INTERNATIONAL STANDARD

ISO/IEC 17922

First edition
2017-09

Information technology — Security techniques — Telebiometric authentication framework using biometric hardware security module

Technologies de l'information — Techniques de sécurité — Infrastructure d'authentification télébiométrique utilisant un module de sécurité matériel biométrique

Reference number
ISO/IEC 17922:2017(E)

ISO copyright office
Ch. de Blandonnet 8 • CP 401
CH-1214 Vernier, Geneva, Switzerland
Tel. +41 22 749 01 11
Fax +41 22 749 09 47
copyright@iso.org
www.iso.org

Foreword

ISO (the International Organization for Standardization) and IEC (the International Electrotechnical Commission) form the specialized system for worldwide standardization. National bodies that are members of ISO or IEC participate in the development of International Standards through technical committees established by the respective organization to deal with particular fields of technical activity. ISO and IEC technical committees collaborate in fields of mutual interest. Other international organizations, governmental and non-governmental, in liaison with ISO and IEC, also take part in the work. In the field of information technology, ISO and IEC have established a joint technical committee, ISO/IEC JTC 1.

The procedures used to develop this document and those intended for its further maintenance are described in the ISO/IEC Directives, Part 1. In particular the different approval criteria needed for the different types of document should be noted. This document was drafted in accordance with the editorial rules of the ISO/IEC Directives, Part 2 (see www.iso.org/directives).

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO and IEC shall not be held responsible for identifying any or all such patent rights. Details of any patent rights identified during the development of the document will be in the Introduction and/or on the ISO list of patent declarations received (see www.iso.org/patents).

Any trade name used in this document is information given for the convenience of users and does not constitute an endorsement.

For an explanation on the voluntary nature of standards, the meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the World Trade Organization (WTO) principles in the Technical Barriers to Trade (TBT) see the following URL: www.iso.org/iso/foreword.html.

This document was prepared by ISO/IEC JTC 1, *Information technology*, SC 27, *IT Security techniques*, in collaboration with ITU-T. The identical text is published as ITU-T X.1085 (10/2016).

INTERNATIONAL STANDARD ISO/IEC 17922
RECOMMENDATION ITU-T X.1085

Information technology – Security techniques – Telebiometric authentication framework using biometric hardware security module

Summary

Recommendation ITU-T X.1085 | ISO/IEC 17992 describes a telebiometric authentication scheme using biometric hardware security module (BHSM) for the telebiometric authentication of proving owner of ITU-T X.509 certificate registered individual at registration authority (RA). This Recommendation | International Standard provides the requirements for deploying the BHSM scheme to securely operate the telebiometric authentication under PKI environments. The scheme focuses on providing how to assure the telebiometric authentication with biometric techniques and hardware security module and it also suggests ASN.1 standard format for including the proposed scheme in ITU-T X.509 framework when telebiometric authentication and ITU-T X.509 certificate are combined to prove the owner of the certificate.

History

Edition	Recommendation	Approval	Study Group	Unique ID*
1.0	ITU-T X.1085	2016-10-14	17	11.1002/1000/13060

Keywords

Biometric hardware security module, BHSM, ITU-T X.509 certificate, ISO/IEC 24761, pseudonymous identifier, PSID, public key infrastructure, PKI, telebiometric authentication.

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

FOREWORD

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

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

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

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

NOTE

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

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

INTELLECTUAL PROPERTY RIGHTS

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

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

CONTENTS

Introduction

This Recommendation | International Standard describes a telebiometric authentication scheme using a biometric hardware security module (BHSM) for the telebiometric authentication of the person who presents the BHSM as the owner of an ITU-T X.509 certificate embedded in the BHSM as registered with the certification authority (CA). This Recommendation | International Standard provides the requirements for deploying a BHSM scheme to provide secure telebiometric authentication within public key infrastructure (PKI) environments. The scheme provides assurance for telebiometric authentication using biometric recognition integrated into a hardware security module. It also provides ASN.1 definitions that allow the biometric authentication to be incorporated into an ITU-T X.509 framework to authenticate the user as the owner of the ITU-T X.509 certificate.

INTERNATIONAL STANDARD
ITU-T RECOMMENDATION

Information technology – Security techniques – Telebiometric authentication framework using biometric hardware security module

1 Scope

To prove ownership of an ITU-T X.509 certificate registered individually with the registration authority (RA), a biometric hardware security module has been considered to provide a high-level biometric authentication. This Recommendation | International Standard provides a framework for telebiometric authentication using BHSM.

Within the scope of this Recommendation | International Standard, the following issues are addressed:

– telebiometric authentication mechanisms using BHSM in telecommunication network environments; and

– abstract syntax notation one (ASN.1) format and protocols for implementing the mechanisms in the ITU-T X.509 framework.

The related standard environment is depicted in Figure 1. The main role of this Recommendation | International Standard is to harmonize with existing telebiometric authentication and public key infrastructure (PKI) standards and to establish a standard mechanism using BHSM to verify the ownership of the ITU-T X.509 certificate in the telebiometric environment.

NOTE – In this Recommendation | International Standard, ITU-T X.509 certificate means ITU-T X.509 public-key certificate.

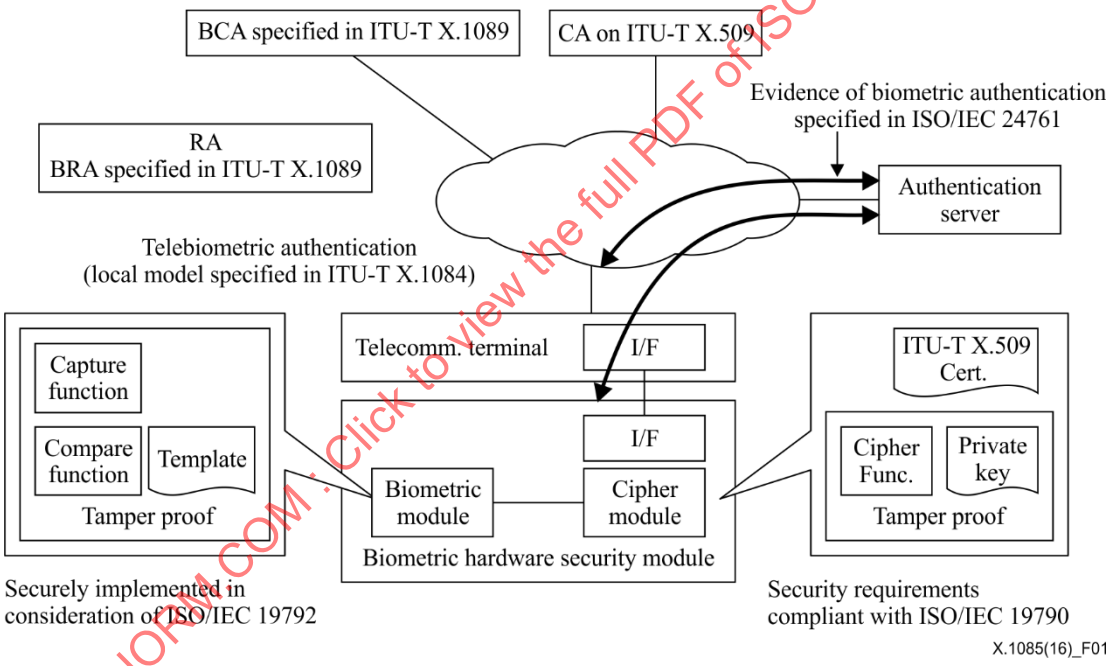

Figure 1 – Standard environment for BHSM

2 Normative references

The following Recommendations and International Standards contain provisions which, through reference in this text, constitute provisions of this Recommendation | International Standard. At the time of publication, the editions indicated were valid. All Recommendations and Standards are subject to revision, and parties to agreements based on this Recommendation | International Standard are encouraged to investigate the possibility of applying the most recent edition of the Recommendations and Standards listed below. Members of IEC and ISO maintain registers of currently valid International Standards. The Telecommunication Standardization Bureau of the ITU maintains a list of currently valid ITU-T Recommendations.

2.1 Identical Recommendations | International Standards

– Recommendation ITU-T X.509 (2016) | ISO/IEC 9594-8:2016, *Information technology – Open Systems Interconnection – The Directory: Public-key and attribute certificate frameworks*.

2.2 Paired Recommendations | International Standards equivalent in technical content

None.

2.3 Additional references

- ISO/IEC 24745:2011, *Information technology – Security techniques – Biometric information protection*.
- ISO/IEC 24761:2009, *Information technology – Security techniques – Authentication context for biometrics*.
- ISO/IEC 19790:2012, *Information technology – Security techniques – Security requirements for cryptographic modules*.
- ISO/IEC 19792:2009, *Information technology – Security techniques – Security evaluation of biometrics*.

3 Definitions

3.1 Terms defined in this Recommendation | International Standard

For the purposes of this Recommendation | International Standard, the following definitions apply:

3.1.1 biometric hardware security module: Hardware security module incorporating biometric sensor(s) and biometric recognition to authenticate the user.

NOTE – In case of a comparison of biometric hardware security modules, they come traditionally in the form of a smart card but recently also in the form of a universal serial bus (USB) type security token which can be attached directly to general purpose computers.

3.1.2 hardware security module: Hardware implementation of a secure crypto-processor using an ITU-T X.509 certificate and a private key to provide secure authentication.

3.1.3 telebiometric authentication: Biometric authentication utilising data communication by telephony, radio or a related technology.

3.2 Terms defined in other International Standards

3.2.1 The following terms are defined in ISO/IEC 2382-37:

a) **biometric reference**: One or more stored biometric samples, biometric templates or biometric models attributed to a biometric data subject and used as the object of biometric comparison.

b) **biometric sample**: Analogue or digital representation of biometric characteristics prior to biometric feature extraction.

3.2.2 The following term is defined in ISO/IEC 9798-1:

a) **entity authentication**: Corroboration that an entity is the one claimed.

3.2.3 The following terms are defined in ISO/IEC 24745:

a) **identity reference**: Non-biometric attribute that is an identifier with a value that remains the same for the duration of the existence of the entity in a domain.

b) **pseudonymous identifier**: Part of a renewable biometric reference that represents an individual or data subject within a certain domain by means of a protected identity that can be verified by means of a captured biometric sample and the auxiliary data (if any).

c) **renewability**: Property of a transform or process to create multiple, independent transformed biometric references derived from one or more biometric samples obtained from the same data subject and which can be used to recognize the individual while not revealing information about the original reference.

d) **renewable biometric reference**: Revocable or renewable identifier that represents an individual or data subject within a certain domain by means of a protected binary identity (re)constructed from the captured biometric sample.

NOTE – A renewable biometric reference consists of a pseudonymous identifier and additional optional data elements required for biometric verification or identification such as auxiliary data.

e) **revocability**: Ability to prevent future successful verification of a specific biometric reference and the corresponding identity reference.

4 Abbreviations

For the purposes of this Recommendation | International Standard, the following abbreviations apply:

ACBio Authentication Context for Biometrics
ASN.1 Abstract Syntax Notation One
BCA Biometric Certificate Authority
BHSM Biometric Hardware Security Module
BIR Biometric Information Record
BRA Biometric Registration Authority
BRT Biometric Reference Template
BR Biometric Reference
CA Certification Authority
CSR Certificate Signing Request
DN Distinguished Name
EPSID Encrypted PSID
HSM Hardware Security Module
I/F Interface
IR Identity Reference
OID Object Identifier
PIN Personal Identification Number
PKI Public-Key Infrastructure
PSID Pseudonymous Identifier
RA Registration Authority
RBR Renewable Biometric Reference
USB Universal Serial Bus

NOTE 1 – Pseudonymous identifier (PSID) used in this Recommendation | International Standard is the same as PI in ISO/IEC 24745.

NOTE 2 – BRT is only used in the BRT certificate.

5 Symbols and terminology

For the purpose of this Recommendation | International Standard, the following conventions apply for mathematical expressions.

E Encryption function

h Hash function

pk Digital signature verification key (public key)

R Bit string random number

R_a Bit string random number used for implementing challenge/response authentication between the CA and the biometric hardware security module (BHSM)

Sign Digital signing

sk Digital signature generation key (private key)

6 Biometric hardware security module for telebiometric authentication

6.1 Additional feature of BHSM to the HSM

A hardware security module (HSM) manages and protects critical private keys using digital signing for the purpose of providing strong authentication. Hardware security modules are physical devices that traditionally come in the form of

smartcards or universal serial bus (USB) security tokens that are tamper resistant against penetration and modification of an internal operation and insertion of active or passive tapping mechanism to disclose secret data or to alter the operation of devices.

The cryptographic material handled by most hardware security modules are public/private key pairs (and certificates) used in public-key cryptography related to ITU-T X.509 certificates used for, e.g., encryption/decryption and digital signature. If the private key is compromised the certificates and digital signatures can no longer be relied on and transactions using the HSM could be fraudulent with potentially serious adverse impacts to the owner of the key and to other parties to the transaction. The physical security provided by a properly implemented HSM can normally be considered as high.

However, physical security is only one factor in the overall security for authentication. The overall security is ultimately limited by the assurance that HSM is being used by its legitimate owner. Typically the binding of the HSM to the owner is provided by means of a secret personal identification number (PIN) or password that should be known only to the legitimate owner. The strength of the binding associated with passwords is generally considered to be low as passwords may be compromised through accident or carelessness on the part of the owner, by deliberate disclosure or by mechanized attacks on password databases. The use of biometric authentication to augment or replace a password or PIN can provide stronger binding and increased authentication assurance.

When a HSM containing a private key is used for a personal public-key infrastructure (PKI) based authentication, the verifier can check only that the HSM certificate belongs to a known legitimate owner. However it cannot validate that the person using the HSM and claiming to be its owner is the legitimate owner. If the HSM comes into the possession of another person, intentionally or by accident, and the password is also transferred, by collusion between the parties or by discovery, the HSM could be used to conduct fraudulent transactions. A biometric hardware security module is a HSM that uses biometrics to authenticate the user locally to the module in order to provide additional assurance for transactions.

6.2 General scenario for use of the BHSM

The use of the BHSM is limited to the authentication of users of services to the providers of the services. As such, it forms part of a larger system that provides the services and the user access to the services. In this kind of scenario, the user interacts with a service through a client interface (I/F), e.g., a personal computer or a mobile device. The BHSM is connected to the client and electrical signals flowing between the BHSM and the user or the service pass through the client as intermediary.

The client connects to the service through a telecommunication link or network, e.g., the Internet. Where the descriptions and protocol in this Recommendation | International Standard refer to data and commands being exchanged between the user and the BHSM or the BHSM and the service, it is understood that they are routed through the client. In some instances the BHSM will be a physically separate device which connects to the client. In other instances the BHSM may be physically embedded in the client (e.g., a mobile phone) but in both cases the BHSM is regarded as a distinct and separate module.

There may be mechanisms in place to protect the communications between the client and the service but these are not addressed is this Recommendation| International Standard. The security measures and protocols described in this Recommendation| International Standard are solely concerned with the authentication of the user to the service using the BHSM. This includes measures to ensure secure end-to-end communication between the BHSM and the service so that, for example, an impostor could not authenticate to a service as an authorized user by means of a stolen or fake BHSM or client.

6.3 Telebiometric authentication using the BHSM

Telebiometric authentication can provide secure user authentication by using the biometric authentication over open networks but in some models biometric information has to be transmitted to authentication servers through the open network. In using biometrics, consideration needs to be given to the security and privacy of the biometric information. To this end, the integration of biometric authentication with a HSM can be a solution since the biometric information can remain under the control of the user within a tamper resistant module. In this case, biometric references are stored only in the BHSM and not on the authentication server and are not required to be transferred over the open network. Consideration should be given to the use of renewable biometric references (RBRs) and pseudonymous identifiers so that, if a biometric reference (BR) becomes compromised, it can be revoked and a new reference provided for the user together with a new pseudonymous identifier. The use of renewable biometric references and pseudonymous identifiers ensures that no biometric data related to the revoked biometric reference can be extracted from the pseudonymous identifier.

The BHSM based telebiometric authentication scheme described in this Recommendation | International Standard relies on an existing PKI and should be integrated with it appropriately. This Recommendation | International Standard supports asymmetric key pairs using RSA cryptography or other types of cryptography that support encryption/decryption. This

Recommendation| International Standard describes a method for binding the biometric information of the registered user of the BHSM with an ITU-T X.509 certificate.

The BHSM operation and transaction protocols described in this Recommendation | International Standard relate to the following role players:

- a user, a BHSM owner whose ITU-T X.509 certificate and biometric reference are stored in BHSM;
- an authentication server, and a relying party that requires the authentication of the user;
- a registration authority which registers the biometric reference of the user and provides biometric recognition information that is stored in the user's BHSM;
- a certification authority (CA) which issues the user's ITU-T X.509 certificate.

Within this Recommendation | International Standard, the following recommendations are stated.

- the CA should be capable of supplying ITU-T X.509 certificates with the PSID;
- the CA shall not use the original biometric reference of the user anywhere within a public-key certificate, in order to avoid the possibility of disclosing the user's private biometric data;
- to protect the user's personally identifiable information and privacy, the user's biometric data should not leave the BHSM. During enrolment and biometric authentication only the PSID should leave the BHSM.

7 Telebiometric authentication with biometric hardware security module

7.1 General

This Recommendation | International Standard describes two methods for enrolment and authentication using a BHSM. The first describes a protocol using an ITU-T X.509 certificate extension to contain the user identification information. The second describes a modified protocol that uses an ITU-T X.509 certificate in association with an ISO/IEC 24761 authentication context for biometrics (ACBio) implementation.

The integrity and assurance of enrolment depends on the existence of a trust relationship between the RA and the CA, and on the enrolment procedures being wholly conducted under the continuous supervision of the RA. The RA in a PKI has a much more limited role than the RA as specified in this Recommendation | International Standard. So, this is an underlying assumption in the enrolment procedures described in 7.2.1 and 7.2.2. Note that if these conditions are not realised, enrolment integrity and assurance may be compromised.

7.2 Enrolment procedures

7.2.1 Enrolment procedure using ITU-T X.509 certificate extension

The enrolment process for issuing a BHSM containing an ITU-T X.509 certificate is shown in Figure 2. For security assurance, the whole of the enrolment process described in steps a)-h) below should be brought under the control of the RA. For a detailed description of digital signatures for non-repudiation, see ISO/IEC 15945.

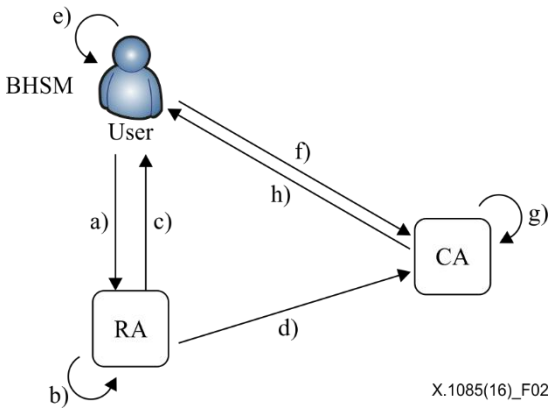

Figure 2 – Enrolment procedure with BHSM

a) The user visits RA in person where their identity and authorization are established. The relevant user biometric characteristics are captured and a biometric reference is generated for the user. RA provides a BHSM for the user and stores the user's biometric reference in BHSM;

b) RA creates a PSID – see 8.1.2 for further information on generating a PSID;

c) RA stores the PSID in the user's BHSM;

d) RA sends the generated PSID to CA;

e) After the user successfully performs biometric authentication to the BHSM, he/she generates his/her private and public keys within BHSM;

f) The user generates certificate signing request (CSR) to CA requesting ITU-T X.509 certificate after successful biometric authentication using BHSM;

g) CA generates the user's ITU-T X.509 certificate including the PSID in the **subjectAltName** extension field containing a **directoryName**;

h) CA sends the user's ITU-T X.509 certificate, which will then be securely stored in the user's BHSM.

NOTE – In this Recommendation | International Standard, the role of user's public and private key are not described in detail since they will be used for conventional public-key crypto systems such as encryption/decryption and digital signature. In addition, the precise public key encryption and signing methodologies used will depend on the crypto-system selected (e.g., RSA vs Elliptic Curve).

7.2.2 Enrolment procedures applying ISO/IEC 24761

The enrolment process for issuing an ITU-T X.509 certificate and a biometric reference template (BRT) certificate, which is specified in ISO/IEC 24761, to use BHSM is depicted in Figure 3. In Figure 3, the complete set of enrolment procedures are depicted. For assuring security, the whole of the enrolment process should be brought under the control of the RA.

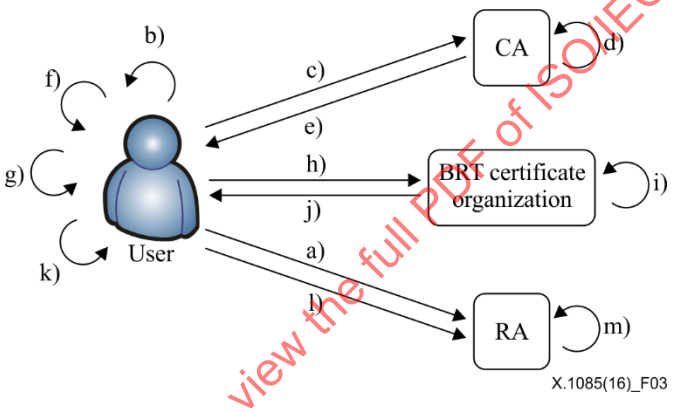

Figure 3 – Enrolment procedure with BHSM using ACBio

a) the user visits RA in person where their identity and authorization are established;

b) the user generates a pair of public and private key in BHSM;

c) the user sends an ITU-T X.509 certificate issuance request to CA;

d) CA generates an ITU-T X.509 certificate following the request;

e) CA sends ITU-T X.509 certificate to the user;

f) the user stores the ITU-T X.509 certificate in BHSM;

g) the user generates a biometric reference and the ACBio instance for enrolment;

h) the user sends the BRT certificate issuance request with the values of **serialNumber** and issuer in the ITU-T X.509 certificate and the ACBio instance for enrolment to the BRT certificate organization;

i) the BRT certificate organization generates the BRT certificate setting the value of **serialNumber** to **pkiCertificateSerialNumber** field, the value of issuer to **pkiCertificateIssuerName** field, and the ACBio instance for enrolment to **enrolmentACBioInstances** field respectively;

j) the BRT certificate organization sends the BRT certificate to the user;

k) the user stores the BRT certificate as well as the biometric reference in BHSM;

l) the user sends the ITU-T X.509 certificate and BRT certificate to RA for registration;

m) RA stores the ITU-T X.509 certificate and the BRT certificate in the user database.

NOTE – Identification is necessary for the issuance of ITU-T X.509 certificates and BRT certificates but the identification process is omitted in the above description.

7.3 Telebiometric authentication processes

7.3.1 Authentication process using ITU-T X.509 certificate extension

The telebiometric authentication process with BHSM can be described as shown in Figure 4, and more detailed information flow in BHSM and the service provider are shown in Figure 5 where the challenge response is added to protect the replay attack.

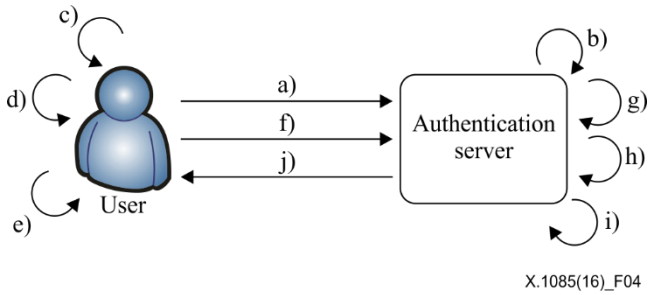

Figure 4 – Telebiometric authentication with BHSM

a) The user accesses a service at the authentication server;

b) The authentication server generates a random number R_a as a challenge. This challenge is sent to the user system and input to the BHSM;

c) The user performs the local biometric authentication using the biometric module in the BHSM;

d) The BHSM takes the PSID and the challenge R_a, and computes a digital signature on the concatenation of these two data items using *sk*, the private key of the BHSM;

e) The digital signature generated in step d) is encrypted using the public encryption key of the authentication server;

f) After successful authentication of the user, the BHSM sends the encrypted digitally signed R_a and PSID generated in steps d) and e) to the authentication server. The ITU-T X.509 certificate is also transmitted in this process;

g) The authentication server decrypts the message using its private key;

h) The authentication server verifies the signature with the ITU-T X.509 certificate of the BHSM using its public signature verification key;

i) The authentication server authenticates the ownership of the ITU-T X.509 certificate by comparing PSID in the ITU-T X.509 certificate and generated R_a in step b) with the extracted PSID and R_a in step g), respectively;

j) If the authentication is successful, then the authentication server provides the requested service to the user otherwise the authentication server rejects the service requested by the user.

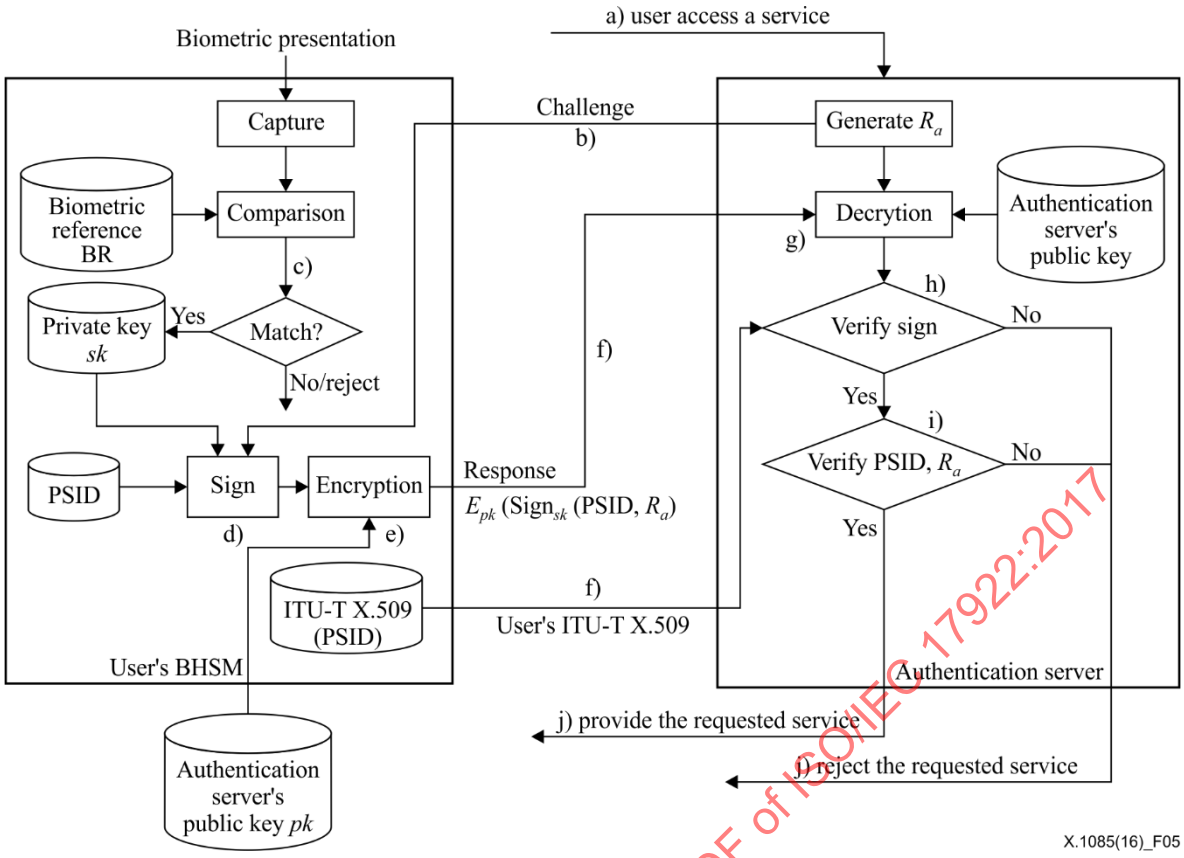

Figure 5 – Information flow in the telebiometric authentication with BHSM

7.3.2 Authentication process applying ISO/IEC 24761

This Recommendation | International Standard can adopt ISO/IEC 24761 to check the validity of the result of a biometric verification process executed in the BHSM. The telebiometric authentication process with BHSM using ACBio is depicted in Figure 6.

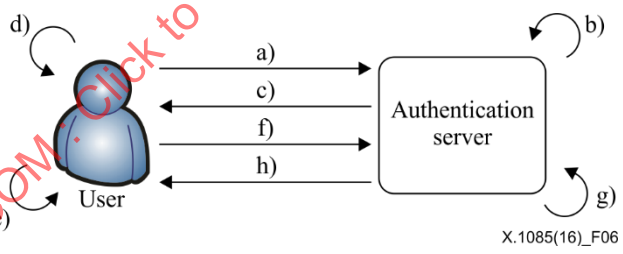

Figure 6 – Telebiometric authentication procedure with BHSM using ACBio

a) The user accesses a service at the authentication server;

b) The authentication server generates a random number Ra as a challenge;

c) The authentication server sends the challenge to the user;

d) The user executes biometric authentication using BHSM and an ACBio instance is generated in the BHSM with the challenge set in **controlValue** field if biometric authentication results in success;

e) The response, a digital signature to the challenge, is generated in BHSM with the private key of the user;

f) The response and ACBio instance are sent to the authentication server;

g) The authentication server verifies the response and validates the ACBio instance;

h) The service is provided to the user from the authentication server if both the verification and validation are successful.

8 BHSM based telebiometric authentication procedures

8.1 PSID generation and ITU-T X.509 certificate

8.1.1 Enrolling biometric reference

After a user is properly identified and authenticated, their relevant biometric characteristics are captured. A corresponding biometric reference is generated by the RA and stored in the BHSM for later use for authenticating the user to the BHSM. The biometric reference shall be protected in accordance with the confidentiality, integrity, renewability/revocability, and privacy requirements for the application. ISO/IEC 24745 provides guidelines for the secure and privacy-compliant management and processing of biometric information.

8.1.2 Generation of the PSID

8.1.2.1 General

A user identifier is needed to identify the authorized user of the BHSM. The identifier will be bound to the user's ITU-T X.509 certificate. The identifier shall be unique in the application domain of the BHSM. It may be generated in any appropriate form according to the requirements of the application. It could be personally identifiable information enabling the true identity of the user to be known; alternatively it could be a pseudonymous identifier which cannot be linked to the true identity of the user but does enable the association of transactions with pseudonymous users in the application domain of the BHSM.

The PSID used with the BHSM is a pseudonymous user identifier which conforms to the following requirements:

- The PSID shall be unique within the context of use of the BHSM;
- The enrolment process shall ensure that the PSID value included in the ITU-T X.509 certificate is the same as the PSID value stored in the BHSM.

8.1.2.2 Generation of PSID using a user's biometric reference

One method of generating a PSID is to base it on a user's biometric reference with additional data to provide renewability and processing to protect personal data and user privacy. The following implementation is specified in this Recommendation | International Standard.

A secure random number (at least 160 bits) shall be properly generated and used together with the biometric reference to generate a PSID. The RA shall generate the PSID to be included in the ITU-T X.509 certificate as follows:

PSID = h(BR, R)

where BR is the biometric reference extracted from the user, R is the random number and h is a suitable hash function. An example of abstract syntax notation one (ASN.1) type for the PSID is described in Annex A. After generation the RA shall securely store the PSID in the user's BHSM and shall also be securely transferred to CA.

8.1.3 Request and issue of the digital certificate

Under the control of the RA, the BHSM requests the CA to issue an ITU-T X.509 certificate for the user. The following information accompanies the request:

a) Encrypted PSID (EPSID) (with the CA's public key);

b) The user's distinguished name

Note – The user's distinguished name (DN) may be the same as the PSID;

c) User's public key;

d) Details of the public/private key generation algorithm used;

e) The validity period of the certificate.

To include EPSID in the certification request message, EPSID should be implemented and saved according to the format described in Annex A.

PSID is encrypted in the certification request message for CA as follows:

EPSID = E(PSID)

Here, the encryption algorithm and relevant public key are extracted from the key distribution certificate of CA. The ASN.1 type for the EPSID is described in 8.3.

8.1.4 Sending a ITU-T X.509 certificate including PSID

When the CA receives a digital certificate request message, the CA checks whether the digital signature generation key in possession is that which matches the user's digital signature verification key. PSID is extracted by decrypting EPSID from the certification request message with the private key of CA. CA can check the genuineness of the extracted PSID by comparing the received PSID from the RA. The PSID shall be configured as described in Annex A and inserted into the **subjectAltName** section among the extended fields of the ITU-T X.509 certificate. CA generates user's ITU-T X.509 certificate including PSID in the extension field.

8.2 BHSM based telebiometric authentication process

The user requests a service and is directed to the authentication server for the service. The authentication server generates a random number R_a and sends it to the BHSM for use in a challenge/response exchange to guard against a replay attack. The user presents the relevant biometric characteristic in order to locally authenticate to the BHSM. The BHSM compares the captured biometric data with the biometric reference for the authorized user stored in the BHSM. If the authentication fails (after the allowed number of attempts), then the BHSM informs the authentication service of the authentication failure and the authentication server terminates the transaction. In that case, any further attempts within a short time frame should fail.

NOTE – Depending on the security policy in force, it may be appropriate to deny any further authentication attempts for a predefined period of time.

If the authentication is successful the BHSM sends the signed PSID and challenge R_a encrypted with the user's private key to the authentication server. The ITU-T X.509 certificate is also sent to the authentication server as part of the transmission. The authentication server authenticates the ownership of the ITU-T X.509 certificate by comparing the PSID in the certificate with the decrypted PSID sent by the BHSM in the previous transmission. If the two are identical, the authentication server accepts the service request and passes it to the service provider for processing.

8.3 ASN.1 type for the encrypted PSID

The **DataSetForEncryptedPSID** has the following components:

- **version** refers to the version number of this Recommendation | International Standard. When this Recommendation | International Standard is referred, the **v1 (0)** value will be used;
- **psidEncAlg** refers to the asymmetric encryption algorithm and parameter used to encrypt the PSID. The algorithm should be the same as that included in the certificate of CA;
- **encryptedPsid** is the encrypted PSID with the public key of the certificate authority.

```
DataSetForEncryptedPSID ::= SEQUENCE {
         version [0] INTEGER DEFAULT 0,
         psidEncAlg    [1] PSIDEncryptionAlgorithm,
         encryptedPsid  [2] EncryptedPsid
}
PSIDEncryptionAlgorithm ::= AlgorithmIdentifier
Encryptedsid ::= OCTET STRING
```

Annex A

PSID and related information

(This annex forms an integral part of this Recommendation | International Standard.)

A.1 General

This annex applies to the mechanism specified in clause 7 and clause 8.

A.2 Encrypted PSID requesting an ITU-T X.509 certificate

A digital certificate request message with the encrypted PSID is sent to CA. PKCS#10 is composed of the user DN and the user's digital signature verification key information, and includes the attributes component for additional information input. The attribute component can include the object identifier (OID) and all attributes that have a concrete structure. Therefore, the component can be included using the OID encrypted PSID for the **EncryptedPsid**.

A.3 ASN.1 for PSID

```
XBHSM {iso(1) standard(0) bhsm(17922) modules(0) version1(1)}
DEFINITIONS AUTOMATIC TAGS ::=
BEGIN
IMPORTS authenticationFramework
        FROM UsefulDefinitions {joint-iso-itu-t ds(5) module(1)
            usefulDefinitions(0) 7}
        ALGORITHM, AlgorithmIdentifier{}
        FROM AuthenticationFramework authenticationFramework;

        DataSetForEncryptedPSID ::= SEQUENCE {
            version  INTEGER DEFAULT 0,
            psidEncAlg      PSIDEncryptionAlgorithm,
            encryptedPsid   EncryptedPsid
            }

        PSIDEncryptionAlgorithm ::= AlgorithmIdentifier
            {{SupportedEncryptionAlgorithms}}

        SupportedEncryptionAlgorithms   ALGORITHM ::= {...}
        EncryptedPsid ::= OCTET STRING
        PSID ::= SEQUENCE {
            hashAlg  HashAlgorithm,
            hashContent     HashContent
            }

        HashAlgorithm ::= AlgorithmIdentifier{{SupportedHashAlgorithms}}
        SupportedHashAlgorithms   ALGORITHM ::= {...}

        HashContent ::= SEQUENCE {
            bR      PrintableString,
            randomNum       BIT STRING
            }

        bhsmpsid  OBJECT IDENTIFIER ::=
            {iso(1) standard(0) bhsm(17922) contentType(2) bhsmps(1)}
        BHSM-PSID ::= TYPE-IDENTIFIER
        bioRef  BHSM-PSID ::=
            {BIT STRING IDENTIFIED BY {bhsmpsid 3}}
        InstanceOfBHSM-PID ::= INSTANCE OF BHSM-PSID({SupportedBHSM-PSID})
        SupportedBHSM-PSID BHSM-PSID ::= {bioRef,...}
END
```

The PSID structure has the following components:

– **hashAlg** refers to the hash algorithm and parameter used to generated a PSID.