

I n t e r n a t i o n a l T e l e c o m m u n i c a t i o n U n i o n

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

X.1080.0

(03/2017)

SERIES X: DATA NETWORKS, OPEN SYSTEM
COMMUNICATIONS AND SECURITY

Information and network security – Telebiometrics

Access control for telebiometrics data protection

Recommendation ITU-T X.1080.0



International
Telecommunication
Union

Documents
Document Sharing Hub

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
PKI related Recommendations	X.1340–X.1349
Internet of things (IoT) security	X.1360–X.1369
Intelligent transportation system (ITS) security	X.1370–X.1379
CYBERSECURITY INFORMATION EXCHANGE	
Overview of cybersecurity	X.1500–X.1519
Vulnerability/state exchange	X.1520–X.1539
Event/incident/heuristics exchange	X.1540–X.1549
Exchange of policies	X.1550–X.1559
Heuristics and information request	X.1560–X.1569
Identification and discovery	X.1570–X.1579
Assured exchange	X.1580–X.1589
CLOUD COMPUTING SECURITY	
Overview of cloud computing security	X.1600–X.1601
Cloud computing security design	X.1602–X.1639
Cloud computing security best practices and guidelines	X.1640–X.1659
Cloud computing security implementation	X.1660–X.1679
Other cloud computing security	X.1680–X.1699

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

Recommendation ITU-T X.1080.0

Access control for telebiometrics data protection

Summary

Recommendation ITU-T X.1080.0 provides specifications on how to protect telebiometrics information against unauthorized access. A service-oriented view is taken, where only information necessary for a particular purpose is provided, i.e., access is given not only on a *right-to-know* basis, but also on a *need-to-know* basis.

The core of this Recommendation is an attribute specification included in an attribute certificate or public-key certificate that specifies in detail what privileges a particular entity has for one or more service types.

Security is provided by using a profile of the cryptographic message syntax (CMS). The CMS profile provides authentication, integrity and, when required, confidentiality (encryption).

This profile is intended to provide security support for telebiometrics specifications in general. The profile assumes, and is dependent upon, the correct deployment of a public-key infrastructure (PKI).

This Recommendation is also dependent on the deployment of a privilege management infrastructure (PMI).

History

Edition	Recommendation	Approval	Study Group	Unique ID*
1.0	ITU-T X.1080.0	2017-03-30	17	11.1002/1000/13193

Keywords

Access control, Diffie-Hellman, PKI, telebiometrics.

* To access the Recommendation, type the URL <http://handle.itu.int/> in the address field of your web browser, followed by the Recommendation's unique ID. For example, <http://handle.itu.int/11.1002/1000/11830-en>.

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/>.

© ITU 2017

All rights reserved. No part of this publication may be reproduced, by any means whatsoever, without the prior written permission of ITU.

Table of Contents

		Page
1	Scope.....	1
2	References.....	1
3	Definitions	2
	3.1 Terms defined elsewhere	2
	3.2 Terms defined in this Recommendation.....	3
4	Abbreviations and acronyms	3
5	Conventions	4
6	Basic concepts and models	4
	6.1 Protection in a single data protection domain	4
	6.2 Cross data protection domain	6
	6.3 Service-oriented model.....	6
	6.4 The object and attribute model	7
	6.5 Basic access control principles.....	7
	6.6 Relationship to other access control schemes	7
	6.7 Protocols overview	8
	6.8 Use of CMS	8
	6.9 Public-key certificate considerations.....	9
7	Provision of privilege information.....	9
	7.1 Use of attribute certificates.....	9
	7.2 Use of public-key certificates	9
	7.3 The access service attribute type	10
	7.4 Operations on objects as a whole	12
	7.5 Operations on attributes.....	12
	7.6 Error handling.....	13
8	Privilege assertion protocol	13
	8.1 Overview	13
	8.2 Common request components	14
	8.3 Accessing a service.....	14
	8.4 Read operation.....	14
	8.5 Compare operation	15
	8.6 Add operation	17
	8.7 Delete operation.....	18
	8.8 Modify operation	18
	8.9 Rename object operation	20
	8.10 Error handling.....	21
	8.11 Information selection.....	21
	8.12 Object information.....	22

	Page
8.13 Defined error codes	22
9 Privilege assignment protocol.....	23
9.1 Scope of protocol.....	23
9.2 Content types	23
Annex A – Object identifier allocation for the ITU-T 1080-series.....	25
A.1 Top level of object identifier tree	25
A.2 Object identifiers for CMS content types.....	25
A.3 Object identifiers for privilege attribute types.....	26
Annex B – Cryptographic message syntax profile.....	27
B.1 General	27
B.2 Use of the signedData content type	28
B.3 Use of envelopedData content type	30
B.4 Use of the authenticated-enveloped-data content type	34
B.5 Attributes	35
B.6 Cryptographic message syntax error codes	36
Annex C – Formal specification of the privilege assertion and assignment protocols	38
Appendix I – Informal specification for the cryptographic message syntax profile.....	44
Bibliography.....	49

iv

Introduction

When collecting telebiometrics data from individuals, there is a risk of infringement of privacy.

There may be several reasons for protecting such information. Information may provide access to a company or an organization or it may be of a sensitive nature that restricts its distribution.

The protection against unwanted disclosure of telebiometrics data has two major aspects:

- protection of data during transmission, typically by encryption, and protection of stored data;
- control of access to stored data.

While telebiometric systems should have a high level of security with respect to confidentiality (encryption), authentication, integrity, physical protection, use of firewalls, virus protection programs, etc., it is also necessary to establish an elaborate access control system for access to stored information, in particular information about individuals. This latter aspect is particularly important for telebiometric systems.

General access control schemes have a shortcoming in that they mainly consider the *right* (or refusal) to information, but do not consider, in detail, the *need-to-know* aspect. A need-to-know implies that it is not sufficient to have the right to see the data, but it also must be established that this information is to be used for legitimate purposes.

Information should only be provided for its intended use. Medical information about a patient is collected to allow optimal treatment of that patient and should not be used for any other purpose, except possibly for tightly controlled research projects that may require use of some pieces of information from a specific collection of patients, otherwise information shall be protected against information trawling.

There are two main types of access control: physical and logical. Physical access control limits access to campuses, buildings, rooms and physical information technology (IT) assets. Logical access limits connections to computer networks, system files and data. Only logical access control is considered in this Recommendation

Access control includes secure authentication of accessors by the service provider. This Recommendation assumes the use of digital signatures and an established public-key infrastructure (PKI).

Recommendation ITU-T X.1080.0 may be referenced by other telebiometrics specifications.

Annex A, which is an integral part of this Recommendation, specifies the allocation of object identifiers used by the ITU-T X.1080-series of Recommendations.

Annex B, which is an integral part of this Recommendation, provides a telebiometrics profile of the cryptographic message syntax (CMS), as discussed in IETF RFC 5652, that is used by this Recommendation. It can also be referenced by other telebiometrics specifications.

Annex C, which is an integral part of this Recommendation, provides a formal specification for the privilege assertion and assignment protocols in the form an Abstract Syntax Notation One (ASN.1) module.

Appendix I, which is not an integral part of this Recommendation, provides an informal specification for the CMS profile in the form of an ASN.1 module.

.....

Recommendation ITU-T X.1080.0

Access control for telebiometrics data protection

1 Scope

This Recommendation provides a specification for how privacy may be protected in a telebiometrics environment by using privacy-based access control for telebiometrics (ACT). While this Recommendation cannot identify all possible information types, it is within the scope to provide general tools for handling all types of information in a secure way. This includes definition of a protocol for assigning privileges and a protocol for accessing information using privilege assertion. This Recommendation provides guidelines and does not contain compliance requirements.

The following is outside the scope of this Recommendation:

- physical protection of the information;
- unauthorized access by operational personal that maintain the security system and therefore having the possibility to circumvent security.

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.500-series] Recommendation ITU-T X.5xx (2016) | ISO/IEC 9594-x series, *Information technology – Open Systems Interconnection – The Directory*.
- [ITU-T X.501] Recommendation ITU-T X.501 (2016) | ISO/IEC 9594-2, *Information technology – Open Systems Interconnection – The Directory: Models*.
- [ITU-T X.509] Recommendation ITU-T X.509 (2016) | ISO/IEC 9594-8, *Information technology – Open Systems Interconnection – The Directory: Public-key and attribute certificate frameworks*.
- [ITU-T X.520] Recommendation ITU-T X.520 (2016) | ISO/IEC 9594-6, *Information technology – Open Systems Interconnection – The Directory: Selected attribute types*.
- [ITU-T X.521] Recommendation ITU-T X.521 (2016) | ISO/IEC 9594-7, *Information technology – Open Systems Interconnection – The Directory: Selected object classes*.
- [ITU-T X.680] Recommendation ITU-T X.680 (2015) | ISO/IEC 8824-1, *Information technology – Abstract Syntax Notation One (ASN.1): Specification of basic notation*.
- [ITU-T X.681] Recommendation ITU-T X.681 (2015) | ISO/IEC 8824-2, *Information technology – Abstract Syntax Notation One (ASN.1): Information object specification*.

- [ITU-T X.682] Recommendation ITU-T X.682 (2015) | ISO/IEC 8824-3, *Information technology – Abstract Syntax Notation One (ASN.1): Constraint specification*.
- [ITU-T X.683] Recommendation ITU-T X.683 (2015) | ISO/IEC 8824-4, *Information technology – Abstract Syntax Notation One (ASN.1): Parameterization of ASN.1 specifications*.
- [ITU-T X.690] Recommendation ITU-T X.690 (2015) | ISO/IEC 8825-1, *Information technology – ASN.1 encoding rules: Specification of Basic Encoding Rules (BER), Canonical Encoding Rules (CER) and Distinguished Encoding Rules (DER)*.
- [ITU-T X.1080.1] Recommendation ITU-T X.1080.1 (2011), *e-Health and world-wide telemedicines – Generic telecommunication protocol*.
- [ITU-T X.1081] Recommendation ITU-T X.1081 (2011), *The telebiometric multimodal model – A framework for the specification of security and safety aspects of telebiometrics*.
- [IETF RFC 2631] IETF RFC 2631 (1999), *Diffie-Hellman Key Agreement Method*.
- [IETF RFC 3185] IETF RFC 3185 (2001), *Reuse of CMS Content Encryption Keys*.
- [IETF RFC 5083] IETF RFC 5083 (2007), *Cryptographic Message Syntax (CMS) – Authenticated-Enveloped-Data Content Type*.
- [IETF RFC 5652] IETF RFC 5652 (2009), *Cryptographic Message Syntax (CMS)*.
- [IETF RFC 5753] IETF RFC 5753 (2010), *Use of Elliptic Curve Cryptography (ECC) Algorithms in Cryptographic Message Syntax CMS*.
- [IETF RFC 5911] IETF RFC 5911 (2010), *New ASN.1 Modules for Cryptographic Message Syntax (CMS) and S/MIME*.
- [IETF RFC 6268] IETF RFC 6268 (2011), *Additional New ASN.1 Modules for the Cryptographic Message Syntax (CMS) and the Public Key Infrastructure Using X.509 (PKIX)*.

3 Definitions

3.1 Terms defined elsewhere

This Recommendation uses the following terms defined elsewhere:

3.1.1 attribute certificate [ITU-T X.509]: A data structure, digitally signed by an attribute authority that binds some attribute values with identification information about its holder.

3.1.2 attribute type [ITU-T X.501]: That component of an attribute which indicates the class of information held by that attribute.

3.1.3 attribute value [ITU-T X.501]: A particular instance of the class of information indicated by an attribute type.

3.1.4 privilege [ITU-T X.509]: An attribute or property assigned to an entity by an authority.

3.1.5 privilege holder [ITU-T X.509]: An entity that has been assigned privilege. A privilege holder may assert its privilege for a particular purpose.

3.1.6 privilege verifier [ITU-T X.509]: An entity verifying certificates against a privilege policy.

3.1.7 source of authority (SOA) [ITU-T X.509]: An attribute authority that a privilege verifier for a particular resource trusts as the ultimate authority to assign a set of privileges for asserting that resource.

3.2 Terms defined in this Recommendation

This Recommendation defines the following terms:

3.2.1 access control: A security technique used to regulate who can do what to information resources in a computing environment.

3.2.2 access service: A service provided by a service provider for the execution of a particular transaction.

3.2.3 accessor: A privilege holder that accesses a particular access service using its privilege.

3.2.4 attribute: A piece of information of a particular type that is associated with an object. Information associated with an object is composed of attributes.

3.2.5 data protection domain: A domain where the information to be protected is under a single management component.

3.2.6 distinguished name: A name identifying an object that is unique within a specific context and which is formed by one or more name components reflecting the object's position in a hierarchy of objects.

3.2.7 object: A person, a department, a professional or some other type of object about which there is information and which is identifiable by a distinguished name.

3.2.8 object class: An identified family of entities that share certain characteristics.

3.2.9 operation: An interaction comprised of a request and a reply between an accessor and a service provider for a particular objective.

3.2.10 specification: An ITU-T Recommendation, an International Standard or any specification developed by a recognized Standards Developing Organization (SDO).

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

AA	Attribute Authority
ABAC	Attribute-based Access Control
ACL	Access Control List
ACT	Access Control for Telebiometrics
AES	Advanced Encryption Standard
ASN.1	Abstract Syntax Notation One
BER	Basic Encoding Rules
CA	Certification Authority
CEK	Content Encryption Key
CMS	Cryptographic Message Syntax
DER	Distinguished Encoding Rules
DH	Diffie-Hellman
ECC	Elliptic Curve Cryptography

ECDH	Elliptic Curve Diffie-Hellman
GCM	Galois/Counter Mode
KEK	Key-Encryption Key
LDAP	Lightweight Directory Access Protocol
MAC	Message Authentication Code
PDU	Protocol Data Unit
PKI	Public-Key Infrastructure
PMI	Privilege Management Infrastructure
SDO	Standards Developing Organization
SOA	Source of Authority

5 Conventions

This Recommendation presents Abstract Syntax Notation One (ASN.1) notation in the **bold courier new typeface**. When ASN.1 types and values are referenced in normal text, they are differentiated from normal text by presenting them in the bold Courier New typeface.

If the items in a list are numbered (as opposed to using "-" or letters), then the items shall be considered steps in a procedure.

6 Basic concepts and models

6.1 Protection in a single data protection domain

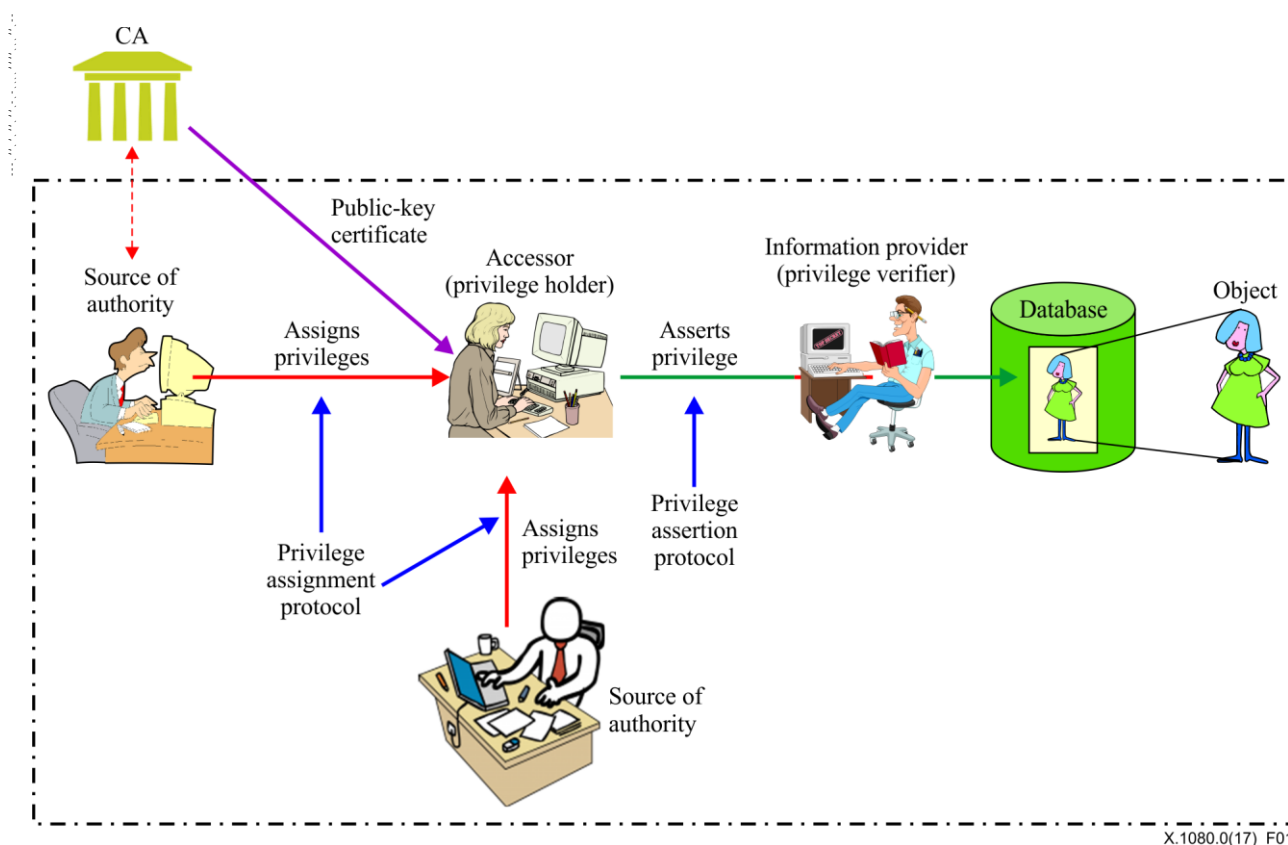


Figure 1 – Single data protection domain model

Figure 1 illustrates the various partners and protocols in an access control environment within a single data protection domain. A data protection domain comprises all entities involved in protection that are under common management.

An entity, called an accessor, may have a job function that requires permission to perform operations on information about objects held by an information provider. As an example, a doctor who is responsible for a patient needs to access the patient's health record to provide optimal treatment, while other doctors not involved with the patient have no need for such information.

Permission to perform a particular operation on information should only be given if the accessor has the *right* and a *genuine need* to perform that operation, i.e., it has been assigned the necessary *privilege*.

It is outside the scope of this Recommendation to specify under what conditions privileges are assigned to entities. It is only within the scope to provide the necessary tools for managing privileges in a secure way.

A data protection domain needs to establish one or more authorities to assign privileges to entities. The term source of authority (SOA) defined in [ITU-T X.509] is used here as the term for the ultimate authority for assigning privileges for a specific area within a data protection domain.

This Recommendation uses certificates to assign privilege to accessors. Privilege may be carried in attribute certificates in the **attributes** component or in public-key certificates in the **subjectDirectoryAttributes** extension. Privileges that are permanent may typically be provided in public-key certificates, while temporary privileges may typically be provided in attribute certificates.

Figure 1 illustrates the relationship among the various components within a single data protection domain. It shows two SOAs each responsible for assigning privileges for different aspects to privilege holders.

Some privileges may be needed for daily operations of the accessor and are therefore of a more permanent nature, while other privileges are assigned for handling special situations and are therefore temporary in nature.

When privileges are assigned to an accessor, the accessor becomes a privilege holder and may use their privilege to access information through the privilege assertion protocol. The privilege verifier, representing the information provider, checks the asserted privilege before allowing access to the information.

An SOA may forward privileges either by local means or by embedding them in a signed attribute certificate in the privilege assignment protocol as illustrated in Figure 1.

Figure 1: Access control environment

6.2 Cross data protection domain

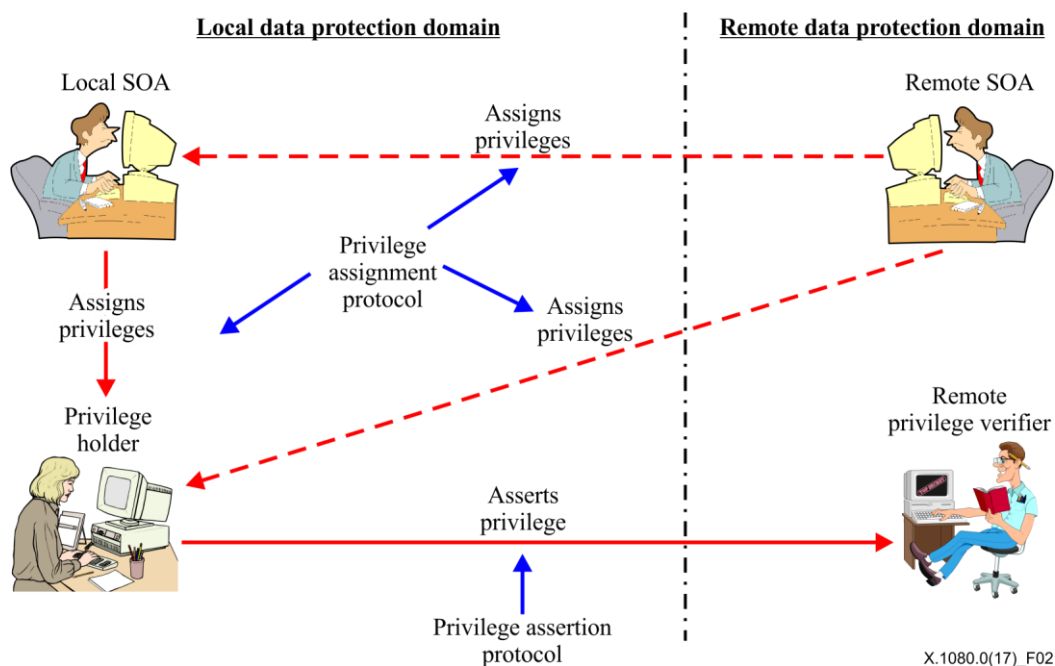


Figure 2 – Cross data protection domain model

Figure 2 illustrates the case where an accessor needs access to information within another data protection domain, e.g., to treat a patient for which vital health information is located in another data protection domain.

In this environment, the accessor either directly or through a local SOA requests access to specific information about a particular object. How this request is forwarded is outside the scope of this Recommendation, but it could be by e-mail or by telephone.

The remote SOA generates an attribute certificate with an attribute of type `accessService` holding the necessary privilege. This attribute certificate is signed by the remote SOA. The `holder` of the attribute certificate may be either the local SOA or it may be the entity that needs the privilege.

If it is the local SOA having the privilege assigned, this SOA:

- decrypts the content if required;
- verifies the signature on the content;
- extracts the attribute certificate from the content;
- validates extracted attribute certificate;
- creates a new attribute certificate with the privilege information taken from the received attribute certificate and with the entity needing the privilege as the holder;
- this attribute certificate together with the one received from the remote SOA is then forwarded to the entity needing the privilege (i.e., the privilege holder).

6.3 Service-oriented model

The access control for telebiometrics is service oriented in the sense that an accessor may invoke a set of distinct functions, called *access services*. An access service is a function provided by a service provider capable of performing the particular access service. An example of an access service is the capability to manipulate patient information within a hospital. An object identifier is used to identify a particular access service type. This Recommendation does not define specific

access services, but provides the tools for establishing access services. Referencing specifications may define access services relevant for their scope.

Although an accessor has access to a particular service, they may not have the privilege that covers all aspects of that service.

6.4 The object and attribute model

The information model defined in [ITU-T X.501] is designed to handle different data structures. This Recommendation uses this information model for access control.

In the ITU-T X.501 model, objects to be protected are organized in object classes, where objects within an object class have common characteristics relevant within a specific context. An object class is identified by an object identifier. [ITU-T 1080.1] expands on this concept by assigning object identifiers to a group of object classes for categories relevant to telebiometrics.

[ITU-T X.521] also defines a set of general usable object classes. In cases where an object class that is not directly related to telebiometrics is required, an already defined object class should be used whenever possible.

The individual objects are identified by distinguished names as defined in [ITU-T X.501]. A distinguished name consists of one or more name components that reflect its position within an object hierarchy.

The information associated with an object is modelled as a set of attributes. Attributes with common characteristics constitute an attribute type. An attribute type is identified by an object identifier. An attribute is a sequence of an object identifier identifying the attribute type and one or more values of that type. An object may only have one attribute of a particular type. [ITU-T X.520] defines a set of general useable attribute types. Already defined attribute types should be used whenever possible. Additional attribute types may be defined as required by individual specifications.

Individual usages of this Recommendation will have to provide a mapping between this information model and the actual data base structure. This mapping becomes easy if the information is maintained in a lightweight directory access protocol (LDAP) directory or in a secure directory based on the specifications in the [ITU-T X.500-series].

6.5 Basic access control principles

The purpose of this clause is to provide an overview of the general principles for establishing access control for telebiometrics. Traditional access control is mostly concerned with the right or refusal of access to data, based on some permanent parameters. This Recommendation takes an extended approach by also considering the need-to-know aspects. This is done by taking the service approach as discussed in clause 6.3. To perform a particular operation, an accessor needs to have privilege permitting access to the relevant access service and privilege permitting access to the necessary information.

This privilege includes access to objects of one or more object classes, possibly limited to some named objects. The type of operation that may be performed, may be different for different object classes and named objects.

The operations on objects may include operation on individual attributes and attribute values. The permitted operations may be different for different types of attributes.

6.6 Relationship to other access control schemes

There are various types of access controls to cover different access control requirements. It is the intension here to briefly describe various access control schemes and to relate them to ACT.

6.6.1 Basic access control as defined by ITU-T X.501

The basic access control as defined by [ITU-T X.501] is used for protecting information in a directory as defined by [ITU-T X.500-series]. It provides for elaborate access control lists that specifies, in detail, how and what different users are allowed to access. It differs from this Recommendation by providing only for the right-to-know, but not for the need-to-know.

6.6.2 Rule-based access control

Both [ITU-T X.501] and [b-ITU-T X.841] define a type of rule-based access control. In this type of access control, the data to be protected are tagged with information about what protection is required, while the accessing users have certified information associated in an access request that specifies the level of clearance they have with respect to accessing certain information. This concept differs from this Recommendation by requiring tagging of stored data items, and by only providing for right-to-know, but not for need-to-know.

6.6.3 Role-based access control as defined for smart grid

Role-based access control as specified in [b-IEC 62351-8] focuses on users and the jobs users perform. A role is a collection of rights to objects (actions that can be performed at certain targets). A user may have one or several roles. For access control, a role is a kind of intermediary that reduces the amount of information needed in the access control list (ACL) by decreasing the granularity of access control information. Permissions to objects of the system are not listed for each user separately, but users are given roles, and rights of each role are only described once.

6.6.4 Attribute-based access control

Attribute-based access control (ABAC) is a logical access control model that is distinguishable because it controls access to objects by evaluating rules against the attributes of entities (subject and object), operations, and the environment relevant to a request. ABAC systems are capable of enforcing both discretionary access control and mandatory access control concepts. ABAC enables precise access control, which allows for a higher number of discrete inputs into an access control decision, providing a greater set of possible combinations of those variables to reflect a larger and more definitive set of possible rules to express policies.

For a good introduction to ABAC, see [b-NIST 800-162].

6.7 Protocols overview

6.7.1 Privilege assessment protocol

The privilege assessment protocol comprises a set of cryptographic message syntax (CMS) content types. Each type of access requires a request content type and a result content type.

An instance of a content type is transmitted using CMS as profiled in Annex B. A formal ASN.1 module is provided in Annex C.

6.7.2 Privilege assignment protocol

The privilege assignment protocol is used for transmitting attribute certificates either between SOAs or from an SOA to the privilege holder.

A single pair of content types is defined for this protocol: one content type for forwarding privilege in the form of attribute certificates, and one content type for reporting the outcome.

An instance of a content type is transmitted using CMS as profiled in Annex B. A formal ASN.1 module is provided in Annex C.

6.8 Use of CMS

A profile for telebiometrics use of CMS is provided in Annex B.

To ensure that the source of information is properly authenticated, contents of types defined by this Recommendation shall be encapsulated in an instance of the **signedData** content type. As sensitive information may be transmitted, it is recommended also to encapsulate it in an instance of the **envelopedData** content type. The **ct-autEnvelopedData** content type is not used by this Recommendation.

6.9 Public-key certificate considerations

An attribute certificate shall be signed by the issuer using its private key and it is to be verified by the use of the corresponding public-key certificate issued to the attribute certificate issuer.

In principle, the same private key could be used for signing the CMS message using the **signedData** content type, which would ease the verification process. However, there are security concerns using the same private key for different purposes. The use of different private keys for the two purposes should be considered, but is not mandated by this Recommendation.

7 Provision of privilege information

7.1 Use of attribute certificates

[ITU-T X.509] allows both public-key certificates and attribute certificates to carry privilege information. In both cases, the privilege specifications are carried in attributes as defined by [ITU-T X.501]. Attribute types for this purpose are distinct from attribute types used for modelling information about objects. While attribute types defined for carrying information about objects should be kept as simple as possible, attribute types for carrying privilege information will, by their nature, be rather complex.

When using an attribute certificate to carry privilege information:

- a) the **holder** component identifies the entity to which privileges are to be assigned. When a privilege holder presents this attribute, certificate holding privileges to a privilege verifier, the privilege verifier shall authenticate the accessor to verify that the accessor is actually the privilege holder of the attribute certificate;
- b) the **issuer** component shall hold the name of the SOA or the name of an attribute authority (AA) that has been delegated to assign privileges. The privilege verifier shall also obtain and validate the public-key certificate of the issuer to validate the signature on the attribute certificate;
- c) the **attributes** component shall hold an attribute of the type **accessService**, as defined in clause 7.3.

The attribute certificate shall be signed by the SOA that approved the privilege or the AA to which issuing has been delegated.

Validation will be simplified if the holder and the issuer have public-key certificates issued by the same certification authority (CA).

7.2 Use of public-key certificates

When using a public-key certificate to carry privilege information:

- a) the **subject** component identifies the accessor to which privileges have been assigned. When an accessor presents this public-key certificate holding privileges to a privilege verifier, the privilege verifier shall authenticate the accessor;
- b) the **issuer** component shall hold the distinguished name of the CA that is responsible for issuing the public-key certificate;
- c) the **subjectDirectoryAttributes** extension shall hold an instance of the **accessService** attribute type (see clause 7.3).

7.3 The access service attribute type

7.3.1 Access service attribute syntax

An attribute of type `accessService` is intended to be included in the `attributes` component of an attribute certificate or in the `subjectDirectoryAttributes` extension of a public-key certificate. It has the following syntax:

```
AccessService ATTRIBUTE ::= {  
  WITH SYNTAX AccessService  
  ID id-at-accessService }
```

An attribute of type `AccessService` provides privilege information to allow a privilege verifier to validate whether an access request should be honoured or not. It is a multi-valued attribute type allowing multiple access service types and associate permissions to be included in the same attribute.

An entity cannot use a service that is not included in this attribute.

The `accessService` attribute type has the following syntax:

```
AccessService ::= SEQUENCE {  
  serviceId OBJECT IDENTIFIER,  
  objectDef SEQUENCE SIZE (1..MAX) OF ObjectSel,  
  ... }
```

The components of a value of the `AccessService` data type are:

- the `serviceId` component shall identify the type of access service for which the accessor has privilege;
- the `objectDef` component shall specify the object classes for which privilege is assigned to the holder of the attribute certificate for the particular service type. It shall have one element for each object class for which privilege has been assigned. For this access service, the privilege holder has no access to object classes not listed by the `objectDef` component.

7.3.2 Selection of objects

The selection of objects for which the accessor has privileges are specified by an instance of the `ObjectSel` data type.

```
ObjectSel ::= SEQUENCE {  
  objecClass OBJECT-CLASS.&id,  
  objSelect CHOICE {  
    allObj [0] TargetSelect,  
    objectNames [1] SEQUENCE SIZE (1..MAX) OF SEQUENCE {  
      object CHOICE {  
        names [1] SEQUENCE SIZE (1..MAX) OF DistinguishedName,  
        subtree [2] DistinguishedName,  
        ... },  
      select TargetSelect,  
      ... },  
      ... },  
      ... }
```

A value of the `objectSel` data type shall specify the privilege for each object class for which privilege has been assigned for the accessed service type. It has the following components:

- the `objectClass` component shall specify the object class for which privileges are assigned;
- the `objSelect` component shall specify what objects of the object class for which privilege has been assigned. It has two alternatives:
 - the `allObj` alternative shall be taken if the assigned privileges apply equally to all objects of the class. It shall hold an instance of the `TargetSelect` data type;