

International Telecommunication Union

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

X.1089

(05/2008)

SERIES X: DATA NETWORKS, OPEN SYSTEM
COMMUNICATIONS AND SECURITY

Telecommunication security

Telebiometrics authentication infrastructure (TAI)

Recommendation ITU-T X.1089

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.1089

Telebiometrics authentication infrastructure (TAI)

Summary

Recommendation ITU-T X.1089 defines an authentication infrastructure, using a range of biometric certificates, for remote authentication of human beings. It extends Recommendation ITU-T X.509 *Public-key and attribute certificate frameworks* and ISO/IEC 24761 *Authentication context for biometrics*. The combination of the X.509 extensions and telecommunications and biometrics is called the telebiometrics authentication infrastructure (TAI). It can be used in authentication applications with or without a public key infrastructure (PKI) and/or a privilege management infrastructure (PMI) based on Recommendation ITU-T X.509, but would normally be used with both. It defines biometric extension fields for use in X.509 certificates, to produce biometric certificates. An important part of this Recommendation is to recognize and provide for biometric devices and associated software to operate at different (certified) security levels, depending on the needs of the application that is being accessed.

Source

Recommendation ITU-T X.1089 was approved on 29 May 2008 by ITU-T Study Group 17 (2005-2008) under Recommendation ITU-T A.8 procedures.

Keywords

Authentication, biometric certificate, biometric policy certification, telebiometrics.

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 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 2009

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

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	4
5	Notation and encodings	5
6	Authorities involved in the telebiometrics authentication infrastructure	5
6.1	Operation of a BCA, revocation and processing of a BC.....	5
6.2	Operation of a TBA, revocation and processing of a BDC or BPC	6
7	Flow of information in the TAI	7
7.1	Scenarios.....	7
7.2	Client side verification	7
7.3	Server side verification.....	8
8	Biometric certificate	8
9	Biometric policy certificate	9
10	Biometric device certificate.....	11
11	TAI extensions defined for X.509	12
11.1	Extension used in a BC to index a PKC	12
11.2	TAI extensions defined for use with PMI	12
11.3	Extension used in the BC for cryptographic key generation.....	12
11.4	Biometric certificate index extension.....	12
11.5	Security level of privilege extension	13
11.6	BPC extension for a BDC.....	14
	Annex A – Complete formal ASN.1 specifications.....	15
	Appendix I – Examples of possible security level lists	19
	Bibliography.....	21

Introduction

Information security plays an increasingly important role in our daily lives. Many efforts have been made to develop an information system that can accurately authenticate, properly authorize, and efficiently audit legitimate users. Among these activities, authentication is the first and most critical link in the security chain. Authentication is a process that verifies a user's identity. As an emerging authentication technique, biometrics authentication is attracting more and more attention.

For more information on the problems and processes involved in biometric authentication (also called biometric verification), see [b-ISO/IEC TR 24741]. For more information on the use of multiple biometrics and the way the results of several comparisons can be combined (multimodal fusion), see [b-ISO/IEC TR 24722].

This Recommendation defines an authentication infrastructure that uses biometric authentication to authenticate a client to a server across a network – the telebiometrics authentication infrastructure (the TAI).

[ITU-T X.509] *Public-key and attribute certificate frameworks* has for many years provided an established base for the use of public keys with certificate chaining to provide a public key infrastructure (PKI).

It defines both public key certificates and attribute certificates. The former supports the PKI (sometimes referred to as PKIX, which is the IETF profiling of [ITU-T X.509]). The latter provides an open-ended mechanism for certificates using the abstract syntax notation one (ASN.1) extension mechanisms. Attribute certificates have many potential uses. They can and do form the basis of the privilege management infrastructure, using the appropriate extensions.

In this Recommendation, further extensions are defined for the X.509 attribute certifications to provide biometric certificates and biometric policy certificates, and to recognize the existence of certification authorities related to the issuing of these.

[ISO/IEC 24761] *Authentication context for biometrics* (ACBio) introduces the concept of a biometric processing unit (BPU), that is, hardware and associated software related to a biometric capture device. In ACBio, a BPU operates at a single security level, and the processing it performs is accompanied by a certified report of the result it has produced (including a hash of the inputs and outputs of the processing where appropriate). Those reports are made available to the entity that eventually takes decisions on the granting of various privileges to a human user.

In ACBio, the BPU consists of the totality of a biometric capture device and the associated processing of the raw data and matching with a previously captured biometric, with all stages being potentially distributed to different systems across a network. In the TAI, the device is kept distinct from the further processing, as there is a distinction to be made between the security levels that can be provided by a device and the levels that can be provided by the use of different processing or matching software and algorithms.

This Recommendation extends both X.509 and ACBio and uses the concepts in [ISO/IEC 19785-1] *Common Biometric Exchange Formats Framework – Part 1: Data element specification* and [ISO/IEC 19785-3] *Common Biometric Exchange Formats Framework – Part 3: Patron format specifications* together with the biometric data formats registered with the International Biometric Industry Association (IBIA – see URL <http://www.ibia.org>) that carry biometric data such as finger-print images, iris images, finger-minutiae, etc.

The concept drawn from [ISO/IEC 19785-1] is of a biometric data block, also called a biometric template that carries this biometric data for comparison purposes. There is no restriction on the type of biometric template used, either standardized or vendor-specific, provided it is registered with the IBIA in their CBEFF Registry as a biometric data block.

The concept drawn from [ISO/IEC 19785-3] is of a biometric template with associated metadata, sometimes called a biometric information record or a patron format. In this Recommendation, it is called a biometric information template (BIT), following the terminology in [b-ISO/IEC 7816-11] *Integrated circuit cards – Part 11: Personal verification through biometric methods*. There is no restriction on the types of BIT that can be used, but the BIT in [b-ISO/IEC 7816-11] is recommended.

In terms of [ITU-T X.509], this Recommendation defines further extensions for use in attribute certificates that carry biometric information. The two most important are the biometric certificate and the biometric policy certificate.

This Recommendation introduces the fundamental concept that a biometric processing unit (BPU) (hardware devices, supporting software, and fusion mechanisms when multiple biometrics are in use) can operate at any one of several security levels. These relate partly to the availability of liveness testing, and the setting of thresholds for a uni-modal biometric comparison, but more importantly to the way in which biometric fusion scores are combined (see [b-ISO/IEC TR 24722]). For example, a low security level might accept a claimant if any of the fingerprints or iris scans were positive (above a perhaps low threshold), a high security level might require that all scores were positive (above a perhaps high threshold), and require liveness testing in any associated biometric devices.

It also recognizes that a client can interact with a server that requires privileges for the operations that the client wishes to perform. In some cases, such as reading a Web page from a Web server, it is possible that no privileges are required (the information is public). In other cases, the same server may have private areas where privileged access is needed. A still higher set of privileges (and hence a higher security level for authentication) may be needed if the client wishes to change the data on the website, or for a technician taking remedial action or uploading new software. Again, for access to a bank account, different privileges may be needed for reading account details, for transferring money, and for maintaining the accounts database. So for transactions that a client wishes to perform with a given server, there can be many different sets of privileges needed, depending on the nature of the transaction.

A key concept in the TAI is that once the privileges required are known by the presentation of an attribute certificate (AC), a security level for the authentication process can be obtained from that AC, and that a BPU can operate at different (certified) security levels. This Recommendation does not define a set of standardized security levels, but Appendix I provides the basis for a template that would contain such definitions, and may be subject to subsequent standardization. The precise definition of security levels is currently a matter for agreement between the BPU, the authority that issues the biometric policy certificate, and the applications that will use the related reports and certificates.

The focus of the TAI is primarily on capture and comparison for verification (authentication) purposes, but the security levels used for capture and enrolment are equally important.

Two types of trusted third party (with trust chained through the certificate chains established by [ITU-T X.509]) are recognized in the telebiometrics authentication infrastructure (TAI).

The first type is a biometric certificate authority (BCA) concerned with enrolling users and issuing a biometric certificate that binds them to their biometric information. In general, a user may be issued with many different biometric certificates (using the same or different biometrics), for example from his employer for access control, from his library, from his sports club, or from his government (passports for border control). The stringency of the enrolment process and the security level needed for enrolment can vary, depending on the requirements of these different BCAs. The same hardware and software may (but need not) be capable of supporting enrolment and verification for all these different BCAs, depending on the security level at which it operates.

The second type of trusted third party is the telebiometrics authority (TBA) that evaluates the security of biometric devices and issues biometric device certificates (BDCs) for a biometric device and biometric policy certificates (BPCs) for the security levels that can be provided by that device in combination with the software that performs the subsequent processing of the raw data, fusion, and/or matching (a biometric processing UNIT (BPU)). Any given BPU may have been issued with multiple BDCs and BPCs, issued by different TBAs that may perform more or less rigorous checks on the extent to which the device and processing software is protected from tampering, hacking, or spoofing.

The normal sequence of events is:

- a) a trusted third party (possibly through certificate chaining) – a TBA – will issue a biometric policy certificate asserting that a BPU (also called a client) is resistant to tampering, and is capable of operating at stated security levels defined in a biometric policy list;
- b) the client (all or part of a BPU) first establishes a secure channel with an SP and sends an attribute certificate (AC), with a privilege management infrastructure (PMI) extension provided by the claimant (the human being wishing to perform a transaction with some service provider), to the service provider (SP); this contains the privileges being requested (and that are needed for the transaction that the claimant wishes to perform);

NOTE 1 – If the secure channel between the client and the SP is terminated, or if validation fails at any step, then the sequence of events described below is aborted.
- c) the SP checks with a trusted privilege verifier (PV) that the AC is valid and that the claimant has access to the requested privileges once an identity verifier (IDV) is satisfied that the claimed identity in the AC has been established, using biometric verification at an appropriate security level (which can be extracted from the biometric extension in the AC);

NOTE 2 – The communication between the SP and the PV will normally be over a secure channel which is terminated once privilege verification is complete.
- d) the SP requests the BPU that includes the client to perform the biometric authentication of the claimant at a specified security level, determined from the supplied AC;

NOTE 3 – Enrolment and vetting procedures and other identity management issues are outside the scope of this Recommendation.
- e) an interaction with the claimant occurs within the BPU, with processing at the requested security level (to support enrolment or authentication); ACBio reports will be produced and used during both the enrolment and the authentication processes and sent to the SP with the results of the biometric verification;
- f) the SP sends these reports and the result to an identity verifier (IDV) over a secure channel that will verify the identity of the claimant;
- g) on satisfactory completion of these processes (and if the secure channel with the client is still intact), the SP will provide the requested services according to the established privileges.

This summarizes the telebiometrics authentication infrastructure (TAI).

A more detailed description of the various stages and interactions is provided in clause 7.

Annex A (normative) contains the complete ASN.1 module definition that supports the data structures specified in this Recommendation. Parts of that definition are included in various clauses to help with the understanding of the English text. If differences exist, it is a defect, but Annex A takes precedence.

Examples of (and guidance on) possible security level definitions are given in Appendix I.

Recommendation ITU-T X.1089

Telebiometrics authentication infrastructure (TAI)

1 Scope

This Recommendation defines a security framework that enhances the security framework provided by a public key infrastructure (PKI) and a privilege management infrastructure (PMI) to provide authentication using biometric certificates and biometric policy certificates to allow authentication at an appropriate security level, depending on the privileges a client needs for the actions or transactions that the client desires to undertake.

It is called the telebiometrics authentication infrastructure (TAI). The specification includes:

- the flow of information in the TAI (see clause 7);
- the definition of a biometric certificate (BC) (see clause 8) issued by a biometric certificate authority (BCA);
- the definition of a biometric policy certificate (BPC) (see clause 9) issued by a telebiometrics authority (TBA);
- the definition of a biometric device certificate (BDC) (see clause 10) issued by a telebiometrics authority (TBA); and
- the definition of extensions for general use in [ITU-T X.509] attribute certificates (see clause 11).

This Recommendation does not provide a full specification of the TAI, but forms the basis for a full specification. A full specification would need further standardization of the meaning of different security levels.

NOTE – Appendix I provides an outline of a possible definition of such security levels.

This Recommendation defines the issuance, management, usage, and revocation of biometric certificates by reference to [ITU-T X.509].

The specification of [ITU-T X.509] attribute certificate extensions in clause 11 allows the TAI specifications to be seamlessly combined with a public key infrastructure (PKI) or privilege management infrastructure (PMI), and the use of the reports defined for the authentication context for biometrics (ACBio).

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.509] Recommendation ITU-T X.509 (2008) | ISO/IEC 9594-8:2008, *Information technology – Open Systems Interconnection – The Directory: Public-key and attribute certificate frameworks*.

[ITU-T X.520] Recommendation ITU-T X.520 (2005) | ISO/IEC 9594-6:2005, *Information technology – Open Systems Interconnection – The Directory: Selected attribute types*.

- [ITU-T X.680] Recommendation ITU-T X.680 (2002) | ISO/IEC 8824-1:2002, *Information technology – Abstract Syntax Notation One (ASN.1): Specification of basic notation.*
- [ITU-T X.681] Recommendation ITU-T X.681 (2002) | ISO/IEC 8824-2:2002, *Information technology – Abstract Syntax Notation One (ASN.1): Information object specification.*
- [ITU-T X.682] Recommendation ITU-T X.682 (2002) | ISO/IEC 8824-3:2002, *Information technology – Abstract Syntax Notation One (ASN.1): Constraint specification.*
- [ITU-T X.683] Recommendation ITU-T X.683 (2002) | ISO/IEC 8824-4:2002, *Information technology – Abstract Syntax Notation One (ASN.1): Parameterization of ASN.1 specifications.*
- [ITU-T X.690] Recommendation ITU-T X.690 (2002) | ISO/IEC 8825-1:2002, *Information technology – ASN.1 encoding rules: Specification of Basic Encoding Rules (BER), Canonical Encoding Rules (CER) and Distinguished Encoding Rules (DER).*
- [ITU-T X.1083] Recommendation ITU-T X.1083 (2007) | ISO/IEC 24708:2008, *Information technology – Biometrics – BioAPI interworking protocol.*
- [ISO/IEC 19784-1] ISO/IEC 19784-1:2006, *Information technology – Biometric application programming interface – Part 1: BioAPI specification.*
- [ISO/IEC 19785-1] ISO/IEC 19785-1:2006, *Information technology – Common Biometric Exchange Formats Framework – Part 1: Data element specification.*
- [ISO/IEC 19785-2] ISO/IEC 19785-2:2006, *Information technology – Common Biometric Exchange Formats Framework – Part 2: Procedures for the operation of the Biometric Registration Authority.*
- [ISO/IEC 19785-3] ISO/IEC 19785-3:2007, *Information technology – Common Biometric Exchange Formats Framework – Part 3: Patron format specifications.*
- [ISO/IEC 24761] ISO/IEC 24761:2009, *Information technology – Security techniques – Authentication context for biometrics (ACBio).*
- [IETF RFC 3986] IETF RFC 3986 (2005), *Uniform Resource Identifier (URI): Generic Syntax.*

3 Definitions

3.1 Terms defined elsewhere

This Recommendation uses the following terms defined elsewhere:

- 3.1.1 **attribute certificate** [ITU-T X.509]
- 3.1.2 **biometric information record** [ISO/IEC 19785-1]
- 3.1.3 **biometric processing unit** [ISO/IEC 24761]
- 3.1.4 **biometric template** [ISO/IEC 19785-1]
- 3.1.5 **certificate revocation list** [ITU-T X.509]
- 3.1.6 **false match rate** [ISO/IEC 19784-1]
- 3.1.7 **privilege management infrastructure** [ITU-T X.509]
- 3.1.8 **public key certificate** [ITU-T X.509]
- 3.1.9 **public key infrastructure** [ITU-T X.509]