Signalling and service interfaces for separating security sensitive telecommunication functions considering multilateral security[1]

Reiner Sailer, University of Stuttgart
Institute of Communication Networks and Computer Engineering (IND)
Pfaffenwaldring 47, D-70569 Stuttgart
E-Mail: sailer@ind.uni-stuttgart.de
http://www.ind.uni-stuttgart.de

Abstract

Data protection and data security become more significant since telecommunication services and innovative applications based on these services use an increasing amount of sensitive data. Modern services, e.g. call forwarding, teleconferencing and voice mail use or store personal data to realize individual services. Sensitive data include personal identities or calling numbers, location information of the communicating parties, service indicators, and time and duration of communication events. Communication profiles of individuals or employees may enable others to deduce further – maybe strategic – information. As public telecommunication services are mostly based on digital networks, this sensitive information can easily be stored and processed.

Functionality within telecommunication networks can be classified with respect to its relevance concerning data protection and data security. Functionalities that process sensitive data or realize sensitive mechanisms are called sensitive functions. We state that sensitive functions must be trustworthy for all parties that rely on them. Trustworthy functions demand attestable software and special hardware platforms that are highly secured against unauthorized access as a prerequisite for their certification by trustworthy organisations. Hence our approach aims at separating sensitive functions – e.g. services realizing anonymous calls or delivering public keys as a basis for security services within the user‘s terminal equipment – from highly complex functions of public telecommunication networks.

This contribution aims at deriving requirements for interfaces over which separated sensitive functions may securely interact with existing core telecommunication functions and services that do not follow security design guidelines. This is not straightforward because separated functions might no longer be trusted by network operators because they are not directly supervised by the network operator. Hence, there is need for enhanced security gateway functions with respect to the robustness, autonomy etc. of those telecommunication networks that are partially enhanced – this means controlled – by separated functions in order to make the related interfaces acceptable. Furthermore some of these sensitive functions are essential for basic network functionality like charging or routing. Because there are several areas of conflicting interests concerning the satisfactory realization of security requirements of different interest groups, this approach will make use of so called Trusted Third Parties which act as mediators between the security interests of users, network operators, service providers and manufacturers. In order to be effective these mediators shall be directly addressable over present telecommunication networks to serve different users, network operators and service providers. These mediators realize multilaterally secure services by balancing the security requirements of the related parties.

1. Introduction

Advanced communication networks satisfy the demand for more flexible services. Individually tailored communication services are growing more important because they are determining the efficiency of many enterprises. Existing communication infrastructure will be used as a basis for future communication services and networks because the investments in these resources are enormous. At the same time the objective of data security and data protection is raising. Security requirements have not been foreseen when today’s communication systems were introduced. Thus, security require-

[1] This work is funded by the Gottlieb Daimler- and Karl Benz-Stiftung in Ladenburg.

ments have been taken into account insufficiently – moreover, security requirements may change quickly depending on individual experience, risk assessment, related charge, and press reports.

Security will gain increasing attention as it has been shown that lacking security can lead to rejection of communication services by potential users of communication networks. Therefore, durable resources will profit from interfaces that grant the ability of providing advanced services particularly concerning arising and changing security requirements. Moreover, we are convinced that the property to satisfy individual security requirements in a multilateral way is a prerequisite for future success of communication services.

First, this paper classifies data concerning their appearance in communication networks and related security mechanisms granting data security and data protection. Afterwards, we address possibilities to integrate security mechanisms into existing communication networks and determine possible locations for these functions referring to the ISO-OSI Reference Model [5].

Exemplary requirements and options are shown for new signalling interfaces over which security services may be accessed by users, service providers and network operators[2]. Restrictions resulting from conflicting security requirements are pointed out. We want to show that open security interfaces can make communication networks more attractive to both users and service providers by enabling user or application driven security enhanced services.

1.1 Requirements Put on Security Mechanisms

Modern forward-looking communication infrastructure will offer interfaces over which security enhanced services may interact to fulfil security requirements. Based on these additional interfaces, it is possible to cope with changing requirements of users and service providers. Therefore, such interfaces may be valuable in an environment of competing network operators and service providers.

Security services will not be for free. Hence, those who will have to pay for security services shall be able to control the degree of security that is necessary. Security services must therefore share some characteristics i.e. they should be

- tailor-made (fitting the individual needs of a network user in a given situation)
- efficient (scalable, easy to integrate, compatible by providing and using standardized interfaces)
- multilateral (balancing security requirements of different interest groups)
- trustworthy (using trustworthy implementations, administration, management, charging etc.)

This paper will especially focus on trustworthy, scalable, multilateral and easy to integrate security. Consequently we will take a closer look on these properties and their impact on signalling and service interfaces when we discuss some examples in section 2.

1.2 Classification of Data and Protection Mechanisms

When speaking about security we must state all security requirements that are to be fulfilled and valid assumptions about system environments and properties of potential attackers. Security requirements for communication services are described in terms of

- *confidentiality*, which means that information may only be visible to authorized people,
- *integrity*, which means that data may not be changed unnoticed by unauthorized people, and

[2] In the following text we refer to the different types of users of communication networks as *network users*. These network users include subscribers, service providers and network operators.

- *availability*, which means that services and data must be at the user‘s disposal as presumed.

These security requirements refer to dedicated data that are be secured. Sensitive data may be user data transmitted via communication lines, the identities of the communicating parties or even the fact that a dedicated communication event occurs. Network operators must be able to control the access to their network to protect their infrastructure against misuse and unauthorized access. Service providers must be able to relate charges comprehensible to those subscribers that cause these charges and may therefore demand for flexible and strong authentication mechanisms. These few examples already illustrate that individual definitions of "sensitive data" lead to a vast variety of different security mechanisms that are needed to grant security requirements with respect to different types of data occurring in communication networks[3].

The need for balancing between conflicting requirements will add further complexity to those mechanisms that are responsible for security management. Balancing security requirements is a precondition to multilateral security and leads to additional requirements with respect to security interfaces. Additional requirements include the negotiation of security services and mechanisms for including trusted third parties into service control in order to enhance present services by multilateral security.

Because security will not be for free, it is necessary to identify those security mechanisms that are needed to meet the requirements. This choice is greatly determined by a risk analysis. The set of required security mechanisms varies over time because it is dependent on the abilities of assumed attackers, the technical environment, and the data or functionality that must be secured. Consequently, the necessary security mechanisms are user and application dependent and must be supported by communication networks in a flexible and scalable way.

Besides from security requirements and related data, it is helpful to take the physical area into account in which data must be secured and where security mechanisms must be located. Areas in which we assume our values (sensitive data and functions) secure are called trusted environment. Hopefully, these environments are worth the trust we put on them. Security mechanisms for example must be located within trustworthy environments. Otherwise, they may be compromised by attackers and therefore fail to accomplish their work.

Both computability and scalability of security will profit from the following classification of functions and protection mechanisms. Fig. 1 illustrates a classification of security functions according to their sphere of influence in relation to the end points of the communication event[4]. We call security functions that are realized within the users’ terminal equipment end-to-end functions [2] because they influence security from one end point of the communication relationship to the other. Values protected by end-to-end functions will be secure everywhere on their way through the communication network concerning confidentiality and integrity.

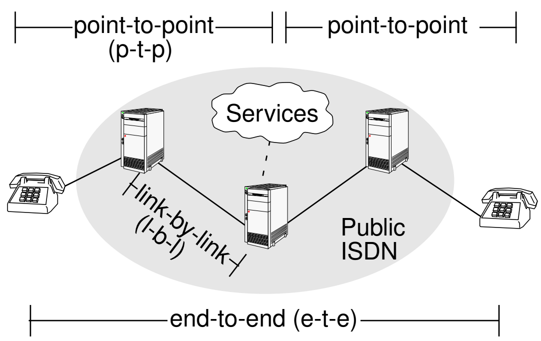


Figure 1: Classification of security functions

This kind of *end-to-end* security is suitable for application data that does not have to be processed within the network. In addition, we need point-to-point security functions that have an effect between the user terminal equipment and the service provider in order to realize efficient access control and charging. Because there may be intermediate switches between the user’s terminal equip-

[3] Some values may be insured with commercial insurances that will pay in case of damage. This assumes that the damage can be repaired by money. Furthermore insurances must be able to assess the risk and policy-holders must be aware of the potential damage to set the sum insured.

[4] A thorough investigation of these aspects is out of the scope of this paper. Interested readers are invited to have a closer look at [1].

ment and the service access point of the corresponding service provider, related security requirements will usually demand for *point-to-point* security functions. Point-to-point functions may be concatenated by using trusted parties as interim nodes within the network to realize security mechanism that offer protection between the communicating peers. Moreover, it may be necessary to secure signalling information *link-by-link* over communication links if we suppose attackers having access to those links. This must be assumed in the case of directional radio links. It is also required that the environments in which values are not explicitly protected by security functions are trustworthy.

The following restrictions affecting the location strategy result from inherent attributes of the respective security functions:

- encrypted data can not be read or processed without knowing the decryption-key
- signed data can not be changed preserving integrity without knowing the signature-key

For example end-to-end encrypted data cannot be processed within the network, hence this data must be transparent to the network. Signed data cannot be changed by switches other network infrastructure – including attackers – outside the signing equipment without destroying integrity.

We distinguish between three types of data: (i) data that is transparent for the communication network and value-added services, (ii) data that must be processed within the network as a basis for communication switching or as a basis for the realization of value-added services, and (iii) data that can be derived from the state of network infrastructure. The following table gives examples of security mechanisms and location strategies according to these classes of sensitive data.

sensitive data/ requirements	**Transparent User Data**	**Control Data**	**State Information & Derived Information**
Confidentiality (C)	e-t-e-encryption, access control	p-t-p/l-b-l encryption, temporary identities, MIXes [3]	broadcast, dummy traffic and MIXes including switching [4] (to protect called or calling party number)
Integrity (I)	e-t-e-authentication, digital signatures	p-t-p-authentication, digital signatures	controlled and verifiable routing, crossing exclusively trusted networks
Availability (A)	backup-connections, -servers (redundant functions & data)	existing routing and congestion control mechanisms (e.g. within SS7)	audit trails without personal information for network failure diagnosis etc.

Table 1: Security mechanisms related to security requirements and type of data to be secured

Transparent user data includes data exchanged between distributed applications located outside the network. This kind of data may be secured by dual *end-to-end security functions* located within the users' terminals if these terminals are trustworthy. Future applications including teleteaching, telebanking, teleconferencing will need strong e-t-e security mechanisms to be successful and applicable.

Control data includes information that is necessary to realize basic network services like routing, additional supplementary services like call forwarding and, with an increasing significance, information that is processed by value-added services realized outside the core network by service providers. Such services include call forwarding depending on the time of day or the called number, televoting services and other services offered by the so called "Intelligent Network". Future digital on-line payment systems may also use signalling to securely exchange payment control data between the user's smart card and respective payment service providers enhancing off-line charging in present public networks. This is a basis for flexible and multilaterally secure services because charging information will otherwise contain large amounts of personal data that could not be controlled by the user and may not be conform with data protection laws in several countries, as e. g. Germany.

A third kind of data can be deduced by state information of the communications infrastructure. For example the calling numbers of the involved terminals of a call can be deduced by using the state information of a participating switch to relate its incoming and outgoing links used by the relevant connection. This practice can be continued until all switches are identified that are used by the connection. Deducing sensitive information from state information of network infrastructure may be difficult for attackers depending on their access to this state information.

The next section will discuss possible signalling interfaces and options for the exchange of control data in order to make services possible that both enhance present services by security and offer new services with respect to changing requirements and new network applications. We take into account the existing protocol architecture of the Integrated Services Digital Network (ISDN) and present requirements of users, network operators, and service providers.

2. Security Services Signalling Interfaces and Protocol Mechanisms

This section introduces two new signalling interfaces. The user-network security interface – called Security Supplementary Services interface (SSS) – serves as a basis for negotiating and realizing security services between user terminal equipment and network services. Furthermore the related protocols may implement interworking functionality to support the exchange of security control information between the user terminal equipment and enhanced security service providers within the public ISDN.

The second interface is located within the common-channel signalling system number 7 (SS7, [10]) and supports services that realize both security enhancements to existing services and new secure services. This network-network security protocol – called Security Application Part (SecAP) – enables the separation of sensitive functions from less sensitive functions of present public telecommunication networks. At the same time it enables enhanced separated services to base on and benefit of existing core services of the underlying network.

First, an authentication service – for verifying the claimed identity of communicating parties – is discussed because the related security mechanisms touch both the user-network interface for exchanging authentication tokens and the common-channel signalling interface e.g. for retrieving valid public keys. This will show an example for *enhancing existing services* by security.

Secondly, we will have a closer look on signalling requirements of anonymity services realized by a MIX-infrastructure. This example demonstrates the use and advantage of security related interfaces within common-channel signalling networks to separate sensitive functions. It serves as an example of *realizing a new service* (MIX service) based on existing telecommunication infrastructure.

We will focus mainly on signalling requirements that means requirements related to the exchange of security control data. Readers who are interested in how MIXes are realized in detail may want to read [3] or [4]. Information about authentication protocols and realization aspects can be found in [6] and [9].

The mechanisms shown in Tab. 1 serve the need for securing different types of data. The chosen examples illustrate the benefit of the proposed security interfaces and related protocol mechanisms for implementing and integrating link-by-link, point-to-point and end-to-end security functions into the existing pubic ISDN.

2.1 Signalling Interface Requirements of Authentication Services

Authentication can serve the users' needs for identifying their communication peers, network operators or service providers. At the same time authentication serves the needs of network operators and service providers to control the access of users to their communication and service infrastructure. Modern authentication protocols for spontaneous communication with changing peers usually base on public key cryptography. Assume a network operator *NO* wants to verify the identity of user *A* as a basis for access control. The idea is that user *A* proves his identity by proving that he knows a secret key related with his identity. *A* proves this by signing a random number received from the authenticating party *NO* with this secret key. The signature is verified by using the public key that is related with user *A*. Of course this public key must be authentic and must be managed by an organization that is trusted by *A* and *NO*.

Tab. 2 illustrates how the SSS interface for authentication may look like. The security signalling messages may serve as containers for authentication tokens. Standardized authentication tokens facilitate compatible authentication mechanisms. Additional parameters may include identifiers for accepted cryptographic functions, certificates for the implementation environments or global title addresses of accepted public key servers.

security signalling messages	included information elements
SEC_Negotiate(...) Auth_Sendtoken(...) Auth_OK(...) Auth_Err(...)	Auth-Token: Sender, Receiver : Id Random : Unsigned Long Time : Octetstring Signature : 1576Bit SecretData : Octetstring Tokenid : (1,2,3) Auth-Cause: Integer

Table 2: Prototype SSS interface

We aim at services enhanced by authentication. Hence, it would be natural to integrate authentication and service control. On the other hand, we want to integrate security enhancements in a flexible way without changing existing network infrastructure too much. Furthermore in order to result in assessable security we need clear and flexible interfaces between complex existing service control functions and security functionality whose implementation and run time environment fulfils enhanced security guidelines. Therefore we propose enhancements in present user-network interfaces over which user terminals and network infrastructure may negotiate security mechanisms that enhance certain services. This resembles existing mechanisms for integrating ISDN supplementary services [8] like call forwarding. Fig. 2 illustrates the use of the proposed Security Supplementary Services (SSS) interface. New control and service functions are emphasized.

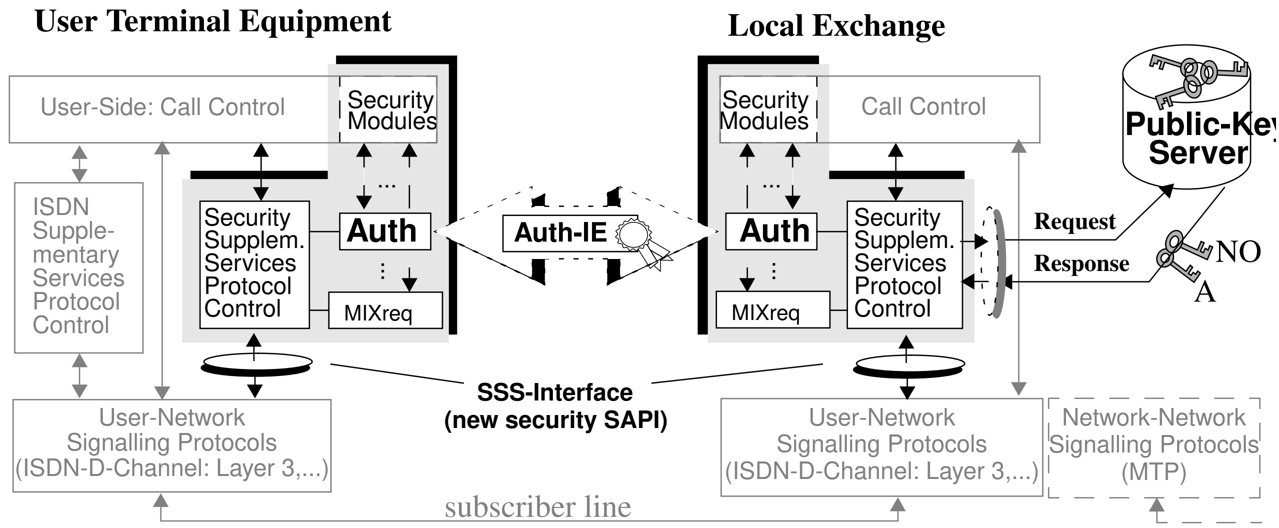


Figure 2: Enhancement of the user-network interface by a seperate Security Supplementary Services interface

Within the authentication procedure, signed control data (Auth-IE in Fig. 2) need to be exchanged between user terminal *A* and local exchange *NO*. Related control messages are generated and verified within the authentication control (AUTH in Fig. 2). For this purpose the authentication control interacts with a smart card or any other security module[5] that offers a trusted environment for storing and

[5] Readers interested in security requirements and design options of security modules are strongly recommended to have a look at [7].

processing secret signature keys. The depicted SSS protocol control may also serve as a security manager and may automatically negotiate and initiate the proper security mechanisms before allowing a connection based on a specified set of security rules. As an example one can think of "black lists" specifying numbers with which connections are only allowed in conjunction with authentication. Consequently dialling one of these number will cause a preceding authentication process. This may enhance existing closed user group services by supporting user level access control. The proposed *S*ecurity *S*upplementary *S*ervices interface may serve for various tasks resulting from the need of security mechanisms including:

- *Negotiation and support of end-to-end security mechanisms*: End-to-end user authentication is supported by the transmission of user authentication tokens via the local exchanges of the communicating parties transparently for the underlying network infrastructure. For example the interface may support charging of such messages, putting upper limits on the amount of exchangeable security control data or getting valid public keys over the signalling network and delivering them to the authenticating parties.
- *Negotiation and support of point-to-point security mechanisms*: Security mechanisms between a user's terminal equipment and security service providers are supported by the SSS interface by enabling signalling based negotiation of security parameters and transmitting authentication tokens between user terminals and service control functions within the network. Because large service providers need access to the signalling system over powerful interfaces, there is also need for interworking functionality to translate user-network security signalling messages to signalling messages within the SS7[6]. This interworking functionality may be implemented within the SSS protocol control or can be realized as separate interworking security functions within the local exchange. SS7 is used in Fig. 2 to retrieve the valid public keys of the authenticating parties from trusted pubic key server databases. In this example the interworking is done by the SSS protocol control.
- *Negotiation and Support of link-by-link security mechanisms*: Mechanisms that secure the user's access to the network are supported by the SSS interface. Enhanced access control services based on authentication procedures may enhance conventional user-network signalling. Such mechanisms may serve for non repudiation of the use of services. They may also protect against attackers that have access to subscriber lines or in-house installations shared by terminals or users with different security levels. The proposed interface enables security enhanced public terminals that offer security services in co-operation with individual security modules of the respective user. Link-by-link security mechanisms applied within the network as depicted in Fig. 1 might not need to follow open interfaces if they do not interfere with predominant security mechanism, but their management would profit from such interfaces.

The discussed interface bases on the user-network signalling protocol of the ISDN (also called ISDN-D-Channel, layer 3). Layer 3 of the ISDN-D-Channel is enhanced by the SSS interface to support the exchange of security control information between user terminals and local exchanges over the subscriber line. This security information may be exchanged by including security information elements within legal signalling messages or by using special security signalling messages that can be processed independently from other ISDN signalling messages. Assigning this interface an new standardized service access point identifier (SAPI) supports the separation of security messages.

The protocols of the SSS interface and internal matters of the SSS protocol control – i.e. its implementation – are out of the scope of this paper. As a first step, the SSS may be integrated into the existing interface for ISDN-supplementary services using *Facility messages* and *Facility information elements* to exchange security control data between user terminals and local exchanges.

---

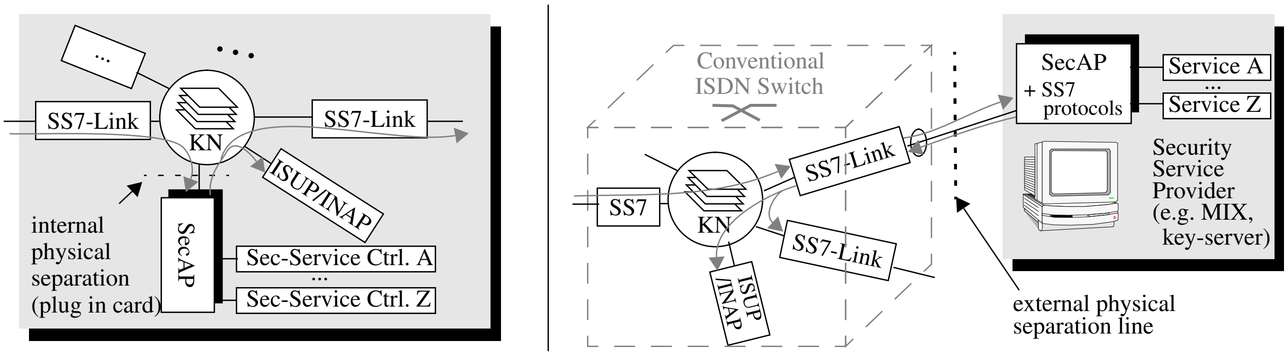
[6] Common-channel signalling system number 7 offers a very powerful interface for exchanging control information between any switches of the ISDN independently from switched traffic channels.

2.2 Integrating Trusted Third Parties into ISDN-Infrastructure

Security Services must be implemented efficiently within trusted environments. Therefore there is need for independent, trustworthy implementations of security services. Carefully engineered security services running on a trustworthy environment – i.e. certified by independent organizations – will be very expensive. Hence to be efficient these services must benefit from the economy of scale. This can be realized by making these services responsive to requests from the whole network and – over the SSS-interface – terminal equipment. In addition these services will benefit a lot from being able to base on existing and working services of conventional telecommunication networks.

Because trust is a judgement that is highly dependent on the respective person, we will need open signalling interfaces to enable independent organizations to offer security services. The resulting competition will favour high quality security services and will result in replaceable security services in the case of misuse or raising security weaknesses.

Consequently, we adapt the security user-network-interface SSS to a security interface that is applicable to the SS7. Taking into account existing protocol architectures and the realization of present more or less decentralized control structures of ISDN switches we propose two alternative implementations of security interfaces leading to varying flexibility in service design (Fig. 3).



(a) Integrated security services using SecAP (signalling and switching)

(b) External security services using remote SecAP (signalling only)

Figure 3: Architectures for security interfaces enhancing common-channel signalling system number 7

Fig. 3a illustrates the use of a security signalling interface SecAP similar to existing (Mobile-, IN-) application parts based on SS7. This solution may be applicable for large service providers or network operators who operate their own switches. It supports security enhancements of existing communication services by enhancing the switch internal routing to make the security application part addressable by owning a unique (new) subsystem number. This is the straightforward approach for realizing or enhancing services based on individual switching and signalling. The security functionality and the SecAP in Fig. 3a may be implemented on a plug in board like present line trunk groups supporting existing application parts but should additionally be certified and tamper proof. Consequently this solution demands an extension of the set of known subsystems within SS7. Assigning the SecAP a unique subsystem number makes this new application part addressable by other network switches and enables selective filtering of signalling messages by the network operator if service providers misuse the interface. Furthermore security services spanning different networks would be enabled if such an interface will be standardized.

Fig. 3b illustrates a restricted interface to allow small organizations that are not able to operate and maintain a whole ISDN switch to offer security services over a restricted signalling interface. There may be mainframes that act as a platform for trusted third parties offering services realized solely over signalling. They do not own any traffic channels and switching functions. The security application part will profit from underlying TCAP and SCCP services offering transaction processing and global title addressing. Global title addressing seems appropriate to facilitate the co-operation of independent service providers to offer trustworthy security services by hiding low level and maybe changing network addresses. On the one hand relying on SS7 offers great flexibility to the service providers because existing ISDN user parts can be addressed directly. On the other hand this means enhanced risks for network operators because their switches may be controlled partly from remote platforms that are not directly supervised by them.

A short example illustrates the use of switches following the architecture of Fig. 3a. Fig. 4 depicts the signalling and switching events to hide the routing of a call. Usually MIX-functions are used to hide the routing of calls [4],[3]. For this purpose they mediate the connection. Instead of connecting users A and B directly, the connection is routed from user A to MIX_1, from MIX_1 to MIX_2 and from MIX_2 to user B. We do not describe the MIX functions in detail, but we assume the following:

- User A wants to call user B using ISDN. He wants to be sure that the network operator is not able to deduce with whom he communicates.
- Anonymity service providers MIX_1 and MIX_2 are trusted by user A and user B and do not work together. A addresses MIX_1, including the encrypted address of MIX_2 to be used by MIX_1. The final address of user B is encrypted by A in a way that only MIX_2 will be able to decrypt the endpoint of the call.
- There is a lot of traffic that ensures that it is not possible for an outsider or the network provider to follow a call through the MIXes because there are so many connection being put up at the same time between the MIXes. In this case an outsider is not able to establish which incoming call belongs to which outgoing call at a MIX without the help of the MIX itself.

Fig. 4 shows the flow of signalling messages for the establishment of the anonymous[7] call. An outsider following the call will lose the call at MIX_1 if starting at user A. He will lose the call at MIX_2 if starting at user B.

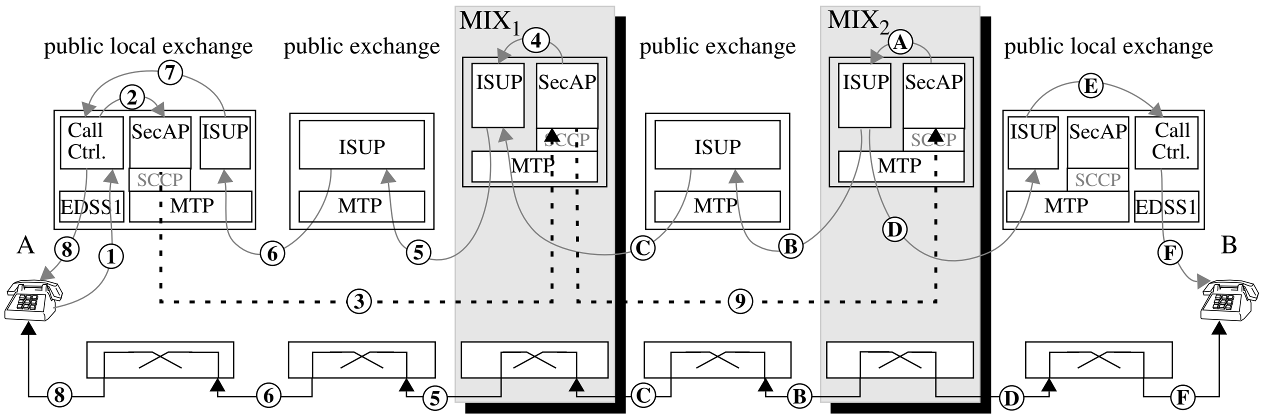


Figure 4: Exemplary use of signalling protocols as a basis for anonymity services

At first user A will book an anonymous call at the local exchange (1 in Fig. 4). This will be indicated over the user-network interface and translated into signalling requests (2) delivered to the first MIX configured for user A (3). A will on-hook and wait for a call-back initiated by MIX_1. Translating request 3 to a connection request for the ISUP within MIX_1 may be done by using a common control part that has access to both ISUP and SAP (4). This part of the connection is established backwards using conventional ISUP-signalling (5, 6, 7). The lower part of Fig. 4 illustrates the sequence in which the switched connection is established between adjacent ISDN exchanges.

[7] Usually anonymity demands stronger mechanisms i.e. more MIXes, stronger requirements and weaker assumptions. We focus mainly on signalling requirements of security services not on the implementation of the security service control itself. This exemplary realization ensures that the connected parties are not deducible by using signalling or state information of the public switches.

The establishment of the second part of the call is done in the same way. MIX_1 decrypts the address of the next MIX (MIX_2) and sends a request to MIX_2 (`9`). MIX_2 translates the request to an ISUP request (`A`) and establishes an ISDN connection with MIX_1 (`B,C`). The two parts of the connection are combined within MIX_1, and cannot be associated by outsiders. MIX_2 recognizes that he is the last MIX and decrypts the final address B. Afterwards MIX_2 establishes a conventional ISDN connection via an ISUP request (also covered by action `A` in Fig. 4) to user B (`D,E`). This incoming anonymous call may be indicated at the user's terminal equipment like a call originating from MIX_2. It is also possible to send additional security control information to the call control of local exchange B in order to indicate user B that there is additional information available. Such information may be the identity of A encrypted in a way that only B is capable to decrypt it.

The three parts of the connection cannot be associated by outsiders or by MIX_1 or MIX_2. MIX_1 doesn't know to whom MIX_2 forwards the connection. MIX_2 does not know from whom the connection was initiated because he only knows that the connection originates from MIX_1. It is not possible to associate the call initiated by user A and the call indicated at user B, if MIX_1 and MIX_2 do not co-operate and the different parts of the connection cannot be concatenated by supervising incoming and outgoing calls at the MIXes (see assumptions above). Of course the identities may be deduced by eavesdropping the data exchanged over the established ISDN connection, but this kind of attack must be handled by end-to-end security mechanisms within the users' terminal equipment. The described solution bases on open interfaces within the common-channel signalling system number 7. Whether there will be open interfaces and which services may be offered by the network operators to third parties will greatly dependent on the development of efficient security mechanisms to protect the core network infrastructure against misuse or integrity attacks over these interfaces.

At this point it is worth to recall the architecture depicted in Fig. 3b. Realizing anonymity services based on remote SecAP services would demand minor changes within existing ISDN switches. The concatenation of adjacent parts of an "anonymous" connection will now be done within the public switches. Alike detection points supporting IN services, our solution would depend on a defined interface to affect the service control within the linked ISDN switch. In the above example remote security services would be requested by ISDN switches to determine the destination of the following part of the respective connection. The ISDN switch will afterwards continue the connection establishment to the respective switch at which the next MIX-service is located. This will continue until the network gets the final address of the connection. An outsider will not be able to follow the connection if he has no access to the ISDN switches at which the remote MIX-functions are located and if the link between the switches and related external MIX functions is appropriately secured. The cost for a network operator to follow a call will be dependent on his network management means to concatenate the various parts of the connection. Spanning multiple networks operated by competing organizations will enlarge the cost to uncover the communicating parties. This demands however, that security application parts are able to interact beyond network boundaries. Work goes on to examine possibilities to base such security functions solely on IN services and consequently on applied and developing signalling interfaces.

3. Conclusion

This paper proposes two related security signalling interfaces based on the public ISDN. The first enhances user-network signalling and the second enhances network-network signalling to support the exchange of control data between distributed, co-operating security functions.

The enhancement of the user-network signalling protocol – called security supplementary services signalling interface – supports the negotiation of link-by-link, point-to-point and end-to-end security mechanisms. The related security supplementary services protocol control within the local exchange serves two purposes: (i) the implementation of link-by-link security functions securing the user-network interface by enhancing existing call control and (ii) the interworking and translation of user-network signalling messages concerning the security interface into network-network signalling messages of the related security application part and vice versa to exchange security control information between user terminals and trusted third parties within the network. Within a user's terminal equipment, co-operation of security supplementary services protocol control and removable security modules (see Fig. 2) enable individual settings for security enhancements per user. The protocol control within the user's terminal equipment may serve as a kind of individual security manager and may therefore be realized within a trusted environment, e.g within a separate security module.

The extension of network-network signalling interfaces enables independent service providers to offer security enhanced services optionally by operating own switches or by using a special signalling interface that enables security enhancements of the existing service control without the need to implement and operate a whole ISDN switch on their own. The chances and flexibility for service providers that result from controlling existing functions within switches of the network (see Fig. 3 b) must be balanced by enhanced security mechanisms (gateway-functions) that preserve the autonomy and integrity of the core ISDN. Network operators offering such an interface must have means at hand to control the use of this interface over which parts of their infrastructure are controlled.

The proposed interfaces base on existing protocol architectures and may serve as a basis for trustworthy, easy to integrate and flexible security services. Promoting the separation of security services they support assessment and certification of security services. Included negotiation properties are the basis for multilateral security. Separation of sensitive service functions from existing insensitive functions leads to clear interfaces and implementations that are physically separated interacting over defined interfaces (processor buses or signalling links). Sensitive functions may be implemented on separate and tamper proof plug in boards. Alternatively they may be implemented by using certified computer hardware and software to realize cost effective security services based solely on signalling interfaces like security application parts or subsets.

Further efforts are concentrated on developing protocols and exemplary specified parts of the proposed interfaces based on authentication and anonymity services as mentioned above. The degree of security and flexibility that may be achieved using existing interfaces like ISUP or INAP for security enhancements must be examined. Prototypical implementation or functional simulation of security service protocols must lead to an estimation of the additional computational power and network resources needed. Charging and other management tasks accompanying network services are to be extended in order to preserve the gain achieved by security enhancements of the service itself.

References

[1] *R. Sailer, H. Federrath, A. Jerichow, D. Kesdogan, A. Pfitzmann:* „Allokation von Sicherheitsfunktionen in Kommunikationsnetzen“, in G. Müller, A. Pfitzmann (Hrsg.) : „Mehrseitige Sicherheit in der Kommunikationstechnik“, Addison Wesley, 1997

[2] J. *H. Saltzer, D. P. Reed, D. D. Clark:* „End-To-End Arguments in System Design“, ACM Transactions on Computer Systems, Vol. 2, No. 4, November 1984, pp. 277-288

[3] *D. L. Chaum*: „Untraceable Electronic Mail, Return Addresses, and Digital Pseudonyms“, Communications of the ACM, Volume 24, No. 2, February 1981, pp. 84-88

[4] *H. Federrath, A. Jerichow, A. Pfitzmann:* „Mixes in mobile communication systems: Location management with privacy“, in R. Anderson (Hrsg.): "Information Hiding", LNCS 1174, Springer Berlin, 1996

[5] ISO 7498 International Standardization Organisation: „Basic Reference Model for Open Systems Interconnection“, 1989

[6] *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“, Addison Wesley, 1997

[7] *A. Pfitzmann, B. Pfitzmann, M. Schunter, M. Waidner:* „Trusting Mobile User Devices and Security Modules“, IEEE Computer, February 1997, pp. 61-68

[8] ITU-T: „Digital Subscriber Signalling System No. 1, Network Layer, User-Network Management“, ITU-T Recommendations Q.930-Q.940, Geneva, 1993

[9] ITU-T: „Data Networks And Open System Communications, Directory, Information Technology - Open Systems Interconnection - The Directory: Authentication Framework“, ITU-T Recommendation X.509, 1993

[10] *R. Manterfield:* „Common-Channel Signalling“, IEE Telecommunications Series 26, Peter Peregrinus Ltd., 1991

6th Open Workshop on High Speed Networks
University of Stuttgart, October 8-9, 1997

Signalling And Service Interfaces For Separating Security Sensitive Telecommunication Functions Considering Multilateral Security

R. Sailer
sailer@ind.uni-stuttgart.de
http://www.ind.uni-stuttgart.de

Overview:

- **Introduction**
- **Security requirements on network services**
- **Signalling interfaces supporting security services**
- **Outlook**

- **The realization of security mechanisms poses strong requirements on runtime environments**
- **Security requirements are taken into account insufficiently in todays networks**

$\Rightarrow$ **Integration of security mechanisms comprises**

- ❍ **implementation of the security mechanisms**
- ❍ **architectural enhancements of the runtime environment**

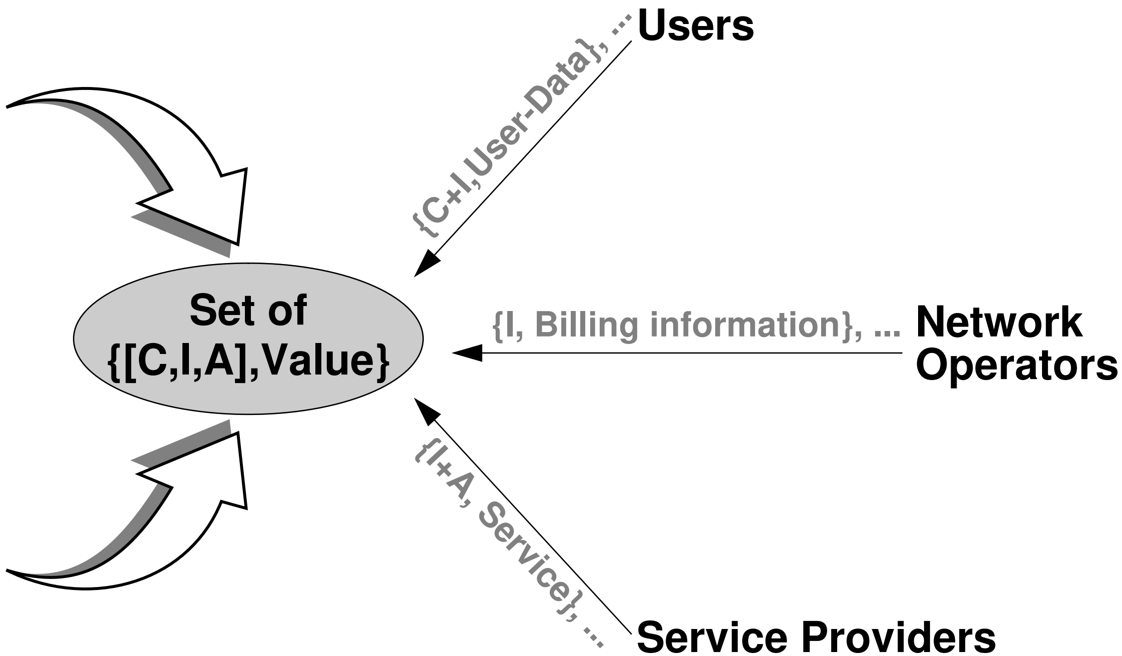
❒ **Forward-looking telecommunication networks must be able to fulfil security requirements**

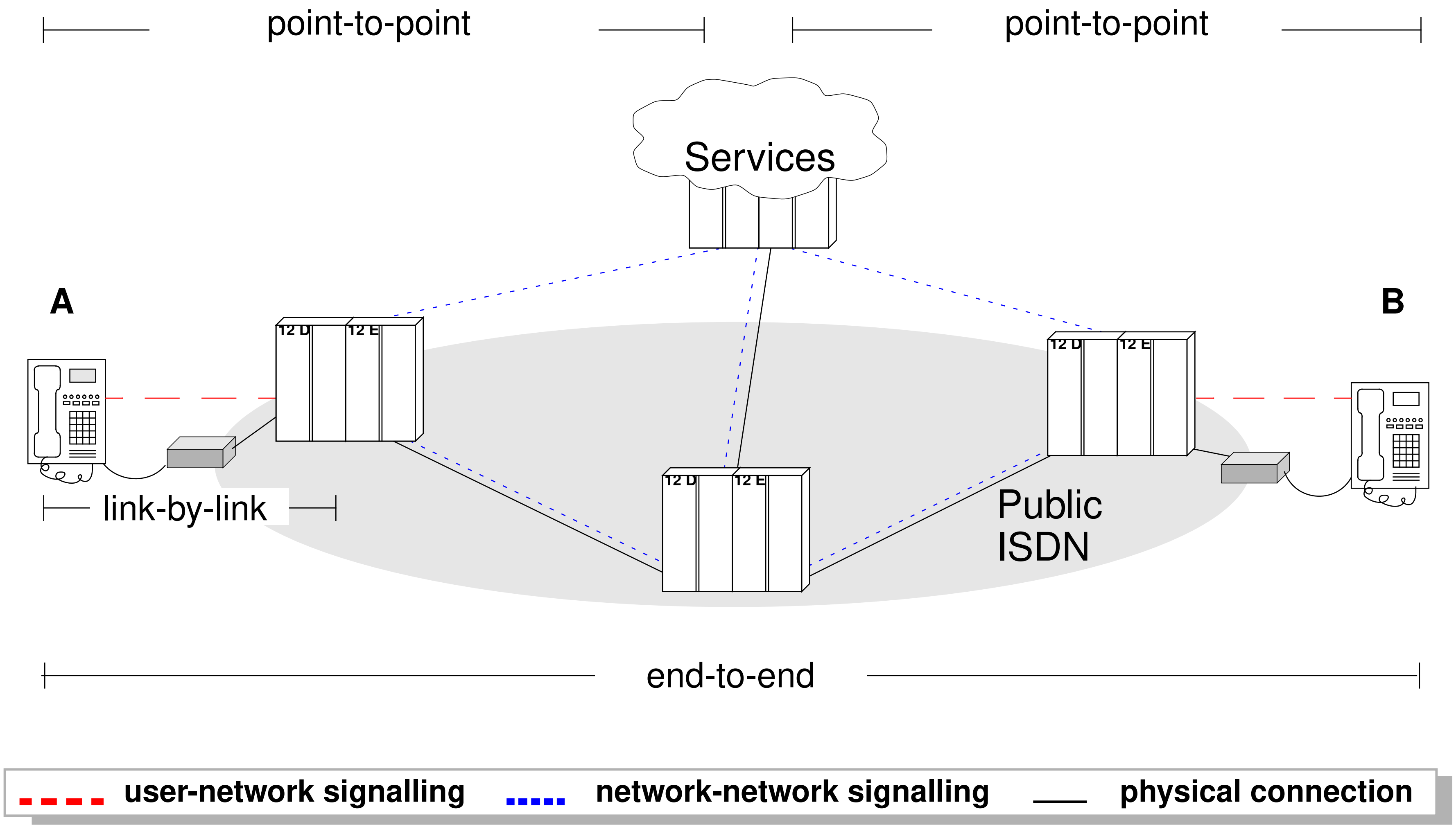
- ❍ **on demand**
- ❍ **efficiently (scalable, easy to integrate, tailor-made)**
- ❍ **multilaterally (balancing requirements concerning different interest groups)**

because security will become a prerequisite for the use of network services

Network Security: Requirements and Objects

- Security requirements
  - C (Confidentiality)
  - I (Integrity)
  - A (Availability)
- Values to be secured
  - Infrastructure
  - Functionality
  - Application Data
  - Control Data
  - State Information




point-to-point
point-to-point
Services
A
B
12 D
12 E
12 D
12 E
12 D
12 E
link-by-link
Public
ISDN
end-to-end
user-network signalling
network-network signalling
physical connection

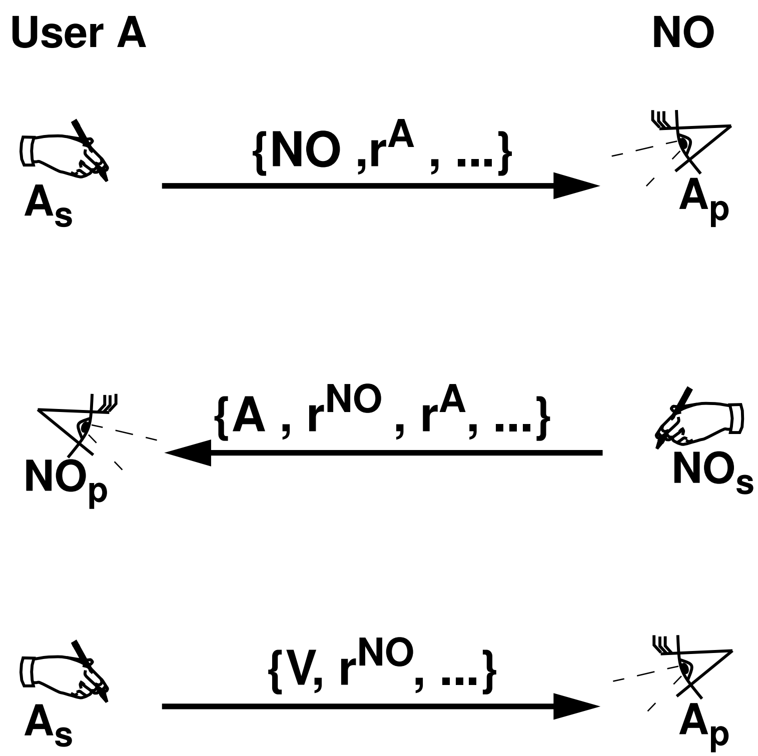
New Requirements

Exemplary service enhancements

- Verification of the identities claimed by user A and network operator NO
- Encryption and integrity mechanisms for user data and control data

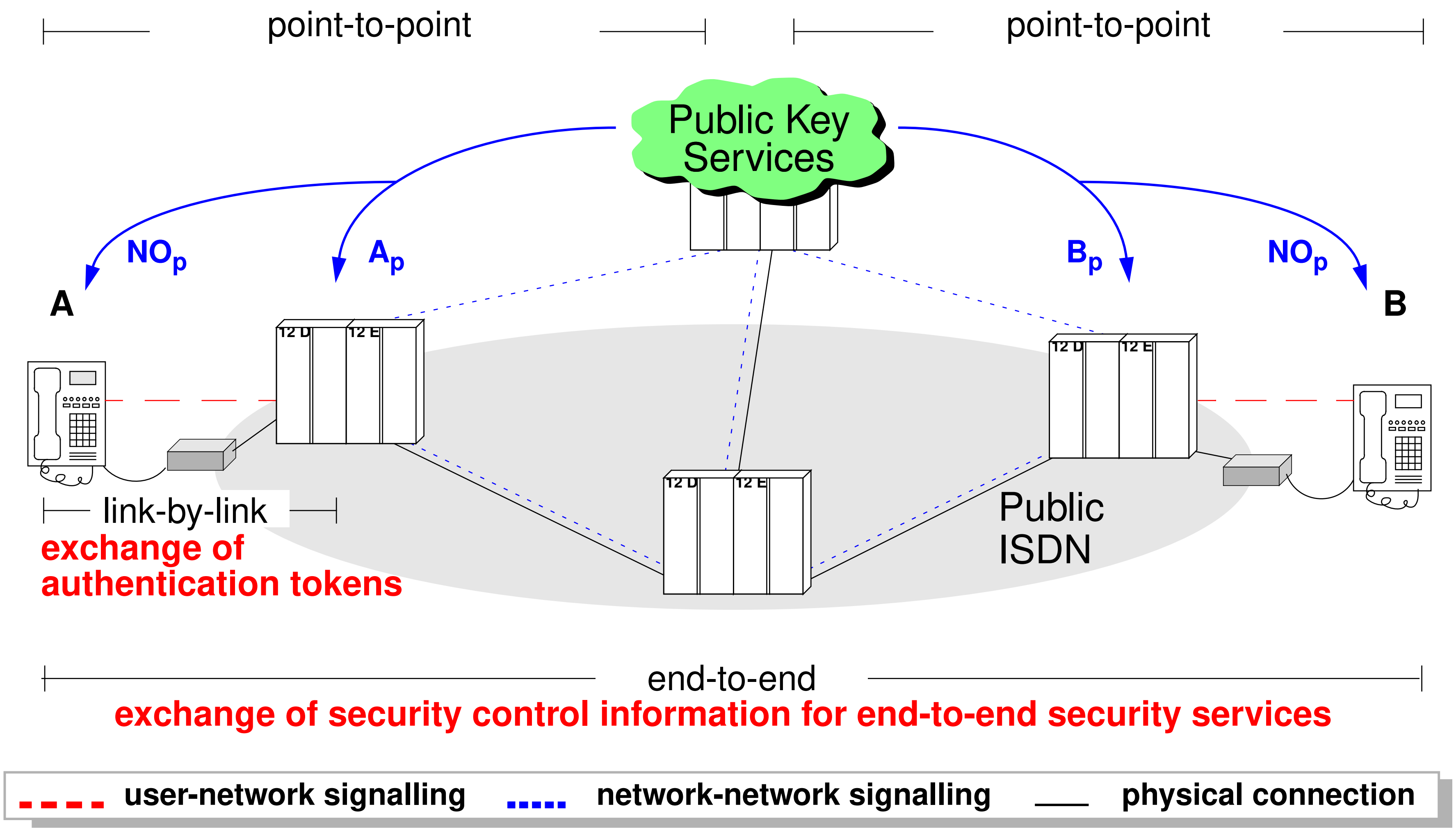
Resulting requirements on signalling

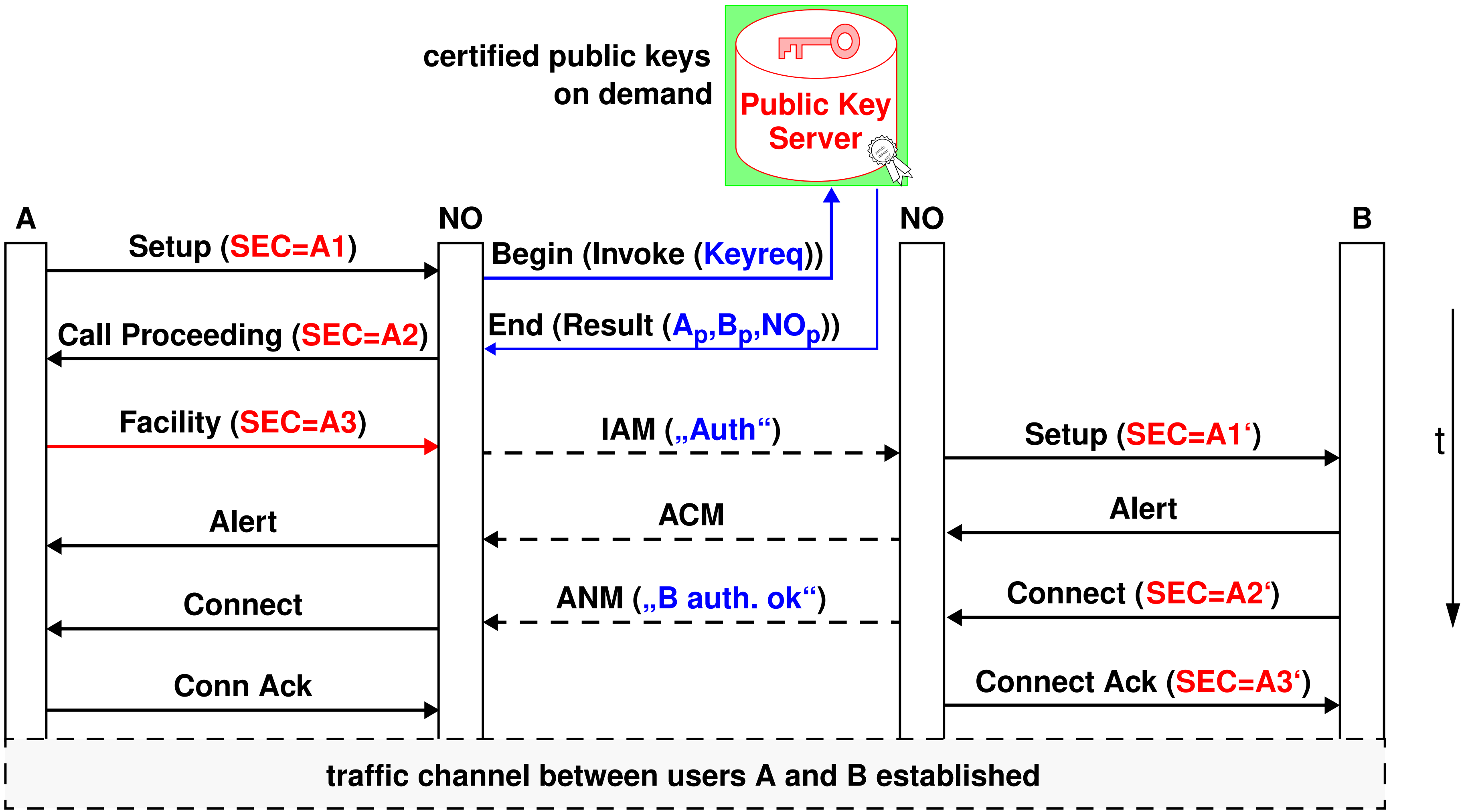
- Exchange of authentication messages
- Retrieval of valid public keys
- Implementation of the authentication protocol control
- Merging authentication and call control

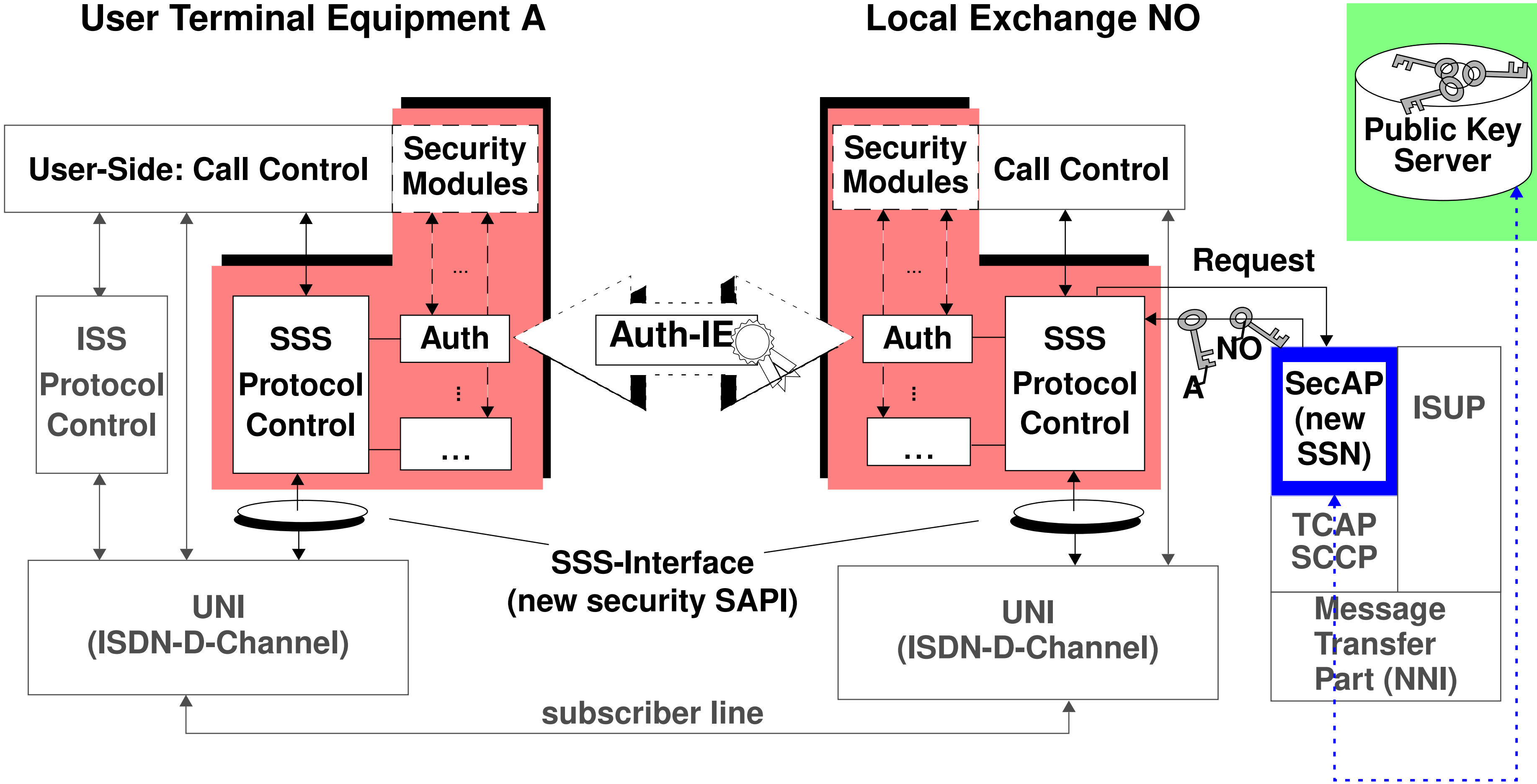


A, NO : claimed identities
A_s, NO_s : secret signature keys
A_p, NO_p : public verification keys

New Scenario




certified public keys
on demand
Public Key
Server
A
NO
NO
B
Setup (SEC=A1)
Begin (Invoke (Keyreq))
Call Proceeding (SEC=A2)
End (Result (A_p,B_p,NO_p))
Facility (SEC=A3)
IAM („Auth“)
Setup (SEC=A1‘)
t
Alert
ACM
Alert
Connect
ANM („B auth. ok“)
Connect (SEC=A2‘)
Conn Ack
Connect Ack (SEC=A3‘)
traffic channel between users A and B established



SSS ... Security Supplementary Services ISS ... ISDN Supplementary Services SecAP ... Security Application Part

Outlook

- Simulation and validation of prototype SSS and SecAP specifications
- Performance evaluation of an exemplary SSS and SecAP protocol control
  - timing requirements of the proposed security enhanced protocols
  - side effects on existing call control protocols and related timing requirements
- Integration of protocol control concerning
  - security supplementary services protocol control
  - security application part
  - exemplary security protocols based on SSS and SecAP
- Integration into existing software and hardware architectures