TS 101 323 V1.2.3 (1999-07)

Technical Specification

Telecommunications and Internet Protocol Harmonization Over Networks (TIPHON); Interoperable security profiles

Reference

DTS/TIPHON-03006 (c9000iq3.PDF)

Keywords

interoperability, IP, profile, security, voice

ETSI

Postal address

F-06921 Sophia Antipolis Cedex - FRANCE

Office address

650 Route des Lucioles - Sophia Antipolis
Valbonne - FRANCE
Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16
Siret N° 348 623 562 00017 - NAF 742 C
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° 7803/88

Internet

secretariat@etsi.fr
Individual copies of this ETSI deliverable
can be downloaded from
http://www.etsi.org
If you find errors in the present document, send your
comment to: editor@etsi.fr

Contents

Intellectual Property Rights

IPRs essential or potentially essential to the present document may have been declared to ETSI. The information pertaining to these essential IPRs, if any, is publicly available for **ETSI members and non-members**, and can be found in SR 000 314: *"Intellectual Property Rights (IPRs); Essential, or potentially Essential, IPRs notified to ETSI in respect of ETSI standards"*, which is available **free of charge** from the ETSI Secretariat. Latest updates are available on the ETSI Web server (http://www.etsi.org/ipr).

Pursuant to the ETSI IPR Policy, no investigation, including IPR searches, has been carried out by ETSI. No guarantee can be given as to the existence of other IPRs not referenced in SR 000 314 (or the updates on the ETSI Web server) which are, or may be, or may become, essential to the present document.

Foreword

This Technical Specification (TS) has been produced by ETSI Project Telecommunications and Internet Protocol Harmonization Over Networks (TIPHON).

The contents of the present document are the result of contributions and discussions in Working Group 3. The structure of the document and overall principles of the standard were agreed upon, but the details described in the text should be seen as a draft version for further study. The complete text is not yet approved.

1 Scope

The present document specifies a set of protocols and associated profiles for security mechanisms that may be used by Internet telephony equipment. Those security mechanisms may provide authorization, confidentiality, access control, non-repudiation, and data integrity. The present document includes sufficient detail so that Internet telephony devices that conform to these specifications will be mutually interoperable.

The present document does ***not*** define security at a service level, and it is ***not*** intended as a means by which network operators can unambiguously define the security of Internet telephony services.

2 References

The following documents contain provisions which, through reference in this text, constitute provisions of the present document.

- References are either specific (identified by date of publication, edition number, version number, etc.) or non-specific.
- For a specific reference, subsequent revisions do not apply.
- For a non-specific reference, the latest version applies.
- A non-specific reference to an ETS shall also be taken to refer to later versions published as an EN with the same number.

[1] TR 101 232: "Telecommunications Security; Glossary of security terminology".

[2] TS 101 312: "Telecommunications and Internet Protocol Harmonization Over Networks (TIPHON); Network architecture and reference configurations; Scenario 1".

[3] ISO 9798-3 (1.5.2): "Information technology; Security techniques; Entity authentication; Part 3: Mechanisms using digital signature techniques".

[4] ISO 11770-3 (7.4): "Information technology; Security techniques; Key management; Part 3: Mechanisms using asymmetric techniques".

[5] IMTC: "Security Profile 1"; from ftp://ftp.imtc-files.org/imtc-site/VoIP-AG/SP1-9810.doc.

[6] ITU-T Recommendation H.225.0 (1998): "Call signalling protocols and media stream packetization for packet-based multimedia communication systems".

[7] ITU-T Recommendation H.245 (1998): "Control protocol for multimedia communication".

[8] ITU-T Recommendation H.235 (1998): "Security and encryption for H-Series (H.323 and other H.245-based) multimedia terminals".

[9] ITU-T Recommendation H.261 (1993): "Video codec for audiovisual services at p x 64 kbit/s".

[10] ITU-T Recommendation H.263 (1998): "Video coding for low bit rate communication".

[11] ITU-T Recommendation X.509 (1997): "Information technology - Open Systems Interconnection - The Directory: Authentication framework".

3 Definitions and abbreviations

3.1 Definitions

For the purposes of the present document, the following terms and definitions apply:

Access Control: prevention of unauthorized use of a resource, including the prevention of use of a resource in an unauthorized manner

Authentication: property by which the correct identity of an entity or party is established with a required assurance

Confidentiality: avoidance of the disclosure of information without the permission of its owner

Integrity: avoidance of the unauthorized modification of information

Non-repudiation: property by which one of the entities or parties in a communication cannot deny having participated in the whole or part of the communication

3.2 Abbreviations

For the purposes of the present document, the following abbreviations apply:

Ack	Acknowledgement
Alg-ID	Algorithm ID, for signature and hash
Caps	Media Capabilities
CBC	Cipher Block Chaining
Cert	Certificate
DES	Data Encryption Standard
DSS	Digital Signature System
E	Encrypted with public key
ECB	Electronic Code Book
g	Diffie-Hellman parameter (generator)
GF	Galois Field
IP	Internet Protocol
K	Media stream key
OID	Object Identifier
p	Diffie-Hellman parameter (prime modulus)
r	Random number
RAS	Registration, Admission and Status
RSA	Public-key cryptosystem for both encryption and authentication; invented by Ron Rivest, Adi Shamir, and Leonard Adleman
RTCP	Real Time Control Protocol
RTP	Real Time Protocol
SecCaps	Security capabilities
SHA	Secure Hash Algorithm
SSL	Secure Socket Layer
Sync	Synchronization
T	Timestamp
TCP	Transmission Control Protocol
TLS	Transport Layer Security

4 Security Profiles

When security is required for interconnection of domains, TIPHON-compliant systems shall provide security services according to one or more of the following interoperable security profiles. These profiles identify their purpose, and they specify the method, cryptographic algorithms, and cryptographic parameters (e.g. key lengths) for:

- the five security services (authentication, access control, non-repudiation, confidentiality, and integrity);
- four or more protocol components (RAS, H.225.0 [6], H.245 [7], RTP);
- the security information flows identified in TS 101 312 [2] (S1-S17).

As a convenient reference, profiles may include a summary matrix of the following form for each security information flow.

Table 4.1a

Security Services	**Call Functions**				
	RAS	**H.225.0 [6]**	**H.245 [7]**	**RTP**	**Other(s)**
Authentication					
Access Control					
Non-Repudiation					
Confidentiality					
Integrity					

Each element in the matrix identifies the security mechanism (Not applicable, None, IPSEC, TLS/SSL, Token, H.235 [7], or Other) and the cryptographic algorithm(s) and parameters supported.

In addition, each profile description includes the detailed information sufficient to ensure interoperability, and lists the attacks it counters, the provided security level, and the potential consequences of a breach in its security.

If a profile includes multiple tables (e.g. for multiple security information flows), then the security mechanisms specified for each service shall not contradict each other.

NOTE: All security profiles are referred to by their section number in this specification (e.g. "Profile 4.1") rather than a descriptive term.

4.1 Security Profile 4.1

The profile 4.1 will enable the user to use an integrated secure key management on H.245 [7] without SSL/TLS.

Table 4.1b: Security Profile 4.1

Security Services	**Call Functions**			
	RAS	**H.225.0 [6]**	**H.245 [7]**	**RTP**
Authentication	None	None	Integrated H.245 [7] Certificate-Based according to ITU-T Recommendation H.235 [8]	As Negotiated by Integrated H.245 [7]
Access Control	None	None	None	None
Non-Repudiation	None	None	None	None
Confidentiality	None	None	protected Key Management according to ITU-T Recommendation H.235 [8]	As Negotiated by Integrated H.245 [7]
Integrity	None	None	protected Key Management according to ITU-T Recommendation H.235 [8]	None

4.1.1 Scope

This key management protocol shall be used on packet based networks over firewalls and in environments where SSL/TLS is either not used or not applicable. The integrated H.245 [7] key management is used on IP-networks (Intra-/Internets) and inside the IP-end-terminal and the gateway. The profile exchanges the media keys securely through firewalls.

4.1.2 Protected Protocols

The profile protects the H.245 [7] key management protocol in the IP-end-terminal and the gateway.

4.1.3 Security Techniques

Profile 4.1 is an integrated H.245 [7] key management and uses cryptographic key management and protocols according to ISO 9798-3 [3]. The key management procedures use security techniques for challenge and response or timestamp based mechanisms and apply asymmetric cryptographic methods with en/decryption and digital signatures and provide optional certificate exchange.

4.1.4 Security Services

Integrated H.245 [7] key management provides the following security services:

- unilateral/mutual authentication of terminals;
- access control upon authentication information;
- comfortable certificate exchange;
- key management for distributing and establishing session keys for the voice channel:
    - protected key distribution (authentication and integrity);
    - key synchronization;
    - key update.

4.1.5 Security Mechanisms

The H.245 [7] key management security services utilize the following security mechanisms:

- challenge and response protocol with random numbers for authentication and replay protection;
- timestamps for replay protection;
- asymmetric encryption;
- digital signature for authentication and key exchange (authentication and integrity).

4.1.6 Cryptographic Algorithms and Parameter

This security profile references figure 1, 2 and 3 where the following security parameters and cryptographic algorithms are used. The cryptographic algorithms are defined with respect to three different security levels. A high security version, a medium security level and an exportable level with restricted security. The low security shall be the default, while medium and high security are options.

- Alg-ID Algorithm ID for signature and hash, depends on the used certificate and the applied signature scheme (RSA, DSS, ...).
  A list of OIDs needs to be defined.
  (e.g. RSA-2 048-SHA1 for high security:
  RSA based signature using 2 048 bit private key and SHA1 for hashing.
  RSA-1 024-SHA1 for medium security:
  RSA based signature using 1 024 bit private key and SHA1 for hashing.
  RSA-512-SHA1 for low/exportable security:
  RSA based signature using 512 bit private key and SHA1 for hashing).

- E Encryption with public key, OIDs need to be defined.
  (e.g. RSA-2 048 for high security:
  RSA based signature using 2 048 bit public key.
  RSA-1 024 for medium security:
  RSA based signature using 1 024 bit public key.
  RSA-512 for low/exportable security:
  RSA based signature using 512 bit public key).

- SecCaps H.235 [8] Capabilities references the OID for the voice encryption algorithm,
  OIDs needs to be defined.
  (e.g. 3key3DES-ECB-168 and 3key3DES-CBC-168 for high security;
  2key3DES-ECB-112 and 2key3DES-CBC-112 for medium security;
  DES-ECB-56 and DES-CBC-56 (see note) for low/exportable security).

NOTE: ISO Entry Name: {iso standard 9979 des(4)}.

4.1.7 Countered Attacks

The profile counters the following attacks:

- masquerade by spoofing IP addresses and other H.245 [7] addressing information;
- interception of exchanged H.245 [7] key management data;
- active as well as unintentional manipulation of H.245 [7] key management data;
- replay of key management messages.

4.1.8 Provided Security Level

The provided security level depends on the strength of the applied cryptographic algorithms as well as on the length of the asymmetric keys (public and private), the quality of the generated random number and the security policy determining the key update cycle and the implementation of the security techniques. Under reasonable assumptions the provided security level is considerably high.

The security level is specifically defined through the used security parameters and the cryptographic algorithms in subclause 4.1.6.

4.1.9 Potential Damage when breached

An attacker may try to attack the H.245 [7] key management by several ways: attacks on the network transmitted data and attacks on the crypto systems in use. When the attacker is able to break the asymmetric encryption algorithms, finds out the private keys of users and certificate authorities as well he will succeed in breaking the entire key management protocol and is finally able to intercept the exchanged voice encryption keys.

In the end the potential damage depends on the actual environment and the confidentiality and value of the communicated data.

4.1.10 Contents of Security Profile

H.245 version 2 defines the "Control Protocol for Multimedia Communication" for audio/video on packet-based networks. All H.245 [7] signalling protocol communication relies on a reliable transport layer (e.g. TCP). H.245 [7] uses in-band negotiation of various capabilities such as terminal, codec and formats, audio/video and network adaptation and protocol capabilities. That negotiation of the capabilities occurs before any media communication takes place. The negotiation does not tell which features are used for a particular logical channel. Merely, the negotiation phase just determines which capabilities the involved terminals offer. After successful capability negotiation the terminals are aware of a common set of capabilities which they can use for their communication. The open logical channel procedure that is executed later on during the call establishment phase indicates which particular capability feature of the negotiated capability set shall be used.

After successful capability negotiation, terminals decide during the master/slave determination phase which one act in the master role and which one is the slave. This is done by a procedure that takes into account the fixed assigned terminal type numbers of gateways, gatekeepers and end-terminal and a 24-bit random number.

H.245 [7] procedures may take quite a long time until final media stream channels have been established.

The H.225.0 [6] fast connect procedure avoids such long round-trip time by circumventing H.245 [7] procedures. During fast connect, all H.245 [7] control channel information is piggy-backed within the Set-up and Connect messages, shortening overall round-trip significantly (see subclause 4.2).

4.1.10.1 Security negotiation by H.245

H.245 [7] allows to negotiate security capabilities for media streams protection ‘in-band’ on the secured H.245 [7] control channels. Presently, only encryption can be negotiated; integrity for the media streams is for further study. The security parameters for the media stream are included in the H.245 [7] capability set. H.245 [7] uses the concept of independent logical channels which can be secured also individually. Whenever a new logical channel is opened the security capability negotiation determines the security services. This allows to negotiate a different encryption algorithm for audio than for video data. Even more fine grained separation is possible when different encryption algorithms) are negotiated depending on the bandwidth and codec format (e.g. H.261 [9] or H.263 [10]). However, it is also possible to apply the same encryption algorithm to all media stream data when always the same encryption algorithm is used.

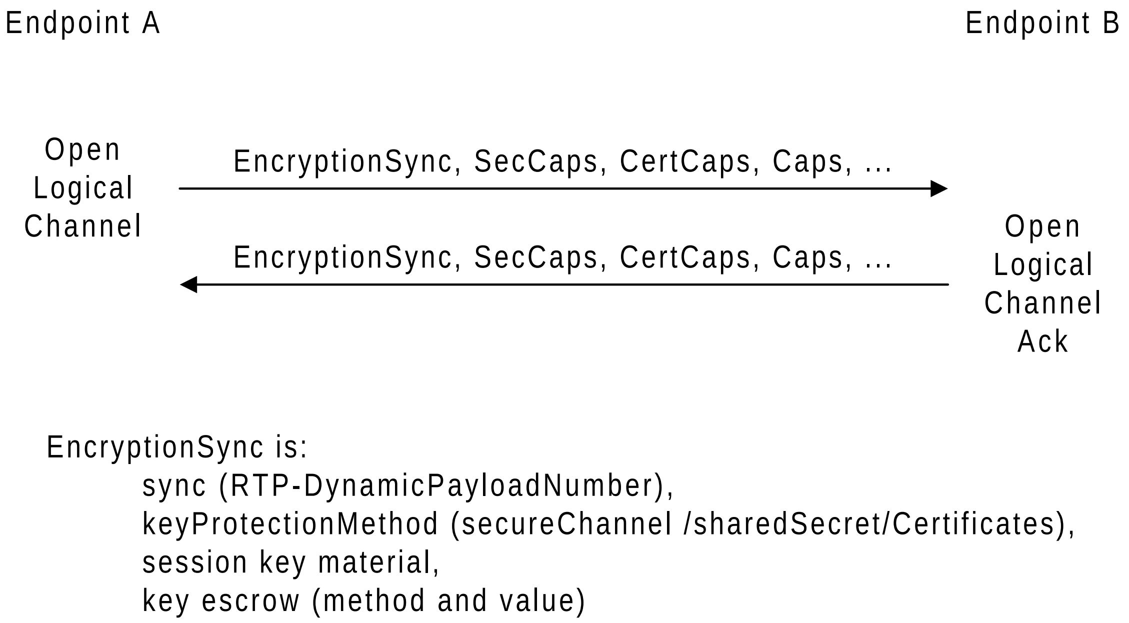
Endpoint A
Endpoint B
Open Logical Channel
EncryptionSync, SecCaps, CertCaps, Caps, ...
EncryptionSync, SecCaps, CertCaps, Caps, ...
Open Logical Channel Ack
EncryptionSync is:
sync (RTP-DynamicPayloadNumber),
keyProtectionMethod (secureChannel /sharedSecret/Certificates),
session key material,
key escrow (method and value)

Figure 1: Open logical channel and security

The negotiation is initiated when a logical channel is opened (Open Logical Channel). As figure 1 shows *Open Logical Channel* and *Open Logical Channel Ack* carry several security related parameters: *Caps* are the regular H.245 [7] terminal capabilities while *SecCaps* are the security capabilities such as encryption capability with encryption algorithm, encryption mode and additional parameters such as block size and key length. The *Encryption Sync* includes several other parameters such as the RTP-dynamic payload number for crypto synchronization, the key protection method, the session key material and key escrow information. The key protection method specifies whether TLS/SSL secured channels are used, whether manual key management and security negotiation is applied using shared secrets or a plain H.245 [7] channel is used with separate authentication and key management protocols using certificates. Key material contains the secret bits of the media session key. Optional key escrow data allows to specify a key escrow method and a key escrow value.

Manual key management with symmetric or pre-negotiated security capabilities (shared secret key protection method) does not use any of H.245 [7] built-in key management features. This method assumes that both entities possess a shared secret and that the negotiation has been done outside of H.235 [8]/H.245 [7]. The shared secret is used to protect the media stream key during fast connect when an authenticated Diffie-Hellman key distribution protocol is. Such a method may also be useful for testing partial implementations or when no key management is available for whatever reason.

4.1.10.2 Authentication and key management on plain text H.245 channels

The **certificate capability** allows the sender to define a set of accepted certification authorities as well as a set of desired "context-based" certificate types such as X.509v3 [11] RSA or X.509v3 [11] DSS certificates. The responder can return its certificate according to the request; if the security policy does not allow to return a certain certificate or such a certificate is not available, then the responder may respond without a certificate. While this feature does not provide specific security it shall facilitate agreeing and using certificates in a more comfortable and faster way than it is possible today (e.g. by SSL/TLS). Note, the TLS does not offer such a menu of potential certificates. Thus, especially when many different certificates are used potentially, chances may be high, that both parties could not agree immediately on a common certificate pair; this would increase round-trip time.

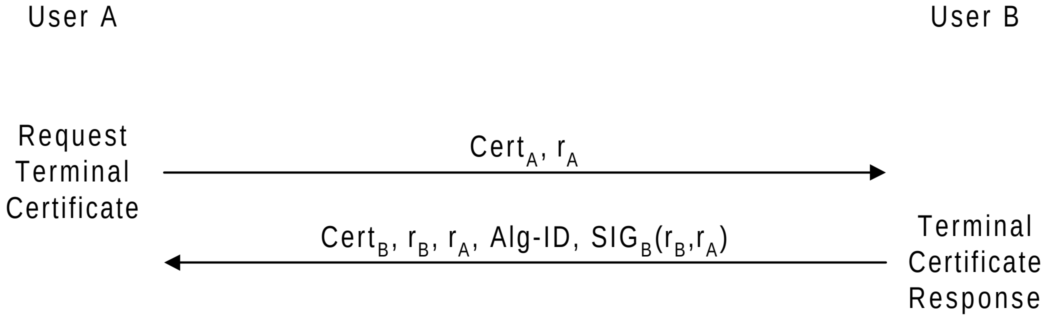
User A
User B
Request Terminal Certificate
$Cert_A$, r_A
$Cert_B$, r_B, r_A, Alg-ID, $SIG_B(r_B,r_A)$
Terminal Certificate Response

Figure 2: Unilateral user authentication on H.245 plain text channels

When TLS/SSL is not available (e.g. due to proxy/firewall use), authentication and session key distribution cannot rely on a TLS/SSL secured H.245 [7] control channel. Then unilateral authentication (see figure 2) by ISO 9798-3 [3] should be used instead. Mutual authentication can be achieved by executing the unilateral authentication protocol in the reverse direction a second time by the remote entity. The authentication protocol uses the H.245 [7] *Request Terminal Certificate/Terminal Certificate Response* handshake protocol. By requesting the unilateral authentication protocol from the other side mutual authentication is achieved.

After the terminals finished the authentication phase, both terminals possess each others certificate and public key. The session key can be requested and distributed by the following key management protocol (see figure 3) according to ISO11770-3 [4]. The master generates the new session key and encrypts it by the slave's public key.

As minimization of round-trip delay for H.245 [7] is not considered a requirement, separation of authentication and key distribution is possible.

4.1.10.3 Key update procedures

Encryption Update and *encryption Update Request* are two specific H.245 [7] security commands. These commands can be used at any time to dynamically update (distribute) or request new session keys in case the actual used key is considered becoming insecure. Reasons for such a key-update are transmission of sufficient amount of encrypted media data (see note), security level of the encryption algorithm and limited lifetime of the session key, detected loss of privacy on a logical channel and other security requirements defined by security policy. The master generates, distributes and indicates a new session key by encryption Update either on its own decision or on request of a slave. The key-update procedures may also be used to distribute new session keys from the master to all involved terminals when a new participant joined the conference or when a participant left the conference. Distribution of a new session key enforces that participants are ejected from the conference and cannot continue to participate and listen anymore to the ongoing communication. The key update procedure can also be used to re-synchronize a logical channel using the dynamic RTP payload number.

NOTE: Exhausting more than half of the ciphertext space.

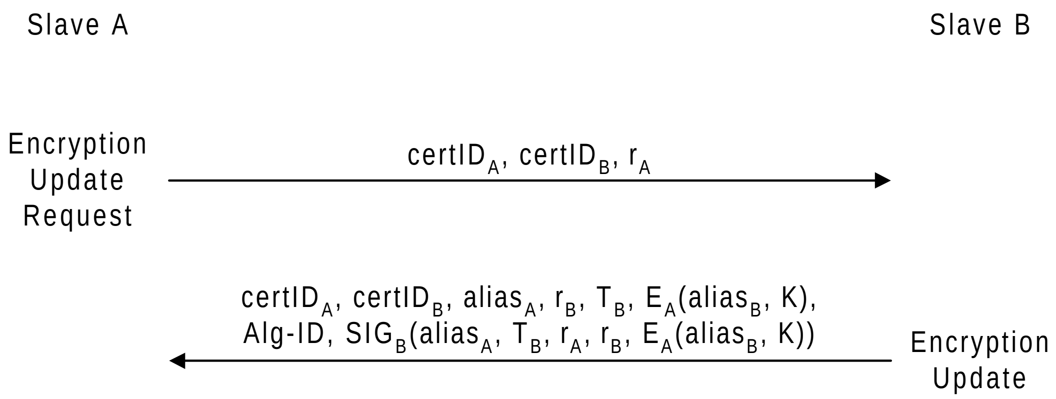
Slave A
Slave B
Encryption Update Request
$certID_A$, $certID_B$, r_A
$certID_A$, $certID_B$, $alias_A$, r_B, T_B, $E_A(alias_B, K)$,
Alg-ID, $SIG_B(alias_A, T_B, r_A, r_B, E_A(alias_B, K))$
Encryption Update

Figure 3: Session key distribution on plain text H.245 channels

Note, that the key management protocol shown in figure 3 actually covers two scenarios: In the first scenario the two-way handshake protocol is used when the slave requests a new session key from the master by a challenge (*encryption Update Request*). Then the master responds using the *encryption Update* without the timestamps. The slave can also send a list of available certificate types and also a list of desired certificates to the master. This mechanism shall facilitate interoperability and speed up the key-distribution process in case when using many different types of certificates. Note, that the master need not respond with the requested certificate types; either because of security policy or lack of appropriate certificates.

The second scenario is just the unidirectional unsolicited *encryption Update* issued by the master without prior request. Since the master does not possess a fresh challenge from the slave, the two-way challenge response protocol cannot be used. Instead of using the slave's random number, timestamps are used to provide timeliness in that case.

4.2 Security Profile 4.2

The profile 4.2 will enable the user to perform a secure fast set-up of a call and to use an integrated secure key management without using SSL/TLS.

Table 4.2: Security Profile 4.2

Security Services	**Call Functions**			
	RAS	**H.225.0 [6]**	**H.245 [7]**	**RTP**
Authentication	None	Integrated H.225.0 [6] Certificate-Based according to ITU-T Recommendation H.235 [8]	Not Applicable	As Negotiated by Integrated H.225.0 [6]
Access Control	None	None	Not Applicable	None
Non-Repudiation	None	None	Not Applicable	None
Confidentiality	None	Protected Key Management according to H.235 [8]	Not Applicable	As Negotiated by Integrated H.225.0 [6]
Integrity	None	Protected Key Management according to ITU-T Recommendation H.235 [8]	Not Applicable	None

4.2.1 Scope

This key management protocol shall be used to reduce the setup time with packet based networks connections over firewalls and in case no SSL/TLS is used. It is used on IP-networks (Intra-/Internets) and inside the IP-end-terminal and the gateway. The profile defines how to exchange the media keys securely through firewalls.

4.2.2 Protected Protocols

The profile protects the piggybacked key management protocol during fast connect in the IP-end-terminal and the gateway.

4.2.3 Security Techniques

Profile 4.2 is a secured fast setup key management profile working on the plain text H.225.0 [6] call signalling channel and provides authenticated Diffie-Hellman key exchange using time stamps, digital signature and optional certificate exchange. This key agreement protocol use Diffie-Hellman techniques and applies asymmetric methods and uses digital signatures.

4.2.4 Security Services

Secure fast connect provides the following security services:

- unilateral/mutual authentication of terminals;
- access control upon authentication information;
- certificate exchange;
- key management for agreeing and establishing session keys for the voice channel:
    - protected key distribution (authentication and integrity).

4.2.5 Security Mechanisms

Secure fast connect utilizes the following security mechanisms:

- challenge and response protocol with random numbers and timestamps;
- Diffie-Hellman key agreement;
- digital signature for key exchange (authentication and integrity).

4.2.6 Cryptographic Algorithms and Parameter

This security profile references figure 4 and 5 where the following security parameters and cryptographic algorithms are used. The cryptographic algorithms are defined with respect to three different security levels. A high security version, a medium security level and an exportable level with restricted security. The low security shall be the default, while medium and high security are options.

- Alg-ID Algorithm ID for signature and hash, depends on the used certificate and the applied signature scheme (RSA, DSS, ...).
  A list of OIDs needs to be defined.
  (e.g. RSA-2 048-SHA1 for high security:
  RSA based signature using 2 048 bit private key and SHA1 for hashing.
  RSA-1 024-SHA1 for medium security:
  RSA based signature using 1 024 bit private key and SHA1 for hashing.
  RSA-512-SHA1 for low/exportable security:
  RSA based signature using 512 bit private key and SHA1 for hashing).

- g Default Diffie-Hellman parameter, primitive root as long integer.
  (e.g. chosen from GF(2 048) for high security with 2 048 bits;
  chosen from GF(1 024) for medium security with 1 024 bits;
  chosen from GF(512) for low/exportable security with 512 bits).

- p Default Diffie-Hellman parameter, prime modulus as long integer.
  (e.g. 2 048 bit for high security;
  1 024 bit for medium security;
  512 bit for low/exportable security).

- H.235 Caps H.235 Capabilities references the OID for the voice encryption algorithm,
  OIDs needs to be defined.
  (e.g. 3key3DES-ECB-168 and 3key3DES-CBC-168 for high security;
  2key3DES-ECB-112 and 2key3DES-CBC-112 for medium security;
  DES-ECB-56 and DES-CBC-56 (see note) for low/exportable security).

NOTE: ISO Entry Name: {iso standard 9979 des(4)}.

4.2.7 Countered Attacks

The profile counters the following attacks:

- masquerade by spoofing IP addresses and other H.225.0 [6] addressing information;
- interception of exchanged of H.225.0 [6] key management data within secure fast connect;
- active as well as unintentional manipulation of secured fast connect key management data;
- replay protection of secure fast connect key management messages.

4.2.8 Provided Security Level

The provided security level depends on the strength of the applied cryptographic algorithms as well as on the length of the asymmetric keys (public and private) and the chosen Diffie-Hellman parameters, the quality of the generated random number and the security policy determining the key update cycle and the implementation of the security techniques. Under reasonable assumptions the provided security level is considerably high.

The security level is specifically defined through the used security parameters and the cryptographic algorithms in subclause 4.2.6.

4.2.9 Potential Damage when breached

An attacker may try to attack the fast connect key management by several ways: attacks on the network transmitted data and attacks on the crypto systems in use. When the attacker is able to break the asymmetric encryption algorithms, finds out the private keys of users and certificate authorities, and breaks the Diffie-Hellman scheme as well he will succeed in breaking the entire key management protocol and is finally able to intercept the exchanged voice encryption keys.

In the end the potential damage depends on the actual environment and the confidentiality and value of the communicated data.

4.2.10 Contents of Security Profile

A new feature in ITU-T Recommendation H.225.0 [6] version 2 is the "Fast Establishment" procedure (see figure 4). Its intent is to reduce the lengthy call establishment with many round-trips (setup/connect, capability negotiation, master-slaver determination and open logical channel) involved on the H.245 [7] call control channel. This procedure establishes four TCP connections until the receiver obtains the first media data. In Internet environments, especially for IP-telephony, this may take far too much time between initial call setup (ringing) and final call establishment (audio answer) from a user’s point of view. Therefore, fast establishment avoids the separate H.245 [7] phases and performs all those activities during the H.225.0 [6] setup and connect. Actually, the Setup and Connect messages carry in a piggy-back way the necessary H.245 [7] control information such as terminal capabilities, RTP/RTCP and H.245 [7] address information for the audio channel. The H.245 [7] phases are optional and do not have to be processed. If the receiver does not want that fast setup, it can just reject the fast setup request and continue with the standard H.245 [7] call control procedures. Moreover, both terminal can go through the H.245 [7] procedures at any time during an already established call in order to establish more logical channels.

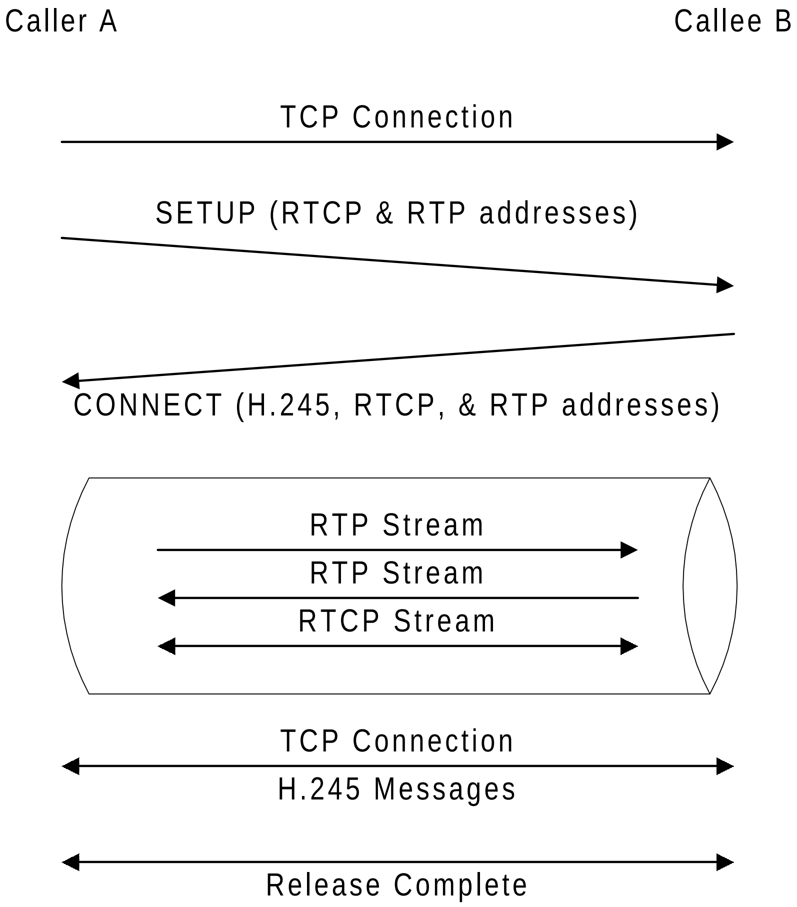

Figure 4: Fast connect

Secure fast connect has to perform authentication and key distribution with just two handshake messages. The H.245 [7] *Open Logical Channel* protocols are inherited from the H.245 [7] protocol and are piggy-backed on the two-way H.225.0 [6] Set-up/Connect messages. This inheritance allows to protect the communicated session key either with a TLS/SSL secured channel implicitly or explicitly by using asymmetric cryptography.

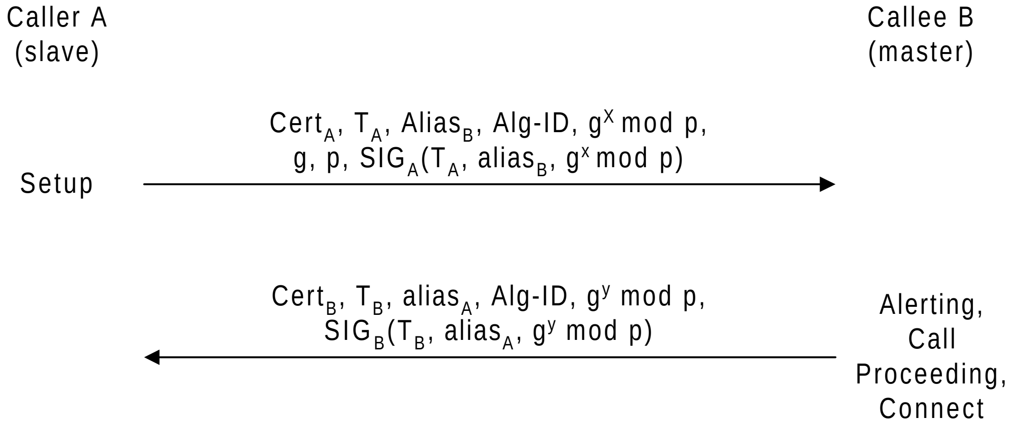
Caller A
(slave)
Callee B
(master)
Cert_A, T_A, Alias_B, Alg-ID, g^X mod p,
g, p, $\mathrm{SIG}_A(T_A$, alias_B, g^x mod p)
Setup
Cert_B, T_B, alias_A, Alg-ID, g^y mod p,
$\mathrm{SIG}_B(T_B$, alias_A, g^y mod p)
Alerting,
Call
Proceeding,
Connect

Figure 5: Authenticated Diffie-Hellman key distribution for fast connect

An authenticated Diffie-Hellman key distribution protocol is executed between caller and caller (see figure 5). After termination both entities share a common shared secret. This secret is used by the master to encrypt the media stream key conveyed within the H.245 [7] Open Logical Channel structure.

4.3 Security Profile 4.3

Security profile 4.3 is defined in [5]. That document contains the complete definition of the profile; for convenience, the following table summarizes its content.

Table 4.3: Security Profile 4.3

Security Services	**Call Functions**				
	RAS	**H.225.0 [6]**	**H.245 [7]**	**RTP**	**Other(s)**
Authentication	HMAC-SHA1 HMAC-MD5	HMAC-SHA1 HMAC-MD5	HMAC-SHA1 HMAC-MD5		
Access Control					
Non-Repudiation					
Confidentiality				56-bit DES or RC2®/168-bit Triple-DES/IPSEC	
Integrity	HMAC-SHA1 HMAC-MD5	HMAC-SHA1 HMAC-MD5	HMAC-SHA1 HMAC-MD5		

History

Document history		
V1.2.3	July 1999	Publication

ISBN 2-7437-3133-8
Dépôt légal : Juillet 1999