild 5-7).

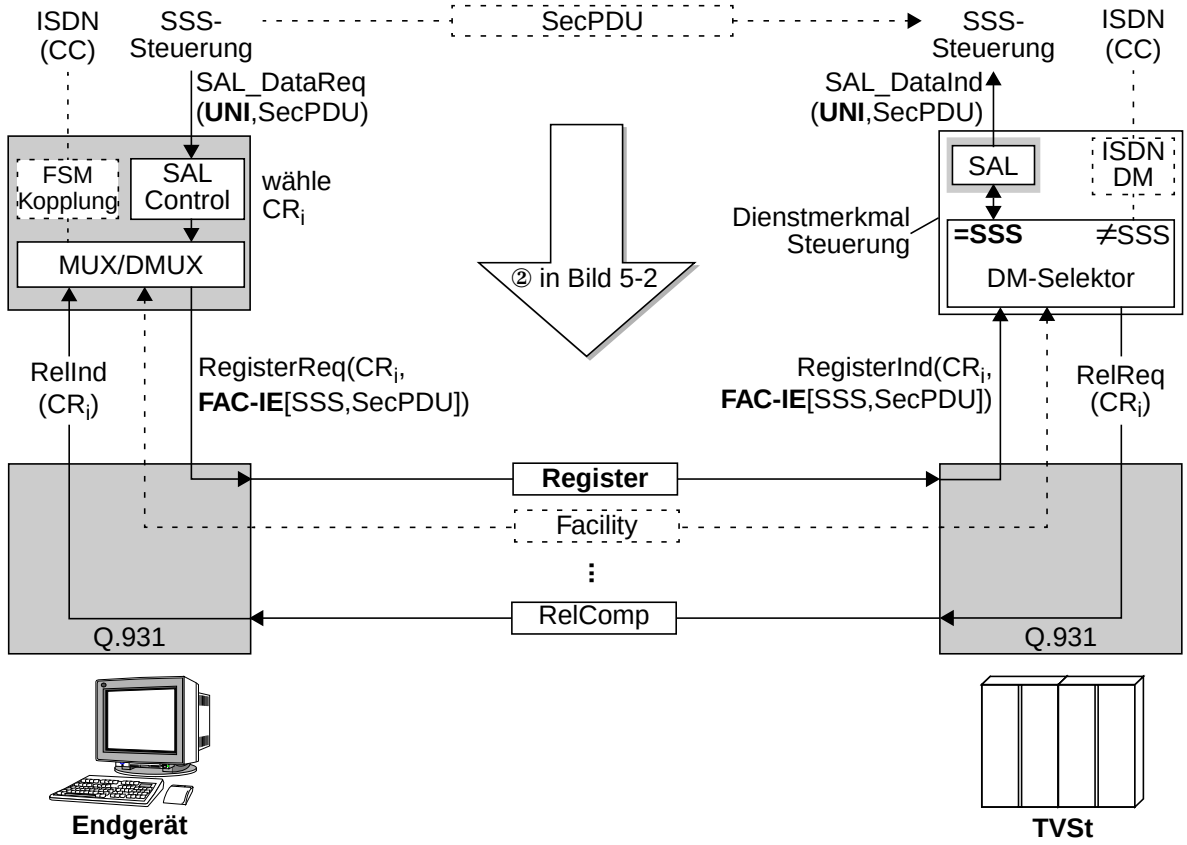


Bild 5-7: Austausch von Steuerinformation an der Benutzer-Netzschnittstelle

Die erste *SecPDU* wird bereits während der Vereinbarung der Call Reference CR_i übertragen. Bei dieser Art der Übermittlung von Sicherheitssteuerungsdaten ist der Overhead wesentlich geringer, als bei der Ende-zu-Ende-Übermittlung mit UUS-Parametern und Verbindungssteuerungs-Nachrichten. Es muß für jede *SecPDU* i.a. eine Schicht 3-Nachricht (*Register* für die erste *SecPDU*, *Facility* für weitere *SecPDUs*) übertragen werden. Dabei können verschiedene Sicherheitsdienste dieselbe Schicht 3-Assoziation (CR_i) nutzen, da die Adressierung der Sicherheitsdienste anhand von Zielinformation der *SecPDU* innerhalb der SSS-Steuerung realisiert wird.

Auch hier ist die maximale Länge der in einem Schritt übertragbaren *SecPDU* durch die maximale Länge eines Schicht 2-Rahmens begrenzt. Eine Segmentierung kann hier – im Gegensatz zur Ende-zu-Ende-Übermittlung – effizient auch innerhalb der SAL durchgeführt werden, da jedes *SecPDU*-Segment nur eine Schicht 3-Nachricht erfordert und im Gegensatz zur Ende-zu-Ende-Übermittlung keine zusätzliche Last innerhalb des Netzes erzeugt.

UNI-Sicherheitsdienste an der Benutzer-Netzschnittstelle ermöglichen z. B. eine hochwertige Authentisierung als Basis der Zugangskontrolle (Schutz des Dienstanbieters). Eine solche Authentisierung kann unabhängig vom Aufenthaltsort und vom Endgerät des Benutzers realisiert werden. Darüberhinaus kann der Schutz von Nutz- und Steuerungsdaten auf der Teilnehmeranschlußleitung und im Zugangsnetzbereich realisiert werden.

Einordnung der SSS in das Funktionale Referenzmodell für ISDN-Dienstmerkmale

Die Sicherheitsdienste auf Anwendungsebene sind vorangehend als zusätzliche Dienstmerkmale zwischen Benutzern (User-to-User-Zeichengabe) und an der Benutzer-Netzschnittstelle (Funktionales Protokoll) modelliert worden. Nachfolgend werden die *Security Supplementary Services*, ihre *Steuerstruktur SSS-Control* und der *Security Adaptation Layer* in das Funktionale Referenzmodell für zusätzliche ISDN-Dienstmerkmale [111] eingeordnet.

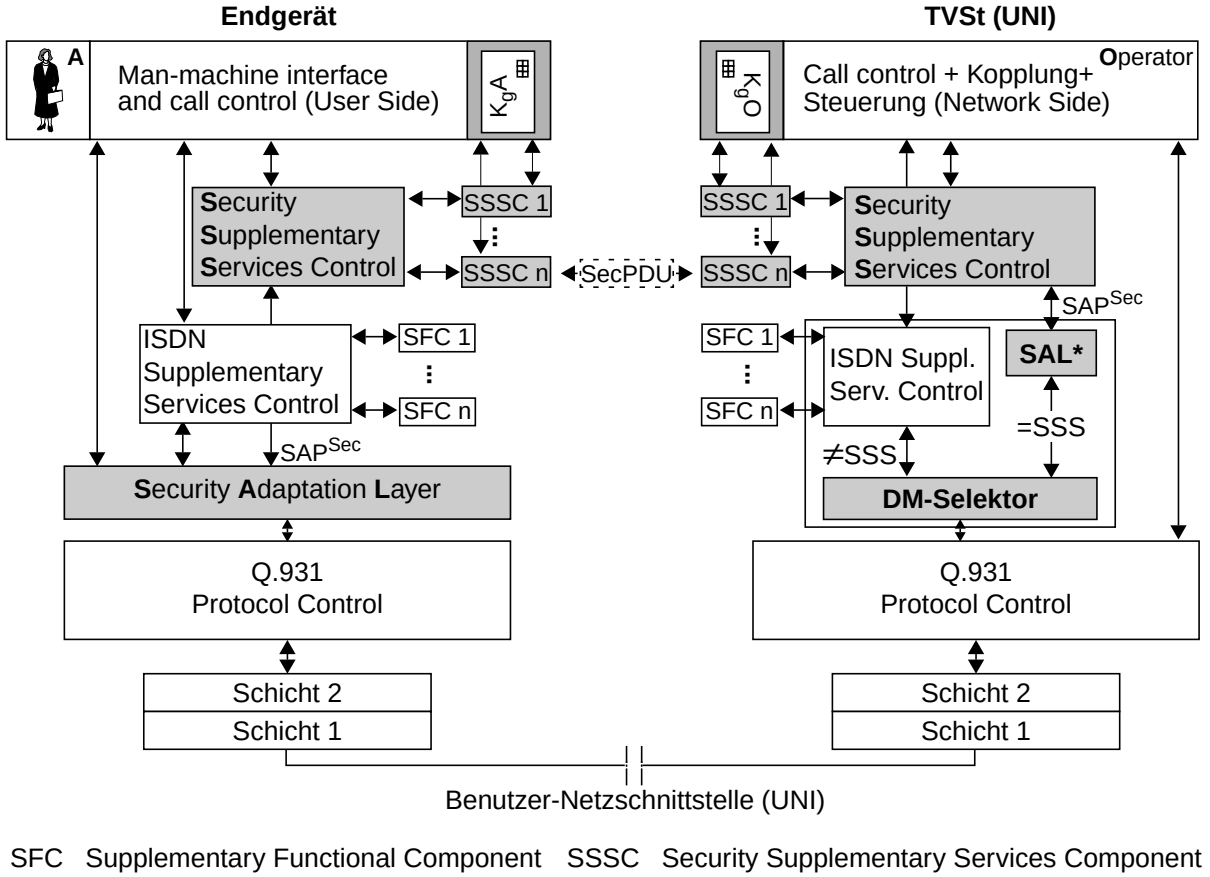


Bild 5-8: Erweitertes Funktionales Referenzmodell basierend auf Q.932

Die Sicherheitsanwendungsdienste selbst sind in einen separaten Block, die sogenannte Security Supplementary Services Control (Sicherheitsdienstesteuerung), integriert. Diese nutzt aus-

schließlich den Dienstzugangspunkt SAP^{Sec} und ist deshalb von den zugrundeliegenden Kommunikationsprotokollen unabhängig.

Im Endgerät wird die Anpassung an das jeweilige Kommunikationsnetz durch die Sicherheitsadaptionsschicht nach Bild 4-23 realisiert. Die SAL integriert im Endgerät folgende Aufgaben:

- Abbildung des Sicherheitsdienstzugangspunktes SAP^{Sec} auf zur Verfügung stehende Netzzugangspunkte (insbesondere Datenübermittlungsdienste)
- Kopplung von Sicherheits- und Kommunikationsdiensten (vgl. Abschnitt 4.4.2)
- Unterstützung der Synchronisierung von Sicherheitskomponenten innerhalb eines Endgerätes (z. B. Sicherheitsfunktionen in Zwischenschichten und Sicherheitsanwendungsdienste)

Der Nachrichtenaustausch zwischen Sicherheitsdiensten (Security Supplementary Services Components in Bild 5-8) an der Benutzer-Netzschnittstelle wird durch *Facility*-Informationselemente (FAC-IE) nach Bild 5-7 realisiert. Die Sicherheitsadaptionsschicht ist somit die umgebungsabhängige Komponente der Sicherheitsarchitektur. Sie muß die zu erweiternden Kommunikationsdienste kennen und beeinflussen. Darüberhinaus muß sie ankommende Nachrichten an die ISDN-Dienstesteuerung, die Sicherheitsdienste-Steuerung (SSS-Steuerung) und gegebenenfalls an die Steuerung von Sicherheits-Zwischenschichten verteilen.

In der Teilnehmervermittlungsstelle werden die Kopplung von Sicherheits- und TK-Diensten sowie die Steuerung der Sicherheitskomponenten direkt in die Rufsteuerung integriert[3]. Ein sogenannter Dienstmerkmalselektor (DM-Selektor in Bild 5-8) ist in die Dienstmerkmalsteuerung zu integrieren. Der DM-Selektor unterscheidet Sicherheits-Dienstmerkmale von ISDN-Dienstmerkmalen. Dienstmerkmalnachrichten mit der Kennung SSS (neu zu standardisieren) werden an eine SAL*-Komponente übergeben. Diese Komponente realisiert die Anpassung der DM-Schnittstelle an den Dienstzugangspunkt SAP^{Sec}, v. a. den Übermittlungsdienst für *SecPDUs*.

EzE-Sicherheitsdienste zwischen Endgeräten werden entsprechend realisiert. Zum Austausch von Sicherheitssteuerungsdaten werden in diesem Fall *User-to-User-Signalling*-Informationselemente (vgl. UUS-IE in Bild 5-6) benutzt.

5.2.2.3 Kompatibilität erweiterter und herkömmlicher ISDN-Endgeräte

Aus Gründen der hohen Investitionen in ISDN-Infrastruktur müssen erweiterte und nicht erweiterte Endgeräte zusammenarbeiten und am selben ISDN-Anschluß betrieben werden können. Herkömmliche Endgeräte dürfen durch die neuen Sicherheitsdienste nicht gestört werden. Das rufende Endgerät muß in der Lage sein, beim Aufbau einer Verbindung gezielt (um Sicherheitsfunktionen) erweiterte Endgeräte anzusprechen. Darüberhinaus muß die SAL eines erweiterten Endgerätes zwischen Steuernachrichten herkömmlicher ISDN-Dienste und Steuernachrichten für Sicherheitsdienste unterscheiden können.

Für diese Aufgaben eignet sich ein Parameter, der bereits im ISDN verwendet wird, um beispielsweise zwischen Telefax- und Telefoniediensten zu unterscheiden: der *High Layer Compatibility* Parameter (HLC) [109]. Der HLC-Parameter wird in der *Setup*-Nachricht zum gerufenen Anschluß übermittelt und dort von den Endgeräten geprüft. Beispielsweise steht

3 Diese Komponenten sind in Endgeräten aufgrund des Aufwandes für Änderungen der Rufsteuerung in der Sicherheitsadaptionsschicht zusammengefaßt.

innerhalb des HLC-Parameters die Kodierung 0x01 (HLC^{Sp}) für Sprachdienste gemäß ITU-Empfehlung G.711 oder 0x04 (HLC^{TF}) für Telefaxdienste der Gruppe 4 gemäß ITU-Empfehlung T.62. Ein Endgerät zeigt der TVSt die Bereitschaft zur Annahme eines Rufes nur dann an, wenn es die geforderten Dienste (Sprach-, Telefaxdienst) unterstützt.

Für um Sicherheitsdienste erweiterte ISDN-Dienste werden bisher reservierte und ungenutzte Kodierungen des HLC definiert (z. B. für erweiterte Sprachdienste HLC^{SpSec} = 0x72), die dem gerufenen Endgerät anzeigen, daß zur Erfüllung der geforderten Eigenschaften ein um die Sicherheitsarchitektur erweitertes (sprachdienstfähiges) Endgerät erforderlich ist. Mit diesem Vorgehen ist es möglich, genau jene Endgeräte eines Anschlusses anzusprechen, die in der Lage sind, den geforderten Mehrwert (hier: Sicherheitsdienste und Sprachdienste) zu erbringen. Ein erweitertes Endgerät muß diesen HLC kennen und eine genau festzulegende minimale Basismenge an Sicherheitsfunktionen zur Verfügung stellen (z. B. Aushandlung, Authentisierung). Nicht erweiterte Endgeräte werden die Dienstanforderung (*SetupReq*) mit der für sie fremden Kodierung des HLC-Parameters ablehnen oder ignorieren. Für die EzE-Übermittlung von Sicherheitssteuerdaten gemäß Bild 5-6 wird ein HLC^{Sec} =0x71 definiert, der den SAL-Übermittlungsdienst adressiert.

Mit der Übermittlung der Verbindungsanforderung und des HLC (*Setup*-Nachricht) wird an jeder Benutzer-Netzschnittstelle eine *Call Reference* etabliert, die zur selben Steuerungstransaktion gehörige Nachrichten kennzeichnet. Alle Steuernachrichten (Rufsteuernachrichten nach Q.931, Dienstmerkmalsteuernachrichten nach Q.932) enthalten eine solche Call Reference, die zur korrekten Verteilung der Steuernachrichten im Demultiplexer der Sicherheitsadaptionsschicht (vgl. Kopplungsstruktur in Bild 4-23) herangezogen wird.

Aus Sicherheitssteuernachrichten werden die *SecPDUs* extrahiert und an die SAL-Steuerung weitergegeben. Bei der Einordnung der Call Reference und bezüglich des Verhaltens der SAL gegenüber der Q.931-Schicht sind zwei Fälle zu unterscheiden:

- Wird die Call Reference durch eine *Setup*-Nachricht etabliert, so wird der darin enthaltene HLC-Parameter zur Einordnung der Call Reference herangezogen. Gilt $HLC = HLC^{Sec}$, so werden zukünftige Steuernachrichten mit derselben Call Reference als Sicherheitssteuernachrichten interpretiert. Die darin enthaltenen *SecPDUs* werden der Steuerung des SAL als *EzE-Sicherheitssteuerungsdaten* übergeben. Das Verhalten der Sicherheitsadaptionsschicht gegenüber der Q.931-Schicht richtet sich in diesem Fall nach Bild 5-6.

- Wird die Call Reference durch eine *Register*-Nachricht etabliert, so wird die Kodierung des darin enthaltenen *Facility*-Informationselementes geprüft. Ist darin ein Sicherheits-Dienstmerkmal kodiert, so werden zukünftige *Facility*-Nachrichten mit dieser CR als Träger von *SecPDUs* interpretiert. Aus den in der *Register*- und den *Facility*-Nachrichten enthaltenen FAC-IEs werden die *SecPDUs* extrahiert und der SAL-Steuerung als *UNI-Sicherheitssteuerungsdaten* übergeben (vgl. Bild 5-7).

Enthält eine empfangene Steuernachricht einen CR, der keine Sicherheitsassoziation kennzeichnet (z. B. Rufsteuernachrichten, ISDN-Dienstmerkmalnachrichten), so wird die Nachricht an den Kopplungsautomaten *FSM_Kopplung* weitergegeben. Von dort wird die Nachricht, falls dies den Sicherheitsvereinbarungen entspricht, an die Rufsteuerung des ISDN-Endgerätes weitergegeben (vgl. Beispiel zur Kopplung von ISDN- und Authentisierungsdienst in Bild 4-24). Mit diesem Mechanismus wird verhindert, daß z. B. die im Rahmen des Austausches von *SecPDUs* nach Bild 5-6 ausgetauschten Verbindungsabbaunachrichten fälschlicherweise über den Kopplungsautomaten an die ISDN-Rufsteuerung übergeben werden.

Der Kopplungsautomat *FSM_Kopplung* ist auch dafür zuständig, den HLC-Parameter in zu sendenden (*SetupReq*) und angezeigten Dienstanforderungen (*SetupInd*) zu behandeln. Ein in einem ankommenden Verbindungswunsch enthaltener HLC^{SpSec} wird beispielsweise in den HLC^{Sp} umgewandelt; zusätzlich werden die ausgehandelten Sicherheitsdienste mit diesem Dienst gekoppelt. Angestoßen werden diese Sicherheitsdienste von der SAL-Steuerung. Bei abgehenden Verbindungswünschen wird ein HLC^{Sp} in einen HLC^{SpSec} umgewandelt, wenn Sicherheitsdienste gefordert sind.

5.2.3 Beispiel: Authentisierung zwischen Endgerät und TVSt

Dieser Abschnitt dient zur Veranschaulichung der Funktionsweise der vorgeschlagenen Sicherheitsarchitektur. Es wird exemplarisch eine Authentisierung beim Verbindungsaufbau zwischen dem rufenden Endgerät und der Teilnehmervermittlungsstelle beschrieben. Im Mittelpunkt der Darstellungen stehen die *Security Supplementary Services* (SSS) sowie die *Sicherheitsadaptionsschicht* und ihr Zusammenspiel mit bestehenden ISDN-Diensten.

Es sei eine Authentisierung zwischen Benutzer und Netzbetreiber (*UNIAuth*) aktiviert (vgl. Anhang A.4.1). Dem Endgerät sei der öffentliche Schlüssel $K_{\ddot{o}}O$ des Netzbetreibers bekannt (vgl. Anhang A.4.2). Der Netzbetreiber verfüge über den öffentlichen Schlüssel des Benutzers ($K_{\ddot{o}}A$). Den Nachrichtenaustausch zwischen Endgerät und Teilnehmervermittlungsstelle zeigt Bild 5-9. Es handelt sich um einen *UNI*-Sicherheitsdienst, an dem das Endgerät und dessen Benutzer sowie die Teilnehmervermittlungsstelle und der Netzbetreiber beteiligt sind.

Die Adaptionsschicht im Endgerät A erkennt zunächst einen Verbindungswunsch des Teilnehmers (vgl. ① in Bild 5-9). Da im Regelsystem der SAL eine *UNI*-Authentisierung als zusätzlicher Sicherheitsdienst spezifiziert ist, wird der HLC^{Sp} für den Sprachdienst beibehalten. Der Verbindungswunsch kann von herkömmlichen ISDN-Endgeräten angenommen werden.[4]

Anschließend stößt die SAL die durch das Regelsystem spezifizierte Authentisierung innerhalb der Sicherheitsdienstesteuerung an (*SSS_Req)*. Diese Anforderung wird – zusammen mit dem öffentlichen Schlüssel $K_{\ddot{o}}O$ des Netzbetreibers – an den Authentisierungsdienst weitergeleitet. Die Steuerung des Dienstes folgt der Schnittstellenbeschreibung für Authentisierungsdienste in Abschnitt 4.3.1.

Anschließend erfolgen der Verbindungsaufbau für den Sprachdienst (gekennzeichnet durch HLC^{Sp}) und die Authentisierung unabhängig voneinander. Bevor die Adaptionsschicht der TVSt die Verbindungsaufbaubestätigung des gerufenen Teilnehmers (*SetupRes*, ② in Bild 5-9) zum Teilnehmer A weiterleitet, kann geprüft werden, ob die Authentisierung erfolgreich abgeschlossen wurde[5]. Im Bild wird die Weitergabe des *SetupRes*-Primitivs für den Sprachdienst nicht mit der Authentisierung gekoppelt, sondern direkt weitergegeben. Falls diese UNI-Authentisierung die Identifizierung des Teilnehmers in der TVSt ersetzen soll[6], dann muß schon die Weiterleitung des Verbindungswunsches zum gerufenen Teilnehmer (*IAM** in Bild 5-9) verzögert werden, bis die Authentisierung des Teilnehmers A abgeschlossen ist.

Die Kopplung innerhalb der Sicherheitsadaptionsschicht des rufenden Endgerätes prüft vor der Weitergabe der Verbindungsaufbaubestätigung (*SetupCnf*, ③ in Bild 5-9) das Ergebnis der Authentisierung. Sollte das Ergebnis der Authentisierung negativ sein, so wird der mit der

4 Wäre ein EzE-Sicherheitsdienst zugeschaltet, so würde die SAL den HLC^{Sp} durch einen HLC^{SpSec} ersetzen. Eine solche Dienstanforderung würde nur von erweiterten ISDN-Endgeräten beantwortet (vgl. Abschnitt 5.2.2.3).

5 Dazu werden u. a. Challenge- (Ch) und Response-Parameter (Res) erzeugt und geprüft (vgl. Abschnitt 4.3.1.1).

6 Darauf basierend kann die Berechtigungsprüfung und die Zuordnung von Entgeltdaten erfolgen.

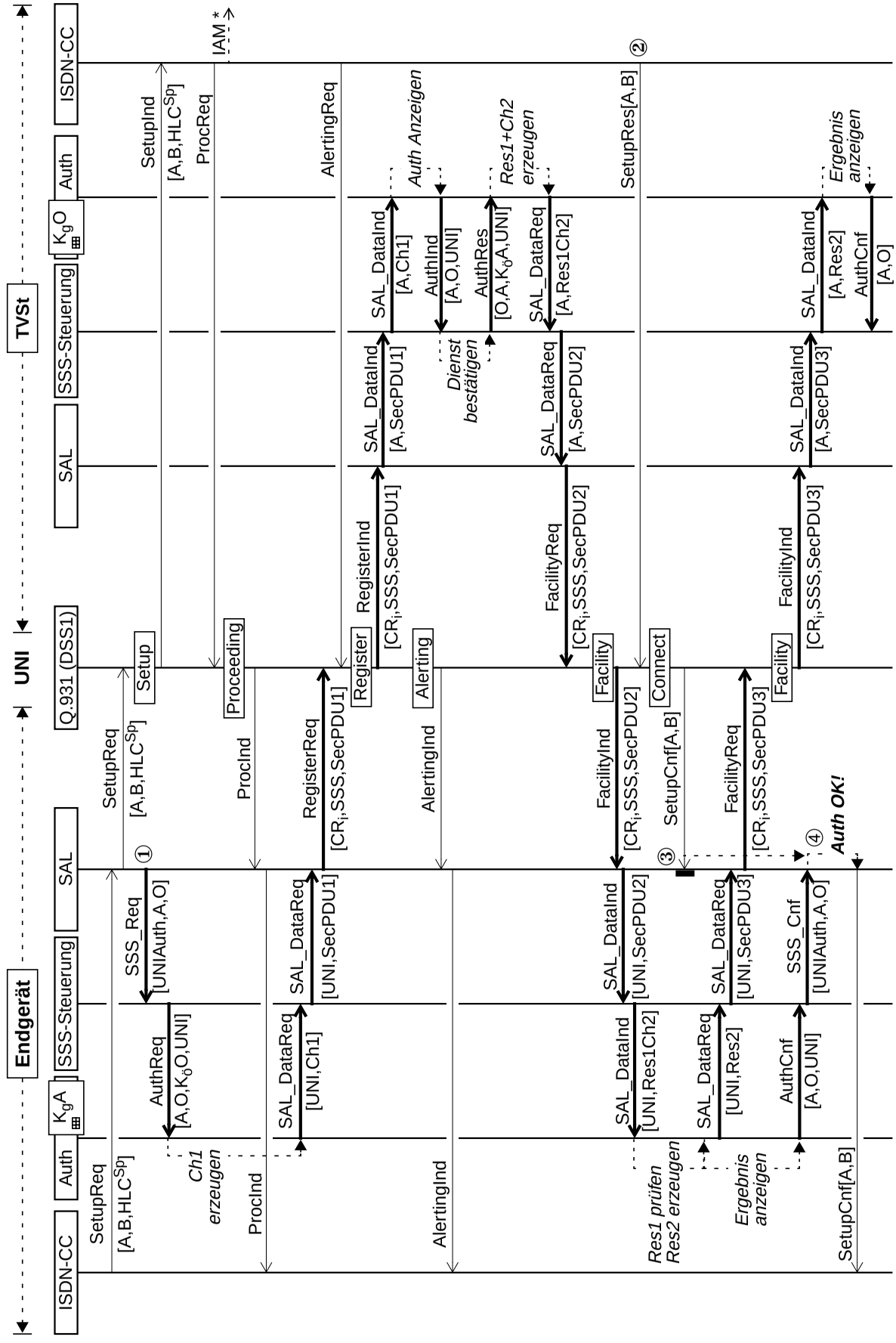


Bild 5-9: UNI-Authentisierung beim Verbindungsaufbau

Authentisierung verknüpfte Verbindungsaufbau abgebrochen. Das Signalisierverhalten des Endgerätes zum Abbruch eines Verbindungsaufbaus folgt in diesem Fall Bild 4-24. Der während einer erfolgreichen Authentisierung zwischen Endgerät und TVSt ausgehandelte geheime Schlüssel kann anschließend von Zwischenschichten für Integritäts- oder Vertraulichkeitsdienste in der Nutzer- und Steuerungsebene am UNI verwendet werden.

Entsprechend erfolgt eine EzE-Authentisierung zwischen Teilnehmern A und B. Die Übermittlung der Authentisierungsnachrichten (*SecPDU1*,..,*SecPDU3*) erfolgt in diesem Fall nicht mit Hilfe von Dienstmerkmalnachrichten nach Bild 5-7 (*Register*, *Facility*), sondern durch die in Bild 5-6 beschriebene Prozedur mit Hilfe von Verbindungssteuerungsnachrichten (*Setup*, etc.).

Weitere Signalisierungs-Zeitdiagramme zur Aushandlung von Sicherheitsdiensten und zur Abfrage öffentlicher Zertifikate bei einem Zertifikatserver werden in Anhang A.4 erläutert. Die Signalisierungs-Zeitdiagramme basieren auf Aufzeichnungen, die aus der Simulation der SDL-Spezifikation des Gesamtsystems gewonnen wurden.

Aus *Sicht des ISDN* laufen ein Verbindungsaufbau und – unabhängig davon – ein ISDN-Dienstmerkmal ab. Aus *Sicht der SAL* wird für einen Verbindungsaufbau ein Sicherheitsdienst UNIAuth aktiviert und im Regelsystem verankert. Parallel zum Verbindungsaufbau werden Sicherheitssteuerungsdaten (*SecPDUs*) zwischen Endgerät und TVSt ausgetauscht (*SAL_DataReq*). Aus *Sicht der SSS* wird eine Authentisierung zwischen Endgerät und TVSt von der Adaptionsschicht angefordert und erfolgreich abgeschlossen.

5.2.4 Implementierung der Sicherheitsarchitektur in einer Linux-Umgebung

Die vorgestellte Sicherheitsarchitektur wurde zunächst spezifiziert und anschließend implementiert.

Spezifiziert wurden die ISDN- und Sicherheitsinfrastruktur-Komponenten in Bild 5-4 sowie der Chipkartenleser und, exemplarisch, eine gegenseitige Authentisierung (Mutual Authentication) von Teilnehmer und Dienstanbieter (vgl. Abschnitt 5.2.3). Die SDL-Spezifikation der Sicherheitsadaptionsschicht und der Security Supplementary Services sind in Anhang A als Blockdiagramme wiedergegeben. Die Spezifikation erfolgte in SDL (Specification and Description Language, [69]) mit dem Werkzeug SDT (SDL Development Toolkit, [70]) von Telelogic.

Implementiert wurden für ISDN-Endgeräte die Sicherheitsadaptionsschicht (SAL) und die Sicherheitsdienstesteuerung (SSS-Control) sowie eine exemplarische Ende-zu-Ende-Authentisierung. Als Implementierungsplattform dienten Linux-Rechner mit ISDN-Adapter. Es liegt die Kernel-Version 2.0.32 des Betriebssystems und die zugehörige ISDN-Implementierung zugrunde. Die Protokollfunktionen des ISDN befinden sich bei der Linux-Implementierung vollständig innerhalb des Betriebssystems. Die Rufsteuerung ist als Anwendungsprozeß implementiert.

Bild 5-10 zeigt die Erweiterung der Endgeräte durch Einbeziehen der Sicherheitsadaptionsschicht und die Realisierung der Schnittstelle SAP^{Sec} (vgl. */dev/SSS* in Bild 5-10) als Treiberschnittstelle zur Kommunikation der Komponenten SAL und SSS-Control.

Die Sicherheitsadaptionsschicht wurde zwischen Schicht 2 und Schicht 3 implementiert, weil diese Schnittstelle einfach zugänglich und wenig komplex ist. Zum Zwischenschalten mußten lediglich die Zeiger auf vier Prozeduraufrufe zum Austausch der Primitive *DL_DataReq*, *DL_DataInd*, *DL_UnitDataReq* und *DL_UnitDataInd* zwischen Schicht 2 und Schicht 3 umprogrammiert werden (vgl. Primitive zwischen Q.931 und Q.921 in Bild 2-8). Da die SAL mit

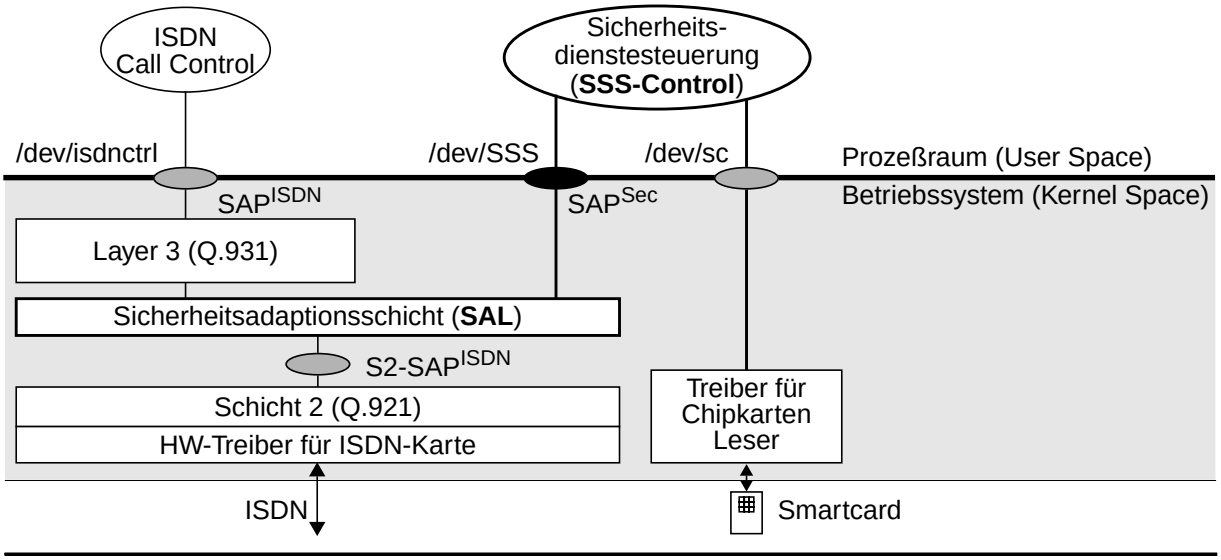


Bild 5-10: Implementierung der Sicherheitsarchitektur in Endgeräten

Nachrichten der Schicht 3 arbeitet, müssen die empfangenen Schicht 2-Rahmen vor der Verarbeitung ausgepackt und interpretiert werden. Dieses ist nicht aufwendig. Jedoch sind Nachrichten der lokalen Rufsteuerung schon durch die Schicht 3 verarbeitet, wenn sie von der Sicherheitsadaptionsschicht empfangen werden. Dieses führt neue zeitliche Randbedingungen für die Bearbeitung dieser Nachrichten innerhalb der SAL ein. Die Schnittstelle (*S2-SAP^{ISDN}* in Bild 5-10) hat sich für die Integration der SAL trotzdem als geeignet erwiesen.

Die Treiberschnittstelle */dev/sc* ist bereits für viele Chipkartenleser auch für das Linux-Betriebssystem verfügbar (vgl. z. B. [76]). Die Treiberschnittstelle */dev/SSS* wurde sehr einfach implementiert. Die Schnittstelle bietet den SSS die Befehle *Write* und *Read* an, mit denen Nachrichten an die SAL geschickt oder von der SAL abgeholt werden können (Polling-Mechanismus). Die Typen der darüber ausgetauschten Primitive des Dienstzugangspunktes *SAP^{Sec}* (*SSS_Req*, *SSS_Cnf*, *SAL_DataReq*, *SAL_DataInd* vgl. Bild 5-5) sind innerhalb der Nachrichten kodiert. Die gesamte Implementierung [71] erfolgte mit Hilfe der Programmiersprache C.

5.2.5 Netztechnische Bewertung des Ansatzes

In Endgeräten spielt der Aufwand für einzelne Implementierungen eine entscheidende Rolle, da Endgeräte keinen zur Netzinfrastruktur vergleichbaren Bündelungsgewinn erzielen. Deshalb spielt gerade bei den Endgeräten die in Abschnitt 4 eingeführte transparente Realisierung mit zentraler Zwischenschicht und separierter Sicherheitsdienstesteuerung eine entscheidende Rolle[7]. Die Trennung von Sicherheits- und TK-Diensten fördert netzübergreifende Sicherheitsdienste (z. B. rufender Teilnehmer am ISDN, gerufener Teilnehmer am GSM oder Internet).

Innerhalb der Teilnehmervermittlungsstellen müssen lediglich neue Dienstmerkmale und der Dienstmerkmalselektor implementiert werden und – bei Bedarf – mit der Rufsteuerung der TVSt gekoppelt werden. Dies ist i. a. durch Erstellen und Einspielen erweiterter Software von zentraler Stelle aus möglich. Eine Kopplung von Sicherheits- und TK-Diensten sowie die

7 Öffentliche Endgeräte können hier eine Ausnahme bilden. Hier könnte der Bündelungsgewinn so hoch sein, daß der Aufwand zur Implementierung von spezifischen Sicherheitsdiensten in die TK-Dienstesteuerung nicht der entscheidende Faktor für die saubere Trennung sein kann.

Steuerung von Zwischenschichten ist nur bei Betrieb von UNI-Sicherheitsdiensten notwendig. Eine Segmentierung wurde nicht implementiert, da die verwendete TK-Anlage UUS-IE bis zur Länge von 128 Oktetts zuläßt. Dieses ist für die Authentisierung mit 512 Bit langen Schlüsseln eines asymmetrischen Kryptosystems ausreichend. Falls Längenbeschränkungen der normalen *Facility*-Informationselemente problematisch sind, so kann auf sogenannte Extended *Facility*-Informationselemente [111] ausgewichen werden.

Bei der netztechnischen Bewertung der Sicherheitsarchitektur stehen die Realisierbarkeit und der Aufwand für die Integration, der Ressourcenverbrauch und die Kompatibilität mit bestehender ISDN-Netzinfrastruktur im Vordergrund.

5.2.5.1 Realisierbarkeit

Die Realisierbarkeit der Sicherheitsarchitektur für ISDN-Endgeräte, d. h. die Implementierung der Sicherheitsadaptionsschicht und der Sicherheitsdienstesteuerung und deren Integration, wurde durch Spezifikation und Implementierung gezeigt. Zur Spezifikation und funktionalen Simulation wurde das SDL-Werkzeug SDT verwendet. Damit konnte die Spezifikation auch durch Eingaben getestet und anhand der Ausgaben des Systems validiert werden. Ausschnitte aus der SDL-Spezifikation sind in den Anhängen A.1, A.2 und A.3 beigefügt.

Die Sicherheitsarchitektur für EzE-Sicherheitsdienste wurde basierend auf der ISDN-Implementierung in Linux-Rechnern exemplarisch implementiert. Die Aufzeichnung des realen Nachrichtenaustausches zur Übertragung einer *SecPDU* zwischen zwei am ISDN angeschlossenen Rechnern ist in Anhang A.6 wiedergegeben und entstammt der Protokollierung der Linux-Rechner sowie der Aufzeichnung von ISDN-Protokollmeßgeräten.

Telekommunikationsanlagen und Teilnehmervermittlungsstellen wurden aus Gründen des Aufwandes und mangels Zugang zu entsprechenden Schnittstellen nicht angepaßt. Für diese UNI-Dienste sind deshalb Signalisierungs-Zeitdiagramme zur Veranschaulichung der Abläufe beigefügt und erklärt (vgl. Anhang A.4). Diese Diagramme basieren auf Simulationen der Spezifikation mit dem SDL-Werkzeug SDT.

5.2.5.2 Aufwand für Implementierung und Betrieb

Der Aufwand für die Implementierung der Sicherheitsarchitektur hängt entscheidend von der Strukturierung des ISDN-Gerätes ab, das erweitert werden soll. Das Linux-Betriebssystem bietet geeignete Schnittstellen zur Integration der Adaptionsschicht zwischen Schicht 2 und Schicht 3 des ISDN-Protokollturms.

Die *Integration* der SSS im Prozeßraum (User Space) und die Implementierung einer Treiberschnittstelle (/dev/SSS in Bild 5-10) zur Kommunikation von SSS und Adaptionsschicht ist programmiertechnische Arbeit, schafft aber keine prinzipiellen Probleme.

Die erweiterten Endgeräte sind bei abgeschalteten Sicherheitsdiensten *kompatibel* zu herkömmlichen ISDN-Endgeräten und herkömmlicher ISDN-Netzinfrastruktur. Dies wurde durch Tests mit herkömmlichen ISDN-Endgeräten und unterschiedlichen Telekommunikationsanlagen sowie am öffentlichen Netz bestätigt. Die Trennung von Sicherheitsdiensten und herkömmlichen TK-Diensten mit Hilfe des HLC-Parameters ermöglicht das Betreiben erweiterter Endgeräte auch am Mehrgeräteanschluß.

Beim *Betrieb von Sicherheitsdiensten* hat sich vor allem die EzE-Übermittlung von Sicherheitssteuerungsdaten (*SecPDUs*) als sehr aufwendig erwiesen. Das Vortäuschen eines Verbindungsaufbaus zur Übermittlung einer *SecPDU* ist sehr aufwendig, da die Steuerprozesse aller

zwischenliegenden Vermittlungsstellen an der Übermittlung beteiligt sind. Die in Bild 5-6 vorgestellte Übermittlung einer *SecPDU* dauerte vom Versenden der *Setup*-Nachricht bis zum Erhalt der *RelComp*-Nachricht ca. 3,4 Sekunden. Darin sind 3 Sekunden enthalten, die die TVSt beim gerufenen Teilnehmer trotz Ablehnung des Rufes durch das gerufene Endgerät wartet, ob sich noch andere Endgeräte melden.[8]

Deshalb wurde das in Bild 5-6 vorgestellte Szenario beschleunigt. Nach Erhalt der *CallProc*-Nachricht wird der Verbindungswunsch beim rufenden Endgerät sofort durch die *Disconnect*-Nachricht widerrufen. Damit läßt sich die *EzE-Übermittlung* einer *SecPDU* von der *Setup*- bis zur *RelComp*-Nachricht auf 0,2 Sekunden verringern (vgl. Bild 5-11). Bei der Messung waren die beiden erweiterten Endgeräte an derselben TK-Anlage bzw. TVSt angeschlossen. Zusätzlich könnten auch andere UUS-Dienste zur Übermittlung von *SecPDUs* genutzt werden.

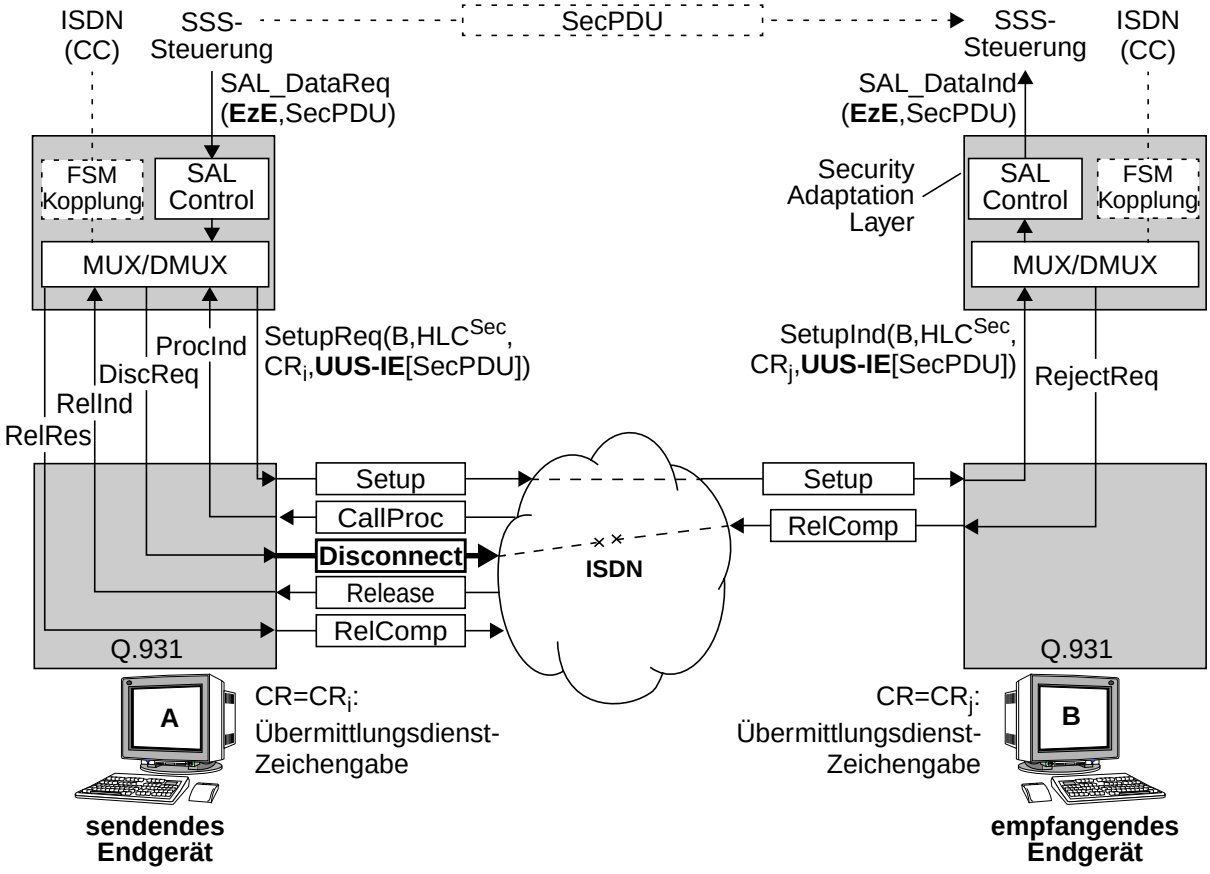


Bild 5-11: Verbesserter Ende-zu-Ende-Übermittlungsdienst

Diese EzE-Übermittlungszeit ist auch beim Austausch von 3 *SecPDUs*, z. B. zur EzE-Authentisierung während eines Verbindungsaufbaus, als Übergangslösung akzeptabel. Aus der Sicht des Netzbetreibers entsteht jedoch erheblicher Signalisier- und Steueraufwand, da beim Übermitteln der *Setup*-Nachricht eine Nutzkanalverbindung zwischen A- und B-Teilnehmer aufgebaut wird, die danach sofort wieder abgebaut wird. Auch die Entgelterfassung ist für diese Art der Dienstnutzung noch zu klären[9]. Die darüberhinaus vorgesehenen, aber zur Zeit nicht angebotenen, UUS-Dienste erlauben die Übertragung weiterer *UUS*-Informationselemente in separaten *USR*-Nachrichten [104]. Eine verbindungslose Übermittlung ist jedoch nicht vorgesehen.

8 Nach ITU-Empfehlung Q.931 sollten es 4 Sekunden (T303) sein, vgl. auch Abschnitt 5.2.2.2.

Die *UNI-Übermittlung* von *SecPDUs* zwischen Endgerät und TVSt hingegen ist effizient gelöst. Für jede *SecPDU* muß nur eine Schicht 3-Nachricht (*Register* bzw. *Facility*) übertragen werden. Da die *SecPDUs* aufgrund kryptographischer Blocklängen meist eine Länge von über 100 Oktetts haben werden, ist der Zusatzaufwand für den schließlich übertragenen Schicht 2-Rahmen (Kopf für Schicht 3, Kopf für Schicht 2, Bestätigung auf Schicht 2) gering. Auf der Teilnehmeranschlußleitung ist i. a. kein Bandbreitenengpaß im Signalisierkanal vorhanden.

Die *Steuerung von zusätzlichen Zwischenschichten* (z. B. in der Nutzer-Ebene) durch die SAL-Steuerung kann zu merklichen Verzögerungen führen, falls die Zwischenschichten eine zusätzliche Synchronisierung fordern (z. B. Schlüsselvereinbarung etc.).

Der *Kopplungsvorgang* innerhalb des *FSM_Kopplung* der Sicherheitsadaptionsschicht im Endgerät ist sehr einfach und bedarf zum Zustandsübergang zwischen Empfang und Weiterleitung einer Nachricht lediglich der Prüfung einer Übergangsbedingung in der Regeldatenbasis. Die durch die Synchronisierung von ISDN- und Sicherheitsdiensten möglicherweise eingeführte Wartezeit ist von den aktivierten Sicherheitsdiensten und teilweise auch von der Interaktion der Teilnehmer (z. B. Einführen einer Chipkarte) abhängig.

Durch zugeschaltete Sicherheitsdienste (Aushandlung, Authentisierung, Verschlüsselung etc.) wird die Zeit vom Verbindungswunsch bis zur Verbindungsbestätigung verändert. Die tatsächliche Verzögerung wird von der Dauer der Übermittlung von *SecPDUs* und von den Funktionen zur Signierung und Signaturprüfung dominiert und liegt bei Software-Lösungen i. a. im Bereich von wenigen Sekunden (z. B. Authentisierung und Verbindungsaufbau).

5.2.5.3 Netzevolution

Die Abhängigkeit der Sicherheitsarchitektur vom zugrundeliegenden Kommunikationsnetz spiegelt sich vor allem in der Übermittlung von Sicherheitssteuerungsdaten und in der Kopplung von ISDN-Diensten und zugeschalteten Sicherheitsdiensten wider. Insbesondere der Austausch von *SecPDUs* zwischen Endgeräten muß zukünftig besser durch das Kommunikationsnetz unterstützt werden. Dazu bietet sich die Einführung eines zusätzlichen ISDN-Dienstmerkmals an, welches die transparente Übermittlung von Steuerinformation zwischen zwei ISDN-Anschlüssen unterstützt.

Die bisher als UUS-Dienste angebotenen Übermittlungsdienste sind dazu nicht geeignet, weil sie sich auf einen einhergehenden Verbindungsaufbau stützen. Außerdem werden diese Dienste zur Zeit nicht angeboten. Dieser neue Dienst könnte als Bestandteil der ISDN-Supplementary Services (vgl. ISS in Bild 2-11) eine logische Verbindung zwischen rufender und gerufener TVSt unterhalten und somit die *SecPDUs* basierend auf TCAP und SCCP im Zwischenamtsbereich (vgl. Abschnitt 2.4.2) schnell und effizient übertragen.

Aus Sicht des Endgerätes unterscheidet sich in diesem Fall die EzE-Übermittlung von der UNI-Übermittlung nur durch die Kodierung der *Facility*-Informationselemente. Insbesondere steht bei dieser Realisierung der zweite B-Kanal für weitere Anwendungen zur Verfügung. Bei der gegenwärtigen Art der Übermittlung von *SecPDUs* wird ein B-Kanal jeweils durch den fingierten Verbindungsaufbau beim Sender unnötig belegt.

---

9 Augenblicklich werden – obwohl technisch verfügbar – keine UUS-Dienste im öffentlichen ISDN angeboten. Deshalb konnten die Tests der EzE-Übermittlung mit UUS-IE ausschließlich an TK-Anlagen durchgeführt werden. Jedoch konnte die Übermittlungszeit auch im öffentlichen Netz nachgewiesen werden, wobei jedoch die UUS-IE nicht beim gerufenen Endgerät ankommen. Das Signalisier-Szenario läuft dort gleich ab.

Darüberhinaus müssen die in Anhang A.5 exemplarisch gewählten Kodierungen von Informationselementen zur Übermittlung von Sicherheitssteuerungsdaten standardisiert werden, um die Kompatibilität unterschiedlicher Implementierungen zu unterstützen.

5.2.6 Sicherheitstechnische Bewertung des Ansatzes

Zur sicherheitstechnischen Bewertung wird das in Kapitel 4.2.3 vorgestellte Modell herangezogen. Als Basis der Bewertung wird davon ausgegangen, daß die ISDN- und Sicherheitsarchitektur-Komponenten in einer sicheren Umgebung korrekt implementiert sind, alle Steuernachrichten die SAL im Endgerät passieren müssen und die zugeschalteten Sicherheitsdienste in Zwischenschichten und innerhalb der SSS korrekt implementiert sind und in sicherer Umgebung ablaufen.

Es wird gezeigt, welche Sicherheit mit dieser Sicherheitsarchitektur durch Zuschalten (Koppeln) von Sicherheitsdiensten mit ISDN-Diensten aus Sicht der Teilnehmer erreichbar ist. Es ist nicht Sinn und Zweck, die Sicherheitsdienste selbst zu bewerten.

Die durch die Sicherheitsarchitektur angebotenen Dienste umfassen (i) den Zugang für Benutzer zu Anwendungsdiensten der SSS-Steuerung, (ii) den UNI- und EzE-Übermittlungsdienst für *SecPDUs* und (iii) die Kopplung von Sicherheits- und ISDN-Diensten. Das Modell für erweiterte Kommunikationssysteme und diesbezügliche Angriffspunkte zeigt Bild 5-12.

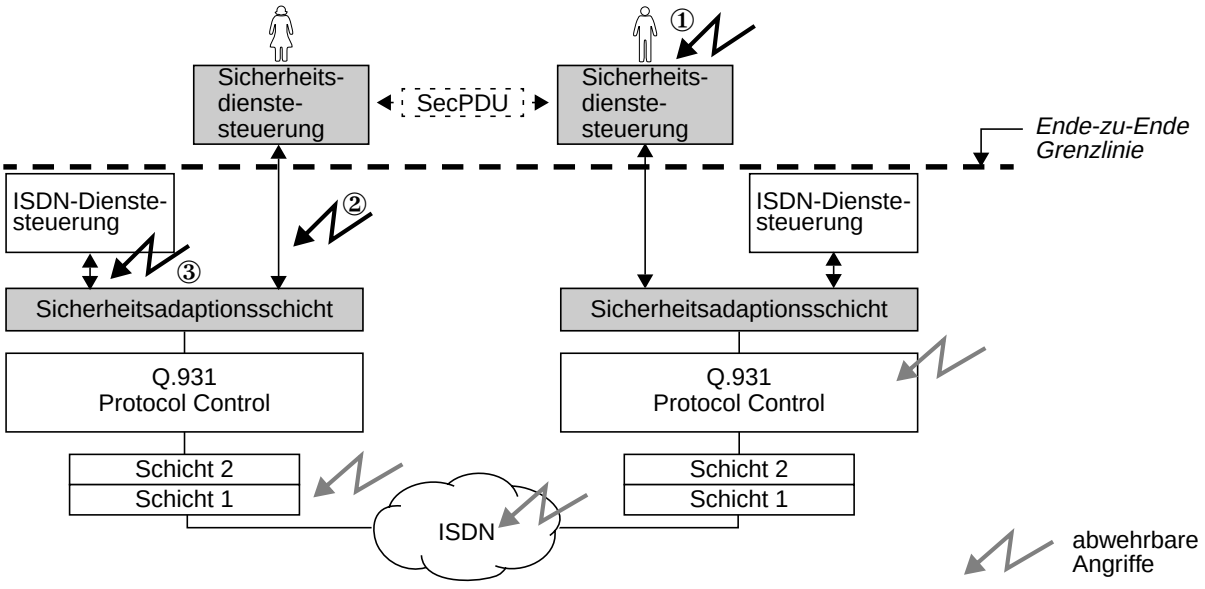


Bild 5-12: Angriffspunkte bezüglich der Sicherheitsarchitektur in der Steuerungsebene

Sicherheitsdienste in der Steuerungs-Ebene

Die *Sicherheitsanwendungen* sind oberhalb der Ende-zu-Ende-Grenzlinie (vgl. Bild 4-7) lokalisiert. Dies bedeutet, daß sie unabhängig von den unterhalb der EzE-Grenzlinie liegenden Funktionen realisierbar sind. Mit diesen Diensten lassen sich Identitäten authentisieren, Schlüssel vereinbaren, Schlüsselzertifikate abfragen etc.

Sind die SSS manipulierbar oder werden Eingaben des Benutzers bzw. Ausgaben an den Benutzer manipuliert (vgl. Schnittstelle ① in Bild 5-12), so sind nachvollziehbar sichere Telekommunikationsdienste nicht mehr realisierbar.

Der *Datenübermittlungsdienst der SAL* ist bezüglich seiner Verfügbarkeit von den genutzten Übermittlungsdiensten des ISDN abhängig, d. h. von der Übermittlung der *UUS*- bzw. *FAC*-Informationselemente. Durch Schutzfunktionen in Zwischenschichten können die zu übermittelnden Daten bezüglich Integrität und Vertraulichkeit auf ihrem Weg (unterhalb der SAL) geschützt werden, da sie für zwischenliegende Funktionen transparent sind.

Die *korrekte Kopplung* von ISDN- und Sicherheitsdiensten innerhalb der SAL in Endgeräten ist abhängig von zwei Einflußfaktoren:

- Die Konfiguration der Regeldatenbasis bei der *Zuschaltung von Sicherheitsdiensten* erfolgt über die SAP^{Sec}-Schnittstelle durch die Sicherheitsdienstesteuerung (vgl. Schnittstelle ② in Bild 5-12). An dieser Schnittstelle müssen Angriffe ausgeschlossen werden, um die Kopplung sicher steuern zu können.

- Die Steuerung der ISDN-Dienste muß durch die Kopplung soweit kontrollierbar sein, daß Dienste abgebrochen oder verzögert werden können, falls damit gekoppelte Sicherheitsdienste nicht erfolgreich ablaufen (vgl. Schnittstelle ③ in Bild 5-12).

In der TVSt erfolgt die Kopplung von UNI-Sicherheitsdiensten und TK-Diensten direkt in der zentralen Rufsteuerung. Der Angriffspunkt ③ entfällt hier bei korrekter Implementierung.

Ist dies gegeben, so kann aufbauend auf einer Authentisierung (und dem dabei vereinbarten geheimen Schlüssel K) die Integrität von Steuernachrichten zwischen Endgeräten oder zwischen Endgerät und TVSt geschützt werden. Dazu können den Zeichengabenachrichten sogenannte Message Authentication Codes beigefügt werden, die mit dem gemeinsamen Schlüssel K geschützt werden. Zum EzE-Integritätsschutz von Rufsteuerungsnachrichten können MACs gebildet werden, die auf den nicht veränderlichen Parametern und dem Typ der Steuerungsnachricht beruhen. Solche selektiven MACs sind EzE verwendbar, obwohl die zugehörigen Steuernachrichten im ISDN teilweise verändert werden. Dieses Verfahren wird beispielsweise für ATM-Netze [72] und für das Internet Protocol IPv6 [136] vorgeschlagen. Die Vertraulichkeit von Rufsteuernachrichten kann lediglich zwischen Teilnehmer und Netzbetreiber realisiert werden, da diese unterhalb der EzE-Grenzlinie im Netz verarbeitet werden (vgl. Bild 4-10).

Die zu aktivierenden Sicherheitsdienste können zwischen Benutzern (EzE) oder zwischen Benutzern und Netzbetreibern (UNI) ausgehandelt werden.

Sicherheitsdienste in der Nutzer-Ebene

Nutzdaten (vgl. Bild 4-9) können im ISDN durch Zwischenschichten Ende-zu-Ende oder am UNI gesichert werden. Die zum Betrieb und zur Synchronisierung der Zwischenschichten notwendigen Parameter lassen sich mit Hilfe von Sicherheitsanwendungsdiensten (z. B. Aushandlung, vgl. Bild 4-21) direkt zwischen den Beteiligten aushandeln. Ist der Steuerungskanal zwischen der Sicherheitsdienstesteuerung und den Zwischenschichten sicher oder gesichert, so sind bezüglich der Nutzdaten alle Schutzziele betreffend Integrität und Vertraulichkeit zwischen Endgeräten (EzE) und zwischen Endgeräten und TVSt (UNI) gegen Angreifer durchsetzbar.

Fazit: Die Sicherheitsarchitektur unterstützt die Aushandlung und Synchronisierung von Sicherheitsdiensten sowie die optionale Zuschaltung von Sicherheitsdiensten zu ISDN-Diensten. Meist wird die Sicherung wie folgt ablaufen: Zunächst verknüpft der Kopplungsautomat der SAL im Endgerät den Verbindungsaufbau mit der Aushandlung von Sicherheitsdiensten und der Authentisierung (*logische Kopplung anhand der Regeldatenbasis*). Anschließend wer-

den ISDN-Dienst und ausgehandelte Sicherheitsdienste mit Hilfe des während der Authentisierung vereinbarten geheimen Schlüssels *kryptographisch verknüpft* (z. B. durch Aktivieren von Zwischenschichten zur Verwenden von MACs oder zur Verschlüsselung).

Die vorgeschlagene Sicherheitsarchitektur unterstützt somit mehrseitig sichere Kommunikationsdienste im Rahmen der Möglichkeiten, die durch prinzipielle Randbedingungen der Plazierung (Endgerät oder TVSt) und des daraus resultierenden Wirkungsbereiches von Sicherheitsfunktionen gegeben sind (vgl. Abschnitt 4.2). Die Implementierung im Endgerät bzw. in der TVSt basiert auf sicheren Endgeräten bzw. sicheren Umgebungen innerhalb der TVSt.

5.3 Auslagerung von Sicherheitsfunktionen

5.3.1 Zusätzliche Geräte im Teilnehmerbereich

5.3.1.1 Auslagerung der Sicherheitsdienstesteuerung

Da der Dienstzugangspunkt für Sicherheitsdienste (vgl. SAP^{Sec} in Bild 5-5) unabhängig vom zugrundeliegenden Telekommunikationsnetz spezifiziert wurde, bietet sich diese Schnittstelle auch als Hardware-Schnittstelle an. Die Adaption dieses Dienstzugangspunktes SAP^{Sec} an die jeweilige Telekommunikationsumgebung und das Endgerät wird durch die SAL vorgenommen. Bild 5-13 zeigt die Schnittstellen bei der Auslagerung der Sicherheitsdienstesteuerung.

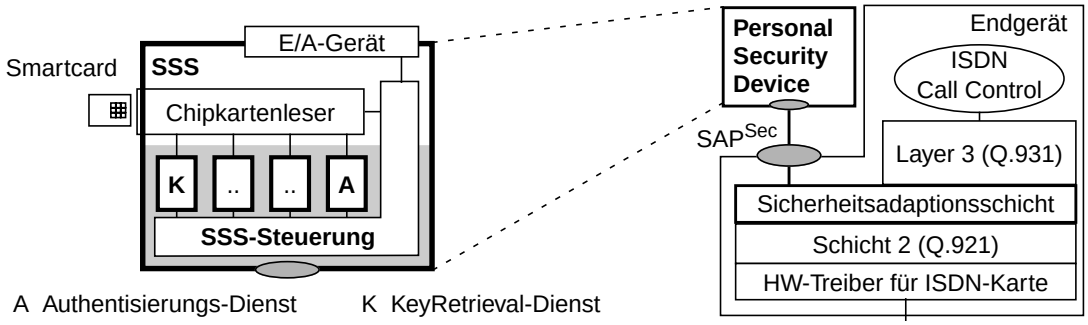


Bild 5-13: Auslagerung der Sicherheitsdienstesteuerung

Der Chipkartenleser ist in das Sicherheitsmodul integriert, in dem auch die SSS-Steuerung implementiert ist. Der sogenannte Personal Security Device kann recht klein und handlich sein und eignet sich zum mobilen Einsatz, z. B. an fremden Endgeräten. Das Gerät ist vom Telekommunikationsdienst unabhängig und kann in GSM, ISDN und IP-Umgebungen (z. B. an öffentlichen Endgeräten) genutzt werden. Zur Bewertung dieser Variante ist basierend auf den Überlegungen in Abschnitt 4.2.4 folgendes anzumerken:

- Zusätzliche Funktionsschichten werden durch die Auslagerung nicht bedingt, weil die HW-Schnittstelle SAP^{Sec} an der Stelle einen Zugangspunkt bietet, an der die ausgelagerten Funktionen integriert werden sollen.
- Damit diese Variante sicherheitstechnisch mit der integrierten Lösung vergleichbar ist, muß der Pfad zwischen Sicherheitsdienstesteuerung und Sicherheitsadaptionsschicht sicher sein. Insbesondere an der Hardware-Schnittstelle darf kein Angriff möglich sein. Bei hohen Schutzanforderungen bzw. starkem Angreifermodell muß die Kommunikation zwischen SSS-Steuerung und SAL (kryptographisch) bezüglich Vertraulichkeit und Integrität der Steuerungsdaten geschützt werden.

- Das Sicherheitsmodul (Personal Security Device) kann aufwendiger gesichert werden, da es universell einsetzbar und nicht an ein spezielles Endgerät oder einen speziellen Benutzer gebunden ist.

Da die meisten Sicherheitsdienste (z. B. KeyRetrieval, Authentisierung) die ausgetauschten Steuerinformationen selbst schützen können, liegt diese neue HW-Schnittstelle im geschützten Bereich (vgl. Bild 4-8). Sie führt folglich keine nicht abwehrbaren Angriffspunkte ein. Bezüglich der Kopplung von TK- und Sicherheitsdiensten und der Implementierung von Zwischenschichten muß dem Endgerät jedoch weiterhin vertraut werden.

5.3.1.2 Auslagerung der gesamten Sicherheitsarchitektur

Kann oder soll die Sicherheitsarchitektur nicht in das Endgerät selbst integriert werden, so bestehen Möglichkeiten zur Implementierung in autonomen Geräten. Dies entspricht ausgelagerten Sicherheitsfunktionen nach Bild 4-13a. Eine vollständige Auslagerung der Sicherheitsarchitektur in eine Black-Box im Teilnehmerbereich zeigt Bild 5-14.

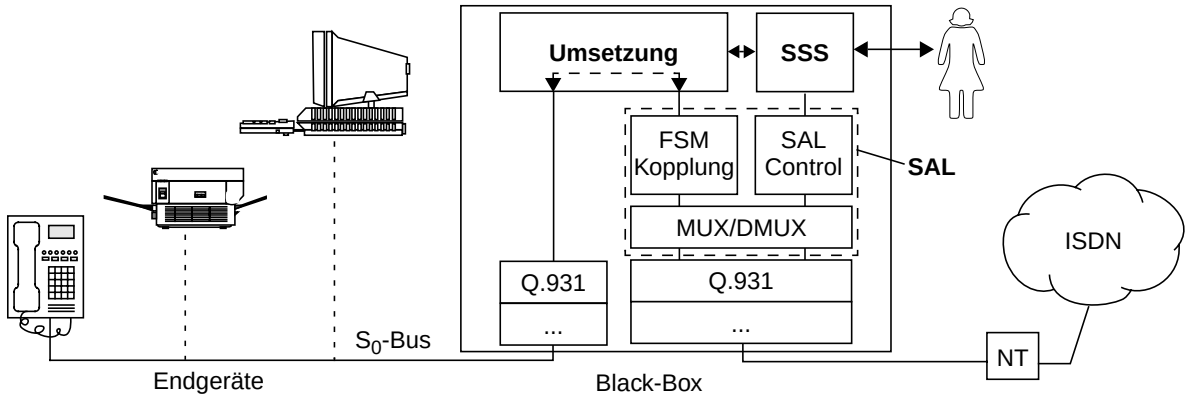


Bild 5-14: Auslagerung der gesamten Sicherheitsarchitektur

Hier wird die Integration einer zusätzlichen Komponente am Referenzpunkt S des einfachen ISDN-Anschlusses zwischen ISDN-Endgeräten und dem NT betrachtet (vgl. Bild 2-4). Die *Umsetzung* und die Sicherheitsadaptionsschicht innerhalb der Black-Box setzen auf der zusätzlich implementierten Vermittlungsschicht auf. Die Umsetzung muß die ankommenden Steuernachrichten zur ISDN-Dienstesteuerung an die Endgeräte bzw. an die Kopplung weiterleiten (z. B. wird ein *SetupInd*-Primitiv von der *SAL* als *SetupReq*-Primitiv an die Q.*931-Schicht* in Richtung der Endgeräte weitergegeben).

Sind die TK-Dienste der Endgeräte ausschließlich über die Black-Box ansprechbar (z. B. durch Zwischenschalten der Black-Box), so gilt für diese Lösung dieselbe sicherheitstechnische Bewertung wie für die integrative Lösung in Bild 5-12[10]. Die Black-Box kann bei entsprechender Auslegung von mehreren Endgeräten genutzt werden (Telefon, Telefax, Rechner).

5.3.2 Auslagerung in spezielle Netzknoten

Dieser Abschnitt skizziert die Einbeziehung zentraler Netzknoten zur Auslagerung von Sicherheitsfunktionen aus Endgeräten. Die vorgeschlagene Vorgehensweise zielt auf die Unterstüt-

10 Wie in Abschnitt 4.2.4 dargelegt, muß der Pfad zwischen der ausgelagerten Sicherheitsadaptionsschicht und der Schicht 3 der Endgeräte sicher sein. Die Black-Box muß eine sichere Ablaufumgebung darstellen.

zung benutzerorientierter Sicherheitsdienste ab und stützt sich stark auf die im Zwischenamtsbereich im ISDN eingesetzte Protokollarchitektur.

5.3.2.1 Zielsetzung

Die Allokationspunkte (Plazierungsmöglichkeiten) für Sicherheitsfunktionen sind bisher auf das UNI (Endgeräte oder Teilnehmervermittlungsstellen) beschränkt. Weitere Infrastruktur ist durch ein Endgerät nicht explizit adressierbar.[11]

Nun sollen auch zentrale Server innerhalb des Netzes in Sicherheitsdienste eingebunden werden können (Mehrwert aus Sicherheitssicht schaffen). Dazu müssen Teile der Sicherheitsarchitektur auch in die Protokollarchitektur im Zwischenamtsbereich des ISDN integriert werden:

- Die Implementierung eines *PzP-Dienstmerkmales* (z. B. als SSS-Dienst) in die TVSt und in zentrale Server unterstützt den Datenaustausch zwischen Endgeräten und ausgelagerten Sicherheitsfunktionen in zentralen Servern (z. B. Verzeichnisdienste für Schlüsselzertifikate, vgl. Abschnitt 4.3.1.3). Im Zuge dieser Erweiterung der Teilnehmervermittlungsstellen soll auch ein EzE-*Dienstmerkmal* integriert werden, das eine verbindungsunabhängige Übermittlung von Ende-zu-Ende-Sicherheitssteuerungsdaten zwischen Endgeräten unterstützt.

- Die Implementierung des *Dienstzugangspunktes SAP^{Sec} in zentralen Servern* ermöglicht deren Partizipieren an Sicherheitsdiensten (z. B. Proxy-Server zum Schutz der Kommunikationsbeziehung, vgl. Abschnitt 4.3.3).

Die Idee sicherheitstechnischer Mehrwertdienste illustriert Bild 5-15. An den Schnittstellen des DSS1 (vgl. ① in Bild 5-15) wird der Zugang zu netzbasierten EzE-Übermittlungsdiensten und der Zugang zu PzP-Sicherheitsdiensten in zentralen Netzknoten mit Hilfe zusätzlicher ISDN-Dienstmerkmale unterstützt.

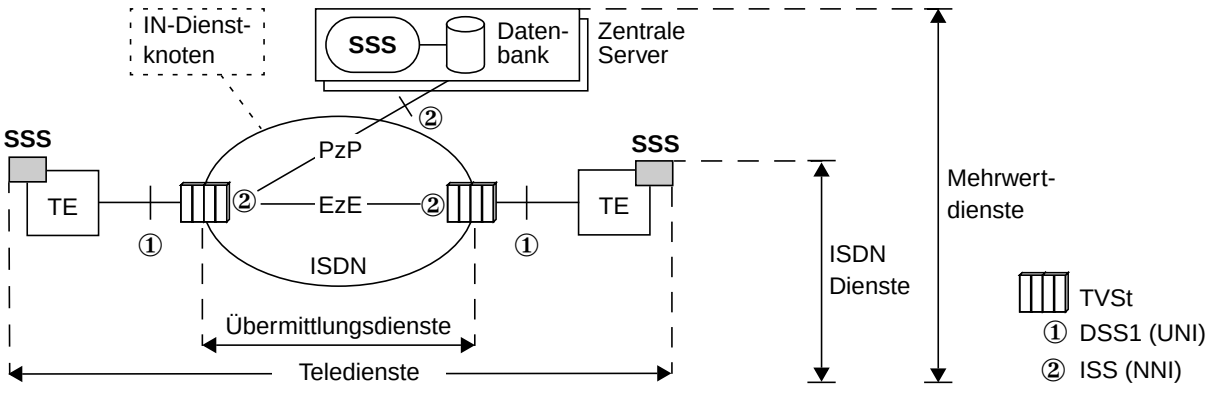


Bild 5-15: Einordnung von Sicherheitsdiensten basierend auf Bild 2-2

Die Adressierung zentraler Server im Netz (über Schnittstelle ② in Bild 5-15) ermöglicht deren Einbinden in Sicherheitsdienste. Der zentrale Server unterstützt hier nicht – wie im Intelligenten Netz – transparent für den Benutzer die Netzdienste, sondern transparent für das Netz die explizit durch den Benutzer zugeschalteten Sicherheitsdienste.

11 Auch im Intelligenten Netz erfolgt die Adressierung der zentralen IN-Infrastruktur nicht explizit durch den Teilnehmer, sondern implizit innerhalb den Netzknoten.

5.3.2.2 Sicherheitsarchitektur für den Zwischenamtsbereich

Die *Unterstützung von EzE-Übermittlungsdiensten* wird im Zwischenamtsbereich durch ein Ende-zu-Ende-Dienstmerkmal realisiert. Die zwischen Endgeräten zu übermittelnden Sicherheitssteuerdaten (*SecPDUs*) werden mit Hilfe eines ISDN-Dienstmerkmales über die Benutzer-Netzschnittstelle (DSS1) an die TVSt weitergegeben. Die Ursprungs-TVSt baut daraufhin über die ISDN-Supplementary Services (ISS)[12] eine Zeichengabe-Assoziation zur Zielvermittlungsstelle auf. Am Ziel-Anschluß werden die Sicherheitssteuerungsdaten dem Endgerät über ISDN-Dienstmerkmal-Nachrichten angezeigt. Die Adressierung der Sicherheitsfunktionen, der Aufbau einer logischen Verbindung zwischen den Teilnehmervermittlungsstellen und der Austausch von *SecPDUs* wird vom EzE-Dienst der SSS-Dienstmerkmalsteuerung gesteuert, vergl. Bild 5-16.

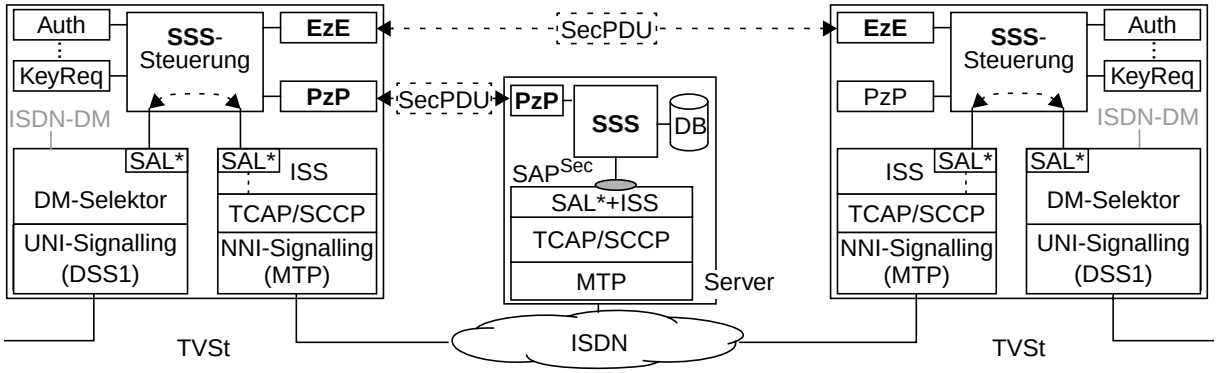


Bild 5-16: Sicherheitsarchitektur basierend auf dem ZGS Nr. 7

Die ISS werden so erweitert, daß der SSS-Steuerung die Übermittlung von *SecPDUs* durch die Primitive *SAL-Req/Ind* zur Verfügung stehen. Diese Funktionen werden in der sogenannten SAL* zusammengefaßt, die direkt auf dem TCAP aufsetzen kann.

Das *Ansprechen von Sicherheitsdiensten in zentralen Servern* (z. B. PKI-Dienste zur Abfrage von Schlüsselzertifikaten über das ZGS Nr. 7, vgl. [11],[28]) kann auf dieselbe Art und Weise mit Hilfe eines *PzP-Dienstmerkmales* realisiert werden. Dazu muß der zentrale Server zum Austausch von Sicherheitssteuerungsdaten durch die Endgeräte adressierbar sein. Die Umsetzung dieser Adresse in eine netzinterne Adresse erfolgt im Netz (z. B. in der TVSt). Auch hier wird zusätzliche Funktionalität (SAL*) zum Zugriff auf die Dienste des TCAP in die ISS integriert. Die Adressierung der SSS innerhalb des Servers erfolgt durch den SCCP über die erweiterten ISS mit deren Subsystemnummer SSN_{ISS}. Die Adreßumsetzung muß also aus der durch den Benutzer vorgegebenen Adresse primär eine MTP-Adresse ableiten. Diese Adresse wird durch den SI_{SCCP} und die Subsystemnummer SSN_{ISS} vervollständigt (vgl. Abschnitt 2.4.2).

Mit Hilfe netzinterner Server können auch Dienste zum Schutz der Kommunikationsbeziehung (vgl. Proxy-Dienst in Abschnitt 4.3.3) oder Anonymitätsdienste durch Verketten von Proxy-Servern [29] realisiert werden.

12 Innerhalb der ISDN-Supplementary Services [104] sind beispielsweise das EzE-Dienstmerkmal *Rückruf bei Besetzt* und die Realisierung geschlossener Benutzergruppen (CUG) basierend auf nutzkanalunabhängiger TCAP-Signalisierung spezifiziert.

5.3.2.3 Beispiel: Anfrage von Schlüsselzertifikaten bei zentralen Servern

Zur Abfrage gültiger Schlüsselzertifikate wird die in Bild 5-16 eingeführte Protokollarchitektur angewendet. Die SSS im Endgerät fordern die Zertifikate bei Bedarf über ein spezielles SSS-Dienstmerkmal (vgl. *FAC-IE(SSS,PzP,KeyReq,KS)* in Bild 5-17) an.

Der SSS-Dienst *Key-Retrieval* im rufenden Endgerät A schickt die Anforderung *KeyReq* für ein Schlüsselzertifikat zusammen mit der Adresse *KS* des Zertifikat-Servers im Dienstprimitiv *RegisterReq* zur Schicht 3. Die Nachricht wird zur TVSt übermittelt und dort aufgrund der *Facility*-Kodierung *SSS* von der Dienstmerkmalsteuerung an die SSS weitergegeben. Dort wird aufgrund der *PzP*-Dienstkodierung der PzP-Dienst adressiert, der zunächst die Adresse KS (z. B. SSS.KS.TTP-AG.de) auf eine Netzadresse (MTP_{KS} + SI_{SCCP}+ SSN_{ISS}) des ZGS Nr. 7 abbildet.[13] Danach wird innerhalb des PzP-Dienstes eine *SecPDU* erzeugt und über die SAL* an die ISS bzw. direkt an den TCAP weitergeleitet. Über den TCAP wird eine Zeichengabeassoziation zum Zertifikat-Server aufgebaut, über die die *SecPDU* übermittelt wird (vgl. *TC-Begin[Invoke(KeyReq)]* in Bild 5-17).

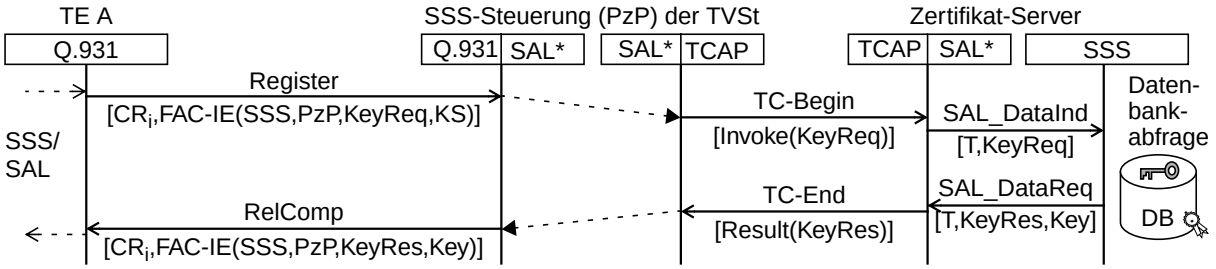


Bild 5-17: Abfrage von Zertifikaten über das ZGS Nr. 7

Innerhalb der *SAL** des Zertifikat-Servers wird die Anfrage mit dem Primitiv *SAL_DataInd* an die SSS-Steuerung weitergegeben, von wo aus die Datenbank angesprochen wird. Das angefragte Schlüsselzertifikat wird über das Primitiv *SAL_DataReq* zur SAL* übergeben, die dieses zusammen mit der Abbaunachricht für die Zeichengabe-Assoziation zur anfragenden TVSt weiterleitet (*TC-End[Result(KeyRes)]* in Bild 5-17). Die Adressierung der Zeichengabeassoziation wird im TCAP über die Transaktionsnummer *T* realisiert.

Schließlich wird das Schlüsselzertifikat im Rahmen des Abschlusses des Dienstmerkmales (*RelComp*-Nachricht) über die Benutzer-Netzschnittstelle zum Endgerät A übermittelt und dort über die SAL und die SSS an den KeyRetrieval-Dienst ausgeliefert.

Abgesehen von der Adressierung über die Transaktionsnummer T ist der Ablauf aus *Sicht der SSS* derselbe wie bei der Implementierung des Zertifikat-Servers als Endgerät (vgl. Anhang A.4.2). Aus *Sicht des ISDN* läuft ein Dienstmerkmal an der Benutzer-Netzschnittstelle (DSS1) ab, das eine Zeichengabetransaktion des TCAP anstößt. Dies entspricht etwa den Vorgängen bei der Abfrage von Datenbanken beim Location Management im GSM.

5.3.2.4 Netztechnische Bewertung der Auslagerung in zentrale Server

Der vorgestellte Ansatz ermöglicht die netzübergreifende Verfügbarkeit von Sicherheitsdiensten basierend auf existierenden Zeichengabeprotokollen des ZGS Nr. 7. Durch Ergänzen der Gateways an Netzgrenzen können *SecPDUs* auch über unterschiedliche Netze hinweg über-

13 Dazu kann beispielsweise der SCCP bzw. der darin enthaltene Global Title Translation Service genutzt werden.

mittelt werden. Damit werden v. a. netzunabhängige Sicherheitsanwendungen (Authentisierung etc.) unterstützt. Die netzübergreifend verfügbaren Sicherheitsdienste kann der Netzbetreiber durch Filtern von Zeichengabenachrichten wie bisher bestimmen (vgl. [29]).

Die Erweiterung des Anwenderteils für Dienstmerkmale im ISDN (ISS) um PzP- und EzE-Übermittlungs-Dienstmerkmale ermöglicht eine effiziente Implementierung des Übermittlungsdienstes für Sicherheitssteuerungsdaten. Für PzP- und EzE-Sicherheitsdienste ist die Netzinfrastruktur ausschließlich bezüglich der Verfügbarkeit der genutzten Übermittlungsdienste relevant. Der Aufwand für den Netzbetreiber bzw. Dienstanbieter ist vergleichbar mit dem Aufwand zur Einführung neuer ISDN-Dienstmerkmale.

Die Auslagerung von Sicherheitsfunktionen in zentrale Server kann aus drei Gründen notwendig oder sinnvoll sein:

- Die Implementierung der Funktionen ist aufwendig und verlangt deshalb einen hohen Bündelungsgewinn (z. B. Zertifikat-Server).
- Die geforderte Verfügbarkeit ist an einem ISDN-Teilnehmeranschluß nicht garantierbar.
- Die Implementierung ausschließlich in Endgeräten ist aufgrund der Randbedingungen für die Plazierung von Sicherheitsfunktionen nicht möglich (vgl. Proxy-Server zur Realisierung von Anonymitäts- oder Pseudonymitätsdiensten in Abschnitt 4.3.3).

5.3.2.5 Sicherheitstechnische Bewertung

Die erreichbare Sicherheit durch Auslagerung von Sicherheitsfunktionen ist dann vergleichbar mit der integrierten Variante, wenn der Kommunikationspfad zwischen den ausgelagerten Sicherheitsfunktionen (Zertifikat-Server) und dem eigentlichen Verwendungsort (z. B. Authentisierungsdienst im Endgerät) sicher ist. Dies kann durch Integration zusätzlicher Sicherheitsfunktionen garantiert werden, falls dieser Pfad nicht vollständig im geschützten Bereich (nach Bild 4-12) liegt[14].

Weiterhin muß der angesprochene Server bezüglich der Erbringung der Sicherheitsfunktionen gegenüber dem jeweiligen Benutzer vertrauenswürdig sein.

5.4 Einordnung und Abgrenzung existierender Ansätze

Die in dieser Arbeit entwickelte Sicherheitsarchitektur berücksichtigt einerseits Ergebnisse verwandter Arbeiten, grenzt sich andererseits aber auch klar gegen diese ab. Hier werden jene Ansätze angesprochen, die direkten Bezug zur vorliegenden Arbeit aufweisen.

Die Sicherheitslösungen, die im GSM und in IP-basierten Netzen eingesetzt werden bzw. für ATM-Netze spezifiziert sind, sind nicht unter der Prämisse der Benutzerorientierung erfolgt. Die Authentisierung im GSM beispielsweise dient vor allem dem Schutz der Netzbetreiber vor unautorisiertem Zugriff; die optionale Verschlüsselung der Nutzdaten auf der Luftschnittstelle ist durch den Netzbetreiber steuerbar und für den Teilnehmer i. a. nicht kontrollierbar. Die in IP-basierten Netzen eingesetzten Sicherheitsdienste und zugrundeliegenden Architekturen wurden in Abschnitt 3.5 vorgestellt. Eine Sicherheitsarchitektur liegt für IP-Dienste (IPSec [138]) vor. Entsprechende Sicherheitsdienste sind jedoch der Vermittlungs- und Transport-

14 Zertifikate sind i. a. während der Übertragung bezüglich der Integrität durch Zeitstempel, Gültigkeitszeitraum und Signatur der Zertifizierungsinstanz geschützt. Sind keine weiteren Sicherheitsanforderungen (Verfügbarkeit, Vertraulichkeit) gegeben, so ist zur Abholung von Zertifikaten kein zusätzlicher Sicherheitsdienst nötig.

Schicht zuzurechnen. Sie sind deshalb für den Benutzer nur schwer kontrollierbar und nachvollziehbar.

Das ATM-Forum arbeitet als Standardisierungs-Gremium schon viele Jahre an Erweiterungen der ATM-Signalisierung zur Unterstützung von Sicherheitsdiensten [72]. Neue Informationselemente zur Synchronisierung von Sicherheitsfunktionen wurden standardisiert. Das Ziel ist jedoch die Standardisierung von Schnittstellen. Die Implementierung von Sicherheitsdiensten innerhalb von Kommunikationssystemen wird nicht festgelegt.

Benutzerorientierte Sicherheitslösungen für das ISDN

Lösungen, die zu bestehender *ISDN-Infrastruktur kompatibel* sind, beschränken sich i. a. auf Ende-zu-Ende-Sicherheitsdienste für Nutzdaten (B-Kanal). Diese Dienste können innerhalb von Endgeräten transparent für das Netz implementiert werden (vgl. z. B. [39],[125]).

Im ISDN-Projekt S-CAPI (vgl. [33], [38]) wurde eine *Sicherheitsarchitektur erarbeitet, die in das ISDN-CAPI* (Common Application Programming Interface) in der Nutzer-Ebene integriert wurde. Diese Lösung ermöglicht eine Authentisierung der Kommunikationspartner und auch den Schutz von Nutzdaten, die über den B-Kanal übertragen werden. Die Architektur ist als Zwischenschicht in der Nutzer-Ebene implementiert. Die Sicherheitsfunktionen werden dabei nach dem Verbindungsaufbau über den B-Kanal ausgehandelt bzw. synchronisiert.

Die oben besprochenen Sicherheitslösungen werden bisher i. a. für geschlossene Benutzergruppen verwendet. Es lassen sich damit keine Informationen schützen, die im Rahmen der Diensterbringung in Netzknoten verarbeitet werden (z. B. Schutz der Kommunikationsbeziehung). Zukünftig können diese Lösungen als *Bearer Security Services* (von der Sicherheitsadaptionsschicht gesteuerte Zwischenschichten) die hier vorgestellte Sicherheitsarchitektur nutzen, bzw. durch sie gesteuert werden.

Die in [30] und [34] besprochenen Authentisierungsdienste werden im Zuge des Verbindungsaufbaus über den D-Kanal synchronisiert und erweitern, im Gegensatz zu den oben genannten Lösungen, die ISDN-Dienstesteuerung selbst. Diese Dienste sind den *Security Supplementary Services* zuzurechnen.

Das *North American ISDN User's Forum* (NIUF) veröffentlichte 1992 ein Dokument, welches mit „ISDN Security Architecture“ überschrieben ist [131]. Darin werden erstmals sogenannte Security Supplementary Services als ergänzende Dienste zur Sicherung von ISDN-Diensten angesprochen. Das Dokument beinhaltet Beschreibungen für (aus Benutzersicht) wünschenswerte Sicherheitsdienste. Es basiert auf ISO 7498-2 und schlägt ISDN-spezifische Authentisierungs-, Zugriffskontroll- und Vertraulichkeits-Dienste vor. Eine Architektur im hier definierten Sinne wird nicht ausgeführt.

Die in [37] und [43] und vielen weiteren Veröffentlichungen vorgestellten Arbeiten zur *Anonymität und Unbeobachtbarkeit* zielen auf den Schutz von Kommunikationsumständen ab. Dies kann nicht ausschließlich durch Ende-zu-Ende-Sicherheitsdienste erreicht werden, da ein Großteil der Umstandsdaten innerhalb des Netzes verarbeitet wird (z. B. Anschlußnummern der Kommunikationspartner oder die Tatsache, daß an einem Anschluß kommuniziert wird). Diese Ansätze erzwingen zur Realisierung meist eine weitreichende Änderung der bestehenden ISDN-Infrastruktur mindestens im teilnehmernahen Bereich. Die Ansätze sind in ihrer derzeitigen Form hauptsächlich für zukünftige Telekommunikationsnetze interessant.

Die in dieser Arbeit eingeführte Sicherheitsarchitektur stellt eine geeignete Plattform für Anonymitäts- und Pseudonymitätsdienste dar. Sie ermöglicht einen Kompromiß zwischen

erreichbarer Sicherheit und dem notwendigen Aufwand (z. B. Verschleierung eines Verbindungsaufbaus im ISDN in [29]).

Betreiberorientierte Sicherheitslösungen für das ISDN

Aus Sicht der Netzbetreiber oder Dienstanbieter stehen im ISDN bisher der Schutz der Netzinfrastruktur vor unautorisierter Dienstnutzung und die Netzintegrität im Vordergrund ([29],[35],[36],[40],[41],[42]). Dazu werden u. a. Filter-basierte Schutzmechanismen an Netzzugängen und Netzübergängen eingesetzt (vgl. z. B. ITU-Empfehlung Q.705, [101]). Die Gateways lassen nur bestimmte Informationselemente und Nachrichten an den Netzschnittstellen passieren und schützen so die netzinternen Knoten vor mißbräuchlichen oder aus Fehlern resultierenden, negativen externen Einflüssen. Sicherheitsdienste werden bis heute hauptsächlich zum Schutz der Netzfunktionen eingesetzt.

Wesentliche Neuerungen der hier vorgestellten Arbeit

Die in dieser Arbeit vorgestellte Sicherheitsarchitektur *strukturiert die Beziehungen zwischen Sicherheits- und Telekommunikationsfunktionen* auf neue Art und Weise. Sicherheitsdienste können damit *benutzerkontrolliert* und zu herkömmlichen ISDN-Diensten optional zugeschaltet oder unabhängig von bestehenden ISDN-Diensten aktiviert werden. Dies ermöglicht die Spezifikation von Schutzzielen für einzelne Dienste und Dienstnutzer und fördert die Kompatibilität von erweiterten Endgeräten mit herkömmlichen Endgeräten und bestehender Netzinfrastruktur.

Der hier vorgestellte Ansatz zielt auf die *geringstmögliche Abhängigkeit der Sicherheitsdienste von Telekommunikationsdiensten* ab. Benutzerorientierte Sicherheitsdienste und bestehende ISDN-Dienste werden in der Sicherheitsadaptionsschicht der Endgeräte explizit und benutzerkontrollierbar verzahnt. Dies unterstützt *nachvollziehbare Sicherheitsdienste* und eine offene Sicherheitsdienstschnittstelle. Die klare Trennung fördert darüberhinaus Möglichkeiten zur Auslagerung von Sicherheitsfunktionen in spezialisierte Ablaufumgebungen und eröffnet Abstraktionsmöglichkeiten bei der Bewertung von Sicherheitslösungen.

Kapitel 6

Zusammenfassung und Ausblick

6.1 Zusammenfassung der Ergebnisse

Die in dieser Arbeit vorgestellte Sicherheitsarchitektur ermöglicht die additive Erweiterung von Telekommunikationsinfrastruktur um Sicherheitsfunktionen. Diese Sicherheitsfunktionen werden entsprechend der zu garantierenden Schutzziele mit herkömmlichen Telekommunikationsdienstfunktionen verknüpft und ermöglichen somit sichere Telekommunikationsdienste.

Die Sicherheitsarchitektur unterstützt die Verläßlichkeit von Telekommunikationsdiensten durch die Kopplung mit Sicherheitsanwendungsdiensten und dem optionalen Zuschalten von Sicherheitsfunktionen in Zwischenschichten. Mehrseitig sichere Kommunikationsdienste werden durch Übermittlungsdienste für Aushandlungsdaten unterstützt. Die flexible und optionale Zuschaltung von Sicherheitsdiensten fördert die die Kontrolle der gegebenen Sicherheit durch den Benutzer.

Die Architekturkomponenten *Sicherheitsadaptionsschicht* und *Sicherheitsdienstesteuerung* lassen sich harmonisch in die bestehende Infrastruktur im ISDN einordnen. Die Zusammenfassung der Kopplung und der Synchronisierung von Sicherheitsfunktionen innerhalb der Sicherheitsadaptionsschicht ermöglicht eine wenig aufwendige Erweiterung von programmierbaren Endgeräten. Die Sicherheitsdienstesteuerung bietet sowohl eine Integrationsmöglichkeit für Sicherheitsanwendungsdienste als auch eine Schnittstelle zum Benutzer. Die Architektur fördert durch die Einführung eines netzunabhängigen Dienstzugangspunktes SAP^{Sec} netzübergreifende Sicherheitsdienste.

Die verschiedenen Varianten der Auslagerung von Sicherheitsarchitekturkomponenten ermöglichen netz- und geräteunabhängige Sicherheitsmodule zur Steuerung der Sicherheitsadaptionsschicht. Die Auslagerung in zentrale Netzknoten und der dadurch erzielbare Bündelungsgewinn rechtfertigen beispielsweise einen höheren Aufwand für sichere Laufzeitumgebungen und die Verwaltung großer Zertifikat-Server. Außerdem kann die Verfügbarkeit logisch zentraler Sicherheitsfunktionen – z. B. durch Spiegelserver – stark erhöht werden.

Diese Arbeit hat auch gezeigt, daß gezielte Erweiterungen der Kommunikationsnetze die Effektivität und Effizienz der Sicherheitsarchitektur entscheidend verbessern können. Dies gilt zum Beispiel für folgende Punkte:

- Ende-zu-Ende-Übermittlungsdienste für Sicherheitssteuerungsdaten

- Adressierungsmöglichkeiten für zentrale Server, d. h. Punkt-zu-Punkt-Übermittlungsdienste zur verbindungslosen Kommunikation mit Sicherheits-Servern (z. B. Public Key Infrastructure)
- Erweiterung des Netzzuganges um Sicherheitsdienstmerkmale zum Schutz vor Dienstemißbrauch (z. B. Ersetzen der Identifizieren-Funktion durch kryptographische Authentisierungsverfahren)

Wie diese Untersuchung zeigt, ist die Basis für entsprechende Erweiterungen im ISDN bereits vorhanden. Das Einführen dieser Dienstmerkmale ist eine Sache des Abwägens von Aufwand und Ertrag. Die technische Realisierbarkeit unter gleichzeitig garantiertem Investitionsschutz bestehender Netzinfrastruktur steht für das ISDN außer Frage.

6.2 Ausblick

In der Zukunft können die für einzelne Kommunikationsnetze verfügbaren Sicherheitsdienste netzübergreifend nutzbar und damit benutzerfreundlicher gemacht werden. Dazu müssen im GSM beispielsweise die netzunabhängigen Sicherheitsdienste (Authentisierung) von den Netzdiensten getrennt realisiert werden. Die netzspezifischen Dienste (Verschlüsselung der Luftschnittstelle) müssen für alle Betroffenen nachvollziehbar und steuerbar werden. Die vorgestellte Sicherheitsarchitektur unterstützt dieses, da die Schaltung und Kopplung der Sicherheitsdienste in einer für die Betroffenen vertrauenswürdigen Umgebung erfolgt.

Die Aushandlungsdienste des in IP-basierten Netzen populären Secure Socket Layer sowie die darin spezifizierte Verwaltung von Sicherheitsassoziationen lassen sich in die vorgestellte Sicherheitsarchitektur als *Security Supplementary Services* (Sicherheitsanwendungsdienste) integrieren. Die in der IPSec-Architektur spezifizierten erweiterten Header für Verschlüsselung und Authentisierung können auch im ISDN als Vorlage für *Security Bearer Services* in Zwischenschichten zum Schutz von Steuerungs- und Nutzdaten eingesetzt werden.

Insgesamt läßt sich feststellen, daß viele von Netzbetreibern und Dienstanbietern angebotenen Sicherheitsdienste i. a. nicht benutzerkontrollierbar und -steuerbar sind. Insbesondere für den Schutz von Kommunikationsumständen gibt es kaum befriedigende Lösungen. Dieses steht im Widerspruch zu der Tatsache, daß die Dienste *für* den Benutzer gemacht sind. Es kann heute durchaus der Eindruck entstehen, die Benutzer seien aus Sicherheitssicht dem Netzbetreiber und Dienstanbieter mehr verpflichtet, als dieser ihnen.

Es darf hier nicht verschwiegen werden, daß eine große Herausforderung darin besteht, die zu Beginn der Arbeit gemachten Voraussetzungen zu schaffen. Hierzu gehören nachvollziehbar sichere Ablaufumgebungen und Endgeräte, prüfbare Betriebssysteme und die Zertifizierung kontrollierter Software. Insbesondere die zunehmende Vernetzung (Internet) und die damit einhergehenden Dienste erschweren die Erzielung einer *nachhaltig* sicheren Laufzeitumgebung. Diese Probleme sind deshalb so schwer zu lösen, weil sie nicht nur von technischen und finanziellen sondern auch von politischen Faktoren abhängig sind.

Absolut sichere komplexe Systeme sind auch zukünftig nicht zu erwarten. Benutzer, Hersteller, Netzbetreiber oder Dienstanbieter werden in ihrer Unvollkommenheit immer als Angreifer bezüglich der (möglicherweise selbst formulierten) Schutzziele betrachtet werden müssen. Dieses ist bei der Verteilung von Aufgaben an automatisierte technische Systeme stets zu bedenken. Möglicherweise ist die Nachvollziehbarkeit – auch das Wissen um die Unvollkommenheiten – und die Kontrollierbarkeit der Technik schlußendlich wichtiger, als der Versuch der Annäherung absoluter Sicherheit. Schließlich hat die Technik den Menschen zu dienen.

Literatur

Veröffentlichungen

[1] R. Dierstein: Duale Sicherheit – IT-Sicherheit und ihre Besonderheiten. In G. Müller, A. Pfitzmann (Hrsg.): „Mehrseitige Sicherheit in der Kommunikationstechnik – Verfahren, Komponenten, Integration“, Addison-Wesley, 1997.

[2] A. Roßnagel, M. J. Schneider: Anforderungen an die mehrseitige Sicherheit in der Gesundheitsversorgung und ihre Erhebung. Informationstechnik und Technische Informatik it+ti, Heft 4, 1996.

[3] K. Rannenberg, A. Pfitzmann, G. Müller: Sicherheit, insbesondere mehrseitige IT-Sicherheit. In G. Müller, A. Pfitzmann (Hrsg.): „Mehrseitige Sicherheit in der Kommunikationstechnik – Verfahren, Komponenten, Integration“, Addison-Wesley, 1997.

[4] J. Bizer, V. Hammer, U. Pordesch: Gestaltungsvorschläge zur Verbesserung des Beweiswertes digital signierter Dokumente. Beiträge zur Informationssicherheit: Strategische Aspekte der Informationssicherheit und staatliche Reglementierung. Hartmut Pohl, Gerhard Weck (Hrsg.), Oldenburg, 1995.

[5] R. L. Rivest, A. Shamir, L. Adleman: A Method for Obtaining Digital Signatures and Public-Key Cryptosystems. Communications of the ACM, Volume 21, No. 2, February 1978.

[6] A. Roßnagel: Kritische Anmerkungen zum Entwurf eines Signaturgesetzes. In G. Müller, A. Pfitzmann (Hrsg.): „Mehrseitige Sicherheit in der Kommunikationstechnik – Verfahren, Komponenten, Integration“, Addison-Wesley, 1997.

[7] B. Preneel, R. Govaerts, J. Vandewalle: Information Authentication: Hash Functions and Digital Signatures. Lecture Notes in Computer Science 741, Computer Security and Industrial Cryptography - State of the Art and Evolution, Belgium, May 1991, Springer Verlag 1993.

[8] D. Chaum: Untraceable Electronic Mail, Return Addresses, and Digital Pseudonyms. Communications of the ACM 24/2 (1981).

[9] J. Saltzer, D. Reed, D. Clark: End-To-End Arguments in System Design. ACM Transactions on Computer Systems, Vol. 2, No. 4, November 1984, pp. 277 - 288.

[10] R. J. Anderson: Why Cryptosystems Fail. Communications of the ACM, Vol. 37, No. 11, November, 1994.

[11] M. Kabatnik: Möglichkeiten des Zugangs zu PKI-Diensten für Anwender der SS7-Infrastruktur des ISDN. Im Tagungsband: 6. Deutscher IT-Sicherheitskongreß des BSI 1999.

[12] J. H. Moore: Protocol Failures in Cryptosystems. Proceedings of the IEEE, Vol. 76, No. 5, May, 1988.

[13] G. Tsudik: Message Authentication with One-Way Hash Functions. ACM Computer Communication Review, Vol. 22, No. 5, October, 1992.

[14] V. L. Voydock, S. T. Kent: Security Mechanisms in High-Level Network Protocols. Computing Surveys, Vol. 15, No. 2, June, 1983.

[15] A. Pfitzmann, B. Pfitzmann, M. Schunter, M. Waidner. Trusting Mobile User Devices and Security Modules. IEEE Computer, February 1997.

[16] R. Anderson, M. Kuhn. Tamper Resistance - a Cautionary Note. Proc. of the 2nd Workshop On Electronic Commerce, California, November 1996.

[17] M. Blaze, W. Diffie, R. L. Rivest, B. Schneier, T. Shimomura, E. Thomson, M. Wiener: Minimal Key Lenghts For Symmetric Ciphers To Provide Adequate Commercial Security. ftp://ftp.research.att.com/dist/mab/keylength.ps, 1996.

[18] M. Abadi, R. Needham: Prudent Engineering Practice for Cryptographic Protocols. Digital, Research Report No. 125, Palo Alto, California, June 1994.

[19] B. C. Neuman, S. G. Stubblebine: A Note on the Use of Timestamps as Nonces. ACM Operating Systems Review, Vol. 27, No. 2, April 1993.

[20] H. Damker, K. Rannenberg, G. Müller: Erreichbarkeitsmanagement und mehrseitige Sicherheit aus Benutzersicht. 4. Deutscher IT-Sicherheitskongreß des Bundesamtes für Sicherheit in der Informationstechnikl, BSI-Druckschrift 7165, Bonn, Mai 1995.

[21] H. Damker, U. Pordesch, K. Rannenberg, M. Schneider: Aushandlung mehrseitiger Sicherheit – Der Erreichbarkeits- und Sicherheitsmanager. In G. Müller, K.-H. Stapf (Hrsg.): „Mehrseitige Sicherheit in der Kommunikationstechnik – Erwartung, Akzeptanz, Nutzung“, Addison-Wesley, 1999.

[22] T. Y. C. Woo, S. S. Lam: A lesson on Authentication Protocol Design. ACM Operating Systems Review, Vol. 28, No. 3, July 1994.

[23] A. Pfitzmann, A. Schill, A. Westfeld, G. Wicke, G. Wolf, J. Zöllner: Flexible mehrseitige Sicherheit für verteilte Anwendungen. In: R. Steinmetz (Hrsg.): Kommunikation in Verteilten Systemen (KiVS), März 1999.

[24] B. Miller: Vital signs of identity. IEEE Spectrum, February 1994.

[25] R. Sailer: Authentikation als Grundlage der Skalierung von Sicherheit in der Kommunikationstechnik. Tagungsband Kommunikation in Verteilten Systemen 1997, Springer-Verlag 1997.

[26] R. Sailer, P. Kühn: Ein Domain-Konzept zur systematischen und wirtschaftlichen Integration von Sicherheit in Kommunikationsnetze. Informationstechnik und Technische Informatik, 38. Jahrgang, Heft 4, 1996.

[27] R. Sailer, P. J. Kühn: Integration von Authentikationsverfahren in Kommunikationsnetze unter Verwendung separat sicherbarer Bereiche. In G. Müller, A. Pfitzmann (Hrsg.): „Mehrseitige Sicherheit in der Kommunikationstechnik – Verfahren, Komponenten, Integration“, Addison-Wesley, 1997.

[28] R. Sailer: An Evolutionary Approach to Multilaterally Secure Services in ISDN /IN. Proceedings of the Seventh International Conference on Computer Communications and Networks, IEEE Society Press, 1998.

[29] R. Sailer: Security Services in an Open Service Environment. Proceedings of the Fourteenth Annual Computer Security Applications Conference, IEEE Society Press, 1998.

[30] R. Sailer: Integrating Authentication into Existing Protocols. Proceedings of the Fifth Open Workshop on High Speed Networks, 1996.

[31] S. Smith, S. Weingart: Building a High-Performance, Programmable Secure Coprocessor. IBM Research Report RC21102(94393), IBM Research Division, T. J. Watson Research Center, Yorktown Heights, New York, February 1998.

[32] International Business Machines Corporation: IBM 4758 PCI Cryptographic Coprocessor, Dezember 1998.

[33] D. Dienst, D. Fox, C. Ruland: Transparente Sicherheitsmechanismen für ISDN-Anwendungen. ITG-Fachbericht 131, November 1994.

[34] T.-K. Kwon, J.-S. Song: A Key Distribution And Authentication Method On The Q.931 Calling Sequence of ISDN. Proceedings of the Twelfth International Conference On Computer Communication (ICCC), Korea, August 1995.

[35] B. Kowalski: Security Management System SMS. Der Fernmelde-Ingenieur, April/Mai 1995.

[36] W. Muhl, H. Stolz: Sicherheitsarchitekturen und -konzepte für Telekommunikationsnetze. Der Fernmelde-Ingenieur, Juni/Juli 1994.

[37] A. Pfitzmann, B. Pfitzmann, M. Waidner: Telefon-MIXe: Schutz der Vermittlungsdaten für zwei 64-kbit/s-Duplexkanäle über den (2*64+16)-kbit/s-Teilnehmeranschluß. Datenschutz und Datensicherung (DuD), 12, 1989.

[38] C. Ruland: Sichere Kommunikation zwischen ISDN-Endgeräten. DATACOM, Heft 1, 1995.

[39] K. Tanaka, I. Oyaizu: A Confidentiality System for ISDN inter-PC High-Speed File Transfer. IEEE INFOCOM ‘94, 1994.

[40] R. Kuhn, P. Edfors, V. Howard, C. Caputo, T. S. Phillips, A. Booz, H. Booz: Improving Public Switched Network Security in an Open Environment. IEEE Computer, August, 1993.

[41] P. Halliden: Network security issues. Computer Communications, Vol. 13, No. 10, December 1990.

[42] K. Ward: The Impact of Network Interconnection on Network Integrity. British Telecommunications Engineering, Vol. 13, January, 1995.

[43] A. Jerichow, J. Müller, A. Pfitzmann, B. Pfitzmann, M. Waidner: Real-Time Mixes: A Bandwidth-Efficient Anonymity Protocol. IEEE Journal On Selected Areas In Communications, Vol. 16, No. 4, May 1998.

[44] R. Sailer, H. Federrath, A. Pfitzmann: Security Functions in Telecommunications – Placement & Achievable Security. In: G. Müller, K. Rannenberg [Eds.] Multilateral Security for Global Communication. Addison-Wesley-Longman, 1999.

[45] D. E. Denning, P. F. MacDoran: Location-based System Delivers User Authentication Breakthrough. Computer Security Institute, 1996.

Allgemeine Literatur

[46] P. J. Kühn: Technische Informatik III – Kommunikationsnetze. Skriptum zur gleichnamigen Vorlesung, Institut für Nachrichtenvermittlung und Datenverarbeitung, Universität Stuttgart, 1997/1998.

[47] G. Bandow, H. Gottschalk, D. Gehrmann, W. Hlavac, H. Koch, W. Müller, D. Schwetje: Zeichengabesysteme - Eine neue Generation für ISDN und intelligente Netze. L.T.U. - Vertriebsgesellschaft mbH, Bremen, 2. Auflage, 1995.

[48] H. Wettstein: Systemarchitektur. Hanser Studienbücher der Informatik, 1993.

[49] A. Roßnagel, P. Wedde, V. Hammer, U. Pordesch: Die Verletzlichkeit der Informationsgesellschaft. Schriftenreihe Sozialverträgliche Technikgestaltung, Band 5, Westdeutscher Verlag, 1990.

[50] V. Hammer (Hrsg.), M. J. Schneider, A. Roßnagel, J. Bizer, C. Kumbruck, U. Pordesch: Sicherheitsinfrastrukturen – Gestaltungsvorschläge für Technik, Organisation und Recht. Springer Verlag 1995.

[51] A. Pfitzmann: Diensteintegrierende Kommunikationsnetze mit teilnehmerprüfbarem Datenschutz. Informatik Fachberichte 234, Springer-Verlag, 1990.

[52] B. Schneier: Applied Cryptography - Protocols, Algorithms, and Source Code in C. Second Edition, John Wiley & Sons 1996.

[53] A. Menezes, P. v. Oorschot, S. Vanstone: Handbook of Applied Cryptography. CRC Press, 1996.

[54] W. Ford: Computer communications security. Prentice Hall P T R, Englewood Cliffs, New Jersey, 1994.

[55] S. Muftic, A. Patel, P. Sanders, R. Colon, J. Heijinsdijk, U. Pulkkinen: Security Architecture For Open Distributed Systems. John Wiley & Sons 1993.

[56] M. - Th. Tinnefeld, E. Ehmann: Einführung in das Datenschutzrecht. Oldenbourg, 1992.

[57] BfD: Bundesdatenschutzgesetz – Text und Erläuterung. Bundesbeauftragter für den Datenschutz (Hrsg.), Bonn, 1991.

[58] Der Hamburger Datenschutzbeauftragte (Hrsg.): Datenschutz bei Multimedia und Telekommunikation. Hamburger Datenschutzhefte, Hamburg, 1997.

[59] W. Bieser: Begründung und Überlegungen zum Signaturgesetz. In G. Müller, A. Pfitzmann (Hrsg.): „Mehrseitige Sicherheit in der Kommunikationstechnik – Verfahren, Komponenten, Integration“, Addison-Wesley, 1997.

[60] David Kahn: The Codebreakers – The Comprehensive History of Secret Communication from Ancient Times to the Internet. New York: Scribner, 1996.

[61] D. E. R. Denning: Cryptography and Data Security. Addison-Wesley, 1983.

[62] D. W. Davies, W. L. Price: Security for Computer Networks. 2nd ed., Wiley series in communication and distributed systems, 1989.

[63] A. Beutelspacher, J. Schwenk, K.-D. Wolfenstetter: Moderne Verfahren der Kryptographie. Vieweg 1995.

[64] T. Hermann: Vergleichende Bewertung von Verfahren zur Benutzerauthentikation. Dissertationsschrift, Shaker Verlag GmbH, 1998.

[65] B. Klein: Authentikationsdienste für sichere Informationssysteme. Dissertationsschrift, Universität Karlsruhe, 1993.

[66] W. Fumy, G. Meister, M. Reitenspieß, W. Schäfer (Hrsg.): Sicherheitsschnittstellen – Konzepte, Anwendungen und Einsatzbeispiele. Proceedings des Workshops: Security Application Programming Inerfaces ‘94. München, November 1994.

[67] M. Hendry: Smart Card Security and Applications. Artech House, 1997.

[68] W. Cheswick, S. Bellovin: Firewalls and Internet Security, Addison-Wesley 1994.

[69] A. Olsen, B. Möller-Pedersen, R. Reed, J. R. W. Smith: Systems Engineering Using SDL-92. Elsevier Science B. V., 1994.

[70] Telelogic: SDT Methodology Guidelines, Tau 3.5. Telelogic AB, Sweden, March 1999.

[71] M. Hoh: Implementierung der Komponenten einer Sicherheitsarchitektur für offene Sicherheitsdienste im ISDN. Studienarbeit am Institut für Nachrichtenvermittlung und Datenverarbeitung, Universität Stuttgart, 1999.

Normen, Empfehlungen und vergleichbare Dokumente

[72] ATM Security Specification – Version 1.0 (Draft). ATM Forum BTD-Security-01.04, September 1997.

[73] Bundesamt für Sicherheit in der Informationstechnik. IT-Grundschutzhandbuch 1996 – Maßnahmen für den mittleren Schutzbedarf. Schriftenreihe zur IT-Sicherheit, Band 3. Bonn: Bundesanzeiger, 1996.

[74] Bundesamt für Sicherheit in der Informationstechnik. IT-Sicherheit durch infrastrukturelle Maßnahmen. Schriftenreihe zur IT-Sicherheit, Band 8. Bonn: Bundesanzeiger, 1997.

[75] Bundesamt für Sicherheit in der Informationstechnik. IT-Sicherheitshandbuch – Handbuch für die sichere Anwendung der Informationstechnik. BSI 7105, Bonn: Bundesdruckerei, 1992.

[76] CT-API 1.1: Anwendungsunabhängiges Card Terminal Application Programming Interface für Chipkartenanwendungen. Deutsche Telekom AG, GMD-Forschungszentrum Informationstechnik GmbH, TÜV Informationstechnik GmbH, TeleTrust Deutschland e. V., Stand 30. Oktober 1996.

[77] DTS/TIPHON-03004: Telecommunications and Internet Protocol Harmonization Over Networks (TIPHON); Interoperable Security Profiles. Draft Technical Specification, V1.1.0, October 1998.

[78] ETS 300 374-1: Intelligent Network (IN); Intelligent Network Capability Set 1 (CS1); Core Intelligent Network Application Protocol (INAP); Part 1: Protocol Specification. European Telecommunications Standards Institute, September 1994.

[79] European Telecommunications Standards Institute: Security Technique Advisory Group (STAG); Security requirements capture. TCR-TR 049, Juli 1996.

[80] FTZ 1 TR 6: Kennzeichenaustausch zwischen DIVO(ISDN)-Vermittlungsstellen und ISDN-Teilnehmereinrichtungen – ISDN-D-Kanal-Protokoll (Schicht 2 und 3). Fernmeldetechnisches Zentralamt, Deutsche Bundespost, Ausgabe 1.90.

[81] FTZ 1 TR 220: Spezifikation der ISDN-Schnittstelle U_{k0} Schicht 1. Deutsche Bundespost Telekom, Fernmeldetechnisches Zentralamt, Referat N13, März 1987.

[82] FTZ 163 TR 73: Anwendungsspezifikation für das Zeichengabesystem Nr. 7 – Steuerteil für Zeichengabeverbindungen (SCCP). Deutsche Bundespost Telekom, Forschungs- und Technologiezentrum Referat F46, April 1993.

[83] FTZ 163 TR 78: Spezifikation der Deutschen Bundespost Telekom für das Zeichengabesystem Nr. 7 – Intelligent Nework Application Protocol (INAP). Deutsche Bundespost Telekom, Forschungs- und Technologiezentrum Referat F46, April 1993.

[84] ISO 3309: Data Communication – High-level data link control procedures – Frame structure. International Organization For Standardization.

[85] ISO 4335: Data Communication – High-level data link control procedures – Consolidation of elements of procedures. International Organization For Standardization.

[86] ISO 7498: Information Processing Systems – Open Systems Interconnection – Basic Reference Model. International Organization For Standardization.

[87] ISO 7498-2: Information Processing Systems – Open Systems Interconnection – Basic Reference Model – Part 2: Security Architecture.

[88] ISO 8372: Modes of Operation for a 64-bit block cipher algorithm. Information Processing, International Standard, International Organization for Standardization, Geneva, 1987.

[89] ISO/IEC 10736: Information Technology – Telecommunications And Information Exchange Between Systems – Transport Layer Security Protocol. 1995.

[90] ISO/IEC 11577: Information Technology – Telecommunications And Information Exchange Between Systems – Network Layer Security Protocol (NLSP). 1995.

[91] ITU-T Recommendation H.235: Infrastructure of audiovisual services – Systems aspects: Security and encryption for H-Series multimedia terminals. International Telecommunication Union 1998.

[92] ITU-T Recommendation I.230: Integrated Services Digital Network – General Structures and Service Capabilities – Bearer Services Supported By An ISDN. International Telecommunication Union 1988.

[93] ITU-T Recommendation I.240: Integrated Services Digital Network – General Structures and Service Capabilities – Teleservices Supported By An ISDN. International Telecommunication Union 1988.

[94] ITU-T Recommendation I.250: Integrated Services Digital Network – General Structures and Service Capabilities – Supplementary Services In ISDN. International Telecommunication Union 1988.

[95] ITU-T Recommendation I.320: ISDN Protocol Reference Model. International Telecommunication Union 1993.

[96] ITU-T Recommendation I.411: ISDN User-Network Interfaces – Reference Configurations. International Telecommunication Union 1993.

[97] ITU-T Recommendation I.430: ISDN User-Network Interfaces – Layer 1 Specification. Annex E: Vocabulary of terms used in connection with Recommendations I.430, I.431, G. 960 and G.961. International Telecommunication Union 1988.

[98] ITU-T Recommendation Q.72: General Recommendations On Telephone Switching And Signalling – Functions And Information Flows For Services In The ISDN – Stage 2 Description For Packet Mode. International Telecommunication Union 1993.

[99] ITU-T Recommendation Q.80: General Recommendations On Telephone Switching And Signalling – Functions And Information Flows For Services In The ISDN – Introduction To Stage 2 Descriptions For Supplementary Services. International Telecommunication Union 1998.

[100] ITU-T Recommendation Q.512: Digital Exchanges – Digital Exchange Interfaces For Subscriber Access. International Telecommunication Union 1995.

[101] ITU-T Recommendation Q.700: Specifications Of Signalling System Number 7 – Introduction To CCITT Signalling System No. 7. International Telecommunication Union 1993.

[102] ITU-T Recommendation Q.704: Specifications Of Signalling System No. 7 – Message Transfer Part – Signalling Network Functions And Messages. Clause 14: Common Characteristics Of Message Signal Unit Formats. International Telecommunication Union 1996.

[103] ITU-T Recommendation Q.713: Specifications Of Signalling System No. 7 – Signalling connection Control Part (SCCP) – Signalling Connection Control Part Formats And Codes. International Telecommunication Union 1996.

[104] ITU-T Recommendation Q.730: Specifications Of Signalling System No. 7 – ISDN Supplementary Services. International Telecommunication Union 1993.

[105] ITU-T Recommendation Q.761: Specifications Of Signalling System No. 7 – Functional Description Of The ISDN User Part Of Signalling System No. 7. International Telecommunication Union 1993.

[106] ITU-T Recommendation Q.920: Digital Subscriber Signalling System No. 1 (DSS1) – ISDN User-Network Interface Data Link Layer – General Aspects. International Telecommunication Union 1993.

[107] ITU-T Recommendation Q.921: Digital Subscriber Signalling System No. 1 (DSS1) – ISDN User-Network Interface Data Link Layer Specification. International Telecommunication Union 1993.

[108] ITU-T Recommendation Q.930: Digital Subscriber Signalling System No. 1 (DSS1) – ISDN User-Network Interface Layer 3 – General Aspects. International Telecommunication Union 1993.

[109] ITU-T Recommendation Q.931: Digital Subscriber Signalling System No. 1 (DSS1) – ISDN User-Network Interface Layer 3 – Specification For Basic Call Control. International Telecommunication Union 1993.

[110] ITU-T Recommendation Q.931 Annex H: Message Segmentation Procedures. International Telecommunication Union 1993.

[111] ITU-T Recommendation Q.932: Digital Subscriber Signalling System No. 1 (DSS1) – Generic Procedures For The Control Of ISDN Supplementary Services. International Telecommunication Union 1993.

[112] ITU-T Recommendation Q.950: Digital Subscriber Signalling System No. 1 (DSS1) – Stage 3 Description For Supplementary Services Using DSS1 – Supplementary Services Protocols, Structure And General Principles. International Telecommunication Union 1993.

[113] ITU-T Recommendation Q.957.1: Digital Subscriber Signalling System No. 1 (DSS1) – Stage 3 Description for Additional Information Transfer Supplementary Services Using DSS1: User-to-User Signalling (UUS). International Telecommunication Union 1996.

[114] ITU-T Recommendation Q.1200: General Recommendations On Telephone Switching And Signalling – Intelligent Network. Q-Series Intelligent Network Recommendation Structure. International Telecommunication Union 1993.

[115] ITU-T Recommendation X.200: Data Networks And Open System Communications: Information Technology – Open Systems Interconnection – Basic Reference Model: The Basic Model. International Telecommunication Union 1994.

[116] ITU-T Recommendation X.509: The Directory: Authentication Framework. International Telecommunication Union 1993. – Identical text published as ISO/IEC International Standard 9594-8.

[117] ITU-T Recommendation X.700: Management Framework for Open Systems Interconnection (OSI) for CCITT applications. International Telecommunication Union 1992.

[118] ITU-T Recommendation X.800: Data Communication Networks: Open Systems Interconnection (OSI); Security, Structure and Applications – Security Architecture For Open Systems Interconnection For CCITT Applications. International Telecommunication Union 1991.

[119] ITU-T Recommendation X.802: Data Networks And Open System Communications Security; Information Technology – Open Systems Interconnection – Lower Layers Security Model. International Telecommunication Union 1995. Identical text published as ISO/IEC International Standard 13594.

[120] ITU-T Recommendation X.803: Data Networks And Open System Communications Security; Information Technology – Open Systems Interconnection – Upper Layers Security Model. International Telecommunication Union 1994. Identical text published as ISO/IEC International Standard 10745.

[121] ITU-T Recommendation X.810: Security Frameworks For Open Systems: Overview. International Telecommunication Union 1995.

[122] ITU-T Recommendation X.811: Security Frame works For Open Systems: Authentication Framework. International Telecommunication Union 1995.

[123] IuKDG: Gesetz zur Regelung der Rahmenbedingungen für Informations- und Kommunikationsdienste. Vom 22. Juli 1997 (BGBl. I S.1870).

[124] NIST Special Publication 800-7: Security in Open Systems. National Institute of Standards and Technology 1994.

[125] NIST Special Publication No. 500-189: Security in ISDN. W. E. Burr, National Institute of Standards and Technology 1991.

[126] NIST Special Publication No. 800-15: Minimum Interoperability Specification for PKI Components (MISPC), Version 1, National Institute of Standards and Technology 1998.

[127] RFC 1308: Executive Introduction to Directory Services Using the X.500 Protocol. C. Weider, J. Reynolds. March 1992. (Status: Informational)

[128] RFC 1035: Domain names – implementation and specification. P. V. Mockapetris. Nov-01-1987. (Status: Standard)

[129] The SSL Protocol – Version 3.0. Netscape Communications Corporation 1996.

[130] IEEE 802.10: Interoperable LAN / MAN Security. IEEE Standards for Local and Metropolitan Area Networks 1992.

[131] NIUF 412-92: ISDN Security Architecture. North American ISDN User's Forum (NIUF), October 1992.

[132] RFC 0793: Transmission Control Protocol. J. Postel. Sep-01-1981. (Status: Standard)

[133] RFC 0791: Internet Protocol. J. Postel. Sep-01-1981. (Status: Standard)

[134] RFC 1718: The Tao of IETF - A Guide for New Attendees of the Internet Engineering Task Force. The IETF Secretariat & G. Malkin. November 1994. (Status: Informational)

[135] RFC 2104: HMAC – Keyed-Hashing for Message Authentication. H. Krawczyk, M. Bellare, R. Canetti. February 1997. (Status: Informational)

[136] RFC 2460: Internet Protocol, Version 6 (IPv6) Specification. S. Deering, R. Hinden. December 1998. (Status: Draft Standard)

[137] RFC 2458: Toward the PSTN/Internet Inter-Networking – Pre-PINT Implementations. H. Lu et. al. November 1998. (Status: Informational)

[138] R. Atkinson: RFC 1825 Security Architecture for the Internet Protocol. RFC 1826 IP Authentication Header. RFC 1827 IP Encapsulating Security Payload (ESP). 1995.

[139] SigV: Verordnung zur digitalen Signatur. In der Fassung des Beschlusses der Bundesregierung vom 8. Oktober 1997.

Abbildungsverzeichnis

Bild 1-1: Beziehungen zwischen TK- und Sicherheitsfunktionen und Benutzern 2
Bild 2-1: Strukturierung der Empfehlungen der ITU zum ISDN 6
Bild 2-2: Wirkungsbereich von Übermittlungsdiensten und Telediensten [46] 7
Bild 2-3: Funktionsgruppen und Referenzpunkte am ISDN-Basisanschluß 9
Bild 2-4: Referenz-Konfigurationen am ISDN-Teilnehmeranschluß 10
Bild 2-5: ISDN-Referenzmodell – Ebenen und Funktionsschichten [95] 12
Bild 2-6: Zeichengabe- und Nutzkanal-Netz im ISDN 13
Bild 2-7: Zeichengabeprotokolle am Teilnehmeranschluß im ISDN 15
Bild 2-8: Dienste und Dienstprimitive der Schicht 2 des ISDN-D-Kanals nach Q.921 16
Bild 2-9: Dienstprimitive und PDUs zum Verbindungsaufbau nach Q.931 17
Bild 2-10: Aufbau von Protokolldateneinheiten nach Q.931 18
Bild 2-11: Funktionsschichten und Protokolle des ZGS Nr. 7 23
Bild 2-12: Funktionsgruppen und Zeichengabe-Schnittstellen des Intelligenten Netzes 26
Bild 3-1: Substitutionseffekt aus dem Blickwinkel dualer Sicherheit 32
Bild 3-2: Szenario eines Datenbankzugriffes mit unterschiedlichen Schutzzielen 34
Bild 3-3: Systemzentrierte Klassifizierung von Bedrohungen – Bedrohungsmodell 40
Bild 3-4: Bausteine einer Sicherheitsarchitektur 43
Bild 3-5: Echtheitsnachweis mit Hilfe symmetrischer Kryptosysteme 49
Bild 3-6: Echtheitsnachweis mit Hilfe asymmetrischer Kryptosysteme 50
Bild 3-7: Echtheitsnachweis mit Hilfe hybrider Verfahren 52
Bild 3-8: Sicherheitsstandards der ITU 54
Bild 3-9: SSL und IPsec in IP-basierten Netzen 56
Bild 4-1: Additiver Ansatz zur Realisierung von Sicherheitsdiensten 60
Bild 4-2: Freiheitsgrade bei der Plazierung von Funktionen im Teilnehmerbereich 63
Bild 4-3: Integration von Sicherheitsfunktionen in Kommunikationssysteme 63
Bild 4-4: Transparenz additiver Sicherheitsfunktionen 64
Bild 4-5: Klassifizierung von kooperierenden Sicherheitsfunktionen 66
Bild 4-6: Herleitung von Grenzlinien für EzE- und PzP-Sicherheitsfunktionen 67
Bild 4-7: EzE-, PzP und Ll-Grenzlinien 68
Bild 4-8: Angriffspunkte – erreichbare Sicherheit 69
Bild 4-9: Nutzer-Ebene im ISDN 71

Bild 4-10: Sicherheits-Gaps der Steuerungs-Ebene im ISDN aus Benutzersicht 71
Bild 4-11: PzP-Annäherung von EzE-Sicherheit 72
Bild 4-12: Effektive EzE-Grenzlinie unter Berücksichtigung von Zwischensystemen 73
Bild 4-13: Auslagerung von Sicherheitsfunktionen 75
Bild 4-14: Generische Dienstschnittstelle für Authentisierungsdienste 78
Bild 4-15: Signalisierungs-Zeitdiagramm einer Authentisierung nach X.509 79
Bild 4-16: Erweiterte Dienstzugangspunkte für transparente Zwischenschichten 82
Bild 4-17: Eine Zwischenschicht zur Verschlüsselung und zum Integritätsschutz 83
Bild 4-18: Schutz von Kommunikationsbeziehungen durch Anonymitätsgruppen 85
Bild 4-19: Komponenten einer Plattform für mehrseitig sichere Dienste 87
Bild 4-20: Beispiele für Sicherheitsassoziationen 90
Bild 4-21: Verfeinerte Struktur der Sicherheitsdienstesteuerung 91
Bild 4-22: Kopplung von Sicherheits- und Telekommunikationsdienst 92
Bild 4-23: Strukturierung der Sicherheitsadaptionsschicht in der Dienstesteuerungsebene .. 94
Bild 4-24: Kopplung von Authentisierung und Verbindungsaufbau im ISDN 97
Bild 5-1: Universelle Sicherheitsdienste 102
Bild 5-2: Übermittlung von Sicherheitssteuerungsinformation 102
Bild 5-3: Ende-zu-Ende-Sicherheitsdienste zwischen ISDN-Endgeräten 103
Bild 5-4: Sicherheitsarchitektur für ISDN-Endgeräte 104
Bild 5-5: Dienstschnittstellen der Sicherheitsarchitektur 105
Bild 5-6: Austausch von Steuerinformation für Ende-zu-Ende-Sicherheitsdienste 106
Bild 5-7: Austausch von Steuerinformation an der Benutzer-Netzschnittstelle 108
Bild 5-8: Erweitertes Funktionales Referenzmodell basierend auf Q.932 109
Bild 5-9: UNI-Authentisierung beim Verbindungsaufbau 113
Bild 5-10: Implementierung der Sicherheitsarchitektur in Endgeräten 115
Bild 5-11: Verbesserter Ende-zu-Ende-Übermittlungsdienst 117
Bild 5-12: Angriffspunkte bezüglich der Sicherheitsarchitektur in der Steuerungsebene ... 119
Bild 5-13: Auslagerung der Sicherheitsdienstesteuerung 121
Bild 5-14: Auslagerung der gesamten Sicherheitsarchitektur 122
Bild 5-15: Einordnung von Sicherheitsdiensten basierend auf Bild 2-2 123
Bild 5-16: Sicherheitsarchitektur basierend auf dem ZGS Nr. 7 124
Bild 5-17: Abfrage von Zertifikaten über das ZGS Nr. 7 125

Anhang

Beispiele zur Spezifikation und Implementierung

A.1 SDL-Blockdiagramm der Sicherheitsarchitektur im Endgerät

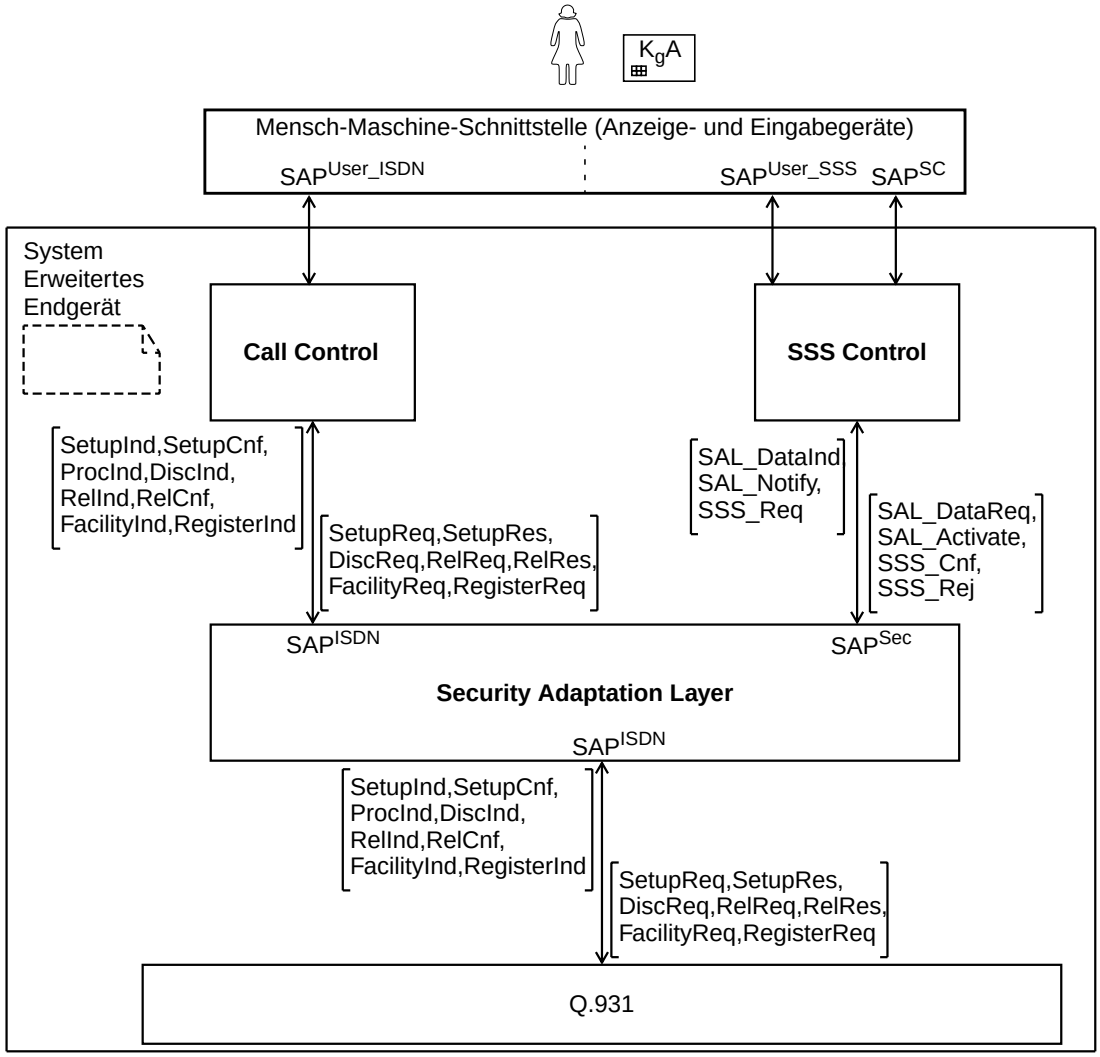


Bild A-1: SDL-Systemdiagramm der Sicherheitsarchitektur eines Endgerätes

A.2 Spezifikation der Sicherheitsadaptionsschicht

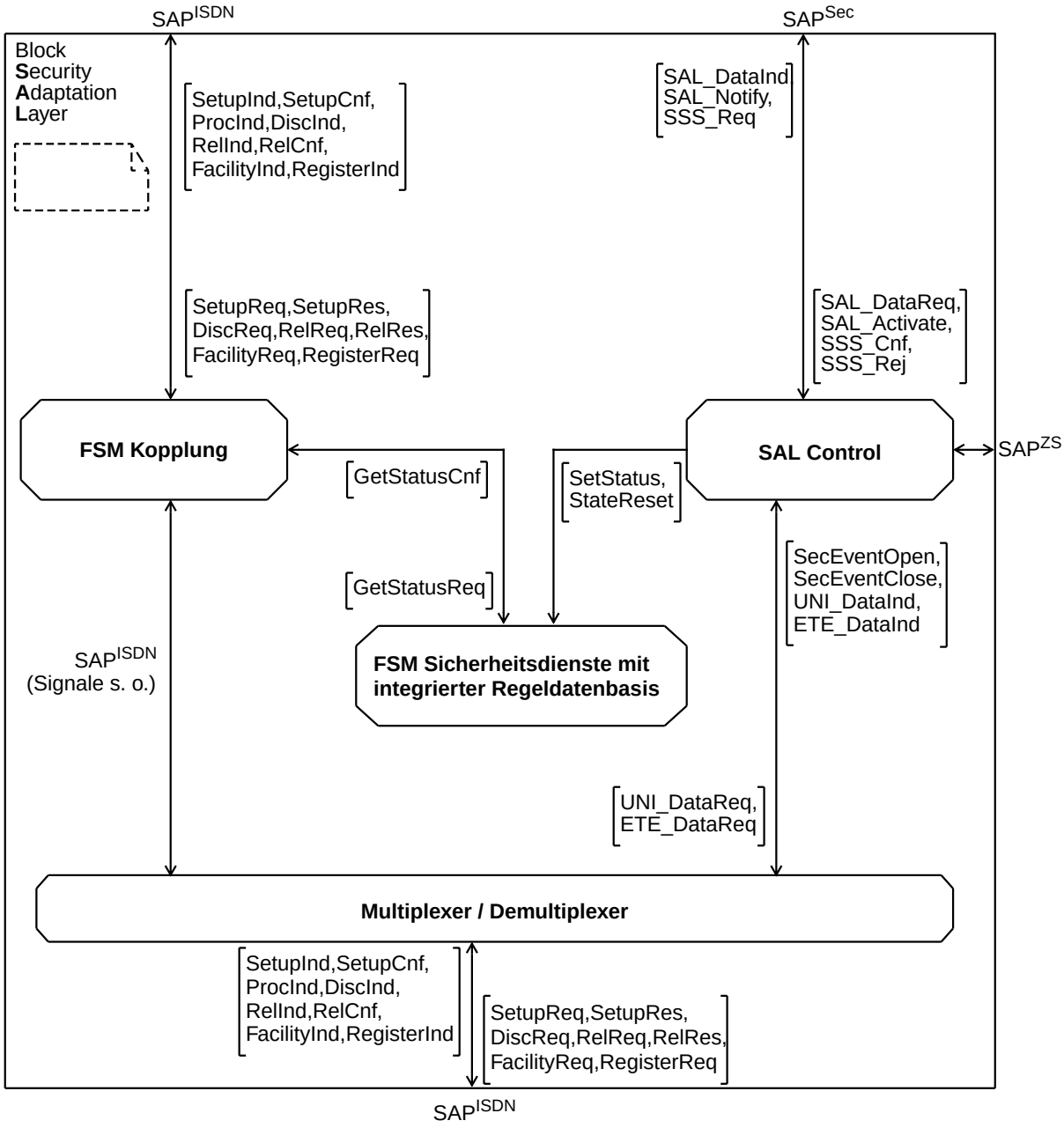


Bild A-2: SDL-Bockdiagramm der Adaptionsschicht SAL (vgl. Bild 4-23)

A.3 Spezifikation der Sicherheitsdienstesteuerung

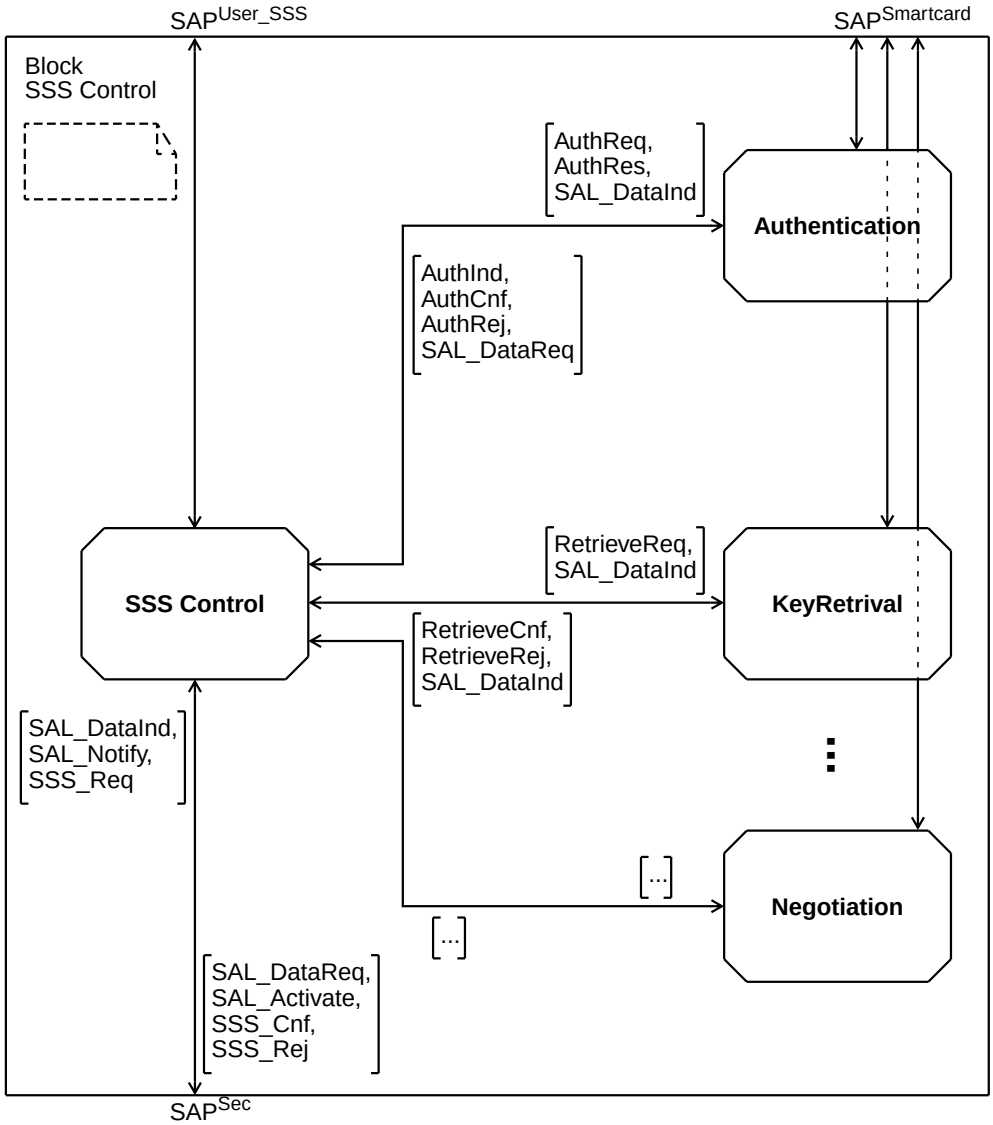


Bild A-3: SDL-Blockdiagramm der Sicherheitsdienstesteuerung (vgl. Bild 4-21)

A.4 Signalisierungs-Zeitdiagramme

A.4.1 Aushandlung von Schutzzielen

Die Aushandlung von Schutzzielen ist durch die an einem Dienst beteiligten Personen durchzuführen. Für den Netzbetreiber bzw. Dienstanbieter kann diese Aushandlung auch automatisiert werden. Bild A-4 zeigt eine einfache, zweistufige Aushandlung von Schutzzielen zwischen den Teilnehmern A und B. Sie kann beliebig um weitere Aushandlungsschritte erweitert werden. Die Aushandlung wird durch Teilnehmerin A über die Mensch-Maschine-Schnittstelle der SSS-Steuerung angestoßen. Die an dieser Schnittstelle spezifizierten Schutzziele (hier: *EzE-Auth)* werden mit Hilfe des Primitivs *NegotiateReq* der Aushandlungsfunktionalität innerhalb der SSS übergeben.

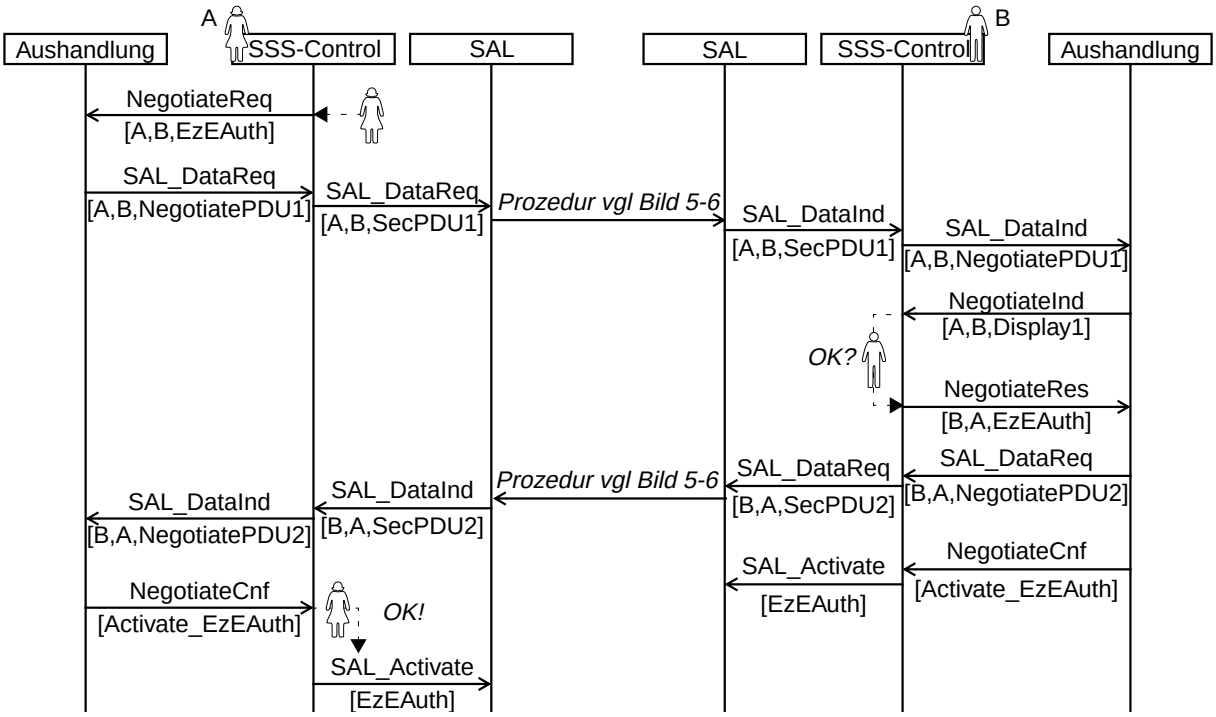


Bild A-4: Exemplarische EzE-Aushandlung von Sicherheitsdiensten

Die Aushandlungsinstanz kodiert diese Schutzziele gemäß eines vereinbarten Standards (*NegotiatePDU1*). Beispielsweise können Kombinationen von Schutzzielen eindeutige Kodierungen zugeordnet werden (siehe z. B. die Vereinbarung von Sicherheitsdiensten beim Secure Socket Layer [129]).

Diese SecPDU wird nun über die SSS-Steuerung mit Hilfe des Übermittlungsdienstes der SAL (*SAL_DataReq*) zur Partnerinstanz übermittelt. Die Adressierung wird im Beispiel explizit vorgegeben (A,B), kann aber auch durch den Kontext bestimmt sein. Es sind die Fälle UNI (Teilnehmer - Dienstanbieter) und EzE (Teilnehmer-Teilnehmer) adressierbar. Die SAL übermittelt die PDUs dann entsprechend der in Bild 5-6 dargestellten Prozedur.

Die Partner-Aushandlungsinstanz im gerufenen Endgerät mit der Rufnummer B zeigt der SSS-Steuerung die von A gewünschten Schutzziele an (*NegotiateInd[Display1]* in Bild A-4). Diese gibt die Schutzziele über das Display an den Teilnehmer weiter. Der Teilnehmer B bestätige hier diese Schutzziele. Dieses wird mit dem Primitiv *NegotiateRes* der Aushandlungsinstanz

angezeigt. Will der B-Teilnehmer die Schutzziele verändern, so wird er stattdessen mit dem Primitiv *NegotiateReq* eine neue Aushandlungsrunde einleiten. Die Aushandlungsinstanz übermittelt der rufenden Aushandlungsinstanz das Ergebnis mit dem Primitiv *SAL_DataReq*.

Daraufhin werden die ausgehandelten Schutzziele (hier: EzE-Authentisierung) automatisch auf Sicherheitsdienste abgebildet. Diese Sicherheitsdienste werden in Endgeräten über die SSS-Steuerung an die Sicherheitsadaptionsschicht übergeben (Primitiv *SAL_Activate*). Diese aktualisiert daraufhin ihre Regeldatenbasis und stößt die zu den Schutzzielen gehörigen Sicherheitsdienste bei Bedarf (synchronisiert mit ISDN-Dienstanforderungen) an. Unerwünschte Wechselwirkungen zwischen Sicherheitsdiensten sind innerhalb der Aushandlungsinstanzen zu erkennen und dem Teilnehmer zur Auflösung anzuzeigen.

Bild A-5 zeigt das Signalisierungs-Zeitdiagramm für die Aushandlung von Schutzzielen bzw. Sicherheitsdiensten an der Benutzer-Netzschnittstelle zwischen Teilnehmerin A und dem Netzbetreiber (bzw. dessen technischem Vertreter). Die ausgehandelte UNI-Authentisierung wird in der Vermittlungsstelle der zentralen Rufsteuerung gemeldet und dort aktiviert.

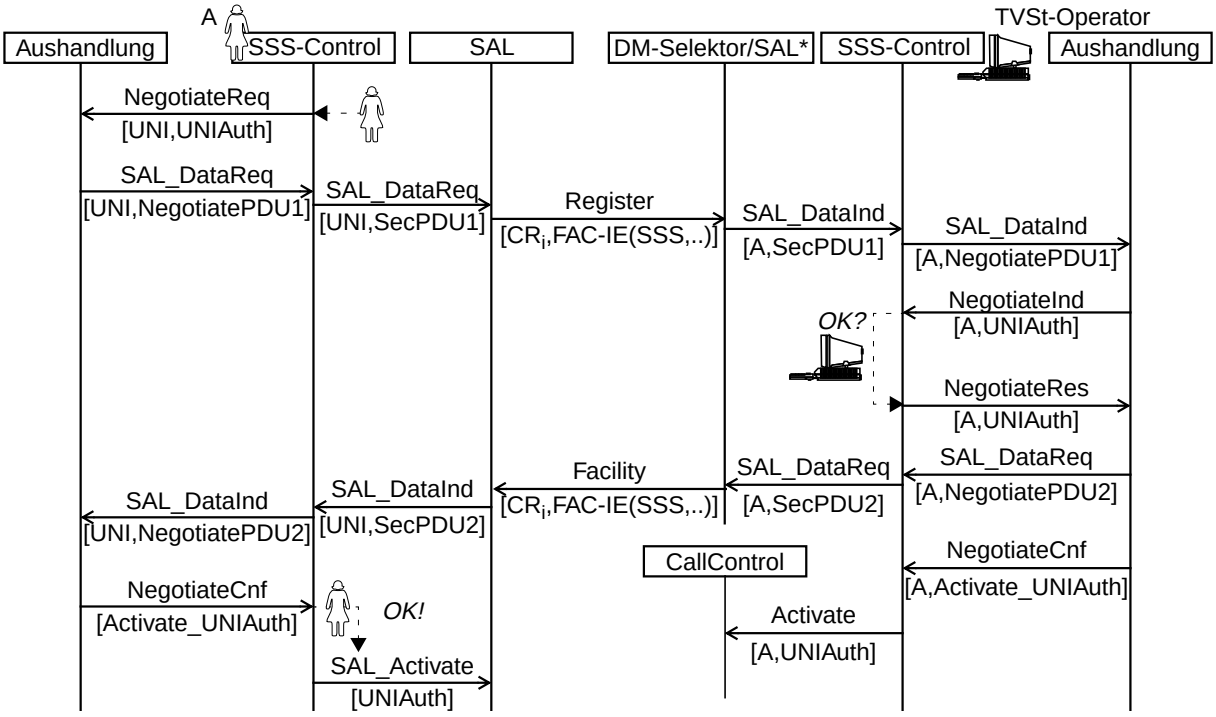


Bild A-5: Exemplarische UNI-Aushandlung von Sicherheitsdiensten

Handeln zwei Teilnehmer die Schutzziele aus, so ist für das *ISDN* für jede übertragene SecPDU eine abgewiesene Verbindungsanforderung sichtbar (Szenario in Bild 5-6). Handelt es sich bei den aushandelnden Parteien um Teilnehmer und Netzbetreiber, so läuft aus Sicht des ISDN ein Dienstmerkmal ab (Szenario in Bild 5-7). Die *SAL* dient hier zur Übermittlung von Aushandlungsdaten zwischen den Beteiligten. Darüberhinaus aktualisiert sie die Regeldatenbank zur Kopplung von ISDN- und Sicherheitsdiensten in Endgeräten und aktiviert die Sicherheitsdienste bei Bedarf. Die *SSS-Steuerung* dient zur Benutzer-Interaktion und zur Koordinierung des Aushandlungsdienstes.

A.4.2 Abfrage von Zertifikaten bei zentralen Zertifikat-Verteildiensten

Die Abfrage von Zertifikaten kann durch den Benutzer über die Mensch-Maschine-Schnittstelle der SSS-Steuerung angestoßen werden. Bild A-6 zeigt den Nachrichtenaustausch zur Abfrage von Zertifikaten bei einem Zertifikat-Server, der als Endgerät (mit der ISDN-Nummer *K*) an das ISDN angeschlossen ist. Es kann sich beispielsweise um einen Datenbank-Server auf einem Linux-Rechner mit ISDN-Karte handeln.

Im Bild wird die Abfrage eines öffentlichen Schlüssels $K_{\ddot{o}}O$ (öffentlicher Schlüssel des Netzbetreibers O) von der SSS-Steuerung angestoßen. Dazu wird der Abfragedienst (KeyRetrieval) durch das Primitiv *RetrieveReq* aktiviert. Der Abfragedienst bestimmt zunächst den zuständigen Schlüsselserver (hier: K) und schickt eine Anfrage zum entsprechenden Endgerät. Zur Übermittlung der entsprechenden SecPDU zum Endgerät mit der Nummer K wird die in Bild 5-6 veranschaulichte Prozedur angestoßen. Eine *Setup*-Nachricht mit einem speziellen Kompatibilitätsparameter HLC^{Sec} wird zum Endgerät *K* geschickt. Die von der TVSt zurückerhaltene Bestätigung *ProceedingInd* wird anhand des HLC^{Sec} dem Übermittlungsdienst der SAL zugeordnet und dort verworfen (① in Bild A-6). Die Setup-Nachricht wird innerhalb des ISDN als Initial Address Message (IAM) zur Zielvermittlungsstelle vermittelt. Dort wird sie als Setup-Nachricht angezeigt. Die im empfangenden Endgerät enthaltene Adaptionsschicht extrahiert das enthaltene UUS-Informationselement und weist – aus Sicht des ISDN – den Verbindungswunsch ab (② in Bild A-6). Die im UUS-Informationselement enthaltene *SecPDU1* wird an die SSS-Steuerung weitergegeben und dort aufgrund der enthaltenen Dienstidentifikation an den Zertifikat-Serverdienst verteilt. Dieser sucht das zum Netzbetreiber *O* gehörige Zertifikat und schickt es – ebenfalls unter Nutzung des EzE-Übermittlungsdienstes der Adaptionsschicht (*SAL_DataReq*) – zum Anfrager.

Beim anfragenden Rechner wird die ankommende *Disconnect*-Nachricht (③ in Bild A-6) mit Hilfe der Call Reference CR^{v} dem Datenübermittlungsdienst zugeordnet und entsprechend mit einer *Release*-Nachricht beantwortet. Die anschließend erhaltene *RelComp*-Nachricht (④ in Bild A-6) wird innerhalb der SAL verworfen.

Die bei Rechner A ankommende Setup-Nachricht wird in der SAL aufgrund der darin enthaltenen Kompatibilitätskennung HLC^{Sec} als Datenübermittlungsnachricht der SAL interpretiert und entsprechend behandelt. Die darin enthaltene *SecPDU2* wird über die SSS-Steuerung an den KeyRetrieval-Dienst weitergegeben. Dieser Dienst extrahiert das darin enthaltene Zertifikat des Netzbetreibers *O* und prüft es. Ist das Zertifikat gültig, so wird der im Zertifikat enthaltene öffentliche Schlüssel $K_{\ddot{o}}O$ der SSS-Steuerung durch das Primitiv *RetrieveCnf* angezeigt. Von dort wird der öffentliche Schlüssel bei Bedarf an andere Sicherheitsdienste übergeben (z. B. zur Authentisierung vgl. Abschnitt 5.2.3).

Aus *Sicht des ISDN* sind zwei Verbindungswünsche sichtbar, die am jeweils gerufenen Anschluß (A bzw. K) abgewiesen werden. Die *Adaptionsschicht* ist ausschließlich im Rahmen der Nachrichtenübermittlung am Dienst beteiligt. Die *SSS-Steuerung* dient als Initiator der Anfrage und als Empfänger des öffentlichen Schlüssels.

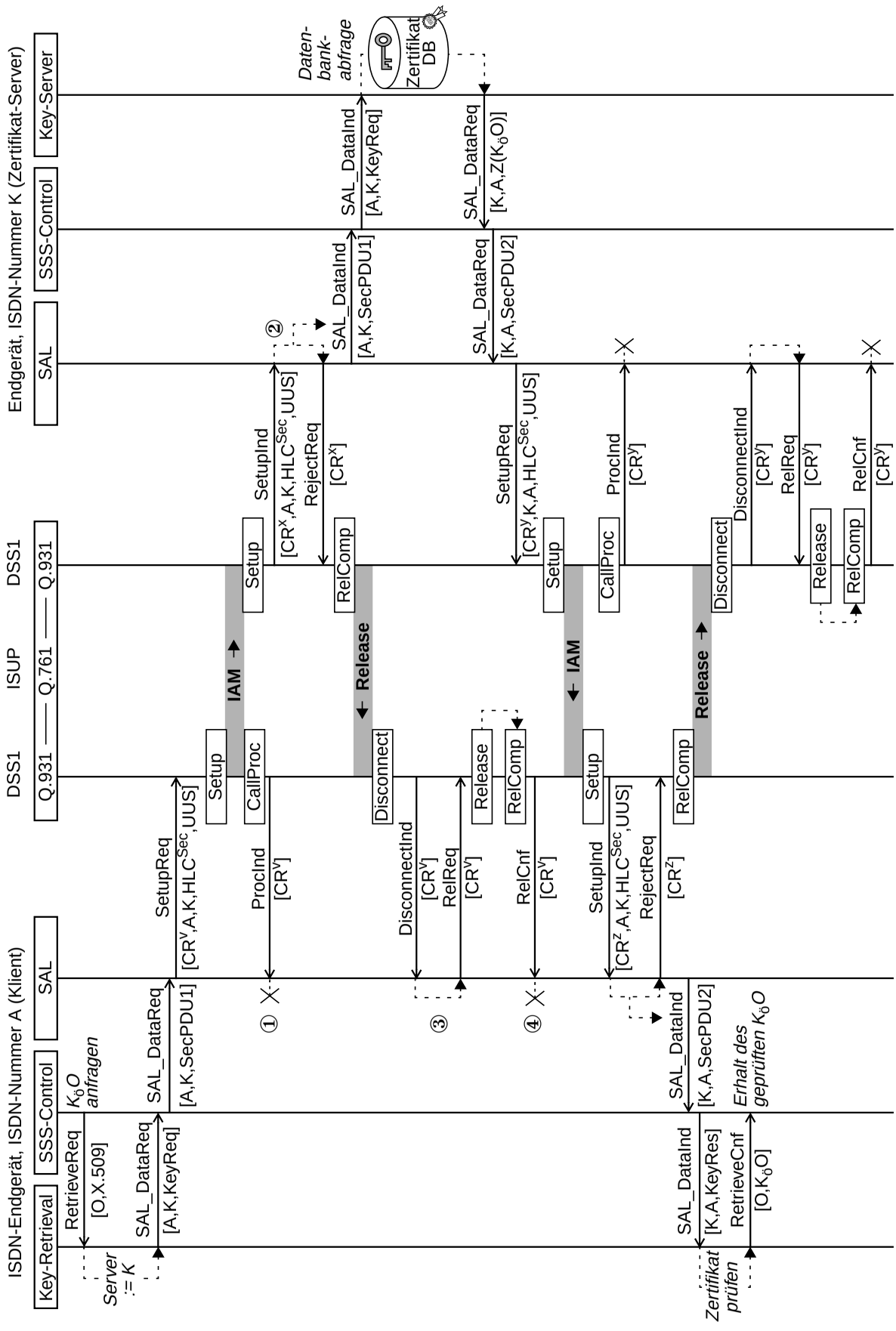


Bild A-6: Exemplarische Abfrage von Schlüsselzertifikaten

A.5 Kodierung von Sicherheitssteuerungsdaten

Zur Kennzeichnung von Informationselementen, die zur Realisierung von Sicherheitsdiensten dienen, werden neue (bisher im ISDN nicht verwendete) Kodierungen eingeführt. Die neuen Informationselemente sind aufgrund der beibehaltenen Struktur kompatibel zu den bestehenden Informationselementen nach Q.931 und Q.932. Im HLC-Informationselement (vgl. Bild A-7a) wird als neuer Identifikator im High Layer Characteristics Identification-Feld der Hexadezimalwert 0x71 (bezeichnet als HLC^{Sec}) eingeführt. Zeichengabetransaktionen, die mit diesem HLC^{Sec} eingeleitet werden, werden dem Übermittlungsdienst der SAL zugeordnet. Dies bedeutet, daß die enthaltene *Call Reference* alle nachfolgenden Signalisiernachrichten zur einer Transaktion zusammenfaßt und als Sicherheitssteuernachrichten kennzeichnet. Weiterhin sind HLCs für herkömmliche ISDN-Dienste, die um Sicherheitsdienste erweitert werden sollen, zu definieren (z. B. HLC^{SpSec}).

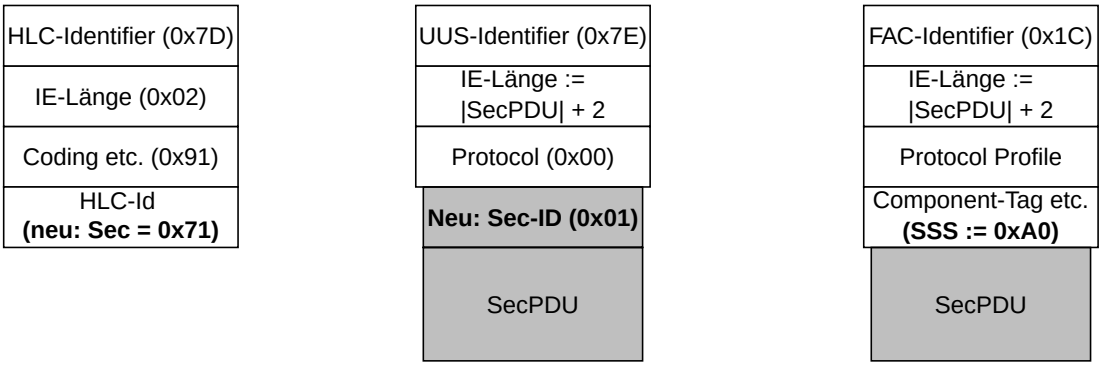


Bild A-7: Spezielle Kodierung von Informationselementen basierend auf [111]

Die *User-To-User-Informationselemente* (vgl. Bild A-7b) besitzen eine Protokoll-Kennung, die für die Übertragung von SecPDUs auf 0x00 (User-Specific-Protocol) gesetzt wird. Zur Unterscheidung möglicher weiterer User-to-User-Protokolle wird vor der eigentlichen SecPDU noch ein weiterer Identifikator gesetzt. Dieser kennzeichnet in der hier genutzten Kodierung (0x01), daß es sich beim Inhalt des UUS-IE um eine SecPDU handelt.

Zur Übermittlung von SecPDUs für Sicherheitsdienste zwischen Endgerät und Teilnehmervermittlungsstelle wird die Kodierung der *Facility-Informationselemente* erweitert (vgl. Bild A-7c). Hier wird für das sogenannte Component-Tag zu den Kodierungen Invoke, Return Result, Return Error und Reject zusätzlich eine Kodierung *0xA0* für die Ansteuerung von SSS-Dienstmerkmalen eingeführt. Nicht erweiterte Endgeräte bzw. TVSt erkennen diese Kodierung nicht und reagieren mit einer Ablehnung (Reject).

Zusätzlich sollten Vereinbarungen über ergänzende Kodierungen des *Cause-Informationselementes* getroffen werden. Das Cause-IE zeigt i. a. den Grund für bestimmte Signalisierabfolgen (z. B. Grund des Verbindungsabbaus) an. Dies ist hilfreich, um z. B. Benutzern und Prozessen bei unerwartetem Dienstverlauf einen Hinweis auf den Grund für dieses Ausnahmeverhalten zu geben.

Abschließend wird die Struktur von Protokolldateneinheiten (SecPDUs) zur Übertragung von Sicherheitssteuerungsdaten dargestellt (vgl. Bild A-8a).

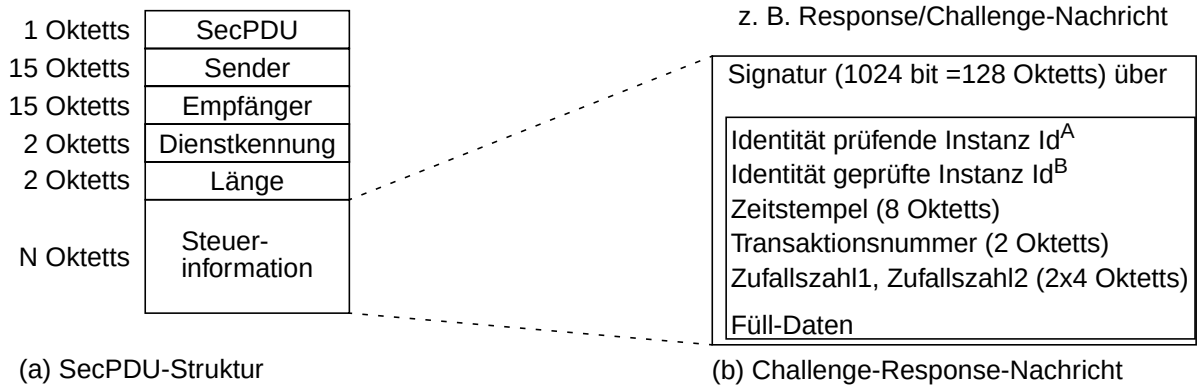


Bild A-8: Kodierung von SecPDUs

Wie im Bild dargestellt, sind mindestens *Absender* und *Empfänger* der SecPDU zu spezifizieren. Aufgrund dieser Information wird die Nachricht vom Übermittlungsdienst der Adaptionsschicht übermittelt (z. B. Sender = Endgerät mit ISDN-Nummer A, Empfänger = Endgerät mit ISDN-Nummer K bei der Zertifikat-Anfrage in Bild A-6). Beim Empfänger muß die SecPDU schließlich über die SSS-Steuerung an den entsprechenden Sicherheitsdienst weitergeleitet werden. Dafür ist eine eindeutige *Dienstkennung* für den Sicherheitsdienst (z. B. UNIAuth, KeyRetrieval, EzE-Encryption, etc.) enthalten. Die weitere Kodierung des Nachrichteninhaltes kann dienstspezifisch vorgenommen werden. Die Response/Challenge-Nachricht, die als SecPDU2 in Bild 5-9 von der TVSt zum Endgerät übertragen wird, kann beispielsweise wie in Bild A-8b dargestellt kodiert werden [25].

A.6 Aufzeichnung eines Signalisierablaufs

Der im folgenden dargestellte Signalisierablauf zeigt die Schicht 3-Nachrichten, welche bei der SAL ankommen bzw. von der SAL abgesendet werden. Die Protokollierung ist folglich am oberen Rand der Schicht 2 lokalisiert (vgl. Implementierung in Bild 5-10). Die Nachrichten wurden mit einem selbst geschriebenen Parser in eine lesbare Darstellung überführt.

EzE-Übertragung von SecPDUs

Die nachfolgend wiedergegebene Aufzeichnung der Übertragung einer SecPDU zwischen ISDN-Endgeräten A (Rufnummer 31) und B (Rufnummer 32) veranschaulicht den Nachrichtenaustausch aus Bild 5-6. Die eigentliche SecPDU wird innerhalb der Setup-Nachricht zum Endgerät B übertragen. Das die SecPDU empfangende Endgerät B weist den Ruf ab und integriert die Bestätigung „SecAck“ in die Release Complete-Nachricht.

```
*********************************************
*   Protokoll-Analysator fuer                *
*   Q.921-Rahmen und Q.931-Nachrichten.      *
*********************************************
--------------------------------------
!  Nachricht Nummer 001 A -> TVSt    !
--------------------------------------
HEX: 00 8d 00 00 08 01 01 05 a1 04 02 88 90 6c 04 00 80 33 31 70
     03 80 33 30 7d 02 91 71 7e 0a 00 01 53 65 63 50 44 55 31 33
Schicht 2 Q.921-Rahmen
C/R=00 SAPI=0 TEI=70 (Signalling)
INFO N(S)=00 N(R)=00 (Info-Frame)

Euro-ISDN Q.931-Message CR: 1\01
SETUP
+Sending complete Len=1
+Bearer service indication Len=2:
     Coding: CCITT
     Capability: UNRESTRICTED DIGITAL INFORMATION
     Transfer mode: CIRCUIT
     Transfer rate: 64 kbit/s
     Structure: 8 kHz integrity (default)
     Configuration: point-to-point (default)
+Calling party number Len=4:
     Type: Unknown
     Plan: Unknown
     Presentation ALLOWED
     User provided, NOT screened
      „3 „1
+Called party number Len=3:
     Type: Unknown
     Plan: Unknown
      „3 „0
+High layer compatibility Len=2:
     Coding: CCITT
     SecurityEnhancedService
+User-user Len=10:
      00 01 „S „e „c „P „D „U „1 „3
```

```
-------------------------------------
!  Nachricht Nummer 002  TVSt -> A   !
-------------------------------------
HEX: 02 8d 00 02 08 01 81 02 18 01 89
Schicht 2 Q.921-Rahmen
C/R=01 SAPI=0 TEI=70 (Signalling)
INFO N(S)=00 N(R)=01 (Info-Frame)

Euro-ISDN Q.931-Message CR: 0\01
CALL PROCEEDING
+Channel identification Len=1:
     Basic Interface
     B1 channel ONLY

-------------------------------------
!  Nachricht Nummer 003 TVSt -> B    !
-------------------------------------
HEX: 02 ff 03 08 01 75 05 a1 04 02 88 90 18 01 8a 6c 04 41 81 33 31 70
     03 c1 33 30 7d 02 91 71 7e 0a 00 01 53 65 63 50 44 55 31 33
Schicht 2 Q.921-Rahmen
C/R=01 SAPI=0 TEI=127 (Signalling)
UI (unnumbered information)

Euro-ISDN Q.931-Message CR: 1\117
SETUP
+Sending complete Len=1
+Bearer service indication Len=2:
     Coding: CCITT
     Capability: UNRESTRICTED DIGITAL INFORMATION
     Transfer mode: CIRCUIT
     Transfer rate: 64 kbit/s
     Structure: 8 kHz integrity (default)
     Configuration: point-to-point (default)
+Channel identification Len=1:
     Basic Interface
     B2 channel ONLY
+Calling party number Len=4:
     Type: Subscriber Number
     Plan: ISDN (E.164)
     Presentation ALLOWED
     User provided, verified and PASSED
      „3 „1
+Called party number Len=3:
     Type: Subscriber Number
     Plan: ISDN (E.164)
      „3 „0
+High layer compatibility Len=2:
     Coding: CCITT
     SecurityEnhancedService
+User-user Len=10:
      00 01 „S „e „c „P „D „U „1 „3
```

```
-------------------------------------
!  Nachricht Nummer 004  B -> TVSt   !
-------------------------------------
HEX: 00 81 70 dc 08 01 f5 5a 08 02 80 d8 7e 0a 00 01 53 65 63 41 63 6b 31 33
Schicht 2 Q.921-Rahmen
C/R=00 SAPI=0 TEI=64 (Signalling)
INFO N(S)=56 N(R)=110 (Info-Frame)

Euro-ISDN Q.931-Message CR: 0\117
RELEASE COMPLETE
+Cause Len=2:
     Rec Q.931 / Coding: CCITT
     Location: user
     normal event
     Incompatible destination
+User-user Len=10:
      00 01 „S „e „c „A „c „k „1 „3

-------------------------------------
!  Nachricht Nummer 005  TVSt -> A   !
-------------------------------------
HEX: 02 8d 02 02 08 01 81 45 08 02 80 d8 7e 0a 00 01 53 65 63 41
     63 6b 31 33
Schicht 2 Q.921-Rahmen
C/R=01 SAPI=0 TEI=70 (Signalling)
INFO N(S)=01 N(R)=01 (Info-Frame)

Euro-ISDN Q.931-Message CR: 0\01
DISCONNECT
+Cause Len=2:
     Rec Q.931 / Coding: CCITT
     Location: user
     normal event
     Incompatible destination
+User-user Len=10:
      00 01 „S „e „c „A „c „k „1 „3

-------------------------------------
!  Nachricht Nummer 006  A -> TVSt   !
-------------------------------------
HEX: 00 8d 02 04 08 01 01 4d
Schicht 2 Q.921-Rahmen
C/R=00 SAPI=0 TEI=70 (Signalling)
INFO N(S)=01 N(R)=02 (Info-Frame)

Euro-ISDN Q.931-Message CR: 1\01
RELEASE

-------------------------------------
!  Nachricht Nummer 007  TVST -> A   !
-------------------------------------
HEX: 02 8d 04 04 08 01 81 5a
Schicht 2 Q.921-Rahmen
C/R=01 SAPI=0 TEI=70 (Signalling)
INFO N(S)=02 N(R)=02 (Info-Frame)

Euro-ISDN Q.931-Message CR: 0\01
RELEASE COMPLETE
```