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/.

CONTENTS

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]

3.2 Terms defined in this Recommendation

This Recommendation defines the following terms:

3.2.1 biometric certificate (BC): A signed data structure binding a user to one of his/her BITs, issued by a biometric certificate authority, and containing the security levels used in the enrolment process.

NOTE – Examples of the semantic content of biometric certificates are the data contained in biometric passports, biometric identity cards or biometric driving licences, or stored in equivalent databases. However, these currently (2008) do not use the standardized formats for a BC defined in this Recommendation, and do not currently identify the security level of the enrolment process.

3.2.2 biometric certificate authority (BCA): A trusted third party that a user can enrol with and that issues or records a biometric certificate. It certifies the binding relationship between the holder of a BC and his/her BIT, using a digital signature.

NOTE 1 – The BCA will normally perform checks on the identity of the user before issuing a BC containing the BIT of that user.

NOTE 2 – The BIT may be included in the certificate, or there may simply be a URI that points to where it is stored.

3.2.3 biometric certificate revocation list (BCRL): A revocation list that includes reference to a biometric certificate.

3.2.4 biometric device: A client or server side device that includes biometric hardware and the associated software and that processes human biometric data to complete all or part of the authentication of a person.

NOTE 1 – This forms the first part (or possibly all) of an ACBio BPU.

NOTE 2 – The BDC is issued to either the client side device or to the server side device, depending on which does the biometric processing and comparison.

3.2.5 biometric device certificate (BDC): A signed data structure (produced by the vendor and authenticated by a TBA) storing the parameters and operation of a secure part of a biometric device.

NOTE 1 – The TBA authenticates (after testing, etc.) that the device can be trusted to provide a given set of security levels in its operation, related mainly to liveness testing and to its resistance to tampering.

NOTE 2 – A secure part of a biometric device normally relates to memory that contains a certificate and performs a capture or other biometric processing function, returning signed data, and that cannot be later modified in any way (read-only memory).

3.2.6 biometric information template (BIT): A data structure used in a BC that contains a biometric template and metadata.

NOTE – This is referred to in [ISO/IEC 19785-1] as a patron format.

3.2.7 biometric policy: A detailed specification containing a list of security levels that a biometric device or BPU can support, and the parameters and actions used by the device or BPU for each level.

NOTE – Examples are the dots per inch used for image capture, quality thresholds for acceptance or rejection of an image, liveness testing to resist spoofing, thresholds applied to produce a comparison score, and the way in which fusion is performed in multi-modal operation. When the client supports multiple biometric modalities, it needs to be determined which modality to use, and how fusion is to be performed if multiple modalities are used. Biometric policy and associated security levels are not standardized in this Recommendation.

3.2.8 biometric policy certificate (BPC): A data structure containing the biometric policy of a biometric device or BPU that has been verified by and is digitally signed and issued by a TBA.

NOTE – Verification means ensuring that the biometric device or BPU has sufficient security mechanisms to ensure that it will reliably perform, without danger of tampering, to the security levels specified in the security policy.

3.2.9 claimant: The human being seeking a biometric verification of his/her identity in order to claim privileges or authorization for an interaction with an SP.

3.2.10 identity verifier (IDV): The entity that makes the determination as to whether or not the identity asserted by a claimant is correct in a biometric verification process performed by one or more biometric systems and fusion processes.

NOTE – The IDV, supported by biometric devices and processes, is that part of the TAI that has the primary responsibility for authentication using biometrics. The final decision of the IDV is based on the TAI certificates and ACBio reports returned from the various parts of the verification process.

3.2.11 privilege verifier (PV): An entity that validates an AC containing a PMI extension (see [ITU-T X.509]) and a biometric extension.

NOTE – A PV verifies that the claimant (holder of the AC) will have access to the requested privileges once an 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).

3.2.12 security level: The security level is an index to a description (in a BPC) of the resistance capability of a biometric system to attacks due to spoofing, masquerade, false matches or false enrolments.

NOTE 1 – The higher the security level, the higher the confidence is of the enrolment process or the verification result of a user's identity.

NOTE 2 – This Recommendation does not define specific security levels, but it is recorded in certificates as an integer in the range 1 (lowest) to 100 (highest).

3.2.13 service provider (SP): Any entity or system on a network that provides a service to a remote client.

NOTE – Examples are a Web server, a social network provider, a store selling books or electronic goods over a network, a bank providing access to an account, and many others.

3.2.14 TAI application: An application or service using the TAI to provide user authentication, authorization and verification using biometrics and associated certificates.

NOTE – Associated certificates refer to biometric certificates, biometric device certificates and biometric policy certificates.

3.2.15 telebiometrics authentication infrastructure (TAI): An infrastructure supporting the management and use of biometric certificates, biometric device certificates, biometric policy certificates, and, possibly, public key certificates and privilege management certificates, to provide biometrics-based authentication and possibly authorization services.

3.2.16 telebiometrics authority (TBA): A trusted third party, responsible for issuing a biometric device certificate and/or a biometric policy certificate, after appropriate inspection of the operation of the device and/or BPU and the associated statement of biometric policy.

3.2.17 underlying biometric process: Those processing activities performed by a biometric device or by a BPU that result in the presentation of TAI certificates that can be used to provide authentication or privilege authorization.

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

AC	Attribute Certificate
ASN.1	Abstract Syntax Notation One (see [ITU-T X.680])
BC	Biometric Certificate
BCA	Biometric Certificate Authority

BCRL	Biometric Certificate Revocation List
BDC	Biometric Device Certificate
BIT	Biometric Information Template
BPC	Biometric Policy Certificate
BPU	Biometric Processing Unit
CBEFF	Common Biometric Exchange Formats Framework
FMR	False Match Rate
IBIA	International Biometric Industry Association (see URL http://www.ibia.org/)
IDV	Identity Verifier
PKC	Public Key Certificate
PKI	Public Key Infrastructure
PMI	Privilege Management Infrastructure
PV	Privilege Verifier
SP	Service Provider
TAI	Telebiometrics Authentication Infrastructure
TBA	Telebiometrics Authority
URI	Uniform Resource Identifier

5 Notation and encodings

5.1 This Recommendation uses the ASN.1 notation specified in [ITU-T X.680], [ITU-T X.681], [ITU-T X.682], and [ITU-T X.683]. These definitions (in accordance with normal practice) are in this `example-ASN.1` text when in line, or, for a block of ASN.1 definitions, are:

```
First line
      Second line
      End
```

5.2 This Recommendation uses the ASN.1 definitions imported from [ITU-T X.509], [ITU-T X.1083], [ISO/IEC 19785-3] and [ISO/IEC 24761].

5.3 The ASN.1 Distinguished Encoding Rules specified in [ITU-T X.690] shall be used for all encodings of biometric certificates, biometric device certificates, biometric policy certificates, and [ITU-T X.509] attribute certificate extensions, including all imported types used in these definitions.

NOTE – These encoding rules produce a self-delimiting encoding that is an integral number of octets.

6 Authorities involved in the telebiometrics authentication infrastructure

There are two types of authority (of which there may be multiple instances) involved in the operation of the TAI. The first of these is a BCA that issues BCs. The second is a TBA that issues BPCs and BDCs. These are trusted third parties that issue certificates. (Chaining of trust via the normal [ITU-T X.509] mechanisms applies.)

6.1 Operation of a BCA, revocation and processing of a BC

6.1.1 A BCA is a trusted third party. It can only remain trusted if the procedures it uses for the issue of BCs are robust and secure. Thus it is not a trivial activity.

6.1.2 A BCA issues BCs that bind a user to one or more of his/her biometrics after an enrolment process with that BCA. A user may have multiple BCs, issued by the same or by different BCAs, depending on the biometric(s) used for enrolment, the security level of the enrolment process, and the extent of checking the user's identity at enrolment time.

6.1.3 The enrolment of the user's biometrics can include capturing the user's biometric, extracting feature data, generation of a biometric template. The BCA uses an applicant's biometric template (or a path to it) and the information required to support the registration in order to generate the BC for the user.

6.1.4 The extent of checking of the existence of a real human user and his/her "persona" can vary from one BCA to another. It is possible to use the existence of bank and credit card accounts, evidence of residence, birth records, statements from neighbours, etc., during the enrolment process (to help guard against multiple enrolments and identity theft), but less checking may be used for enrolment with a sports club or a library. The precise definition of security levels during enrolment is outside the scope of this Recommendation, but will vary depending on the nature of the BCA and the intended application. It is possible for a BCA to accept as evidence of identity a BC issued by a different BCA (usually enrolling at a higher security level).

NOTE – If evidence of identity used in enrolment is retained after the BC is issued, this should be regarded as private information, and privacy laws will normally require that this is held securely and not released. Another option is to delete all such private records after issuing the BC, keeping only a record of the type of the checks that have been (successfully) performed.

6.1.5 In general, the privileges a user will be able to gain from use of a BC will depend on both of the security level of the BPU used during enrolment, and on the security level of the BPU used during verification, and on the AC supplied by the claimant when trying to obtain services from an SP.

6.1.6 The operation of a BCA may require a large amount of checking and vetting (which would normally be required if the BCA was a government department, and the BC was to be used in sensitive areas such as border control, driving licences, or identity cards). However, if the BCA is issuing a BC for limited commercial purposes, the checking and vetting may be less. It could also be done by a simple reference to a BC issued by a BCA employing stronger checking and vetting procedures.

NOTE – A BC will normally contain some (perhaps randomly allocated) identification that will be recorded for audit purposes whenever the BC is used. The existence of multiple BCAs and multiple BCs reduces the privacy concerns over the tracking of individuals by their use of a single BC and a single identification issued by a single BCA.

6.1.7 A BC can be revoked using a BCRL. The certificate revocation list mechanism is defined in clause 8 of [ITU-T X.509].

NOTE – The TAI assumes that all applications using BCs will use certificate revocation lists in an appropriate manner. However, their precise use is outside the scope of this Recommendation.

6.1.8 The certificate path processing for BC certificates is the same as that used for public-key certificates – see clause 10 of [ITU-T X.509].

6.2 Operation of a TBA, revocation and processing of a BDC or BPC

6.2.1 A TBA is a trusted third party. It can only remain trusted if the procedures it uses for the issue of BDCs and BPCs are robust and secure, and ensure adequate testing and verification of the device or BPU to which the certificate is issued. Thus it is not a trivial activity.

6.2.2 In the case of a BDC, issuing a BDC will involve checking that the manufacturer of the device has provided some secure write-once memory that can securely perform the operations that it is certifying, at the security levels that are being offered. The BDC is also needed in order for the IDV to validate the ACBio reports produced by the device.

NOTE – The device may be a mobile phone, a card in a PC, or any other biometric device operating remotely. In the case of point-of-sale terminals and border control devices, assessment may be based on both supervision and use, and on the inherent security of the write-once memory providing biometric verification and network transmission of the result.

6.2.3 In the case of a BPC (typically covering one or more devices together with possibly remote software modules), the TBA will need to be assured that all devices used by the BPU are certified, and that the security mechanisms supporting remote software modules and communications within the BPU are sufficient for the claimed security levels. The BPC is used by the PV to ensure and determine the security level for the BPU authentication, depending on the privileges that the client requires for the intended actions.

NOTE – The mechanisms for checking this, the precise form of a BPU claim to provide specified security levels when requesting a BPC, and the assessment of those claims are outside the scope of this Recommendation.

6.2.4 A BDC or BPC can be revoked using a BCRL. The certificate revocation list mechanism is defined in clause 8 of [ITU-T X.509].

NOTE – The TAI assumes that all applications using BCs will use certificate revocation lists in an appropriate manner. However, their precise use is outside the scope of this Recommendation.

6.2.5 The certificate path processing for BDCs and BPCs is the same as that used for public-key certificates – see clause 10 of [ITU-T X.509].

7 Flow of information in the TAI

The TAI uses the `BPUReportInformation` defined in ACBio from a BPU, which is a certified report of the processing (and the security levels employed) of a BPU in biometric operation.

7.1 Scenarios

There are two scenarios that are supported. These are described in clauses 7.2 and 7.3.

In both scenarios, a biometric device at the client side acquires user's biometric live biometric data and sends it with the claimant's biometric certificate to an IDV for the biometric identification verification. It also sends the user's privilege attribute information (i.e., AC) to a PV to declare the user's privilege. The IDV generates an identity authentication result based on the biometric parameter information acquired from a biometric policy certificate for all the related biometric processing.

7.2 Client side verification

7.2.1 The BPU (including a biometric capture device and associated software) is at the client side of the interaction, and signal processing and comparison sub-processes are all within the client (typically in a PC or mobile phone) which is fully trusted and certificated by a TBA. It operates at a defined security level, obtained from an AC provided by the claimant (and verified by a PV through the PS) for the actions the claimant wishes to perform.

7.2.2 The client obtains an AC from the claimant, and sends it over a secure link (established between the client and the server, using a PKI infrastructure) to the SP, which interacts securely with a PV to verify it, and informs the client of success or failure of the verification process over the secure link. The AC contains the security level at which the BPU containing the client is required to operate for this AC. The client sends to the verifier side the unique identifier of some security level, which is used to acquire the corresponding biometric parameters and the latter are sent back to the client for further use in the capture process and biometric processing. The result of the biometric processing will be finally accepted or rejected by the IDV.

7.2.3 The client side BPU completes the verification process (using the biometric parameters for the security level extracted from the AC) and sends over the secure link the results of the verification process based on enrolment data provided by the claimant in an BC, possibly stored on a smart-card or possibly in the phone or PC itself. It includes all relevant certificates (including the BPC of the BPU, any necessary BDCs, and the BPU report) to the SP.

7.2.4 The SP sends the certificates and reports to an IDV over a secure channel, and if it receives a positive response, it allows the transaction permitted by the granted privileges, provided the secure channel with the client has not been disconnected.

7.2.5 These privileges will remain available to the client over the secure link, so long as that secure link remains established.

7.3 Server side verification

This differs from the client side verification only if that part of the BPU verification (typically the matching part) forms part of or is accessed by the SP. In this case, the SP needs to receive the BC (containing the BIT) from the client.

NOTE – In some smart-card applications, the client side processing is called "match-on-card", and the server side processing is called "match-off-card".

8 Biometric certificate

8.1 A biometric certificate is a signed [ITU-T X.509] attribute certificate with at least one attribute that carries a BIT.

8.2 The ASN.1 definition of the BC is as follows:

```
BiometricCertificate ::= SIGNED { BiometricCertificateInfo }
      -- Signed by a BCA

BiometricCertificateInfo ::= AttributeCertificateInfo -- see X.509
      (WITH COMPONENTS {
            ...,
            attributes (SIZE(1..MAX))})
      -- the attributes in BiometricCertificateInfo shall contain at
      -- least one BIT attribute – see 8.4 to 8.6.
      -- Multiple BIT attributes can be included,
      -- if the associated Biometric Information Templates are all
      -- enrolment data with the same BCA.
```

8.3 A BIT is used in biometric-based user authentication as input to the biometric matching process. In other standards, the contents of the `BiometricInformationTemplate` type used below is called a biometric information record, or a patron format. The BIT attribute may contain the patron format itself or a URI (see [IETF RFC 3986]) that references it, but should always contain a signature of the encoding, using the example of the recommended BIT attribute below. The BIT has to be supported by integrity mechanisms, and should also have confidentiality applied.

8.4 It is recommended that the BIT attribute `biometricInformationTemplate` (see clause 8.6) that is defined using the BIT specified for use in on-card matching in CBEFF (see [ISO/IEC 19785-3], clause 11) be used (see below). Other BIT formats (patron formats) are defined in [ISO/IEC 19785-3] and others can be defined (and assigned object identifiers) either by other standards, trusted third parties or even the biometric device vendors or TAI applications. They can all be used with this Recommendation, provided there is a definition of a new attribute with its syntax and object identifier, for example:

```
otherbiometricInformationTemplate ATTRIBUTE ::= {
      WITH SYNTAX  OtherBIT
      ID           OID-of-other-BIT }
```

8.5 It is recommended (but not required) that, to promote interworking, all BITs (patron formats) should be registered (if not already registered) with the IBIA, but this is not a requirement. (See [ISO/IEC 19785-2] for registration procedures.)

8.6 The recommended BIT attribute is `biometricInformationTemplate`:

```
biometricInformationTemplate ATTRIBUTE ::= {
      WITH SYNTAX   BiometricInformationTemplateorPointer,
      ID            id-tai-at-BiometricInformationTemplate }
      -- See Annex A for the definition of ID values.

BiometricInformationTemplateorPointer ::= CHOICE{
      bcBiometricInformationTemplate  BCBiometricInformationTemplate,
      referenceToBCBiometricInformationTemplate
                                      URI -- Pointing to the BIT --,
                                      ... }
      -- The use of "..." means future extensions of this
      -- specification may add further alternatives, without changing
      -- the encoding of the currently listed alternatives

BCBiometricInformationTemplate ::=
      SIGNED {BCBiometricInformationTemplateContent}
      -- Signed by a BCA that may be different from the BCA
      -- signing the BC.

BCBiometricInformationTemplateContent ::= SEQUENCE{
      biometricTemplateVersion          BiometricTemplateVersion,
      biometricTemplateInfo             BiometricTemplateInfo,
      issuerDigitalSignatureAlgorithm   AlgorithmIdentifier
                                              {{SupportedAlgorithms}} OPTIONAL,
      bioTempIssuer                     BioTempIssuer  OPTIONAL }

BiometricTemplateVersion ::= INTEGER {v0(0)}(v0, ...)

BioTempIssuer ::= [0] SEQUENCE {
      issuerName             GeneralNames OPTIONAL,
      baseCertificateID [0]  IssuerSerial OPTIONAL,
      objectDigestInfo  [1]  ObjectDigestInfo OPTIONAL -- [b-ISO/IEC TR 24741] --}
```

The `biometricTemplateVersion` is the version of the BIT in the BC.

The types `GeneralNames`, `IssuerSerial`, `ObjectDigestInfo` and `AlgorithmIdentifier` are imported from [ITU-T X.509]. See Annex A for a definition of `URI`. This is a reference to a stored BIT.

8.7 The `biometrictemplateInfo` is the BIT data in the BC.

```
BiometricTemplateInfo ::= CHOICE {
      biometricTemplateInfo19785  BiometricInformationTemplate
                                  -- imported from ISO/IEC 19785-3 --,
                                        ...}
```

9 Biometric policy certificate

9.1 A BPC is a signed [ITU-T X.509] attribute certificate with at least one attribute that is a `bioSecLevelReference`.

9.2 The ASN.1 definition of the BPC is as follows:

```
BiometricPolicyCertificate ::=
      SIGNED {BiometricPolicyCertificateInfo}
      -- Signed by a TBA

BiometricPolicyCertificateInfo ::= AttributeCertificateInfo
      (WITH COMPONENTS {
      ...,
      attributes(SIZE(1..MAX))})
      -- the attributes in BiometricPolicyCertificateInfo shall
      -- contain at least one bioSecLevelReference attribute
```

```
bioSecLevelReference  ATTRIBUTE ::= {
      WITH SYNTAX        SecurityLevelBioReference
      ID                 id-tai-at-bioSecLevelReference }
```

9.3 The `SecurityLevelBioReference` contains information on the relation between the biometric algorithm parameters and a security level, authenticated by the TBA, called biometric policies. In the underlying biometric process, the BPC provides the authenticated parameters needed for assurance of the BPU activity. If there are more than one `bioSecLevelReference` included, they shall all have different values for the `securityLevelNum`.

```
SecurityLevelBioReference  ::=  SEQUENCE{
      securityLevelNum            INTEGER,
      securityLevelBioRef         SecurityLevelBioRef}
```

9.4 The `SecurityLevelBioReference` is a data structure which contains an identifier `SecurityLevelNum`, with the associated `SecurityLevelBioRef` containing the mapping of a security level identifier to information for that security level.

9.5 The specification of security levels and their semantics is out of the scope of this Recommendation. A particular security level references the biometric parameter information and other parameters in the biometric policy of a BPU.

NOTE – The means of evaluation of the modality policy and biometric parameter information (and their secure performance) for each stated security level is out of the scope of this Recommendation.

9.6 A security level corresponds to modality policy and other biometric parameters, specified in the `SecurityLevelBioRef`:

```
SecurityLevelBioRef  ::=  SEQUENCE{
      biometricSecurityLevelId    BiometricSecurityLevelId,
      modalityPolicy              ModalityPolicy,
      biometricPara                     BiometricPara,
                                        ... }

BiometricSecurityLevelId::= BIT STRING
```

9.7 The `biometricSecurityLevelId` is a unique identifier for the biometric security level. It can (but need not be) a hash value for the set of modality policy and biometric parameter values.

NOTE – The unique identifier may be put into the biometric extension field of an AC certificate when the AC is created for use by TAI applications.

9.8 The `ModalityPolicy` is the policy on the choice of appropriate biometric modality, actions during capture (such as the number of trials, checks for liveness, etc.), fusion, and so on in order to achieve associated security level. There are many possible different modality policies. Possible modality policies are identified in Appendix I. The precise specification of modality policies is outside the scope of this Recommendation, but values of `"unimodal"`, `"unimodalWithLiveDetection"`, `"multimodalWithScoreFusion"` are recommended where appropriate, but should be accompanied by precise descriptions.

9.9 The ASN.1 definition of `ModalityPolicy` is:

```
ModalityPolicy ::= UniversalString
```

9.10 The `BiometricPara` is a set of values of important and usually adjustable biometric parameters that can include the biometric type of a capture device, algorithms employed for comparison, FMR and other parameters.

9.11 The type of the algorithm contains at least the processing algorithm to obtain the biometric sample data, the raw data processing algorithm and the matching/decision algorithm.

9.12 The ASN.1 definition of the type `BiometricPara` is as follows:

```
BiometricPara  ::= SEQUENCE OF SEQUENCE{
      biometricType          BiometricType,
                             --CBEFF defined type
```

```
        fMR-Value                      BioAPI-FMR,
        trialNumber                INTEGER OPTIONAL,
        requestQuality             INTEGER OPTIONAL,
                                         ... }
```

9.13 The `biometricPara` specifies the one (for a single modaliy) or more (for multiple modalities) parameters. If there is more than one item in the `biometricPara` sequence-of, then the fusion mechanism should be identified in the corresponding `ModalityPolicy`.

9.14 The `fMR-Value` is used to determine the threshold values that will be applied by the BPU to determine whether the captured biometric is to be considered to match the biometric template in the BC, and hence to determine whether success or failure of the authentication process is to be reported to the IDV.

NOTE – It would be possible to extend the biometric parameters to allow either FMR or FNMR (i.e., false non-match ratio) to be specified.

9.15 The `trialNumber` is the number of trials that will be allowed by the BPU on each biometric device, for this security level.

9.16 The `requestQuality` refers to the biometric data quality that can be accepted (see [ISO/IEC 19784-1]).

10 Biometric device certificate

10.1 A biometric device is part of a BPU, and typically contains an element that is normally considered tamper proof (such as a write-once memory). It is the operation of this part of the device that is certified.

10.2 A BDC is a signed [ITU-T X.509] AC with at least one attribute that is a `bDCReportContentInformation`, and includes a report certificate `BPUReportInformation` which is issued to the biometric device by the TBA (or, typically, installed by the vendor of the device if trusted by the TBA). The BDC contains information on the vendor, the TBA, information about the functional capabilities and limitations of the biometric device, the related performance evaluation report, and information on the security performance of the biometric device.

10.3 A BDC also includes a public-key certificate (or a URI that references it).

10.4 The BDC is defined as follows:

```
BiometricDeviceCertificate ::=
      SIGNED {BiometricDeviceCertificateInfo}
      -- Signed by a TBA

BiometricDeviceCertificateInfo ::= AttributeCertificateInfo
      (WITH COMPONENTS {
      ...,
      attributes(SIZE(1..MAX))})
      -- the attributes in BiometricDeviceCertificateInfo shall contain at least
      one bDCReportContentInformation attribute

bDCReportContentInformation ATTRIBUTE ::= {
      WITH SYNTAX       BDCReportContentInformation
      ID                id-tai-at-bDCReportContentInformation }
      -- Object identifier values are specified in Annex A

BDCReportContentInformation ::= SEQUENCE {
      bdcPKCInformation            BdcPKCInformation,
      bdcReportInformation         BPUReportInformation }
        -- BPUReportInformation is imported from [ISO/IEC 24761]
```

10.5 The public-key certificate of a biometric device is an X.509 public-key certificate that provides a public-key pair for the device. It is defined as follows:

```
BdcPKCInformation ::= CHOICE {
      bdcPublicKeyCertificate            Certificate,
                 -- Certificate is imported from [ITU-T X.509]
```

```
        bpuCertificateReference      URI
                                              -- Pointing to a Certificate --}
```

11 TAI extensions defined for X.509

11.1 Extension used in a BC to index a PKC

11.1.1 When the BC extension is used in a PKC, the BC extension includes the PKC issuer, PKC serial number and PKC key usage. This extension is used to index the associated public-key certificate of the BC holder.

11.1.2 The extension is defined as follows:

```
 publicKeyCert EXTENSION ::= {
     -- BC extension used in a PKC
     SYNTAX PublicKeyCert
     IDENTIFIED BY id-tai-ce-publicKeyCert }

 PublicKeyCert ::= SEQUENCE{
     pkcIssuer         Name,
     pkcSerialNumber   CertificateSerialNumber,
     pkcUsage          KeyUsage}
```

11.2 TAI extensions defined for use with PMI

11.2.1 If a TAI uses PMI (see [ITU-T X.509]), the BC attributes may also contain the privilege attribute providing information on a PMI AC of the BC holder. This extension field can include any Directory attribute values related to the holder of the BC.

11.2.2 The extension is defined as follows:

```
holderDirectoryAttributes EXTENSION ::= {
      SYNTAX             AttributesSyntax
      IDENTIFIED BY      id-tai-ce-holderDirectoryAttributes }

AttributesSyntax ::= SEQUENCE SIZE (1..MAX) OF Attribute{{SupportedAttributes}}
```

11.3 Extension used in the BC for cryptographic key generation

11.3.1 If a BC is used to generate a cryptographic key, the BC extension contains additional information, alignment help data and biometric key binding data that are used for adjustment of biometric input data. The biometric key binding data is not standardized, and is used to provide the cryptographic key generation reference information between the BIT and a biometric digital key. The alignment help data is not standardized, but will typically contain adjustment information for enhancing the matching function on fingerprint-based biometric authentication systems.

11.3.2 The extension is defined as follows:

```
dkgExtensionData EXTENSION ::= {
      SYNTAX            DkgExtensionDataSyntax
      IDENTIFIED BY id-tai-ce-dgkExtensionData }

DkgExtensionDataSyntax ::= SEQUENCE {
      alignmentHelpData      OCTET STRING(SIZE(1..MAX)),
      biometricKeyBindingData      OCTET STRING(SIZE(1..MAX))}
```

11.4 Biometric certificate index extension

11.4.1 To be able to interwork with biometric authentication, some information about the BC needs to be included in an extension of the AC.

11.4.2 To authenticate privileges with an AC, the system has to first establish the user's identity. Before the authentication of the privilege, the PV should have received the AC from the client, together with his/her claimed privileges and the associated BC. Before it proceeds, it validates the match between the BC and the `baseCertificateID` in the AC. The associated BC is then used to authenticate the user, and a positive result will then allow the user to operate with the privileges previously determined by the PV.

```
bioCert EXTENSION ::= {
      SYNTAX                BioCert
      IDENTIFIED BY         id-tai-ce-bioCert }

BioCert::= SEQUENCE{
      baseCertificateID [0]    IssuerSerial OPTIONAL,
      -- the issuer and serial number of the holder's BC
      entityName        [1]    GeneralNames OPTIONAL -- [b-ISO/IEC TR 24741] --,
      -- the name of the entity or role
      objectDigestInfo  [2]    ObjectDigestInfo OPTIONAL -- [b-ISO/IEC TR 24722] --
      --used to directly authenticate the holder
      }
      (CONSTRAINED BY { -- at least one of baseCertificateID,
                         -- entityName or
                            -- objectDigestInfo shall be present
                        })
```

11.4.3 BC issuer and BC serial number are the BC basic index information, which identify a biometric certificate that is used to authenticate the identity of this holder when privilege in attribute is asserted.

11.4.4 The `entityName` component, if present, identifies one or more names for the AC holder. If `entityName` is the only component present in the index, any biometric certificate that has one of these names as its subject can be used to authenticate the identity of this holder when asserting privileges with this AC. If the basic index information and `entityName` are both present, only the certificate specified by the basic index information may be used. In this case, `entityName` is included. (It is included to help the privilege PV locate the identified biometric certificate.)

11.4.5 The `objectDigestInfo` component, if present, is used directly to authenticate the identity of an AC holder, including an executable holder (e.g., an applet). The holder is authenticated by comparing a digest of the corresponding information (the biometric certificate's `version`, `serialNumber`, `validity`, `holder` and `issuerUniqueID`, `issuer` and `issueUniqueID`, attributes containing a `BiometricTemplate` value, etc.), created by the PV with the same algorithm identified in `objectDigestInfo` with the content of `objectDigestInfo`. If the two are identical, the holder is authenticated for purposes of asserting privileges with this AC.

NOTE – The BC index must contain at least one of the BC issuer and BC serial number, `entityName`, `objectDigestInfo` component to confirm the correspondence between AC and biometric certificate.

11.5 Security level of privilege extension

11.5.1 This extension of the AC asserts certain security levels, so that biometric policy certificates can be employed to enable the privilege attributes with different security or strictness requirements for the biometric authentication of the AC holder.

11.5.2 It stores the `bioSecLevel` (e.g., `biometricSecurityLevelId` in clause 9.7) of the biometric policy certificate with the same holder of the AC. The extension is added to the basic privilege management certificate extension – see clause 15.1.2 of [ITU-T X.509].

```
securityLevelofPrivilege EXTENSION ::= {
      SYNTAX      SecurityLevelofPrivilege
      IDENTIFIED BY   id-tai-ce-biometricSecurityLevelOfPrivilege }

SecurityLevelofPrivilege::= SEQUENCE{
      bioSecLevel       CHOICE {
                         x520identifier   UniqueIdentifierOfBioParaInfo,
                      simpleidentifier   INTEGER } }

UniqueIdentifierOfBioParaInfo ::= UniqueIdentifier
                                                  -- Imported from [ITU-T X.520]
```

11.5.3 `bioSecLevel` is used to identify the biometric authentication result security level. The value of `bioSecLevel` may be `uniqueIdentifierOfBioParaInfo`, or a `simpleidentifier` assigned by the issuer of the AC.

11.6 BPC extension for a BDC

11.6.1 In the implementation of a TAI application, it is helpful to associate a BPC with some particular BDCs, to help the IDV evaluate and judge the underlying biometric processing. Some BDC information could be used to verify the biometric devices that are included with the BPC. Other BDCs could be used for further evaluation by the TAI application itself. As an attribute certificate, the BPC can have extension fields to index such BDCs.

11.6.2 The extension is defined as follows:

```
bDCCertificate EXTENSION ::= {
    SYNTAX           BDCCertificateReferer
    IDENTIFIED BY id-tai-ce-bDCCertificate }

BDCCertificateReferer ::= SEQUENCE{
    bdcIssuer        Name,
    bdcSerialNumber  CertificateSerialNumber,
    bdcUsage         KeyUsage}
```

Annex A

Complete formal ASN.1 specifications

(This annex forms an integral part of this Recommendation)

```
TAI {itu-t recommendation x tai(1089) modules(0) framework(0) version1(1)}
DEFINITIONS AUTOMATIC TAGS ::=
BEGIN

IMPORTS

-- Directories imports from [ITU-T X.509]
ATTRIBUTE,Name,Attribute{}, SupportedAttributes
      FROM InformationFramework
      {joint-iso-itu-t ds(5) module(1) informationFramework(1) 6}

SIGNED{},EXTENSION,CertificateSerialNumber,Certificate,ALGORITHM,
AlgorithmIdentifier{}, SupportedAlgorithms
      FROM AuthenticationFramework
      {joint-iso-itu-t ds(5) module(1) authenticationFramework(7) 6}

AttributeCertificateInfo
      FROM AttributeCertificateDefinitions
      {joint-iso-itu-t ds(5) module(1) attributeCertificateDefinitions(32) 6}

GeneralNames,KeyUsage
      FROM CertificateExtensions
      {joint-iso-itu-t ds(5) module(1) certificateExtensions(26) 6}

IssuerSerial,ObjectDigestInfo
      FROM AttributeCertificateDefinitions
      {joint-iso-itu-t ds(5) module(1) attributeCertificateDefinitions(32) 6}

UniqueIdentifier
      FROM SelectedAttributeTypes
      {joint-iso-itu-t ds(5) module(1) selectedAttributeTypes(5) 6}

ID
      FROM UsefulDefinitions
      {joint-iso-itu-t ds(5) module(1)usefulDefinitions(0) 6}

-- The BioAPI False Match Rate is imported from the
-- Biometric Interworking Protocol (BIP) [ITU-T X.1083]
BioAPI-FMR
      FROM BIP
      {joint-iso-itu-t bip(41) modules(0) bip(0) version1(1)}

-- BiometricType and Biometric InformationTemplate are imported from
-- CBEFF [ISO/IEC 19785-3]
BiometricType
      FROM CBEFF-DATA-ELEMENTS
      {iso standard 19785 modules(0) types-for-cbeff-data-elements(1)}

BiometricInformationTemplate
      FROM CBEFF-SMARTCARD-BIDO
      {iso standard 19785 modules(0) types-for-smartcard(8)};

-- START OF X.tai definitions.

-- URI definition - used in a BDC and in a BPC
URI ::= UTF8String(CONSTRAINED BY {
      -- shall be a valid URI as defined in [IETF RFC 3986] --})

-- BC definition – (see 8.2 for additional comments)
BiometricCertificate ::= SIGNED { BiometricCertificateInfo }

BiometricCertificateInfo ::= AttributeCertificateInfo
      (WITH COMPONENTS {
            ...,
            attributes (SIZE(1..MAX))})
```

```
-- Definition of the biometricInformationTemplate attribute
-- contained in a BC (see 8.6 and 8.7 for additional comments)
biometricInformationTemplate ATTRIBUTE ::= {
       WITH SYNTAX   BiometricInformationTemplateorPointer
       ID            id-tai-at-BiometricInformationTemplate }

BiometricInformationTemplateorPointer ::= CHOICE{
      bcBiometricInformationTemplate  BCBiometricInformationTemplate,
      referenceToBCBiometricInformationTemplate
                                      URI,
                                              ... }

BCBiometricInformationTemplate ::=
      SIGNED {BCBiometricInformationTemplateContent}

BCBiometricInformationTemplateContent ::= SEQUENCE{
      biometricTemplateVersion               BiometricTemplateVersion,
      biometricTemplateInfo                  BiometricTemplateInfo,
      issuerDigitalSignatureAlgorithm   AlgorithmIdentifier{{SupportedAlgorithms}}
      OPTIONAL,
      bioTempIssuer                           BioTempIssuer  OPTIONAL}

BiometricTemplateVersion ::= INTEGER {v0(0)}(v0,...)

BioTempIssuer ::= [0] SEQUENCE {
      issuerName            GeneralNames OPTIONAL,
      baseCertificateID[0]  IssuerSerial OPTIONAL,
      objectDigestInfo [1]  ObjectDigestInfo OPTIONAL -- [b-ISO/IEC-TR 24741] --}

BiometricTemplateInfo ::= CHOICE {
      biometricTemplateInfo19785  BiometricInformationTemplate,
                                        ...}

-- BPC definition – (see clause 9 for additional comments)
BiometricPolicyCertificate ::=
      SIGNED {BiometricPolicyCertificateInfo}

BiometricPolicyCertificateInfo ::= AttributeCertificateInfo
      (WITH COMPONENTS {
      ...,
      attributes(SIZE(1..MAX))})

bioSecLevelReference  ATTRIBUTE ::= {
      WITH SYNTAX       SecurityLevelBioReference
      ID                id-tai-at-bioSecLevelReference }

SecurityLevelBioReference  ::=  SEQUENCE{
      securityLevelNum            INTEGER,
      securityLevelBioRef         SecurityLevelBioRef}

SecurityLevelBioRef  ::=  SEQUENCE{
      biometricSecurityLevelId    BiometricSecurityLevelId,
      modalityPolicy              ModalityPolicy,
      biometricPara                     BiometricPara}

BiometricSecurityLevelId::= BIT STRING

ModalityPolicy ::= UniversalString

BiometricPara  ::= SEQUENCE OF SEQUENCE{
      biometricType          BiometricType,
                             --CBEFF defined type
      fMR-Value                   BioAPI-FMR,
      trialNumber            INTEGER OPTIONAL,
      requestQuality         INTEGER OPTIONAL,
                                  ... }

-- BDC definition – (see clause 10 for additional comments)
BiometricDeviceCertificate ::=
      SIGNED {BiometricDeviceCertificateInfo}

BiometricDeviceCertificateInfo ::= AttributeCertificateInfo
      (WITH COMPONENTS {
      ...,
      attributes(SIZE(1..MAX))})
```

```
bDCReportContentInformation ATTRIBUTE ::= {
      WITH SYNTAX       BDCReportContentInformation
      ID                id-tai-at-bDCReportContentInformation }

BDCReportContentInformation ::= SEQUENCE {
      bdcPKCInformation           BdcPKCInformation,
      bdcReportInformation        BPUReportInformation }

BdcPKCInformation ::= CHOICE {
      bdcPublicKeyCertificate           Certificate,
                 -- Certificate is imported from [ITU-T X.509]
      bpuCertificateReference     URI}

-- BPUReportInformation as defined in ACBio [ISO/IEC 24761]

BPUReportInformation ::= CHOICE {
            bpuReport BPUReport,
            bpuReportReferrer URI}

CONTENT-TYPE ::= TYPE-IDENTIFIER

BPUReport ::= SEQUENCE {
            contentType CONTENT-TYPE.&id({ContentTypeBPUReport}),
            content [0] EXPLICIT CONTENT-TYPE.&Type
                  ({ContentTypeBPUReport}{@contentType})}

ContentTypeBPUReport CONTENT-TYPE ::= {bpuReport}

bpuReport CONTENT-TYPE ::= {
            BPUReport
            IDENTIFIED BY id-bpuReport   }

id-bpuReport OBJECT IDENTIFIER ::=
            {iso(1) standard(0) acbio(24761) contentType(2) bpuReport(4)}

-- TAI EXTENSION in a PKC (see 11.1)
publicKeyCert EXTENSION ::= {
      SYNTAX PublicKeyCert
      IDENTIFIED BY id-tai-ce-publicKeyCert }

PublicKeyCert ::= SEQUENCE{
      pkcIssuer        Name,
      pkcSerialNumber  CertificateSerialNumber,
      pkcUsage         KeyUsage}

-- TAI EXTENSION used with PMI (see 11.2)
holderDirectoryAttributes EXTENSION ::= {
      SYNTAX           AttributesSyntax
      IDENTIFIED BY    id-tai-ce-holderDirectoryAttributes }

AttributesSyntax ::= SEQUENCE SIZE (1..MAX) OF Attribute{{SupportedAttributes}}

-- TAI EXTENSION used for digital keys (see 11.3)
dkgExtensionData EXTENSION ::= {
      SYNTAX           DkgExtensionDataSyntax
      IDENTIFIED BY id-tai-ce-dgkExtensionData }

DkgExtensionDataSyntax ::= SEQUENCE {
      alignmentHelpData      OCTET STRING(SIZE(1..MAX)),
      biometricKeyBindingData      OCTET STRING(SIZE(1..MAX))}

-- TAI EXTENSION in an AC for BC Index (see 11.4)
bioCert EXTENSION ::= {
      SYNTAX               BioCert
      IDENTIFIED BY        id-tai-ce-bioCert }

BioCert::= SEQUENCE{
      baseCertificateID[0]   IssuerSerial OPTIONAL,
      entityName       [1]   GeneralNames OPTIONAL -- [b-ISO/IEC-TR 24741] --,
      objectDigestInfo [2]   ObjectDigestInfo OPTIONAL -- [b-ISO/IEC-TR 24722] --}
      (CONSTRAINED BY { -- at least one of baseCertificateID,
                        -- entityName or
                           -- objectDigestInfo shall be present –
                       })
```

```
-- TAI EXTENSION for security level in PMI (see 11.5)
securityLevelofPrivilege EXTENSION ::= {
      SYNTAX      SecurityLevelofPrivilege
      IDENTIFIED BY   id-tai-ce-biometricSecurityLevelOfPrivilege }

SecurityLevelofPrivilege::= SEQUENCE{
      bioSecLevel       CHOICE {
                        x520identifier   UniqueIdentifierOfBioParaInfo,
                        simpleidentifier INTEGER} }

UniqueIdentifierOfBioParaInfo ::= UniqueIdentifier

-- TAI EXTENSION used in a BDC (see 11.6)
bDCCertificate EXTENSION ::= {
      SYNTAX            BDCCertificateReferer
      IDENTIFIED BY id-tai-ce-bDCCertificate }

BDCCertificateReferer ::= SEQUENCE{
      bdcIssuer         Name,
      bdcSerialNumber   CertificateSerialNumber,
      bdcUsage          KeyUsage}

-- ID values used in this module
id-tai-at-BiometricInformationTemplate  ID ::=
      {iso registration-authority cbeff(19785)
      biometric-organization(0) jtc1-sc37(257) patronformat(1)
      tlv-encoded(5)}

id-tai ID ::= {itu-t(0) recommendation(0) x(24) tai(1089)}

id-tai-at ID ::= {id-tai attributes(1)}

id-tai-ce ID ::= {id-tai certificate-extensions(2)}

id-tai-at-bioSecLevelReference ID ::= {id-tai-at 1}

id-tai-at-bDCReportContentInformation ID ::= {id-tai-at 2}

id-tai-ce-bDCCertificate ID ::= {id-tai-ce 1}

id-tai-ce-bioCert ID ::= {id-tai-ce 2}

id-tai-ce-biometricSecurityLevelOfPrivilege ID ::= {id-tai-ce 3}

id-tai-ce-publicKeyCert ID ::= {id-tai-ce 4}

id-tai-ce-holderDirectoryAttributes ID ::= {id-tai-ce 5}

id-tai-ce-dgkExtensionData ID ::= {id-tai-ce 6}

END
```

Appendix I

Examples of possible security level lists

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

I.1 An illustrative example of a biometric security level list is shown in Table I.1.

Table I.1 – An example of a security level list

Biometric security level		**Modality policy**	**Biometric parameter information**		
Hash_i	Security degree (A_i)	Unimodal (A)	Biometric type	Biometric algorithm	FMR_i
Hash_j	Security degree (B_j)	Unimodal + live detecting (B)	Biometric type	Biometric algorithm	FMR_j
Hash_k	Security degree (C_k)	Multimodal (C)	Biometric type	Biometric algorithm	FMR_k
Hash_l	Security degree (D_l)	Multimodal + live detecting (D)	Biometric type	Biometric algorithm	FMR_l
…	…	…	…	…	…

I.2 Policy: "A" is a unimodal verification; policy "B" is a unimodal verification with liveness detection; policy "C" is a multimodal verification; policy "D" is a multimodal verification with liveness detection. In general, the increasing order of security level in the policy is as follows:

– unimodal (lowest)

– unimodal plus live detection

– multimodal

– multimodal plus live detection (highest).

Additional security-related policies can be added as new columns, but the security level should always be specified so that a higher level means "more secure". Precise values are not standardized in this Recommendation, but may be subject to future standardization.

I.3 Security degree: This is the combination of the security level, the algorithm (or algorithms used) and the FMR or FMRs used, and any additional security features.

I.4 In Table I.1, for all values if "i" to "l", security degree A_i denotes the security degree of a unimodal policy; B_j denotes the security degree of a unimodal plus live detection policy; C_k denotes the security degree of a multimodal policy; D_l denotes the security degree of a multimodal plus live detection policy. $Hash_i$, etc., is the corresponding hash value of the security degree and the biometric parameters information and it uniquely identifies the biometric security level and the biometric parameters. The hash value is not necessarily a unique identifier for the parameter information without the security degree.

I.5 For unimodal policies, a biometric type may have several different biometric processing algorithms. For example, there are various algorithms for the processing and matching of fingerprints. For multimodal policies, the same combination of biometric types may have various combinations of algorithms, and, in addition, there will be a fusion algorithm that needs to be specified. For example, the algorithm combinations for fingerprint and iris may include: fingerprint algorithm 1 and iris algorithm 1 fused with fusion algorithm 1, fingerprint algorithm 2 and iris algorithm 2 fused with fusion algorithm 2, etc.

I.6 Every algorithm or algorithm combination can produce different FMR values depending on the threshold used in the matching process. The FMR value for the security level determines the threshold to be used in matching, depending on the technology.

NOTE – The FMR and FNMR curves are not always precisely defined, so the mapping between FMR and threshold values can be imprecise.

Bibliography

[b-ISO/IEC 7816-11]	ISO/IEC 7816-11: 2004, *Identification cards – Integrated circuit cards – Part 11: Personal verification through biometric methods*.
[b-ISO/IEC TR 24741]	ISO/IEC TR 24741:2007, *Information technology – Biometrics tutorial.*
[b-ISO/IEC TR 24722]	ISO/IEC TR 24722:2007, *Information technology – Biometrics – Multimodal and other multibiometric fusion.*

SERIES OF ITU-T RECOMMENDATIONS

Series A	Organization of the work of ITU-T
Series B	Available
Series C	Available
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 W	Available
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