

COMMITTEE DRAFT Recommendation ITU-T X.1085 I ISO/IEC 1st CD 17922		Reference number: ISO/IEC JTC 1/SC 27 N14160	
Date: 2014-06-20		Supersedes document SC 27 N13389	
THIS DOCUMENT IS STILL UNDER STUDY AND SUBJECT TO CHANGE. IT SHOULD NOT BE USED FOR REFERENCE PURPOSES.			
ISO/IEC JTC 1/SC 27 Information technology - Security techniques Secretariat: Germany (DIN)	Circulated to P- and O-members, and to technical committees and organizations in liaison for comments by: 2014-09-22 Please submit your comments via the online balloting application by the due date indicated.		
Recommendation ITU-T X:1085 I ISO/IEC 1st CD 17922 Title: Information technology -- Security techniques – Telebiometric authentication framework using biometric hardware security module Project: 1.27.98 (X.1085 I 19722)			
Explanatory Report			
Status	SC 27 Decision	Reference documents	
		Input	Output
<i>For details regarding previous development stages please refer to the 2nd page of the explanatory report.</i>			
Recommendation ITU-T X:1085 I ISO/IEC 17922 3rd WD	15 th WG 5 meeting, April 2013, Resolutions 1, 2, P6 (N12555); 25 th SC 27 Plenary, April 2013, Resolutions 19, 13 (Deleg. of Auth f. CD) (N12739).	SoCom (N12266).	Liaisons to: IITU-T SG 17 (N12518); JTC 1/SC 37 (12523); DoC (N12547); Text f. 3 rd WD (N12548).
Recommendation ITU-T X:1085 I ISO/IEC 17922 4th WD	16 th WG 5 meeting, Oct. 2013, Resolutions 1, 2, 8 (N13373).	GB com. (N12986); JP com. (N12990).	Request for limit dates extension (N13466); Liaisons to: IITU-T SG 17 (N13348); JTC 1/SC 37 (13341); DoC (N13388); Text f. 4 th WD (N13389).
Recommendation ITU-T X:1085 I ISO/IEC 17922 1st CD	17 th WG 5 meeting, April 2014, Resolutions 1, P2 (N14199); 26 th SC 27 Plenary, April 2014, Resolution 1 (N14200).	SoCom. (N13776).	JTC 1 endorsement on limit dates (N13407); Liaisons to: IITU-T SG 17 (N14128); JTC 1/SC 37 (14121); DoC (N14159); Text f. 1 st CD (N14160).
CD Registration and Consideration In accordance with resolution 1 (contained in SC 27 N14200) of the 26 th SC 27 Plenary meeting held in Hong Kong, China, 14-15 April 2014, the hereby attached document has been registered with the ISO Central Secretariat (ITTF) as a 1 st Committee Draft (CD) and is being circulated for a 1 st CD letter ballot closing by <div style="text-align: center; margin: 20px 0;">2014-09-22</div> MEDIUM: http://isotc.iso.org/livelink/livelink/open/jtc1sc27 NO. OF PAGES: 2 + 22			

Explanatory Report, 2nd page			
Status	SC 27 Decision	Reference documents	
		Input	Output
NWIP Preliminary draft	12 th WG 5 meeting, Oct. 2011, Resolutions 17 (N10525).		Liaisons to: ITU-T SG 17 (N10532); SC 37 (N10528 NWIP (N10549).
Recommendation ITU-T X:1085 I ISO/IEC 17922 1st WD	13 th WG 5 meeting, May 2012, Resolutions 1, 2, P4, P7 (N11280); 24 th SC 27 Plenary, May 2012, resolution 20 (N11330).	SoV (N10723); ITU-T SG 17 comm. (N10914)..	Liaisons to : ITU-T SG 17 (N11274); JTC 1/SC 37 (N11258); Text f. 1 st WD (N11254).
Recommendation ITU-T X:1085 I ISO/IEC 17922 2nd WD	14 th WG 5 meeting, Oct. 2012, Resolutions 1, 14 (N11701).	JP com (N11549); ITU-T SG 17 com. (N11561).	Liaisons to : ITU-T SG 17 (N11711); JTC 1/SC 37 (N11705); DoC (N11745); Text f. 2 nd WD (N11744)..

ITU

International
Telecommunication Union



ISO

International Organization
for Standardization



IEC

International
Electrotechnical
Commission



ITU-T Recommendation X.1085 |
International Standard ISO/IEC CD 17922

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

Contents

	Page
Foreword.....	ii
Summary	iii
1 Scope	1
2 Normative references	2
3 Definitions	2
4 Abbreviations	4
5 Symbols and terminology	4
6 Biometric hardware security module for telebiometric authentication	5
6.1 Additional feature of BHSM to HSM	5
6.2 Telebiometric authentication using BHSM	5
7 Telebiometric authentication with biometric hardware security module	6
7.1 Enrolment procedures	6
7.2 Telebiometric authentication Processes	8
8 BHSM based telebiometric authentication procedures	10
8.1 PSID generation and X.509 certificate	10
8.2 BHSM based telebiometric authentication process	11
8.3 ASN.1 type for the encrypted PSID	11
Annex A – Locations for PSID and related information	12
Annex B – Procedures for inserting PSID	14
Bibliography	16

Foreword

The International Telecommunication Union (ITU) is the United Nations specialized agency in the field of telecommunications. The ITU Telecommunication Standardisation 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 standardising telecommunications on a world-wide basis. The World Telecommunication Standardisation Assembly (WTSA), which meets every four years, establishes the topics for study by the ITU-T study groups that, 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 that fall within ITU-T's purview, the necessary standards are prepared on a collaborative basis with ISO and IEC.

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.

International Standards are drafted in accordance with the rules given in the ISO/IEC Directives, Part 2.

The main task of the joint technical committee is to prepare International Standards. Draft International Standards adopted by the joint technical committee are circulated to national bodies for voting. Publication as an International Standard requires approval by at least 75 % of the national bodies casting a vote.

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.

ISO/IEC 17922 was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 27, *Security techniques*. The identical text is published as ITU-T Recommendation X.1085.

Summary

This Recommendation | International Standard describes a telebiometric authentication scheme using biometric hardware security module (BHSM) for the telebiometric authentication of proving owner of X.509 certificate registered individual at RA (Register Authority). This Recommendation | International Standard provides the requirements for deploying a BHSM scheme to provide secure telebiometric authentication within 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 X.509 framework to authenticate the user as the owner of the X.509 certificate.

INTERNATIONAL STANDARD <17922>
ITU-T RECOMMENDATION <X.1085>

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

1 Scope

For high level telebiometric authentication of proving ownership of X.509 certificate registered individual at the RA, BHSM has been considered. This Recommendation | International Standard provides a framework for telebiometric authentication using the BHSM.

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

- telebiometric authentication mechanisms using the BHSM in telecommunication network environments; and
- ASN.1 format and protocols for implementing the mechanisms in the 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 PKI standards and to establish standard mechanism using the BHSM for verifying the ownership of the X.509 certificate in the telebiometric environment.

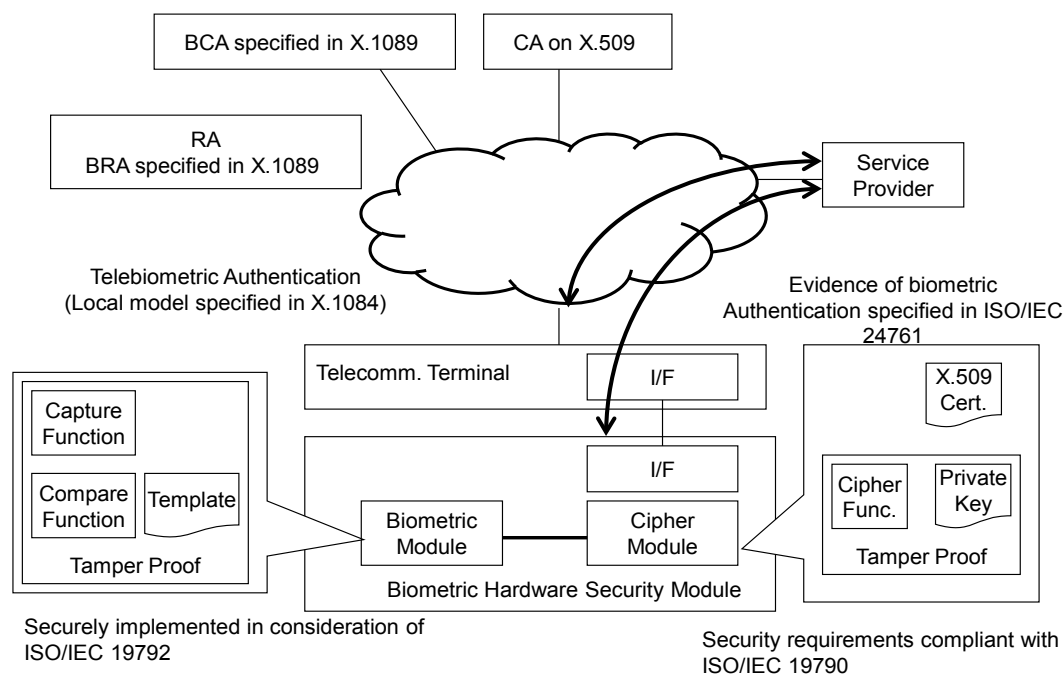


Figure 1 – Standard environment for BHSM

2 Normative references

The following ITU-T Recommendations and other references 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 other references are subject to revision; users of this Recommendation | International Standard 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 | International Standard does not give it, as a stand-alone document, the status of a Recommendation or International Standard.

- | | |
|-----------------|---|
| [ISO 13491-1] | ISO 13491-1:2007, <i>Banking – Secure cryptographic device (retail)-Part 1: Concepts, requirements and evaluation methods</i> . |
| [ISO/IEC 24745] | ISO/IEC 24745:2011, <i>Information Technology – Security Techniques – Biometric Information Protection</i> . |
| [ISO/IEC 24761] | ISO/IEC 24761:2009, <i>Information Technology – Security Techniques- Authentication Context for Biometrics</i> . |
| [IETF RFC 4683] | IETF RFC 4683:2006, <i>Internet X.509 Public Key Infrastructure Subject Identification Method (SIM)</i> . |

3 Definitions

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

3.1

biometric hardware security module

physically combined hardware consisting of a hardware security module and a biometric module equipped one or multiple biometric sensors.

NOTE – In case of comparison on biometric hardware security module, it comes traditionally in form of smart card but recently also in form of USB type security token which can be attached directly to general purpose computers.

3.2

biometric reference

one or more stored biometric samples, biometric templates or biometric models attributed to a biometric subject and used for comparison [ISO/IEC 19784-1]

3.3

biometric sample

information obtained from a biometric sensor, either directly or after further processing [ISO/IEC 19784-1]

3.4

entity authentication

corroboration that an entity is the one claimed

[ISO/IEC 9798-1].

3.5

hardware security module

hardware of secure cryptoprocessor targeting at managing X.509 certificate and private key for providing secure authentication.

3.6

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

[ISO/IEC 24745].

3.7

Pseudonymous identifier

PSID

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)

[ISO/IEC 24745].

3.8

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 [ISO/IEC 24745].

3.9

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

[ISO/IEC 24745].

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

3.10

revocability

ability to prevent future successful verification of a specific biometric reference and the corresponding identity reference

[ISO/IEC 24745].

NOTE Rejection of an entity may occur on the grounds of its appearance on a revocation list.

3.11

telebiometric authentication

biometric authentication over a telecommunications channel

4 Abbreviations

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

ACBio	Authentication Context for Biometrics
BCA	Biometric Certificate Authority
BHSM	Biometric Hardware Security Module
BRA	Biometric Register Authority
BRT	Biometric Reference Template
BR	Biometric Reference
CA	Certificate Authority
DN	Distinguished Name
EPSID	Encrypted PSID
HSM	Hardware Security Module
IR	Identity Reference
OID	Object Identifier
PSID	Pseudonymous Identifier
RA	Registration Authority
RBR	Renewable Biometric Reference

5 Symbols and terminology

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 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 HSM

A hardware security module manages and protects critical private keys in terms of digital signings for providing strong authentication. They are physical devices that traditionally come in the form of smartcard or some other USB type security token that is tamper resistant against penetration or modification of an internal operation and/or insertion of active or passive tapping mechanism to disclosure secret data or to alter the operation of devices.

The cryptographic materials handled by most HSMs are public/private key pairs (and certificates) used in public-key cryptography related to X.509 certificate such as encryption/decryption and digital signatures [2]. If the keys are 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 the HSM is being used by its legitimate owner. Typically the binding of the HSM to the owner is provided by means of a secret PIN or password that should be known only to the legitimate owner. However 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 mechanised 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 private key is used for personal 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 (BHSM) is a HSM that uses biometrics to authenticate the owner and provide security assurance for telebiometric transactions.

6.2 Telebiometric authentication using 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 [1]. Especially in such cases, one shall consider the security and privacy of the biometric information. For this, securely connected biometric module with the HSM can be one of favorable solutions since the biometric information can be under control of the subject and tamper resistant. Although biometric references are not stored to the authentication server or transferred over the open network, one should consider the use of renewable and pseudonymous identifier so that a compromised biometric reference can be revoked and that no meaningful biometric data related to the revoked biometric reference can be extracted from the pseudonymous identifier.

A BHSM based telebiometric authentication scheme relies on an existing public key infrastructure (PKI). The scheme should be properly integrated with the existing PKI to minimize the costs and maximize the efficiency of telebiometric authentication. To achieve this, the method for binding the biometric information with the X.509 certificate is an important consideration.

The BHSM operation and transaction protocols described in this standard relate to the following role players:

- User, a BHSM owner whose X.509 certificate and biometric reference are stored in the BHSM
- Authentication server which requires to authenticate user
- Registration Authority which registers the biometric reference of the user and provides biometric recognition information that is stored in the user's BHSM
- CA which issues user's X.509 certificate.

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

- The CA should adopt the PSID scheme with X.509 extension field for employing BHSM based telebiometric authentication.
- The CA should not use the original biometric reference of the user for encoding the X.509 extension field, in order to avoid the possibility of disclosing the user's private biometric data.
- To protect user's biometric privacy, the biometric privacy requirements (irreversibility, unlinkability, and confidentiality) described in ISO/IEC 24745 should be satisfied.
- The biometric reference should not leave the BHSM so that the control of the biometric data resides solely with the user. At the stage of requesting a X.509 certificate to the CA or performing the telebiometric authentication, only the pseudonymous identifier should be allowed to leave the BHSM.

7 Telebiometric authentication with biometric hardware security module

7.1 Enrolment procedures

7.1.1 Enrolment procedures using X.509 certificate extension

The enrolment process for issuing an X.509 certificate with BHSM is depicted as Figure 2. Here, conventional enrolment procedures are not described. For the detail description of digital signatures for non-repudiation, see [4].

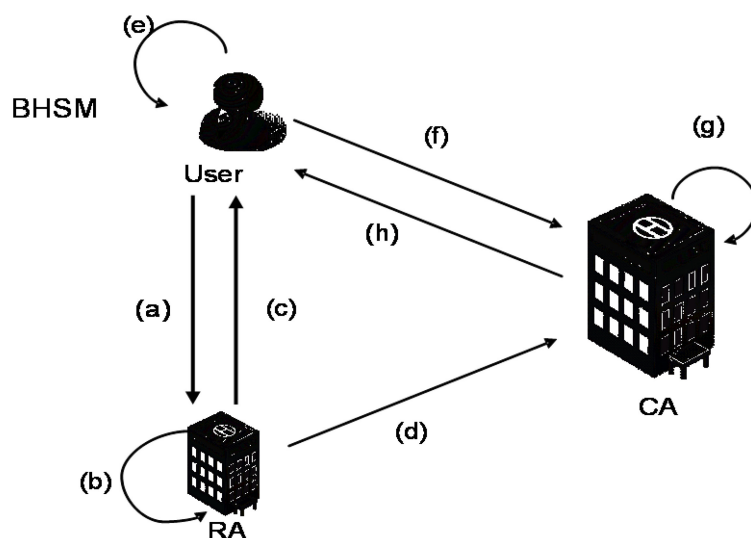


Figure 2 – Enrolment procedure with BHSM

- a. After the visiting user is properly identified and authenticated, his/her accurate, authorized and complete biometric characteristic is captured by the RA. Then obtained biometric reference is stored in his/her BHSM.
- b. The RA generates a random number R which shall be used together with user's biometric reference to create a PSID.
- c. The RA stores the random number R in the user's BHSM under control of the RA .
- d. The RA sends the generated PSID to the CA.
- e. The user generates his/her private and public keys within the BHSM.
- f. The user sends a requesting message for X.509 certificate to CA.
- g. The CA generates user's X.509 certificate including the PSID in the extension field.
- h. The CA sends user's X.509 certificate and it will be securely stored in the user's BHSM.

NOTE: In this 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.

7.1.2 Enrolment procedures with BHSM using ACBio

The enrolment process for issuing an X.509 certificate and a BRT certificate, which is specified in ISO/IEC 24761 ACBio, to use BHSM is depicted in Figure 3.

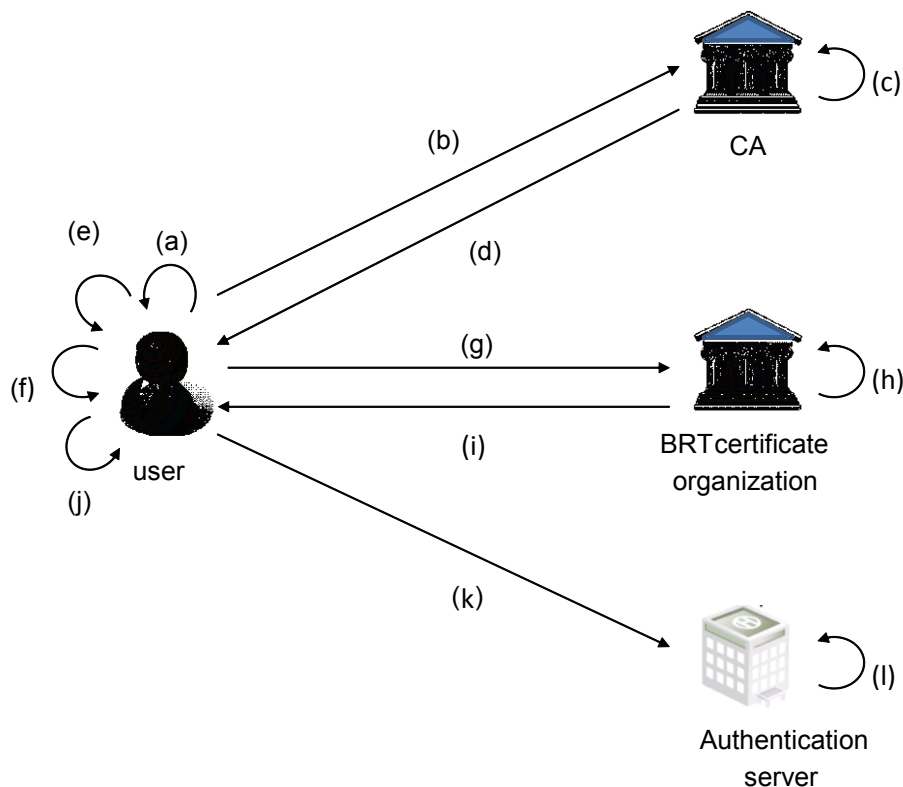


Figure 3 – Enrolment procedure with BHSM using ACBio

- a. The user generates a pair of public and private key in the BHSM.
- b. The user sends X.509 certificate issuance request to the CA.
- c. The CA generates an X.509 certificate for the request.
- d. The CA sends X.509 certificate to the user.
- e. The user stores the X.509 certificate in the BHSM.

- f. The user generates a biometric reference and the ACBio instance for enrolment.
- g. The user sends BRT certificate issuance request with the values of serialNumber and issuer in the X.509 certificate and the ACBio instance for enrolment to the BRT certificate organization.
- h. 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.
- i. The BRT certificate organization sends the BRT certificate to the user.
- j. The user stores the BRT certificate in the BHSM in couple with the biometric reference.
- k. The user sends the X.509 certificate and BRT certificate to the authentication server for registration.
- l. The authentication server stores the X.509 certificate and BRT certificate in the user database.

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

7.2 Telebiometric authentication Processes

7.2.1 Telebiometric authentication with BHSM

The telebiometric authentication process with BHSM can be described as Figure 4 and more detail information flow in the BHSM and the service provide as shown in Figure 5 where the challenge response is added for protecting against a replay attack.

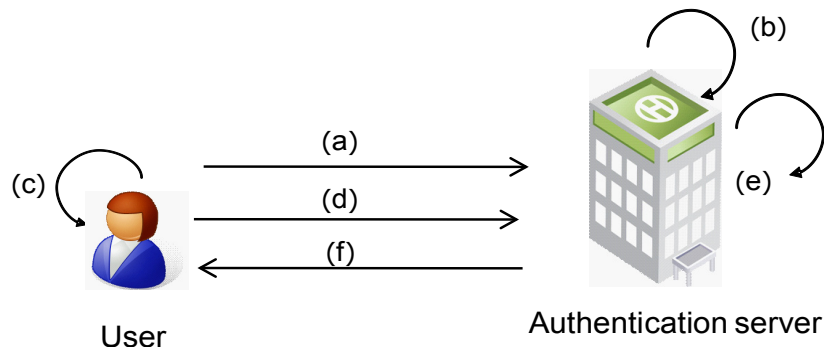


Figure 4 – Telebiometric authentication with BHSM

- a. The user access a service at the authentication server.
- b. The authentication server generates a random number R_a as a challenge.
- c. The user performs local biometric authentication using the biometric module in the BHSM.
- d. After successful authentication of user, he/she sends the encrypted digitally signed double hashing of the pair of biometric reference and random number R stored in the BHSM and R_a to the authentication server with his/her private key (sk) in the BHSM. The X.509 certificate is also transmitted in this process. Here, double hashing is adopted to avoid the hash collision.
- e. Authentication server authenticates the ownership of the X.509 certificate by comparing the PSID in the X.509 certificate with the decrypted hashing value of the received value.
- f. Authentication server provides the requested service for user.

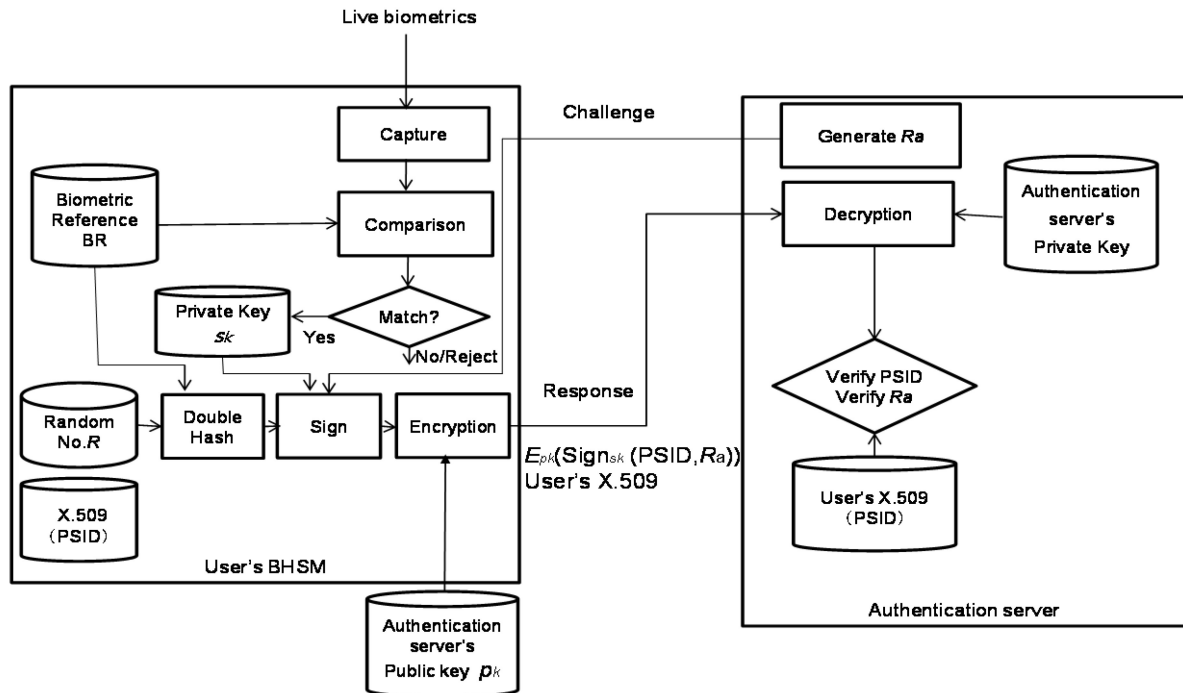


Figure 5 – Information flow in the telebiometric authentication with BHSM

7.2.2 Telebiometric authentication with BHSM using ACBio

This Recommendation | International Standard can adopt the ISO/IEC 24761: Authentication Context for Biometrics(ACBio) 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.

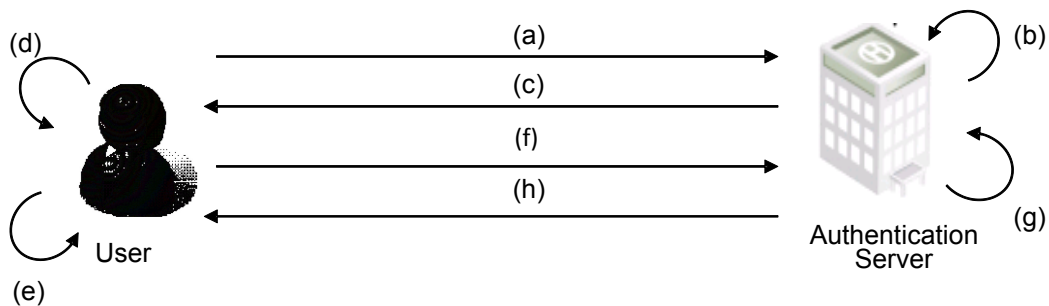


Figure 6 – Telebiometric authentication procedure with BHSM using ACBio

- The user accesses a service at the authentication server.
- The authentication server generates a random number as a challenge.
- The authentication server sends the challenge to the user.
- The user executes biometric authentication using the BHSM and an ACBio instance is generated in the BHSM with the challenge set in controlValue field if biometric authentication results in success.
- The response to the challenge is generated in the BHSM with the private key of the user.
- The response and ACBio instance are sent to the authentication server.
- The authentication server verifies the response and validates the ACBio instance.
- The service is provided to the user from the authentication server if both of the verification and validation result in success.

8 BHSM based telebiometric authentication procedures

8.1 PSID generation and X.509 certificate

8.1.1 Enrolling biometric reference

After a user is properly identified and authenticated, his/her accurate, authorized and complete biometric reference is captured by the RA. Then the obtained biometric reference is stored in his/her BHSM. The RA shall protect the biometric information under various requirements of confidentiality, integrity, renewability/revocability, and privacy according to the ISO/IEC 24745 which provides guidelines for the secure and privacy-compliant management and processing of biometric information.

8.1.2 A random number R for the BHSM

A secure random number (at least 160 bits) shall be generated properly such as described in [3] and used in this Recommendation | International Standard by the RA. Random number R is used together with the biometric reference to generate a PSID. The generated random number R shall be securely stored in the BHSM under control of the RA with standardized format described in Annex A.

8.1.3 Generating a PSID

RA shall generate the PSID to be included in the X.509 certificate as follows:

$$\text{PSID} = h(h(\text{BR}, R))$$

where BR is the biometric reference extracted from the user and R is the random number generated in 8.1.2 and also a hash function is used twice for double hashing. An example of ASN.1 type for the PSID is described in Annex A. The generated PSID shall be securely transferred to CA.

8.1.4 Digital signature keys

The public/private key pair is generated in the BHSM and the public key is sent to the CA for binding to the X.509 certificate. The X.509 certificate that is passed back to the user from the CA shall be stored in the BHSM. The digital signature generation key (private key) shall be stored in the user's BHSM.

8.1.5 Digital certificate request message

The user sends a requesting message for X.509 certificate to CA. The digital certificate request message shall contain the following information when being generated:

- 1) User's DN
- 2) User's digital signature verification key (public key)
- 3) EPSID

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

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

$$\text{EPSID} = E(\text{PSID})$$

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.

8.1.6 Sending a X.509 certificate including PSID

When CA receives a digital certificate request message, the authority checks whether the digital signature generation key in possession is that which matches the user's digital signature verification key. The PSID is extracted by decrypting the EPSID from the certification request message with the private key of the CA. The 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 X.509 certificate. The CA generates user's X.509 certificate including the PSID in the extension field.

8.2 BHSM based telebiometric authentication process

User requests a service at the authentication server. Then the authentication server generates a random number R_a as a challenge and sends it to the client to protect the replay attack. At the same time, user performs local biometric authentication using the biometric module in the BHSM by presenting his/her live biometric reference. The captured biometric reference is compared with the registered biometric reference in the BHSM by the RA. If the comparison score is lower than a predefined threshold value, then the authentication process shall be terminated. That is, the authentication server shall reject requesting service.

In case of successful authentication of user in the client, he/she shall send the encrypted digitally signed double hashing of the pair of biometric reference and random number R stored in the BHSM and R_a to the authentication server with his/her private key in the BHSM. The X.509 certificate shall be also transmitted in this process. Authentication server authenticates the ownership of the X.509 certificate by comparing the PSID in the X.509 certificate with the decrypted EPSID. If the authentication is successful, the authentication server provides the requested service for user.

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

EncryptedPsid ::= OCTET STRING
  
```

Annex A (Normative)

Location for PSID and related information

A. 1 Random number *R*

The random number *R* should be saved according to the [PKCS#5v2.0] and [PKCS#8] with the digital signature generation key.

A. 2 Encrypted PSID requesting a X.509 certificate

A digital certificate request message with the encrypted PSID is sent to the 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 OID and all attributes that have a concrete structure. Therefore, the component can be included using the OID encrypted PSID for the EncryptedPSID.

RFC 2510 defines the protocol related to digital certificate management, such as digital certificate issuance request, renewal, disposal, and key recovery. RFC 2510 also defines the message format used in the public key infrastructure.

A. 3 Attributes and ASN.1 for PSID

The PSID structure has the following components:

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

The HashContent structure has the following components:

- bR is the biometric reference extracted from the biometric information. Any biometric modality (fingerprint, face, iris, etc.) can be used. The bR should consist of numbers and should be described in PrintableString.
- randomNum is the random number R.
-

NOTE It is recommended that the biometric reference is expressed with Biometric Information Record (BIR) specified in in ISO/IEC 19785-1. .

```
PSID ::= SEQUENCE {
    hashAlg      HashAlgorithm,
    hashContent HashContent
}
```

```
HashAlgorithm ::= AlgorithmIdentifier
```

```
HashContent ::= SEQUENCE {
```

```

bR      PrintableString,
randomNum BIT STRING

```

```

}

```

A. 4 PSID in the X.509 certificate

To insert the PSID in the X.509 certificate, it shall be saved in the subjectAltName extension field as INSTANCE OF OTHER-NAME.

BHSM-PSID-CLASS ::= TYPE-IDENTIFIER

```

bioRef BHSM-PSID-CLASS ::=
    {BIT STRING IDENTIFIED BY {bhsm-psid 3}}

```

```

INSTANCE OF BHSM-PSID-CLASS ::= SEQUENCE {
    type-id BHSM-PSID-CLASS.&id,
    value [0] BHSM-PSID-CLASS.&Type
}

```

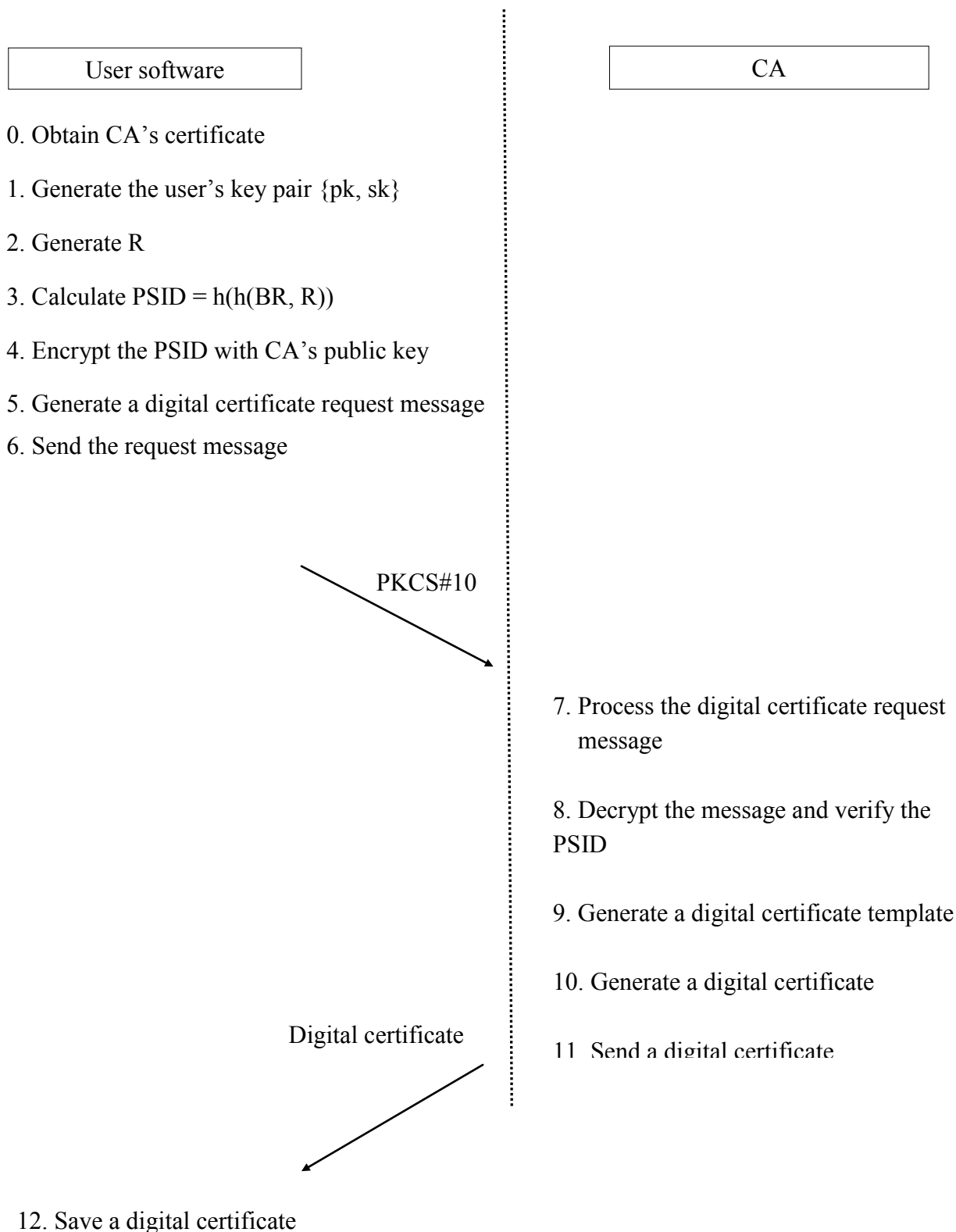
The realName field contains the UTF8String encoded name of the digital certificate owner and the userInfo field contains the additional identification information of the digital certificate owner, as well as PSID.

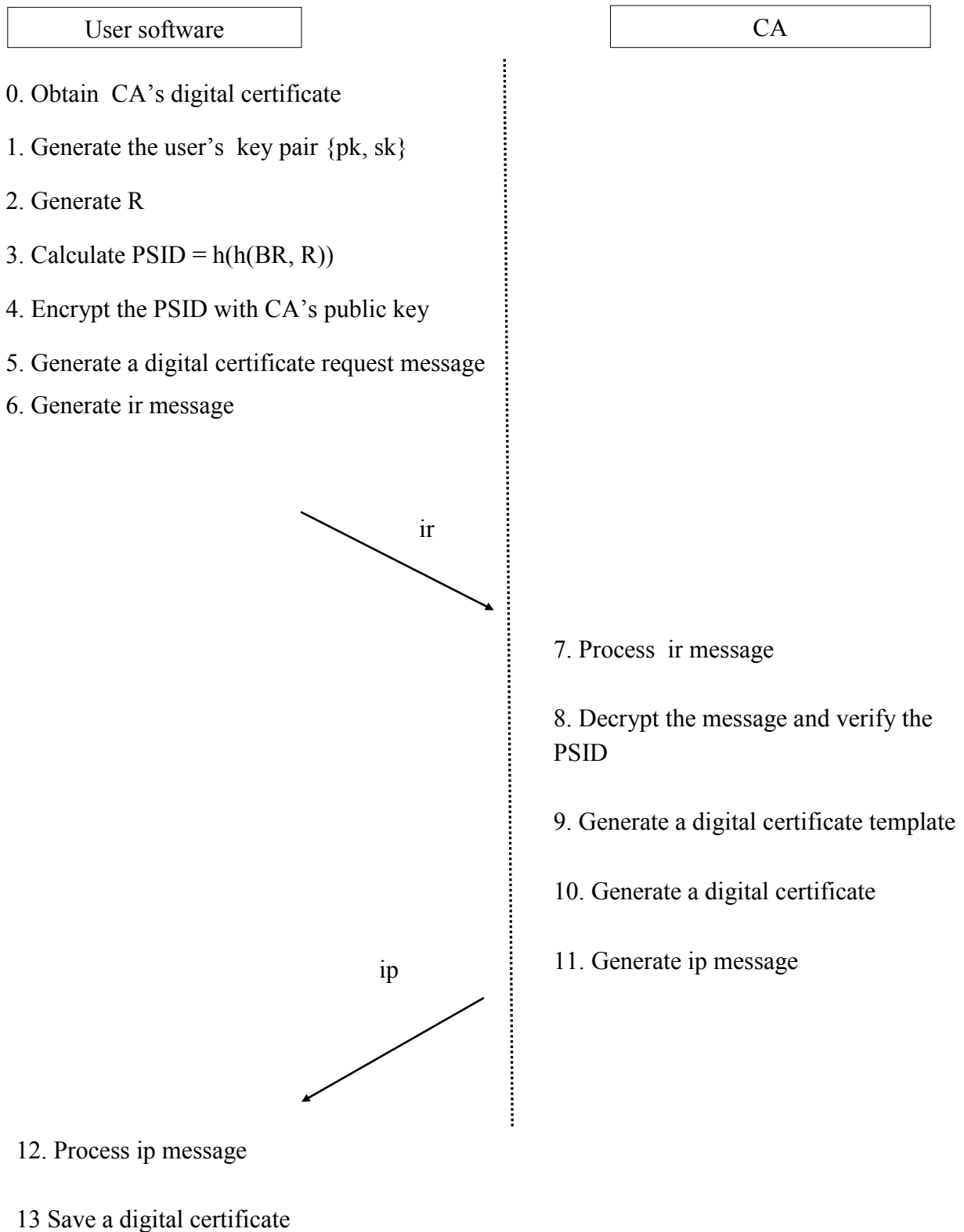
Annex B

(Informative)

Procedures for inserting PSID

B.1 Procedures for inserting PSID using PKCS #10



B.2 Procedures for inserting PSID using RFC 6712

Bibliography

- [1] ITU-T X.1086 (Telebiometrics Protection Procedures-Part1): A guideline of technical and managerial countermeasures for biometric data security
- [2] ISO/IEC 9594-8: 2014, Information technology - Open System Interconnection – The Directory-Part8: Public-key and attribute certificate frameworks
- [3] ISO/IEC 18031: 2011, Information technology - Security techniques – Random bit generation
- [4] ISO/IEC 15945: 2002, Information technology - Security techniques – Specification of TTP services to support the application of digital signature