International Telecommunication Union

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

X.1113

(11/2007)

SERIES X: DATA NETWORKS, OPEN SYSTEM COMMUNICATIONS AND SECURITY

Telecommunication security

Guideline on user authentication mechanisms for home network services

ITU-T Recommendation X.1113

ITU-T X-SERIES RECOMMENDATIONS

DATA NETWORKS, OPEN SYSTEM COMMUNICATIONS AND SECURITY

PUBLIC DATA NETWORKS	
Services and facilities	X.1–X.19
Interfaces	X.20–X.49
Transmission, signalling and switching	X.50–X.89
Network aspects	X.90–X.149
Maintenance	X.150–X.179
Administrative arrangements	X.180–X.199
OPEN SYSTEMS INTERCONNECTION	
Model and notation	X.200–X.209
Service definitions	X.210–X.219
Connection-mode protocol specifications	X.220–X.229
Connectionless-mode protocol specifications	X.230–X.239
PICS proformas	X.240–X.259
Protocol Identification	X.260–X.269
Security Protocols	X.270–X.279
Layer Managed Objects	X.280–X.289
Conformance testing	X.290–X.299
INTERWORKING BETWEEN NETWORKS	
General	X.300–X.349
Satellite data transmission systems	X.350–X.369
IP-based networks	X.370–X.379
MESSAGE HANDLING SYSTEMS	X.400–X.499
DIRECTORY	X.500–X.599
OSI NETWORKING AND SYSTEM ASPECTS	
Networking	X.600–X.629
Efficiency	X.630–X.639
Quality of service	X.640–X.649
Naming, Addressing and Registration	X.650–X.679
Abstract Syntax Notation One (ASN.1)	X.680–X.699
OSI MANAGEMENT	
Systems Management framework and architecture	X.700–X.709
Management Communication Service and Protocol	X.710–X.719
Structure of Management Information	X.720–X.729
Management functions and ODMA functions	X.730–X.799
SECURITY	X.800–X.849
OSI APPLICATIONS	
Commitment, Concurrency and Recovery	X.850–X.859
Transaction processing	X.860–X.879
Remote operations	X.880–X.889
Generic applications of ASN.1	X.890–X.899
OPEN DISTRIBUTED PROCESSING	X.900–X.999
TELECOMMUNICATION SECURITY	**X.1000–**

For further details, please refer to the list of ITU-T Recommendations.

ITU-T Recommendation X.1113

Guideline on user authentication mechanisms for home network services

Summary

Some environments necessitate the authentication of the human user rather than a process or a device. In authenticating human users, the authentication system requires human users to prove their uniqueness. Such uniqueness is generally based on various authentication means such as something known, something possessed or some immutable characteristics for each human user.

In this Recommendation, a guideline on user authentication mechanism for home network services is provided. It also considers various security issues according to ITU-T Recommendation X.1111, which specifies the framework of security technologies for home network. Finally, the security assurance level and authentication model are defined according to authentication service scenarios.

Source

ITU-T Recommendation X.1113 was approved on 13 November 2007 by ITU-T Study Group 17 (2005-2008) under the ITU-T Recommendation A.8 procedure.

Keywords

Authenticated key exchange, client authentication, mutual authentication, security assurance level, server authentication, user authentication, user secrets.

NOTE

In this Recommendation, the expression "Administration" is used for conciseness to indicate both a telecommunication administration and a recognized operating agency.

Compliance with this Recommendation is voluntary. However, the Recommendation may contain certain mandatory provisions (to ensure e.g. interoperability or applicability) and compliance with the Recommendation is achieved when all of these mandatory provisions are met. The words "shall" or some other obligatory language such as "must" and the negative equivalents are used to express requirements. The use of such words does not suggest that compliance with the Recommendation is required of any party.

INTELLECTUAL PROPERTY RIGHTS

ITU draws attention to the possibility that the practice or implementation of this Recommendation may involve the use of a claimed Intellectual Property Right. ITU takes no position concerning the evidence, validity or applicability of claimed Intellectual Property Rights, whether asserted by ITU members or others outside of the Recommendation development process.

As of the date of approval of this Recommendation, ITU had not received notice of intellectual property, protected by patents, which may be required to implement this Recommendation. However, implementers are cautioned that this may not represent the latest information and are therefore strongly urged to consult the TSB patent database at http://www.itu.int/ITU-T/ipr/.

CONTENTS

ITU-T Recommendation X.1113

Guideline on user authentication mechanisms for home network services

1 Scope

The goal of this work is to provide a guideline for user authentication mechanisms to enable secure home network services. To this end, this Recommendation first identifies the home entities and their relationships, security threats to the home network and security components to protect the home network from such threats. Likewise, it defines security assurance level and specifies authentication models classified by service access flow to the home network. Finally, the appropriate security assurance level is applied to each authentication model.

Specifically, this Recommendation:

- defines the service architecture for the user authentication mechanisms between the home entities based on the general security framework defined in [ITU-T X.1111];
- describes the classes of home entities applicable to user authentication mechanisms;
- describes the considerations between classes of home entities for user authentication mechanisms;
- identifies the security threats and the functional requirements related to user authentication mechanisms;
- defines the security components of user authentication mechanisms;
- defines the security assurance levels for user authentication, and;
- describes the authentication models.

2 References

The following ITU-T Recommendations and other references contain provisions which, through reference in this text, constitute provisions of this Recommendation. At the time of publication, the editions indicated were valid. All Recommendations and other references are subject to revision; users of this Recommendation are therefore encouraged to investigate the possibility of applying the most recent edition of the Recommendations and other references listed below. A list of the currently valid ITU-T Recommendations is regularly published. The reference to a document within this Recommendation does not give it, as a stand-alone document, the status of a Recommendation.

[ITU-T J.190] ITU-T Recommendation J.190 (2002), *Architecture of MediaHomeNet that supports cable-based services*.

[ITU-T J.192] ITU-T Recommendation J.192 (2004), *A residential gateway to support the delivery of cable data services*.

[ITU-T X.800] ITU-T Recommendation X.800 (1991), *Security architecture for Open Systems Interconnection for CCITT applications*.

[ITU-T X.803] ITU-T Recommendation X.803 (1994), *Information technology – Open Systems Interconnection – Upper layers security model*.

[ITU-T X.810] ITU-T Recommendation X.810 (1995), *Information technology – Open Systems Interconnection – Security frameworks for open systems: Overview*.

[ITU-T X.811] ITU-T Recommendation X.811 (1995), *Information technology – Open Systems Interconnection – Security frameworks for open systems: Authentication framework*.

[ITU-T X.814] ITU-T Recommendation X.814 (1995), *Information technology – Open Systems Interconnection – Security frameworks for open systems: Confidentiality framework.*

[ITU-T X.815] ITU-T Recommendation X.815 (1995), *Information technology – Open Systems Interconnection – Security frameworks for open systems: Integrity framework.*

[ITU-T X.1111] ITU-T Recommendation X.1111 (2007), *Framework of security technologies for home network.*

[ISO 19092-1] ISO 19092-1:2006, *Financial services – Biometrics – Part 1: Security framework.*

3 Terms and definitions

3.1 Terms defined elsewhere

This Recommendation uses the following terms defined elsewhere:

3.1.1 administrator of home network: [ITU-T X.1111]

3.1.2 biometric: [ISO 19092-1]

3.1.3 biometric data: [ISO 19092-1]

3.1.4 capture: [ISO 19092-1]

3.1.5 extraction: [ISO 19092-1]

3.1.6 home access: [ITU-T J.190]

3.1.7 home application service provider: [ITU-T X.1111]

3.1.8 home bridge: [ITU-T J.190]

3.1.9 home client: [ITU-T J.190]

3.1.10 home device: [ITU-T X.1111]

3.1.11 home user: [ITU-T X.1111]

3.1.12 ID certificate: [ITU-T X.1111]

3.1.13 match: [ISO 19092-1]

3.1.14 raw biometric data: [ISO 19092-1]

3.1.15 remote terminal: [ITU-T X.1111]

3.1.16 remote user: [ITU-T X.1111]

3.1.17 security console: [ITU-T X.1111]

3.1.18 secure home gateway: [ITU-T X.1111]

3.1.19 template: [ISO 19092-1]

3.2 Terms defined in this Recommendation

This Recommendation defines the following terms:

3.2.1 authentication server: Authentication servers refer to servers that provide authentication services to users or other systems. Authentication is generally used as the basis for authorization (determining whether a privilege will be granted to a particular user or process), privacy (preventing the disclosure of information to non-participants), and non-repudiation (not being able to deny having done something that was authorized to be done based on the authentication).

3.2.2 client authentication: Client authentication models a situation in which the server wants to verify the client's identity. The client responds by sending his/her credentials such as digital certificate, shared secret or password.

3.2.3 home portal: A home portal is a functional element that provides management and translation functions to provide the user with home network services such as the control of home devices, multimedia contents, various applications, etc. In general, a home portal is a website that provides a gateway or portal to information related to various home network services. It also allows the home user to maintain and set up his/her home using the Internet. Finally, a home portal is designed to use distributed applications and different numbers and types of middleware and hardware to provide services from a number of different sources. In other words, a home portal offers information to home network services from various home entities in a unified manner.

3.2.4 identity proof: Identity proof refers to a process that a user proves who he/she is. To prove his/her identity in a digital environment, the user uses a set of security credentials such as user name and password, or certificates. For identity proof, those credentials shall include the user's ID corresponding to the user secret. In general, when the user can successfully demonstrate possession and control of a secret token to an authentication system through an authentication protocol, identity proof of the user can be achieved.

3.2.5 implicit authentication: Implicit authentication is a type of authentication without identity proof. Thus, anyone who has the correct secret can access the services.

3.2.6 mutual authentication: Mutual authentication refers to a type of authentication that enables both server authentication and client authentication.

3.2.7 policy database: A policy database refers to a list of policy needs to be created in a file. In the user authentication context, this file defines the rules required for user authentication protocol.

3.2.8 security token: This is a cryptographic key stored in a special hardware device or a general-purpose computing device.

3.2.9 server authentication: Server authentication models a situation in which the client wants to verify the server's identity. The server answers by sending its credentials such as digital certificate or shared secret.

3.2.10 session key: The session key is a temporary key used to encrypt data for the current session only. The use of session keys keeps the secret keys even more secret because they are not used directly to encrypt the data. Secret keys are used to derive the session keys using various methods that combine random numbers from either the client or server or both.

3.2.11 user database: A user database pertains to a list of users and their secrets as created in a file. For security reasons, this file should not be in clear text format. The file consists of a list of usernames and a secret for each user.

3.2.12 user secret: A user secret is a secret key generated by a user itself. A user secret is generally used for providing evidence of the user identity in an authentication mechanism.

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

AS	Application Server
CA	Certification Authority
CRL	Certificate Revocation List
EAP	Extensible Authentication Protocol
EKE	Encrypted Key Exchange

HAS	Home Application Server
HAVi	Home Audio Video interoperability
HD_A	Type A Home Device
HD_B	Type B Home Device
HD_C	Type C Home Device
ID	Identity or Identifier
IKE	Internet Key Exchange
IPsec	IP Security
Jini	Java intelligent network infrastructure
MITM	Man-in-the-Middle
RT	Remote Terminal
SA	Security Association
SAID	Security Association Identifier
SAL	Security Assurance Level
SHG	Secure Home Gateway
SRP	Simple Retransmission Protocol
TLS	Transport Layer Security
TLV	Type/Length/Value
UPnP	Universal Plug and Play
VPN	Virtual Private Network

5 Conventions

None.

6 Home network architecture

6.1 General model

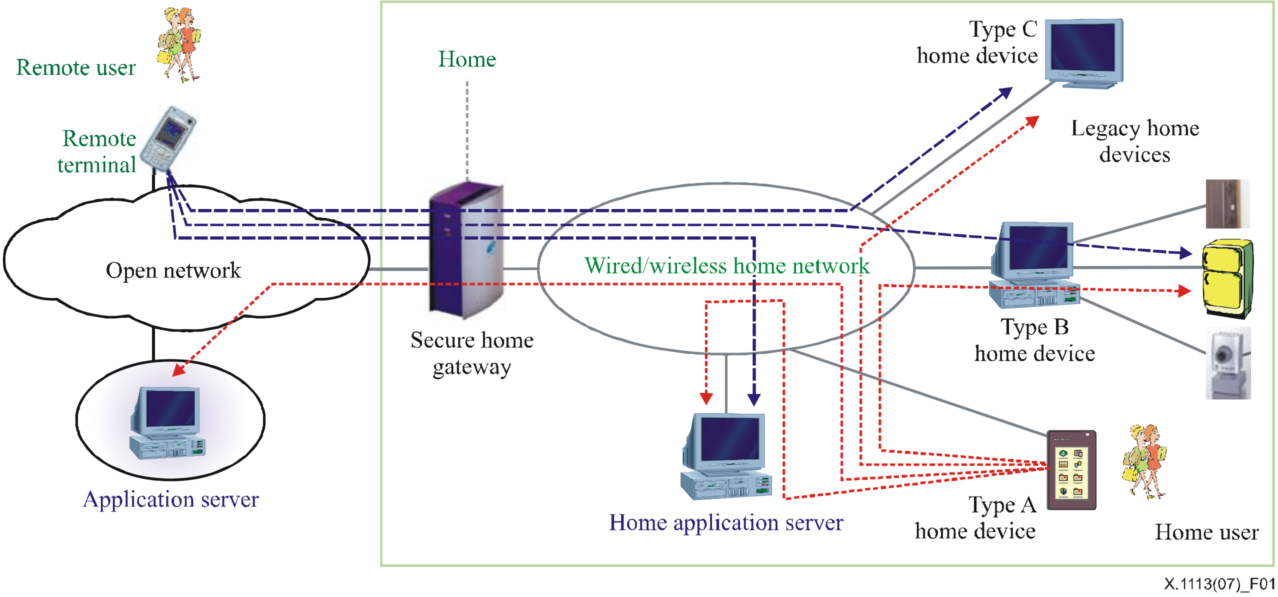

Figure 6-1 – Authentication service flow based on the general home network model for home network security

Before specifying the user authentication, a study of the home network architecture is required. The home network architecture can be well defined by entities making up the home network. This Recommendation refers to seven entities defined in [ITU-T X.1111] that specifies the framework for security technologies for the home network. One example is a home device. Home devices are divided into three categories: type A as a device with control capability; type B as a home bridge; and type C is a device providing some sort of service to the rest of the home devices. In particular, a type C device has no communication interface to the home network; as such, it is typically connected to a home network through a type B device. Since it is merely a bridge, a type B device is not an entity that is likely to participate in the user authentication procedure. This Recommendation tries to identify home network entities related to home services requiring user authentication.

Figure 6-1 shows several service flows based on a general model of a home network defined in [ITU-T X.1111]. A remote user tries to access several entities within the home, whereas a home user tries to access several entities within or outside the home. Details related to home network services are discussed in the following clause.

6.2 Service architecture for user authentication

Since home network users are general persons such as a father, a mother, their parents and their children, the home network should provide user-friendly services. Thus, this Recommendation assumes a functional element that provides a variety of home services to home network users conveniently. That is defined as a home portal. The home portal is a kind of proxy server that offers network services to allow clients to make indirect network connections to home network services. A client connects to the home portal, and then requests a connection, file or other resource available on a different server. The home portal provides the resource either by connecting to the specified server or by serving it from a cache. In some cases, the home portal may alter the client's request or the server's response for various purposes. For example, when collecting a user's commands to control the home device, the home portal may need to transform them appropriately to conform to the protocol specified for control of the corresponding device. Of course, home network users should be authenticated by the authentication system before they access the home services through the home portal. In general, a home portal is expected to reside in a secure home gateway or the home application server. For purposes of simplicity, the home portal is assumed to be a functional entity residing in the secure home gateway.

For service architecture, this Recommendation has several viewpoints for accessing home network services: remote access to the home network; access to an open network from the home; and access within home. For remote access, two cases are considered: direct access to home entities and indirect access to home entities via a home portal. On the other hand, users within the home seem to access other entities directly using a type A device (HD_A). Figure 6-2 shows the service architecture based on a general model for the home network defined in [ITU-T X.1111]. The dotted line in the figure represents that remote access is indirectly achieved by the home portal; the full line denotes direct access to the resources or home entities.

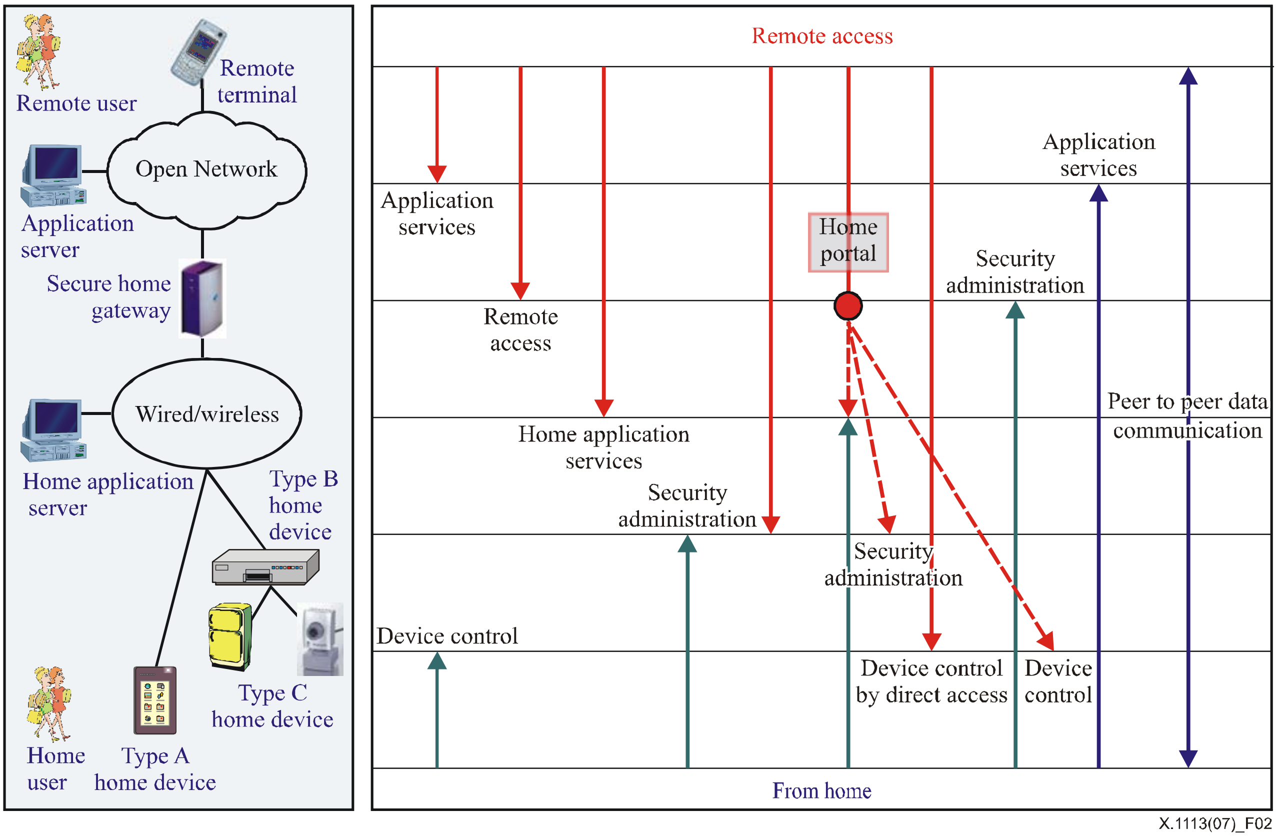

Figure 6-2 – Service architecture of a home network

7 Classification of home entities for user authentication

Many home network users use client/server systems without even realizing it. Software applications and programs are held and run on the server, and displayed on the client machine. Client-server applications allow the home network administrator to centralize information, thus facilitating maintenance and protection. Client-server applications free users from the burden of maintaining information and from the cost of allotting sufficient hard disk space to store such information. Considering these benefits, the majority of home network services are provided by client-server applications. The same is true with the user authentication mechanism; it depends on the service architecture of applications as well. In particular, user authentication mechanisms should consider much more issues such as computing power and device user interfaces, service architecture, security risk of the network, and so on. Consequently, these characteristics are helpful to decide whether a device is suitable for a client (or server) or not.

Usually a client system and a server system are two separate devices, each customized for their designed purpose. For example, an application server will often have large memory and disk space, whereas clients often offer features to support the graphical user interface of the browser such as high-end video cards and large-screen displays. In Table 7-1, the letters 'H', 'M' and 'L' mean High, Middle and Low respectively. These letters symbolize the levels of characteristics provided by each entity. Such levels are used as criteria for deciding the role of a device for user authentication. The letter 'Y' means that the corresponding role is appropriate for a specific entity in table row.

Table 7-1 – Roles and characteristics of home entities for user authentication

Home entities	**Characteristics of home entities**						**Roles for user authentication**	
	User interface	**Network availability**	**Computing power**	**Home services**	**Storage**	**Security (network)**	**Client**	**Server**
Remote terminal	H	H	M	L	M	H	Y	
Application server	L	H	H	H	H	H		Y
Secure home gateway	L	H	M	L	L	H		Y
Home application server	L	H	H	H	H	H		Y
Type A device	H	H	M	L	M	H	Y	
Type B device	L	H	L	L	L	L		Y (in the case of security console)
Type C device	M (in the case of security console)	L	L	M	L	M	Y (in the case of security console)	

As shown in Table 7-1, the home network user authentication mechanism typically runs in a client-server structure wherein the client part is deployed to the remote terminal (RT) or HD_A, as client devices, and the server part is deployed to the home application sever (HAS), secure home gateway (SHG) or application server (AS). If the computing power of home devices is allowed, such home devices can also play the role of server in the user authentication mechanism for home network services.

8 Consideration for user authentication between home entities

In this clause, this Recommendation describes the security considerations for user authentication between authentication clients and other home entities. HD_A and RT are considered as client devices for user authentication within the home and outside the home respectively.

8.1 Remote terminal (RT) and application server (AS)

For the application services from an AS, a remote user with RT accesses the AS. Since all transactions occur in the public network, authentication between RT and AS must be supported such that the sensitive data is protected by the key shared between the client and the server during running of the authentication protocol. Mutual authentication must be supported.

8.2 Remote terminal (RT) and secure home gateway (SHG)

This is a case of remote access to the home network. SHG protects the home network from various threats outside the home. Therefore, a remote user with RT must be authenticated by SHG. In particular, a security tunnel can be established between these entities through the authenticated key exchange. In addition, sensitive data during authentication procedure should be protected by the shared key between RT and SHG as in clause 8.1. Mutual authentication must be supported as well.

8.3 Remote terminal (RT) and home application server (HAS)

For direct access to HAS, a remote user with RT accesses SHG first, followed by HAS. In this case, the user authentication mechanism between RT and SHG will be the same as that in clause 8.2. Afterwards, RT will be authenticated to HAS. At this time, server authentication between RT and HAS is optional because RT has already authenticated SHG. On the other hand, in case of indirect access to HAS via the home portal, authentication between RT and HAS may be replaced by an appropriate protection mechanism such as device authentication between SHG and HAS. In this case, the home portal of SHG will provide home application services coming from HAS.

8.4 Remote terminal (RT) and type A device (HD_A)

The communication between RT and HD_A refers to the communication between a remote user and a home user. Similarly, peer-to-peer communication is characterized by the initiator playing the role of an authentication client. Thus, user authentication must provide the end-to-end security.

8.5 Remote terminal (RT) and type B device (HD_B)

In general, HD_B will be controlled by HD_A or RT. Therefore, authentication with HD_B can be applied to RT as a security console as described in [ITU-T X.1111].

8.6 Remote terminal (RT) and type C device (HD_C)

For the home device control services provided from HD_C, RT will try to access HD_C. At this time, a remote user with RT accesses SHG first, followed by HD_C. In this direct access case, the user authentication mechanism between RT and SHG will be the same as that in clause 8.2. Afterwards, RT will be authenticated to HD_C. At this time, server authentication between RT and HD_C is optional because RT has already authenticated SHG. On the other hand, in case of indirect access to HD_C via the home portal, authentication between RT and HD_C may be replaced by an appropriate protection mechanism such as device authentication between SHG and HD_C. In this case, the home portal of SHG will provide home application services coming from HD_C.

8.7 Type A device (HD_A) and application server (AS)

This is a case wherein the home user requests for services from the internal home network to the open network. For the application services from AS, a home user with HD_A accesses AS. Given the presence of AS in the public network, server authentication is required. The client authentication between them must be supported such that the sensitive data is protected by the key shared between HD_A and AS during authentication.

8.8 Type A device (HD_A) and secure home gateway (SHG)

This is a typical case of accessing the Internet or controlling SHG. Client authentication between HD_A and SHG should be supported. When the home user with HD_A is authenticated by SHG, either HD_A can be connected to the open network or it can control SHG. Server authentication is optional, however.

8.9 Type A device (HD_A) and home application server (HAS)

This is a case wherein the home user with HD_A requests for home application services within the home network. For home application services from HAS, the home user with HD_A accesses HAS. Client authentication for home application services between HD_A and HAS should be supported. Server authentication is optional.

8.10 Type A device (HD_A) and type B device (HD_B)

If security ownership of HD_B is required, HD_A plays the role as a security console as described in [ITU-T X.1111]. In this case, client authentication should be supported. Server authentication is optional, however.

8.11 Type A device (HD_A) and type C device (HD_C)

When HD_C is directly controlled by HD_A, the user authentication mechanism should be applied between these devices. In this case, client authentication should be supported. Server authentication is optional, however.

9 Security threats and security requirements for user authentication mechanisms

The home device with the biggest security needs should be within the home network's most secure zone. For such devices, the home network should provide only SHG for the provision of connectivity to the open network. From this viewpoint, this Recommendation assumes that the communication within the home is comparably secure. Therefore, security threats and security requirements in this Recommendation are mainly concerned with remote access to the home network or communication with the open network.

9.1 Security threats

- Eavesdroppers: Eavesdroppers listen passively to the authentication protocol exchange, and then attempt to learn secrets such as passwords or keys.
- Active on-line attacks: The attacker can transmit data to one or both of the parties, or block the data stream in one or both directions. The attacker may also be located between the communicating parties. In this case, the attacker can stop all or parts of the data sent by the communicating parties. This attacker can also try to take the place of the client (or server) once the authentication procedure has been performed. Without integrity checks of the received data, the server will not detect that the origin of the data is not the authenticated person. These kinds of attacks are divided into two categories.
  - Simple on-line attacks: The attacker takes the role of authentication client with a genuine authentication server:
    - On-line password-guessing attacks: An impostor attempts to guess a password in repeated log-on trials and succeeds when he/she is able to log onto a system.
    - Replay attacks: An attacker records and replays some part of a previous protocol run to the authentication server.
  - Complex on-line attacks: The attacker alters the authentication channel in some way:
    - Hijacking sessions after authentication is complete.

- Server impersonation attacks: The attacker impersonates the server and gets the client to reveal his/her secret.
- Man-in-the middle attacks: The attacker is able to read, insert and modify at will, messages between two parties without either party knowing that the link between them has been compromised. In this case, the attacker is assumed to be able to observe and intercept the messages exchanged between the two victims.

9.2 Resistance against security threats

- Eavesdropping resistance: It is impractical for an eavesdropper to learn the private key, biometric data, secret key or password, or obtain information that will allow him/her to impersonate the client. Eavesdropping-resistant protocols make it impractical for an attacker to launch an off-line attack wherein the attacker records and analyses on his/her own system an authentication protocol run for an extended period.
- On-line password-guessing resistance: It is impractical for the attacker, with a *priori* knowledge of the password, to find the password through repeated authentication attempts with guessed passwords. In this case, the authentication system requires high-entropy passwords and a limit to the number of accessing failures.
- Replay resistance: It is impractical for the attacker to realize successful authentication by recording and replaying a previous authentication message. Blocking a replay attack generally requires the use of a nonce with challenge-response technique that is never repeated with the same key.
- Hijacking resistance: This is accomplished by generating during the authentication process a session key that is subsequently used by the client and server to authenticate the transfer of all sensitive information.
- Server impersonation resistance: Even though the attacker acts the authentication server, he/she should not learn the user's secret. The attacker can bypass secure protocols by fooling the client into using another weak protocol. To block this kind of attack, the client should authenticate the server carefully.
- MITM resistance: Both parties should authenticate each other such that the undetected participation of a third party is prevented.

9.3 Security requirements

As described above, authentication mechanisms are realized by secrets such as passwords, certificates or biometrics. Authentication mechanisms can also be implemented at a variety of layers. However, none of these mechanisms have been specifically designed for the home network. The home network is known to have a diverse nature, such as heterogeneous networks as well as a variety of devices with varying capabilities. Owing to such a diverse nature in the home network, there are various requirements for security as well. Moreover, a multitude of security levels and capabilities are necessary.

In designing a user authentication mechanism, there exist various security issues to be considered. As an example, many communication environments are known to be vulnerable to MITM attack. This makes the design of the user authentication mechanism more difficult. Still the home network is a little different because its security needs to be at a different level based on home network environment. For example, SHG protects the home network from various threats that may be launched by attackers over the open network. Thus, communication within home is believed to be more secure compared to that over open network. From this viewpoint, this Recommendation specifies how the security level is applied to the home network. It requires that the appropriate authentication mechanism should be chosen by considering security risks from various home network service environments.

Secret user information must not be exposed to an attacker during the user authentication process or storage. In the case of biometrics, using biometrics as an input to a cryptographic function such as a hash function is generally difficult since measurement of biometrics does not always generate the same results; hence the difficulty in making a cryptographic protocol by challenge-response using biometrics. Consequently, a secure channel like TLS is required for authentication using biometrics between two parties. Besides, since biometric data is generally an unchangeable secret, it should be stored securely. In the case of a password, the attacker might extract password information from his eavesdropping messages because passwords have low entropy. Thus, it needs to have a strong password-based authentication protocol resistant to password guessing attack such as dictionary attack. Otherwise, a password should be transferred through a secure session like TLS. Of course, a simple password authentication protocol can also be used in more secure environments.

In certain circumstances, identity protection for user privacy is required. For example, it is very important in the home network to keep user identity a secret because the exposure of user identity may mean the exposure of important information on the home. That is to say, an attacker should neither know the identity of users involved in an ongoing protocol nor have a way of determining whether the user is at home or not.

Therefore, this Recommendation defines the following requirements for user authentication:

- Mutual authentication in case of communication over an open network or wireless network within the home.
- Support for authenticated key exchange in case of communication over an open network.
- Protection of biometric data transferred via an open network.
- Secure management of stored user secrets.
- User ID protection over an open network.
- The use of an appropriate authentication mechanism according to security risks.

10 User authentication mechanism

In this clause, the user authentication mechanism for the home network is described: its scope, components, set-up, security association, the required security services, security assurance level (SAL) and authentication model. Due to some different risks according to home network models, the security requirement should be different too. This Recommendation defines three SALs. Each level is applied to the home network authentication model classified by service access flow.

10.1 Scope of user authentication mechanism

Figure 10-1 shows the scope of user authentication mechanism for home network services. As shown in Figure 10-1, the user authentication mechanism is basically operated in the client-server environment. The communication between the client and the server will be performed over an open network or home network. First, both the client and the server have to set up the security parameters prior to the running of the user authentication protocol. Security parameters include operation methods, functions, initial values and so on. However, this Recommendation defines only the user authentication mechanism and several factors related to it, not the specific encryption, signature algorithm or their values. Client data require protection for purposes of privacy during the running of the user authentication protocol.

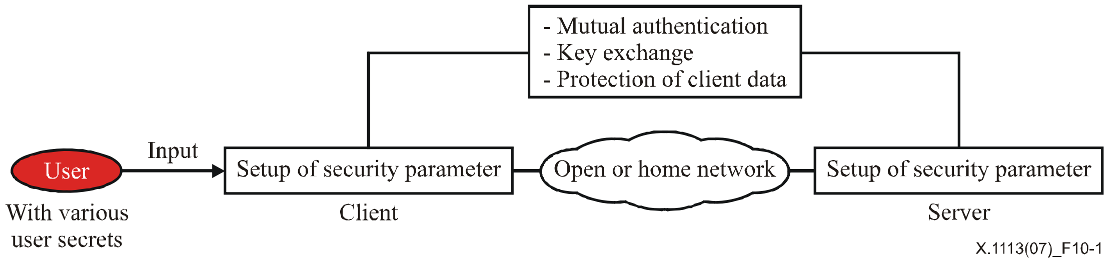
- Mutual authentication
- Key exchange
- Protection of client data
Input
User
With various user secrets
Setup of security parameter
Client
Open or home network
Setup of security parameter
Server
X.1113(07)_F10-1

Figure 10-1 – Scope of the user authentication mechanism

10.2 Security components of the user authentication mechanism

Figure 10-2 shows the security components of the user authentication mechanism for home network services. The client terminal needs to have some interfaces for the input of user secrets, whereas the server should have a database for each user. To support the various authentication means, the server's database should be able to manage various secrets corresponding to the user. The protocol modules of the client or the server should be controlled by policies configured by the user or administrator of the home network. Such policies are generally stored and managed in the policy database or configuration file. In relation to the use of certificates, the user authentication protocol should interact with both the CA and CRL servers.

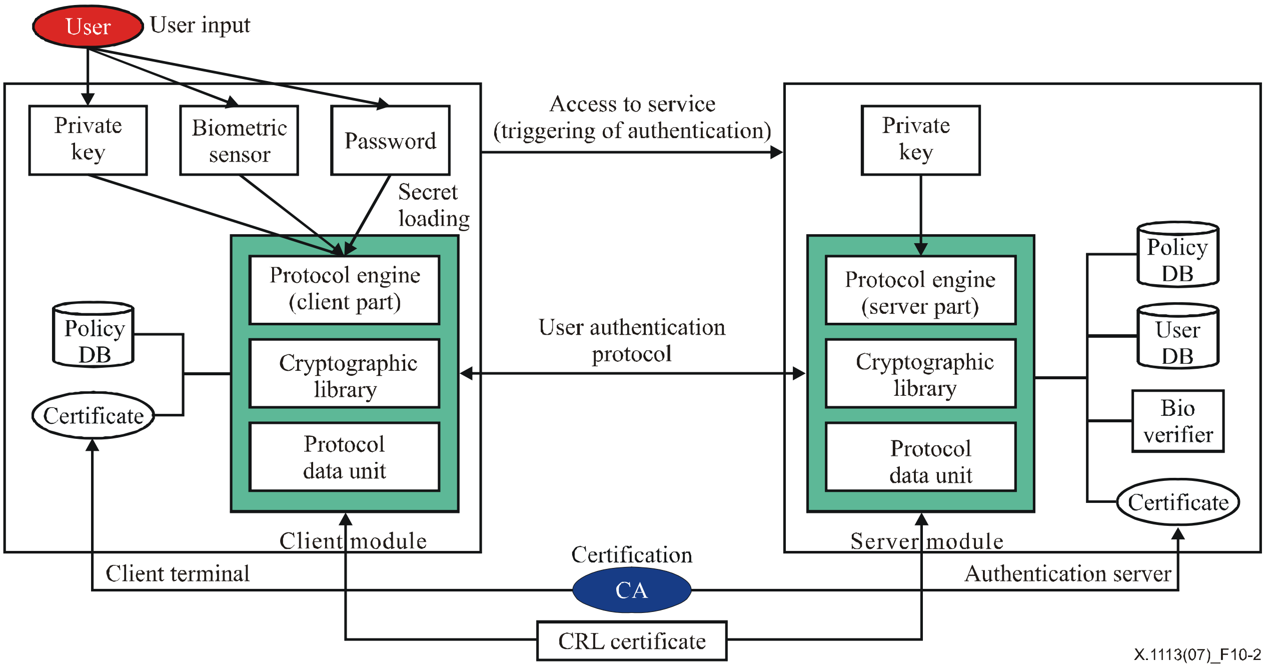

Figure 10-2 – Security components of user authentication mechanism

Table 10-1 illustrates the functionality of each security component for user authentication.

Table 10-1 – Functionality of security components for the user authentication

Components			Description
Client system	User interface for secret input	Private key	Interface related to the loading of private key
		Biometric sensor	Interface related to the sensing of biometric data
		Password	Interface related to the input of user password
	Authentication client module	Protocol engine	Control of protocol status
		Crypto library	Provision of cryptographic library related to the authentication protocol
		Protocol data unit	Generation of authentication protocol payloads
	Policy database	Policy management	Management of a set of rules related to the enforcement of SA, authentication methods, priority of methods, strategy and configuration, etc.
		Security association	Management of parameters related to the running of authentication protocol such as key size, algorithm, lifetime, etc.
	Key management module	Key generation	Generation of key materials for authenticated key exchange
		Session key management	Management of session key resulting from authentication
		Key revocation	Revocation of secrets such as private/public key, session key, password according to lifetime
		Stored key management	Loading and updating of private/public key pair and password of client
	Biometric processing module	Data collection	Collection of biometric data extracted by biometric sensor

Table 10-1 – Functionality of security components for the user authentication

Components			Description
Server system	Manager interface	User secret management	Interface related to user secrets such as password, biometric template data, etc.
		Policy management	Interface related to policies for user authentication
		Configuration management	Interface related to the configuration of user authentication
	Authentication server module	Protocol engine	Control of protocol status
		Crypto library	Provision of cryptographic library related to the authentication protocol
		Protocol data unit	Generation of authentication protocol payloads
	Policy database	Policy management	Management of a set of rules related to the enforcement of SA, authentication methods, priority of methods, strategy and configuration, etc.
		Security association management	Management of parameters related to the running of authentication protocol such as key size, algorithm, lifetime, etc.
	User database	User list	Management of user information
		User secrets	Referring to and updating of private/public key pairs, passwords and biometric data related to each user
	Key management module	Key generation	Generation of key materials for authenticated key exchange
		Session key management	Management of session key resulting from authentication
		Key revocation	Revocation of secrets such as public/private key, session key, password based on lifetime
	Biometrics verifier	Extraction	Transforming raw biometric data into the form required for matching
		Matching	Comparing the extracted biometric data with the stored biometric template
		Decision	Interpreting the results of a matching score

10.3 Set-up for the user authentication mechanism

With rapid development of the Internet and related networking technologies, client devices for the user are no longer stationary and continually wired to a static Ethernet switch port. Such kinds of devices are smart, handheld and portable. In this environment, a user can have fast and easy connection to his/her home network from his/her office, remote area, etc., anytime. However, as such devices proliferate, so do the associated security risks. As a result, securing the sensitive data on such a client device is required. For stronger security, users may use a physical token such as a card. Such a card will be used to retain private/public key pairs for the user authentication mechanism.

On the other hand, supporting various authentication means requires a client terminal to provide a user interface that will enable a user to choose his/her preferred authentication means. Otherwise, only a certain type of user secret may be used via configuring in default mode. Moreover, the authentication server needs a database that can manage various authentication means for each user. In addition, user authentication should be properly deployed for securing home network services.

As such, a set of rules can be created and laid down, specifying which users have access to which resources and under what conditions. For example, in the case of communication via wireless network in the home network, the authentication policy should indicate the use of a more secure authentication protocol. Such a secure protocol will be able to prevent eavesdropping at the very least.

10.4 Required security services for user authentication between home entities

There are many security threats and vulnerabilities in the IT world and the home network is no exception. In general, a risk refers to the potential of a threat to exploit a vulnerability and cause damage or loss to an asset. In other words, security vulnerabilities combined with security threats result in a security risk. To remove these security risks, topology of a home network also needs to be considered. For example, critical devices such as physical home security systems should not be placed in the wireless network since it may be easily accessed by many entities. In other words, the wireless network may allow an attacker to access the home network without going through a firewall or a VPN server with a security tunnel. Therefore, we carefully use the wireless network for security. On the other hand, the wired network is generally more secure than the wireless network. As such, the wired network within the home may not need some security services such as security tunnel, server authentication, ID protection, etc. Consequently, such security services may be optionally provided. For user authentication, Table 10-2 illustrates the security services to thwart various security threats and vulnerabilities related to the home network. These security services are based on the security requirements presented in clause 9.3. As shown in Table 10-2, the letter 'Y' means that the corresponding security service shall be constructed for a specific entity or relationship, and the letter 'O' means that the corresponding security service is optionally provided for a specific entity or relationship. In the case of remote access, server authentication for other entities such as HAS, HD_A, HD_B and HD_C is not necessary because, for that, SHG is required. Key exchange is the same as that in the case above. In case HD_B is a mere bridge, the protection of the stored user secret of HD_B is optional, not necessary. That is why HD_B may have no relation to the security of user authentication in such a case. Table 10-2 is basically consistent with [ITU-T X.1111].

Table 10-2 – The required security services for user authentication between home entities or their relationships

Home entities \ Security functions		Authentication		Key exchange	Protection of stored user secret	ID protection
		Server auth.	Client auth.			
Stored data	RT				Y	
	HD_A				Y	
	AS				Y	
	SHG				Y	
	HAS				Y	
	HD_B				O	
	HD_C				Y	

Table 10-2 – The required security services for user authentication between home entities or their relationships

Security functions Home entities			Authentication		Key exchange	Protection of stored user secret	ID protection
			Server auth.	Client auth.			
Communication data	Remote access over open network	Between RT and AS	Y	Y	Y		Y
		Between RT and SHG	Y	Y	Y		Y
		Between RT and HAS	O	Y	O		Y
		Between RT and HD_A	O	Y	O		Y
		Between RT and HD_B	O	Y	O		Y
		Between RT and HD_C	O	Y	O		Y
	Within home	Between HD_A and AS	Y	Y	Y		Y
		Between HD_A and SHG	O	Y	O		O
		Between HD_A and HAS	O	Y	O		O
		Between HD_A and HD_B	O	Y	O		O
		Between HD_A and HD_C	O	Y	O		O

10.5 Security association

Running the authentication protocol requires defining and negotiation security associations between participants for authentication. Security association (SA) refers to the set of security information shared by authentication entities to establish a secure transmission session. It involves the negotiation of the method for authentication and encryption as well as the exchange of secret keys. In general, all these security data are grouped logically for convenience. The logical group itself is a security association. Each SA has its own ID called a security association identifier (SAID). Authentication entities share SAID and derive all the security parameters related to SAID. The negotiation of SAs is usually achieved using the predefined SAs or priority of SA proposal based on SAID. For the establishment of SAs, authentication mechanisms should generally define the policies in their SA-related database. Usually, the negotiation of SAs precedes the running of the actual authentication protocol. These SAs can also be described as a cipher suite and a protocol suite as in TLS. On the other hand, IPsec negotiates bidirectional SAs through IKE. Appendix I outlines the classification and attributes of SA for authentication.

10.6 Security assurance level

To provide the required security assurance for home network service, this Recommendation defines security assurance levels (that is SALs) in relation to the authentication mechanism. The basic rules for defining SALs include taking into account the characteristics of the home network, such as the limitation of device performance, architecture of the home network, kind of networks, etc. For example, even though communication within the home is believed to be more secure than that over an open network due to the protection of SHG, there is a little difference as to whether a network within the home is a wireless network or a wired network. For security of the home network, a wireless home network should be just as secure as the wired home network. As such, any attack by an eavesdropper should be blocked in the wireless network. Moreover, most of the home appliances exhibit limited performance. Thus, the appropriate security mechanism, considering the limitation related to device performance, is required by home appliances.

In this Recommendation, SAL consists of three levels and states specific technical requirements for each of the three levels at the very least. Level 1 is the lowest assurance, and level 3 is the highest assurance. Table 10-3 shows the defined SALs for the authentication mechanism.

Table 10-3 – Security assurance levels for authentication mechanism

Security assurance levels	**Level 1**	**Level 2**	**Level 3**
Minimum security requirements	– No identity proof – Client authentication (implicit authentication) – Single factor authentication – Read-protection and write-protection of stored user secrets	– Identity proof – Mutual authentication – Single factor authentication – Use of one-way hash, encryption or salt for storing user secrets	– Identity proof – Mutual authentication – Key exchange – Use of one-way hash, encryption or salt for storing user secrets – Two-factor authentication – The protection of sensitive or subsequent data by key shared during authentication protocol

10.6.1 Level 1

The target of Level 1 requirements is the protection of a wired network within the home. Since there is a protection by SHG, level 1 allows a wide range of authentication technologies. It specifies the requirements for security at a minimum level. Thus, it does not require the identity proof, the mutual authentication and the two-factor authentication, and so on.

Since there is no identity proof requirement at this level, anyone who has the correct secret is able to access home network services. In other words, level 1 provides implicit authentication that the correct user will be accessing protected data. It also means that the server authentication is not required.

Besides, level 1 does not require cryptographic methods that block off-line attack by eavesdroppers. A kind of password challenge-response protocol satisfies requirement of this level. In terms of storing user secrets, level 1 does not require any method such as cryptographic processing. The most obvious approach is for the system to store user secrets in clear text format in a system file, and then the system shall provide both read-protection and write-protection.

10.6.2 Level 2

The target of level 2 requirements is the protection of a wireless network within the home. In general, a wireless network enables the attacker to eavesdrop the communication data. Thus, cryptographic methods are required additionally to prevent eavesdroppers. Moreover, this level requires mutual authentication to protect the home network from compromise by server impersonators over a wireless network.

The user secret should be stored in encrypted or one-way hashed form. For example, passwords should be concatenated to a salt and then hashed with an approved algorithm.

10.6.3 Level 3

The target of level 3 requirements is to protect communication over an open network. This level requires two-factor authentication wherein users need to employ passwords or biometrics to activate the key. It also requires cryptographic strength mechanisms that prevent compromising primary authentication secrets due to eavesdropping, replay, on-line guessing, server impersonation and MITM. Besides, level 3 authentication also requires key exchange to allow the entire session, or much of it, to be cryptographically authenticated. How to store the user secrets is the same as those of level 2. In conclusion, level 3 is to provide the highest authentication assurance.

10.7 Protection level of SALs

This Recommendation describes several security threats and resistance against them in clauses 9.1 and 9.2. These security threats need to be managed efficiently according to the characteristics of the home network. For such management, this Recommendation defines three security assurance levels. Each SAL keeps a certain protection level and resists threats. Table 10-4 shows the resistance level against threats according to SAL.

Table 10-4 – Relationship between threat resistance and SALs

Security levels Type of resistance	Level 1	Level 2	Level 3
On-line guessing resistance	√	√	√
Replay resistance	√	√	√
Eavesdropping resistance		√	√
Server impersonation resistance		√	√
MITM resistance			√
Session hijacking resistance			√

10.8 Authentication models

This clause defines three models for user authentication in the home network:

1) remote access model;
2) authentication model for communication within the home, and;
3) access model from home to open network.

10.8.1 Remote access model

For remote access to the home network, the user first needs to be authenticated by SHG. The user tries to access home network services via the home portal in SHG. SHG then requires the authentication of the user. At this time, the authentication mechanism requires a higher level of security assurance, such as level 3, since the authentication process is performed over an open network. These levels can provide a security tunnel via the key shared by authentication between RT and SHG. If the section between SHG and the back end such as HD and HAS is protected by device authentication instead of user authentication, level 1 or level 2 user authentication may not be required. In this case, the user authentication will run between RT and SHG, with SHG transferring the user's command to HD or HAS under the protection of device authentication between RT and HD or HAS. In most cases of home automation or entertainment, these commands can generally be transferred by middle-ware protocol such as UPnP, Jini and HAVi. Therefore, the end of authentication protocol for remote access will actually be the home portal within SHG. Figure 10-3 shows how authentication levels are applied to home entities in the case of remote access.

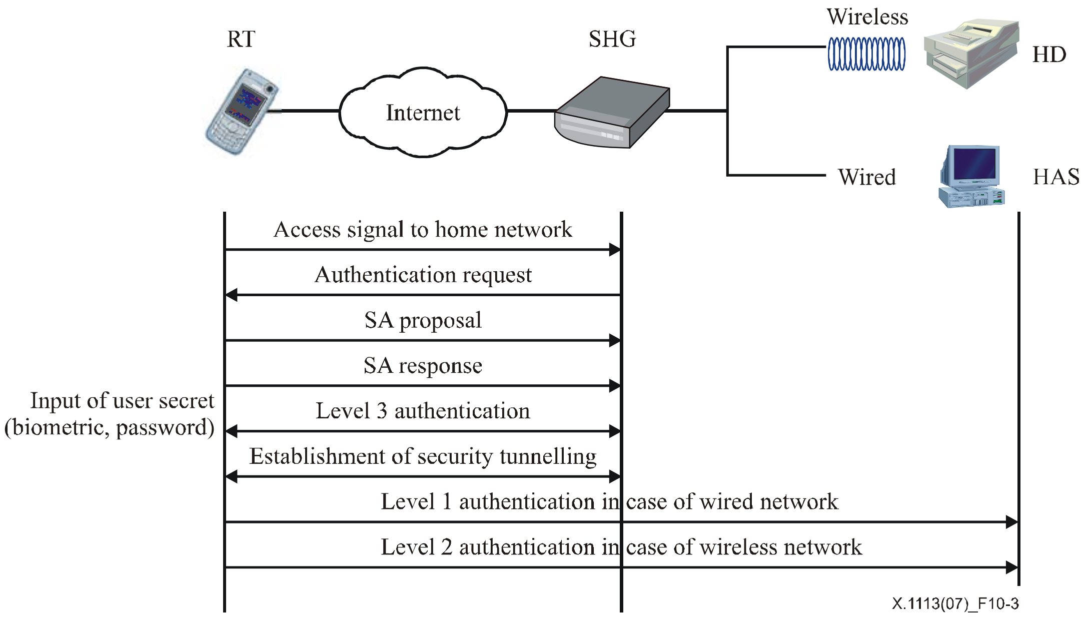
RT
SHG
Wireless
HD
Internet
Wired
HAS
Access signal to home network
Authentication request
SA proposal
SA response
Input of user secret (biometric, password)
Level 3 authentication
Establishment of security tunnelling
Level 1 authentication in case of wired network
Level 2 authentication in case of wireless network
X.1113(07)_F10-3

Figure 10-3 – Authentication model for remote access

10.8.2 Home communication model

Home communication suggests that all instances of communication occur at home. The user will use HD_A to access HD_C or HAS. For this scenario, security threats are generally not serious compared to the open network. In this case, the authentication system requires level 1 or level 2 authentication. Figure 10-4 shows how authentication levels are applied to home entities in the case of the home communication model.

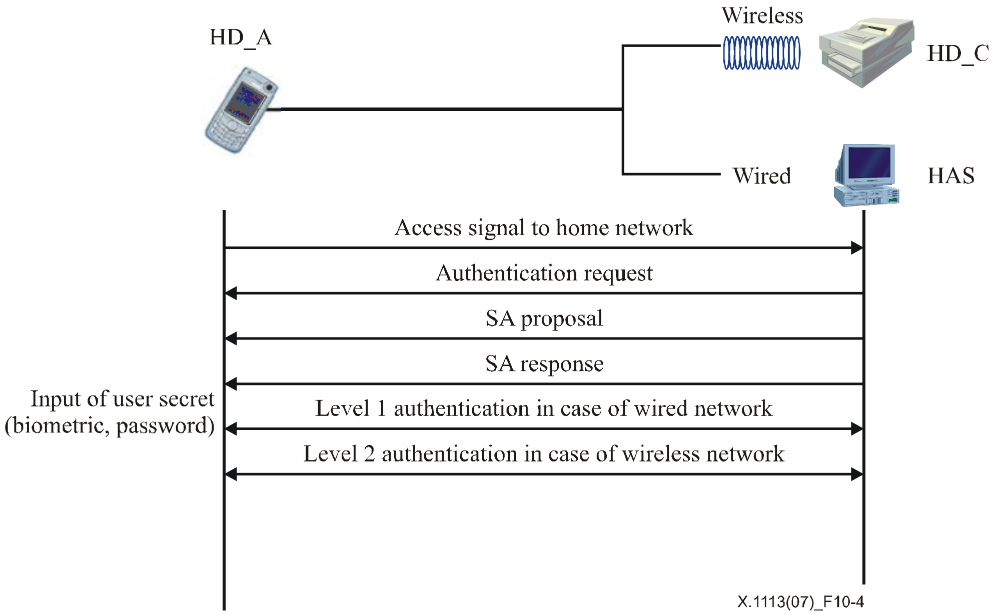
HD_A
Wireless
HD_C
Wired
HAS
Access signal to home network
Authentication request
SA proposal
SA response
Input of user secret (biometric, password)
Level 1 authentication in case of wired network
Level 2 authentication in case of wireless network
X.1113(07)_F10-4

Figure 10-4 – Authentication model for home communication

10.8.3 Home-to-open communication model

In home-to-open communication, the user within the home wants to access the open network. In this case, the user will use HD_A to access AS. For this scenario, security threats are comparably more serious, thus requiring level 3 authentication. Figure 10-5 shows how authentication levels are applied to home entities in the case of the home-to-open communication model.

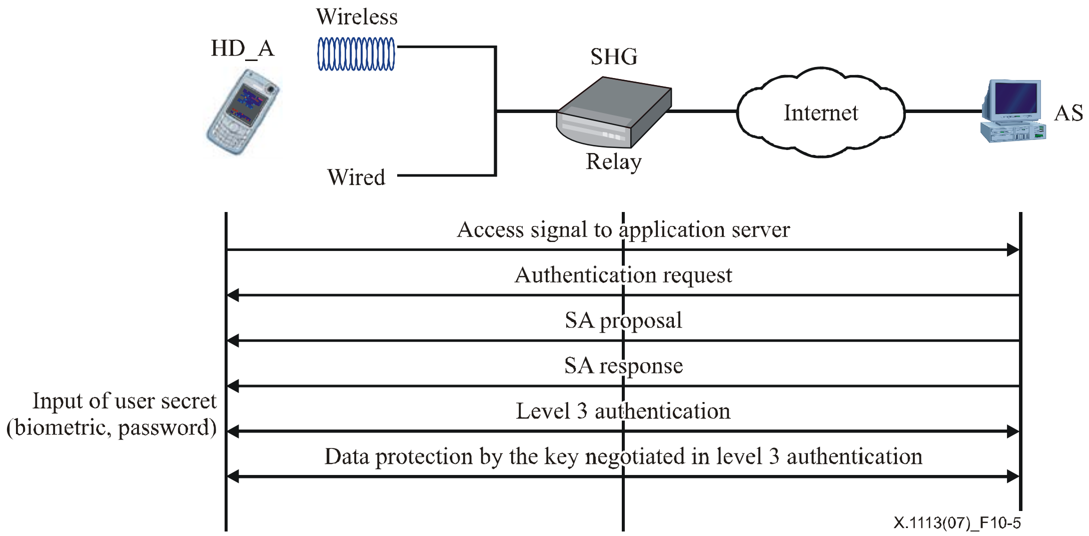

Figure 10-5 – Authentication model for home-to-open network communication

10.9 Relationship between SAL and home network security requirement

Table 10-5 illustrates the relationship between the home network security requirement and SALs. The letters 'R', 'H' and 'H-O' denote "remote access", "communication within the home" and "communication from home-to-open network" respectively. For example, the case of key exchange in the R column of the table requires a level 3 authentication mechanism. The ID protection column has a slightly different meaning, i.e., ID protection is achieved via security tunnelling accompanied by level 3 authentication. On the other hand, considering the difference in risk between the wired and wireless networks, as shown in the 'H' column, level 1 authentication is applied to the wired network, and level 2 authentication to the wireless network.

Table 10-5 – The relationship between SAL and home network security requirement

Security Requirement	Authentication						Key exchange			Protection of user secret			ID protection		
	Client auth.			Server auth.											
SAL	R	H	H-O	R	H	H-O	R	H	H-O	R	H	H-O	R	H	H-O
Level 1		√ (wired)									√ (wired)				
Level 2		√ (wireless)			√ (wireless)						√ (wireless)				
Level 3	√		√	√		√	√		√	√		√	Security Tunnelling		Security Tunnelling

Appendix I

Security association used in IPsec

(This appendix does not form an integral part of this Recommendation)

In IPsec, SA refers to the relationship between authentication entities. Specifically, it describes how the entities will utilize security services to communicate securely. This relationship is represented by a set of information that can be considered as a contract between the entities. Such information must be agreed upon and shared between all entities. Establishing such a relationship requires SA attributes. SA attributes are inclusive of, but not limited to authentication methods, cryptographic algorithms, algorithm modes, SA lifetimes and group types. The authentication protocol and corresponding SA attributes vary according to the authentication means. Therefore, the use of various authentication means requires negotiating or predefining the SA attributes for each of the authentication protocols. Of course, an authentication protocol with a predefined SA can also be applied between authentication entities. In this case, the negotiation of SA is not required. Table I.1 shows SA types and their attributes.

Table I.1 – Security association

Classification of SA		SA attributes	Description
Transforms	Encryption algorithm	DES_IV64, DES, 3DES, RC5, IDEA, CAST, BLOWFISH, 3IDEA, DES_IV32, AES_CBC, AES_CTR, SEED	
	Pseudo-random function	HMAC_MD5, HMAC_SHA1, HMAC_TIGER, AES128_XCBC	
	Integrity algorithm	HMAC_MD5_96, HMAC_SHA1_96, DES_MAC, KPDK_MD5, AES_XCBC_96	
	Diffie-Hellman group type	768-bit MODP, 1024-bit MODP, elliptic curve group over GF(p), elliptic curve group over GF(2^N)	Use of secure prime corresponding to bit size
Identification		IPV4_ADDR, FQDN, RFC822_ADDR, IPV6_ADDR, DER_ASN1_DN, DER_ASN1_GN, KEY_ID	Dependent on the object of identification
Certificate encoding		PKCS #7 wrapped X.509 certificate, PGP certificate, DNS signed key, X.509 certificate – Signature, Kerberos token, certificate revocation list (CRL), authority revocation list (ARL), SPKI certificate, X.509 certificate – Attribute	Need to use appropriate certificate according to the object of authentication service
Authentication method		RSA digital signature, shared key message integrity code, DSS digital signature	Dependent on the design of authentication method
SA lifetime		Seconds or kilobytes	Actual length defined in TLV format

Appendix II

Existing authentication mechanisms

(This appendix does not form an integral part of this Recommendation)

Some information is necessary to authenticate the human user. Such information is generally called a user secret which is a secret key owned by users. This secret key is used for providing evidence of the user's identity in the authentication protocol. This can be done because the secret key is unique for each user. Such uniqueness is generally based on something known, something possessed or some immutable characteristic for each human user. Examples include passwords, certificates, biometrics, etc.

As the strongest form in a common authentication system in general, the certificate for authentication has been widely used in protecting VPN connections or e-banking services. For example, certificate-based authentication can be used for secure tunnelling protocol over IPSec-based VPN connections and EAP with the smartcard or other certificate EAP type, also known as EAP-TLS. An advantage of EAP is that it supports multiple authentication mechanisms without the need to pre-negotiate a particular one. Thus, EAP can be a good solution for the use of various authentication means as a kind of container to include different authentication protocols, it can be a good solution for the use of various authentication means.

As a standard document on the authentication mechanism using biometric data, [ISO 19092-1] specifies the minimum security requirements for effective management of biometric data. Within the scope of [ISO 19092-1], the following topics are addressed: security for the collection, distribution and processing of biometric data, encompassing data integrity, authenticity and non-repudiation; management of biometric data across its life cycle, consisting of enrolment, transmission and storage, verification, identification, and termination processes; use of biometric technology, including one-to-one and one-to-many matching, for the identification and authentication of banking customers and employees; application of biometric technology for internal and external, as well as logical and physical access control; encapsulation of biometric data; techniques for the secure transmission and storage of biometric data; security of the physical hardware used throughout the biometric data life cycle; techniques for integrity and privacy protection of biometric data. However [ISO 19092-1] does not define a specific key distribution scheme to protect biometric data between the client and the server. Therefore, the user authentication mechanism based on biometric data must have a method to share a key to protect it.

On the other hand, the low entropy of a password makes it vulnerable to password-guessing attacks. Some password authentication protocols such as EAP-MD5 are actually not suitable for public Ethernets or wireless LANs because attackers can easily sniff identities and password hashes of nodes, or masquerade as access points to trick nodes into authenticating with them instead of the real run. In 1992, EKE was introduced as a new strong password-based protocol that allows both parties to share a common key by using only a password. Later, similar schemes such as A-EKE, SPEKE and SRP have followed. These strong password-based protocols are not a limited scheme compared to the public key scheme using certificates. Those provide very strong authentication without the use of certificates or a long secret key. Users can accomplish strong authentication and key exchange by using only passwords. These strong password-based protocols are designed to be immune to password-guessing attacks such as dictionary attacks, where the dictionary means a list of probable passwords.

Bibliography

[b-ITU-T X.509] ITU-T Recommendation X.509 (2005), *Information technology – Open Systems Interconnection – The Directory: Public-key and attribute certificate framework*.

[b-IETF RFC 2119] IETF RFC 2119 (1997), *Key words for use in RFCs to Indicate Requirement Levels*, <http://www.ietf.org/rfc/rfc2119.txt>.

[b-IETF RFC 2246] IETF RFC 2246 (1999), *The TLS Protocol Version 1.0*, <http://www.ietf.org/rfc/rfc2246.txt>.

[b-IETF RFC 2401] IETF RFC 2401 (1998), *Security Architecture for the Internet Protocol*, <http://www.ietf.org/rfc/rfc2401.txt>.

[b-IETF RFC 2408] IETF RFC 2408 (1998), *The Internet Security Association and Key Management Protocol* (*ISAKMP*), <http://www.ietf.org/rfc/rfc2408.txt>.

[b-IETF RFC 2409] IETF RFC 2409 (1998), *The Internet Key Exchange (IKE)*, <http://www.ietf.org/rfc/rfc2409.txt>.

[b-IETF RFC 3546] IETF RFC 3546 (2003), *Transport Layer Security (TLS) Extensions*, <http://www.ietf.org/rfc/rfc3546.txt>.

[b-IETF RFC 3748] IETF RFC 3748 (2004), *Extensible Authentication Protocol (EAP)*. <http://www.ietf.org/rfc/rfc3748.txt>.

[b-IETF RFC 4306] IETF RFC 4306 (2005), *Internet Key Exchange (IKEv2) Protocol*, <http://www.ietf.org/rfc/rfc4306.txt>.

[b-Bellovin] Bellovin S. and Merritt M. (1992) *Encrypted Key Exchange: Password-Based Protocols Secure Against Dictionary Attacks*, Proceedings IEEE Computer Society Symposium on Research in Security and Privacy, pp. 72-84.

[b-HAVi] HAVi Organization, HAVi SPECIFICATION Version 1.1, <http://www.havi.org/technical/specifications.asp>.

[b-Jablon] Jablon D.P (1996), *Strong Password-Only Authenticated Key Exchange*, ACM Computer Communications Review, Vol. 26, No. 5, October, pp. 5-26.

[b-Jini] Jini Technology, Category: Jini Specifications, <http://www.jini.org/wiki/Category:Jini_Specifications>.

[b-NIST 800-63] NIST Special Publication 800-63 Version 1.0.2 (2006), *Electronic Authentication Guideline*, <http://csrc.nist.gov/publications/nistpubs/800-63/sp800-63v1_0_2.pdf>.

[b-UPnP] UPnP Forum (2003), *Device Security and Security Console V1.0,* <http://www.upnp.org/standardizeddcps/security.asp>.

[b-Wu] Wu T., *The Secure Remote Password Protocol*, Internet Society Symposium on Network and Distributed System Security, <http://srp.stanford.edu/ndss.htm/>.

SERIES OF ITU-T RECOMMENDATIONS

Series A	Organization of the work of ITU-T
Series D	General tariff principles
Series E	Overall network operation, telephone service, service operation and human factors
Series F	Non-telephone telecommunication services
Series G	Transmission systems and media, digital systems and networks
Series H	Audiovisual and multimedia systems
Series I	Integrated services digital network
Series J	Cable networks and transmission of television, sound programme and other multimedia signals
Series K	Protection against interference
Series L	Construction, installation and protection of cables and other elements of outside plant
Series M	Telecommunication management, including TMN and network maintenance
Series N	Maintenance: international sound programme and television transmission circuits
Series O	Specifications of measuring equipment
Series P	Telephone transmission quality, telephone installations, local line networks
Series Q	Switching and signalling
Series R	Telegraph transmission
Series S	Telegraph services terminal equipment
Series T	Terminals for telematic services
Series U	Telegraph switching
Series V	Data communication over the telephone network
Series X	**Data networks, open system communications and security**
Series Y	Global information infrastructure, Internet protocol aspects and next-generation networks
Series Z	Languages and general software aspects for telecommunication systems

Printed in Switzerland
Geneva, 2008