Möglichkeiten des Zugangs zu PKI-Diensten für Anwender der SS7-Infrastruktur des ISDN

Matthias Kabatnik[1]

Kurzfassung
Der zunehmende Bedarf an Sicherheitsmechanismen für Kommunikationsvorgänge erfordert innerhalb der diensteintegrierenden digitalen Netze (Integrated Services Digital Network, ISDN) unter anderem den Einsatz von kryptographischen Methoden zur Realisierung von Sicherheitsfunktionen. Diese Methoden setzen die Verfügbarkeit von geheimen und öffentlichen Schlüsseln sowie Einrichtungen zu deren Generierung, Verteilung und Überwachung voraus. In diesem Papier werden Möglichkeiten vorgeschlagen und untersucht, die sich eignen, solche Dienste innerhalb des Zentralkanalsignalisiernetzes Nr. 7 (SS7-Netz) im ISDN einzurichten bzw. sie aus dem ISDN netzübergreifend in TCP/IP-Netzen anzusprechen.

Stichwörter: Zertifikate, PKI, SS7, ISDN

1 Motivation

Mit steigender Verfügbarkeit neuer Technologien werden viele Abläufe des täglichen Lebens auf elektronische Dienste abgebildet. Zu diesen Abläufen gehören neben Zahlungsvorgängen auch Rechtsgeschäfte, wie beispielsweise der Abschluß eines Kaufvertrages. Bei diesen Vorgängen besteht die Notwendigkeit, die Beteiligten zu authentisieren, die ausgetauschten Informationen vertraulich und integritätsgesichert zu verarbeiten und ggf. Rechtsverbindlichkeit sicherzustellen.

Um diesen Sicherheitsanforderungen zu genügen, wurden und werden Verfahren wie beispielsweise Public-Key-Verschlüsselung entwickelt (siehe z. B. [1]) und durch Integration in Anwendungsprogramme am Markt etabliert. Ein Problem bei dieser Form von Kryptographie ist die Generierung und Verteilung der dafür erforderlichen öffentlichen Schlüssel, deren Integrität und Authentizität sichergestellt sein muß.

In diesem Kapitel wird eine Möglichkeit zur Umsetzung dieser Anforderungen in Form einer Public Key Infrastruktur (PKI) eingeführt und einige Anwendungsfälle im SS7 vorgestellt. In Kapitel 2 werden Randbedingungen erläutert, die bei der Integration neuer Sicherheitsfunktionen im ISDN relevant sind. Kapitel 3 enthält einige Lösungsansätze, die zur Realisierung des PKI-Zugangs für verschiedene Anwendungsfälle in Frage kommen. Die Vorschläge werden schließlich in Kapitel 4 bezüglich verschiedener Gesichtspunkte wie z. B. Integrierbarkeit und Skalierbarkeit bewertet.

---

[1] Universität Stuttgart, Institut für Nachrichtenvermittlung und Datenverarbeitung (IND)

1.1 Public Key Infrastruktur

Einen Ansatz, der asymmetrische Kryptographie mit vielen Kommunikationspartnern sinnvoll einsetzbar macht, stellt eine Public Key Infrastruktur (PKI) dar.

Ein Bestandteil einer PKI sind die sogenannten Zertifizierungsstellen (Certification Authorities, CAs). Diese generieren und verteilen Schlüsselpaare oder zertifizieren die öffentlichen Schlüssel von Personen oder anderer Instanzen der PKI. Für Zertifikate gibt es standardisierte Formate. Für die hier vorgestellten Überlegungen soll grundsätzlich der Standard X.509 in der Version 3 als Grundlage dienen.

Neben den CAs gibt es weitere Einrichtungen. Hierzu gehören die Verzeichnisdienste, die den Zugriff auf öffentliche Schlüssel, Zertifikate und Widerrufslisten von Zertifikaten (Certificate Revocation Lists, CRL) anbieten. Zertifikate bestätigen die Authentizität und Integrität eines elektronischen Dokumentes, z. B. eines öffentlichen Schlüssels. Weiterhin gibt es Einrichtungen zur Registrierung von neuen Teilnehmern der PKI (Registration Authorities) und übergeordnete Instanzen, die zur Aufstellung und Überwachung von Sicherheitspolitiken für die PKI zuständig sind (Policy Authorities). Auf die beiden letztgenannten Einrichtungen wird an dieser Stelle nicht weiter eingegangen, sondern z. B. auf [4] verwiesen.

Zur Zeit beschränken sich Implementierungen solcher PKIs hauptsächlich auf den Bereich der paketvermittelnden Netze auf der Basis von TCP/IP (im folgenden als TCP/IP-Netze bezeichnet), in denen die meisten neuen elektronischen Dienste, wie beispielsweise E-Mail oder Internet Shopping, angesiedelt sind.

1.2 Public Key Infrastrukturen im Signalisiersystem Nr. 7

Neben dem Datenaustausch im Internet findet jedoch ein sehr großer Teil der Kommunikation im geschäftlichen und privaten Umfeld im Bereich des ISDN[2] mit seinen Diensten zur Sprach-, Fax- und Datenübertragung statt.

Durch die Diskussion der Sicherheitsaspekte für neue Dienste in TCP/IP-Netzen sind Nutzer und Dienstanbieter auch hinsichtlich der über ISDN geführten Kommunikation in Fragen der Sicherheit aufgeschlossener geworden. Laufende Forschungsarbeiten beschäftigen sich daher mit der Integration von Sicherheitsfunktionen im Bereich der ISDN-Dienste [5]. Um diese Dienste zu realisieren, ist auch im ISDN die oben genannte PKI notwendig.

Ein Anwendungsbeispiel ist die sichere Authentisierung des Gesprächspartners bei Telefonverbindungen. Durch geeignet erweiterte Endgeräte und Protokolle kann diese über Verfahren nach X.509 erfolgen, welche entsprechende Verzeichnis- und Zertifizierungsdienste benötigen [5].

---

[2] Das ISDN vermittelt auch Sprach-, Daten- und Faxverkehr, der über analoge Zugangsnetze zugeführt wird.

Hierzu müssen durch das Telefonnetz entsprechende CA- und Verzeichnisdienste zur Verfügung gestellt werden, die über das SS7-Netz zugänglich sind.

Durch die Öffnung der Telekommunikationsnetze für den freien Wettbewerb sind viele neue nationale Netzbetreiber entstanden. Bei der Schaffung von Diensten, die über Netzgrenzen hinweg operieren, gibt es bisher keinerlei Möglichkeit der Authentisierung von Nachrichten oder Einsatz kryptographischer Verfahren im Bereich der Signalisierung. An dieser Stelle können ebenfalls Mechanismen eingerichtet werden, die durch Verwendung von Authentikationsverfahren die vorhandenen Schnittstellen sicherer machen oder neue Schnittstellen ermöglichen. Ein Beispiel hierfür ist eine Öffnung der Netzgrenzen zur Weiterleitung von Meldungen der Fernwartung von Signalisierknoten, die mit den heutigen Schnittstellen nicht ohne Risiken durchführbar ist [8].

Bei einer solchen Anwendung werden Vermittlungsstellen zu Nutzern (Clients) einer PKI und es werden ihnen zertifizierte Schlüssel zugeordnet. Es müssen daher geeignete Kontrollmechanismen zur Überwachung der korrekten Bindung von Schlüssel und Vermittlungs- oder Signalisiereinrichtung geschaffen werden.

2 Technische und organisatorische Randbedingungen

Soll in ein bestehendes System wie das ISDN eine PKI integriert werden, so müssen die technischen Randbedingungen, die durch die vorhandene Netztechnik gegeben sind, betrachtet werden. Überdies ist auch der organisatorische Rahmen bedeutsam, der durch einen offenen Kommunikationsmarkt mit vielen Anbietern von Kommunikationsdienstleistungen entstanden ist. Im folgenden werden diese Randbedingungen aufgeführt.

2.1 Technisches Umfeld

Bei der Betrachtung der Integration von PKI-Technologie in die ISDN-Kommunikationsabläufe sind die technischen Gegebenheiten des ISDN-Netzes als relevante Randbedingungen zu berücksichtigen.

Das ISDN verfügt durch die Trennung von Nutz- und Signalisierkanälen und die Verwendung der Zentralkanalzeichengabe mit dem Signalisiersystem Nr. 7 (SS7) über ein sehr leistungsfähiges Signalisiernetz. Dieses Signalisiernetz kann zur Übertragung von Nachrichten genutzt werden, wie sie zwischen Instanzen einer PKI auftreten. Die damit verbundenen Abläufe müssen jedoch über die verfügbaren Basisprotokolle abgewickelt werden. Bild 1 zeigt einen Ausschnitt der Protokollschichtung des SS7.

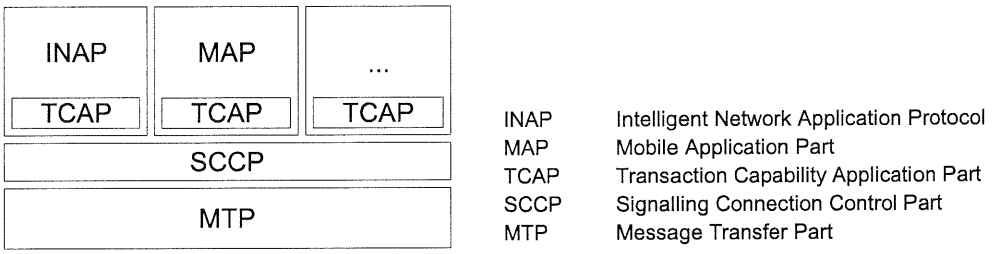

Bild 1: Protokollschichtung des SS7 (vereinfacht)

Der Message Transfer Part (MTP) stellt den darüberliegenden Protokollschichten ein sehr leistungsfähiges Netz zur gesicherten Übertragung paketorientierter Signalisiernachrichten zur Verfügung. Allerdings lassen sich innerhalb des MTPs nur Instanzen im eigenen Netz adressieren. Ein Ziel in einem fremden Netz kann nicht angesprochen werden.

Der Signalling Connection Control Part (SCCP) erweitert die Fähigkeiten des MTP durch die Möglichkeit, Daten verbindungsorientiert auszutauschen. Er hat darüber hinaus die Fähigkeit, auch Ziele außerhalb des eigenen Netzes anzusprechen. Hierzu werden als Adressen die sogenannten Global Titles (GTs) verwendet. Diese Adressen sind mit einer netzübergreifend gültigen Rufnummer vergleichbar, die dazu verwendet werden kann, Funktionen zu adressieren, ohne ihre Lokalisierung im Netz zu kennen. Da ein GT nicht direkt zur Adressierung im MTP verwendet werden kann, erfolgt eine Umsetzung mit Hilfe einer Global Title Translation (GTT). Mit dieser GTT kann entweder das endgültige Ziel der Nachricht oder eine für eine weitere Adreßumsetzung zuständige Vermittlungseinheit bestimmt werden. Durch diesen Mechanismus lassen sich Adressierungsräume sehr flexibel realisieren.

Der Transaction Capability Application Part (TCAP) unterstützt den Austausch von nicht nutzkanalbezogener Information zwischen Anwenderteilen des SS7 untereinander oder mit Datenbanken im Netz. Es werden dabei Operationen und Dialoge unterstützt. Operationen sind Vorgänge, die von einem Kommunikationspartner (Originating Entity) angestoßen werden, beim Empfänger (Destination Entity) ausgeführt werden und deren Ergebnis ggf. zurückgemeldet wird. Diese Operationen und ihre Ergebnisse können wieder zu Dialogen zusammengefaßt werden, die zwischen zwei Kommunikationspartnern ablaufen. Der TCAP liefert die notwendigen Protokollelemente, um diese Dialogfunktionen zu unterstützen. Er ist deshalb sehr gut zur Unterstützung der in einer PKI auftretenden Kommunikationsvorgänge geeignet. Der TCAP wird in der Regel als integraler Bestandteil des jeweiligen darüberliegenden Anwenderteils realisiert.

Die Anwenderteile (Application Parts, AP) der SS7-Signalisiernetze sind verschiedene anwendungsspezialisierte Funktionseinheiten. Hier seien beispielhaft der für die Ausführung der Mobilfunksignalisierung zuständige Mobile Application Part (MAP) und der Protokollteil für Kommunikationsvorgänge im Intelligenten Netz (Intelligent Network Application Protocol, INAP) genannt.

Sollen aus dem intelligenten Netz oder dem Mobilfunknetz heraus über diese Anwenderteile PKI-Funktionen genutzt werden, so müssen diese über die darunterliegenden Protokolle erreichbar sein.

Eine ausführliche Darstellung der Protokolle findet sich in [6] und [7].

2.2 Organisatorische Gegebenheiten

Von der organisatorischen Seite sollen im Wesentlichen zwei Punkte berücksichtigt werden.

Einer dieser Punkte ist die Einbeziehung von bestehender Infrastruktur bei der Realisierung einer PKI. Die Entwicklung von PKI-Anwendungen hat bisher hauptsächlich für TCP/IP-basierte Netze stattgefunden. Aus diesem Grund wird derzeit auf dieser Plattform an vielen Implementierungen gearbeitet. Es ist daher sinnvoll, daß ein Netzbetreiber, der sowohl über ein SS7- als auch ein TCP/IP-Netz verfügt, eine bereits vorhandene PKI des TCP/IP-Bereiches für die Anwendungen im SS7 verwendet. Für einen solchen Fall sind Lösungen zu suchen, die die Anbindung von Nutzern des SS7 an die Dienste im Intranet ermöglichen.

Der andere zu berücksichtigende Aspekt ist die Situation im Telekommunikationsmarkt. Es gibt nicht mehr nur die Netze der nationalen Telefongesellschaften innerhalb eines Landes, sondern inzwischen eine ganze Reihe nationaler, konkurrierender Netze, die miteinander verbunden sind.

Diese Situation begünstigt das Entstehen verschiedener, unabhängiger PKIs. Sollen jedoch Zertifikate über die Netzgrenzen hinaus verwendet werden, so bedarf es einer übergeordneten Struktur, die netzübergreifende Vertrauenspfade[3] realisiert.

3 Lösungsvorschläge

Nachdem im vorigen Kapitel einige zu beachtende Randbedingungen eingeführt wurden, werden in diesem Abschnitt Vorschläge für mögliche Implementierungen gemacht. In Kapitel 4 werden diese Ansätze dann hinsichtlich ihrer Eignung bewertet und – soweit sinnvoll – miteinander verglichen.

3.1 SS7-Dienst über TCAP und SCCP

Sollen PKI-Funktionseinheiten wie CAs und Verzeichnisdienste innerhalb des SS7 implementiert werden, so können diese über einen eigenständigen PKI-Anwenderteil auf den Protokollstack aufgesetzt werden.

Ein solcher Anwenderteil ist somit vergleichbar mit den Anwenderteilen des INAP oder des MAP, die ebenfalls auf dem TCAP aufsetzen und diesen zur Steuerung ihrer

[3] Vertrauenspfade bezüglich einer Instanz sind Wege durch eine PKI-Struktur, deren Zertifikatkette durch die Instanz validiert werden kann.

aus Operationen aufgebauten Dialoge mit anderen Anwendern verwenden. Bild 2 veranschaulicht dieses Beispiel.

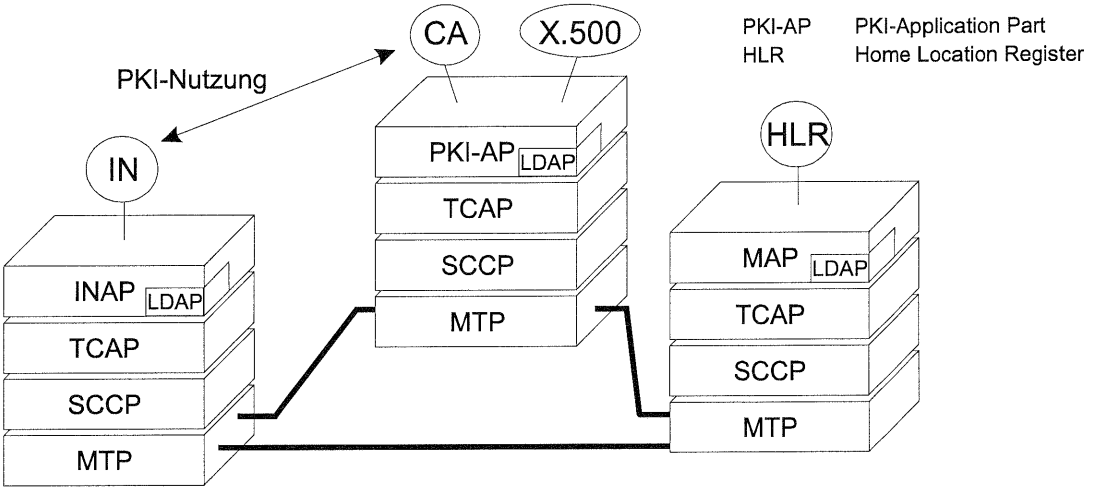

Bild 2: CA und Verzeichnisdienst als SS7-Applikation

Die Unterscheidung zwischen den verschiedenen Anwenderteilen innerhalb eines Signalisierknotens wird bei der Adressierung durch die Subsystem-Nummer (SSN) bewirkt. Für den neuen Dienst muß deshalb eine eigene SSN definiert werden.

Die im Bild 2 gezeigten Anwenderteile MAP und INAP müssen mit einer entsprechenden Funktionalität zur Nutzung der PKI-Elemente ausgestattet werden. Hierbei können die Dialogfunktionen des TCAP-Protokolls genutzt werden. Die Dialogstruktur und die Formate der verwendeten Nachrichten können als standardisiertes Protokoll (z. B. Lightweight Directory Access Protocol, LDAP) implementiert und auf die TCAP-Funktionen abgebildet werden.

Zur Adressierung von Funktionseinheiten auf Anwendungsebene, also in den X.509-Zertifikaten, werden Unified Resource Identifiers (URIs) verwendet, die eine plattformunabhängige Kompatibilität der Zertifikate gewährleisten. Daraus ergibt sich das Problem der Adreßumsetzung von URI auf GT-Adressierung des SCCP. Bis zur Einrichtung im SS7-Netz verfügbarer Adreßauflösungsmechanismen muß hier mit fest konfigurierten Tabellen gearbeitet werden.

Für die Einrichtung der PKI-spezifischen Dienste (z.B. CAs) muß eine spezielle Hardware-Plattform geschaffen werden oder es müssen die dafür vorgesehenen Netzelemente durch geeignete Module erweitert werden. Die zur Zeit in der Vermittlungstechnik eingesetzten Hardware-Plattformen entsprechen nicht den Anforderungen, die im Zusammenhang mit einer PKI gestellt werden, da sie keine sicheren kryptographischen Module und keine abgeschirmten Speicherbereiche enthalten.

Wenn eine große Menge von Zertifikaten benötigt wird, z. B. beim Einsatz von Teilnehmerzertifikaten, dann kann sich eine notwendige hierarchische Struktur von CAs an den Netzebenen der Vermittlungsstellen und den Einzugsbereichen einzelner Teilnehmervermittlungsstellen orientieren. In diesem Fall ist auch eine elektronische

Anbindung der CA an die Registrierungsstellen notwendig, so daß als CA fungierende Signalisierknoten auch einen Übergang zum TCP/IP-Netz benötigen.

3.2 Dienst im TCP/IP-Netz

Eine weitere Möglichkeit ist die Anordnung der Dienste im TCP/IP-Netz bzw. die Nutzung bereits existierender Strukturen. Hierbei ist ein entsprechender Übergang zwischen dem SS7-Netz und der TCP/IP-Technologie notwendig. Dieser Übergang kann auf verschiedene Weise gestaltet werden.

a) Eine Möglichkeit besteht darin, jeden der Signalisierknoten mit einem Übergang zum TCP/IP-Netz auszustatten, wie dies in Bild 3 gezeigt wird.

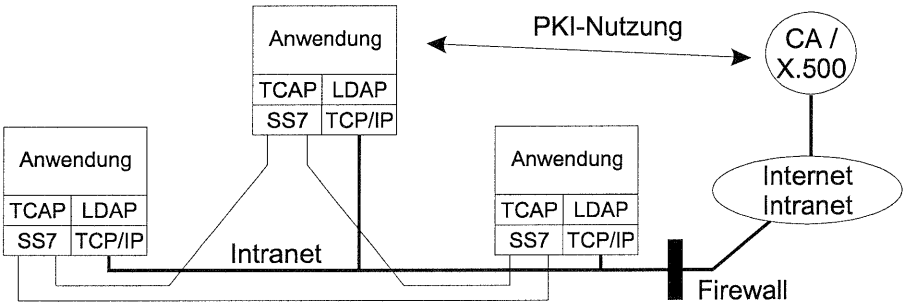

Bild 3: Zugang zu Sicherheitsdiensten über TCP/IP-Netze

Es müssen dazu die TCP/IP-Protokoll-Stacks in den Signalisierknoten implementiert werden oder vorhandene TCP/IP-Anbindungen für die betroffenen Anwenderteile des SS7 zugänglich gemacht werden. Diese Anwenderteile des SS7 müssen ebenfalls erweitert werden, da sie auf die neue interne Schnittstelle zugreifen.

Die Adressierung der Funktionseinheiten der PKI kann damit direkt aus den Anwendungen erfolgen, die durch Zugriff auf die TCP/IP-Schnittstelle die TCP/IP-Adressierung verwenden können.

Zur Adreßauflösung der URIs in den Zertifikaten können die im TCP/IP-Netz eingesetzten Namensverzeichnisdienste (Domain Name Server, DNS) genutzt werden.

Es sind wie bei der SS7-Lösung sichere Umgebungen für Kryptomodule und Speicherung der Schlüssel innerhalb der Signalisierknoten einzurichten.

Bei der Anbindung an ein TCP/IP-Netz müssen Schutzmaßnahmen zur Bereichstrennung durchgeführt werden. In Bild 3 wird eine Lösung mit einem Intranet gezeigt, das alle Signalisierpunkte miteinander verbindet. Wird dieses Netzsegment ausschließlich für die PKI-Daten verwendet, d.h. sind keine weiteren Nutzer angeschlossen, so kann die Abschirmung durch einen Firewall am Übergangspunkt zu anderen Netzsegmenten erfolgen.

Wenn die Kopplung der Signalisierknoten nicht in dieser Form erfolgen kann (z. B. bedingt durch die räumliche Verteilung der verschiedenen Standorte der Signali-

sierknoten), kann der Übergang in das Internet oder ein anderes Intranet auch jeweils direkt am Signalisierpunkt eingerichtet werden. Dabei wird an jedem Übergang ein entsprechender Firewall benötigt.

Ein weiterer zu beachtender Punkt ist die Abgrenzung der unterschiedlichen Protokollwelten innerhalb der Signalisierknoten. Hier muß eine klare Trennung der Netzfunktionen durchgeführt werden, um unerwünschte Wechselwirkungen zwischen den Netzen und ihren Anwendungen zu vermeiden. So darf beispielsweise eine Überlastsituation im Bereich des SS7-Stacks nicht zu Beeinträchtigungen der TCP/IP-Funktionen führen und umgekehrt.

b) Eine anderer Ansatz, mit dem SS7-Anwenderteile auf eine TCP/IP-PKI zugreifen können, ist ein zentraler Übergang über einen ausgezeichneten Signalisierknoten durch Realisierung eines Proxy-Dienstes. Dieser Ansatz wird in Bild 4 gezeigt.

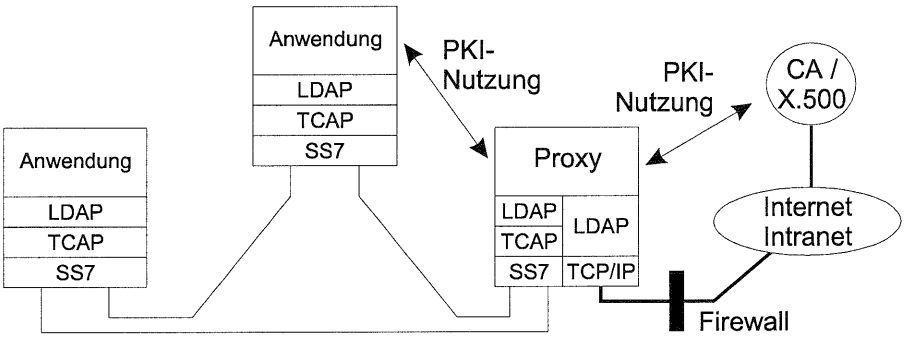

Bild 4: Zentraler Zugang mit Proxy-Dienst

Bei dieser Variante wird der Zugriff über einen speziell für diesen Zweck eingerichteten Signalisierknoten geführt, in dem ein sogenannter Proxy-Dienst aufgesetzt wird (siehe Bild 4). Dieser stellt sich für die Anwender aus dem SS7 wie der eigentliche Sicherheitsdienst dar, den diese über die SS7-Signalisierung ansprechen. Er leitet die Anfragen seinerseits an den im TCP/IP-Netz befindlichen Dienst weiter.

Über einen solchen Proxy-Dienst werden sowohl CAs als auch Verzeichnisdienste angesprochen. Zur Adressierung von Diensten kann bei Verwendung eines Proxies auch der Adreßtyp des Zielnetzes (hier TCP/IP) verwendet werden, indem die Adressen durch Tunnelung des LDAP-Protokolles über den TCAP von den Anwendern zum Proxy übertragen werden.

Die Adressierung des Proxies erfolgt über GT-Adressen. Dadurch kann die Position des Proxies durch Ausnutzung der Anpassungsmöglichkeiten im Routing innerhalb eines SS7-Netzes sehr variabel gehalten werden. Prinzipiell ist es auch möglich, den Proxy in einem fremden Netz zu nutzen, da mit dem SCCP-Protokoll Kommunikationsbeziehungen auch über Netzgrenzen hinweg aufgebaut werden können.

Die Kontrolle der über die Netzgrenze ausgetauschten Daten kann durch den Proxy erfolgen. Damit lassen sich Filterfunktionen zur Trennung der verschiedenen Netzbereiche einrichten.

c) Grundsätzlich sind auch hybride Ansätze möglich, die Aspekte der verteilten Struktur aus a) mit zentralen Einrichtungen des Ansatzes b) kombinieren.

Eine Variante ist der Einsatz mehrerer wahlweise ansprechbarer Proxy-Übergänge innerhalb des SS7-Netzes. Diese Maßnahme kann sowohl aus Lastgründen wie auch zur Erhöhung der Ausfallsicherheit eingesetzt werden.

Die Einführung mehrerer in ihrer Funktion gleichartiger Proxies kann ohne Veränderung der Clients erfolgen, da die transparente Adressierung durch Global Titels mit Adreßumsetzung im SCCP die Ausnutzung mehrfach vorhandener Systeme unterstützt.

Grundsätzlich können auch Signalisierknoten mit direktem TCP/IP-Zugang mit Knoten kombiniert werden, die den Zugang über Proxy-Server erhalten. Diese Mischformen sollen an dieser Stelle jedoch nicht weiter betrachtet werden.

3.3 Dienst an der Bereichsgrenze

Wenn verschiedene PKIs zusammenarbeiten sollen, so müssen, wie bereits in Kapitel 2.2 angesprochen, Möglichkeiten bereichsübergreifender Vertrauenspfade bereitgestellt werden.

Eine dafür geeignete Vorgehensweise ist die Zertifizierung der jeweiligen Principal-CAs durch eine übergeordnete CA (z. B. nationale Root-CA). Sollen jedoch nur Teilbereiche (also nur die von bestimmten CAs ausgegebenen Zertifikate) in die Ausweitung des Wirkbereiches miteinbezogen werden, so kann der Einsatz einer sogenannten Bridge-CA in Betracht kommen [3]. Diese Bridge-CA stellt Cross-Zertifikate für einzelne CAs der zu verbindenden PKIs aus und kann dabei auch Gültigkeitsbeschränkungen verwenden. Durch eine übergeordnete Instanz muß jedoch die Verträglichkeit der Sicherheitspolitiken der zu zertifizierenden CAs geprüft werden [4].

Wenn eine PKI eines SS7-Netzes in dieser Form mit der PKI eines TCP/IP-Netzes verbunden werden soll, kann eine Anbindung nach Bild 5 eingesetzt werden. Die entsprechende CA und ggf. ein Verzeichnisdienst werden sowohl mit einer Schnittstelle zu TCP/IP-Netzen wie auch zu SS7-Netzen versehen.

Soweit keine anderen Kopplungspunkte zwischen den Netzen bestehen, muß dieser Dienst auch den Zugriff auf alle CRLs der verbundenen Netze ermöglichen. Dies kann entweder durch Sammlung der CRLs in dem ausgezeichneten Knoten an der Netzgrenze erfolgen oder durch Weiterleitung der Anfragen an die zugehörigen Verteilungspunkte der CRLs. Im zweiten Fall, der bei großen PKIs notwendig werden kann, muß die CA/X.500-Funktion durch Proxy-Dienste zur Abfrage von fernen CRLs ergänzt werden.

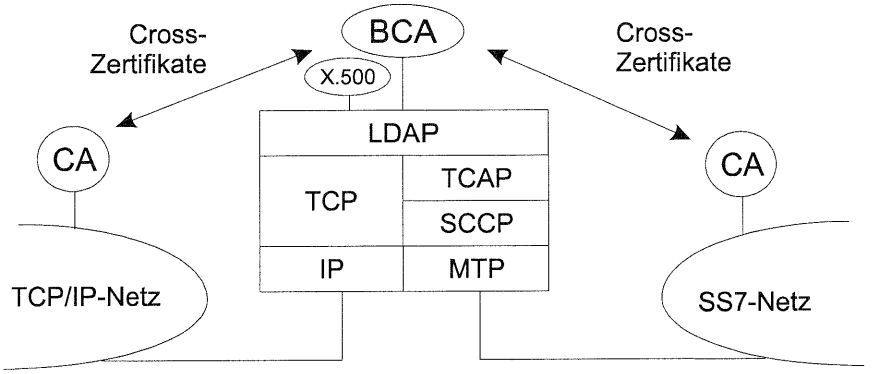

Bild 5: Verbindung unterschiedlicher PKI-Bereiche und Übergang zwischen Technologien durch (Bridge-)CA

4 Bewertung

Die verschiedenen vorgeschlagenen Realisierungsmöglichkeiten müssen abschließend hinsichtlich ihrer Eignung bewertet werden. Dazu werden folgende Teilbereiche betrachtet:

- Integrierbarkeit in bestehende Strukturen
- Skalierbarkeit der Dienste
- Adressierung der Dienste
- Verfügbarkeit
- Abgrenzung der Plattformen

4.1 Integrierbarkeit

Bei Einführung neuer Dienste oder Leistungsmerkmale ist es von entscheidender Bedeutung, wie hoch der Aufwand für die Integration in die bestehende Infrastruktur ist. Besonders günstig sind Lösungen, die als sogenanntes „Add-on" auf bestehenden Schnittstellen aufsetzen können und daher ohne eine Veränderung der bestehenden Technik auskommen. Sind Veränderungen im bestehenden System nicht zu vermeiden, so muß untersucht werden, wie umfangreich die Änderungen sind bzw. an wievielen Stellen diese durchgeführt werden müssen.

Die Schaffung einer völlig eigenständigen PKI im SS7 bedingt die Anpassung der Systeme an einigen Stellen, die hier nochmals kurz aufgeführt werden:

- Schaffung spezialisierter Signalisierknoten für PKI-Funktionen
- Erweiterung der PKI-Vermittlungsstellen mit Kryptomodulen
- Erweiterung der Anwenderteile um Funktionen zur PKI-Nutzung
- ggf. Schnittstellen zur Anbindung von Registrierungsstellen an die CAs

Ähnliches gilt für den Ansatz aus Kapitel 3.2 a) bei der Nutzung von Infrastruktur im TCP/IP-Bereich. Hier entfällt zwar der Aufwand für die Einrichtung der speziellen CA/X.500-Signalisierknoten, allerdings müssen alle Signalisierknoten mit Netzübergängen ausgestattet[4] und somit sowohl Hardware- wie auch Softwareänderungen durchgeführt werden. Zusätzlicher Aufwand entsteht durch die aus Sicherheitssicht in jedem Knoten notwendige Abgrenzung verschiedener Signalisiernetze.

Der Vorteil dieses Ansatzes ist die Vermeidung von PKI-spezifischer Signalisierung im SS7-Netz. Dieser Vorteil kommt jedoch nur in sehr leistungsschwach dimensionierten Netzen zum Tragen.

Im Gegensatz dazu kommen Ansätze mit zentralen Übergängen mit einem geringeren Hardwareaufwand aus. Die Signalisierknoten müssen die Kryptomodule erhalten und die Software der Anwender muß um ein Modul erweitert werden, das den Aufruf der kryptographischen Funktionen und ggf. die Generierung von LDAP-Anfragen beherrscht. Der Aufwand zur Schaffung neuer Schnittstellen in allen Knoten entfällt und es genügt, einen speziellen Signalisierknoten im Netz einzufügen, dessen Hard- und Software auf die Anforderungen eines PKI-Proxy-Dienstes oder einer (Bridge-)CA zugeschnitten werden kann. Der Aufwand für Softwarepflege und Wartung ist bei einem zentralen Ansatz deutlich geringer als bei verteilten Lösungen.

Insbesondere die Trennung der verschiedenen Funktionsbereiche kann bereits beim Neuentwurf einer speziellen Signalisiereinheit gezielt berücksichtigt werden. Somit ist es möglich, die internen Schnittstellen im Hinblick auf Sicherheitskriterien zu optimieren. Dies ist in der Regel einfacher als die nachträgliche Integration in ein bestehendes, gewachsenes System.

Insgesamt ist der Änderungsaufwand bei Ansätzen mit zentralen Funktionselementen geringer. Dieser Vorteil wird jedoch durch eine Konzentration des PKI-Datenverkehrs an diesen zentralen Punkten erkauft. Bei Fehldimensionierung kann diese Stelle zu einem „Flaschenhals“ werden.

Ein ebenfalls sehr wichtiger Aspekt ist die Herstellerabhängigkeit, die bei Änderungen und Erweiterungen in Vermittlungssystemen und Signalisierknoten besteht. Wird eine Funktion an einer zentralen Stelle im Netz eingeführt und durch standardisierte Protokolle angesprochen, so kann diese von beliebigen Herstellern bezogen werden.

4.2 Skalierbarkeit

Werden bei der Dimensionierung von Netzkomponenten die anfallende Verkehrsmenge bzw. die Häufigkeit einer Dienstnutzung oder die zu verarbeitenden Datenmengen unterschätzt oder wachsen diese Größen mit der Zeit an, so müssen die Systeme später entsprechend erweitert werden.

---

[4] Bei Signalisierknoten, die bereits über einen auf TCP/IP aufsetzenden Wartungszugang verfügen, verringert sich dieser Aufwand entsprechend.

Wird eine Erweiterung der Kapazitäten beim Einsatz von individuellen Übergängen (3.2 a) notwendig, so müssen unter Umständen alle Systeme erweitert werden. Beim Einsatz eines zentralen Proxy-Übergangs können weitere solche Übergänge hinzugenommen werden. Das bestehende System bleibt in seiner Struktur unverändert. Es müssen allerdings die neuen Möglichkeiten zur statischen oder dynamischen Lastteilung in den GTT vorgesehen werden. Die Erweiterung durch den Einsatz zusätzlicher Systeme ist darüberhinaus herstellerunabhängig.

Ein weiterer Aspekt der Skalierbarkeit ist die Möglichkeit, eine eingerichtete PKI-Struktur in eine übergeordnete netz- und technologieübergreifende PKI-Organisationsstruktur einzubinden bzw. kurze Validierungspfade zu anderen PKIs zu ermöglichen. Beim Entwurf einer eigenständigen PKI muß daher bedacht werden, daß zu einem späteren Zeitpunkt eine Cross-Zertifizierung mit CAs anderer PKIs möglich sein muß. Dadurch kann der Wirkbereich erweitert werden.

Da alle vorgestellten Ansätze auf Anwendungsebene Zertifikate verwenden können, die nach X.509v3 gestaltet sind, ist es leicht möglich, diese mit anderen Bereichen auszutauschen (ASN.1-Codierung). Es ist ebenfalls in allen Ansätzen die Einführung von Bridge-CAs möglich und somit kann auch für jeden Ansatz eine einfache und flexible Ausweitung der Vertrauensbereiche erfolgen.

Durch die Verwendung standardisierter Protokolle wie LDAP sind die Anwendungen von den darunterliegenden Mechanismen unabhängig und können bei Verfügbarkeit eines anderen Zugangs leicht an diesen angepasst werden.

4.3 Adressierung der Dienste

Auf Anwendungsebene können durch die Möglichkeit der Verwendung standardisierter Zertifikate Unified Resource Identifiers verwendet werden. Bei den Ansätzen, die direkt oder über Tunnelung auf TCP/IP-basierte Dienste zugreifen, gibt es bereits geeignete Methoden der Adreßauflösung durch Nutzung der bestehenden DNS.

Müssen URIs auf Global Title Adressen abgebildet werden, so ist derzeit keine geeignete dynamische Umsetzung der Adressen in den Signalisierknoten vorhanden[5]. Werden statische Adreßzuordnungen eingesetzt, so kommt es bei Veränderungen in der PKI zu höheren Antwortzeiten bei der Systemanpassung. Die Validierung von Zertifikaten aus fremden Bereichen, zu denen es keine Einträge in den Routingtabellen gibt, ist mit statischer Adreßzuordnung nicht möglich.

4.4 Verfügbarkeit

Der Verfügbarkeit von PKI-Diensten kommt im Bezug auf Sicherheit eine besondere Bedeutung zu, da die Verwendung von Sicherheitsfunktionalität Einfluß auf die Verfügbarkeit besitzen kann. Der Übergang aus einem SS7-Netz mit hoher Verfüg-

[5] Es gibt jedoch Projekte, die geeignete Ansätze verfolgen (z.B. TINA).

barkeit in ein Best-Effort-Netz, wie es die TCP/IP-Netze darstellen, ist daher ein zu betrachtender Aspekt.

Obwohl die Zuverlässigkeit von TCP/IP-basierten Netzen ständig durch Weiterentwicklung der Komponenten zunimmt, ist derzeit die Netzgüte und Verfügbarkeit von SS7-Netzen deutlich höher. Daher ist die Führung von PKI-Daten über SS7-Netze zu bevorzugen. Somit haben die Ansätze, die sich ausschließlich der SS7-Technologie bedienen oder ihre Daten bis zu einem zentralen Übergangspunkt im SS7 führen, einen klaren Vorteil gegenüber dem schnellstmöglichen Übergang in TCP/IP-Netze.

Ob die Verwendung von TCP/IP-Netzen und deren Komponenten aus Verfügbarkeitssicht überhaupt in Frage kommt, hängt in erster Linie von der Verwendung des TCP/IP-Netzes ab. Kann die Nutzung auf Netzsegmente beschränkt werden, die exklusiv für PKI-Daten zur Verfügung stehen, sind die notwendigen Verfügbarkeitswerte eher zu erreichen, als im Fall der gemeinsamen Nutzung von Netzinfrastruktur durch die PKI und andere Anwendungen.

4.5 Abgrenzung

Wenn Netze durch Gateways verbunden werden, so treffen an dieser Stelle unter Umständen Bereiche mit unterschiedlichem Sicherheitsniveau zusammen. Es muß daher sichergestellt werden, daß zwischen diesen Netzen keine unbeabsichtigten oder mißbräuchlichen Wechselwirkungen auftreten. Hierzu müssen die Übergänge durch eine Firewall-Funktion gesichert sein. In Abhängigkeit von Anzahl und Art der bestehenden Übergänge führt dies zu unterschiedlich hohem Aufwand für Schutzfunktionen. Deshalb müssen die verschiedenen Ansätze auch hinsichtlich dieser Fragestellung miteinander verglichen werden.

Da an jedem Übergang zwischen Netzen Maßnahmen durchgeführt werden müssen, die sowohl vor ungewollter Interaktion der verschiedenen Technologien wie auch vor gezielter Manipulation schützen, ist hinsichtlich des Verwaltungsaufwandes ein zentraler Übergang zu bevorzugen. Hier darf der Aufwand für Schutzmaßnahmen, z. B. eine Firewall-Funktion, relativ hoch sein, da er nur einmal durchgeführt werden muß.

Ein weiterer Vorteil des zentralen Übergangs wurde bereits in Kapitel 4.1 genannt. Da die Proxy-Server speziell für ihre Aufgabe neu entwickelt werden, lassen sich Fragen der Abgrenzung besser berücksichtigen, als bei nachträglicher Integration.

Nachteil eines zentralen Dienstes ist jedoch immer die Gefahr von Angriffen auf die Verfügbarkeit. Deshalb sollte vermieden werden, daß ein Proxy-Dienst aus dem Inter- oder Intranet direkt ansprechbar ist. Geht man von einer Plazierung der PKI-Ressourcen in einem abgeschirmten Netzsegment aus, so relativiert sich dieser Gefahrenpunkt wieder.

5 Zusammenfassung und Ausblick

In diesem Papier wurden verschiedene Ansätze vorgestellt, um Anwendungen der SS7-Protokolle Zugang zu Diensten einer Public Key Infrastruktur zu ermöglichen. Verschiedene Vor- und Nachteile der einzelnen Lösungen wurden aufgezeigt.

Welche Ansätze in der praktischen Umsetzung verfolgt werden, hängt von den jeweiligen konkreten Randbedingungen und dem Gewicht ab, das den einzelnen Bewertungskriterien jeweils zugeteilt wird.

Wegen seiner großen Flexibilität und den vergleichsweise geringen Änderungen im SS7-Netz wird der Ansatz auf Basis eines Proxy empfohlen.

Einige zukünftig zu behandelnde Aspekte sind:

- Geeignete Adreßauflösung für die Umsetzung von URIs auf Global Title Adressen
- Leistungsuntersuchung der verschiedenen Ansätze mit unterschiedlichen Anwendungsszenarien (Zahl der Anwender, Häufigkeit des CRL-Abrufs)
- Abrechnungsmöglichkeiten für die Nutzung der verschiedenen Dienste
- Konkretisierung der Anforderungen an die Trennung der verschiedenen Netzbereiche an Umsetzungspunkten

Diese Fragen müssen durch weitergehende Untersuchungen geklärt werden. Insbesondere ist die Vertiefung der Betrachtungen in Hinblick auf Anforderungen interessant, die sich bei Einbindung von Funktionen der mehrseitigen Sicherheit in das ISDN nach [5] ergeben.

Literatur

[1] Schneier, B.: Applied Cryptography, Second Edition: protocols, algorithms, and source code in C, John Wiley & Sons, Inc., 1996

[2] Burr, W., et. al.: MISPC - Minimum Interoperability Specification for PKI Components, Version 1; NIST; 1997

[3] Burr, W. E.: Proposed Federal PKI Architecture; NIST Preleminary Draft, TWG-98-29; 1998

[4] Achter, S. : PKI - Public Key Infrastruktur: Tagungsband des 5. IT-Sicherheitskongreß des BSI, 1997

[5] Sailer, R.: An Evolutionary Approach to Multilaterally Secure Services in ISDN / IN. Proceedings of the Seventh International Conference on Computer Communications and Networks (IC3N). Lafayette, Lousiana. October 1998. IEEE Computer Society Press

[6] ITU-T Recommendation Q.7xx: Specification Of Signalling System No. 7. Melbourne 1988-1998

[7] Bandow, G.; Gottschalk, H. et al.: Zeichengabesysteme: eine neue Generation für ISDN und intelligente Netze. — Bremen : LTU-Vertriebsgesellschaft. 2. Aufl. — 1995

[8] Gottschalk, H.; Gotthardt, B.: Zeichengabesystem Nr. 7. - Stabilität und Sicherheit, Einsatz eines Monitorsystems, Der Fernmeldeingenieur, 49. Jg, Nr. 11/12, 1995