INTEGRATING CRYPTOGRAPHY IN ISDN

Kåre Presttun
Standard Telefon og Kabelfabrik A/S
Po. Box 60, Økern, N-0508 OSLO 5

1. INTRODUCTION

Security services in ISDN have been briefly discussed earlier in the literature [25, 26 and 27]. This paper deals with the protocol aspects of integrating cryptography in ISDN.

2. AUTHENTICATION AND KEY DISTRIBUTION

Authentication and key distribution should be based on the CCITT SG VII "Authentication Framework" [1]. The framework uses public key cryptography for authentication and optionally key distribution.

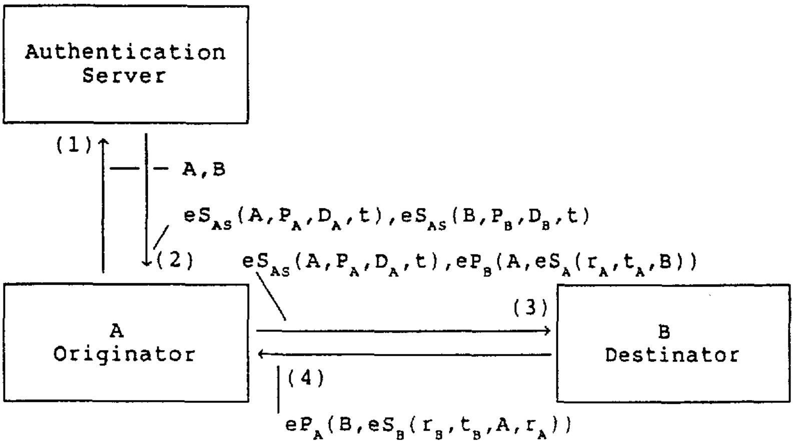

Authentication Server
(1)
A,B
$eS_{AS}(A,P_A,D_A,t),eS_{AS}(B,P_B,D_B,t)$
(2)
$eS_{AS}(A,P_A,D_A,t),eP_B(A,eS_A(r_A,t_A,B))$
(3)
A Originator
B Destinator
(4)
$eP_A(B,eS_B(r_B,t_B,A,r_A))$

Figure 1: Authentication with certificates

With this protocol A and B do not have to reveal any secret to the Authentication Server (the directory), which contains the public keys of all the users.

In the first message A says to the AS: I am A, I will talk to B. This message can optionally be signed with A's secret key. The signature can be used by the AS to see if somebody is trying to impersonate A,

C. Pomerance (Ed.): Advances in Cryptology - CRYPTO '87, LNCS 293, pp. 9-18, 1988.

requesting certificates from AS. It has no security implications beceause only the real A can create message 3 anyway, but can avoid that A get billed for certificates requested by somebody else.

The reply comes back with two certificates signed with the secret key of the AS (eS_{AS}), (eS_{AS} must be interpreted as the signed massage hash). These certificates contain the public keys of A and B (P_A, P_B), and the first and last day they are valid (D_A, D_B). This is the current CCITT format. We will recommend also to include the current time (t) as recommended by ECMA [17], and shown on the figure. This means that the certificates must be generated on line, and not off line as proposed by CCITT. The reason for this is that the current recommendation does not provide adequate means for revocation of cerificates.

In the third message, A forwards his certificate to B and appends an authentication token containing a random number he has generated and his time protected by B's public key, and signed by A.

The fourth message is B authenticating himself to A by sending a random number, his time and returning A's random number in his authentication token.

If a real time communication is not available, as in electronic mail, the fourth message cannot be used, and we end up with a one way authentication scheme instead of two way. If A and B want to send encrypted data, they can use r_A as a key for encryption A to B and r_B for encryption B to A. Alternatively they can form a common key by adding r_A and r_B bit by bit modulo two. The data encryption can be performed by a conventional encryption algorithm.

Alternatively the tokens can be modified to be used with the exponential key exchange as proposed in [25]. They will then read:

$$A, eS_A(\alpha^X \bmod q, t_A, B) \qquad (1)$$

$$B, eS_B(\alpha^Y \bmod q, t_B, A, t_A) \qquad (2)$$

where X and Y are random numbers in the range 1...q.

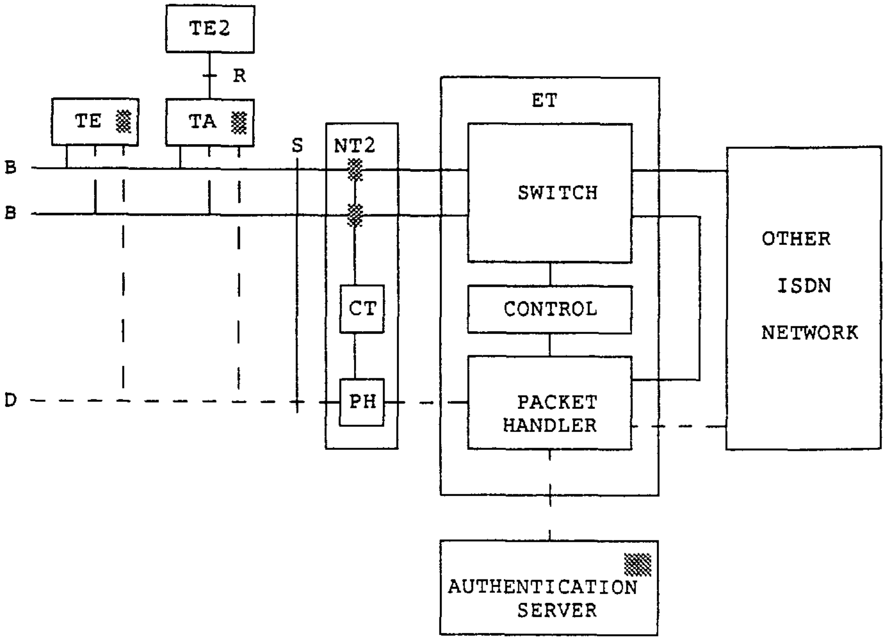
This gives us a general authentication and key distribution method for both real time communication and store and forward type communication.

3. CRYPTOGRAPHY IN ISDN

One of the main properties of ISDN (Integrated Services Digital Network, see [2,3,4]) is that a signalling/data channel (D), independent of the information channels (B), always is available to the Terminal Equipment or Terminal Adapter (Figure 2). This channel can be used for key distribution and security service management. The S interface is the standardized ISDN Basic Access, and can act as a bus with up to 8 terminals connected.

3.1 Location of the crypto processes

Proposed locations of the crypto processes are shown on figure 2. Because we want to use the D-channel for key distribution, the crypto processes must be located at points where D-channel layer 3 is processed. Possible locations are then TE, TA, NT2 and ET.



▨ Crypto Module

Figure 2: ISDN model with crypto processes located

3.2 Carrying keys

To implement the authentication framework, the first two messages (see figure 1) are transferred using the "User-to-user signalling via temporary signalling connection" facility [7]. The messages are conveyed in a new "encryption" information element in the SETUP, CONNect and USER INFOrmation messages. The "encryption" information element should carry higher layer protocols that transfer the request to the authentication server and the reply with the cerificates. This new information element should be treated like a user-user information element by the network, alternatively the user-user information element could be used. The benefit of introducing this new encryption information element is from the network operators point of view that there may be a different policy for the amount of traffic etc. to be carried in this element compared to the policy for the user-user information element.

How higher layer protocols are inserted into the "encryption" information element is shown in figure 3.

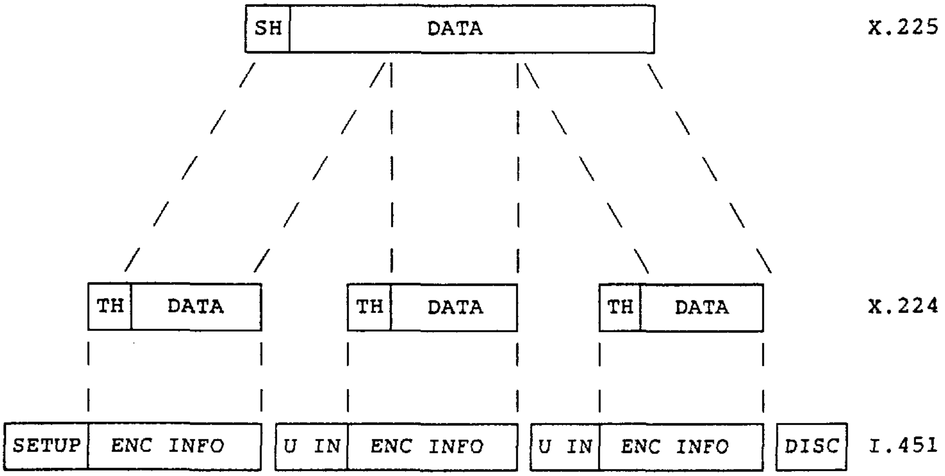


Figure 3: Inserting higher layer protocols into the D-channel protocol

The transport protocol can be of class 0 (simple class), and is needed to do segmenting and reassembling of Transport Service Data Units [15]. This is so because the length of the user-user information element is limited to 32 bytes. Embedded in the TSDU's is the Session Protocol Data Units [16]. To do a transfer of certificates and authentication tokens, only the kernel part of the session protocol is needed.

Messages 3 and 4 are transferred using the "User-to-user signalling in association with a B-channel connection" and are also conveyed in the "encryption" information element in the SETUP, CONNect and USER INFOrmation messages.

3.3 Secure Bearer services

An ISDN bearer service [5] is a service for transport of information through an ISDN network. An example of a bearer service is: 64 kbit/s, transparent, 8 kHz integrity structure, circuit switched. Our feeling is that the ISDN bearer service should not provide any end to end security measures. However, the request for bulk-encrypted trunklines could be signalled on a per call basis. This could be done by giving the encrypted trunk network a transit network code and use the "Transit network selection" information element in the SETUP message [7] to signal the request. Encryption could be provided on trunks with capacity depending on traffic requirements.

3.4 Secure Teleservices

A teleservice in ISDN [6] is a fully standardized end user service. Examples include: Telephony and Teletex. Teleservices should have security functions standardized as options at the presentation layer.

Looking at digital telephony from the OSI point of wiew, it can be regarded as having layer 1 as 64 kbit/s unrestricted with 8 kHz structure or another capability, layer 2 - 5 empty, and the voice coding method specified as layer 6 transfer syntax. The transfer syntax can be octets coded as A-law PCM or µ-law PCM, or other standardized coding methods. Thus encryption can be done at layer 6 (on the B-channel), and key management can be done via the D-channel. The signalling to indicate telephony should then be done in the "Bearer capability" information element, with information transfer capability set to unrestricted digital information, and layer and protocol (layer 1) identification set to appropriate rate and structure. Further should the actual coding and teleservice be indicated in the "High layer compatibility" information element. This is however not in line with the current understanding of bearer [5] and tele services [6], and the way a connection is requested [7]. But it seems to be in line with the basic definition of services [4] and the OSI model [14]. Here it is an inconsistency in the work done by CCITT in the previous study period.

In the recommendations for bearer services and signalling [5,7], speech transmission is regarded as a bearer service, while the actual teleservice, Telephony, is unspecified. In the signalling system the speech coding is signalled as "user information layer 1 protocol".

A proposed way to do security enhancements to Telephony in ISDN is: Signal the way now specified in the signalling system, include the "encryption" informaton element in SETUP and CONNect, and indicate encryption in the "CCITT-standardized facilities" information element in SETUP message to prevent the network from doing signal processing on the encrypted voice signal.

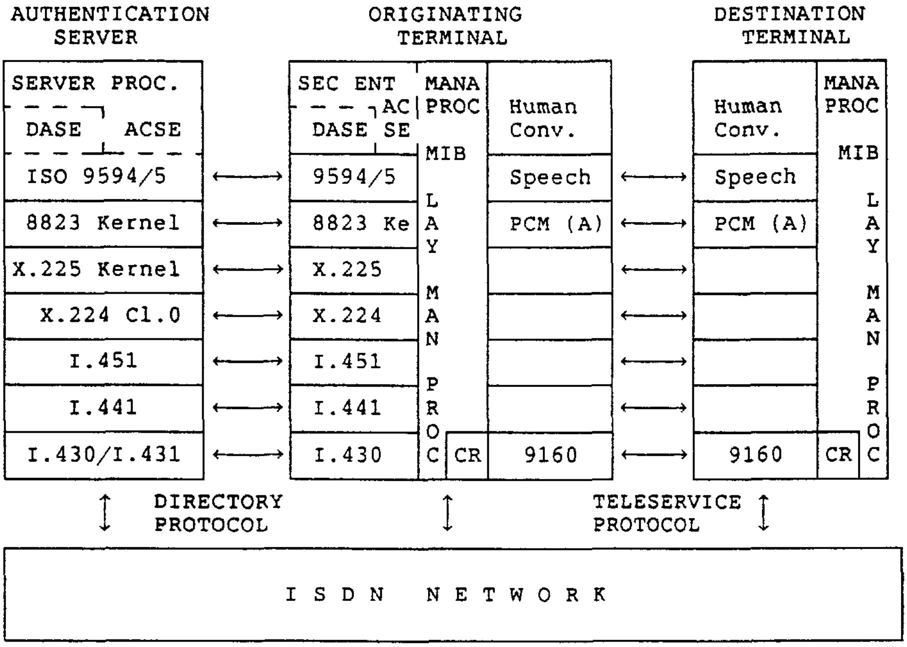


Figure 4: Protocol System for Secure Voice

Figure 4 shows how the protocol hierarchy can be built up. On top of the session protocol we find the kernel of the presentation layer [20]. As there is no need for context management, only the kernel part of the presentation protocol is needed. The Association Control Service Elements (ACSE) [19] operate on the session kernel functions and control the association for key material transfer. The Directory Access Service Elements (DASE) [23] operates on the Directory Access Protocol (DAP) [24] and is the actual application protocol used to retrieve the cerificates.

On top of the service elements is the actual server process [22]. The management process in the originating terminal communicates with the server process via these service elements. The retrieved certificates are kept in the Management Information Base (MIB) [18]. The management process communicates with cryptoservices in the terminal to verify the certificates and to generate keys and authentication tokens. The keys for data encryption are then installed in the crypto process at the actual layer by the Layer Management Process.

For voice the encryption takes place at layer 1, using appropriate parts of the physical layer encryption standard [21].

To implement security in other teleservices than telephony, the security services should be implemented at layer 6. For packet mode terminals both the association with the authentication server and the end to end association should be established as normal packet mode calls. Protocols to be used for authentication and key distribution, utilizing the authentication framework, and data transfer are shown in figure 5.

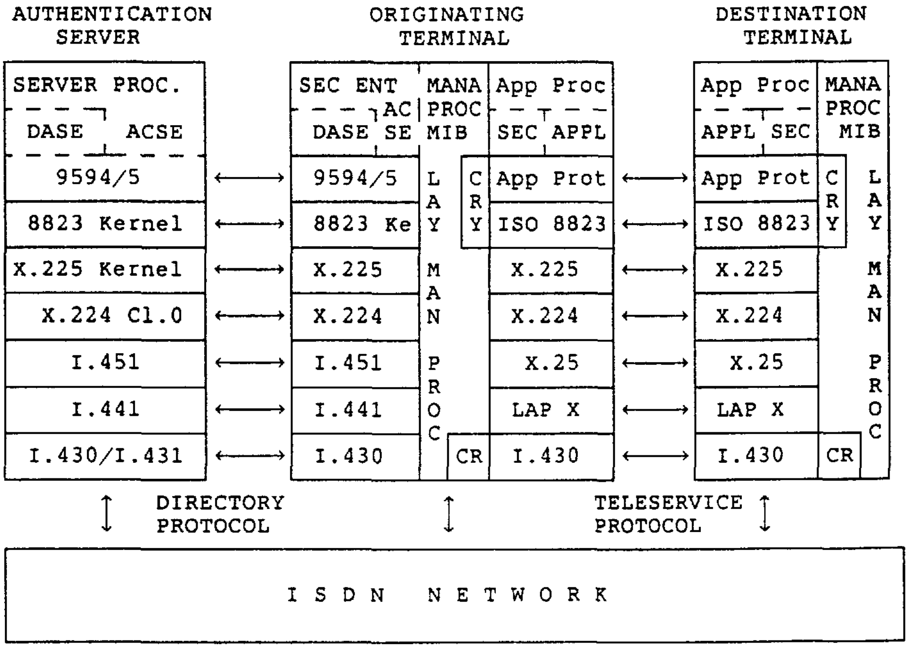


Figure 5: Protocol System for Secure Teleservices

The main difference from the voice case (in figure 4) is the protocols used for data transfer. The protocols are specified for the actual teleservice, and figure 5 shows the general case.

3.5 Support of existing terminals

A series of recommendations for the support of existing terminals on an ISDN have been developed [8,9,10,11,12]. We will recommend security enhancements to be worked out for circuit switched services only. For packet mode terminals the security services should be built into the higher layer protocols.

For circuit mode connections, a service with automatic key distribution can be developed if both terminals are connected to an ISDN. Whether it can be done with one of the terminals connected to a CSPDN (Circuit Switched Public Data Network) with maximum integration [9] needs further study. The minimum integration case does not seem to be applicable for automatic key distribution.

Encryption can be implemented, superposed on circuit switched services [9,11,12] according to ISO recommendations [21], in TAs (see figure 2) utilizing the D-channel for keymanagement.

4. ISDN AUTHENTICATION SERVER

An ISDN authentication server should be connected to a D-channel at the lowest layer in the exchange hierarchy. The data rate of the channel is dependent on the traffic. By indicating the higher layer protocols used for communication with the AS when a call to the AS is made, it is possible to build an AS common to all needs.

When the number of terminals with encryption capabilities increases, there will be a need for networks of authentication servers, constituting a distributed authentication system. At higher layers in the exchange hierarchy where the D-channel protocol is not available, ISUP [13] in signalling system No. 7 must be used for communication between the exchange and the AS. The communication between AS's will be based on the Directory System Protocol (DSP) [24]. There does not exist any direct relationship between the hierarchy of exchanges and the hierarchy of AS's as both hierarchies are developed according to traffic demands in the two systems.

5. CONCLUSION

In this paper it has been illustrated how existing work in ISO, CCITT, and ECMA can be utilized to integrate cryptography in ISDN. Necessary protocol mechanisms have been selected in such a way that interworking with cryptographic functions in other networks than ISDN should be possible.

There is a lot of standardization issues that must be addressed by CCITT and ISO before the security services can be implemented at a large scale internationally. It is expected that results will come from CCITT during the next studyperiod 1989 - 1992.

REFERENCES

[1] CCITT SG VII, Draft Recommendation X.ds7, The Directory - Authentication Framework, Geneva, October 1986.

[2] CCITT red book, I.120, Integrated Services Digital Networks (ISDNs), Malaga-Torremolinos 1984.

[3] CCITT red book, I.130, Attributes for the Characterization of Telecommunication Services Supported by an ISDN and Network Capabilities of an ISDN, Malaga-Torremolinos 1984.

[4] CCITT red book, I.210, Principles of Telecommunication Services Supported by an ISDN, Malaga-Torremolinos 1984.

[5] CCITT red book, I.211, Bearer Services Supported by an ISDN, Malga-Torremolinos 1984.

[6] CCITT red book, I.212, Teleservices supported by an ISDN, Malaga-Torremolinos 1984.

[7] CCITT red book, I.451 (Q.931), ISDN user-network interface layer 3 specification, Malaga-Torremolinos 1984.

[8] CCITT red book, I.460, Multiplexing, rate adaption and support of existing interfaces, Malaga-Torremolinos 1984.

[9] CCITT red book, I.461 (X.30), Support of X.21 and X.21 bis based DTEs by an ISDN, Malaga-Torremolinos 1984.

[10] CCITT red book, I.462 (X.31), Support of Packet Mode Terminal equipment by an ISDN, Malaga-Torremolinos 1984.

[11] CCITT red book, I.463 (V.110), Support of DTEs with V-series type interfaces by an ISDN, Malaga-Torremolinos 1984.

[12] CCITT red book, I.464, Rateadaption, multiplexing and support of existing interfaces for restricted 64 kbit/s transfer capability, Malaga-Torremolinos 1984.

[13] CCITT red book, Q.761, Functional Description of the ISDN User Part of Signalling System No. 7, Malaga-Torremolinos 1984.

[14] CCITT red book, X.200, Reference model of Open Systems Interconnection for CCITT applications, Malaga-Torremolinos 1984.

[15] CCITT red book, X.224, Transport Protocol Specification for Open Systems Interconnection for CCITT applications, Malaga-Torremolinos 1984.

[16] CCITT red book, X.225, Session Protocol Specification for Open Systems Interconnection for CCITT applications, Malaga-Torremolinos 1984.

[17] ECMA/TC32-TG9/87/12, CCITT SG VII Contribution, Security of Directories, February 1987.

[18] ISO 7498/4, Open Systems Interconnection - OSI Management Framework.

[19] ISO/DP 8649/2, Open Systems Interconnection - Association Control: Service Definition.

[20] ISO/DIS 8823, Open Systems Interconnection - Connection Oriented Presentation Protocol Specification.

[21] ISO/DP 9160, Information Processing - Data Encipherment - Physical Layer Interoperability requirements.

[22] ISO/DP 9594/1, Open Systems Interconnection - The Directory - Part 1: Overview of Concepts, Models and Secvices.

[23] ISO/DP 9594/3, Open Systems Interconnection - The Directory - Part 3: Access and System Service Definition.

[24] ISO/DP 9594/5, Open Systems Interconnection - The Directory - Part 5: Access and System Protocols Specification.

[25] B. O'Higgins, W. Diffie, L. Strawczynski, R. de Hoog, Encryption and ISDN - A Natural Fit, Proc. ISS'87, Phoenix, March 15-20, 1987, pp 863 - 869.

[26] Kåre Presttun, Security Measures in Communication Networks, Electrical Communication, Vol 60 No 1, 1986, pp 63 - 70.

[27] K. Siuda, Technische Massnahmen für die sichere Informationsübertragung in zukünftigen Fernmeldenetzen (ISDN), Bull. SEV/VSE 77(1986) 1, 11. Januar, pp 5 - 11.

NOTE

A tutorial on higher layer OSI can be found in: ISO/TC68/SC5/N174, Methodology and Guidelines for Application Protocol Development.