International Telecommunication Union

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

X.1114

(11/2008)

SERIES X: DATA NETWORKS, OPEN SYSTEM COMMUNICATIONS AND SECURITY

Telecommunication security

Authorization framework for home networks

Recommendation ITU-T X.1114

ITU-T X-SERIES RECOMMENDATIONS

DATA NETWORKS, OPEN SYSTEM COMMUNICATIONS AND SECURITY

PUBLIC DATA NETWORKS	X.1–X.199
OPEN SYSTEMS INTERCONNECTION	X.200–X.299
INTERWORKING BETWEEN NETWORKS	X.300–X.399
MESSAGE HANDLING SYSTEMS	X.400–X.499
DIRECTORY	X.500–X.599
OSI NETWORKING AND SYSTEM ASPECTS	X.600–X.699
OSI MANAGEMENT	X.700–X.799
SECURITY	X.800–X.849
OSI APPLICATIONS	X.850–X.899
OPEN DISTRIBUTED PROCESSING	X.900–X.999
INFORMATION AND NETWORK SECURITY	
General security aspects	X.1000–X.1029
Network security	X.1030–X.1049
Security management	X.1050–X.1069
Telebiometrics	X.1080–X.1099
SECURE APPLICATIONS AND SERVICES	
Multicast security	X.1100–X.1109
Home network security	**X.1110–X.1119**
Mobile security	X.1120–X.1139
Web security	X.1140–X.1149
Security protocols	X.1150–X.1159
Peer-to-peer security	X.1160–X.1169
Networked ID security	X.1170–X.1179
IPTV security	X.1180–X.1199
CYBERSPACE SECURITY	
Cybersecurity	X.1200–X.1229
Countering spam	X.1230–X.1249
Identity management	X.1250–X.1279
SECURE APPLICATIONS AND SERVICES	
Emergency communications	X.1300–X.1309
Ubiquitous sensor network security	X.1310–X.1339

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

Recommendation ITU-T X.1114

Authorization framework for home networks

Summary

Alongside the wide deployment of home network services and the increasing development of a variety of technologies for telecommunication, contents provision, remote control, etc., concerns over the security of the home network are increasing. As a basic security function for protecting the home network, authorization ensures that only an authorized entity (including user, device) can access the home network resources. Recommendation ITU-T X.1114 describes the security threats and authorization requirements for the home network, identifies the authorization entities and methods, and develops authorization models and authorization modes for guaranteeing the security of the home network.

Source

Recommendation ITU-T X.1114 was approved on 13 November 2008 by ITU-T Study Group 17 (2009-2012) under Recommendation ITU-T A.8 procedure.

Keywords

Access control, access control list, authorization framework, authorization mode, authorization model, role-based access control.

FOREWORD

The International Telecommunication Union (ITU) is the United Nations specialized agency in the field of telecommunications, information and communication technologies (ICTs). The ITU Telecommunication Standardization Sector (ITU-T) is a permanent organ of ITU. ITU-T is responsible for studying technical, operating and tariff questions and issuing Recommendations on them with a view to standardizing telecommunications on a worldwide basis.

The World Telecommunication Standardization Assembly (WTSA), which meets every four years, establishes the topics for study by the ITU-T study groups which, in turn, produce Recommendations on these topics.

The approval of ITU-T Recommendations is covered by the procedure laid down in WTSA Resolution 1.

In some areas of information technology which fall within ITU-T's purview, the necessary standards are prepared on a collaborative basis with ISO and IEC.

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

Recommendation ITU-T X.1114

Authorization framework for home networks

1 Scope

This Recommendation describes an authorization framework for home networks, which includes a number of home network resources such as home network users, three types of home devices, the service servers, the services provided, a variety of applications and the heterogeneous network protocols and middleware for communication and service development.

The scope of this Recommendation covers the authorization framework for home networks as described below:

– Security threats in authorization for the home network.

– Authorization requirements for the home network.

– Relationship between security threats and authorization requirements.

– Classification of authorization entities.

– Authorization model for the home network.

– Authorization mode required while enforcing access control.

The following items are also described in the appendices:

– Authorization methods for the home network.

– Conceptual policy model used in authorizing the home network.

– Service scenario of the authorization mode.

– Use case of the authorization model.

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 X.1111] Recommendation ITU-T X.1111 (2007), *Framework of security technologies for home network.*
<http://www.itu.int/rec/T-REC-X.1111>

3 Terms and definitions

3.1 Terms defined elsewhere

This Recommendation uses the following terms defined elsewhere:

3.1.1 access control [b-ITU-T X.800]: The prevention of unauthorized use of a resource, including the prevention of use of a resource in an unauthorized manner.

3.1.2 access control list [b-ITU-T X.800]: A list of entities, together with their access rights, which are authorized to have access to a resource.

3.1.3 application server [b-ITU-T X.1121]: An entity that connects to an open network for data communication with mobile terminals.

3.1.4 authentication [b-ITU-T X.811]: The provision of assurance of the claimed identity of an entity.

NOTE – The usage of the word identity is made with the understanding that, in the context of telecommunications, it is an identifier or set of identifiers that is trusted, meaning it is considered to be reliable for the purposes of a particular situation to represent a network element, network terminal equipment, or user, after the completion of a validation process. As the term is used here, one cannot conclude that trusted identifiers constitute positive validation of a person.

3.1.5 authorization [b-ITU-T X.800]: The granting of rights, which includes the granting of access based on access rights.

3.1.6 availability [b-ITU-T X.800]: The property of being accessible and useable upon demand by an authorized entity.

3.1.7 capability [b-ITU-T X.800]: A token used as an identifier for a resource such that possession of the token confers access rights for the resource.

3.1.8 confidentiality [b-ITU-T X.800]: The property that information is not made available or disclosed to unauthorized individuals, entities or processes.

3.1.9 data integrity [b-ITU-T X.800]: The property that data has not been altered or destroyed in an unauthorized manner.

3.1.10 decision [b-ITU-T X.1142]: The result of evaluating a rule, policy or policy set.

3.1.11 identification [b-NIST SP800-47]: The process of verifying the identity of user, process or device, usually as a prerequisite for granting access to resources in an IT system.

3.1.12 identifier [b-ITU-T Y.2091]: A series of digits, characters and symbols or any other form of data used to identify subscriber(s), user(s), network element(s), function(s), network entity(ies) providing services/applications, or other entities (e.g., physical or logical objects). Identifiers can be used for registration or authorization. They can be either public to all networks, shared between a limited number of networks or private to a specific network (private identifiers are normally not disclosed to third parties).

3.1.13 password [b-ITU-T X.800]: Confidential authentication information, usually composed of a string of characters.

3.1.14 permission [b-ITU-T X.1142]: The ability or right to perform some action on some resource, possibly only under certain specified conditions.

3.1.15 policy (security policy) [b-ITU-T X.800]: The set of criteria for the provision of security services.

3.1.16 privacy [b-ITU-T X.800]: The right of individuals to control or influence what information related to them may be collected and stored and by whom, and to whom that information may be disclosed.

3.1.17 resource [b-ITU-T X.1142]: Data, service or system component.

3.1.18 role [b-ITU-T X.1142]: A job function within the context of an organization that has associated semantics regarding the authority and responsibility conferred on the user assigned to the role.

3.1.19 role based access control (RBAC) [b-ITU-T X.1142]: A model for controlling access to resources where permitted actions on resources are identified with roles rather than with individual subject identities.

3.1.20 rule [b-ITU-T X.1142]: A target, an effect and a condition, a component of a policy.

3.1.21 subject [b-ITU-T X.1142]: An actor whose attributes may be referenced by a predicate.

3.1.22 target [b-ITU-T X.1142]: The set of decision requests, identified by definitions for resource, subject and action, that a rule, policy or policy set is intended to evaluate.

3.1.23 threat [b-ITU-T X.800]: A potential violation of security.

3.2 Terms defined in this Recommendation

This Recommendation defines the following terms:

3.2.1 authorization administrator: A person who is responsible for the management of policy used in authorization.

3.2.2 authorization server: An entity that is in charge of authorizing a home subject by controlling access from the home subject to a home resource.

3.2.3 home resource: A resource that provides home network services based on the decision by the authorization server.

3.2.4 home subject: A home user or home device that has a profile, i.e., an identifier, that wants to access the home resource within the home network.

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

ACL Access Control List

AS Authorization Server

CA Certificate Authority

CCTV Closed-Circuit Television

DAC Discretionary Access Control

HR Home Resource

HS Home Subject

MAC Mandatory Access Control

PDP Policy Decision Point

PEP Policy Enforcement Point

RBAC Role Based Access Control

URI Uniform Resource Identifier

URL Uniform Resource Locator

5 Conventions

None.

6 Authorization for the home network

The purpose of authorization for the home network is to protect the home network from illegal or unnecessary access by restricting the privilege of the accessing entity and controlling access even though the entity has been successfully authenticated. The accessing entity includes devices, users and other resources, depending on the application. When a certain entity is going to use the home network service, the authorization function makes a decision as to whether to permit access or not based on the authorization policy managed by the authorization administrator. The decision can be

made by the service provider itself, a trusted third party responsible for the authorization, or the owner of the accessed resource after an appropriate instant confirmation procedure, e.g., personal allowance or person-to-person conversation.

The authorization database includes the policy used for access control consisting of a set of records wherein each record must implicitly contain the following information:

– Subject's information, which uniquely identifies an accessing entity or a set of entities.
– Resource's information, which uniquely identifies the accessed entity or a set of entities.
– Information on the permission of the subject: May be either an allowance or a rejection.

The identifier of the HS is supposed to be provided by a corresponding authenticator, the subjects themselves or other trusted functions and must be addressed in the authorization policy.

The identifier of the HR is likely to be a part of the access request information and may be for either a single entity or a group of entities depending on the home network service and policy.

The authorization function may be based on the use of the following items:

– Authentication information such as passwords and possession whose subsequent presentation serves as evidence of the accessing entity's authorization.
– Authorization information containing capabilities whose subsequent presentation serves as evidence of the right to access the entity or resource defined by the capability.
– Authorization certificate.
– Security labels that may be used to grant or deny access when associated with an entity (usually according to a security policy).
– Time of attempted access.
– Route of attempted access.
– Duration of access.
– Physical location of the attempted access.
– Logged data.
– Characteristics of each user.
– Specific operations for the resource.

If the identifier of the accessing entity does not exist in the authorization database, or in case the accessing entity tries to access a resource beyond its/his/her authority range, dynamic authorization may be initiated to make a temporary policy since there is no authorization policy of a requesting HS in the AS.

The items above are the factors used in deciding whether to permit access or not. They may be referred to while enforcing authorization or composing materials containing authorization-related information. In other words, the authorization materials should reflect them.

There may be a variety of authorization materials depending on the application. The following are the generally used authorization materials:

– Authorization database.
– Authorization certificate.
– Authorization token.

Unlike authorization, whose main purpose is to restrict access by an entity based on the authorization policy even after successful authentication, the main purpose of authentication is to identify an entity and verify that it is qualified to access a resource. Note, however, that authorization is generally regarded as a post-process of authentication using the entity's identifier resulting from the successful authentication.

The interface between authentication and authorization is unidirectional from authentication to authorization. It mainly includes the entity's identifier such as user ID, name, serial number, etc., which are unique within a specified domain.

7 Authorization entities for the home network

A number of network protocols and various types of services coexist within the home network, and applications vary in terms of requirements and domains. The home network may involve a majority of the existing technologies employed in the open network. The scale of a single domain for the home network varies from a single home to a large-scale portal service domain.

Figure 1 shows the authorization entities in the home network.

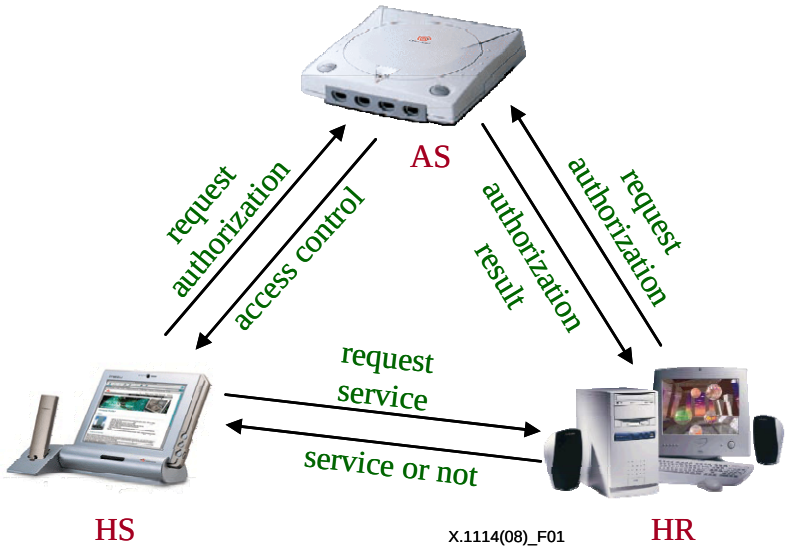

Figure 1 – Authorization entities for the home network

Authorization for the home network consists of three entities: AS, HS and HR.

Whenever HS is going to use HR, it can directly reach HR. Otherwise, it may go through AS, which is responsible for controlling access to HR. Naturally, AS should authorize HS to access HR on all occasions. Even though HS reaches HR, HR is expected to receive help from AS in deciding whether to permit access or not.

AS is an entity that enforces authorization and manages the authorization information, etc., for maintenance. The functions performed by AS are composed of two modules as follows:

– PDP makes an authorization decision based the authorization policy. The authorization policy should cover every possible access within the service domain and have no conflicts in its policy.

– Upon receiving a request from HS, PEP controls access based on the decision by PDP. PEP may be executed separately from PDP, where an additional way for securing communication between the two entities is required.

In general home network applications, AS is installed in the home gateway, service provider's server or a separate trusted AS. AS also may be installed in each service server or home device providing service depending on the service application.

HS refers to an accessing entity that will use the home network service. It requests permission from the AS or directly connects the HR that it wants to use. The type A home device defined in

[ITU-T X.1111] may be one typical example of HS. HS cannot define its own accessing privilege in case AS is not HS.

HR is an entity that is either controlled or used by HS. Every device and service deployed in the home network, including home appliances, home services and application servers can be considered HR. HR should have a PEP function in case HR receives the access request from HS.

8 Authorization models for the home network

The home network consists of heterogeneous network protocols and devices as well as a variety of services depending on the service provider. In designing the authorization module for the home network, the practical types and flows of authorization should be considered. Figure 2 shows the general model of authorization for the home network.

The boundary of the service domain controlled by a single secure home gateway may be either the home itself or another kind of service domain such as an apartment complex or a specific service network exclusive to subscribers. The categorization of the service domain is logical and completely dependent on the application of the home network.

The services in the home network can be categorized into four flows: service flow from the home user to the home application server or the home device; service flow from the home user to the application server; service flow from the remote user to the home application server or the home device, and; service flow from the remote user to the application server.

The authorization module may be enforced anywhere depending on the requirements and environment to which the home network applies. Note, however, that the secure home gateway is recommended to perform authorization since it is located at the border of each home and is responsible for providing the appropriate home network service.

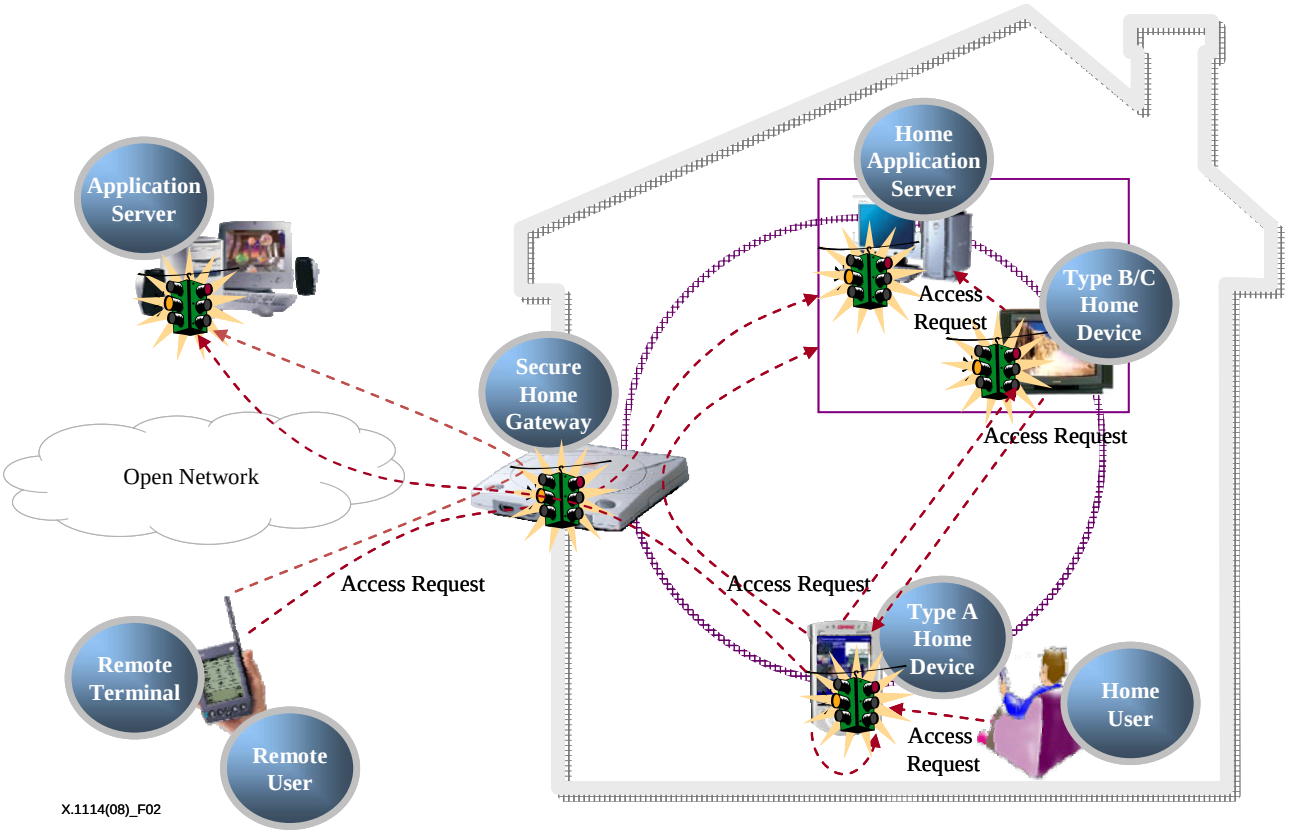

Figure 2 – General model of authorization for the home network

The dotted arrows represent the direction of service requests from the HS to the HR. It means that each HS can access the HRs along the dotted lines. The signal lamp also ensures that it performs authorization over the corresponding access.

Authorization for the home network can be categorized into two models: centralized authorization model and distributed authorization model.

The authorization models can be categorized based on conceptual service architecture. To make it concrete, it is necessary to establish an authorization model/method. The authorization method involves explicitly implementing authorization and indicating a specific mechanism. The policy model specifies the authorization policy in an efficient manner. They are introduced in Appendix I and Appendix II, respectively.

The following are detailed descriptions of these authorization models:

8.1 Centralized authorization model

The centralized authorization model adopts a centralized authority for performing authorization. Each centralized authority is responsible for controlling access and restricting privilege within the boundary of the designated service domain.

The centralized authorization model is generally used to provide legacy authorization service since it seems to be manageable and adequate for the actual service.

To deploy a centralized authorization model, the designated centralized AS and all materials for authorization from it should be trusted. Moreover, the centralized AS must be kept reliable and secure.

This model is considered relatively more manageable than the distributed authorization model. In the general application of the home network, the secure home gateway or the application server is expected to play a central role as a service server and establish connection between HS and HR. This model can minimize redundancy due to a variety of network protocols and middleware.

Figure 3 describes the centralized authorization model for the home network.

The fact that AS is responsible for authorization does not always mean that it directly controls access by itself.

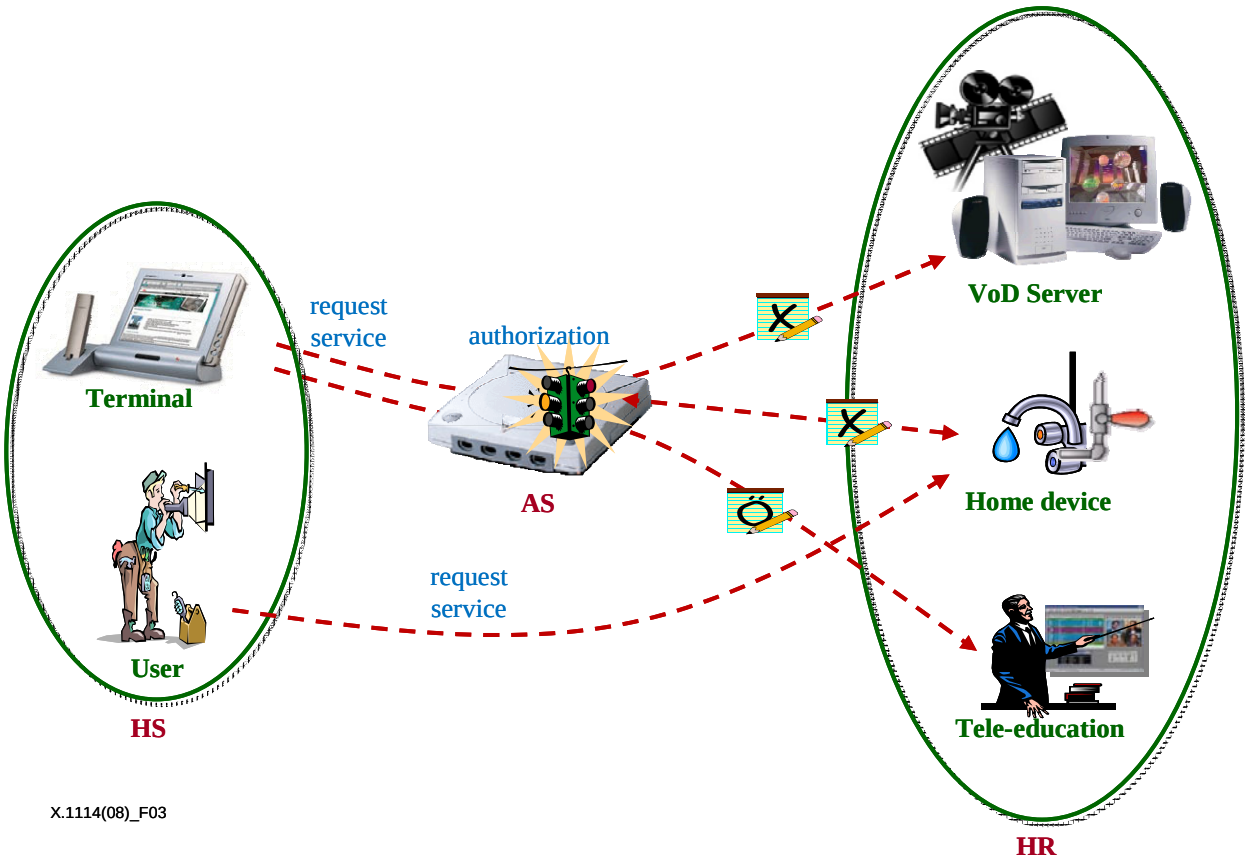

Figure 3 – Centralized authorization model for the home network

In the centralized authorization model, all permissions related to access to the home network must be managed by AS. In other words, HS may be controlled while either accessing to use HR through AS or directly accessing HR with some type of material for authorization as issued from a trusted AS.

For the application of the centralized authorization model to the home network, the secure home gateway among the seven entities defined in [ITU-T X.1111] should implement AS. In addition, the application server or the home application server may implement AS if necessary.

In summary, the centralized authorization model can apply to both client-server service and peer-to-peer service.

Figure 4 shows the centralized authorization model for the client-server service model.

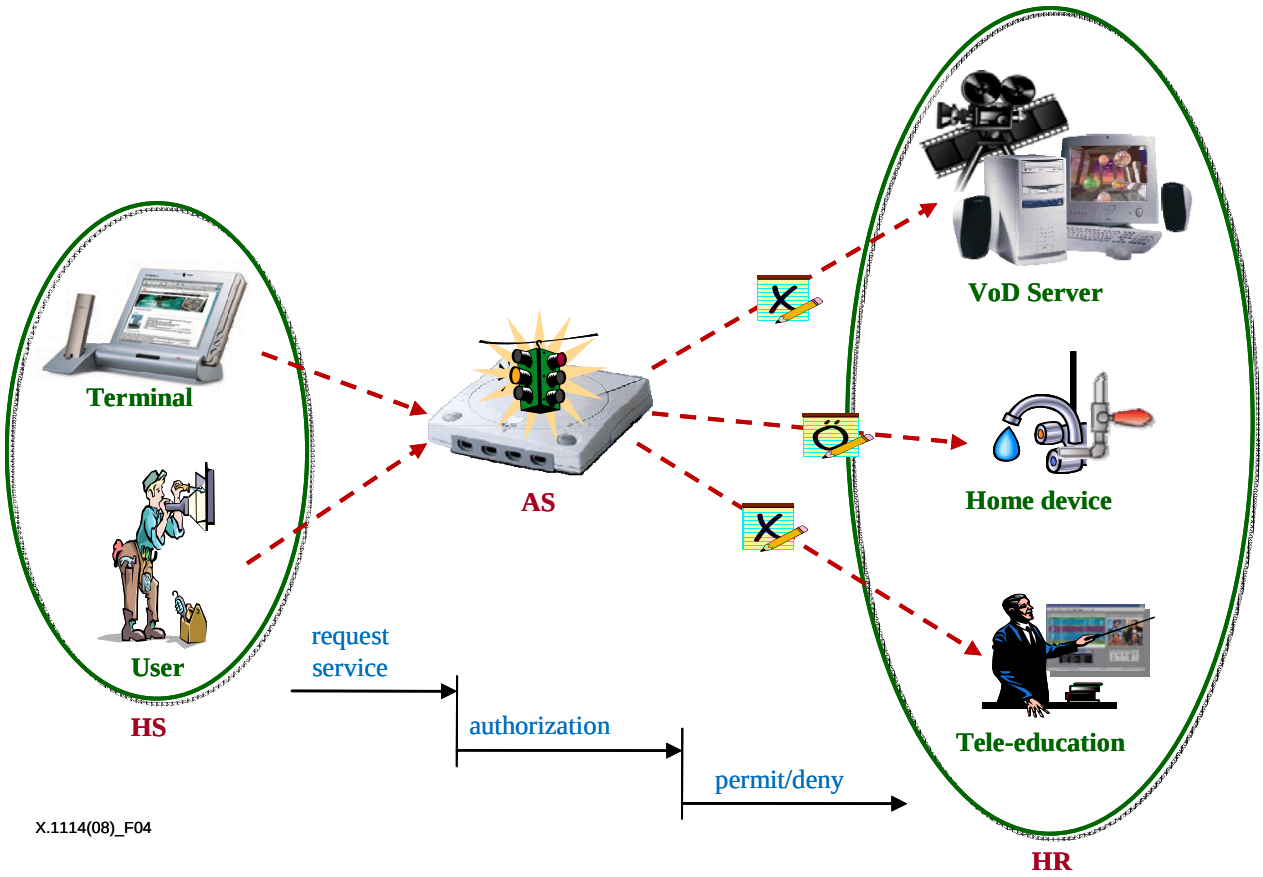

Figure 4 – Centralized authorization model for the client-server service

In the client-server service, every access for HR physically goes through AS. Thus, AS controls all real-time accesses. It is considered efficient, manageable and adequate for a relatively small-scale service domain.

Figure 5 shows the centralized authorization model for the peer-to-peer service.

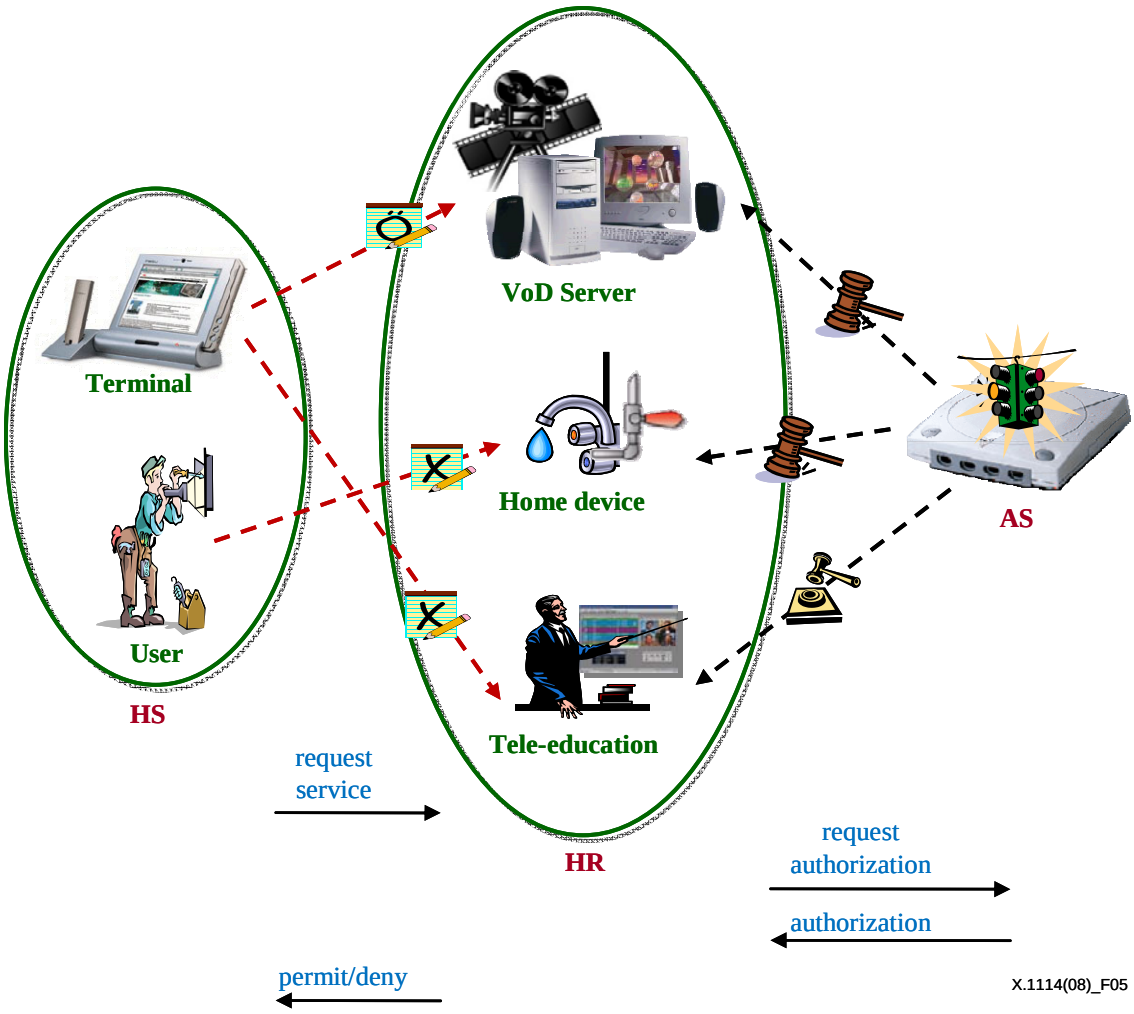

Figure 5 – Centralized authorization model for the peer-to-peer service

In the peer-to-peer service, each access from HS does not pass AS. Thus, the HR providing the home network service should decide whether to permit access or not upon receiving a request of access from HS.

An AS may issue a certain type of material containing information on the access privilege of HS in a secure manner. This material may be an authorization certificate, a temporary token for access control, etc.

Furthermore, we must guarantee security in issuing and using the material for authorization, which depends on the application and falls beyond the scope of this Recommendation.

8.2 Distributed authorization model

The distributed authorization model for the home network enables the home user or remote user to control the home device or use the home network service without the help of a centralized AS.

Figure 6 shows the distributed authorization model.

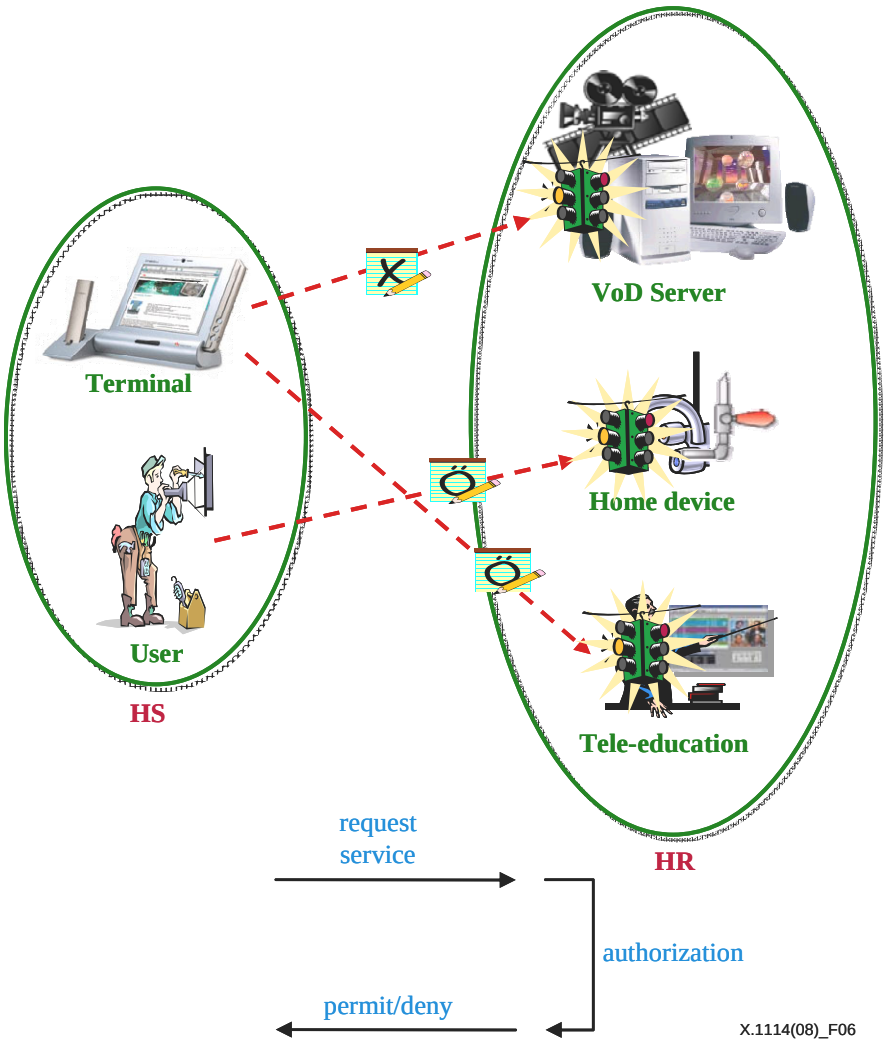

Figure 6 – Distributed authorization model

For the distributed authorization model, each entity – which may be either a home application server or a type B/C home device – defines the access control information and controls every access by itself. To do so, each device and application server must provide its own authorization policy and function. Note, however, that this authorization model seems to lack manageability; maintaining consistency among a number of authorization databases is also difficult.

9 Relationship between authorization entities and home network entities

Table 1 shows the relationship between home entities and authorization entities (the authorization entities come from the general model of the home network discussed in [ITU-T X.1111]).

Table 1 – Relationship between authorization entities and home network entities

Home entities / Authorization entities	Remote user/terminal	Home/application server	Secure home gateway	Home user	Home device
AS		Y	Y		Y
HS	Y			Y	Y
HR		Y			Y

In Table 1, "Y" means that a home entity may implement the corresponding authorization entities.

Since it is located on the border of each home and is responsible for the majority of the home network services, a secure home gateway is required to implement AS. An application server and a home application server may also implement AS.

Entities accessing HR, e.g., a remote user, a remote terminal, a home user and a home device, should implement HS.

Entities providing the home network service, such as an application server, a home application server and a home device, should implement HR.

10 Authorization modes

When an entity accesses a resource of the home network, the authorization function makes a decision based on the authorization database or the temporary authorization policy obtained through a dynamic authorization procedure of the owner of the accessed resource.

Authorization is categorized into two modes: static authorization mode and dynamic authorization mode.

If there is a relative policy for authorization in the authorization database, then authorization is said to be in static authorization mode. The known device and user are authorized to access the known resources (including device and content) based on the policies in the authorization database.

The authorization policy is likely to address all possible entities and conditions. However, there may be some cases wherein access may not be controlled by the appropriate policy due to missing policies or other mistakes committed by an authorization administrator.

The interpretation of such a situation may vary depending on the implementation and authorization policy. Access may be considered to be either unauthorized or undefined. In case of unauthorized access, we can simply reject it. For undefined access, however, we may need an additional function for temporarily permitting access, i.e., operating in dynamic authorization mode. In other words, the resource owner authorizes the accessing entity instantaneously when the accessing entity accesses a certain resource.

10.1 Static authorization mode

The home administrator is responsible for authorization within the service domain, pre-assigning the relative authorization policy wherein each policy consists of the accessing entity and its access rights. ACL, RBAC, authorization certificate or another type of authorization material is likely to be used for authorization depending on the implementation and policy.

The majority of the authorization activities are enforced in static authorization mode. Moreover, managing the authorization database is recommended to address all possible accessing entities. As such, all authorizations are performed in static authorization mode.

10.2 Dynamic authorization mode

When an accessing entity that is not yet registered in the authorization database, but is considered to have access privileges, is going to use a home network service, a separate procedure is required to grant temporary access rights. This procedure includes several steps: a phase for the confirmation of the identifier of the accessing entity; a phase for the generation of a temporary authorization policy; and a phase for enforcing the temporarily generated authorization policy.

Considering security, temporary privileges should be valid for a short period of time.

There are several factors making up the dynamic authorization mode:

1) **Authorization request**: The accessing entity initiates the authorization request while accessing the resource.

2) **Accessing range**: The accessing entity should specify the accessing range in the authorization request, e.g., accessed device and content.

3) **Subject of authorization**: The authorizer must be the resource's owner or be responsible for the services related to the resource.

4) **Confirmation of identifier of the accessing entity**: The accessing entity's identifier is confirmed based on a certain authentication procedure, which falls beyond the scope of this Recommendation.

5) **Dynamic authorization policy**: The temporarily generated authorization policy for the undefined accessing entity.

6) **Period of validity**: The period of validity can be valid for one-time use or for the designated short period.

The dynamic authorization mode can apply to both the centralized authorization model and the distributed authorization model.

10.2.1 Dynamic authorization mode for the centralized authorization model

Figure 7 shows the dynamic authorization mode for the centralized authorization model.

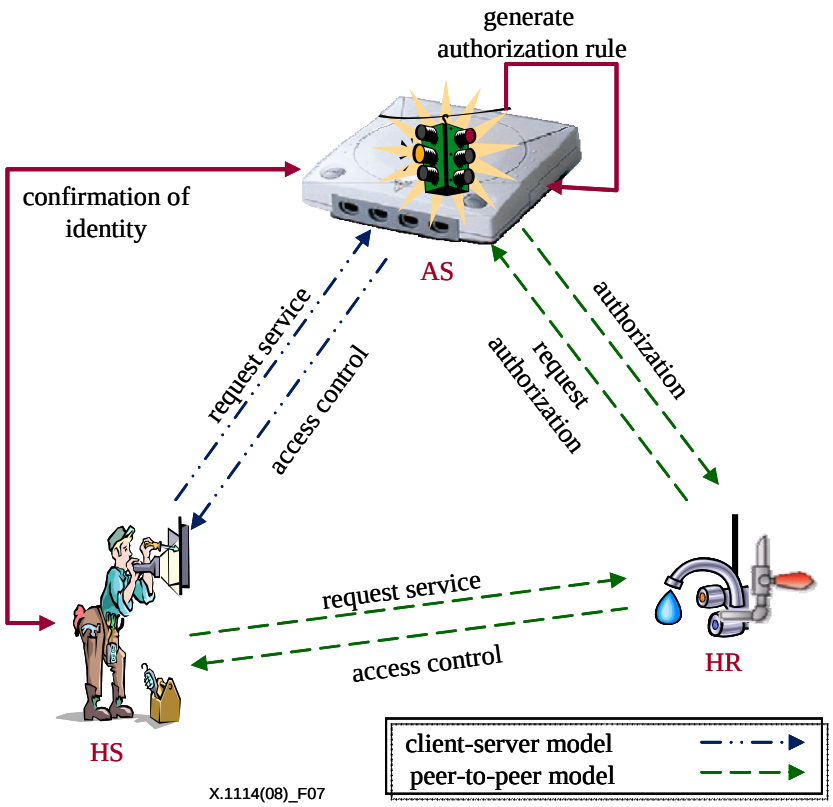

Figure 7 – Dynamic authorization mode for the centralized authorization model

In the centralized authorization model, AS performs authorization in the route between HS and HR. Thus, AS is required to identify the accessing entity whose authorization policy is not yet defined. The confirmation procedure for the access entity may be delegated to a trusted third party depending on the application.

According to the adopted service model, two different service flows are possible. In the client-server model, HS requests for service through AS. In the peer-to-peer model, however, HS directly requests for service from HR. HR additionally requests authorization from AS.

Whenever HR receives an authorization request, AS inspects its authorization policy and makes a decision as to whether to provide it or not. If there is no authorization policy defined for access from HS, a temporary authorization policy should be generated in dynamic authorization mode. The first step is to identify HS in a relatively secure manner. It includes existing authentication mechanisms as well as physical identification processes such as a phone call, a video camera, etc. After the successful authentication process, AS starts to generate the authorization policy. The generated authorization policy may be temporarily valid; the specific process of generating the authorization policy depends on the implementation and falls beyond the scope of this Recommendation.

10.2.2 Dynamic authorization mode for the distributed authorization model

Figure 8 shows the dynamic authorization mode for the distributed authorization model.

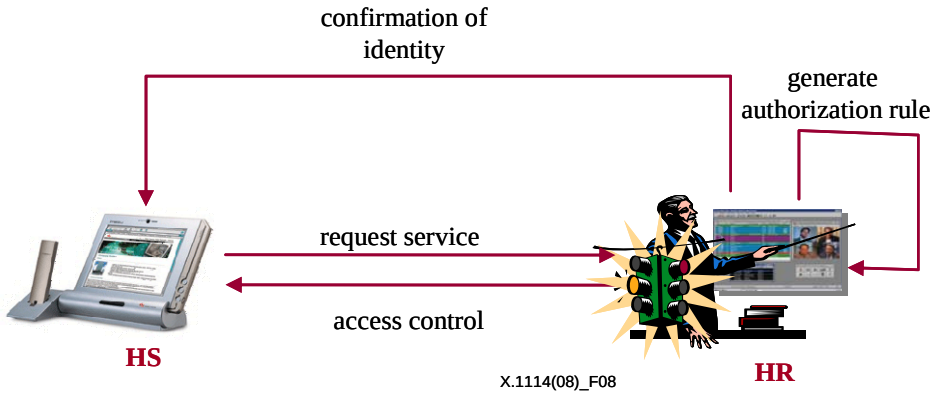

Figure 8 – Dynamic authorization mode for the distributed authorization model

In the distributed authorization model, each HR is responsible for authorization. Thus, HR is required to identify an HS whose authorization policy is not yet defined. After the confirmation procedure for HS, HR generates its own temporary authorization policy for HS. Moreover, the identification procedure may be delegated to a trusted third party such as a centralized authorization model.

Compared to the dynamic authorization mode for the centralized authorization model, HR should perform every step including receipt of an access request, confirmation of identifier, generation of authorization policy and enforcement of authorization.

11 Security threats for authorization in the home network

Since the home network consists of a variety of network protocols and service models, most of the security threats appearing in the legacy open network are also assumed to exist in the home network. The following are the security threats in the home network as cited in [ITU-T X.1111]:

– Eavesdropping/disclosure/interception.
– Interruption/communication jamming.
– Injection and modification of data.
– Unauthorized access.
– Repudiation.

– Shoulder surfing.
– Lost remote terminal.
– Stolen remote terminal.
– Unprepared communication shutdown.
– Misreading.
– Input error.
– Packet abnormal-forwarding.

The detailed descriptions of the above-mentioned security threats are provided in [ITU-T X.1111].

Among them, the following are the security threats that are assumed to be related to authorization for the home network:

– Eavesdropping/disclosure/interception

  Private information that is intercepted or revealed to an unauthorized entity may be used to access the home network illegally; thus preventing stable service and making the home network insecure and unavailable.

– Injection and modification of data

  An unauthorized entity, including a user, a program or a device, may modify information transmitted between entities as defined in [ITU-T X.1111] or insert some malicious codes. This threat attacks integrity.

– Unauthorized access

  Unauthorized access to PDP results in critical problems in the home network including illegal use of services, disclosure of private information, unintended control of home appliances, etc. The term "unauthorized" means both illegal and unnecessary.

– Shoulder surfing

  Shoulder surfing is used to gather the private information of other authorized entities illegally and to enable access to home network services without permission.

– Lost remote terminal

  A remote terminal may contain private information for accessing the home network. An authorized entity may access the home network using the lost remote terminal and cause damage, especially when it contains authentication-related information or if there is a trusted relationship between the lost remote terminal and an application server.

– Stolen remote terminal

  This threat is similar to the threat of a lost remote terminal. Note, however, that a remote terminal stolen intentionally is likely to cause more damage than a lost remote terminal.

12 Authorization requirements for the home network

From the authorization point of view, the requirements that are considered in authorizing the home network should conform to those defined in [ITU-T X.1111].

12.1 Data confidentiality

Data confidentiality protects authorization data from unauthorized disclosure. It prevents the data from being read or used illegally since this may result in the disclosure of critical information, infringement of privacy, denial of service, etc. Data exchanged through an insecure channel corresponding to authorization should be rendered confidential.

12.2 Data integrity

Data integrity ensures that data is correct or accurate without any revision. Data is protected against unauthorized modification, deletion, creation and replication, and the corresponding indication is enabled whenever any of the above occurs. The authorization framework must ensure integrity to all data exchanged for authorization.

12.3 Authentication

Authentication is the process of determining whether individuals or devices are who/what they claim to be, or ensuring the identifier of the sender from whom the message claims to be sent. The authorization process must follow the authentication process.

12.4 Availability

Availability ensures that a home network entity can use the home network service at all times, particularly when it accesses the home network and such access is proven to be authorized. Disaster recovery solutions are included in this category.

12.5 Consistency

Authorization information may be distributed over multiple entities wherein each entity can enforce authorization by itself. Consistency ensures that the database containing authorization policy in each entity is consistent, and that the latest version is maintained. Maintaining consistency of the authorization policies among the distributed authorization databases requires appropriate methods that fall beyond the scope of this Recommendation.

13 Relationship between security threats and requirements

Table 2 shows the relationship between security threats and requirements for authorization in the home network.

Table 2 – Relationship between authorization requirements and security threats

Security threats / Authorization requirements	Eavesdropping/ disclosure/ interception	Injection/ modification of information	Unauthorized access	Shoulder surfing	Lost remote terminal	Stolen remote terminal
Confidentiality	Y	Y	Y			
Integrity		Y				
Authentication			Y		Y	Y
Availability						
Consistency		Y	Y			

In Table 2, "Y" means that an authorization requirement in the first column in each row can address the corresponding security threats listed in the first row.

As shown in Table 2, shoulder surfing cannot be addressed by any defined authorization requirement since such private information is likely to be revealed by shoulder surfing. In such a case, there is no way of preventing unauthorized access resulting from shoulder surfing. Note, however, that damage due to shoulder surfing may be minimized by authorization.

Appendix I

Authorization methods

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

ACL

ACL includes all accessing privileges in the access control list of the subject and directly specifies the relationship between HS and HR. Using ACL is simple and adequate for the relatively small-scale service domain.

ACL is divided into two types: a standard ACL and an extended ACL. A standard ACL checks only the identifier of the subject in deciding policy, whereas an extended ACL may check extra material such as accessing time, location of the subject and other environmental information as well as the identifier of the subject.

DAC

DAC performs access control based on the owner of the resource to be used, and uses ACL. In DAC, the access rights may be modified by the owner of the resource. Therefore, it is hardly adequate in enterprises or government organizations requiring integrity.

MAC

In MAC, access control is enforced by the operation system, which in turn may invalidate the decision of the owner of the resource. MAC is generally used in an environment where security is of utmost importance, such as for military organizations. Commercial use cases may focus more on how to counter the illegal modification of information than on confidentiality.

RBAC

RBAC indirectly specifies a relationship between HS and HR through a third component called role. It is assumed to be adequate for a relatively large-scale service domain and may be used for the home network, which may include a number of resources or where changes in its entities occur frequently.

Authorization certificate

The authorization certificate contains information for controlling access. It may vary in terms of format according to the service domain where it applies. Furthermore, the authorization certificate must include the following:

– Ownership information for the authorization certificate.
– Validity period of the authorization certificate.
– Authorization information, which may be of type ACL, RBAC, etc.
– Security-related information, i.e., digital signature, for guaranteeing the authenticity and integrity of the authorization certificate.

The profile and operating mechanism of the authorization certificate are almost the same as those of the authentication certificate of [b-ITU-T X.509]. Note, however, that there are a few differences between the authorization certificate and the authentication certificate.

– The authorization certificate includes information for access control (not included in the authentication certificate).

– The entity issuing an authorization certificate is responsible for each service within the home network domain. In contrast, the entity issuing an authentication certificate, such as CA, does not concern itself with the service but merely guarantees the validity of the issued authentication certificate.

– Generally, the validity period of an authorization certificate is much shorter than that of an authentication certificate.

Appendix II

Conceptual policy model for authorization

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

The main objective of authorization is to grant to an authorized HS the right to access HR and to prevent unauthorized access. There are various implementations for authorization; their running environments and materials for determining access rights vary depending on the application.

Even though specifying the policy model for authorization is difficult, a description of the concept of the policy model for authorization may be needed.

Figure II.1 describes the conceptual policy model for authorization.

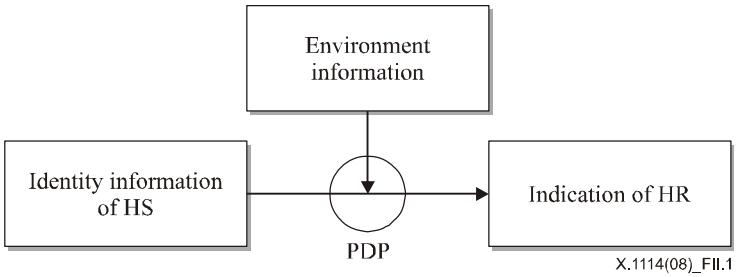

Figure II.1 – Conceptual policy model for authorization

The authorization policy model applies to authorization methods based on both ACL and RBAC.

The following items should be considered:

– Identifier of HS
  - Unique ID of user, device or other types of HS.
  - URI or URL of HS.
  - Address of HS.
  - Others.
  - Combination of the items above.

– Identifier of HR
  - Unique ID of HR.
  - URI or URL of HR.
  - Address of HR.
  - Others.
  - Group ID with the above-mentioned items.

– Information on access rights
  - Permit or deny.

– Environment information
  - Accessing time.
  - Accessing place.
  - History information.
  - Information on the situation, e.g., emergency, event occurrence, etc.
  - Others.

Appendix III

Service scenario of the dynamic authorization mode

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

Figure III.1 describes a service scenario of the dynamic authorization mode.

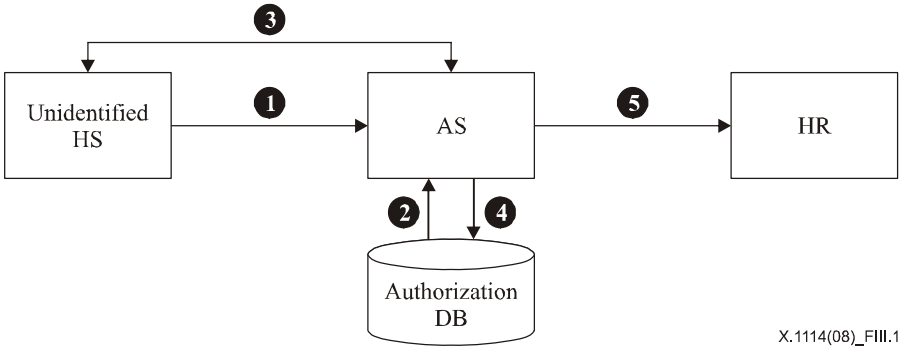

Figure III.1 – Service scenario of the dynamic authorization mode

In this service scenario, there are three entities as follows:

– Unidentified HS: Gas-meter reader.

– AS: Secure home gateway.

– HR: Gas-meter.

The following are the steps for the dynamic authorization mode:

– Step 1: Phase of access request by an unidentified HS
  - Alice, a gas-meter reader, is going to access a gas meter in Bob's home.
  - This step may include a related authentication procedure.

– Step 2: Phase of referencing the authorization database
  - The corresponding authorization policy for Alice is not yet defined.
  - AS decides whether to deny or shift to dynamic authorization mode.

– Step 3: Phase of identifying HS
  - AS identifies Alice in an offline manner, e.g., telephone, face-to-face conversation or guarantee of a trusted third party.
  - Online authentication is also possible in case step 1 does not include a related authentication procedure.

– Step 4: Phase of establishment of the newly generated authorization policy
  - AS generates a temporary authorization policy for permitting Alice's access.
  - The newly generated authorization policy is valid for a short period of time.
  - The newly generated authorization policy may be stored in the authorization database permanently or used for one-time access only.

– Step 5: Phase of access control based on the newly generated authorization policy
    - AS permits Alice to gauge the meter.

Moreover, additional step may follow depending on the application.

– Phase of removal of the temporarily generated authorization policy from the authorization database.

Appendix IV

Use cases of authorization models

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

There are two authorization models defined: centralized authorization model for the client-server service and distributed authorization model.

Here, use cases of the above-mentioned authorization models are introduced.

1) Use case of the centralized authorization model for the client-server service

In the centralized authorization model for the client-server service, the authorization policy used for access is maintained in the centralized AS. Authorization is also enforced in a centralized manner.

Generally deployed in actual authorization enforcements, this authorization model has a number of benefits.

Figure IV.1 describes a use case of the centralized authorization model for the client-server service.

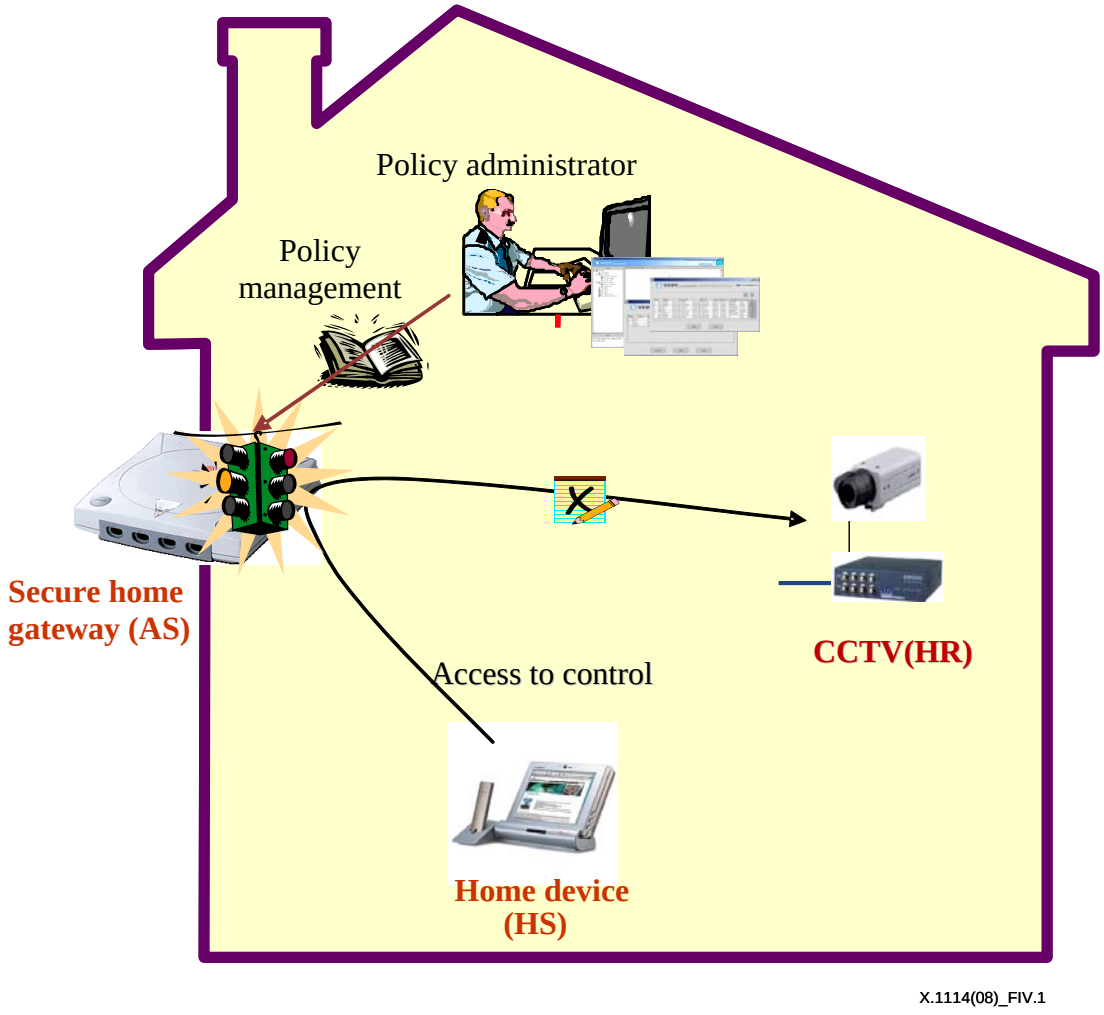

Figure IV.1 – Use case of the centralized authorization model for the client-server service

CCTV is considered to be an important home device for providing a home security service. To monitor and control the operation of CCTV, the home device should access the secure home gateway. Then, the secure home gateway verifies the right of HS to access the CCTV. The authorization policy is already stored in the secure home gateway by the policy administrator. Based on the authorization policy, the secure home gateway decides whether to permit the access or not. In this use case, authorization is performed in the centralized AS called the secure home gateway and direct access to the CCTV is not allowed.

2) Use case of the distributed authorization model

In the distributed authorization model, each entity provides a service, maintains its own authorization policy and enforces it by itself. The service provided by the content server may adopt the peer-to-peer service model; it may serve as a simple example of using the distributed authorization model.

Figure IV.2 shows a use case of the distributed authorization model.

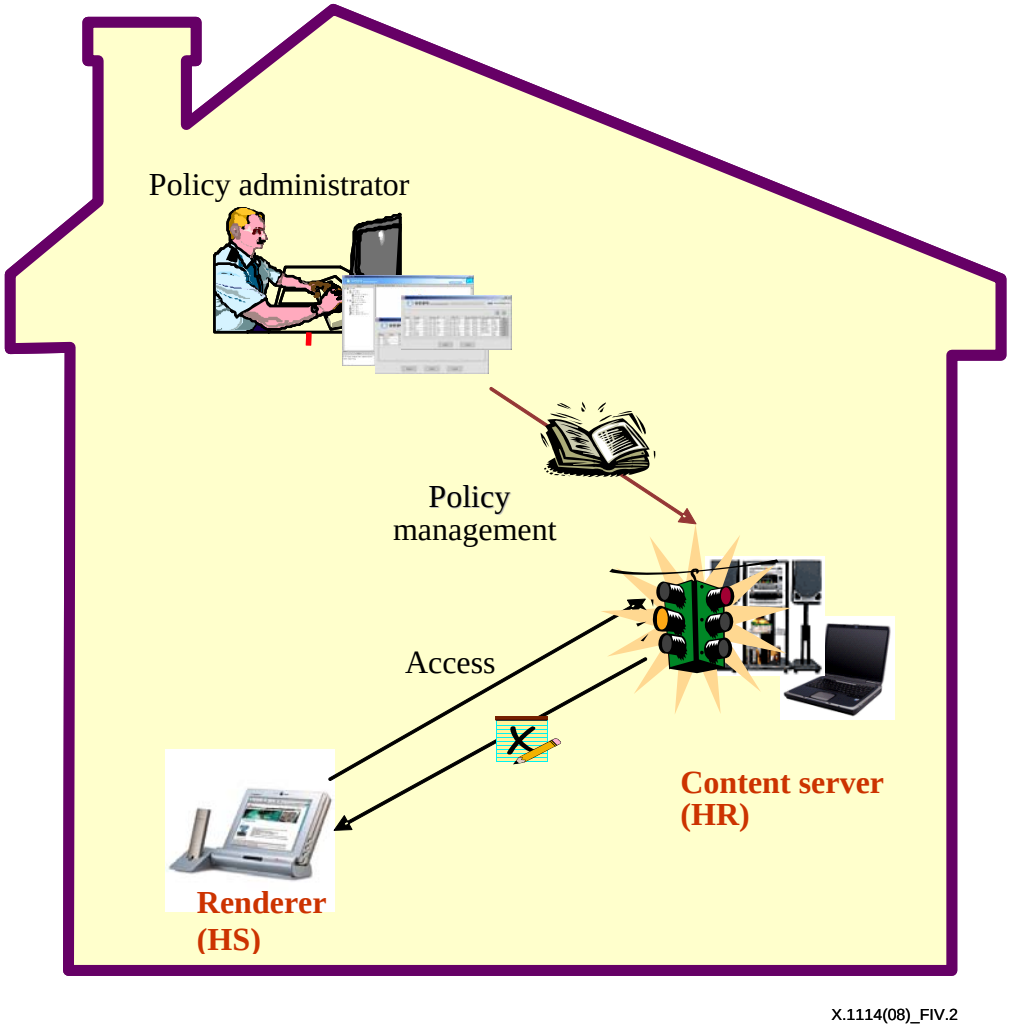

Figure IV.2 – Use case of the distributed authorization model

Each device (renderer) can directly access other devices (content server). Each content server provides contents without the intervention of the centralized secure home gateway. Therefore, the authorization policy is managed in each content server providing service.

In this use case, each HR maintains an authorization policy and enforces access control by itself.

Bibliography

[b-ITU-T X.509] Recommendation ITU-T X.509 (2005) | ISO/IEC 9594-8:2005, *Information technology – Open Systems Interconnection – The Directory: Public-key and attribute certificate frameworks*.
<http://www.itu.int/rec/T-REC-X.509>

[b-ITU-T X.800] Recommendation ITU-T X.800 (1991), *Security architecture for Open Systems Interconnection for CCITT applications*.
<http://www.itu.int/rec/T-REC-X.800>

[b-ITU-T X.805] Recommendation ITU-T X.805 (2003), *Security architecture for systems providing end-to-end communications*.
<http://www.itu.int/rec/T-REC-X.805>

[b-ITU-T X.811] Recommendation ITU-T X.811 (1995) | ISO/IEC 10181-2:1996, *Information Technology – Open Systems Interconnection – Security frameworks for open systems: Authentication framework*.
<http://www.itu.int/rec/T-REC-X.811>

[b-ITU-T X.1112] Recommendation ITU-T X.1112 (2007), *Device certificate profile for the home network*.
<http://www.itu.int/rec/T-REC-X.1112>

[b-ITU-T X.1113] Recommendation ITU-T X.1113 (2007), *Guideline on user authentication mechanisms for home network services*.
<http://www.itu.int/rec/T-REC-X.1113>

[b-ITU-T X.1121] Recommendation ITU-T X.1121 (2004), *Framework of security technologies for mobile end-to-end data communications*.
<http://www.itu.int/rec/T-REC-X.1121>

[b-ITU-T X.1142] Recommendation ITU-T X.1142 (2006), *eXtensible Access Control Markup Language (XACML 2.0)*.
<http://www.itu.int/rec/T-REC-X.1142>

[b-ITU-T Y.2091] Recommendation ITU-T Y.2091 (2008), *Terms and definitions for Next Generation Networks*.
<http://www.itu.int/rec/T-REC-X.2091>

[b-NIST SP800-47] National Institute for Standards and Technology SP800-47 (2002), *Security Guide for Interconnecting Information Technology Systems*.
<http://csrc.nist.gov/publications/nistpubs/800-47/sp800-47.pdf>

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, 2009