Security Services in an Open Service Environment

Reiner Sailer
Institute of Communication Networks and Computer Engineering
University of Stuttgart, Pfaffenwaldring 47, D-70569 Stuttgart, Germany
sailer@ind.uni-stuttgart.de

Abstract

Emerging telecommunication services use, store, or transmit sensitive personal data to form individual network services. We suggest an add-on approach to realize secure telecommunication services which saves the huge investments into existing network infrastructure of the ISDN. This is done by adding trusted runtime environments that contain security functions to existing service infrastructure. This approach aims at separating sensitive service functions from highly complex functions of public telecommunication networks. We propose an enhancement of existing network service interfaces by standardized security service interfaces to enable the provision of open security services. Separated security control functions of independent service providers, however, might not be trusted by network operators. Therefore, this contribution particularly considers gateway functions implementing access control and ancillary conditions concerning network integrity.

1 Introduction

The term t*elecommunication service* (also called *service)* denotes a set of related functions of telecommunication systems that support a certain communication between remote terminal equipment or between terminal equipment and central servers located within networks. Telecommunication services are classified in terms of bearer services and teleservices. This classification bases on the location of those functions that are involved in a service.

Bearer services only include functions of the network. Consequently, bearer services support switched connections between terminals or between terminals and centralized network infrastructure (e. g. servers). *Teleservices* base on bearer services and additionally include functions within terminal equipment or shared network servers.

We discuss telecommunication services as applications, because they evolve to be used independently of data channels in the future. Furthermore, teleservices process more and more personal data and are no longer restricted to a single telecommunication network.

Generally, requirements on telecommunication services concerning security are described in terms of *confidentiality*, *integrity* and *availability*. These terms are broadly known and understood. Security requirements must be related to objects (data or functions that are to be protected) to form *security goals*.

Def.: Services that offer a verifiable "degree of security" by use of security functions are called *security services*. Thereby, a security function directly contributes to the implementation of security goals.

Consequently, security services satisfy certain security requirements in a comprehensible way. They comprise both security enhanced conventional services and new services.

Def.: A *service is called secure* concerning one party, if and only if all security goals of this party with respect to this service are fulfilled in a comprehensible way.

Fig. 1 illustrates the classification of telecommunication services depending on the location of the respective service functions. The proposed "add-on" approach shows: conventional teleservices plus additional security functions enable (i) security enhanced telecommunication services (e. g. anonymous calls, encrypted data transfer) and (ii) new autonomous security services (e. g. public key certificate retrieval services). In doing so, added security functions are executed on security enhancements of terminal equipment (e. g. security modules, [18]) or on trusted servers reachable over telecommunication networks (Fig. 1).

Signalling systems are used by distributed service functions to exchange synchronization data in order to interactively realize complete telecommunication services. In ISDN, we distinguish signalling protocols applied at user network interfaces (UNI, e. g. DSS1, [7]) and at network node interfaces (NNI, e. g. SS7, [12]). There are additional protocols that enhance the signalling interface between network nodes and centralized service nodes of the Intelligent

This work has been funded by the Gottlieb Daimler- and Karl Benz-Foundation (Ladenburg, Germany) as part of its Kolleg *Security in Communication Technology*.

R. Sailer: Security Services in an Open Service Environment. Proceedings of the Fourteenth Annual Computer Security Applications Conference, Scottsdale (Arizona), December 1998, pp. 223-234.

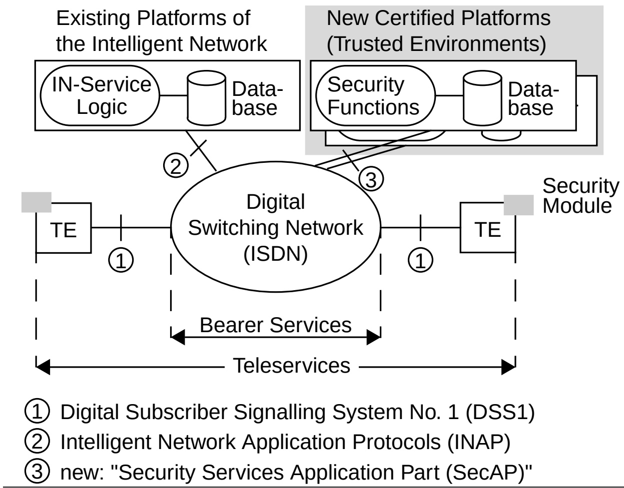

Figure 1: Services and interfaces of the ISDN / IN

Network (INAP, [13]). The ISDN user part (ISUP, [12]) bases on the SS7 and includes functions to setup and clear connections in ISDN (not explicitly shown in Fig. 1).

We focus on teleservices that span functions within terminal equipment, network nodes and certified service platforms. Today's value-added services are realized by use of the so called Intelligent Network (IN). The IN has mainly been introduced to accelerate service creation and service provision. In its current peculiarity, the respective IN application protocols are not flexible enough to serve as a basis for open and network independent security services.

Therefore, enhancements of the user network signalling system (DSS1, see Fig. 1) are proposed that support the synchronization of security services. These protocols are summarized as Security Supplementary Services (SSS).

Furthermore, there is need for additional signalling protocols between core network functions and specialized security service functions (interface 3 in Fig. 1). Following the naming convention of existing users of the SS7, these new application level protocols altogether are referred to as the Security Services Application Part (SecAP).

This contribution introduces open service interfaces that enable trusted service functions to be included into existing telecommunication services. In addition, standardized protocols are added (SecAP basing on SS7, SSS basing on DSS1) that support the synchronization of distributed security functions. The proposed interfaces promote an evolution of existing telecommunications infrastructure to satisfy currently ignored and evolving security goals.

Arising obstacles – resulting of requirements like robustness and autonomy of existing telecommunication services of the ISDN – introduced by enhancements of open interfaces form an interesting research area and are particularly addressed within this contribution.

Challenges concerning the addition of security functions to existing service infrastructure are discussed in section 2. In section 3, a domain concept is introduced that leads to efficient and effective location strategies for security functions in heterogeneous service environments. The application of the domain concept to single communication systems and communication networks is described in section 4. Proposals for more efficient gateway functions (firewall functions, etc.) that secure signalling interfaces against outsider attacks complete section 4. Finally, section 5 illustrates the use of open security signalling interfaces by an exemplary anonymity service.

2 Challenges and related work

There are several possibilities to allocate security functions. Security functions serving users should be located as close to the user as possible, e. g. within security modules, user terminals, or additional black boxes controlled by users. The allocation of security functions serving users within telecommunication networks is justified if and only if they contribute to or profit from the following attributes:

- availability of security functions or security control data (e. g. certificates)
- centralized operation, administration, and maintenance
- economy of scales (e. g. shared use of very expensive highly secure runtime environments)

As the public ISDN was not planned to fulfil developing security requirements, we must search for possibilities to integrate new security infrastructure into existing networks. This infrastructure must satisfy existing and emerging security requirements. One way to reach this goal is to provide interfaces over which remote security service functions may interact with core network functions.

Based on these interfaces, it is possible to cope with changing requirements of users, service providers and network operators. Security goals stated for telecommunication services may differ, depending on the parties involved. The next definition extends the definition of secure services related to a single party to a definition taking into account security needs of all parties, affected by a service:

Def.: A telecommunication service is called *multilaterally secure*, if and only if security goals of all parties, that are affected by this service, are taken into account in a balanced way.

Affected parties include subscribers, users, network operators, service providers, and manufacturers. Concerning multilateral security, it is not necessary that all security goals are guaranteed because they may be inconsistent with one another.

The definition of multilaterally secure services is not as strong as the definition of secure services concerning one party. But it is the strongest definition addressing the security needs of all parties that are affected by a service.

R. Sailer: Security Services in an Open Service Environment. Proceedings of the Fourteenth Annual Computer Security Applications Conference, Scottsdale (Arizona), December 1998, pp. 223-234.

2.1 Requirements of security services

We discuss security services that base on the signalling systems SS7 and DSS1. These services should be independent of a specific network infrastructure and therefore must base on open and standardized interfaces. Security functions must be located wherever sensitive data appears. Therefore, they must be distributed over different networks to realize global security services. For this reason, synchronization of respective service functions – i. e. the exchange of control data – extends across network boundaries.

Fig. 2 shows *distributed security functions* that cooperatively form security services. Addressing and access to services supported by existing signalling networks is done over service access points (SAP^{Sec}). Supplementary functions included in Fig. 2 provide means for the exchange of security control data between communication systems that host distributed security functions (addressing, routing, link functions, security message and parameter types).

Services of the signalling network (SS7) and the user network signalling (DSS1) must be enhanced to offer this kind of supplementary services. An adaptation sublayer enhances DSS1 to provide SAP^{Sec} (see section 4.1); the enhancement of SS7 is included within SecAP. The SAP^{Sec} must be an open and standardized interface in order to enable flexible use of such interfaces by different implementations of security functions or plug-in security modules.

Protocols describe the messages, their interpretation by receiving entities (here: security functions), and the synchronization of associated distributed security functions. These protocols between security functions will differ at the UNI and NNI. At the UNI these protocols are summarized as Security Supplementary Services Protocols (SSS).

These protocols are mostly used to support end-to-end security services or access to shared security servers reachable over the network. They base on SAP^{Sec} service interfaces. At the NNI these protocols are called Security Services Application Part (SecAP). The SecAP not only enables access to central security services, but also provides means to link security functions and existing services (e. g. services basing on the ISUP). Interworking between SSS and SecAP protocols can be done within local exchanges. This enables network operators, to control the services accessed by use of their network infrastructure (see also section 4) over the UNI. Requirements on environments for distributed security functions form a first challenge:

Challenge 1 – Environmental Requirements: Security functions need *secure runtime environments*. They must share *means for synchronization*, i. e. means for the exchange of security control information. Security functions need open service access points to interact with core network services (SAP^{Sec} in Fig. 2). Standardized protocols (SSS, SecAP) are needed for the interaction of different implementations of security functions forming security services. There must be mechanisms *to link security functions with existing services* in order to achieve secure telecommunication services.

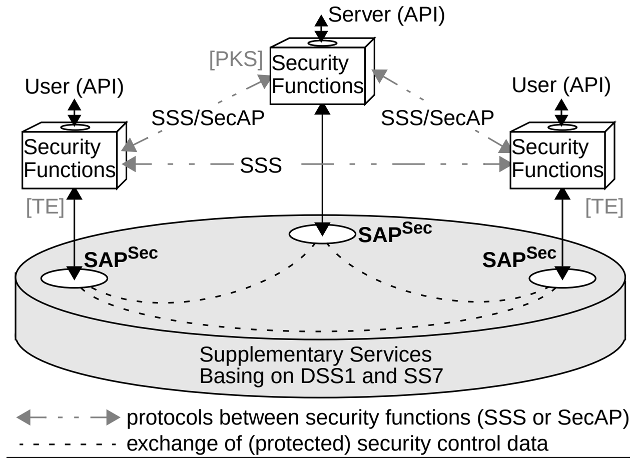

Figure 2: Protocols and SAPs for security services

Authentication services and public key certificate retrieval services are examples of autonomous security services. Authentication processes within the users' terminal equipment (TE, see Fig. 2) exchange authentication tokens within signalling messages (e. g. by use of SAP^{Sec} basing on services of the underlying SS7 or DSS1).

In this example, the terminals retrieve the required public key certificates from a public key certificate server (PKS) reachable over the network. An interaction of the related security functions with existing network services is not necessary. This kind of security services is called autonomous. Autonomous services only depend on the underlying signalling network in order to exchange security control information (authentication tokens, public key certificates, valid certificate revocation lists).

Within user terminals, of course, also autonomous security services may be linked with conventional telecommunication services to achieve secure telecommunication services. This means for example, that a connection setup may be admitted if and only if an accompanying authentication has been completed successfully. From a network service view, end-to-end authentication and connection setup are independent from each other. However, they can be linked within user terminals on demand. Which conventional services are combined with which security services is a matter of the security policy applied.

Assume a security service that satisfies security goals concerning one party. Consequently, respective service functions that form this security service must run on a runtime environment that is trusted by this party. Otherwise the security functions may be compromised and no matter what security goals are demanded by a party, the resulting

R. Sailer: Security Services in an Open Service Environment. Proceedings of the Fourteenth Annual Computer Security Applications Conference, Scottsdale (Arizona), December 1998, pp. 223-234.

service will not satisfy them in a comprehensible way. Concerning different parties that are affected by telecommunication services, areas of tension include:

- access control to network, service, or terminal resources
- access control to sensitive user data processed by core network services or value-added services
- call accounting and billing

Some areas of tension are negligible, if network operator and service provider are identical. More conflicting security goals appear, if several network operators or service providers are involved in a single service (see example in section 5).

Challenge 2 – Inclusion of Trusted Third Parties: There is need for trusted runtime environments and trusted service functions within service processing. In order to enable multilaterally secure services, there is need for the interaction of core network service functions with security service functions hosted in remote runtime environments. Accordingly, we need *interfaces to include functions of TTPs* into existing telecommunication services.

It is quite unlikely that there will be a single TTP that is trusted by all participating parties. Therefore, a logical "Common Trusted Third Party" will comprise of several TTPs that interact to solve conflicting security goals.

2.2 Requirements concerning network integrity

Especially, requirements of users and network operators concerning the robustness and autonomy as prerequisites of *network integrity* must be explicitly addressed by solutions that shall enhance network and service security. We quote from some other literature to backup the outstanding relevance of these aspects of network security:

Recent public network outages have shown that robustness and autonomy are really threatened even by existing signalling and service interfaces and by network functions that are mainly controlled by experienced operating personal. J. C. McDonald concluded in [4] – with respect to SS7 outages in 1988 – that the most serious mistake was to rely on an assumption that major failures could not happen. Another mistake was to ignore the serious consequences of large computer network failures in terms of economic disruption and the loss of industry credibility.

An assumption made by K. Ward [5], that "the integrity problems are fundamentally concerned with network control; that is, the transmission and processing of control information" has proven to be valid.

Concerning the telecommunication infrastructure, new threats arise by processing control data that originates from external security service infrastructure. Falsified control data may cause huge damage within telecommunication networks. The most severe consequences include:

- network nodes crash because of software failures
- network functions are manipulated (e. g. accounting)
- unauthorized and unrecognized access to network functions (e. g. administration accounts, service profiles)

Because software and hardware are very complex and are subject to permanent changes, it cannot be excluded that forged or incorrectly composed signalling messages also harm network infrastructure that only routes and forwards these messages. Even signalling network functions of the Message Transfer Part of the signalling system (layers 1 to 3) are subject to attacks concerning the availability and integrity of network nodes. As a consequence, also the availability and integrity of services depending on such network nodes are threatened. In addition, the network load introduced by the exchange of security control data is subject to accounting, at least if the related security service is not correlated with the network provider offering the exchange capabilities.

Consequently, there is need for access control concerning (security) control data before it is processed within the network. Concerning security services, the related access control functions have to be included in the path between security functions that are not (or not equally) trusted.

Open security signalling interfaces (protocols for the exchange of security control data between distributed security functions) support *security gateway functions* by offering standardized identifiers that enable protection by screening and filtering. Thus, open interfaces enable network operators to switch dedicated security functions on and off and to react quickly to misuse of service features or to software errors that might be exploited by attackers.

Challenge 3 – Network Integrity: Interconnecting separated service infrastructure with core network infrastructure implies *the need for strong security gateways to screen and filter on control data* that originates from separated security infrastructure or other networks (not equally trusted infrastructure) before this data is processed within or transported by the respective telecommunication network.

Finally, there must be fall-back mechanisms to ensure network operation even without the availability of additional security service functions to maintain the autonomy and robustness of today's ISDN services.

2.3 Related work

Concerning environmental requirements (challenge 1), there is a lot of ongoing work. Security modules as a runtime environment for security functions are discussed in [18]. End-to-end security functions are discussed in [1], [8], [9], and many other contributions. Solutions to anonymity services are discussed in [6] and [19], but their implementation within existing service environments is not straightforward. Compatibility of security functions is promoted by the ATM Forum [20]. It agrees on broadly applicable encoding and algorithms that are used in ATM user network signalling and network node signalling protocols.

Regarding the inclusion of TTPs into network services (challenge 2), there is a long way to go. Secure runtime environments for TTPs are already in use, but neither are they connected to networks for on-line access via signalling nor are there any standardized protocols to include such TTPs into network service provision.

Referring to network integrity connected with control data originating from external network infrastructure (challenge 3), a lot of firewall-like solutions have been proposed for public networks (e. g. Q.705, [12]). Gateway functions are established at network boundaries that block all except basic and verified signalling messages. By this, unauthorized manipulative or accidental control of internal network functions caused by processing foreign control data is restricted. Mostly, these gateway functions have a very bad granularity and a lot of services do not work over network boundaries. There is some work on firewalls for IP networks (dynamic filtering, etc.) that might improve existing solutions if applied to SS7 and DSS1. Today, mainly screening and filtering is applied at these gateways. No cryptographic functions are currently applied. Therefore, the authenticity of control messages arriving over transit networks can't be verified. The worth of screening and filtering such messages is therefore restricted.

3 Domain concept – separation & mediation

The domain concept introduced here bases on an early article by Rushby and Randell [14]. Their idea is developed to a method whose application promotes assessable and scalable security in heterogeneous service environments.

A domain is characterized by *uniform* threats, assumptions about attackers, security goals, and ancillary conditions concerning security. The domain boundaries are supervised by gateways. Consequently, a domain is a part of a service environment that can be secured independently from other parts of the service environment. In order to enable interaction of associated parts of the service environment over domain boundaries, data can enter or leave a domain by means of so called mediation functions. Mediation functions implement access control functionality.

Fig. 3 shows a telecommunication network that is divided into five different domains. For example, functions within domains A, B and TTP may interact to realize security services (exchange of control data: type 1, 2 in Fig. 3). The figure illustrates also remote access to TTPs (type 3 in Fig. 3), whereby the supporting operator of the signalling network may account the exchange of control data by flat

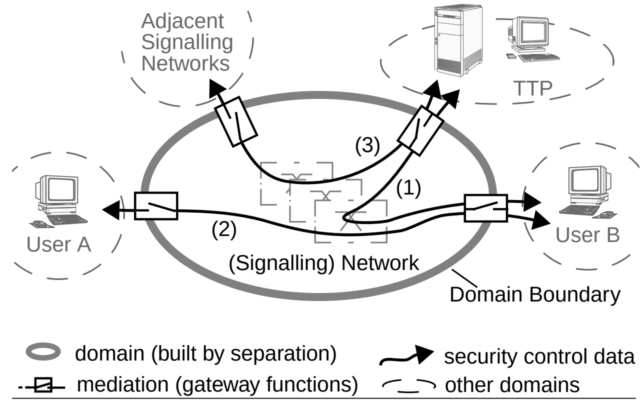

Figure 3: Security domains regarding signalling

rates or based on the amount of control data exchanged. Concerning network integrity, we focus on scalable protection measures that can be applied by network operators to control remotely produced control data that is transmitted over their signalling network or processed within their service nodes. Such control data includes security control data exchanged between domains A, B and TTP to realize security services.

Separation aspects of signalling network domains: Separation mechanisms (mostly access control mechanisms) ensure that control data enters a domain only through a few well defined gateways. By this, separation ensures that all data is inspected by mediation functions before it leaves or enters the network domain.

This contribution focuses on a network operator's signalling network and on respective control data that is processed within this signalling network. Control data created within the network operator's domain is trusted by default, i. e. the network domain consists of equally trusted infrastructure and administration staff.

Mediation aspects of signalling network domains: Control data enters and leaves a network operator's domain to synchronize distributed functions forming teleservices and network services spanning multiple networks. Mediators inspect control data before it leaves or enters the network operator's domain (Fig. 3). The kind of security function applied on control data that is leaving a domain depends on the security goals related with the respective control data and the domains that will be crossed. Efficient access control functions are applied on control data that enters the network operator's domain. For example, well known firewall functions can act as mediators for incoming control data at the domain boundary.

If there are areas within a domain which are less secure – and therefore need stronger security mechanism – than other parts of the respective domain, this domain should be refined into subdomains. Consequently, additional gateways must be installed and administrated to secure these emerging subdomain boundaries. Resulting subdomains can be secured in an efficient and effective way. Finally, the impact of security breaches within one domain on other domains is limited. The number of separate domains and belonging gateways must be weighted up against advantages resulting of more efficient security mechanism and achieved autonomy and robustness.

Outsourcing sensitive service functions like access control and call accounting to TTPs would lastly reduce security requirements on core network switches. This would contribute to more independence between network operators and switch manufacturers.

Today, call accounting and access control are partly included in local exchanges. The security of these sensitive functions depends on the security of the underlying hardware and software. Both hardware and software modules are very complex and hardly verifiable by network operators.

4 Applying the domain concept to security services in ISDN/IN

This section proposes enhancements of service environments by additional functions and physical network infrastructure to show possible approaches regarding the challenges in section 2. The domain concept introduced in section 3 is applied to achieve efficient and effective security gateway functions.

Respective gateways must secure the signalling network of a network operator against outsiders that might try to misuse open security service interfaces of this signalling network. In addition, they restrict the impact of failures of adjacent signalling networks. The main ideas are summarized briefly:

- Sensitive functions located within the public network are separated from less sensitive network functions by introducing new network infrastructure (hardware and software) that is operated by Trusted Third Parties and adapted to evolving needs of network users. Security functions within user terminals may run on plug-in security modules.
- The proposed security services are included into the public ISDN over security service interfaces. Service functions supporting these interfaces are implemented in application level signalling protocols (application parts of the SS7), protocols of the user network interface (basing on DSS1), service control functions, or management functions of the public ISDN.

The goal is an overlay security service network that has designated links to existing service infrastructure in order to profit from the huge investments into existing network infrastructure. These links are used to access security services, to exchange security control data, and to combine separated security functions with conventional services.

4.1 Communication system level approach

This section depicts the application of the domain concept to single communication systems. It is suited for security enhancements of user terminals, security servers reachable over the network, and for single network nodes that need an independent security environment (e. g. management centers). As an example, Fig. 4 shows different ways for enhancing service interfaces of communication systems by an interface to access or include additional security service functions.

We consider communication systems basing on DSS1 for this approach (e. g. conventional user terminals, small security servers using DSS1 signalling, user side of local exchanges). Communication systems basing on SS7 are handled in the next section.

Fig. 4a shows an approach, where new security functions are integrated into existing service control functions. This approach is not scalable, needs changes of existing service functions, and has low capabilities to build domains. This approach is not considered because it does not contribute to open security service interfaces and because it is not flexible.

Fig. 4b shows the approach followed within this contribution. Clearly separated security functions may run in specialized security modules. Open interfaces (SAP^{Sec}) promote compatibility and availability of implementations satisfying changing needs of users in different environments (ISDN, GSM, B-ISDN, etc.). This results in independent security functions that may be employed as plug-in security enhancements for various telecommunication services. The separated address space (by use of separated service access points) enables independent filtering and screening. The Security Adaptation Layer (SAL) includes

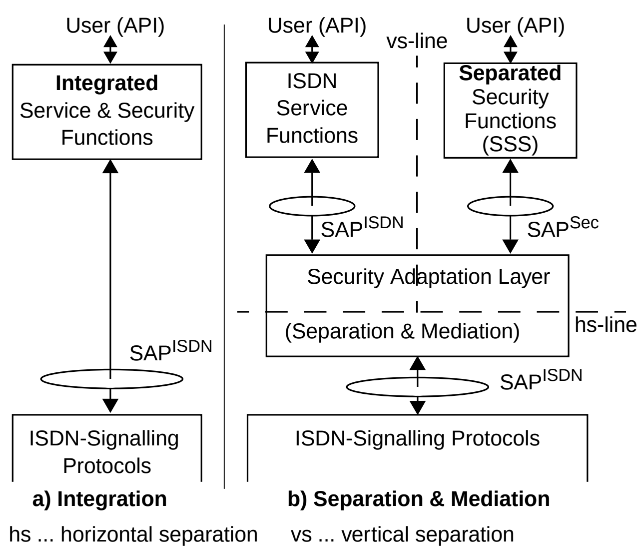

Figure 4: Security enhancements of ISDN services

gateway functions to separate the internal services from the signalling network (horizontal separation). At the same time, the SAL separates security functions from conventional ISDN service functions by use of isolated service access points (vertical separation in Fig. 4b).

Consequently, there are three domains, that are controlled by a single adaptation layer: the external network domain (no security assessment possible for users), the highly secure domain hosting security functions (building signatures, authentication functions), and the moderately secure domain of conventional services (connection control, applications). Mediation is done within the SAL by invoking security functions (e. g. authentication) that enhance conventional services. The SAL is called an adaptation layer because it translates requests at the SAP^{Sec} to requests of the SAP^{ISDN} and vice versa. The SAL is implemented as a transparent sublayer in between layer 2 and layer 3 or above layer 3 of the D-Channel protocols.

The separated security functions (SSS) may be implemented in specialized security modules [18] that are plugged into a terminal on demand. The SSS can be implemented similar to the ISDN supplementary services. Security service functions thereby are triggered either on demand by the user (via an application programming interface, API) or automatically by the SAL (via SAP^{Sec}).

Encapsulating separation, mediation, and adaptation into a single transparent sublayer saves the investments in existing network and terminal infrastructure and represents a flexible approach to security services on demand.

4.2 Communication network level approach

The proposed approach to enhance communication network services by security functions particularly takes into account the economy of scales reached by shared security functions. Therefore, the building blocks of the domain concept (*separation*, *mediation*) and the building blocks for security enhancements (*adaptation* to existing infrastructure, *linking* security functions and conventional services, *secure runtime environments*) are not implemented within a single adaptation layer in every network node as for single communication systems.

The network domain consists of many network nodes that are equally trusted. To build a domain boundary, every network node that is connected to external infrastructure (gateway exchanges, local exchanges) must implement *separation* functions. *Adaptation* functions are responsible for the inclusion of separated security functions. They are supported and implemented where needed: (i) at local exchanges, the SSS security protocols of the UNI must be translated to SecAP security protocols of the NNI and vice versa (similar to ISDN supplementary services); (ii) at shared security servers and security enhanced network nodes, adaptation functions are needed to include security functions into service provision.

The SAP^{Sec} for the network internal access of security functions and the adaptation of separated security functions is implemented by a new application part of the SS7, namely the Security Services Application Part (SecAP). This application part is addressed by use of a new subsystem number that is to be configured into the MTP-routing (as an equivalent to a new identifier for the SAP^{Sec} at the UNI). The synchronization of security functions and conventional service functions is done at the application service level (e. g. by service control functions).

If the set of security functions that can be accessed over network boundaries shall be restricted, there is need for further interworking at network boundaries. The network internal SecAP may be restricted for internetworking (similar to restrictions according to the international ISUP [10]). This results in restricted services spanning multiple networks. In this case, the SecAP and the restricted SecAP must be implemented in every gateway exchange over which security services are enabled.

M*ediation* functions are responsible for inspecting service control data leaving or entering the network domain (access control functions). These are to be integrated between level 2 and 3 of the MTP or within the SecAP in order to inspect incoming and outgoing signalling messages. There are two basic approaches to implement mediation functions for network domains:

- Mediation functions are integrated in every gateway exchange and local exchange (integrated with separation functions). This approach is currently implemented for ISDN internetworking. One reason for this is, that at the gateway exchange there is some context information available that is used for access control (distinguishing network operators by information about the incoming link or link set, screening calling party numbers by use of their association with subscriber lines, etc.).
- The other extreme denotes separation functions at network boundaries that redirect all messages (that shall leave or enter the network domain) via central network nodes implementing mediation functions.
- Making profit from both extremes, mediation functions are located both at the gateways and within shared network nodes. Most of the signalling traffic should be handled directly at the gateways and only traffic that needs particular inspection (security control data concerning accounting, electronic coins for on-line payment, etc.) is relayed over specialized security nodes.

The lower part of Fig. 5 shows an exemplary configuration of terminals and TTPs interconnected by a communication network. The upper part of Fig. 5 depicts the signalling protocols that are included in the terminals, TTPs, and ISDN-exchanges to synchronize security functions. To

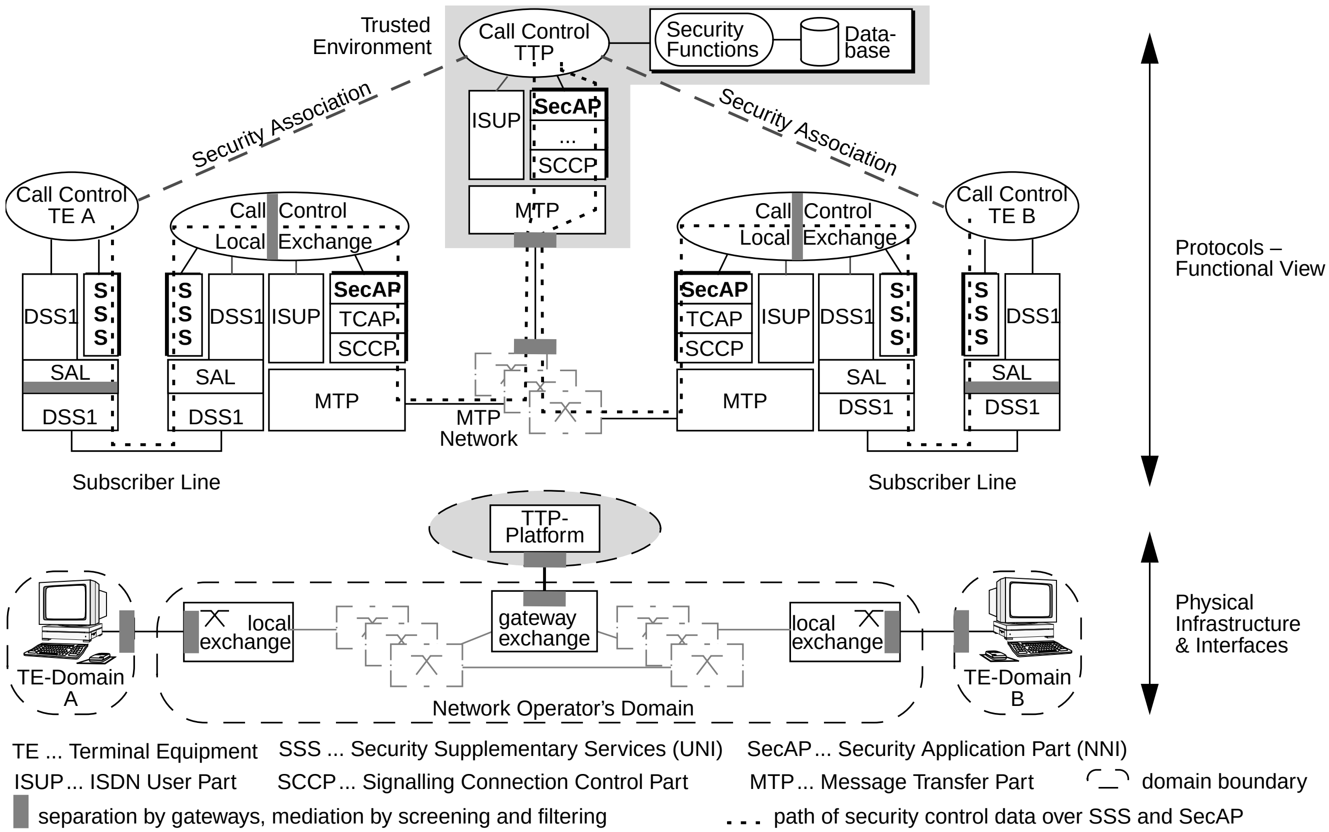

Figure 5: Network level approach to "add-on" security – allocation strategy for security and gateway functions

reduce complexity, only a single network operator and a single service provider are participating in the service.

In the exemplary configuration of Fig. 5, the network operator may not be affected by the service (except from transporting control data between the security functions). Classical examples of such services are end-to-end authentication services that are supported by TTPs (e.g. public key servers, see [17]). Security services that protect user data that affects network functions need synchronization with service functions of the core network. Section 5 presents an anonymity service by inserting multiple TTPs in the connection establishment.

Fig. 5 depicts the enhancements at the UNI and at the NNI to support the synchronization of security service functions. The *SSS* enhancement of the UNI serves as a basis for negotiating and realizing security services over the user network interface. The SSS base on the SAP^{Sec} that is provided by the security adaptation layer (SAL, see also Fig. 4b).

The NNI is enhanced by the SecAP. It bases on the Message Transfer Part (MTP) and the Signalling Connection Control Part (SCCP) of the SS7. The MTP offers services to transport signalling messages to a given destination signalling node. The SCCP uses services of the MTP and offers connectionless and connection-oriented network services. The SCCP is used by the TCAP to exchange security control data between distributed security service functions. The SecAP uses the Transaction Capabilities Application Part (TCAP) of the SS7 to realize powerful security protocols. Synchronization of security services with core network services over SecAP and ISUP is shown in more detail in section 5 and in [17].

4.3 Access control at network boundaries

Providing open interfaces, we should not forget to study the consequences. Kuhn et al state in [2] that "when switching from proprietary to standardized open interfaces, intruders can more easily attack a system whose behaviour is standardized and well known, or which shares common flaws with other systems built on the same standards".

This effect must be compensated by specialized strong security gateway functions supervising these interfaces. On the other hand, open interfaces enable quick response to known threats and promote high quality products by competition among manufacturers and service providers.

In the following, we will focus on access control mechanisms to protect the robustness and autonomy of the core network against outsider attacks over the SecAP and SSS interfaces. Thereby, we focus on the SecAP, over which service providers or adjacent network operators insert control data that is processed or merely transported by control functions of the core network. However, the SSS interface also bears some potential misuse (that can be treated similar to the approach proposed for the SecAP below):

- By supporting the exchange of security control data between terminal equipment (end-to-end), covered channels may be established by users. These channels can be used for fraudulent exchange of data.
- The synchronization of security services and core network services may lead to dependencies between both. Therefore, fraudulent use of SSS may trigger security service functions of TTPs or functions within the network that decrease the robustness of network services.

The SecAP bears more serious potential for misuse of network resources, because the SecAP directly binds separated security service functions into network services. Concerning network resources, the level of control over the SecAP is much higher than control achievable by security functions triggered over the SSS interface. Therefore, there is need for strong *mediation* functions.

Control data is exchanged within the signalling system by means of so called message signalling units (MSU). MSUs include standardized field identifiers depicting the included type of control data. These identifiers depend on the protocols used by the service functions to exchange control data (ISUP, TCAP, SCCP, SecAP, SSS in Fig. 5).

At first, access control is implemented by the common channel signalling system (SS7) itself: the outband signalling system prevents control or management processes within the network from being directly manipulated by user data (natural separation). In addition, parameters of signalling messages are inspected by interworking functions within local exchanges before they are translated from DSS1 to ISUP.

Accordingly, access control concerns signalling messages and parameters that originate from adjacent signalling networks. Two protection mechanisms are employed at the respective external signalling interfaces:

- *Filtering* decides, whether a signalling message may pass into (or leave) the network based on access control lists (ACLs). These ACLs specify for each identifier and respective contents and for each direction (in / out), whether a message may pass or whether the respective message or parameter should be discarded. Today, filtering is mainly done on address information.
- *Screening* is stronger than filtering. The address information contents of a signalling message that serves as a basis for filtering is verified, using context information. Such context information may be the signalling link, on which the message has been received and related addresses that are accessible over this link. At the network node interface, claimed address information includes the network indicator and the originating signalling point code. If the contents of a message field have proven to be invalid, the screening function either discards the message, inserts screening information and default contents, or corrects the contents if possible.

No attackers are assumed inside the network domain. For that reason, mediation (by screening and filtering on control data) at the network boundary is effective against attacks. This facilitates the management of access control lists, screening functions, and filtering functions applied in the respective gateways and minimizes the number of gateways to be installed. Basing on open signalling interfaces, these gateway functions protect core network infrastructure against misuse due to forged or incorrectly composed signalling messages inserted at network boundaries.

Message Signalling Units include several identifiers that may serve as a basis for screening or filtering [15],[16]:

- network indicators (bind the validity of a message to a network domain, e. g. national network or international network)
- originating/destination point codes (network addresses)
- subsystem numbers and service indicators (denoting the protocols used to exchange control data within a signalling message)

The quality of access control depends on the authenticity of the identifiers that are screened and filtered. Fig. 6 illustrates the screening of signalling messages and the filtering on various parts of addresses used in the common channel signalling system in ISDN.

Introducing powerful service interfaces like SecAP, over which sensitive network functions may be controlled, demands for stronger access control functions at network boundaries. Today, control data that applies to sensitive network functions (billing, management etc.) is not sent over network boundaries. Respective parameters or messages are dependent of the respective network provider. These so called national parameters or national messages are usually discarded when crossing gateways of the signalling network. The adjective "national" is to be superseded by "operator dependent" considering a rising number of emerging network operators. Therefore, keeping to this strong strategy would disable or limit a significant part of value-added services also within a single country.

More powerful screening functions are enabled by introducing message fields that identify services or service providers that are responsible for their contents. Based on such message fields, screening and filtering functions can switch services on and off depending on the respective provider or security service. This is done by discarding or forwarding respective parameters or messages. Consequently, messages exchanged by the SecAP shall additionally include (standardized) identifiers denoting security service providers and classes of security service functions (SecSI, Fig. 6).

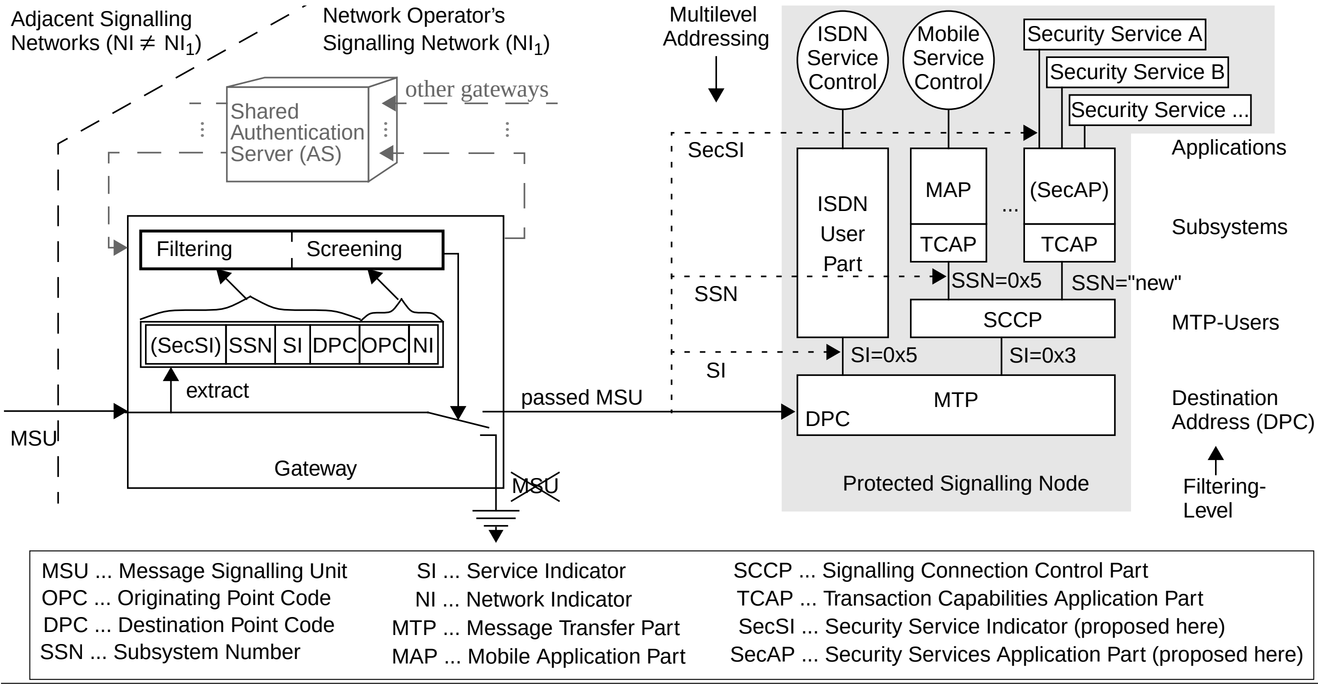

Figure 6: Access control at network boundaries by screening and filtering on address information

However, to achieve effective access control, there is need for *more effective authentication* of the contents of signalling messages. New parameters are to be introduced into signalling messages. These parameters may denote digital signatures or message authentication codes of service providers and serve as a basis for decisions whether a message is discarded or passed through the screening function. Such cryptographic authentication data can be used in cases where given context information is not sufficient to verify screening data (e. g. address information).

Taking into account a composition of the extreme approaches mentioned in section 4.2, more time consuming and costly authentication, screening, and filtering can be done in a shared authentication server that is unique to a signalling network whereas less complicated checks (screening, filtering) are done within the gateways. As outlined in Fig. 6, signalling messages that need authentication are transferred to the authentication server (AS). The AS discards signalling messages or parameters that fail to pass the integrity and authentication checks. Authenticated messages are sent back to the gateway. The gateway recognizes the authenticated messages by the incoming link. If the whole signalling message is transferred to the AS (not shown in Fig. 6), there is no need for keeping state information within the gateways. The ATM-Forum's approach to signatures computed over selected fields of signalling messages [20] and new approaches to signing variable parameters (e. g. addresses as a result of global title translations) should be taken into consideration.

Altogether, an enhancement of "context information" by cryptographic information improves screening by offering authentic information for access control. Network operators are enabled to switch dedicated services on and off by screening on the respective identifiers. Cryptographic context information (e. g. message authentication codes, signatures) promote the independence of logical information for screening from physical context information. This is particularly important for roaming services increasing strongly along with Open Network Provisioning. With roaming services, only few physical context information can be utilized because related control data is received over intermediate signalling systems. The respective international standards dealing with network interconnection in ISDN and in general ([10], [11]) can be enhanced by procedures to handle such cryptographic context information.

5 Exemplary service – anonymous calls

A short example illustrates the use of external services to realize anonymity services. This example also includes the control of data channels (ISUP) and the synchronization of additional security functions and core network functions. Fig. 7 depicts the signalling and switching events needed to hide the routing of a call. Usually MIX-functions are used to hide the association of communicating parties in a call [6]. For this purpose, MIXes 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

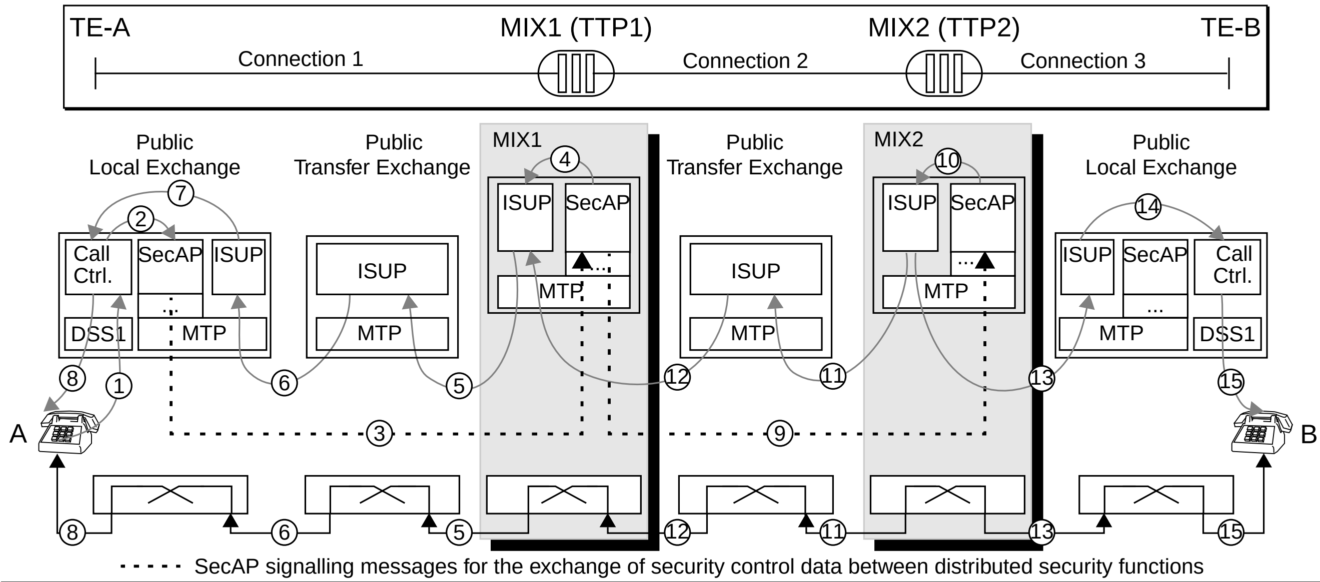

Figure 7: Exemplary use of signalling protocols as a basis for anonymity services

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 services. He wants to be sure that the network operator is not capable 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 to break the anonymity. 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 setup or shutdown through the MIXes because there are many connections being put up and shut down 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. 7 shows the flow of signalling messages for the establishment of an anonymous 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. Usually, anonymity demands for stronger mechanisms, i. e. more MIXes due to stronger requirements and weaker assumptions. We focus mainly on signalling requirements of security services; not on the implementation of the security services itself. This exemplary realization ensures that the connected parties are not deducible by using signalling or state information of the public switches. They are not intended to be absolutely secure against timing attacks.

At first, user A will book an anonymous call at the local exchange (1 in Fig. 7) by using SSS and SecAP (SSS is not shown in Fig. 7). 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. This callback solution is flexible concerning the billing of the call and tolerant against timing requirements. Translating request 3 to a connection request for the ISUP within MIX_1 may be done by using a common control that has access to both ISUP and SecAP (4). This part of the connection is established backwards using conventional ISUP-signalling (5,6,7). The lower part of Fig. 7 illustrates the sequence in which the switched data channel is established between adjacent ISDN exchanges. The identifiers are related to the respective call setup signalling using the ISDN User Part.

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 (10) and establishes an ISDN connection with MIX_1 (11,12). 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 10 in Fig. 7) to user B (13,14). This incoming anonymous call may be indicated at the user's terminal equipment like a call originating from MIX_2 (15). 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.

R. Sailer: Security Services in an Open Service Environment. Proceedings of the Fourteenth Annual Computer Security Applications Conference, Scottsdale (Arizona), December 1998, pp. 223-234.

The three segments of the connection (upper part of Fig. 7) 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 by 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. Of course the communicating parties might be deduced by eavesdropping the data exchanged over the established ISDN connection. But this kind of attack must be handled by security mechanisms within the users' terminal equipment and the MIXes. They have to recode user data to hinder the association of incoming user data with outgoing user data.

The described solution bases on open interfaces within the SS7. 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 (see also section 4).

6 Conclusion and outlook

In fact, the proposed approach applies the framework of Open Network Provisioning (ONP) to security service providers and to providers of sensitive network functions (accounting, etc.). This leads to new requirements on service interfaces over which these – from a network operator's view – outsourced service features may be integrated into network services [3]. Consequently, such interfaces must (i) be internationally standardized, (ii) provide compatibility mechanisms, and (iii) provide or support powerful means to protect interconnected network infrastructure. This ensures the presumed overall service behaviour and limits the risk of network disruption, degradation of the quality of services, and the risk of outages resulting from misuse or incorrect operation of network functions.

Introducing cryptographically protected context information enables the verification of parameters that are used as a basis for access control. It preserves the autonomy of network operators and the robustness of services and represents a prerequisite for efficient fall-back mechanisms.

There is need for efficient implementations of screening and filtering in order to prevent security functions from getting the bottleneck of interworking. The proposed interfaces are valuable in an environment of competing network operators, service providers, and manufacturers and promote *tailor-made* (fitting individual needs), *efficient* (scalable, easy to integrate, compatible), *multilaterally secure* (balancing security goals), and *trustworthy* services.

7 References

[1] W. Burr: Security in ISDN. NIST Special Publication No. 500-189, September 1991.

[2] R. Kuhn, P. Edfors, V. Howard, C. Caputo, T. S. Phillips, A. Booz, H. Booz: Improving Public Switched Network Security in an Open Environment. IEEE Computer, August, 1993.

[3] R. Kickartz, H. Gottschalk: Concepts of Telekom for Open Network Provision (ONP) - Considerations on Network Integrity and Network Operators Autonomy. XV ISS, April 1995, Vol. 2.

[4] J. C. McDonald: Public Network Integrity - Avoiding a Crisis in Trust. IEEE JSAC, Vol. 12, No. 1, January, 1994.

[5] K. Ward: The Impact of Network Interconnection on Network Integrity. British Telec. Engineering, Vol. 13, January, 1995.

[6] A. Pfitzmann, B. Pfitzmann, M. Waidner: ISDN-MIXes: Untraceable Communication with Very Small Bandwidth Overhead. Proceedings KiVS, Mannheim, Februar 1991.

[7] ITU-T: Digital Subscriber Signalling System No. 1, Network Layer. ITU-T Recommendations Q.930-Q.940, Geneva, 1993.

[8] E. D. Myers: STU-III – Multilevel Secure Computer Interface. Proceedings of the 10th Annual Computer Security Applications Conference, Orlando, Florida, December, 1994.

[9] R. Sailer: Integrating Authentication into Existing Protocols. 5th Open Workshop on High Speed Networks, Paris, 1996.

[10] CCITT Recommendation Q.767: Application Of The ISDN User Part Of CCITT Signalling System No. 7 For International ISDN Interconnections. Geneva 1991.

[11] CCITT Recommendations Q.601-Q.699: Interworking Of Signalling Systems. Melbourne, November 1988.

[12] CCITT Recommendations Q.700-Q.766: Specifications Of Signalling System No. 7. Melbourne, November 1988.

[13] ITU-T Q.1211: Introduction To Intelligent Network Capability Set 1. International Telecommunication Union, March 1993.

[14] J. Rushby, B. Randell: A Distributed Secure System. IEEE Computer, July, 1983.

[15] H. Gottschalk, B. Gotthart: Zeichengabesystem Nr. 7 – Stabilität und Sicherheit, Einsatz eines Monitoringsystems. Der Fernmelde-Ingenieur, 49. Jahrgang, Heft 11/12 1995.

[16] B. Kowalski: Security Management System SMS. Der Fernmelde-Ingenieur, 49. Jahrgang, Heft 4/5 1995.

[17] R. Sailer: An Evolutionary Approach to Multilaterally Secure Services in ISDN / IN. Proc. of the 7th International Conference on Computer Communications and Networks. Lafayette, LA, October 1998.

[18] A. Pfitzmann, B. Pfitzmann, M. Schunter, M. Waidner: Trusting Mobile User Devices and Security Modules. IEEE Computer, February 1997.

[19] A. Jerichow, J. Müller, A. Pfitzmann, B. Pfitzmann, M. Waidner: Real-Time Mixes: A Bandwidth-Efficient Anonymity Protocol. IEEE JSAC, Vol. 16, No. 4, May 1998.

[20] ATM Security Specification – Version 1.0 (Draft). ATM Forum BTD-SECURITY-01.04, September 1997.