

An Evolutionary Approach to Multilaterally Secure Services in ISDN / IN¹

Reiner Sailer

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

Abstract

Data protection and data security become more significant since telecommunication services and innovative applications based on these services handle an increasing amount of sensitive data. Modern services, e.g. call forwarding, tele-conferencing, and voice mail services use or store personal data to implement individual services. Sensitive data include personal identities or calling numbers, location information of the communicating parties, service indicators, number translation tables, reachability information, and time and duration of communication events. Generally usable open security services interfaces are proposed, that promote security services implemented in user terminals or Trusted Third Parties in order to satisfy currently ignored and evolving security requirements in a more flexible and scalable way. This approach will both save the huge investments in today's telecommunication infrastructure and promote open security services that are independent of the underlying network infrastructure.

1 Introduction

Existing telecommunication infrastructure will be used as a basis for future telecommunication services and networks because the investments into these resources are enormous. At the same time the importance of data security and data protection is growing. Security requirements were not foreseen when today's telecommunication systems were introduced. Thus, security requirements have been taken into account insufficiently – moreover, security requirements may change quickly depending on individual experience, risk assessment, related charge, and public opinion.

This contribution focuses on control data that cannot be secured end-to-end because it is processed by telecommunication services of the ISDN or Intelligent Network. It

depicts requirements for signalling interfaces over which new security functions may securely interact with existing telecommunication services of the ISDN. Thereby, existing telecommunication functions do not need to follow the same security design guidelines as the separated security functions.

1.1 Security Requirements

Requirements for telecommunication services concerning security may be described in terms of *confidentiality*, *integrity* and *availability*. These terms are broadly known and understood. Respective security requirements must be related to data or functions to form *security goals*.

Def.: A service is called *secure*, if and only if all security goals related to this service are fulfilled.

The security goals stated for a telecommunication service may differ, depending on the interest group affected by this service: subscribers, users, network operators, service providers and manufacturers.

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

It is not a preliminary for multilateral security that all security requirements are fulfilled because there may be conflicting security requirements. However, these conflicts must be solved in a way that is satisfactory for all affected parties.

The need for balancing conflicting security requirements will add further complexity to security management. Additionally, conflicting requirements demand for the negotiation of security services. Trusted Third Parties (TTPs) are included into service control to mediate between different interests. These TTPs may enhance present telecommunication services by introducing and offering additional functionality that promotes multilaterally secure services.

¹ This work has been funded by the Gottlieb Daimler- und Karl Benz-Foundation (Ladenburg, Germany) as part of its Kolleg "Security in Communication Technology".

Today's telecommunication networks satisfy mainly security requirements of network operators and service providers. The users' needs for keeping their identity or a communication event secret are not suitably addressed within public networks. The same holds for user needs regarding call accounting and access control.

New applications will push the need for new security requirements that cannot be satisfied by existing telecommunication services. Therefore, new security functions must be included into existing services to fulfil new and currently ignored security requirements of users. We propose a solution that includes security functions as a service option.

It is taken into account, that solutions that shall enhance network and service security must explicitly address requirements of network operators concerning the robustness and autonomy as prerequisites of network integrity. We quote from some other sources 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 [8] – with respect to Signalling System Number 7 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. K. Ward stated in [9], that the integrity problems are fundamentally concerned with network control; that is, the transmission and processing of control information. This has also proven to be valid.

Therefore, gateway functions have been established at network boundaries to verify control data that enters a network before it is processed by service functions within the network.

Hence, combining security infrastructure (that is not operated by the network operator) with core network infrastructure implies the need for strong security gateways to screen and filter control data that originates from additional security infrastructure, before it is transmitted or processed within the core network. These functions enable network operators to switch the support of dedicated security service functions on and off, i. e. to react quickly to misuse or software failures.

1.2 Goals

The set of required security functions varies over time because it depends on the abilities of assumed attackers, the technical environment, and the security goals. Consequently, the necessary security functions are dependent on

the user and the respective applications and must be supported by communication networks in a flexible and scalable way. Resulting security services shall be:

- *tailor-made* – fitting the individual needs of network users in a given situation
- *efficient* – scalable, easy to integrate, compatible (based on standardized and open interfaces)
- *multilaterally secure* – balancing security requirements of different interest groups
- *trusted* – using trusted implementations, administration, management, charging etc.

This contribution depicts the enhancement of existing services in the public ISDN by supplementary security services. Users are empowered to control their security on their own by including the respective security functions into user controlled devices or into additional network infrastructure that is trusted by the user. We use authentication as an example, because authentication not only enhances user security but also empowers network operators and service providers as an effective means against misuse of services [24].

1.3 Evolutionary Approach

The proposed approach aims at enhancing both services on the logical layer and physical infrastructure to host the respective security service functions in a trusted environment. It takes into account the requirements discussed above. At the same time, it mediates between the needs of users, network operators and service providers. The main ideas are shortly summarized and will be made clear by the remaining part of this contribution.

- Security functions concerning users are located *within the users' terminal equipment* and separated from less sensitive terminal functions. The respective functions (e. g. authentication, encryption) may be located within a separate security module [12]. This module is controlled by the user and can also be used to personalize public terminals.
- Security functions located within the network are separated from less sensitive network functions by introducing *separated network infrastructure*. This infrastructure is operated by trusted organizations (Trusted Third Parties) and may be adapted to evolving needs of network users.
- Security functions, hosted on the proposed *separated security infrastructure* are included in services of the public ISDN or IN by enhancements of existing service interfaces. Separated security infrastructure interacts with existing ISDN infrastructure over these interfaces. The proposed security architecture is easily adapted to GSM and B-ISDN because the respective interfaces base on the predominant Signalling System No. 7.

Software and hardware components of the separated security infrastructure must be independent of existing network infrastructure (except availability). This security infrastructure serves many users and therefore will reach high economy of scales. The *separated security infrastructure may be introduced as an overlay network* in the same way as Intelligent Network services have firstly been introduced e.g. in German field trials. The degree of security may be determined by the concerned network users.

In fact, the proposed approach applies the framework of Open Network Provisioning (ONP) to security service providers. As stated in [6], ONP leads to the following requirements on signalling interfaces over which – from a network operator’s view – external service features may be integrated into network services: respective interfaces must be internationally standardized, provide powerful compatibility mechanisms, and provide or support means to protect interconnected service and switching platforms.

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.

2 Security Services Interfaces for ISDN / IN

Security will gain increasing attention as it has been shown that lack of security may lead to rejection of telecommunication services. Therefore, durable resources will profit from interfaces that support advanced services particularly concerning arising and changing security requirements.

The proposed control plane architecture for security services bases on the protocols of the Digital Subscriber Signalling System No. 1 (DSS1 [14]) and the Common Channel Signalling System No. 7 (SS7 [15]).

The security services interface at the user network interface (UNI) – called *Security Supplementary Services* (SSS) – serves as a basis for negotiating and realizing security services between users, network operators and service providers (e. g. access control, retrieval of public keys).

The security services interface located at the network node interface (NNI) within the Signalling System No. 7 is called *Security Network Services* (SNS). The proposed SNS interface enables the inclusion of centralized security services (running on trusted servers) in core network services. It enables new security services to base on and benefit from existing core services of the underlying signalling network. The proposed extension of the NNI is applicable to all network services that base on the SS7, including GSM and B-ISDN.

Authentication serves as a motivation to introduce the proposed security services interfaces. Authentication can

serve the users’ needs for identifying their communication peers, network operators or service providers. Additionally, authentication serves the needs of network operators and service providers to control the access of users to their communication and service infrastructure.

Authentication protocols for spontaneous communication with changing peers usually base on public key cryptography. Assume a network operator NO wants to verify the identity of user A as a basis for access control. The idea is that user A proves his identity by proving that he knows a secret key related with his identity. A proves this by signing a random number received from the authenticating party NO with his secret key. A proves this by signing a random number received from the authenticating party NO with his secret key. The signature is verified by NO using A’s public key A_p that is related with user A. Of course, this public key must be authentic and must be managed by an organization that is trusted by A and NO.

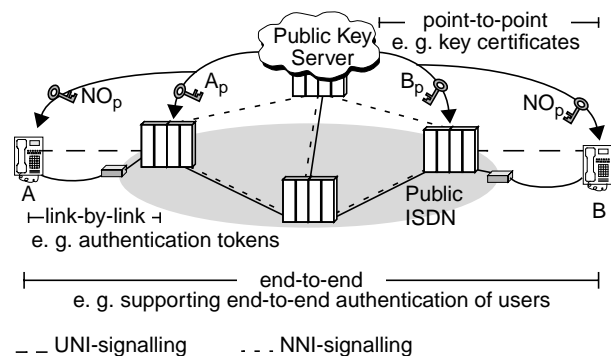


Figure 1: Authentication – requirements on signalling

Within a mutual authentication procedure, signed authentication tokens need to be exchanged between user terminal A and local exchange NO (using the SSS interface). Furthermore, the public keys of the authenticating parties must be retrieved before received authentication tokens can be verified (see Fig. 1). The retrieval of public keys includes transactions within the SS7 to access public key servers (over the SNS interface). Further, it includes transactions within the user network signalling to pass the respective public key certificates to the users’ terminal equipment (over the SSS interface).

Section 2.1 will depict, how security control information may be exchanged between the users’ terminal equipment and the local exchange. The proposed architecture illustrates, how various security services may be controlled similar to ISDN supplementary services. Section 2.2 describes the exchange of security control information (e. g. certified public keys) over the network node signalling system (SS7). A signalling diagram for an authentication supplementary service during connection setup is described in detail in section 2.3 using the introduced architecture.

2.1 Security Services Interface at the UNI

On the one hand, it would be natural to integrate security functions into the call control processes. On the other hand, we want to integrate security enhancements in a flexible way without changing existing network infrastructure too much. Furthermore, we need clear and flexible interfaces between existing service control functions and additional security functions to achieve assessable security.

Therefore, we introduce security functions as supplementary services that can be combined with conventional ISDN services on demand. *Security Supplementary Services* (SSS) include authentication (Auth in Fig. 2), encryption, and access to anonymity services (MIXreq in Fig. 2). Our approach makes use of two components to implement security services at the UNI in a flexible way:

- The **security adaptation layer (SAL)** is inserted as a sublayer in between the protocols of the control and user plane of terminals and their peers (local exchanges, peer terminals). The SAL is transparent to existing protocols but it examines all data that is exchanged between the terminal and the network.
- A new control process, the **Security Supplementary Services (SSS) protocol control**, controls the permeability of the SAL concerning both signalling messages and user data directed to the network and originating from the network. This control process coordinates the combination of various security supplementary services like authentication and encryption.

The SAL serves two main purposes: Firstly, the SAL enables the *exchange of security control data* over the UNI. The UNI signalling in ISDN (Q.931 [14]) already offers an interface to exchange control data for ISDN supplementary services. The SAL enhances this UNI interface by an SSS interface to fit the needs of flexible and generally usable security functions.

Secondly, the SAL *links the SSS to conventional ISDN services*. It ensures for each incoming or outgoing connection or supplementary service request that the security preliminaries (e. g. successful authentication) are fulfilled.

The *Security Supplementary Services protocol control* coordinates the use of security supplementary services. Further, it is responsible for solving problems resulting from security service interaction or from conflicting security goals of the communicating parties (e. g. authentication and anonymity). The SSS may be activated on demand by the user (over the call control) or may be triggered by the SAL due to user defined security rules at communication events like connection setup.

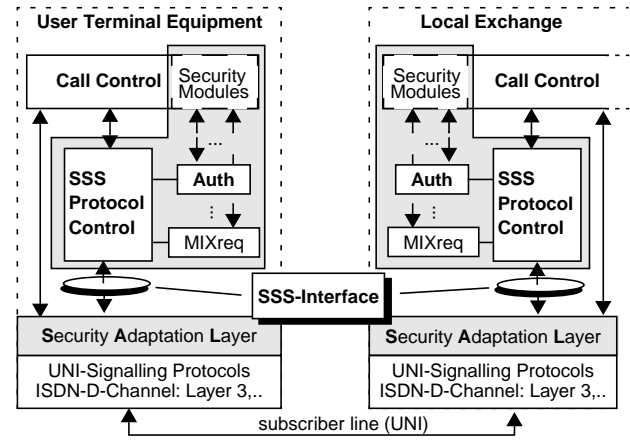


Figure 2: UNI plus Security Supplementary Services

Fig. 2 illustrates the use of the proposed Security Supplementary Services and the SAL. New control and service functions are emphasized. To summarize, the *Security Supplementary Services* support:

- *end-to-end security services* by providing means for the exchange and processing of control data regarding security functions within user terminals.
- *point-to-point security services* by providing means for the exchange and processing of control data (e. g. public keys) concerning cooperating security functions within user terminals and TTPs inside the network. This includes addressing capabilities for the respective services.
- *link-by-link security services* by negotiation of services that protect the users' access to network services, e. g. strong access control services based on explicit user authentication.

2.2 Security Services Interface at the NNI

Carefully engineered security services, running on a trustworthy environment, certified by independent organizations, will be very expensive. Hence, these services must benefit from the economy of scales. This can be achieved by making these services responsive to requests from the whole network and (over the SSS-interface) even to requests originating from user terminal equipment. In addition, developing security services will benefit a lot from using existing services of the SS7 to exchange security control data.

Because trust is a judgement that is highly dependent on the respective interest group (network operators, users, etc.), we propose open security services interfaces. These interfaces enable independent organizations to offer security services. The resulting competition favours high quality security services and results in replaceable security services in case of misuse or raising security weaknesses.

The proposed *Security Network Services* (SNS) interface supports:

- *end-to-end security services* by providing means for the exchange and processing of security control data related to security functions within user terminals (in conjunction with the SSS at the user network interface).
- *point-to-point security services* to access central security servers within the network. Therefore, the SNS interface shall provide Uniform Resource Locators (URL) for addressing central security servers (TTPs). These URLs are translated into signalling network addresses (MTP addresses). Further, the SNS provide means to exchange security control data between user terminals and central security network servers (in conjunction with the SSS at the respective UNI). Finally, security services spanning multiple service providers are enabled by standardized interfaces.
- *network integrity* by providing strict identifiers for service providers and services; this enables network operators to switch services on and off by filtering on the respective identifiers at network boundaries.

This contribution introduces three components to implement an SNS interface that fulfils the above requirements within the existing protocol architecture of the ISDN. Fig. 3 shows these components and their location within the protocol architecture of the ISDN.

- The **Security Application Part** (SecAP) implements the respective functions concerning the SNS with a maximum of profit of the existing signalling network.
- The definition of a **security services access point** assigns unique identifiers to services and providers.
- The **Security Interworking** within local exchanges implements the translation of security service requests received over the SSS interface (at the UNI) to requests of the SecAP (at the network node interface) and vice versa.

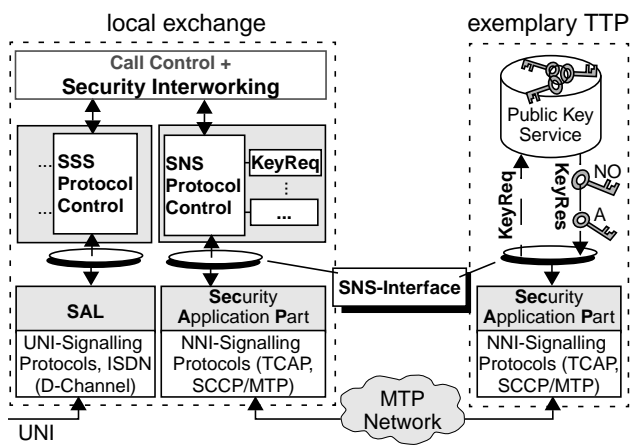


Figure 3: NNI plus Security Network Services

The SecAP bases on the TCAP and SCCP of the SS7 and provides the Security Network Services interface to its users, i. e. to security functions or to the security interworking. The SecAP profits from underlying TCAP and SCCP services [15] that offer transaction processing and global title addressing. Global title addressing using URLs seems appropriate to facilitate the co-operation of independent service providers to offer trustworthy security services by hiding low level and maybe changing network addresses (e. g. MIX chains to realize anonymity services [25]). Moreover, using URL-addresses will facilitate the inclusion of IP-based security servers that will derive along with the growing together of the public ISDN and IP-based networks. In this case, the well known domain name service may be used instead of SCCP global title address resolution.

The Security Interworking is located within local exchanges to mediate the users' access to central security servers or end-to-end security data exchange services. It may also mediate security services that cross network boundaries to realize application level gateway functions.

Taking into account the existing protocol architecture of the SS7 and the more or less decentralized control structures of ISDN exchanges, we depict two design options for the implementation of central security services offered by TTPs. The choice of the respective design option has a significant influence on the flexibility in service design and on the degree of achievable security.

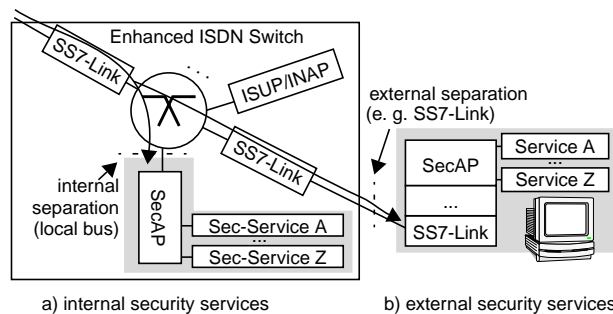


Figure 4: Security services using SecAP – design options

Fig. 4a illustrates the use of the SecAP similar to existing (Mobile-, IN-) application parts and protocols based on SS7. This solution is suited for large service providers or network operators operating their own switches. It enhances existing communication services by enabling the node internal routing to address the security application part by a unique (new) subsystem number. This is the straightforward approach for enhancing services based on individual switching and signalling. The security functions and the SecAP in Fig. 4a are implemented on a plug-in board in the same way as line trunk groups implement ISDN user parts or IN application protocols. These boards should be certified and tamper proof.

Fig. 4b illustrates a design, that allows small companies to offer security services over a SS7 interface. These independent service providers do not need to operate and maintain a whole ISDN switch. Main-frame computers are a suitable platform for Trusted Third Parties offering services realized solely over signalling (e.g. public key retrieval services, see Fig. 1). Data channels cannot directly be secured following this design option.

Relying on SS7 offers great flexibility to the service providers because existing ISDN and IN services can be addressed directly by security functions. This means enhanced risks for network operators because their switches are partly controlled by remote platforms that are not directly supervised by them. Therefore, powerful gateway filtering functions shall be installed at the external separation line in Fig. 4b. These filtering functions may look similar to those that are installed within gateways to the international signalling network.

The proposed solution demands an extension of the set of known subsystems within SS7. By assigning the SecAP a unique subsystem number, it can be addressed directly by other network nodes. Further, this enables selective filtering of signalling messages by the network operator in case of misuse. Finally, security services spanning different networks are enabled if such an interface will be standardized internationally.

Implementing security services as IN-services is also possible. But today's Intelligent Network application protocols [16] do not offer suitable interfaces. Consequently, security services solely based on IN application protocols will lack flexibility.

2.3 Authentication Services at the UNI

Fig. 5 illustrates, how the additional components (SAL, SSS protocol control, authentication control, smart card as security module) and the existing entities (Q.931 protocol control, call control) interact at the user network interface to realize an authentication service accompanying an ISDN connection setup. This is a refinement of the architecture depicted in Fig. 2. As a first solution, the exchange of security control information can be realized by using Facility information elements (FacilityIE in Fig. 5) that are used for the exchange of control information related to conventional ISDN supplementary services like call forwarding. If basic call control messages are exchanged (e.g. SetupReq), these Facility information elements can be included. If not, there is a Facility message type defined in Q.931 (DSS1) to exchange Facility information elements independently from basic call signalling messages.

The authentication protocol used is not shown in detail. It is based on the X.509 authentication framework

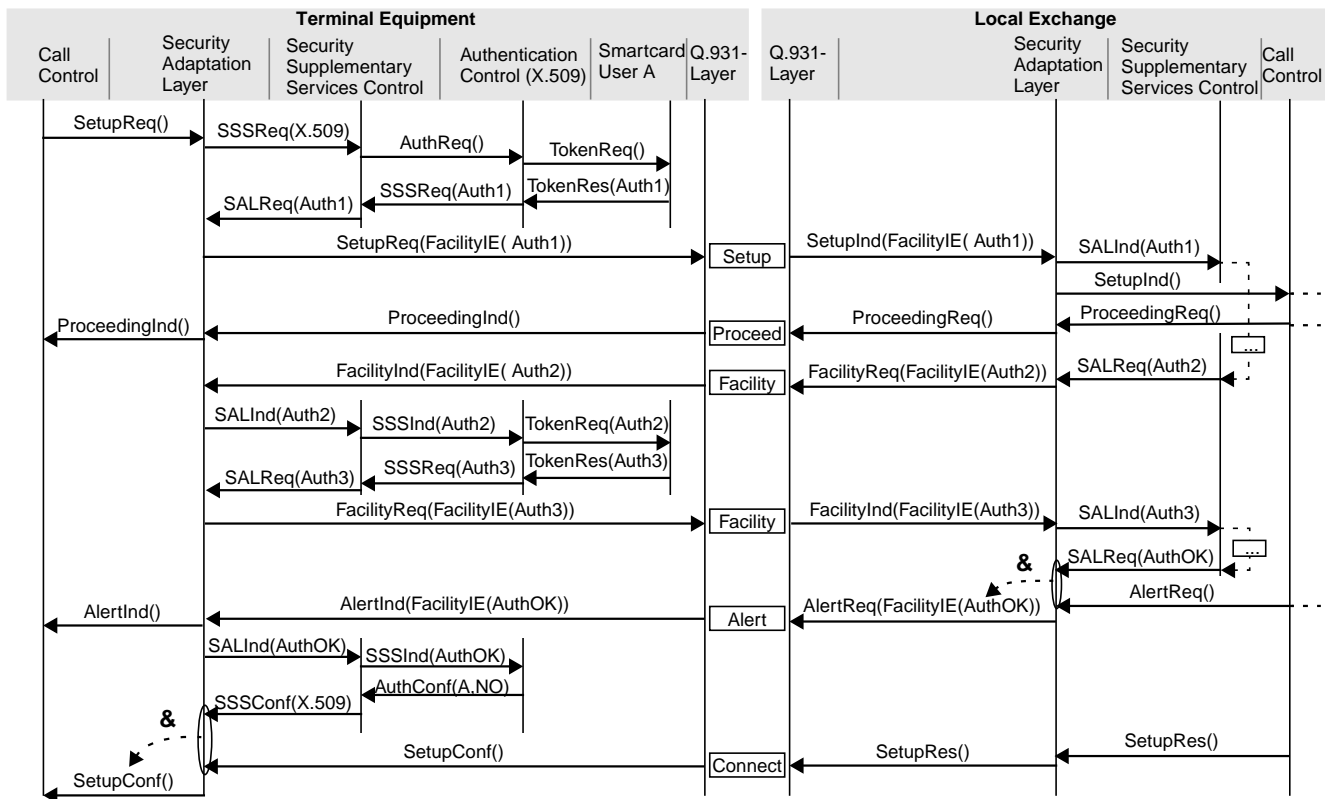


Figure 5: Diagram of an authenticated connection establishment (reworked trace based on output of an SDL-Tool)

[17] and realizes a three way handshake protocol. The authentication procedure is triggered by the SAL at connection setup (SSSReq in Fig. 5). The initiator (here: user) sends the first digitally signed authentication token Auth1 to the local exchange. The answer is a second authentication token Auth2 which demands a third token Auth3 as a reply. These tokens are generated within smart-cards and checked within the authentication control processes. The authentication control implements the authentication protocol including error handling, generates random numbers and time stamps (if needed), and synchronizes with the respective smart card.

The SAL is responsible for inserting security control data into Facility information elements and for extracting security control data from incoming signalling messages. The SAL indicates incoming security control data by sending an SALInd primitive to the Security Supplementary Services protocol control. The SSS protocol control uses the SALReq primitive to request the transfer of security control data (authentication tokens, etc.) to the peer SSS entity. The SAL ensures that specified security requirements are satisfied before a connection setup is completed, i. e. it synchronizes security supplementary services and conventional ISDN services. Therefore, the SetupConf primitive in Fig. 5 is delayed until the SSSConf primitive indicates a successful authentication accompanying the connection setup.

The SSS control indicates an unsuccessful authentication to the SAL by sending an SSSReject(X.509Auth) primitive. In this case, the SAL sends a DisconnectReq primitive to the Q.931-Layer and a DisconnectInd primitive to the call control process indicating within the cause information element that authentication failed (new standardized codes are necessary). For the sake of simplicity, we didn't figure out the retrieval of public keys – using trusted public key servers within the network – needed to examine digital signatures, and the segmentation and reassembly of security control data. Segmentation and reassembly is necessary, if security control data contains too many bytes to be inserted into a single Q.931 message.

3 Related Work

There are several proposed solutions to enhance security within public telecommunication networks. The solutions can be classified regarding the location where security functions are implemented.

One class of approaches bases on security functionality that is implemented solely within the users' terminal equipment. These approaches may be used for end-to-end security functions related to user data that is transparently exchanged over the network. For examples see [1], [7], [18], [19], [20]. Solutions basing on these approaches are

mainly used with closed user groups. Data that must be processed within telecommunication networks (calling numbers, type of service, etc.) is not suitably protected with these solutions.

Other approaches demand for the change of existing telecommunication infrastructure and services to eliminate the need for sensitive user data (identities, location information) within networks that might not be trusted by the user [11], [13], [22]. These approaches are mainly applicable for future telecommunication networks because basic network functions must be changed considerably. Concerning these solutions, security functions are located within conventional ISDN exchanges. Hence, from a security view, it is not possible to differ between security service providers and network operators that control these exchanges.

The resulting solutions are hardly flexible and scalable and lack the ability to adjust quickly to arising security requirements, threats, and attackers. Additionally, these approaches may result in a new telecommunication network that perhaps does no longer meet the requirements of network operators or service providers concerning autonomy, robustness or network diagnosis.

The ATM-Forum [23] works on security enhancements by introducing specialized information content identifiers into ATM signalling. New information elements are agreed that support the exchange of security control data. Additionally, agreements on identifiers for supported security protocols, related parameters, and protocols are done. The ATM-Forum approach addresses ATM-security. Consequently, it is rather unlikely that this approach will lead to network independent security services. This means, that the approaches developed by the ATM-Forum do not compensate the need for approaches that focus on security services that cross network boundaries (e. g. mobile to fixed calls). However, predominant approaches may profit from the definition of security services, protocols, and parameters.

The sublayer approaches of the IEEE and ISO mainly address local and metropolitan area networks [3],[4],[5]. Moreover, these approaches aren't suited for user controlled security services basing on ISDN / IN.

4 Conclusions and Outlook

This contribution has depicted some enhancements of existing signalling and service interfaces in order to promote multilaterally secure ISDN services.

The proposed security interfaces are based on the signalling systems of the ISDN but they are not restricted to those protocols. The proposed Security Adaptation Layer and Security Application Part are specific to the DSS1 and SS7 respectively. However, the Security Supplementary

Services and the Security Network Services interfaces are independent of the underlying network protocols. These services may be adapted to IP-based networks, too. Along with the growing together of ISDN and IP technology, security network services may also be based on IP technology and can be accessed via ISDN-to-IP-Gateways. Gateways that realize IP to MTP translations may substitute the SS7 link in Fig. 4b. This design option is applicable for security services that do not need access to data channels.

Mobile security modules that implement security functions based on these security services interfaces are applicable to all networks offering these service interfaces. This holds for security services both at the user network interface and at the network node interface.

Open security interfaces are a preliminary for the negotiation of security mechanisms as a basis for multilaterally secure services. The negotiation and flexible enhancement of security services will promote services that empower users and enable applications in the future.

Charging and other management tasks, that accompany network services, are to be extended in order to preserve the gain achieved by security enhancements of the service itself.

As a second step, it seems to be necessary to implement the most sensitive network functions (identification, access control, charging, location management) on separated network infrastructure that is trusted both by the user and the network operator and service provider.

Finally, as today's intelligent network services confirm, it is hard to foresee the consequences of the combination of different, independently implemented features [21]. The same problems may arise, if independently realized and distributed security features like authentication, pseudonymity, anonymity, encryption, non-repudiation and liability functions are combined. This may evolve to a main topic in realizing multilateral security. It enriches the areas of tension resulting from conflicting security goals by conflicts that result from security feature interaction and security service interaction.

5 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] IEEE 802.10: Interoperable LAN / MAN Security. IEEE Standards for Local and Metropolitan Area Networks, 1992.
- [4] ISO/IEC 11577: Network Layer Security Protocol. 1995
- [5] ISO/IEC 10736: Transport Layer Security Protocol. 1995
- [6] R. Kickartz, H. Gottschalk: Concepts of Telekom for Open Network Provision. XV Int'l Switching Symposium, April 1995
- [7] K. Tanaka, I. Oyaizu: A Confidentiality System for ISDN inter-PC High-Speed File Transfer. IEEE INFOCOM '94, 1994.
- [8] J. C. McDonald: Public Network Integrity - Avoiding a Crisis in Trust. IEEE JSAC, Vol. 12, No. 1, January, 1994.
- [9] K. Ward: The Impact of Network Interconnection on Network Integrity. British Telecommunications Engineering, Vol. 13, January, 1995.
- [10] D. L. Chaum: Untraceable Electronic Mail, Return Addresses, and Digital Pseudonyms. Communications of the ACM, Vol. 24, No. 2, 1981.
- [11] 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.
- [12] A. Pfitzmann, B. Pfitzmann, M. Schunter, M. Waidner: Trusting Mobile User Devices and Security Modules. IEEE Computer, February 1997.
- [13] H. Federrath, A. Jerichow, A. Pfitzmann: Mixes in mobile communication systems: Location management with privacy. In R. Anderson (Editor): "Information Hiding", LNCS 1174, Springer Berlin, 1996.
- [14] ITU-T Recommendations Q.931 - Q.940: Digital Subscriber Signalling System No. 1. Geneva, 1993.
- [15] ITU-T Recommendations Q.7xx: Specifications Of Signalling System No. 7. Melbourne, 1988.
- [16] ITU-T Recommendation Q.1211: General Recommendations On Telephone Switching And Signalling – Intelligent Network. Helsinki, 1993.
- [17] ITU-T Recommendation X.509: The Directory: Authentication Framework. 1993.
- [18] R. Sailer: Integrating Authentication into Existing Protocols. 5th Open Workshop on High Speed Networks, Paris, 1996.
- [19] T. K. Kwon, J. S. Song: A Key Distribution And Authentication Method On The Q.931 Calling Sequence of ISDN. Proc. Twelfth Int'l Conf. on Computer Communication, Seoul, 1995.
- [20] E. D. Myers: STU-III – Multilevel Secure Computer Interface. Proc. 10th Annual Computer Security Applications Conference, Orlando, Florida, December, 1994.
- [21] E. J. Cameron, N. Griffeth, Y. - J. Lin, M. E. Nilson, W. K. Schnure, H. Velthuijsen: A Feature-Interaction Benchmark for IN and Beyond. IEEE Communications Magazine, March 1993.
- [22] A. Pfitzmann, B. Pfitzmann, M. Waidner: ISDN-MIXes: Untraceable Communication with Very Small Bandwidth Overhead. Proc. Kommunikation in Verteilten Systemen, 1991.
- [23] ATM Security Specification – Version 1.0 (Draft). ATM Forum BTD-SECURITY-01.04, September 1997.
- [24] F. Simonds: Network Security. McGraw-Hill Series on Computer Communications, 1996.
- [25] R. Sailer: Signalling and service interfaces for separating security sensitive telecommunication functions considering multilateral security. Proc. 6th Open Workshop On High Speed Networks, Stuttgart, October 1997.