

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

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

X.1084

(05/2008)

SERIES X: DATA NETWORKS, OPEN SYSTEM
COMMUNICATIONS AND SECURITY

Telecommunication security

**Telebiometrics system mechanism – Part 1:
General biometric authentication protocol and
system model profiles for telecommunications
systems**

Recommendation ITU-T X.1084

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.1084

Telebiometrics system mechanism – Part 1: General biometric authentication protocol and system model profiles for telecommunications systems

Summary

Biometric technologies are developed in various products and populated in application systems such as border control, physical access control, etc., for identity verification. These technologies are also expected to be applied to open network systems for reliable user authentication. However, open network systems need to manage risks in biometric products and system configurations for secure remote services. Recommendation ITU-T X.1084 specifies biometric authentication protocols and profiles for telecommunication systems in open networks.

Source

Recommendation ITU-T X.1084 was approved on 29 May 2008 by ITU-T Study Group 17 (2005-2008) under Recommendation ITU-T A.8 procedures.

Keywords

Telebiometric authentication profiles, telebiometric authentication protocol, telebiometric system mechanism, transport layer security.

FOREWORD

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

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

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

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

NOTE

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

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

INTELLECTUAL PROPERTY RIGHTS

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

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

© ITU 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	Vocabulary definitions within ISO/IEC JTC 1/SC 37 [b-SC37SD2V8].....	2
3.2	Terms defined in this Recommendation.....	2
4	Abbreviations.....	3
5	Conventions	4
6	Prerequisites.....	4
7	Authentication models	5
8	Security threats for each models.....	10
9	General requirements.....	12
10	General protocol	13
10.1	Requirement of the biometrics handshake protocol	13
10.2	Alert protocol for biometric handshake.....	16
10.3	Implementation of the extended protocol.....	17
11	Requirements of the biometric transportation stage for each model	18
11.1	Local model.....	19
11.2	Download model	20
11.3	Attached model.....	20
11.4	Centre model	21
11.5	Reference management on TTP for local model	21
11.6	Reference management on TTP for centre model	22
11.7	Comparison outsourcing by client model.....	23
11.8	Comparison outsourcing by server model	25
11.9	Storage and comparison outsourcing model.....	26
	Annex A – ASN.1 definitions for modified TLS extension protocol	30
	Appendix I – Telebiometrics system mechanism definitions by TLS extension.....	41
I.1	Extensions for biometric transfer protocol	41
I.2	Biometrics Verify	43
I.3	Biometrics Retry Request.....	45
I.4	Finished Biometrics.....	45
I.5	Biometrics TTP Request.....	46
I.6	Biometrics TTP response	47
I.7	Extension alert protocol.....	47

	Page
Appendix II – Implementation example of the biometric transfer protocol using BIP	50
II.1 Local model.....	51
II.2 Download model	52
II.3 Attached model.....	52
II.4 Centre model	53
II.5 Comparison outsourcing by client model.....	53
II.6 Reference management on TTP for local model	54
II.7 Reference management on TTP for centre model	55
II.8 Comparison outsourcing by server model	56
II.9 Storage and comparison outsourcing model.....	57
Appendix III – Template registration and updating process for this Recommendation	59
III.1 Registration process.....	59
III.2 Updating or revocation process	60
Appendix IV – ASN.1 definitions for the protocol of TSM based on Appendix I.....	63
Appendix V – ECN modules for Appendix IV.....	75
V.1 EDM module	75
V.2 ELM module.....	97
Bibliography.....	100

Introduction

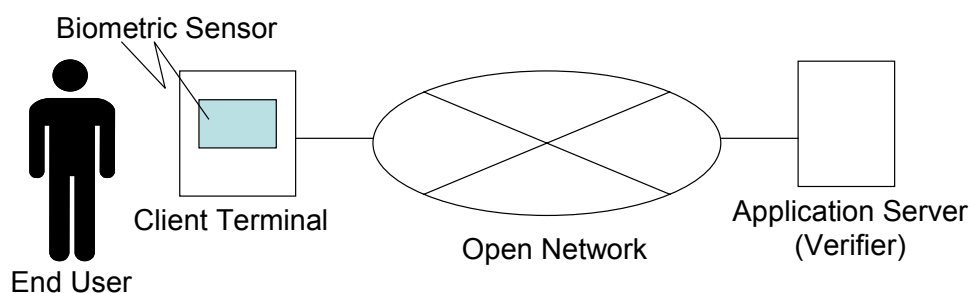
With the rapid and widespread diffusion of the Internet, various network services are now in operation. In high value services, such as Internet banking, Internet shopping, Internet trading, etc., illegal trading by obtaining a personal identification number (PIN) by means, such as phishing, are occurring with increasing regularity. Therefore, high security authentication mechanisms are increasingly required, such as can be provided by biometrics.

We have the following problems in standardizing biometric authentication on the Internet:

- Service providers do NOT have any information regarding what biometric devices are in use at the end-user's end, what security level is this device set at, or how it is operated.
- According to each biometric product, the accuracy (False Accept Rate) determined by the threshold parameter differs between different biometric products. Therefore, the service provider can NOT claim to maintain a uniform accuracy level.
- The accuracy of biometric verification may decline with the aging of end-users because biometrics uses features of the human body.

To solve these problems, protocols for biometric authentication between unspecified end-users and service providers on open networks are greatly required.

The figure below illustrates the environment of this Recommendation for a biometric security mechanism that authenticates a user via a non-face-to-face open network.



Environment of this Recommendation

The meaning of the open network:

- Many unspecified verifiers connect to the network and use varying biometric methods.
 - High value service provider
 - Efficient government service provider
 - Online shopping provider.
- A large number of unspecified end-users also connect to the network, and their identity is verified through biometric authentication in order to use services from the aforementioned providers.

The verifier here is "open" in the following sense. The purpose of biometric authentication is different for each verifier, and the risk/value for the verifier is also different for each. Therefore, each verifier has a different authentication security policy.

The user here is "open" in the sense that each user uses different biometric authentication methods. Each user can select any biometric authentication method to use, according to the acceptability or privacy policy they follow.

Recommendation ITU-T X.1084

Telebiometrics system mechanism – Part 1: General biometric authentication protocol and system model profiles for telecommunications systems

1 Scope

This Recommendation specifies the biometric authentication protocols and profiles for telecommunication systems. It defines the protocols for biometric authentication of unspecified end-users and service providers on open networks. In the open network, there are a range of biometric communication devices for the end-users. There are also a variety of security policies for network services for the providers. This Recommendation defines nine telebiometrics authentication models depending on the configuration of the client, the server, and the trusted third party. It also defines the negotiation protocol for the policies and the device environments using the models. Furthermore, it specifies the requirements of biometric transportation data for each model.

2 References

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

- [ITU-T X.509] Recommendation ITU-T X.509 (2005) | ISO/IEC 9594-8:2005, *Information technology – Open Systems Interconnection – The Directory: Public-key and attribute certificate frameworks*.
- [ITU-T X.1089] Recommendation ITU-T X.1089 (2008), *Telebiometrics authentication infrastructure (TAI)*.
- [ISO/IEC 15408-1] ISO/IEC 15408-1:2005, *Information technology – Security techniques – Evaluation criteria for IT security – Part 1: Introduction and general model*.
- [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 19795-1] ISO/IEC 19795-1:2006, *Information technology – Biometric performance testing and reporting – Part 1: Principles and framework*.
- [ISO/IEC 24761] ISO/IEC 24761:2009, *Information technology – Security techniques – Authentication context for biometrics*.
- [IETF RFC 3986] IETF RFC 3986 (2005), *Uniform Resource Identifier: Generic Syntax*.
- [IETF RFC 4346] IETF RFC 4346 (2006), *The Transport Layer Security (TLS) Protocol Version 1.1*.
- [IETF RFC 4366] IETF RFC 4366 (2006), *Transport Layer Security (TLS) Extensions*.
- [X9.84-CMS] OASIS X9.84-CMS (2003), *XML Common Biometric Format*.

3 Definitions

3.1 Vocabulary definitions within ISO/IEC JTC 1/SC 37 [b-SC37SD2V8]

This Recommendation uses the following terms defined elsewhere:

3.1.1 biometric (adjective): Of or having to do with biometrics.

3.1.2 biometrics (noun): An automated recognition of individuals based on their behavioural and biological characteristics.

3.1.3 biometric template: A set of stored biometric features comparable directly to biometric features of a recognition biometric sample.

3.1.4 biometric reference: One or more stored biometric samples, biometric templates or biometric models attributed to a biometric data subject and used for comparison.

3.1.5 biometric sample: Analogue or digital representation of biometric characteristics prior to biometric feature extraction process, and obtained from a biometric capture device or biometric capture subsystem.

3.1.6 comparison (match/matching): Estimation, calculation or measurement of similarity or dissimilarity between recognition biometric sample(s)/biometric features/biometric models and biometric reference(s).

3.1.7 comparison decision: Determination of whether the recognition biometric sample(s) and biometric reference(s) have the same biometric source, based on a comparison score(s), a decision policy(ies), including a threshold, and possibly other inputs.

3.1.8 comparison score: Numerical value (or set of values) resulting from a comparison.

3.1.9 false match: Comparison decision of "match" for a recognition biometric sample and a biometric reference that are not from the same source.

3.1.10 false non-match: Comparison decision of "non-match" for a recognition biometric sample and a biometric reference that are from the same source.

3.1.11 match: Decision that the recognition biometric sample(s) and the biometric reference are from the same source.

3.1.12 non-match: Decision that the recognition biometric sample(s) and the biometric reference are not from the same source.

3.2 Terms defined in this Recommendation

This Recommendation defines the following terms:

3.2.1 biometric authentication: The process of confirming an individual's identity, either by verification or by identification.

3.2.2 decision policy: Logic through which a biometric system provides match/no match decisions, for example, through the setting of the threshold and number of attempts.

3.2.3 false accept rate (FAR): Measure of the probability that a biometric comparison process will incorrectly identify an individual or will fail to reject an impostor.

3.2.4 false reject rate (FRR): Measure of the probability that a biometric comparison process will incorrectly fail to identify an individual.

3.2.5 failure to acquire: Failure of a biometric system to capture a biometric sample, or to extract biometric data from a biometric sample, sufficient to generate a biometric template for matching.

3.2.6 failure to enrol: Failure of a biometric system to capture one or more biometric samples, or to extract data from one or more biometric samples, sufficient to generate a biometric template for successful enrolment.

3.2.7 registration: The process in which a person proves their identity by presenting credentials to the biometric service provider prior to being allowed to enrol and being assigned an electronic identifier.

3.2.8 risk management: Coordinated activities to direct and control an organization with regard to risk.

3.2.9 threshold: A predefined value which establishes the degree of similarity or correlation, (i.e., score), necessary for a biometric sample to be deemed an accurate comparison with a biometric reference template.

3.2.10 verifier: A service provider based on a biometric authentication on telecommunication environments.

3.2.11 client: A client terminal that provides a biometric function for telecommunication service applications.

3.2.12 biometric certification authority: One of third trusted party which certifies for an integrity of biometric reference and procedure of biometric product evaluation report.

3.2.13 user: The receiver of the telecommunication service using the client.

4 Abbreviations

This Recommendation uses the following abbreviations:

ACBio	Authentication Context for Biometrics
BC	Biometric Certificate
BCA	Biometric Certification Authority
BDC	Biometric Device Certificate
BFP	Biometric Function Provider
BioAPI	Biometric Application Programming Interface
BPU	Biometric Processing Unit
BSP	Biometric Service Provider
CA	Certificate Authority
CBEFF	Common Biometric Exchange File Format
CC	Common Criteria
CRL	Certificate Revocation List
EAL	Evaluation Assurance Level
PKI	Public Key Infrastructure
PP	Protection Profile
ST	Security Target
TLS	Transport Layer Security
TSM	Telebiometrics System Mechanism
TTP	Trusted Third Party

5 Conventions

None.

6 Prerequisites

This Recommendation contains the following prerequisites:

- A trusted third party (TTP) such as a certificate authority (CA) is required to authenticate a user's public key and to issue a certificate as specified in [ITU-T X.509].
- A TTP such as biometric certification authority (BCA) is required to authenticate user-registered biometric reference information, and to digitally sign that information using the biometric certificate (BC) in [ITU-T X.1089].
- A TTP such as BCA is required to authenticate both the threshold of each biometric technology in use and the accuracy evaluation result, using the biometric processing unit (BPU) report as specified in [ISO/IEC 24761]. BCA is required to grant the report by a digital signature using the biometric device certificate (BDC) in [ITU-T X.1089].
- A TTP is required to authenticate the security evaluation result based on the common criteria scheme for a biometric device, and to digitally sign the evaluation report using the biometric device certificate (BDC) in [ITU-T X.1089].
- Depending on the model, a TTP may also be required to manage biometric registration information.
- Depending on the model, a TTP may be required to perform biometric comparison.

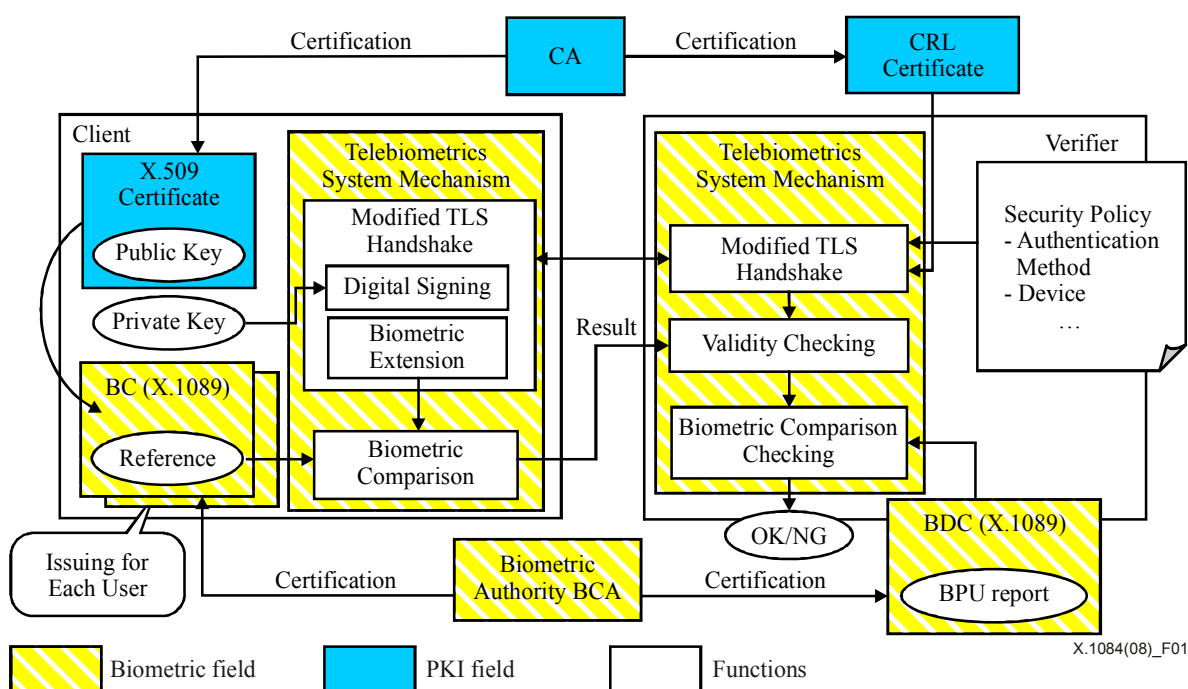


Figure 1 – Outline system of this Recommendation

7 Authentication models

This Recommendation takes into account the two perspectives below, dividing models into nine categories (all combinations of the three items in the two lists below).

- Biometric reference template location
 - Client terminal-side (user) storage of template
 - Server-side (verifier) storage of template
 - TTP-side storage of template
- Biometric comparison location
 - Client terminal-side (user) comparison
 - Server-side (verifier) comparison
 - TTP-side comparison

Table 1 – Authentication models

Store Comparison	Client	Server	TTP
Client	Local	Download	Reference management on the TTP for client comparison
Server	Attached	Centre	Reference management on the TTP for server comparison
TTP	Comparison outsourcing by client	Comparison outsourcing by server	Storage & comparison outsourcing

1) Local model

Figure 2 illustrates a local model.

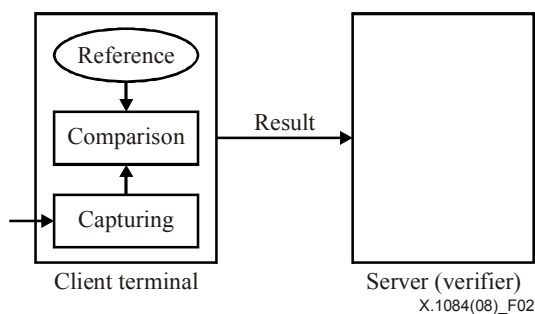


Figure 2 – Local model

The client terminal takes the request from the verifier; it acquires sample data, compares it with the registered user's template, and transfers the result to the verifier.

Template ID information is required, which is the comparison result.

For the local model, we assume that the server side cannot bear the biometric-processing load, and the user terminal-side is given sufficient processing resources. (The processing resources must be sufficient to acquire sample data and compare.)

This model can be used when the server side trusts the client-side processing procedures.

This is practical when put to use for access control systems that verify each process and transfer and save a log to the server.

2) Download model

Figure 3 illustrates a download model.

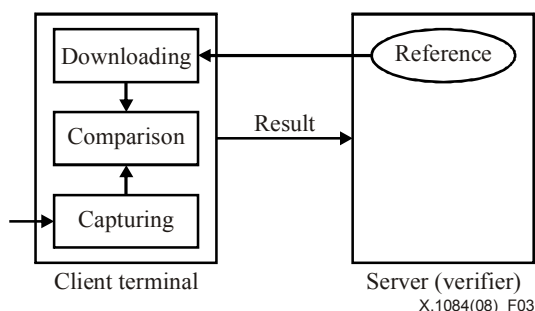


Figure 3 – Download model

The verifier sends the registered user's template and request of verification to the client terminal. It compares the acquired sample data with the received template, sending the result to the verifier.

The download model has the same sequence as the local model, excluding the transfer template from the verifier. Template ID information is required. This then forms the comparison result.

For the client terminal, we assume a temporary-use terminal (e.g., credit authorization terminal).

Under this structure, it is practical to use many terminals. This is suitable for the web-verification model, as users can connect to the server from any client terminal. This download model requires registration of the biometric reference template to the verifier.

This model also requires the server to trust the client-side processing procedure.

3) Attached model

Figure 4 illustrates an attached model.

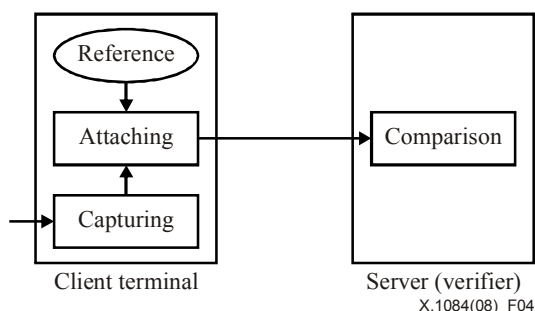


Figure 4 – Attached model

The verifier requires the comparison function, which is needed for template and captured sample data. The client terminal transfers the acquired sample data and template to the verifier, and the comparison is ultimately conducted within the verifier.

For an attached model, we assume each user utilizes a biometric algorithm that has a heavy import load (cost, private device). It is also possible for a user to utilize only a trusted verifier to judge and to send sensitive biometric data (which is similar to ID certification).

The server trusts client capture-data.

This is practical for use in credit authorization systems, as a comparison algorithm is not required for all client terminals.

4) *Centre model*

Figure 5 illustrates a centre model.

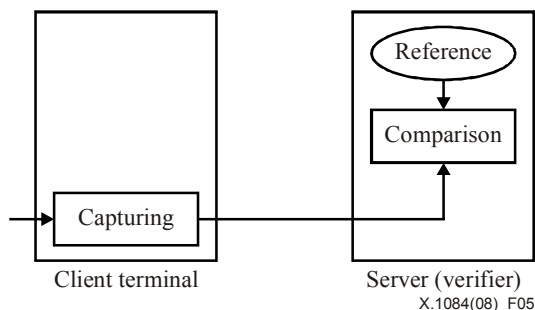


Figure 5 – Centre model

The verifier requests the sample data required for verification, the client terminal acquires sample data and transfers it to the verifier, and the verifier finally compares it with the user's template.

For the centre model, we assume that the user-side terminal cannot guarantee sufficient resources in terms of processing power, memory, etc.

The user registers its biometric reference in advance with a verifier that has a trusted biometric reference template.

This model requires that the server trusts the data captured from a client.

5) *Reference management on TTP for local model*

Figure 6 illustrates a reference management on TTP for local model.

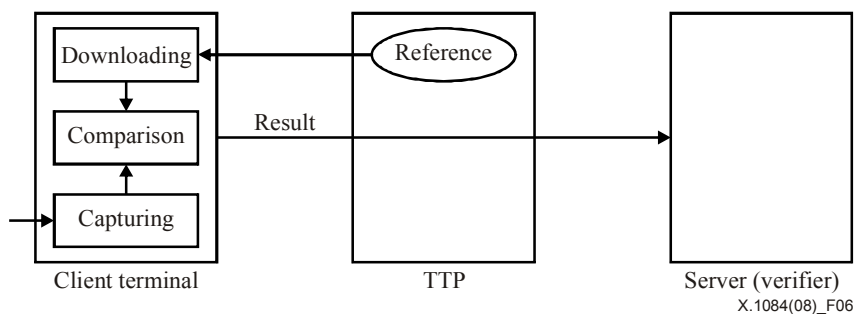


Figure 6 – Reference management on TTP for local model

The verifier requests verification, the client terminal acquires sample data, and requests the user's template to TTP. Then the client terminal compares the template which is transferred from TTP with the captured sample data, and transfers the result data to the verifier.

For this model, we assume that a user seeks to use multiple services on a temporary-use terminal, for example, a common credit card authorization terminal.

Template ID information is required. This forms the comparison result.

A user registers its biometric reference template in advance with TTP. This structure is the same as a local model, except that TTP manages the template.

The server is required to trust processing on the client side. The client and the verifier of the structure require guaranteed stability in the TTP process.

6) *Reference management on TTP for centre model*

Figure 7 illustrates a reference management on TTP for centre model.

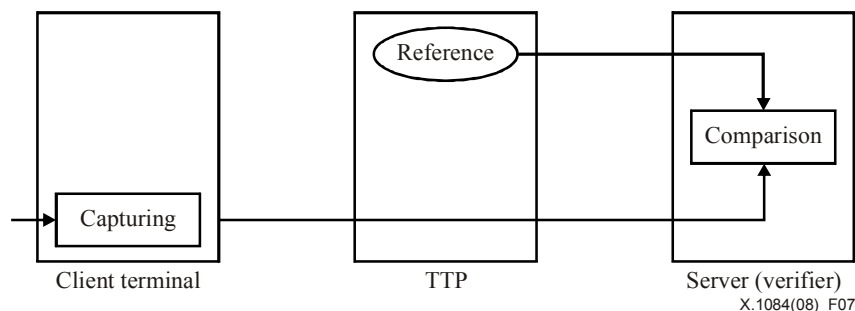


Figure 7 – Reference management on TTP for centre model

The verifier requests sample data to the client terminal and the user's template to the TTP. The client terminal captures the sample data and transfers it to the verifier, and TTP transfers the registered user's template to the verifier. Then, the verifier compares the received sample data with the received user's template.

For this model, users register their biometric reference template in advance with a TTP, and the verifier compares it with the reference and capturing data on the client terminal based on the verifier's policy.

The server is required to trust the client capture-data.

The client and the verifier are required to guarantee TTP process stability.

Taking account of privacy protection policies, a TTP is required to receive permission in advance to present both user data and verifier data.

This is the same as the centre model, except that the template is managed by TTP.

7) *Comparison outsourcing by client model*

Figure 8 illustrates a comparison outsourcing by client model.

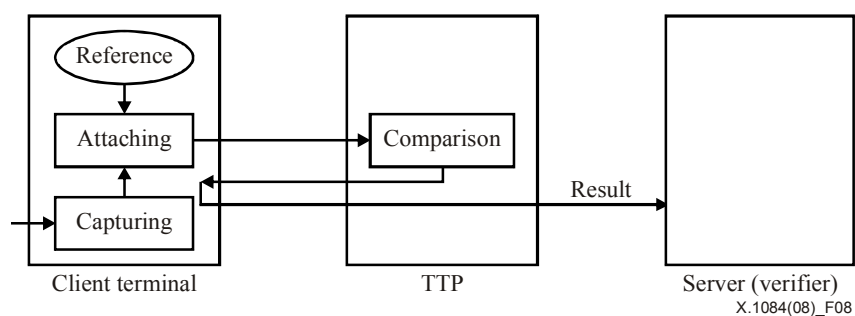


Figure 8 – Comparison outsourcing by client model

When the verifier requests verification, the client terminal first acquires sample data and requests a comparison with the user's template from a TTP. Therefore, the TTP transfers the result to the client terminal. It is then transferred from the client terminal to the verifier.

In this model, we assume that a client cannot trust the server, but a client can trust a third party. Accordingly, a client, as well as a server, request a TTP to perform comparison procedure.

Template ID information is required in the comparison result.

This model requires a TTP to process client capture-data.

8) *Comparison outsourcing by server model*

Figure 9 illustrates a comparison outsourcing by server model.

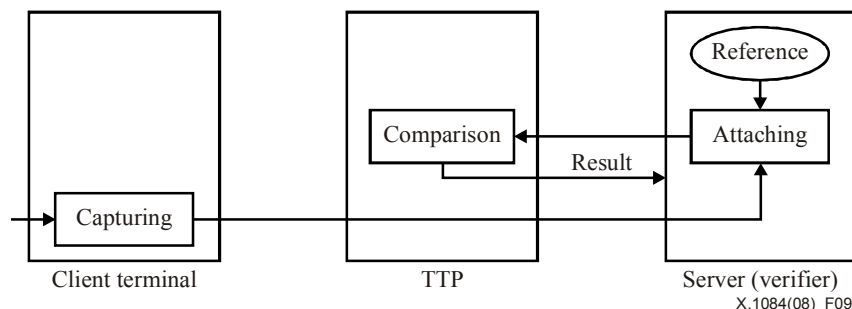


Figure 9 – Comparison outsourcing by server model

The verifier requests sample data from the client terminal, and verification with the user's template to TTP. TTP then achieves the comparison, and transfers the result to the verifier.

For this model, we assume a server cannot handle the cost of multiple biometric modes, so it requests a TTP to handle biometric modes.

This model requires trust in the data captured by a client.

Taking account of privacy protection, a server receives advance approval from a user to outsource the comparison to a TTP.

Template ID information is required in the comparison result.

9) *Storage and comparison outsourcing model*

Figure 10 illustrates the storage and comparison outsourcing model.

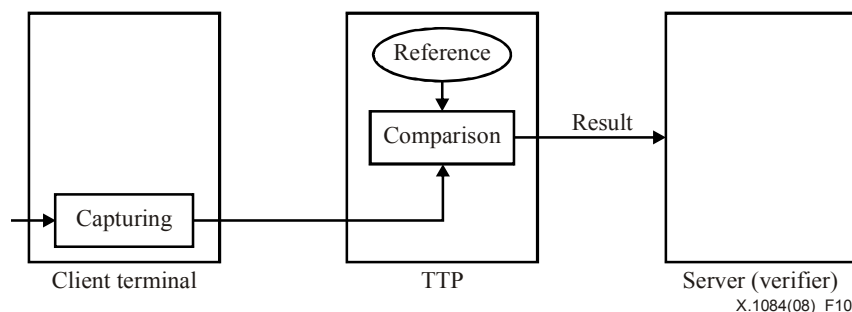


Figure 10 – Storage and comparison outsourcing model

For this model, we assume that client resources (memory, disk, etc.), are insufficient, and that the server-side has no comparison ability, meaning the client does not trust the server.

This can be compared with the outsourcing by client model and outsourcing by server model.

In the former case, the verifier requests verification from the client terminal. The client terminal captures the sample data, and requests the verification result from a TTP with the captured sample data. Therefore, the TTP compares sample data with the registered user's template, and transfers the result to the client terminal. The final result is transferred from the client terminal to the verifier.

In the latter case, on the other hand, the verifier requests sample data from the client terminal, and it obtains the captured sample data from the client terminal. The verifier requests, the verification result from a TTP. The result is transferred to the verifier.

A user registers its biometric reference template in advance with a TTP and outsources the comparison processing to the same TTP.

This model also requires the TTP, (server), to trust client capture-data. Template ID information is required in the comparison result.

8 Security threats for each models

Table 2 shows security threats allowing illegal use by an unauthorized user and possible counter measures for each model.

Table 2 – Security threats for each model

Model	Threats allowing illegal use by unauthorized users	Possible countermeasures
1) Local	– They may use illegal biometric reference template data – They may use an illegal comparison program – They may replace illegal capture data, such as stolen or altered data – They may replace illegal result data	– Reference with signature – Secure client – Client authentication
2) Download	– They may use an illegal comparison program – They may replace illegal capture data, such as stolen or altered data – They may replace illegal result data	– Secure client – Client authentication
3) Attached	– They may use illegal biometric reference template data – They may replace illegal capture data, such as stolen or altered data	– Reference with signature – Secure client – Client authentication
4) Centre	– They may replace illegal capture data, such as stolen or altered data	– Secure client – Client authentication
5) Reference management on TTP for local	– They may use an illegal comparison program – They may replace illegal capture data, such as stolen or altered data – They may replace illegal result data	– Secure client – Client authentication
6) Reference management on TTP for centre	– They may replace illegal capture data, such as stolen or altered data	– Secure client – Client authentication

Table 2 – Security threats for each model

Model	Threats allowing illegal use by unauthorized users	Possible countermeasures
7) Comparison outsourcing by client	– They may use illegal biometric reference template data – They may use an illegal comparison program – They may replace illegal capture data, such as stolen or altered data	– Reference with a signature – Secure client – Client authentication
8) Comparison outsourcing by server	– They may replace illegal capture data, such as stolen or altered data	– Secure client – Client authentication
9)-1 Storage and comparison outsourcing by client	– They may replace illegal capture data, such as stolen or altered data – They may use an illegal party	– Secure client – Client authentication – Validity check to the TTP of the client
9)-2 Storage and comparison outsourcing by server	– They may replace illegal capture data, such as stolen or altered data – Unauthorized user may request an illegal party	– Secure client – Client authentication – Validity check to the TTP of the server

In addition, Figure 11 illustrates specific threats for cooperation of PKI, and a biometric authentication, such as the environment of this Recommendation. For a model that incorporates PKI, there remains the threat of a private key leaking out, and that somebody may use it illegally, such as case a). Even without private key leakages, such as case b), the relation between PKI information and biometric template information may not be guaranteed. Therefore, the biometric template information should require the identifying information of the PKI certificate and the validity information for itself. This Recommendation assumes the use of a biometric certificate (BC) of [ITU-T X.1089] as the biometric template.

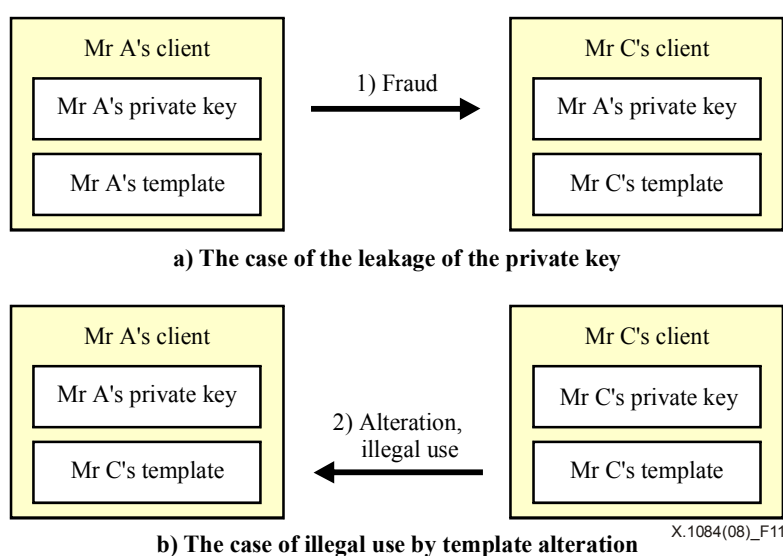


Figure 11 – Risk of illegal use by falsification of the template

Possible threats to private information protection on a server or with a TTP are listed below:

- Biometric and private information fraud through an illegal server.
- Biometric and private information fraud through an illegal TTP.
- Biometric and private information fraud through connecting to an illegal network.

Countermeasures are listed below:

- Authenticate a server using the PKI.
- Authenticate a TTP using the PKI.
- Encrypt the session key exchange by use of TLS protocol as specified in [IETF RFC 4346].

9 General requirements

1) *Requirement for authentication policies in the verifier*

The following are conditions for a security policy which is required to offset threats to server-side biometrics.

- A statement of the acceptable biometric technologies (modality, device, algorithm), with ordering by use of priorities
- A statement of the acceptable false acceptance level (threshold for each biometric technology, number of attempts)
- A statement of the acceptable client security level ([ISO/IEC 15408-1] authentication protection profile (PP), evaluation assurance level (EAL) for PP)
- A statement of the acceptable biometric system models (9 models – see clause 7) with priorities
- A statement of the acceptable cryptography procedures (method, key length) with priorities
- A statement of the acceptable biometric data quality (reference and captured sample quality)
- A statement of the acceptable biometric TTP site for the use of TTP models.

In addition to the security conditions listed above, the verifier should manage the following parameters:

- Profiles for suitable biometric technology when comparison is performed on an application server, such as the attached model, centre model, or storage outsourcing by server model
- Profiles of biometric technology (device, algorithm) which should be approved in advance.

2) *Authentication parameter in the client*

There are two types of parameter for the authentication parameter in the client. Those are the profile of the client terminal and the privacy settings by client user. The profile of the client terminal should be certified by TTP, with regard to its performance and security assurance level. This certificate or report is provided in BDC in [ITU-T X.1089].

- Regarding a profile of client terminal:
 - Profiles (quality as specified in [ISO/IEC 19785-1]) for collectable biometric sample using the client-side
 - Profiles (authentication accuracy as specified in [ISO/IEC 19795-1]) for suitable biometric modes using the client-side
 - Type of biometric reference template held by a client user
 - Client security guarantee (EAL, functional level as specified in [ISO/IEC 15408-1])
 - Client cryptography (method, key length).

- Regarding privacy settings by client user:
 - System model acceptable to a user (9 models) for each service provider
 - Application server, acceptable to a user, that presents biometric sample
 - TTP, acceptable to a user, that presents biometric sample.

10 General protocol

This Recommendation provides a handshake protocol as specified in [IETF RFC 4346] for a negotiation of the policies in the verifier and the functions and acceptable system model in the client. Furthermore, this Recommendation provides a transfer protocol for a biometric data for each negotiated system model (see Figure 12).

However, the transfer protocol for the biometric data has variable implementations. This clause describes the handshake protocol, and clause 11 describes the requirements for biometric transportation data for each system model. The transfer protocol is described in Appendices I and II.

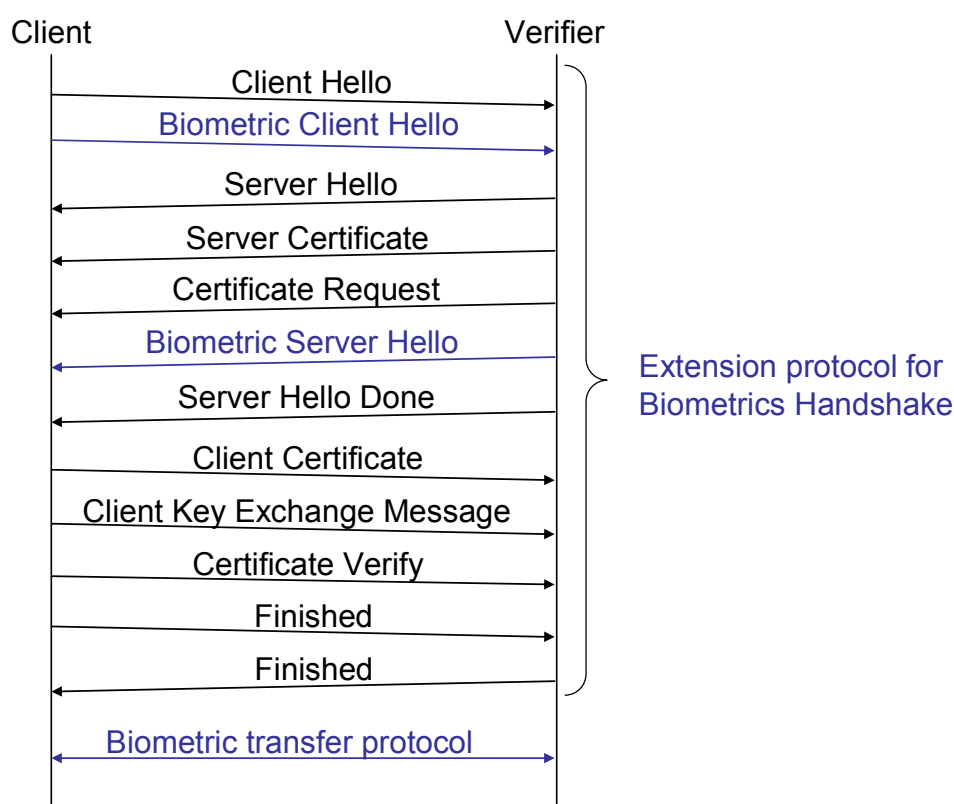


Figure 12 – Extended TLS protocol for biometrics handshake

The following subclauses describe the extended TLS protocol for a biometrics handshake, as specified in [IETF RFC 4366].

10.1 Requirement of the biometrics handshake protocol

10.1.1 Extended protocol for biometric handshake protocol

This Recommendation recommends the use of two extended handshake messages, namely, "Biometric Client Hello" and "Biometric Server Hello". These messages are described in clauses 10.1.2 and 10.1.3. The extended handshake message structures are as follows:

```

Handshake ::= SEQUENCE {
    type          HANDSHAKE.&id({Handshakes}),
    value         HANDSHAKE.&Type({Handshakes}){@type}}
  
```

```

    }

    HANDSHAKE ::= CLASS {
        &Type,
        &id HandshakeType    UNIQUE
    }
    WITH SYNTAX {
        &Type IDENTIFIED BY &id
    }

    HandshakeType ::= INTEGER{
        hello-request          (0),
        client-hello           (1),
        server-hello           (2),
        certificate             (11),
        server-key-exchange     (12),
        certificate-request     (13),
        server-hello-done      (14),
        certificate-verify      (15),
        client-key-exchange     (16),
        finished                (20),
        biometric-client-hello  (101),
        biometric-server-hello  (102)
    } (0..255)

    Handshakes HANDSHAKE ::= {
        helloRequest |
        clientHello |
        serverHello |
        certificateList |
        serverKeyExchange |
        certificateRequest |
        serverHelloDone |
        certificateVerify |
        clientKeyExchange |
        finished |
        biometricClientHello |
        biometricServerHello,
        ...
    }

```

10.1.2 Biometric Client Hello

A list is sent from the client to the verifier. The list contains client-supported biometric models and user-approved biometric system models.

```

    biometricClientHello HANDSHAKE ::= {
        BiometricClientHello    IDENTIFIED BY biometric-client-hello
    }

    BiometricClientHello ::= SEQUENCE SIZE(1..MAX) OF BiometricMethod

```

Each biometric method contains the biometric type, a biometric function provider, a network authentication model and third-party information. The third-party information is required by the TTP models. It specifies the network address for the third party (URI as specified in [IETF RFC 3986]).

```

    BiometricMethod ::= SEQUENCE{
        biometricType          BiometricType,
        biometricFunctionProvider BSP-BFP-Schema,
        networkAuthenticationModel NetworkAuthenticationModel,
        thirdPartyInfo         UTF8String
    }

```

The biometric type and the BSP-BFP-Schema are defined in standard specifications of ISO/IEC JTC 1/SC 37 as specified in [ISO/IEC 19784-1]. This Recommendation complies with these reference standards for the following:

```

    BiometricType ::= BioAPI-BIR-BIOMETRIC-TYPE

    BioAPI-BIR-BIOMETRIC-TYPE ::= BIT STRING {
        typeMultipleBiometricTypes    (0),

```

```

typeFace                (1),
typeVoice                (2),
typeFinger               (3),
typeIris                 (4),
typeRetina               (5),
typeHandGeometry         (6),
typeSignatureSign        (7),
typeKeystroke             (8),
typeLipMovement          (9),
typeGait                 (12),
typeVein                 (13),
typeDNA                  (14),
typeEar                  (15),
typeFoot                 (16),
typeScent                 (17),
typeOther                (30),
typePassword             (31)
} (SIZE(32))

BSP-BFP-Schema ::= CHOICE {
    bSPSchema    BioAPI-BSP-SCHEMA,
    bFPSchema    BioAPI-BFP-SCHEMA
}

BSP-BFP-Schemas ::= SEQUENCE(SIZE(1..MAX)) OF BSP-BFP-Schema

```

This Recommendation describes network authentication models in clause 7. Each model is identified by the following numbers:

```

NetworkAuthenticationModel ::= BIT STRING {
    no-value                (0), -- no selection --
    local-model             (1),
    download-model          (2),
    attached-model          (3),
    center-model            (4),
    ref-onttp-for-local-model (5),
    ref-onttp-for-center-model (6),
    comparison-outsourcing-by-client-model (7),
    comparison-outsourcing-by-server-model (8),
    storage-comparison-outsourcing-by-client-model (9),
    storage-comparison-outsourcing-by-server-model (10)
} (SIZE (0..10))

```

10.1.3 Biometric Server Hello

Based on the server's security policy (user authentication policy), a supported biometric model and an approved biometric system are selected from a client-user list, and sent to the client by the verifier.

```

biometricServerHello    HANDSHAKE ::= {
    BiometricServerHello IDENTIFIED BY biometric-server-hello
}

BiometricServerHello ::= SEQUENCE {
    request    BiometricAuthenticationRequest
}

```

If the Biometric Client Hello does not have permissive network authentication models or biometric types, the server sends an alert message to the client (refer to clause 10.2) using one of the following description values.

```

AlertDescription ::= ENUMERATED{
    ...,
    unacceptable-model                (115), -- Extension item
    unacceptable-biometrics           (116), -- Extension item
    ...
}

```

The Biometric Authentication Request message is filled out according to the server's biometric authentication policy. It lists the selected biometric method, requests the score level of result in biometric comparison (request FMR as specified in [ISO/IEC 19784-1]), requests the number of

trials for biometric comparison process (request trial number), and requests the sample quality for biometric data.

```
Quality ::= INTEGER(0..100)

BiometricAuthenticationRequest ::= SEQUENCE {
    biometricMethod      BiometricMethod,
    requestFMR           BioAPI-FMR, -- (32-bit integer value:requestFMR/231-1)
    requestTrialNumber   INTEGER(1..15),
    requestQuality        Quality,
    requestTemplateData   XtsmTemplate OPTIONAL
    -- for download model (no value available)
}
```

10.2 Alert protocol for biometric handshake

The following describes the extended alert protocol of TLS for this Recommendation. This Recommendation defines the alert description number, from 115 to 117, in order to avoid a conflict with the TLS Extension definition as specified in [IETF RFC 4366].

- unsupported-extension (110)

This alert is the message of TLS extension [IETF RFC 4366]. This alert may be returned if the verifier received this extended biometrics handshake protocol in an unsupported fashion. This message is always fatal.

- unacceptable-model (115)

This alert may be returned if the verifier received the unacceptable models only (those that do not conform to the verification policy of the verifier). This message is always fatal.

- unacceptable-biometrics (116)

This alert may be returned if the verifier received unacceptable biometrics, modalities, biometric algorithms, or biometric devices only, which do not conform to the verification policy of the verifier. This message is always fatal.

- unsupported-biometrics (117)

In the server comparison models, the server received unsupported biometric algorithms only, which are not supported by the verifier. This message is always fatal.

```
Alert ::= SEQUENCE {
    level      AlertLevel,
    description AlertDescription
}

AlertLevel ::= ENUMERATED {
    warning (1),
    fatal (2)
}

AlertDescription ::= ENUMERATED {
    close-notify           (0),
    unexpected-message     (10),
    bad_record-mac         (20),
    decryption-failed      (21),
    record-overflow        (22),
    decompression-failure  (30),
    handshake-failure      (40),
    --41 is not defined, for historical reasons
    bad-certificate        (42),
    unsupported-certificate (43),
    certificate-revoked     (44),
    certificate-expired     (45),
    certificate-unknown     (46),
    illegal-parameter      (47),
    unknown-ca             (48),
    access-denied          (49),
}
```

```

decode-error                (50),
decrypt-error               (51),
export-restriction          (60),
protocol-version            (70),
insufficient-security       (71),
internal-error              (80),
user-canceled               (90),
no-renegotiation            (100),
unsupported-extension        (110),
certificate-unobtainable    (111),
unrecognized-name           (112),
bad-certificate-status-response (113),
bad-certificate-hash_value  (114),
unacceptable-model          (115),      -- Extension item for TSM
unacceptable-biometrics     (116),      -- Extension item for TSM
unsupported-biometrics       (117),      -- Extension item for TSM
}

```

10.3 Implementation of the extended protocol

10.3.1 Modification of the TLS record layer protocol

TLS protocol is able to be extended by using [IETF RFC 4366], with IETF consensus.

This Recommendation is based on [IETF RFC 4366] for this biometrics handshake protocol. [IETF RFC 4366] extended the message contents of Client Hello and Server Hello for TLS Extension protocol. However, this Recommendation does not comply with [IETF RFC 4366] without IETF consensus. Therefore, this Recommendation modifies the Record Layer of TLS as an original protocol, as outlined below:

```

TSMPlainText ::= SEQUENCE {
    protocolID ProtocolIdentifier,
    version     ProtocolVersion,
    fragment    CHOICE {
        change-cipher-spec-opaque ChangeCipherSpec,
        alert-opaque               Alert,
        biometric-handshake-opaque Handshake,
        application-data-opaque    ApplicationData
    }
}

ProtocolIdentifier ::= UINT8

ProtocolVersion ::= SEQUENCE {
    major  UINT8,
    minor  UINT8
}

ChangeCipherSpec ::= ENUMERATED {
    change-cipher-spec(1),
    ...
}

ApplicationData ::= Opaque

TSMCipherText ::= SEQUENCE {
    protocolID ProtocolIdentifier,
    type        ContentType,
    version     ProtocolVersion,
    fragment    CHOICE {
        stream GenericStreamCipher,
        block  GenericBlockCipher
    }
}

ContentType ::= ENUMERATED {
    change-cipher-spec (20),
    alert               (21),
    handshake           (22),
    application-data    (23),
    ...
}

```

10.3.2 General extension mechanism for the biometrics handshake protocol

These extended messages are described as follow:

1) Extended Client Hello (Client to Server)

As with the TLS Extension handshake protocol, a client sends a list of supported encryption methods and cipher suites (challenge code 1).

Extended Client Hello is given as follows:

```
clientHello HANDSHAKE ::= {
    ClientHello IDENTIFIED BY client-hello
}

ClientHello ::= SEQUENCE{
    client-version      ProtocolVersion,      -- Same as TLS protocol
    random              Random,                -- Same as TLS protocol
    session-id          SessionID,            -- Same as TLS protocol
    cipher-suites       CipherSuite,          -- Same as TLS protocol
    compression-methods CompressionMethod,    -- Same as TLS protocol
    ...,
    ...,
    client-hello-extension-list ExtensionValues -- Same as TLS Extension
}

EXTENSION ::= CLASS {
    &id ExtensionType UNIQUE,
    &Type
}
WITH SYNTAX {
    &Type IDENTIFIED BY &id
}

ExtensionType ::= INTEGER(0..66535)

Extensions EXTENSION ::= {
    ...
}

ExtensionValues ::= SEQUENCE OF ExtensionValue

ExtensionValue ::= SEQUENCE {
    extension-type      EXTENSION.&id({Extensions}),
    extension-data      EXTENSION.&Type({Extensions}{@extension-type})
}
```

2) Extended Server Hello (Server to Client)

As with the TLS Extension handshake protocol, a server selects (and sends) an encryption method from the list of encryption methods from the client, generates a cipher suite (challenge code 2), and then sends back a server hello message.

```
serverHello HANDSHAKE ::= {
    ServerHello IDENTIFIED BY server-hello
}

ServerHello ::= SEQUENCE{
    server-version      ProtocolVersion,      -- Same as TLS protocol
    random              Random,                -- Same as TLS protocol
    session-id          SessionID,            -- Same as TLS protocol
    cipher-suites       CipherSuite,          -- Same as TLS protocol
    compression-methods CompressionMethod,    -- Same as TLS protocol
    ...,
    ...,
    server-hello-extension-list ExtensionValues -- Same as TLS Extension
}
```

11 Requirements of the biometric transportation stage for each model

The following clauses describe the requirements of the exchange of data contents for all the models.

11.1 Local model

Figure 2 outlines a local model. Table 3 lists four items required for the result data.

Table 3 – Items required for local model

#	Items	Details
1	Information on biometric service/function providers (BSPs) for client processes	The verifier needs to know how the biometric process operates for the client. It divides some functions: capturing, pre-processing, and comparing. In BioAPI as specified in [ISO/IEC 19784-1], the services and functions define the BSPs (or BFPs). There are varying types of BSPs that provide all functions or only one function, or pre-processing and comparison functions. If the client anticipates all types of functions to be provided, it uses various BSPs together. Therefore, this item should be made able to define various BSPs. The verifier can then check whether the security level and the performance of all BSPs for the verifier's service are sufficiently high.
2	Reference template information for client processes	The verifier needs to know whose reference template is being used. However, this model is of the privacy protection type for the reference template. Therefore, this item should at minimum include reference template ID information. The verifier can then check the revocation template.
3	Sample data quality and comparison score (similarity) for client processes	The verifier needs sample data quality for input data of a comparison process as well as the comparison results in order to enable appropriate risk management of the verifier's service.
4	Security code of client processes	The verifier requires the assurance of the integrity of the client processes.

The following are examples for this message:

```

BDforLocalModel ::= SEQUENCE {
    biometricClientProcess      BiometricClientProcess,
    digitalSignature             SignedData,
    acforBioOnClient            ACBioInformation OPTIONAL
    -- see ISO/IEC 24761
}

BiometricClientProcess ::= SEQUENCE {
    bFPSchemaForClientProcess   SEQUENCE SIZE(1..MAX) OF BSP-BFP-Schema,
    templateID                  TemplateID,
    sampleQuality                Quality, -- specified in ISO/IEC 19784-1
    score                       BioAPI-FMR -- specified in ISO/IEC 19784-1
}

TemplateID ::= SEQUENCE {
    certificateIssuerName       Name, -- see Rec. ITU-T X.509
    serialNumber                CertificateSerialNumber, -- see Rec. ITU-T X.509
    templateinfo                TemplateInfo
}

TemplateInfo ::= SEQUENCE {
    biometricType               BiometricType,
    creator                     UTF8String,
    createdBFPSCHEMA            BSP-BFP-Schema, -- specified in ISO/IEC 19784-1
    templateID                  CertificateIDInformation
    -- such as CertificateSerialNumber (no value available)
}

```

Copyright © 2008 ITU-T. All rights reserved.

CertificateIDInformation ::= CertificateSerialNumber

11.2 Download model

Figure 3 outlines a download model.

It contains the same items required for the results data as the local model (see Table 3).

The following is a sample of Biometric Data for the download model on Biometric Verify. The content is the same as for the local model.

```
BDforDownloadModel ::= SEQUENCE {
    biometricClientProcess    BiometricClientProcess,
    digitalSignature          SignedData,
    aCforBioOnClient          ACBioContentInformation OPTIONAL
    -- see ISO/IEC 24761
}
```

Table 4 lists the items required for download data from the server in the download model. The verifier requires the template ID (=Certificate ID) in order to retrieve the reference template DB for this message (Client to Server). However, the verifier already has the certificate ID on the TLS handshake.

Table 4 – Items required for download data for download model

#	Item	Details
1	Reference template	The client requires the reference template for the comparison process (Server to Client).

This message includes the message of the Biometric Server Hello.

```
BiometricServerHello ::= SEQUENCE {
    request    BiometricAuthenticationRequest
}

BiometricAuthenticationRequest ::= SEQUENCE {
    biometricMethod    BiometricMethod,
    requestFMR          BioAPI-FMR, -- (32-bit integer value:requestFMR/231-1)
    requestTrialNumber  INTEGER(1..15),
    requestQuality       Quality,
    requestTemplateData  XtsmTemplate OPTIONAL
    -- for download model (no value available)
}
```

11.3 Attached model

Figure 4 outlines an attached model.

Table 5 lists the items required for the attached data for the attached model.

Table 5 – Items required for attached data for attached model

#	Items	Details
1	Reference template	The verifier requires the reference template for the comparison process in the server.
2	Sample data	The verifier requires sampling data and sampling device information. If the sampling data complies with [ISO/IEC 19784-1], then the data (BIR) contains BSP information. The verifier can then check the security level and the quality of the sampling data from the sensor device for the comparison process.
3	Security code of client process	The verifier requires the assurance of the integrity of the client processes.

The following is an example of this message:

```
BDforAttachedModel ::= SEQUENCE {
    templateData      XtsmTemplate,
    sampleData        SampleData,          -- BIR: BioAPI defined format --
    digitalSignature   SignedData,
    aCforBioOnClient  ACBioContentInformation OPTIONAL
                    -- see ISO/IEC 24761
}
```

11.4 Centre model

Figure 5 outlines a centre model. Table 6 lists the items required for the centre model.

Table 6 – Items required for the centre model

#	Item	Details
1	Sample data	The verifier requires sampling data and sampling device information. If the sampling data complies with [ISO/IEC 19784-1], then the data (BIR) contains BSP information. The verifier can then check the security level and the quality of the sampling data from the sensor device for the comparison process.
2	Security code of client process	The verifier requires the assurance of the integrity of the client processes.

The following is an example of this message:

```
BDforCenterModel ::= SEQUENCE {
    sampleData        SampleData,          -- BIR: BioAPI defined format --
    digitalSignature   SignedData,
    aCforBioOnClient  ACBioContentInformation OPTIONAL
                    -- see ISO/IEC 24761
}
```

11.5 Reference management on TTP for local model

Figure 6 outlines the reference management on TTP for the local model.

It has the same items required for the result data as the local model, except for the addition of reference registered third-party information and the process information on TTP.

The following is an example of this message:

```
BDforRefOnTTPforLocalModel ::= SEQUENCE {
    thirdPartyInfo      UTF8String,
    biometricClientProcess BiometricClientProcess,
```

```

aCforBioOnTTP      ACBioInformation,
digitalSignaturebyClient SignedData,
aCforBioOnClient   ACBioContentInformation OPTIONAL
-- see ISO/IEC 24761
}

```

Table 7 lists the items required for the download data from TTP for this model. The TTP requires a template ID (=Certificate ID) in order to retrieve a reference template DB for this message (Client to TTP). However, it should maintain the secure transportation between TTP and the client. Therefore, TTP already includes the certificate ID on the TLS handshake.

Table 7 – Items required for download data from TTP

#	Item	Details
1	Reference template	The client requires the reference template in TTP for the comparison process on the client terminal (TTP to client).
2	Security code of TTP process	The client and the verifier require an assurance of the integrity of the TTP processes.

The following is an example of this message:

```

BiometricTTPProcess ::= SEQUENCE {
    templateData      XtsmTemplate,
    digitalSignature   SignedData,
    aCforBioOnTTP     ACBioContentInformation OPTIONAL
-- see ISO/IEC 24761
}

```

Alert messages should be defined for illegal cases during the transmission between TTP, such as, for example, no response of TTP, or no reference template in TTP.

11.6 Reference management on TTP for centre model

Figure 7 outlines reference management on TTP for the centre model.

It has the same items as required for the captured data as the centre model, except for the addition of the reference registered third-party information.

The following is an example of this message:

```

BDforRefOnTTPforCenterModel ::= SEQUENCE {
    thirdPartyInfo    UTF8String,
    sampleData        SampleData,      -- BIR: BioAPI defined format --
    digitalSignature   SignedData,
    aCforBioOnClient  ACBioContentInformation OPTIONAL
-- see ISO/IEC 24761
}

```

Tables 8 and 9 list the items required for the download data from TTP for this model.

Table 8 – Items required for download request to TTP

#	Item	Details
1	Reference template ID	TTP requires the template ID (=Certificate ID) in order to retrieve a reference DB (Server to TTP). It should maintain the secure transportation between TTP and the server.

The following is an example of this message:

```

TTPRequestRefOnTTPforCenterModel ::= SEQUENCE {
    templateID        TemplateID
}

```

Table 9 – Items required for download data from TTP

#	Item	Details
1	Reference template	The verifier requires the reference template in TTP for the comparison process on the server (TTP to Server).
2	Security code of TTP process	The verifier requires an assurance of the integrity of the TTP processes.

The following is an example of this message:

```

TTPResponseRefOnTTPforCenterModel ::= SEQUENCE {
    templateData      XtsmTemplate,
    digitalSignature   SignedData,
    aCforBioOnTTP     ACBioContentInformation OPTIONAL
    -- see ISO/IEC 24761
}

```

Alert messages should be defined for illegal cases during the transmission between TTP, such as, for example, no response of TTP, or no reference template in TTP.

11.7 Comparison outsourcing by client model

Figure 8 outlines comparison outsourcing by the client model.

1) Client to TTP

**Table 10 – Items required for data attached to TTP
for comparison outsourcing by client model**

#	Items	Details
1	Reference template	TTP requires a reference template in the client terminal for the comparison process in TTP.
2	Sample data	TTP requires sampling data on the client terminal for the comparison process in TTP. The sampling data should comply with [ISO/IEC 19784-1] (BIR). The BIR format contains BSP information.

The following is an example of this message:

```

TTPRequestCObyClientModel ::= SEQUENCE {
    templateData      XtsmTemplate,
    sampleData        SampleData      -- BIR: BioAPI defined format --
}

```

2) TTP to Client

**Table 11 – Items required for comparison result data to client
for comparison outsourcing by client model**

#	Items	Details
1	Information on BSP(s) for TTP process	The verifier needs to know how the biometric process operates in TTP. This item clarifies information on BSPs in the TTP process.
2	Sample data quality and comparison score (similarity) for TTP process	The verifier requires sample data quality for input data of the comparison process, and the results of the comparison to enable appropriate risk management of the verifier's services.
3	Security code of TTP process	The client & the verifier require the assurance of the integrity of TTP processes.

The following is an example of this message:

```
TTPResponseCObyClientModel ::= SEQUENCE {
    bFPSchemaOnTTPProcess SEQUENCE SIZE(1..MAX) OF BSP-BFP-Schema,
    templateID             TemplateID,
    sampleQuality           Quality,
    score                   BioAPI-FMR,
    digitalSignature        SignedData,
    aCforBioTTP             ACBioContentInformation OPTIONAL
    -- see ISO/IEC 24761
}
```

Alert messages should be defined for illegal cases during the transmission between TTP, such as, for example, no response of TTP.

3) Client to Server

Table 12 – Items required for local model

#	Items	Details
1	TTP information	The verifier needs to know who the outsourcer is, and who operates the biometric comparison process, so as to enable appropriate risk management of the verifier's services.
2	Information on BSP(s) for client & TTP processes	The verifier needs to know how the biometric process operates for the client. It divides some functions: capturing, pre-processing, and comparing. In [ISO/IEC 19784-1], the services and functions define the BSPs (or BFPs). There are varying types of BSPs that provide all functions or only one function, or pre-processing and comparison functions. If the client anticipates all types of functions to be provided, it uses various BSPs together. Therefore, this item should be made available to define various BSPs. The verifier can then check whether the security level and the performance of all BSPs for the verifier's service are sufficiently high.
3	Reference template information for client process	The verifier needs to know whose reference template is being used. However, this model is of the privacy protection type for the reference template. Therefore, this item should at minimum include reference template ID information. The verifier can then check the revocation template.
4	Sample data quality and comparison score (similarity) for TTP processes	The verifier needs sample data quality for input data of a comparison process as well as the comparison results in order to enable appropriate risk management of the verifier's service.
5	Security code of all processes	The verifier requires the assurance of the integrity of client and TTP processes.

The following is an example of this message:

```
BDforCObyClientModel ::= SEQUENCE {
    bFPSchemaForClientProcess SEQUENCE SIZE(1..MAX) OF BSP-BFP-Schema,
    thirdPartyInfo            UTF8String,
    bFPSchemaforTTPProcess    SEQUENCE SIZE(1..MAX) OF BSP-BFP-Schema,
    templateID                TemplateID,
    sampleQuality              Quality,
    score                      BioAPI-FMR,
    digitalSignaturebyClient   SignedData,
    digitalSignaturebyTTP      SignedData,
    aCforBioOnClient           ACBioContentInformation OPTIONAL,
    aCforBioOnTTP              ACBioContentInformation OPTIONAL
    -- see ISO/IEC 24761
}
```

}

11.8 Comparison outsourcing by server model

Figure 9 outlines comparison outsourcing by the server model.

1) Client to Server

Table 13 – Items required for comparison outsourcing by server model

#	Item	Details
1	Sample data	The verifier requires sampling data and sampling device information. If the sampling data complies with [ISO/IEC 19784-1], then the data (BIR) contains BSP information. The verifier can then check the security level and the quality of the sampling data from the sensor device for the comparison process.
2	Security code of client processes	The verifier requires the assurance of the integrity of the client processes.

The following is an example of this message:

```
BDforCObyServerModel ::= SEQUENCE {
    sampleData      SampleData,      -- BIR: BioAPI defined format --
    digitalSignature SignedData,
    acforBiometrics ACBioContentInformation OPTIONAL
    -- see ISO/IEC 24761
}
```

2) Server to TTP

Table 14 – Items required for attached data for comparison outsourcing by server model

#	Items	Details
1	Reference template	TTP requires a reference template for the comparison process in TTP.
2	Sample data	TTP requires a sample BIR for the comparison process in TTP.

The following is an example of this message:

```
TTPRequestCObyServerModel ::= SEQUENCE {
    templateData XtsmTemplate,
    sampleData SampleData      -- BIR: BioAPI defined format --
}
```

3) TTP to Server

Table 15 – Items required for comparison outsourcing by server model

#	Items	Details
1	Information on BSP(s) for TTP process	The verifier needs to know how the biometric process operates in the client. TTP must obtain comparison results from the received data. This item clarifies information on BSPs in the TTP process.
2	Sample data quality and comparison score (similarity) for TTP process	The verifier requires sample data quality for input data of the comparison process and the comparison results, so as to enable appropriate risk management of the verifier's services.
3	Security code of TTP process	The verifier requires the assurance of the integrity of TTP processes.