Zeitschrift: Bulletin des Schweizerischen Elektrotechnischen Vereins, des Verbandes Schweizerischer Elektrizitätsunternehmen = Bulletin de l'Association suisse des électriciens, de l'Association des entreprises électriques suisses

Herausgeber: Schweizerischer Elektrotechnischer Verein ; Verband Schweizerischer Elektrizitätsunternehmen

Band: 77 (1986)

Heft: 1

Artikel: Technische Massnahmen für die sichere Informationsübertragung in zukünftigen Fernmeldenetzen (ISDN)

Autor: Siuda, K.

DOI: https://doi.org/10.5169/seals-904134

Technische Massnahmen für die sichere Informationsübertragung in zukünftigen Fernmeldenetzen (ISDN)

K. Siuda

In zukünftigen öffentlichen Fernmeldenetzen (ISDN) wird die Sicherheit der Informationsübertragung eine wesentliche Rolle spielen. Es werden Sicherheitsdienste nötig sein. Der Beitrag beschreibt die allgemeinen Randbedingungen, die Ziele, die Sicherheitsdienste und eine mögliche Realisierung durch geeignete Sicherheitsmechanismen. Es wird gezeigt, dass die von CCITT definierten ISDN-Strukturen und Signalisiersysteme kompatible Lösungen möglich machen.

La sécurité de la transmission de l'information jouera un rôle essentiel dans les futures réseaux de télécommunication publics (RNIS). Les nouveaux services de télécommunications devraient s'accompagner de nouveaux services de sécurité. L'article décrit les conditions-cadres générales, les objectifs, les services de sécurité et une réalisation praticable au moyen de mécanismes de sécurité appropriés.

Adresse des Autors

K. Siuda, Hasler AG, Belpstrasse 23, 3000 Bern 14.

1. Einleitung

Mit der Einführung von dienstintegrierten digitalen Fernmeldenetzen (ISDN) wird das Angebot an neuen Telekommunikationsdiensten stark zunehmen. Mit der Anwendung dieser Dienste werden Sicherheitszusatzdienste benötigt werden, welche die Integrität der übertragenen Information garantieren. Eine weltweite sichere Übertragung von Informationen über das öffentliche Fernmeldenetz ist nur dann möglich, wenn die notwendigen Normen in den internationalen Gremien (CCITT, ISO) erarbeitet werden. Der Aufsatz beschreibt Lösungsmöglichkeiten für die Sicherheitszusatzdienste, die in etwa dem weltweiten Trend entsprechen und mit den von CCITT normierten ISDN-Strukturen (Tab. I) und Signalisiersystemen voll kompatibel sind.

2. Randbedingungen für die Sicherheitszusatzdienste im öffentlichen Fernmeldenetz

Die Randbedingungen, welche die Sicherheitszusatzdienste im öffentlichen Fernmeldenetz berücksichtigen müssen, lassen sich wie folgt angeben.

- Die Anzahl der an das öffentliche Fernmeldenetz angeschlossenen Teilnehmer, die untereinander verschlüsselte Informationen austauschen können, ist nach oben praktisch nicht beschränkt.
- Jeder Teilnehmer soll mit irgendeinem beliebigen anderen Teilnehmer verschlüsselte Informationen austauschen können.
- Jede Art digitaler Information (Daten, Sprache, Bild) soll verschlüsselt übertragen und vermittelt werden können.
- Die Sicherheitsdienste sind Zusatzdienste im öffentlichen Fernmeldenetz, die nur denjenigen Teilnehmern belastet werden sollen, die diesen beanspruchen.
- Das Hinzufügen der Sicherheitsfunktionen im öffentlichen Fernmeldenetz sollte praktisch keinen Einfluss auf die Netzstruktur und die Netzfunktionen haben, d.h., die Sicherheitsfunktionen sind als Zusatzdienste zu realisieren.
- Die für die Sicherheitsdienste gewählten Prozeduren sollen die normalen Signalisierungsprotokolle nicht beeinflussen, d.h., es wird eine totale Trennung zwischen Netzfunktionen und Sicherheitsfunktionen gefordert.
- Die Schlüsselverwaltung (Tab. II) soll vollständig automatisiert werden, d.h., wenn ein Teilnehmer seine Nachricht verschlüsselt senden will, gibt er dies mit einer Zusatzinformation in der Teilnehmersignalisierung dem Netz bekannt. Dieses sorgt für eine automatische Schlüsselzuteilung. Der Teilnehmer hat mit der Schlüsselverwaltung somit nichts zu tun.
- Die Ver- und Entschlüsselung der Information ist Aufgabe der Endgeräte und nicht des Fernmeldenetzes.
- Die On-line-Übertragungsrate verschlüsselter Informationen sollte beim Schmalband-ISDN bis 64 kbit/s und bei Breitband-ISDN bis 140 Mbit/s betragen.
- Die On-line-Übertragung einer verschlüsselten Nachricht sollte keine unzulässige Übertragungsverzögerung hervorrufen.
- Das Einfügen der Sicherheitsfunktionen im öffentlichen Fernmeldenetz soll dieses nicht wesentlich verteuern.
- Der Teilnehmer sollte von einem Anruf zum anderen wählen können, ob er seine Information offen oder verschlüsselt senden will.
- Eine weltweite Übertragung und Vermittlung von verschlüsselten Informationen über das öffentliche Fernmeldenetz sollte möglich sein.

- Das öffentliche Fernmeldenetz ist das einzige Kommunikationsmittel zwischen den an dieses Netz angeschlossenen Teilnehmern.
- Die Schlüsselverwaltung und das Nachführen des zentralen aktuellen Schlüsselverzeichnisses ist Aufgabe des Netzes.
- Die Sicherheitszusatzdienste im öffentlichen Fernmeldenetz sollen derart konzipiert werden, dass auch zukünftige Verschlüsselungsmethoden ohne Änderung der Grundkonzeption eingeführt werden können.

3. Sicherheitszusatzdienste im öffentlichen Fernmeldenetz

3.1 Ziele der Sicherheitsmassnahmen

Bei der sicheren Informationsübertragung in einem öffentlichen Fernmeldenetz sind die folgenden Ziele zu erreichen:
- Sicherung gegen Abhören von Nachrichten,
- Sicherung gegen Verfälschen von Nachrichten,
- Sicherung gegen nicht autorisierten Zugang zu Informationen,
- fälschungssichere Authentifizierung der Informationsquelle,
- Sicherung gegen Wiedereinschleusen abgefangener Nachrichten,
- fälschungssichere Authentifizierung des Absenders,
- fälschungssichere Erzeugung von Unterschriften,
- Verhinderung einer Beeinträchtigung des Nachrichtenübermittlungsdienstes,
- Verhinderung eines unerwünschten Verbindungsaufbaus.

Diese Ziele können in 2 Hauptgruppen unterteilt werden:
- Verhinderung der Bedrohung durch Dritte (passive bzw. aktive Bedrohung),
- Verhinderung einer Bedrohung durch den Partner (fälschungssichere Beglaubigung von Informationen).

3.2 Sicherheitszusatzdienste

Um die in Abschnitt 3.1 beschriebenen Ziele zu erreichen, müssen im öffentlichen Fernmeldenetz Sicherheitszusatzdienste eingeführt werden, die folgendermassen definiert werden können:

Der *Teilnehmer-Authentifizierungsdienst* stellt sicher, dass die Verbindung zwischen den *gewünschten* Teilnehmern aufgebaut wird.

Der *Zugangskontrolldienst* ermöglicht, dass nur autorisierte Teilnehmer Zugang zu geschützten Informationen erhalten. Dieser Dienst kann auf einzelne Teilnehmer beschränkt oder auf Teilnehmer einer bestimmten Gruppe (geschlossene Benützergruppe) erweitert werden.

Der *Informationsgeheimhaltungsdienst* ermöglicht den Schutz der übertragenen Informationen gegen nicht autorisierte Enthüllung. Der Dienst bezieht sich ebenfalls auf den Schutz der Information, die aus der Beobachtung des Verkehrsflusses abgeleitet werden könnte.

Tabelle I

Abkürzungen

A-Teilnehmer	rufender Teilnehmer
B-Kanal	64-kbit/s-Informationskanal
B-Teilnehmer	gerufener Teilnehmer
CCITT	Comité Consultatif International Télégraphique et Téléfonique
D-Kanal	16-kbit/s-Signalisierkanal
H_A	Hauptschlüssel des A-Teilnehmers
I_A	Initialschlüssel des A-Teilnehmers
ID_A	Identifikator (nur einmal verwendet) des A-Teilnehmers
ID_B	Identifikator (nur einmal verwendet) des B-Teilnehmers
INF	Information
$[INF]^K$	Information, verschlüsselt mit dem Kommunikationsschlüssel
ISDN	Integrated Services Digitial Network (dienstintegriertes digitales Fernmeldenetz)
ISO	International Standard Organisation
ISZ	Internationales Schlüsselverwaltungszentrum
K	Kommunikationsschlüssel
NSZ	nationales Schlüsselverwaltungszentrum
O_A	öffentlicher Schlüssel des A-Teilnehmers
OSI	Open Systems Interconnection (offenes Kommunikationssystem)
P_A	privater Schlüssel des A-Teilnehmers
SC	Study Commitee
SZ	Schlüsselverwaltungszentrum
T	Zeitangabe
TC	Technical Commitee

Der *Informationsintegritätsdienst* soll eine aktive Bedrohung entdecken, d.h. verhindern, dass eine Information verfälscht bzw. eine abgehörte Nachricht wieder eingeschleust wird.

Der *Informationsquellen-Authentifizierungsdienst* soll sicherstellen, dass die Information aus der gewünschten Informationsquelle und nicht von irgend einer anderen Quelle kommt.

Der *Unterschriftsdienst* hat 2 Aufgaben zu erfüllen.

a. Der Empfänger der Information erhält eine Bestätigung des Informationsursprunges, die jeden Versuch des Absenders verunmöglichen soll, das Absenden der Information zu bestreiten.
b. Der Absender der Information erhält eine Bestätigung, dass er die Information an den Empfänger übertragen hat, so dass dieser den Empfang der Information nicht bestreiten kann.

Der Unterschriftsdienst muss deshalb die drei Forderungen, Sicherheit gegen Unterschriftsfälschung, Authentizität und Verhinderung einer späteren Nichtanerkennung einer Unterschrift, erfüllen.

Der *Notariatsdienst* gewährleistet die Integrität betreffend Ursprung oder Empfang der zwischen zwei Teilnehmern übertragenen Information (z. B. Dokument mit Unterschrift) mittels einer autorisierten Vermittlung einer dritten vertrauenswürdigen Instanz (zum Beispiel des Notariats-Servers).

Beispiele von Notariatsdiensten sind: Angabe der Zeit der Registrierung des Dokumentes, Beglaubigung des Inhaltes und des Ursprunges des Dokumentes sowie Angabe der Zeit der Ablieferung der registrierten Information an den Empfänger.

3.3 Sicherheitsmechanismen

Die verschiedenen in Abschnitt 3.2 beschriebenen Sicherheitszusatzdienste erfordern entsprechende Sicherheitsmechanismen, die nachfolgend beschrieben werden.

Die *Verschlüsselungsmechanismen* sind für die Geheimhaltung der zu übertragenden Information und für die Realisierung anderer Sicherheitsmechanismen von ausschlaggebender Bedeutung. Zwei Klassen von Verschlüsselungsmethoden stehen im Vordergrund:

a. symmetrische Verschlüsselungsmethoden, bei denen zur Verschlüsse-

Tabelle II

Definitionen

Aktive Beeinträchtigung (active threat) bewirkt eine nicht autorisierte Veränderung, Unterdrückung, Erweiterung oder Zerstörung übertragener Information.

Asymmetrische Kryptosysteme (asymmetrical cryptosystems, public-key-Verschlüsselungssysteme) sind Systeme mit unterschiedlichem Verschlüsselungs- und Entschlüsselungsschlüssel. (Die Kenntnis des einen Schlüssels ermöglicht noch nicht das Auffinden des anderen Schlüssels.)

Authentifizierung (authentication) dient zur Verifikation der Authentizität und des Ursprunges beim Austausch von Informationen. Authentifizierung beinhaltet immer eine Identifizierung.

Informationsintegrität (information integrity). Die Eigenschaft der Information, nicht durch nichtautorisierte Eingriffe verändert worden zu sein.

Identifizierung (identification) ist ein Prozess, der die Identität einer Person feststellt. Ein typisches Beispiel einer Identifizierung ist die Erkennung des Sprechers bei einem Telefongespräch anhand der persönlichen Charakteristik seiner Sprache.

Kryptoanalyse (cryptoanalysis, Entschlüsselungsangriff) ist die Wissenschaft, verschlüsselte Informationen ohne Kenntnis des Schlüssels zu entschlüsseln.

Kryptographie (cryptography) ist die Wissenschaft der geheimen Informationsübertragung.

Kryptographische Checkfunktion (cryptographic check function) ist diejenige Information, die beim Durchführen eines kryptographischen Prozesses an der betreffenden Informationseinheit erhalten wird. Diese ist somit das Resultat einer mathematischen Funktion des Schlüssels und der Informationseinheit. Beispiel: Nachrichtenintegritäts-Code MIC (message integrity code).

Kryptokomplexität (cryptocomplexity) ist der Schwierigkeitsgrad der Kryptoanalyse. Sie wird mit dem notwendigen Rechenzeit- und Speicherbedarf gemessen.

Kryptologie (cryptology) ist die Wissenschaft der Kryptographie und Kryptoanalyse.

Kryptosicherheit (cryptosecurity): Gesamtheit der Mechanismen und Techniken, die die Information gegen nicht autorisierte Zugriffe schützen.

Kryptosystem (cryptosystem) ist eine Verschlüsselungsmethode. Man unterscheidet symmetrische und asymmetrische Kryptosysteme.

On-line-Übertragung (on-line-transmission): Die Information wird gleichzeitig verschlüsselt und übertragen.

Passive Beeinträchtigung (passive threat) bewirkt einen illegalen Zugriff zu übertragenen oder gespeicherten Informationen, die jedoch nicht verändert werden.

Schlüssel (key): Eine Sequenz von Symbolen, die das Verschlüsseln und Entschlüsseln von Informationen steuert.

Schlüsselverwaltung (key management): Erzeugung, Speicherung, sichere Verteilung und Anwendung von Schlüsseln.

Symmetrische Kryptosysteme (symmetrical cryptosystems, konventionelle oder Ein-Schlüssel-Verschlüsselungsmethoden) sind solche, bei denen der Verschlüsselungs- und Entschlüsselungsschlüssel identisch ist.

Verschlüsselung (encipherment): Veränderung einer Information mittels eines Schlüssels, um diese gegen nicht autorisierte Eingriffe zu schützen.

Verschlüsselungsalgorithmus (encryption algorithm) ist ein Satz von Regeln zum Verschlüsseln von Informationen.

Zusatzdienste (supplementary services) verändern oder ergänzen einen Basistelekommunikationsdienst. Die Zusatzdienste werden immer zusammen mit einem Basistelekommunikationsdienst ausgeführt. Somit sind Zusatzdienste nicht alleinstehend.

lung und Entschlüsselung derselbe Schlüssel verwendet wird,

b. asymmetrische Verschlüsselungsmethoden, bei denen zur Verschlüsselung der öffentliche und zur Entschlüsselung der private Schlüssel verwendet wird.

Die Existenz eines Verschlüsselungsmechanismus impliziert die Verwendung eines Schlüsselverwaltungsmechanismus mit den Aufgaben:

a. Erzeugen von geeigneten Schlüsseln in bestimmten vom geforderten Sicherheitsgrad abhängigen Zeitintervallen,
b. geeignete, geschützte Speicherung der Kopie eines jeden Schlüssels,
c. Verteilung der Schlüssel an die Teilnehmer des öffentlichen Fernmeldenetzes in einer sicheren Art und Weise.

Die asymmetrische und die symmetrische Verschlüsselung bedingen verschiedene Prinzipien der Schlüsselverwaltung. Die sichere Übertragung der Schlüssel im öffentlichen Fernmeldenetz ist von derselben Bedeutung wie die sichere Übertragung der Information. Es gibt somit Schlüssel, die Informationen, und Schlüssel, die Schlüssel verschlüsseln.

Weitere Aspekte, die bei der Schlüsselverwaltung berücksichtigt werden müssen, sind die physische Verteilung der Schlüssel bei der Initialisierung des Sicherheitssystems, das Speichern der Schlüssel und das Aufteilen der Verantwortung derart, dass keine Einzelperson den vollen Schlüssel besitzt.

Die *Unterschriftsmechanismen* werden von einer Gruppe von Instanzen (z. B. Teilnehmern) vereinbart. Dieser Mechanismus führt eine Transformation der Information mit folgenden Eigenschaften durch:

- Die Transformation wird von einer einzigen Instanz ausgeführt (z. B. dem Autor der Unterschrift),
- das Resultat der Transformation kann nicht geändert werden, ohne dass dies erkannt wird,
- das Resultat der Transformation kann von allen Instanzen der Gruppe verifiziert werden.

Ein Unterschriftsmechanismus verwendet z. B. asymmetrische Verschlüsselungsalgorithmen, er benutzt den dem Absender zugeordneten Privatschlüssel für eine kryptographische Checkfunktion. Jeder Besitzer des entsprechenden öffentlichen Schlüssels kann nun verifizieren, dass die kryptographische Checkfunktion aus den Daten nur mittels des privaten Schlüssels erzeugt werden konnte. Dadurch ist bewiesen, dass der Absender der Daten mit dem Besitzer des privaten Schlüssels identisch ist.

Die *Zugangskontrollmechanismen* verwenden die Authentizität der Teilnehmer, um ein Anrecht auf einen Zugang zu bestimmten geschützten Informationen zu überprüfen. Versucht der Teilnehmer Zugang zu nicht autorisierten geschützten Informationen zu erhalten, dann wird dieser Versuch abgewiesen und eine Alarmmeldung initialisiert.

Die Informationsintegritätsmechanismen: Es gibt zwei Aspekte der Informationsintegrität, die Integrität von einzelnen Informationseinheiten oder Informationsfeldern und die Integrität einer Sequenz von Informationseinheiten oder Informationfeldern.

- Der Schutz der Integrität von einzelnen Informationseinheiten erfolgt mit Manipulations-Erkennungscodes (Blockprüfung und Redundanz) und mit kryptographischen Checkfunktionen. Der Manipulations-Erkennungsmechanismus benötigt 2 Prozesse, einen auf der Sendeseite und einen auf der Empfängerseite. Die Sendeseite ergänzt die zu übertragenden Informationen mit einer Grösse, die eine Funktion der Information selbst ist. Diese Grösse kann eine kryptographische Checkfunktion sein. Die Empfangsseite erzeugt eine entsprechende Grösse und vergleicht diese mit der empfangenen Grösse, um festzustellen, ob die Informationseinheit während der Übertragung modifiziert wurde.
- Der Schutz der Integrität einer Sequenz von Informationseinheiten oder Informationfeldern benötigt irgendeine Form der Sequenznumerierung.

Die *Authentifizierungsmechanismen* verwenden verschiedene Techniken:

a. Passwörter, die von der Quelle erzeugt und vom Empfänger überprüft werden,
b. kryptographische Techniken, die mit «hand-shaking»-Protokollen kombiniert werden können, um das Wiedereinschleusen von zuvor empfangenen Nachrichten zu verhindern,
c. Verwendung allgemeiner Charakteristiken der Teilnehmer.

Die *Notariatsmechanismen* gewährleisten die Integrität der zwischen 2 Teilnehmern übertragenen Information betreffend deren Ursprung oder Empfang durch Vermittlung einer anderen Instanz (zum Beispiel des Notariats-Servers). Der Sicherheitszusatzdienst, der solch einen Mechanismus benötigt, muss ein spezielles Protokoll verwenden. Beispiele von Notariatsdiensten sind Schlüsselübersetzungsdienste und Registrierdienste für Anwendungsdaten. Datenregistrierzentren können die Zeit der Registrierung, den Inhalt der Nachricht sowie den Ursprung der registrierten Information beglaubigen.

4. Die Kompatibilität der Sicherheitszusatzdienste mit dem ISDN-Konzept

Das ISDN spielt bei den internationalen Normierungsarbeiten des CCITT eine Schlüsselrolle; es existieren dazu eine Vielzahl von Empfehlungen, die als I-Serie bezeichnet werden. Nach den Rahmenvorgaben des CCITT stellt das ISDN ein Fernmeldenetz dar, das über eine begrenzte Anzahl von standardisierten Schnittstellen digitale Verbindungen von Teilnehmer zu Teilnehmer ermöglicht, und damit einen weiten Bereich von Diensten (Fernsprech- und Nichtfernsprechdiensten) anzubieten vermag. In Figur 1 ist das ISDN-Grundkonzept dargestellt.

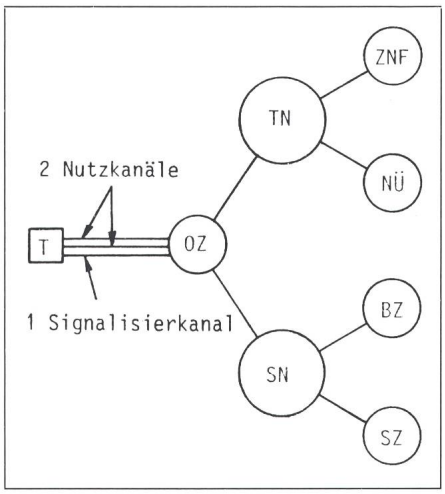


Fig. 1 ISDN-Grundkonzept

BZ Betriebs- und Unterhaltszentrum
NÜ Netzübergänge zu anderen Netzen
OZ Ortszentrale
SN Signalisiernetz
SZ Schlüsselverwaltungszentrum
T Teilnehmer
TN Transitnetz für Nutzinformationen
ZNF Zentralisierte Netzfunktionen

4.1 Telekommunikationsdienste

Es werden grundsätzlich zwei Typen von Telekommunikationsdiensten unterschieden:

- *Transportdienste,* bei denen dem Teilnehmer ein *transparenter* Übertragungskanal zur Verfügung gestellt wird,
- *standardisierte Teledienste,* die in allen OSI-Schichten, d. h. auch in den Anwendungsschichten, eindeutig beschrieben sind und damit auch weitgehend Einfluss auf die Gestaltung der Endgeräte ausüben.

Die Telekommunikationsdienste können durch teilnehmerbezogene Dienstmerkmale (sogenannte Zusatzdienste) erweitert werden. Das hier vorgeschlagene Sicherheitskonzept basiert auf folgendem:

- Eine End-zu-End-Verschlüsselung wird als die optimale Lösung angesehen. Die Verschlüsselung der Information erfolgt in den höheren Schichten, so dass für die Übertragung einer verschlüsselten Information Teledienste zur Anwendung kommen, bei denen die Verschlüsselung der Information im Terminal selber erfolgt.
- Die im Abschnitt 3.2 aufgezählten Sicherheitszusatzdienste sind teilnehmerbezogene Dienstmerkmale. Sie werden gleich behandelt wie die anderen ISDN-Zusatzdienste.

4.2 Teilnehmerschnittstellen

CCITT legt die verschiedenen Kanalarten fest, die an der Teilnehmerschnittstelle auftreten können, sowie die sich aus der Kombination der Kanalarten ergebenden Kanalstrukturen. Die Basiskanalstruktur der Teilnehmerschnittstelle enthält zwei Nutzkanäle (B = 64 kbit/s) und einen Signalisierkanal (D = 16 kbit/s). Die Primärmultiplexstruktur weist 30 B-Kanäle für die Übertragung der Nutzinformation und einen D 64-Kanal für die Signalisierung auf.

4.3 Signalisierung

Die B-Kanäle werden für die Übertragung der verschlüsselten Information verwendet, während der D-Kanal vorwiegend für die Signalisierung zwischen *Teilnehmer und Netz* bestimmt ist. Über diesen Kanal erfolgt die Schlüsselverteilung vom Schlüsselverteilungszentrum zu den Teilnehmern.

Das Verständigungsmittel zwischen den *Zentralen* ist die Signalisierung. Sie ist bei jedem Verbindungsauf- und abbau erforderlich, aber auch bei der Abwicklung von Zusatzdiensten. Im ISDN wird für die Signalisierung zwischen den Zentralen das von CCITT normierte Common-Channel-Signalisiersystem Nr. 7 verwendet, in dem für die Signalisierung eigene, von den Nutzkanälen getrennte Übertragungskanäle verwendet werden. Damit kann man ein autonomes Signalisiernetz mit eigenen Signalisierknoten aufbauen. Die Signalisierrate in diesem Netz beträgt 64 kbit/s. In bestimmten Signalisierknoten können die Schlüsselverwaltungszentren untergebracht werden. Die Schlüsselverteilung von diesen zu den Ortszentralen erfolgt über das Signalisiernetz, von den Ortszentralen zu den Teilnehmern über den D-Kanal.

Die verschlüsselte Information selbst wird im B-Kanal übertragen. Diese Trennung bei der Übertragung von verschlüsselter Information und verschlüsseltem Schlüssel erhöht die Kryptosicherheit wesentlich.

5. Einfügung der Sicherheitszusatzdienste in das OSI-Referenzmodell

Das OSI-Referenzmodell (CCITT-Empfehlung X.200) dient als Referenz für die CCITT zur Erarbeitung von normierten Kommunikationsprotokollen für Telekommunikationsdienste. Die Sicherheitszusatzdienste sollen optimal in das OSI-Referenzmodell eingefügt werden. Die Grundforderung ist, dass die Sicherheitsfunktionen als Zusatzdienste im öffentlichen Fernmeldenetz zu konzipieren sind, d. h. die Sicherheitsfunktionen sind von den Netzfunktionen vollständig zu trennen. Aus diesem Grunde sind die Sicherheitsfunktionen in die höheren Schichten des OSI-Modells einzufügen, entweder in der Darstellungsschicht (presentation layer) oder in der Anwendungsschicht (application layer). Werden die Sicherheitsfunktionen in die Anwendungsschicht eingefügt, dann müssen sich die einzelnen Anwendungsinstanzen mit den Sicherheitsmassnahmen beschäftigen. Dies erschwert die Normierung wesentlich. Aus diesem Grunde eignet sich die Darstellungsschicht am besten für das Einfügen der Sicherheitsfunktionen in das OSI-Referenzmodell.

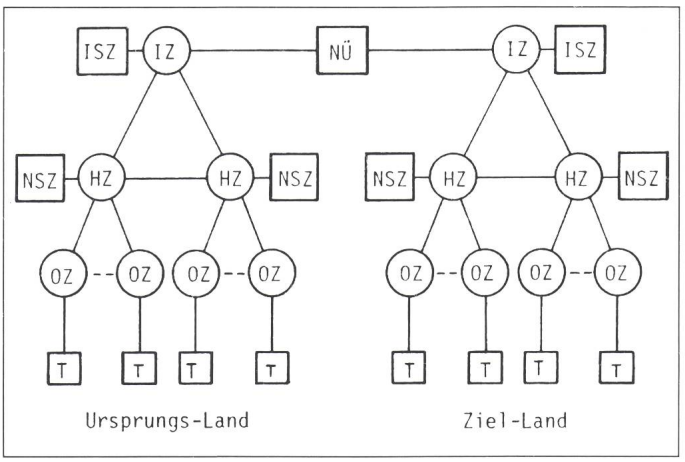
6. Schlüsselverwaltung

Das zentrale Problem jeder gesicherten Informationsübertragung ist die Schlüsselverwaltung, d.h. das Erzeugen der Schlüssel, das Verteilen der Schlüssel zum rufenden und gerufenen Teilnehmer und die Verifikation derselben. Bei grossen öffentlichen Fernmeldenetzen wird die Schlüsselverwaltung zum zentralen Problem der Sicherheitszusatzdienste, da folgende Voraussetzungen erfüllt sein müssen:

- Jeder Teilnehmer soll mit irgendeinem beliebigen anderen Teilnehmer verschlüsselte Informationen austauschen können.
- Der einzelne Teilnehmer soll von der Schlüsselverwaltung vollständig entlastet werden.
- Das öffentliche Fernmeldenetz ist das einzige Kommunikationsmittel zwischen den an dieses Netz angeschlossenen Teilnehmern.
- Das zeitgerechte Nachführen eines grossen Schlüsselverzeichnisses kann nur in bestimmten Netzknoten erfolgen, in denen dieses elektronisch gespeichert ist.

Fig. 2
Hierarchische Struktur der Schlüsselverwaltungszentren

ISZ internationales Schlüsselverwaltungszentrum
IZ internationale Kopfzentrale
HZ Hauptzentrale der Netzgruppe
NSZ nationales Schlüsselverwaltungszentrum
NÜ Netzübergang
OZ Ortszentrale
T Teilnehmer



6.1 Schlüsselverwaltungszentren

Die oben erwähnten Anforderungen sind nur dann erfüllbar, wenn in bestimmten Knoten des öffentlichen Fernmeldenetzes Schlüsselverwaltungszentren vorgesehen werden, welche die Verwaltung der Schlüssel vollständig autonom übernehmen. Für eine weltweite Übertragung von verschlüsselten Informationen sind mehrere Schlüsselverwaltungszentren notwendig. Eine mögliche hierarchische Gliederung derselben ist in der Figur 2 dargestellt.

Die *nationalen Schlüsselverwaltungszentren* (NSZ) übernehmen die Schlüsselverwaltung bei nationalen Verbindungen. Ein NSZ kann zum Beispiel pro Netzgruppe vorgesehen werden. Gehören beide Teilnehmer derselben Netzgruppe an, dann erhalten sie die Schlüssel von demselben NSZ. Sind jedoch die beiden Teilnehmer an verschiedene NSZ angeschlossen, dann erhalten sie die Schlüssel von den ihnen zugeordneten NSZ. In diesem Fall ist ebenfalls ein Informationsaustausch zwischen diesen beiden NSZ erforderlich. Die NSZ sind untereinander mittels des Common-Channel-Signalisiernetzes verbunden.

Die *internationalen* Schlüsselverwaltungszentren (ISZ) übernehmen die Schlüsselverwaltung bei internationalen Verbindungen. Da nicht immer angenommen werden kann, dass im Ursprungs- und im Zielland dasselbe Verschlüsselungsverfahren angewendet wird, muss im ISZ eine Umschlüsselung vorgenommen werden, d. h. es muss ein Übergang von einem Verschlüsselungsverfahren zum anderen realisiert werden. Die ISZ müssen die teilnehmerbezogenen Informationen (z. B. Hauptschlüssel) bei den NSZ abfragen.

6.2 Schlüsselarten und Schlüsselverteilung bei symmetrischen Verschlüsselungsmethoden

Bei symmetrischen Verschlüsselungsmethoden sind 3 Schlüsselarten vorgesehen, der *Initialschlüssel* für die verschlüsselte Übertragung der Hauptschlüssel bei der Initialisierung des Teilnehmerterminals, der *Hauptschlüssel* für die verschlüsselte Übertragung der Kommunikationsschlüssel, der *Kommunikationsschlüssel* für die verschlüsselte Übertragung der Nutzinformation. Dieser wird pro Verbindung erzeugt.

Initialschlüssel: Das zentrale Problem jeder Schlüsselverwaltung ist die Verteilung der Initialschlüssel vom Schlüsselverwaltungszentrum zu den Teilnehmern mit kryptographischen Terminals. Diese Verteilung muss *ausserhalb* des öffentlichen Fernmeldenetzes erfolgen. Folgendes Verteilungsverfahren sollte eine genügende Kryptosicherheit aufweisen. Bevor das kryptographische Terminal beim Teilnehmer installiert wird, wird es im Schlüsselverwaltungszentrum mit dem Initialschlüssel geladen und plombiert. Der Initialschlüssel wird nur für die Initialisierung des Sicherheitssystems verwendet, d. h. mit dem Initialschlüssel wird der Hauptschlüssel verschlüsselt und über das öffentliche Fernmeldenetz zum Teilnehmer übertragen.

Hauptschlüssel: Dieser dient zur verschlüsselten Übertragung der Kommunikationsschlüssel. Jedem Teilnehmer wird ein individueller Hauptschlüssel zugeordnet, der zur Erhöhung der Sicherheit häufig, z. B. einmal pro Stunde, ausgewechselt werden kann.

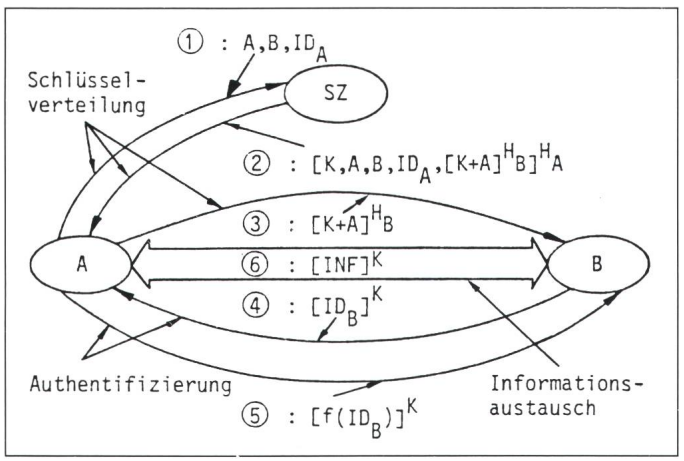


Fig. 3
Meldungsablauf bei symmetrischen Verschlüsselungsmethoden

① Meldung 1
② Meldung 2
③ Meldung 3
④ Meldung 4
⑤ Meldung 5
⑥ Meldung 6

Übrige Bezeichnungen s. Tabelle I

Kommunikationsschlüssel: Der Kommunikationsschlüssel dient zur verschlüsselten Übertragung der Information. Er wird vom Schlüsselverwaltungszentrum für jede Verbindung neu bestimmt und zu den beiden Teilnehmern übertragen; er ist somit nicht teilnehmerindividuell, sondern verbindungsbezogen.

6.3 Schlüsselarten und Schlüsselverteilung bei asymmetrischen Verschlüsselungsmethoden

Bei der asymmetrischen Verschlüsselungsmethode werden dieselben drei Schlüsselarten wie bei der symmetrischen verwendet. Der einzige Unterschied besteht darin, dass zwei verschiedene Kommunikationsschlüssel pro Verbindung benötigt werden. Der rufende Teilnehmer erhält den öffentlichen Schlüssel und der gerufene Teilnehmer den privaten Schlüssel.

6.4 Weitere Anforderungen an die Schlüsselverwaltung

Das Schlüsselverwaltungszentrum muss in der Lage sein, für jetzige und zukünftige Verschlüsselungsmethoden die Schlüssel zu erzeugen, zu verteilen und zu verwalten. Je nach Sicherheitsdienst wird das Schlüsselverwaltungszentrum die eine oder die andere Verschlüsselungsmethode wählen.

Der Hauptschlüssel soll periodisch gewechselt werden, wobei dieser zur Übertragung mit dem vorangehenden Hauptschlüssel verschlüsselt wird. Der einzige Unterschied zwischen der asymmetrischen und der symmetrischen Methode besteht in der unterschiedlichen Erzeugung der Kommunikationsschlüssel. Dank dem raschen Wechsel der Schlüssel hat ein Schlüsselverlust keine grossen Folgen. Bei der hybriden Verschlüsselungsmethode werden pro Verbindung die symmetrische und die asymmetrische Verschlüsselungsmethode gleichzeitig angewendet, zum Beispiel die symmetrische Methode für die Sicherung der zu übertragenden Information und die asymmetrische Methode für die Verifikation der Unterschrift.

7. Meldungsablauf bei symmetrischen Verschlüsselungsmethoden

Diese Operation ist in Figur 3 dargestellt. Der A-Teilnehmer besitzt den Hauptschlüssel H_A, der B-Teilnehmer den Hauptschlüssel H_B. Der jedem Teilnehmer individuell zugeordnete Hauptschlüssel ist im Teilnehmerterminal und im Schlüsselverwaltungszentrum gespeichert. Zum Aufbau einer Verbindung sendet der A-Teilnehmer die 1. Meldung an das SZ mit der A-Teilnehmernummer, B-Teilnehmernummer und dem Identifikator ID_A. Das SZ sendet zum A-Teilnehmer den Kommunikationsschlüssel K, eine Kopie der Anrufanforderung (A, B, ID_A) sowie die Information $[K+A]^{H_B}$, die der A-Teilnehmer später zum B-Teilnehmer sendet, um die Verbindung aufzubauen und seine Identität dem B-Teilnehmer bekanntzugeben. Diese Meldung ist mit dem Hauptschlüssel des A-Teilnehmers (H_A) verschlüsselt. Somit ist der A-Teilnehmer der einzige, der diese Meldung empfangen kann. Der A-Teilnehmer überprüft den Identifikator ID_A, um sich zu überzeugen, dass diese nicht eine eingeschleuste, früher empfangene Anrufanforderung ist. Er überprüft zusätzlich, dass die Anrufanforderung bis zum SZ nicht verändert wurde. Danach sendet der A-Teilnehmer dem B-Teilnehmer die 3. Meldung, die den Kommunikationsschlüssel und die A-Teilnehmernummer enthält. Diese ist mit dem Hauptschlüssel des B-Teilnehmers verschlüsselt. Der B-Teilnehmer kennt nun den A-Teilnehmer und den Kommunikationsschlüssel, weiss aber noch nicht, ob es sich bei der empfangenen Meldung nicht um eine eingeschleuste, von Dritten früher empfangene Meldung handelt. Deshalb sendet der B-Teilnehmer dem A-Teilnehmer in einer 4. Meldung seinen Identifikator ID_B, der mit dem Kommunikationsschlüssel verschlüsselt ist. Der A-Teilnehmer führt mit dem Identifikator ID_B eine Funktion aus und sendet das Resultat in der 5. Meldung zum B-Teilnehmer zurück. Nun weiss der B-Teilnehmer, dass dies tatsächlich der A-Teilnehmer ist und nicht eine Wiederholung einer vorher empfangenen und wieder gesendeten Meldung. Mit der 6. Meldung erfolgt die Informationsübertragung zwischen den beiden Teilnehmern. Die Information ist mit dem Kommunikationsschlüssel verschlüsselt.

8. Meldungsablauf bei asymmetrischen Verschlüsselungsmethoden

Diese Operation ist in Figur 4 dargestellt. Der A-Teilnehmer besitzt den Hauptschlüssel H_A, der B-Teilnehmer den Hauptschlüssel H_B. Der dem betreffenden Teilnehmer individuell zugeordnete Hauptschlüssel ist im Teilnehmerterminal und im Schlüsselverwaltungszentrum gespeichert. Zum Aufbau einer Verbindung sendet der A-Teilnehmer die 1. Meldung an das SZ, welche A-Teilnehmernummer, B-Teilnehmernummer und Zeitangabe T enthält. Das SZ prüft, ob beide Teilnehmer autorisiert sind, verschlüsselte Informationen untereinander auszutauschen. Ist dies der Fall, dann wird vom SZ zum A-Teilnehmer die 2. Meldung übertragen, die folgende Information enthält: die Kopie der 1. Meldung (A- und B-Teilnehmernummer, Zeitangabe T), privater und öffentlicher Schlüssel des A-Teilnehmers, öffentlicher Schlüssel des B-Teilnehmers und eine Information, die der A-Teilnehmer später zum B-Teilnehmer sendet, um die Verbindung aufzubauen und die Identität des A-Teilnehmers zu überprüfen.

Die 2. Meldung ist mit dem Hauptschlüssel des A-Teilnehmers verschlüs-

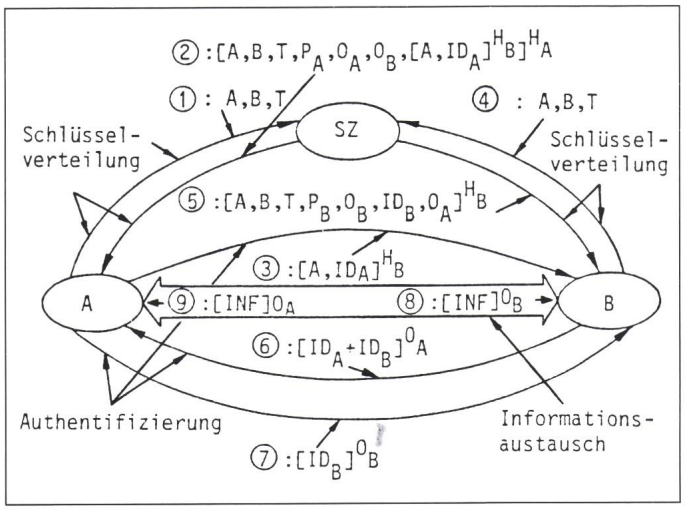


Fig. 4
Meldungsablauf bei asymmetrischen Verschlüsselungsmethoden

① Meldung 1
② Meldung 2
③ Meldung 3
④ Meldung 4
⑤ Meldung 5
⑥ Meldung 6
⑦ Meldung 7
⑧ Meldung 8
⑨ Meldung 9

Übrige Bezeichnungen s. Tabelle I

selt, der diese somit entschlüsseln kann. Die Zeitangabe garantiert, dass die Meldung aktuell, d. h. keine alte, von einem Dritten vorher empfangene und wieder eingefügte Meldung ist. Mit Hilfe der Kopie seiner 1. Meldung kann der A-Teilnehmer verifizieren, dass seine 1. Meldung auf dem Übertragungsweg zum SZ nicht verfälscht wurde.

Um ein Wiedereinschleusen früher empfangener Meldungen durch Dritte zu verhindern und um sich zu identifizieren, sendet der A-Teilnehmer dem B-Teilnehmer eine 3. Meldung mit der A-Teilnehmernummer und einem Identifikator ID_A, die mit dem Hauptschlüssel des B-Teilnehmers verschlüsselt ist. Dieser sendet zum SZ eine 4. Meldung (A, B, T), um in der 5. Meldung nebst der Kopie der 4. Meldung seinen privaten und öffentlichen Schlüssel (P_B, O_B), seinen Identifikator ID_B und den öffentlichen Schlüssel O_A des A-Teilnehmers zu erhalten. In einer 6. Meldung sendet der B-Teilnehmer dem A-Teilnehmer den von diesem erhaltenen Identifikator ID_A und seinen eigenen Identifikator ID_B, beide verschlüsselt mit dem öffentlichen Schlüssel des A-Teilnehmers. Der A-Teilnehmer entschlüsselt die Meldung und ist jetzt sicher, dass er mit dem gewünschten B-Teilnehmer verbunden ist. Der A-Teilnehmer sendet als 7. Meldung dem B-Teilnehmer seinen Identifikator ID_B, so dass dieser ebenfalls sicher ist, mit dem A-Teilnehmer verbunden zu sein. Jetzt sendet der A-Teilnehmer zum B-Teilnehmer Informationen (8. Meldung), die mit dem öffentlichen Schlüssel des B-Teilnehmers verschlüsselt sind. Desgleichen sendet der B-Teilnehmer dem A-Teilnehmer Informationen, die mit dem öffentlichen Schlüssel des A-Teilnehmers verschlüsselt sind (9. Meldung).

Das obige Schlüsselverteilungsverfahren erfordert 7 Meldungen, bevor der verschlüsselte Informationsaustausch zwischen den beiden Teilnehmern beginnen kann. Dank der hohen Signalisierrate in digitalen Netzen ist die Anzahl der Meldungen pro Verbindung tragbar. Dafür ist beim Teilnehmer weder der private noch der öffentliche Schlüssel dauernd gespeichert. Diese beiden Schlüssel werden erst während des Verbindungsaufbaues vom SZ an die betreffenden Teilnehmer verteilt. Dadurch wird erreicht, dass die beiden Schlüssel dem letzten Stand entsprechen.

9. Normierungsbestrebungen für Datensicherheit der Telematikdienste

Die Sicherheitsdienste werden in den zukünftigen Fernmeldenetzen eine grosse Rolle spielen. Damit gesicherte Verbindungen weltweit hergestellt werden können, müssen die Sicherheitsdienste weltweit normiert werden. Sowohl in der ISO (TC97/SC 20 N) als auch im CCITT (Study Group VIII) werden Normen ausgearbeitet, die die Sicherheitsdienste im öffentlichen Fernmeldenetz betreffen. Die beiden internationalen Organisationen wollen miteinander eng zusammenarbeiten und ihre Normierungsarbeiten koordinieren. Die Studienkommission VIII des CCITT hat von der Plenarversammlung in Malaga-Torremolinos, im Herbst 1984, den Auftrag erhalten, die Frage Nr. 28/VIII mit dem Titel «Sicherheitsmassnahmen für Telematikdienste« zu studieren. Dabei sollen insbesondere die folgenden Aspekte untersucht werden:

- die Ziele der Sicherheitsmassnahmen,
- die notwendigen Sicherheitsdienste,
- die Entwicklung von Normen für die Schlüsselverwaltung in öffentlichen Fernmeldenetzen,
- die Frage, welche Verschlüsselungsmethoden zu normieren sind,
- die Entwicklung von Normen für den Unterschriftsdienst,
- die Frage, ob von der CCITT Verschlüsselungsalgorithmen normiert werden sollten und
- welche Massnahmen zu treffen sind, um die Normierung zukunftssicher zu gestalten.

10. Schlussfolgerung

Die Sicherheits-Zusatzdienste können in zukünftigen digitalen Fernmeldenetzen als Zusatz eingefügt werden, ohne dass das Netz allzu stark zusätzlich belastet wird. Eine weltweite Übertragung von verschlüsselten Informationen über das öffentliche Fernmeldenetz ist aber nur dann möglich, wenn von den internationalen Normierungsgremien (CCITT, ISO) die notwendigen Normen aufgestellt werden. In CCITT hat man mit den Normierungsarbeiten erst begonnen. Mit dem Abschluss dieser Arbeiten durch Herausgabe der entsprechenden CCITT-Empfehlungen ist erst in der kommenden Studienperiode 1989–1992 zu rechnen.