International Telecommunication Union

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

X.1093

(11/2018)

SERIES X: DATA NETWORKS, OPEN SYSTEM COMMUNICATIONS AND SECURITY

Information and network security – Telebiometrics

Telebiometric access control with smart ID cards

Recommendation ITU-T X.1093

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 (1)	
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 (1)	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 (2)	
Emergency communications	X.1300–X.1309
Ubiquitous sensor network security	X.1310–X.1319
Smart grid security	X.1330–X.1339
Certified mail	X.1340–X.1349
Internet of things (IoT) security	X.1360–X.1369
Intelligent transportation system (ITS) security	X.1370–X.1389
Distributed ledger technology security	X.1400–X.1429
Distributed ledger technology security	X.1430–X.1449
Security protocols (2)	X.1450–X.1459
CYBERSECURITY INFORMATION EXCHANGE	
Overview of cybersecurity	X.1500–X.1519
Vulnerability/state exchange	X.1520–X.1539
Event/incident/heuristics exchange	X.1540–X.1549
Exchange of policies	X.1550–X.1559
Heuristics and information request	X.1560–X.1569
Identification and discovery	X.1570–X.1579
Assured exchange	X.1580–X.1589
CLOUD COMPUTING SECURITY	
Overview of cloud computing security	X.1600–X.1601
Cloud computing security design	X.1602–X.1639
Cloud computing security best practices and guidelines	X.1640–X.1659
Cloud computing security implementation	X.1660–X.1679
Other cloud computing security	X.1680–X.1699

For further details, please refer to the list of ITU-T Recommendations.

Recommendation ITU-T X.1093

Telebiometric access control with smart ID cards

Summary

The biometrics-on-card can be classified into three types such as store-on-card, which is a form in which biometric information is stored in a smart card, compare-on-card in which biometric information is compared in a smart card, and sensor-on-card in which a biometric sensor is embedded in a smart card to acquire, store and compare the biometric information within the card. The application scheme is also divided into two types depending on whether or not the digital signature function is provided by embedding the ITU-T X.509 certificate.

Recommendation ITU-T X.1093 describes the general scheme for logical and/or physical access control using the biometrics-on-card. This Recommendation can be applied to the recent emerging area of requiring secure physical and also logical access control management.

History

Edition	Recommendation	Approval	Study Group	Unique ID*
1.0	ITU-T X.1093	2018-11-13	17	11.1002/1000/13725

Keywords

Access control, biometrics-on-card, ID card, telebiometrics.

* 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/.

Table of Contents

Recommendation ITU-T X.1093

Telebiometric access control with smart ID cards

1 Scope

This Recommendation addresses the telebiometric access control requirements and architecture of personal identity verification platform, which allows users to ensure personal identification using biometrics with smart ID cards for logical and physical access control. Biometrics has been considered for the telebiometric authentication of proving ownership of a smart ID card registered with a registration authority. This Recommendation provides functional requirements for deploying the smart ID card scheme to securely operate the telebiometric authentication under PKI environments. The scheme focuses on providing how to assure the telebiometric authentication with biometric techniques when telebiometrics and [ITU-T X.509] certificate are combined.

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 (2016) | ISO/IEC 9594-8:2017, *Information technology – Open systems interconnection – The directory: Public-key and attributes certificate frameworks*.

3 Definitions

3.1 Terms defined elsewhere

This Recommendation uses the following terms defined elsewhere:

3.1.1 access control [b-ISO/IEC 29146]: Granting or denying an operation to be performed on a resource.

3.1.2 telebiometric authentication [b-ISO/IEC 17922]: Biometric authentication utilising data communication by telephony, radio or a related technology.

3.2 Terms defined in this Recommendation

This Recommendation defines the following terms:

3.2.1 biometrics-on-card: A contact or contactless type of any pocket-sized card that has embedded at least one of a number of biometric processing units such as storing, comparing, and sensing for biometrics.

3.2.2 logical access control: A mechanism that performs the granting or denying of access for computers, programs, processes, and information systems.

3.2.3 physical access control: Electro-mechanical suite that performs the granting or denying of access at controlled entry points of a facility.

3.2.4 smart ID card: A contact or contactless type of any pocket sized card that has embedded integrated circuits that hold a user's identity information. This can employs a PKI, which stores an encrypted digital certificate issued from the PKI provider with other relevant identity information.

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

ACL Access Control List

BoCHUID Biometrics-on-Card Holder Unique Identifier

CRL Certificate Revocation List

PIN Personal Identification Number

PKI Public Key Infrastructure

5 Conventions

None.

6 Access management system and biometric-on-card

6.1 Access management system

Access management is a set of processes to manage the granting or denying of an operation to be performed on a resource. As denoted in Figure 1, access management consists of two main processes. The subject to be permitted to access a resource is needed to undergo the authentication process. To implement the authentication process, secure authentication method should be deployed. In this Recommendation, biometrics-on-card provides the required authentication mechanism. The authorization makes decision to allow or deny access to the resource based on a policy. Authorization is supported by administrative activity which assigns subject privileges in accordance with the access management policy.

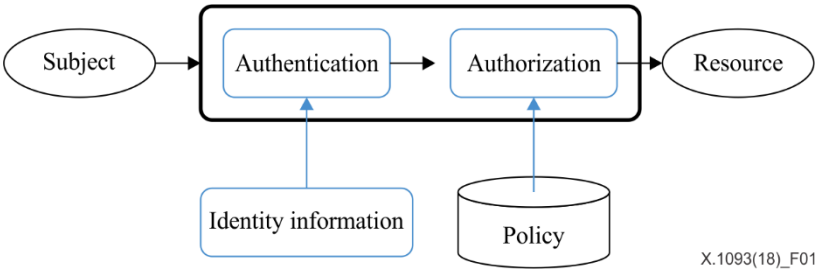

Figure 1 – Access management system

6.2 Biometrics-on-card based personal authentication system

6.2.1 Biometrics-on-card

The biometrics-on-card has an embedded integrated circuit chip that provides storage space and computation capability in consideration of portability, and has at least one of the following functional units: biometric sensor, a comparison unit, and a storage for biometric information processing. In the case of using an existing smart card, confirming the identity of the card holder is processed by applying a personal identification number stored in the card. However, since the personal identification number is easily exposed by the attacker, the necessity of multi-factor personal authentication using the card holder unique identifier and the biometric information has arisen.

The biometrics-on-card developed to meet this demand can be mainly classified into three types according to where the processing of biometric information is performed. In this Recommendation, three type of biometrics-on-card are considered. A store-on-card in which biometric information is stored in a smart card, a compare-on-card in which a matching is performed in a smart card, and sensor-on card in which a biometric sensor is embedded in a smart card can be adopted for personal authentication. In addition, a public key type certificate is embedded in each biometrics-on-card, and a digital signature and personal authentication using it are divided into two according to whether the function is embedded.

A biometrics-on-card system for personal authentication may include various identity authentication mechanisms within the card. This Recommendation describes biometric identification and digital signatures only, except for the basic PIN-based mechanism. Therefore, the biometrics-on-card system authenticates the identity of the cardholder by using what the user has and who the user is. Accordingly, the following authentication information must be included in the biometrics-on-card:

– biometric-on-card holder unique identifier;

– biometrics-on-card authentication data (PKI key pair, certificate) including biometric information.

In addition to personal authentication, symmetric keys for managing cards are not described in this Recommendation.

The overall structure of the access management system with biometrics-on-card is depicted in Figure 2.

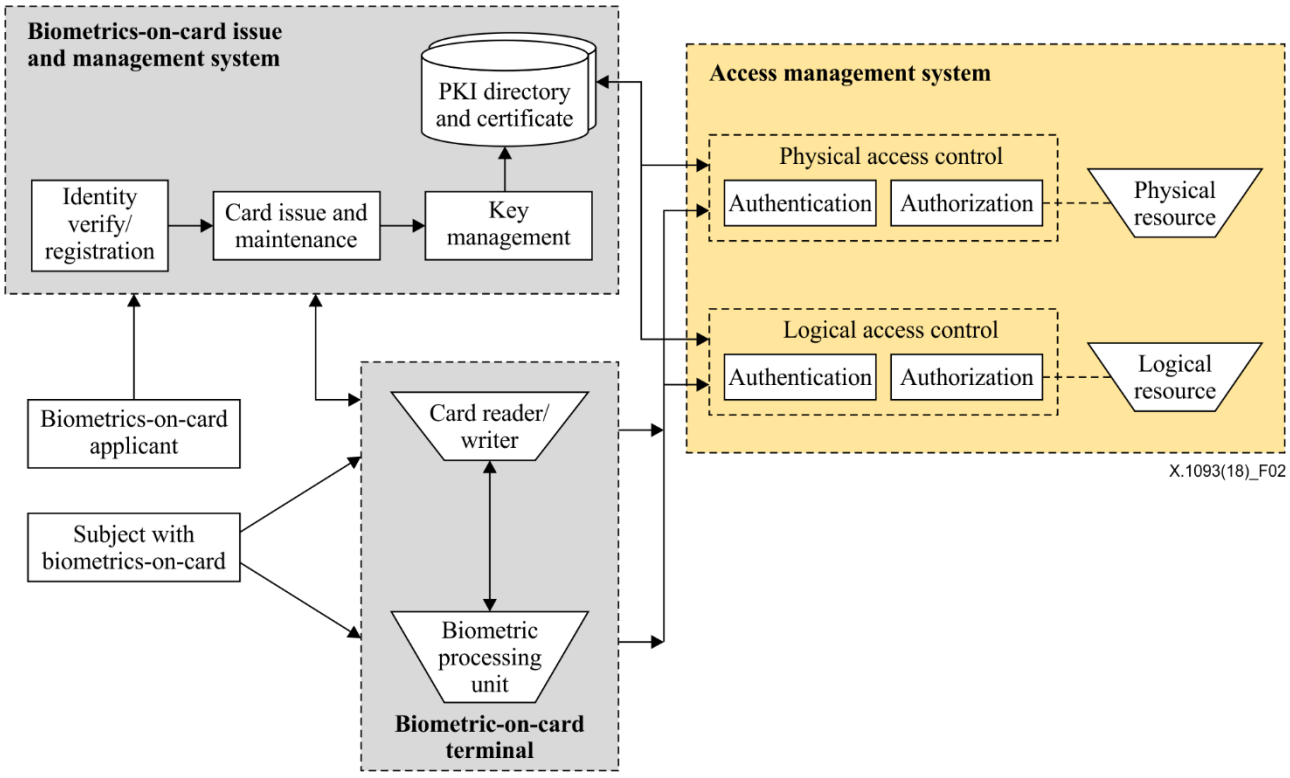

Figure 2 – Access management with biometrics-on-card

The hardware and software specifications of the smart IC card to be used as a biometrics-on-card should be referenced to the domestic and international standards in accordance with the application field. Therefore, this Recommendation describes the following functional requirements related to biometrics in addition to the general smart card specification.

6.2.1.1 Store-on-card

Store-on-card refers to a card that is designed to perform a comparison of biometric information outside the smart IC card, and thus the IC card is used only as a storage medium for storing biometric references. This can be divided into two types as shown in Figures 3 and 4, depending on whether or not there is a digital signature function with an ITU-T X.509 certificate.

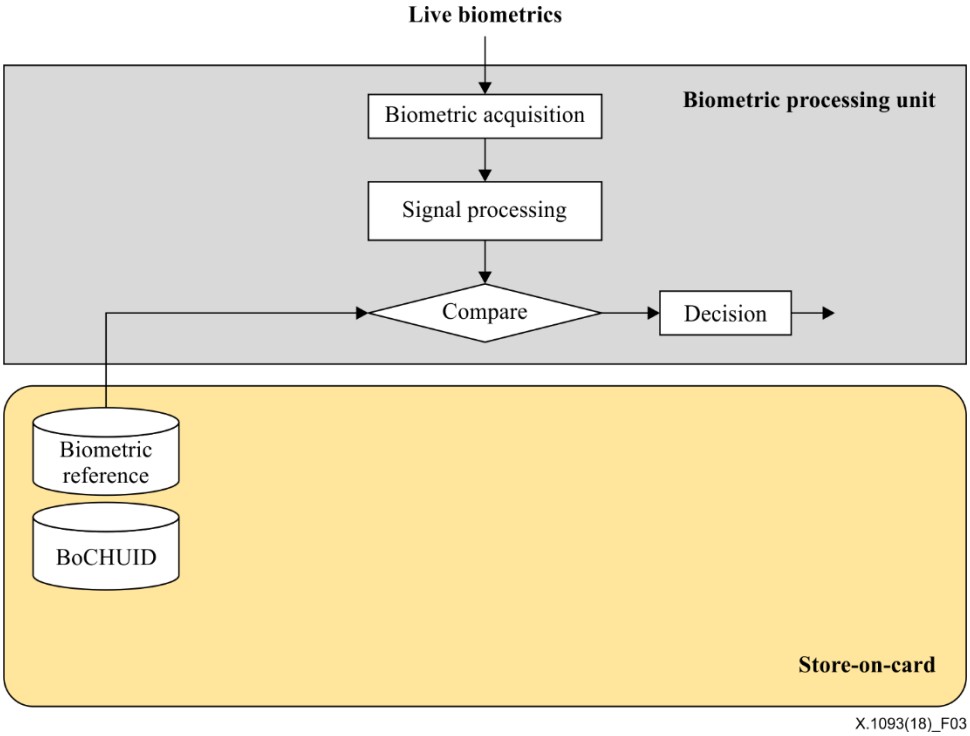

Figure 3 – Store-on-card without digital signature function

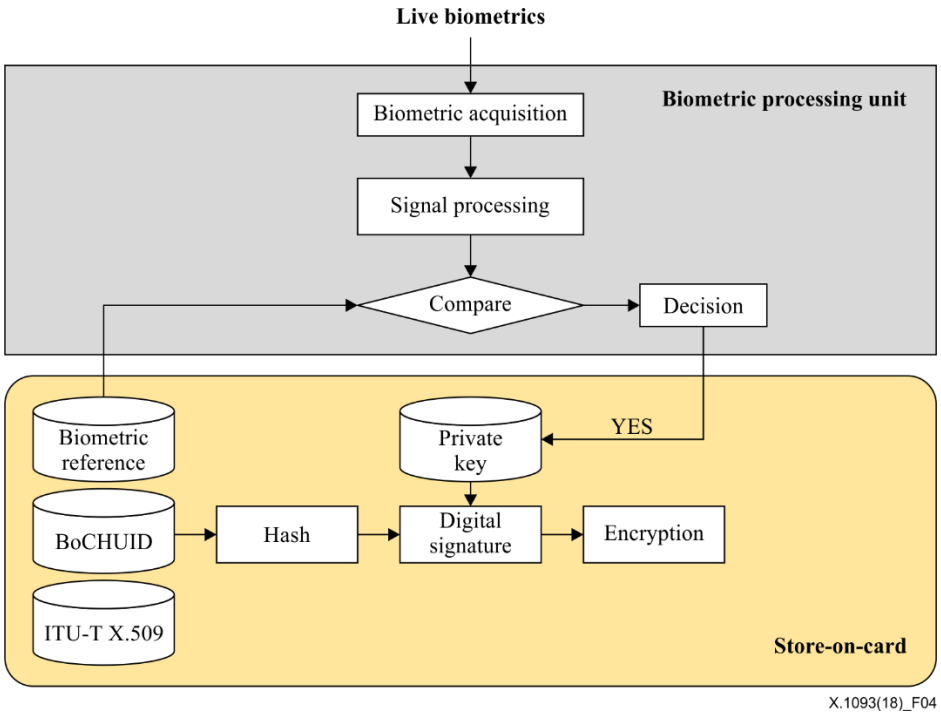

Figure 4 – Store-on-card with digital signature function

6.2.1.2 Compare-on-card

The compare-on-card refers to a card that is designed to perform a comparison of biometric reference within a smart IC card, and thus the IC card requires an additional computational capability of comparing in addition to storing the biometric reference. For the on-card comparison, the biometric processing unit acquires live biometrics, extracts feature information from the biometric information, and transmits it to the card. This can be divided into two types as shown in Figures 5 and 6, depending on whether or not there is a digital signature function with an ITU-T X.509 certificate.

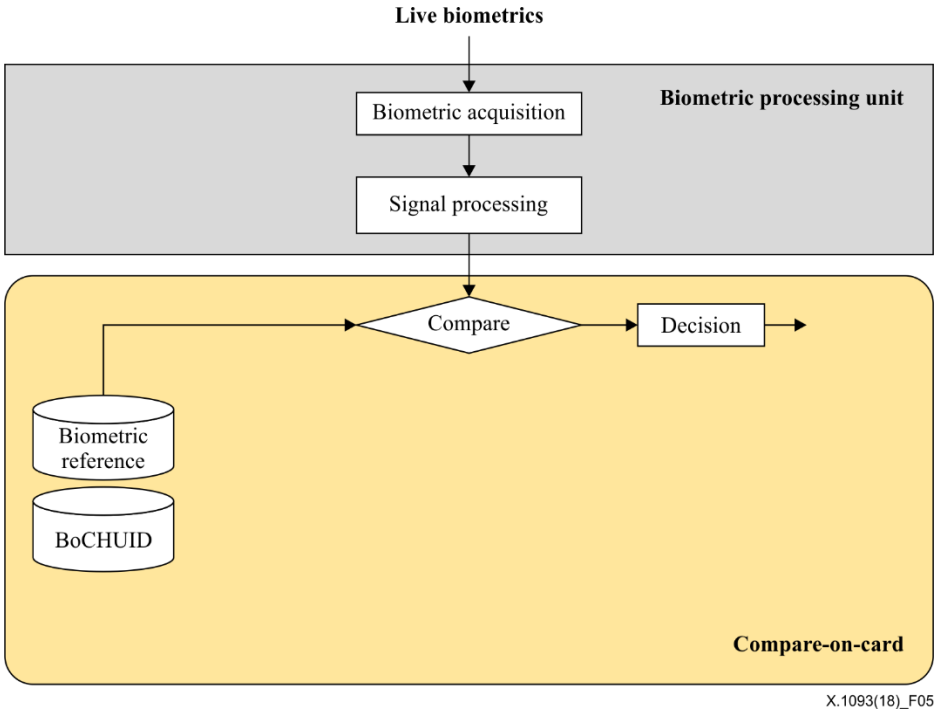

Figure 5 – Compare-on-card without digital signature function

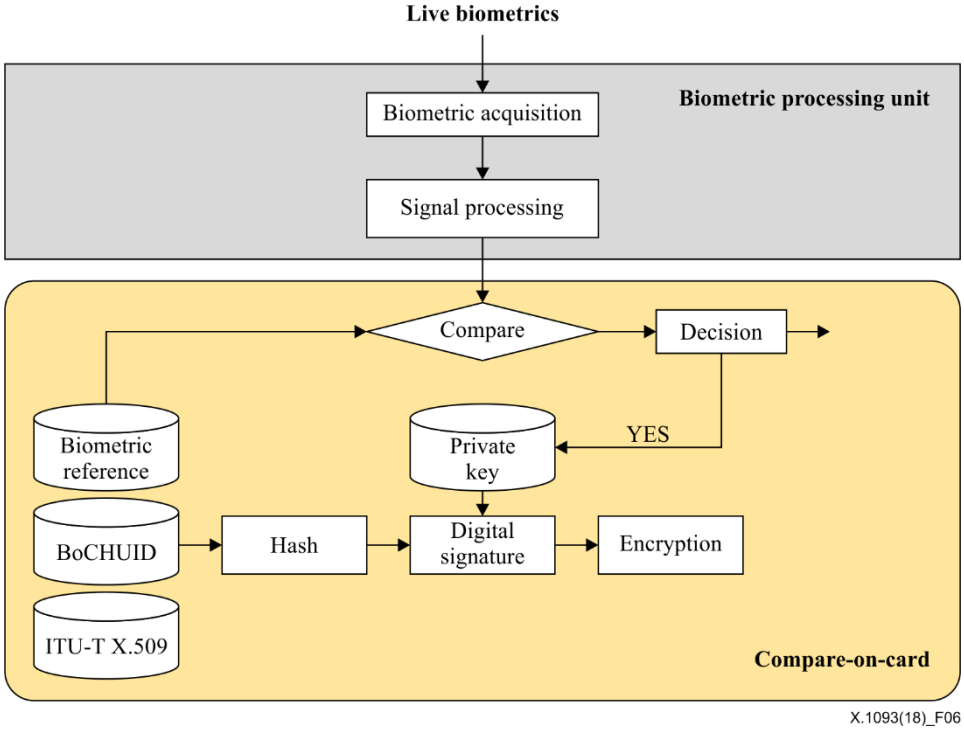

Figure 6 – Compare-on-card with digital signature function

6.2.1.3 Sensor-on-card

Sensor-on-card refers to a card that is designed to perform the entire biometric recognition process inside the IC card. Therefore, the IC card can process live biometrics, extract features and compare the stored biometric references, and so additional computational power is required. When this sensor-on-card is adopted, not only the registered biometric reference but also the acquired biometric information is not transmitted outside of the card, which is a useful method for securing the biometric security of the user. This can be divided into two types as shown in Figures 7 and 8, depending on whether or not there is a digital signature function with an ITU-T X.509 certificate.

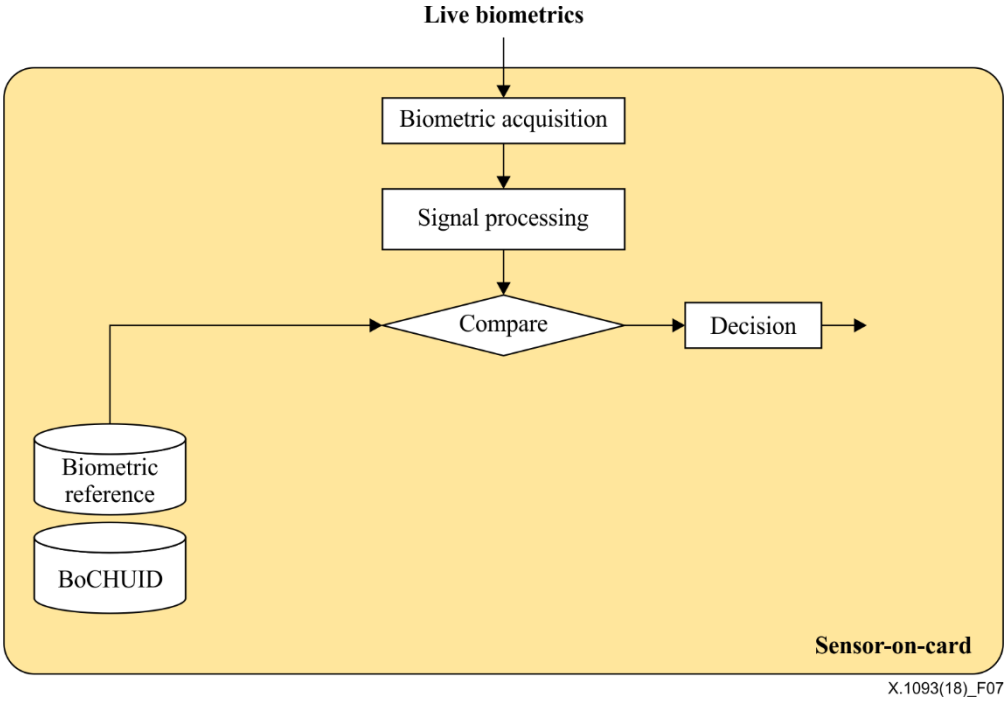

Figure 7 – Sensor-on-card without digital signature function

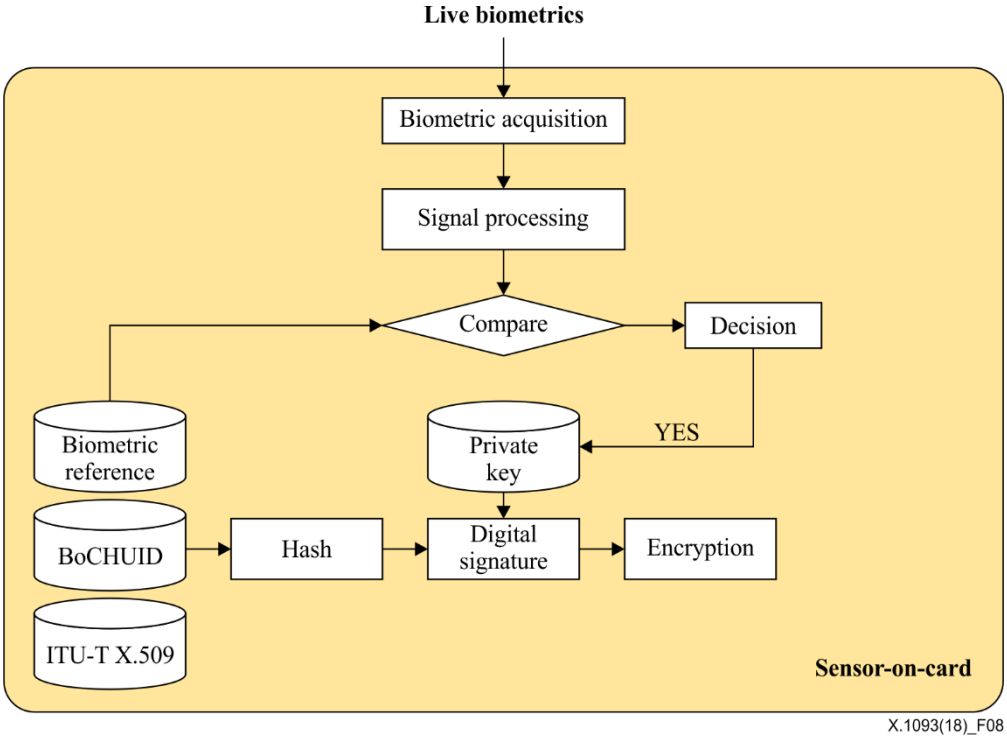

Figure 8 – Sensor-on-card with digital signature function

6.2.2 Biometric processing unit

The biometric processor is located at the point where the biometrics-on-card holder wishes to authenticate himself/herself. The role of the biometric information processing unit depends on whether the biometrics-on-card used is a store-on-card, a compare-on-card or a sensor-on-card. In each case, the required function is shown in Figures 3 to 8. In the case of the sensor-on-card, the biometric authentication result is received from the card, so that the actual biometric processing function is not required.

6.2.3 Biometrics-on-card reader and writer

The biometrics-on-card reader is located at the point where the cardholder will logically and physically access using the biometrics-on-card. The reader retrieves the appropriate information and communicates with the biometrics-on-card for transmission to the access control system for approval or denial of access. On the other hand, the card writer stores and initializes personal authentication related information in the biometrics-on-card. The biometric-on-card terminal consists of the biometric-on-card reader and writer and the biometric processing unit.

6.2.4 Biometrics-on-card issue and management system

The biometrics-on-card issue and management system relates to the handle biometric-on card applicant for issuing the card under a registration process and also managing the life cycle of the issued card according to the deployed policy. Detailed process and procedures are described in clause 7.

6.3 Biometrics-on-card personal authentication processes

6.3.1 Personal authentication using store-on-card

The biometrics-on-card provides signed biometric information that can be read from the card after simple owner verification using the cardholder's PIN. At this time, when issuing the biometrics-on-card, the biometric reference should be digitally signed to provide strong security for manipulation of the biometric reference.

Personal authentication using the store-on-card without digital signature function proceeds in the following order:

1) The cardholder presents the card through the local system of the access control point.
2) The local system reads the biometrics-on-card holder unique identifier (BoCHUID) of the biometrics-on-card owner.
3) The local system verifies the expiration date to ensure that the expiration date of the biometrics-on-card is not expired.
4) The local system receives the PIN from the card owner, and then requests verification from the biometrics-on-card.
5) When the validity of the cardholder's PIN is confirmed, the local system reads the biometric reference in the biometrics-on-card.
6) Check whether the digital signature of the cardholder's biometric is signed by a trusted authority and whether the biometric information stored on the card has not been altered.
7) The local system scans the live biometric information of the cardholder, compares it with the biometric reference stored in the card, verifies whether the cardholder is the same, and outputs the personal authentication result.

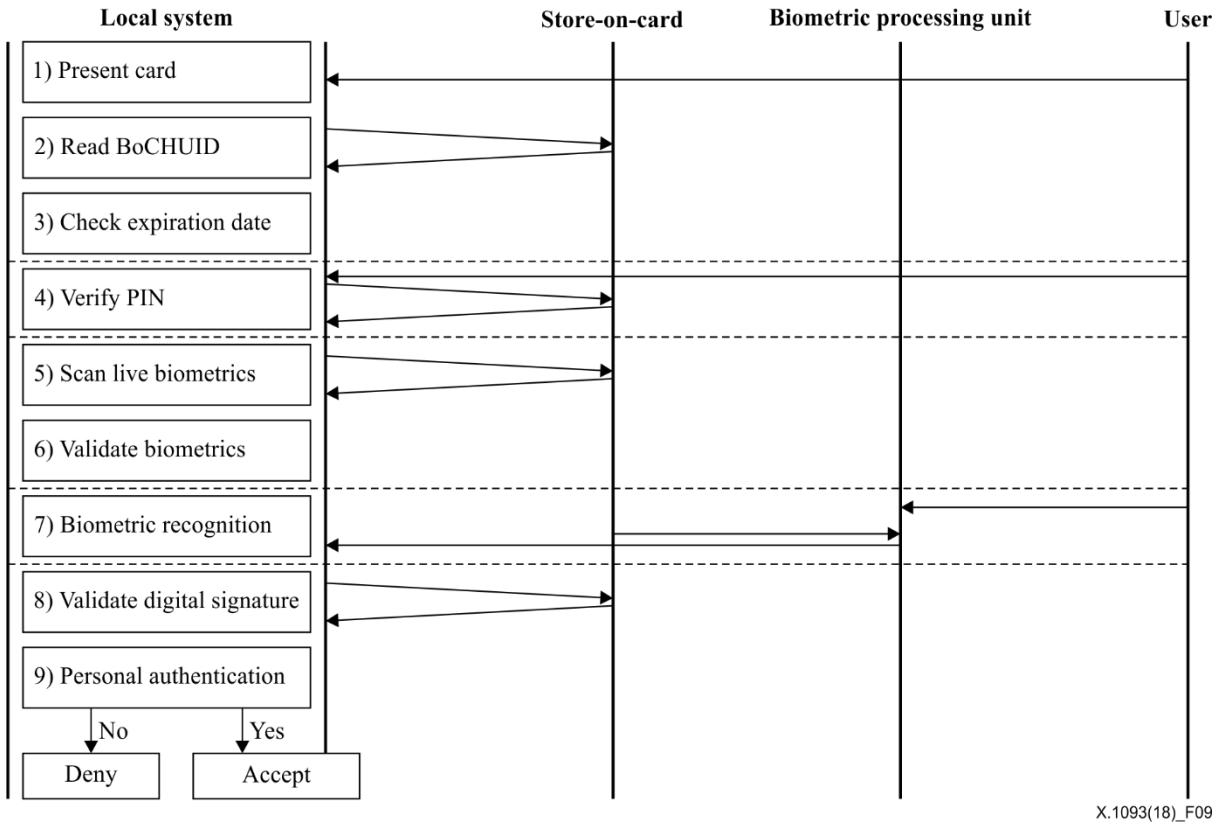

Figure 9 – Personal authentication using store-on-card

In the store-on-card with digital signature function, authentication using the private key is composed of a process of verifying the certificate in the biometrics-on-card and a request of signing the existence of the private key corresponding to the certificate. Therefore, the biometrics-on-card must contain an asymmetric private key and corresponding certificate in it. By using the digital signatures in addition to biometrics, more secure multi-factor personal authentication can be performed. However, this requires additional infrastructure to enable the online status checking of certificates. In this case, overall personal authentication processes shown in Figure 9 are as follows:

1) The cardholder presents the card through the local system of the access control point.
2) The local system reads the BoCHUID of the presented biometrics-on-card.
3) The local system verifies the expiration date to ensure that the expiration date of the biometrics-on-card is not expired.
4) The local system receives the PIN from the card owner, and then requests verification and receives the result.
5) When the validity of the cardholder's PIN is confirmed, the local system reads the biometric reference in the biometrics-on-card.
6) Check whether the digital signature of the cardholder's biometric is signed by a trusted authority and whether the biometric reference stored on the card has not been altered.
7) The local system scans the actual biometric information of the cardholder and compares the biometric information stored in the card with the biometric reference stored in the card to check whether the cardholder is the same, and then it confirms the cardholder's legitimacy.
8) The local system verifies the signature included in the card certificate and checks the validity period and certificate revocation. The local system retrieves the signature algorithm and key length specified in the certificate and requests the card to sign the BoCHUID.
9) By verifying the signature for the BoCHUID returned from the card, the cardholder finally authenticates the user that it has the correct private key.

6.3.2 Personal authentication using compare-on-card

Personal authentication using a compare-on-card without digital signature function proceeds in the following order:

1) The cardholder presents the card through the local system of the access control point.
2) The local system reads the BoCHUID of the presented biometrics-on-card.
3) The local system verifies the expiration date to ensure that the expiration date of the biometrics-on-card is not expired.
4) The local system receives the PIN from the card owner, and then requests verification from the biometrics-on-card.
5) When the cardholder's PIN is confirmed, the local system scans the cardholder's live biometrics and transmits the characteristic point to the biometrics-on-card.
6) The card is compared with the stored biometric information to check whether the owner of the card is the same and transmits the result to the local system.

On the compare-on-card with digital signature function, authentication using the authentication key consists of a certificate verification in the biometrics-on-card and a procedure of requesting signature by checking whether the private key corresponding to the certificate is owned. Therefore, the biometrics-on-card shall contain an asymmetric private key and corresponding certificate in it. In this case, overall personal authentication processes shown in Figure 10 are as follows:

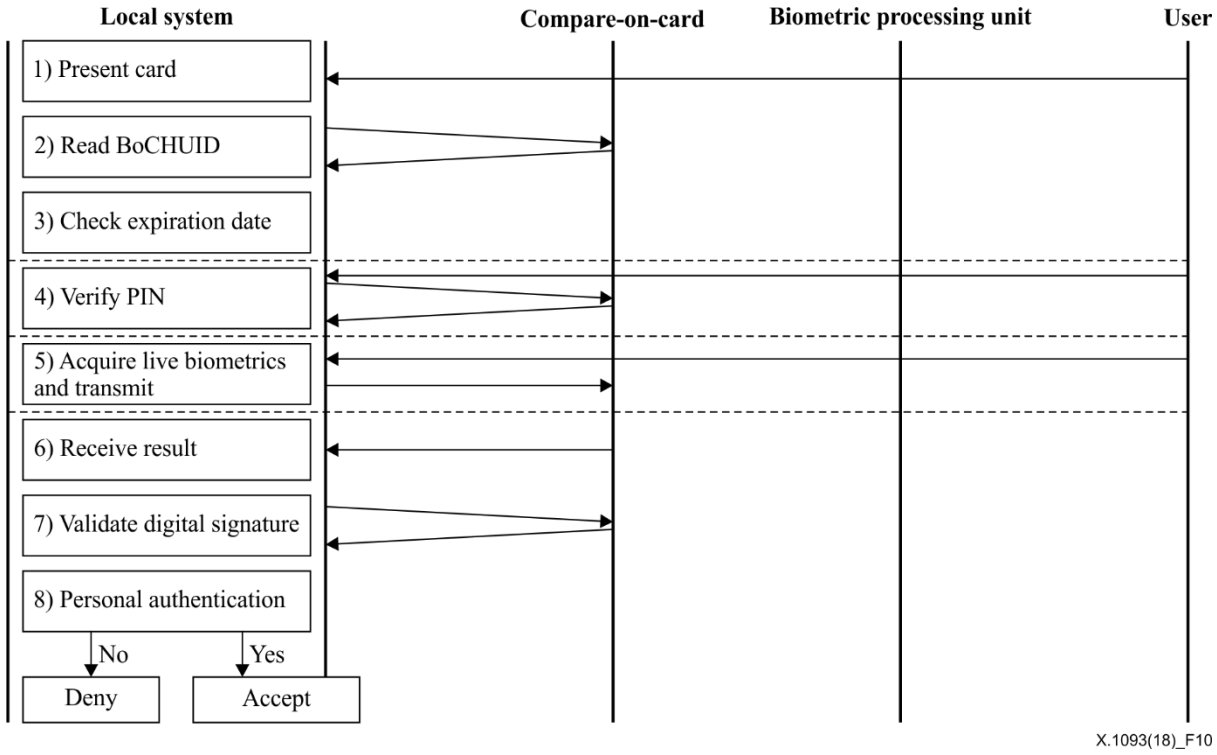

Figure 10 – Personal authentication using compare-on-card

1) The cardholder presents the card through the local system of the access control point.
2) The local system reads the BoCHUID of the presented biometrics-on-card.
3) The local system verifies the expiration date to ensure that the expiration date of the biometrics-on-card is not expired.
4) The local system receives the PIN from the card owner, and then requests verification and receives the result.

5) When the cardholder's PIN is confirmed, the local system scans the cardholder's live biometric information and transmits the characteristic point to the biometrics-on-card.

6) The card is compared with the stored biometric information to check whether the owner of the card is the same and transmits the result to the local system.

7) If the authentication succeeds in the previous step, the local system verifies the signature included in the card certificate and checks the validity period or certificate revocation. The local system retrieves the signature algorithm and key length specified in the certificate and requests the card to sign the BoCHUID.

8) By verifying the signature on the BoCHUID returned from the card, the cardholder finally authenticates the user that he or she has the correct private key.

6.3.3 Personal authentication using sensor-on-card

Personal authentication using the sensor-on-card without a digital signature function proceeds in the following order:

1) The cardholder presents the card through the local system of the access control point.

2) The local system reads the BoCHUID of the biometrics-on-card.

3) The local system verifies the expiration date to ensure that the expiration date of the biometrics-on-card is not expired.

4) The local system receives the PIN from the card owner, and then requests verification from the biometrics-on-card.

5) If the cardholder's PIN is confirmed, the biometrics-on-card is requested to be authenticated.

6) The biometrics-on-card scans the live biometrics of the card owner and compares it with the biometric reference stored in the card to confirm whether the card holder is the same or not, and transmits the result to the local system.

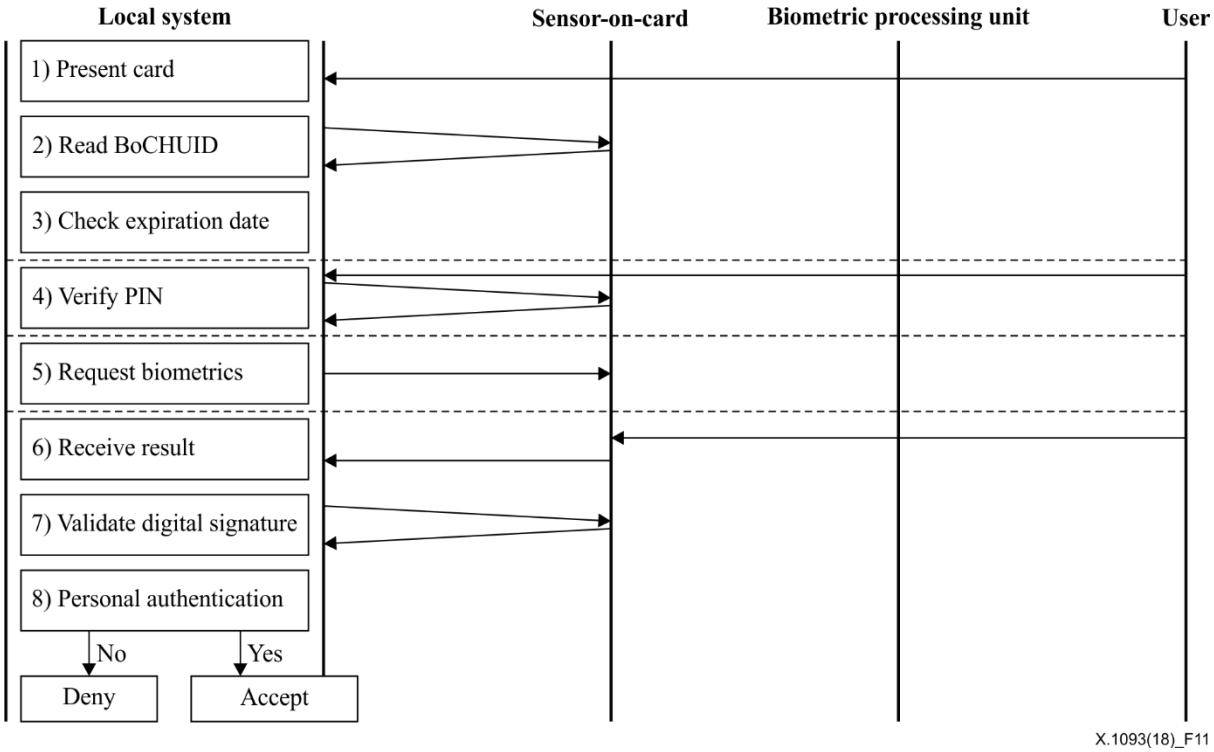

Figure 11 – Personal authentication using sensor-on-card

In this case, personal authentication processes using the sensor-on-card with digital signature are shown in Figure 11 as follows:

1) The cardholder presents the card through the local system of the access control point.
2) The local system reads the BoCHUID of the biometrics-on-card.
3) The local system verifies the expiration date to ensure that the expiration date of the biometrics-on-card is not expired.
4) The local system receives the PIN from the card owner, and then requests verification and receives the result.
5) If the cardholder's PIN is confirmed, the biometrics-on-card is requested to be authenticated.
6) The biometrics-on-card scans the live biometric information of the card owner and compares it with the biometric reference stored in the card to confirm whether the card holder is the same or not, and transmits the result to the local system.
7) If authentication succeeds in the previous step, the local system verifies the signature included in the card certificate and checks the validity period or certificate revocation. The local system retrieves the signature algorithm and key length specified in the certificate and requests the card to sign the BoCHUID.
8) By verifying the signature on the BoCHUID returned from the card, the cardholder finally authenticates the user that he or she has the correct private key.

7 Management of biometrics-on-card lifecycle

The biometrics-on-card is managed according to the following seven life cycles to securely store important personal authentication information such as personal information and biometric information.

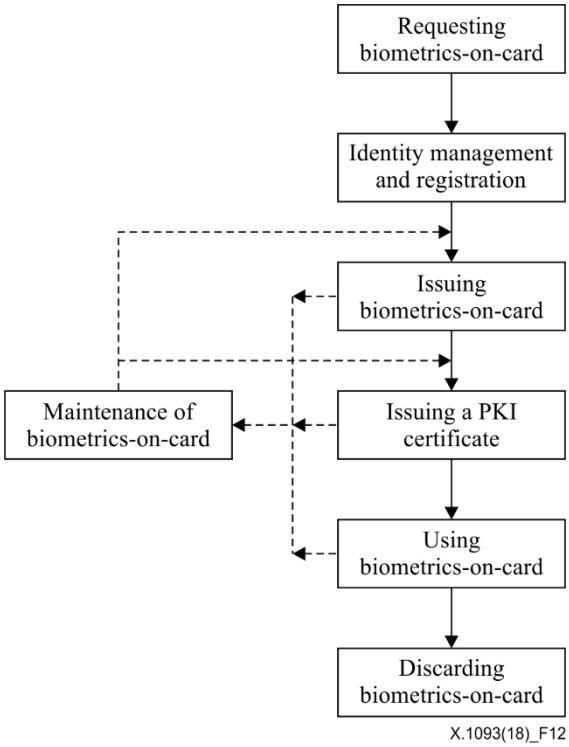

Figure 12 – Personal authentication using sensor-on-card

7.1 Requesting biometrics-on-card

The applicant requests issuance of the biometrics-on-card.

7.2 Identity management and registration

The identity and registration of the applicant is added to the biometrics-on-card management system.

7.3 Issuing biometrics-on-card

The biometric and personal information is stored in the card based on the information of the applicant when the card is issued.

7.3.1 Biometrics-on-card players and roles

– Biometrics-on-card registrar: This is the person who receives information of the applicant and proves the legitimacy of card issuance and requests issuance of the card to the person in charge of issuance;

– Biometrics-on-card issuer: This is the person who issues the biometrics-on-card to the applicant after the applicant's identity verification has been completed;

– Biometrics-on-card certification authority: This includes the issuing authority for digital signature, private certification authority and accredited certification authority.

7.3.2 Issuing procedures

The process for issuing the biometrics-on-card to a legitimate user is done as follows:

Applicants must submit a card application form and related documents to the biometrics-on-card registration person and submit their personal identification (ID) documents (e.g., passport, driver's license, institution or ID card) together.

The registrar will review the card issuer's qualification based on the documents submitted by the applicant. If there is no abnormality, the registration person acquires the biometric information (face image, fingerprint, etc.) of the applicant and stores it. The original image of biometric identification information that has been issued later is discarded according to the security policy. The person in charge of registration can use the biometric information of the applicant for issuance of the biometrics-on-card.

The issuer personalizes the card based on the applicant's information. The applicant must verify the identity of the card issuer by 1: 1 face-to-face contact with the card issuer and receive the biometrics-on-card when the following identification and issuance procedures has been completed:

1) Applicant submits personal identification ID documents to the person in charge of issuance, and the person in charge of issuance confirms the name and photograph of the newly created biometrics-on-card and the personal ID documents received from the applicant. Also they make sure that the photo of the newly created biometrics-on-card matches the applicant.

2) The issuer confirms whether the biometric reference stored in the newly created biometrics-on-card matches the biometric information of the applicant.

3) The person in charge of issuance generates a PIN number and notifies the applicant of the PIN number.

4) The applicant generates an encryption key pair for the biometrics-on-card and obtains the corresponding certificate from the certification authority.

5) The person in charge of issuance stores the name of the card recipient, the identity of the issuer, the card number, and the PKI certificate information in the biometrics-on-card system database.

7.4 Issuing a PKI certificate

A certificate is issued to authenticate the cardholder and it is stored on the card. The certificate can be used simultaneously for personal authentication and also message authentication by a digital signature.

7.5 Using biometrics-on-card

In terms of using the biometrics-on-card for personal authentication, the use of the card is the same as that of the existing ID card. The cardholder is given access to the physical access and logical access to the facility access, information system and all facilities within the institution through his / her biometrics-on-card. However, the owner of the card determines the level of access to the facility and determines access to and access to the facility in accordance with his or her prior security rating. In other words, the access ID for accessing the existing ID card and the password or access ID for accessing the system are integrated into a biometrics-on-card, minimizing the waste of resources and controlling the physical access through the control personnel at the same time. This enables strong security and minimizes the manpower requirement by adopting the biometrics-on-card and the electronic access control device.

7.6 Maintenance of biometrics-on-card

This is the step of continuously updating the biometrics-on-card and stored data.

7.7 Discarding biometrics-on-card

The biometrics-on-card may be discarded due to a change of the user's identity. It shall be discarded if the card is lost, stolen, or if it is required to be replaced. Disposal of a biometrics-on-card is the process of permanently invalidating the data and keys in the card to prevent the card from being used again, and destroying the card.

8 Telebiometric access management with biometrics-on-card

8.1 Telebiometric access models with biometrics-on-card.

The telebiometric access management system consists of several biometrics-on-card based access management systems which belong to remotely located physical facilities or logically separated resources. Each access management system shall satisfy the functional and managerial requirements described in clauses 6 and 7. Telebiometric access is needed in cases where a subject requires permission to access other resources which belongs to another access management system.

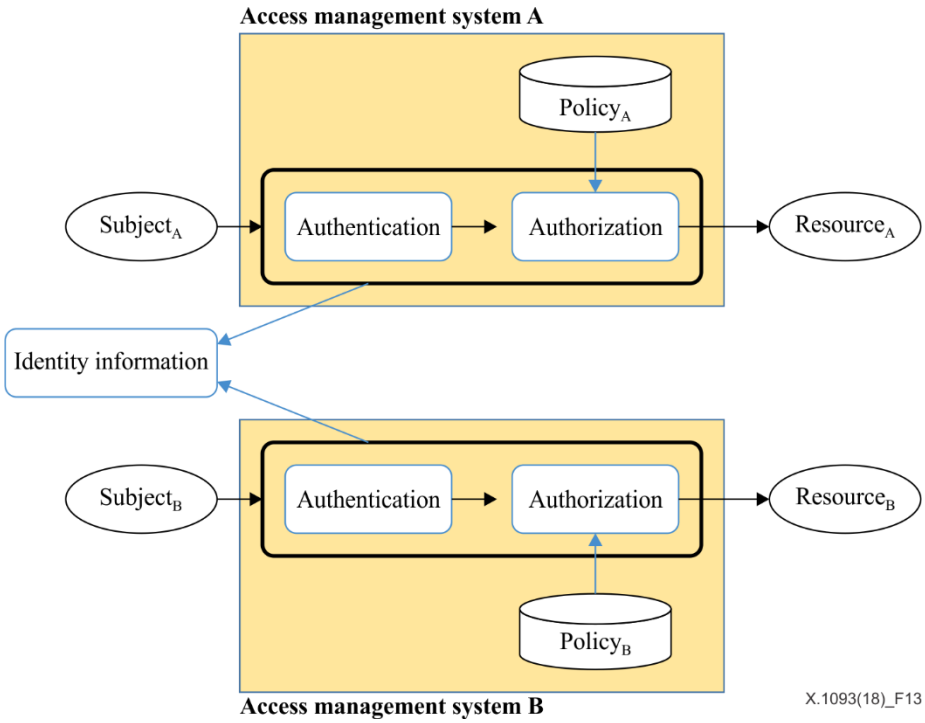

Figure 13 – Telebiometric access model with shared identity information

To implement the telebiometric access model, the identity information should be shared with other access management systems as shown in Figure 13. In this case, each access manage system authenticates a requested subject according to each policy. Moreover, each access manage system can independently update and manage its policy.

Each access system can share not only identity information but also policy as shown in Figure 14. In this case each management system should synchronize the identity information and access management policies to be operated in a unified way, so all participating organizations can implement the same security policy.

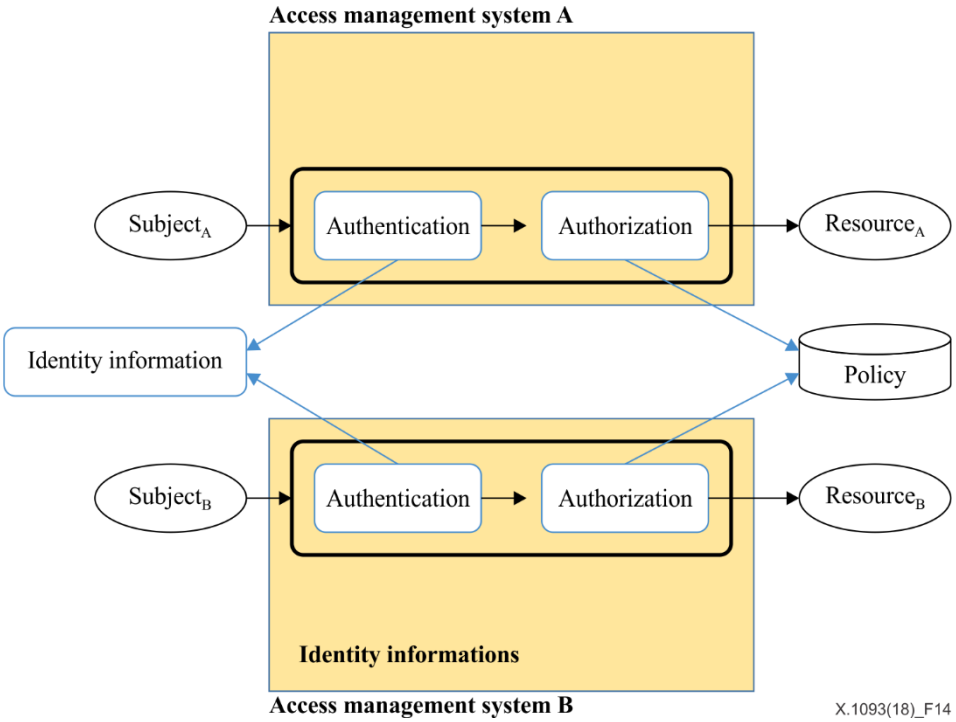

Figure 14 – Telebiometric access model with shared identity information and policy

8.2 Federated telebiometric access management with biometrics-on-card

Federated access management is required when an authenticated subject from one organization attempts to access a resource in another organization. Figure 15 shows an example of a federated access control system. For a subject to be authenticated in an access management system, federated access control requirements are implemented by the members of the federation in accordance with a shared trust relationship and common policies agreed by the organizations participating in the federation.

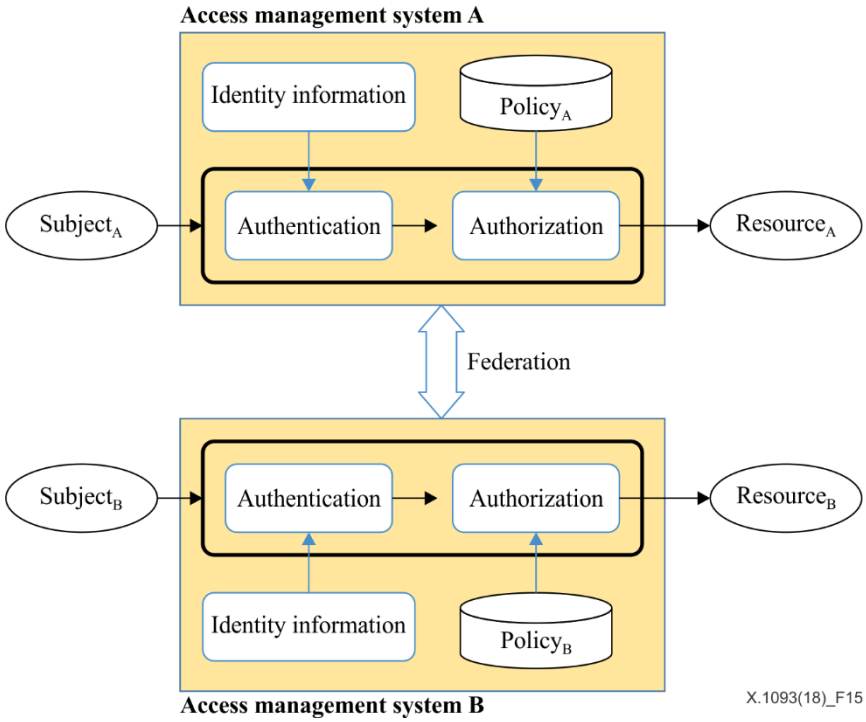

Figure 15 – Federated telebiometric access management

8.3 Telebiometric access privilege management with biometrics-on-card

Under biometrics-on-card access control, privilege management is performed on the subject identity registered in clause 7.2. This scheme employs mechanism such as access control lists (ACLs) related to the certificate revocation list (CRL) to specify the identities of those allowed to access a resource. In this scheme, the granting of resource access privileges to a subject is made prior to any subject access request and subject identity and access privileges are added to the relevant resource ACL(s).

If a subject identity matched an identity recorded in the relevant ACL, the subject is given access to the resource in accordance with their access privileges.

Privilege management requires the following activities:

1) creation of the set of privileges to be used to denote and set the types of operation performed on the resource;
2) establishing the rules specifying the assignment of privileges according to the access control policy;
3) update and revocation of privileges and identity attributes.

Bibliography

[b-ITU-T X.1080.0] Recommendation ITU-T X.1080.0 (2017), *Access control for telebiometrics data protection*.

[b-ITU-T X.1085] Recommendation ITU-T X.1085 (2016), *Information technology – Security techniques – Telebiometric authentication framework using biometric hardware security module*.

[b-ISO/IEC 24745] ISO/IEC 24745:2011, *Information Technology – Security techniques – Biometric information protection*.

[b-ISO/IEC 24761] ISO/IEC 19761:2009, *Information Technology – Security techniques – Authentication context for biometrics*.

[b-ISO/IEC 29146] ISO/IEC 29146:2016, *Information Technology – Security techniques – A framework for access management*.

SERIES OF ITU-T RECOMMENDATIONS

Series A	Organization of the work of ITU-T
Series D	Tariff and accounting principles and international telecommunication/ICT economic and policy issues
Series E	Overall network operation, telephone service, service operation and human factors
Series F	Non-telephone telecommunication services
Series G	Transmission systems and media, digital systems and networks
Series H	Audiovisual and multimedia systems
Series I	Integrated services digital network
Series J	Cable networks and transmission of television, sound programme and other multimedia signals
Series K	Protection against interference
Series L	Environment and ICTs, climate change, e-waste, energy efficiency; construction, installation and protection of cables and other elements of outside plant
Series M	Telecommunication management, including TMN and network maintenance
Series N	Maintenance: international sound programme and television transmission circuits
Series O	Specifications of measuring equipment
Series P	Telephone transmission quality, telephone installations, local line networks
Series Q	Switching and signalling, and associated measurements and tests
Series R	Telegraph transmission
Series S	Telegraph services terminal equipment
Series T	Terminals for telematic services
Series U	Telegraph switching
Series V	Data communication over the telephone network
Series X	**Data networks, open system communications and security**
Series Y	Global information infrastructure, Internet protocol aspects, next-generation networks, Internet of Things and smart cities
Series Z	Languages and general software aspects for telecommunication systems

Printed in Switzerland
Geneva, 2019