International Telecommunication Union

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

X.1087

(10/2016)

SERIES X: DATA NETWORKS, OPEN SYSTEM COMMUNICATIONS AND SECURITY

Information and network security – Telebiometrics

Technical and operational countermeasures for telebiometric applications using mobile devices

Recommendation ITU-T X.1087

International Telecommunication Union

ITU-T X-SERIES RECOMMENDATIONS

DATA NETWORKS, OPEN SYSTEM COMMUNICATIONS AND SECURITY

PUBLIC DATA NETWORKS	X.1–X.199
OPEN SYSTEMS INTERCONNECTION	X.200–X.299
INTERWORKING BETWEEN NETWORKS	X.300–X.399
MESSAGE HANDLING SYSTEMS	X.400–X.499
DIRECTORY	X.500–X.599
OSI NETWORKING AND SYSTEM ASPECTS	X.600–X.699
OSI MANAGEMENT	X.700–X.799
SECURITY	X.800–X.849
OSI APPLICATIONS	X.850–X.899
OPEN DISTRIBUTED PROCESSING	X.900–X.999
INFORMATION AND NETWORK SECURITY	
General security aspects	X.1000–X.1029
Network security	X.1030–X.1049
Security management	X.1050–X.1069
Telebiometrics	**X.1080–X.1099**
SECURE APPLICATIONS AND SERVICES	
Multicast security	X.1100–X.1109
Home network security	X.1110–X.1119
Mobile security	X.1120–X.1139
Web security	X.1140–X.1149
Security protocols	X.1150–X.1159
Peer-to-peer security	X.1160–X.1169
Networked ID security	X.1170–X.1179
IPTV security	X.1180–X.1199
CYBERSPACE SECURITY	
Cybersecurity	X.1200–X.1229
Countering spam	X.1230–X.1249
Identity management	X.1250–X.1279
SECURE APPLICATIONS AND SERVICES	
Emergency communications	X.1300–X.1309
Ubiquitous sensor network security	X.1310–X.1339
PKI related Recommendations	X.1340–X.1349
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.1087

Technical and operational countermeasures for telebiometric applications using mobile devices

Summary

Biometric technology in mobile devices is frequently used in various areas which require a high level of reliability such as e-banking, and procurement services. It is necessary to make efforts to develop a security system that can pre-emptively cope with potential security threats for the purpose of ensuring mobile biometric data security. Since biometric technology handles sensitive personally identifiable information (PII), some of the privacy issues for biometric in mobile devices should be considered.

Recommendation ITU-T X.1087 specifies the implementation model and threats in the operating telebiometric systems in mobile devices. It provides a general guideline for security countermeasures from both the technical and operational perspectives in order to establish a safe mobile environment for the use of telebiometric systems.

History

Edition	Recommendation	Approval	Study Group	Unique ID*
1.0	ITU-T X.1087	2016-10-14	17	11.1002/1000/13061

Keywords

E-payment, fast identity on-line, FIDO, mobile device, telebiometric applications, telebiometric authentication model.

* 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.1087

Technical and operational countermeasures for telebiometric applications using mobile devices

1 Scope

This Recommendation provides a framework to ensure security and reliability of the flow of biometric information for telebiometric applications using mobile devices. This Recommendation defines 12 telebiometric authentication models depending on the configuration of the biometric sensor, the mobile device, and the server. It also specifies the threats in the operating telebiometric systems in the mobile devices and proposes a general guideline for security countermeasures from both the technical and operational perspectives in order to establish a safe mobile environment for the use of telebiometric systems.

The following topics are addressed within the scope of this Recommendation:

– Telebiometric security reference models in operating telebiometric systems using a mobile device including cloud computing services.

– General related threats and countermeasures to ensure security and reliability for telebiometric applications using mobile devices.

The related standard environment is depicted in Figure 1.

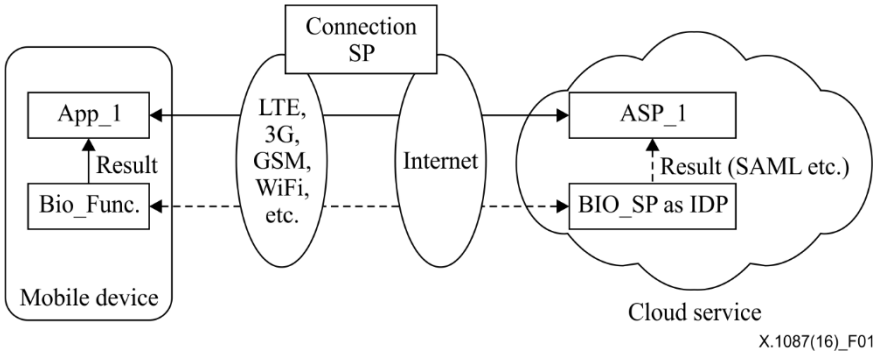

Figure 1 – Standard environment for telebiometric applications using mobile devices

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.1089] Recommendation ITU-T X.1089 (2008), *Telebiometrics authentication infrastructure (TAI).*

[IETF RFC 4346] IETF RFC 4346 (2008), *The Transport Layer Security (TLS) Protocol Version 1.2.*

3 Definitions

3.1 Terms defined elsewhere

This Recommendation uses the following terms defined elsewhere:

3.1.1 biometric (adjective) [b-ISO/IEC 19784-1]: Pertaining to the field of biometrics.

3.1.2 biometrics (noun) [b-ISO/IEC 19784-1]: Automated recognition of individuals based on their behavioural and biological characteristics.

3.1.3 biometric reference [b-ISO/IEC 19784-1]: One or more stored biometric samples, biometric templates or biometric models attributed to a biometric data subject and used for comparison.

3.1.4 biometric sample [b-ISO/IEC 2382-37]: Analogue or digital representation of biometric characteristics prior to biometric feature extraction process.

3.1.5 biometric template [b-ISO/IEC 19784-1]: Set of stored biometric features comparable directly to probe biometric features.

3.1.6 comparison (match/matching) [b-ISO/IEC 19794-1]: Estimation, calculation or measurement of similarity or dissimilarity between biometric probe(s and biometric reference(s).

3.1.7 comparison decision [b-ISO/IEC 2382-37]: Determination of whether the recognition biometric probe(s) and biometric reference(s) have the same biometric source, based on a comparison score(s), a decision policy(ies) including a threshold, and possibly other inputs.

3.1.8 comparison score [b-ISO/IEC 19784-1]: Numerical value (or set of values) resulting from a comparison.

3.1.9 false match [b-ISO/IEC 2382-37]: Comparison decision of "match" for a biometric probe and a biometric reference that are not from different biometric capture subjects.

3.1.10 false non-match [b-ISO/IEC 2382-37]: Comparison decision of "non-match" for a biometric probe and a biometric reference that are from the same biometric capture subject and of the same biometric characteristics.

3.1.11 match [b-ISO/IEC 2382-37]: Comparison decision stating that the biometric probe(s) and and the biometric reference are from the same source.

3.1.12 mobile device [b-ITU-T X.1158]: A small, hand-held computing device with a subscriber identity module (SIM) card, typically having a display screen with touch input and/or a miniature keyboard and is not heavy.

3.1.13 non-match [b-ISO/IEC 2382-37]: Comparison decision stating that the biometric probe(s) and the biometric reference are not from the same source.

3.2 Terms defined in this Recommendation

This Recommendation defines the following term:

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

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

APDU Application Protocol Data Unit

API Application Programming Interface

App Application

BC	Biometric Certificate
BioAPI	Biometric Application Programming Interface
CPU	Central Processing Unit
FIDO	Fast Identity On-line
ICC	Integrated Circuit Card
ID	Identification
MNO	Mobile Network Operator
MoC	Match on Card
NFC	Near Field Communication
OS	Operating System
OTA	Over The Air
PAN	Private Access Network
PII	Personally Identifiable Information
PKI	Public Key Infrastructure
POS	Point-Of-Sale
SD	Secure Digital
SE	Secure Element
SP	Service Provider
TSP	Token Service Provider
USB	Universal Serial Bus
USIM	Universal Subscriber Identity Module
TLS	Transport Layer Security
TSM	Telebiometrics System Mechanism
WiFi	Wireless Fidelity

5 Conventions

None.

6 Prerequisites

None.

7 Authentication models

7.1 Overview

This Recommendation takes into account the three perspectives below, dividing the models into 12 categories depending on the configuration of the biometric sensor, the mobile device, and the server. It also specifies the threats in the operating telebiometric systems in the mobile devices and proposes a general guideline for security countermeasures from both the technical and operational perspectives in order to establish a safe mobile environment for the use of telebiometric systems.

Table 1 – Authentication models

	Biometric sensor	Mobile device	Server
Model 1	Capturing	Comparison Store*	
Model 2	Capturing	Comparison	Store
Model 3	Capturing		Comparison Store
Model 4	Capturing Comparison		Store
Model 5	Capturing Comparison	Store	
Model 6	Capturing Comparison Store		
Model 7	Capturing Store	Comparison	
Model 8	Capturing Store		Comparison
Model 9	Capturing	Store	Comparison
Model 10		Capturing Comparison Store	
Model 11		Capturing	Comparison Store
Model 12		Capturing Comparison	Store
* Biometric reference template location.			

7.2 Model 1

Figure 2 illustrates model 1.

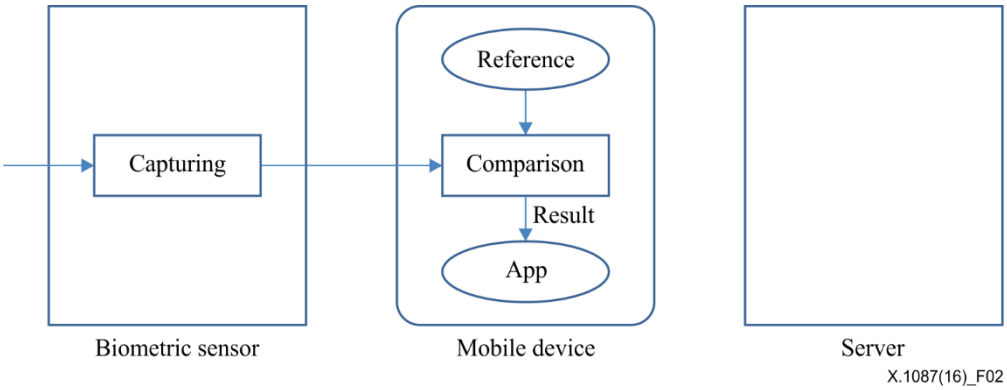

Figure 2 – Model 1

The mobile device takes the request from the application (App); it acquires sample data, compares it with the registered user's template, and transfers the result to the App.

Template identification (ID) information is required, which is the comparison result. For model 1, it is assumed that the mobile device is in a difficult situation to telecommunicate with the server including the wireless environment, and the mobile device side such as smartphones is given sufficient processing resources. The processing resources must be sufficient to acquire sample data and compare it. External biometric sensors communicate with the mobile device using near field communication (NFC) when the mobile device cannot support the sensor because of a modality or applicability characteristic. This model can be used when the server side trusts the mobile device-side processing procedures.

7.3 Model 2

Figure 3 illustrates model 2.

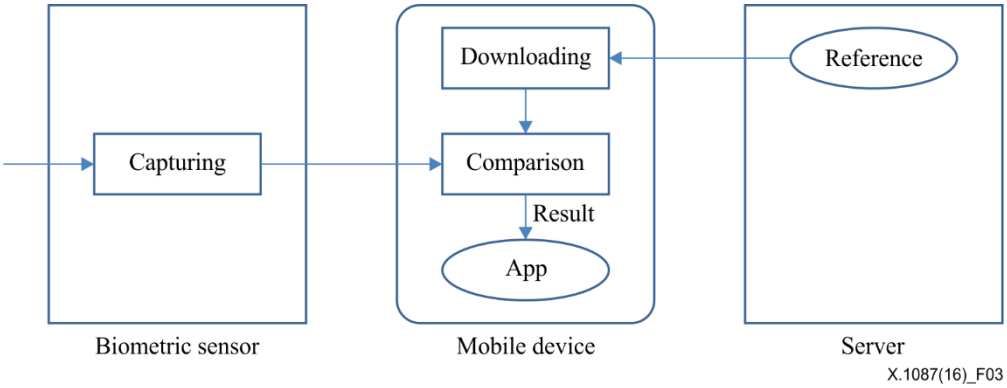

Figure 3 – Model 2

The App requests verification from the server. The server sends the registered user's template. The mobile device compares the acquired sample data with the received template, and sends the result to the App Model 2 that has the same sequence as model 1, with the exception of the transfer of the template from the server. Template ID information is required. This then forms the comparison result. Under this structure, it is recommended to use as many terminals as possible. This is suitable for the web-verification model, as users can connect to the server from any mobile device. Model 2 requires the registration of the biometric reference template with the server. This model also requires the server to trust the mobile device processing procedure.

7.4 Model 3

Figure 4 illustrates model 3.

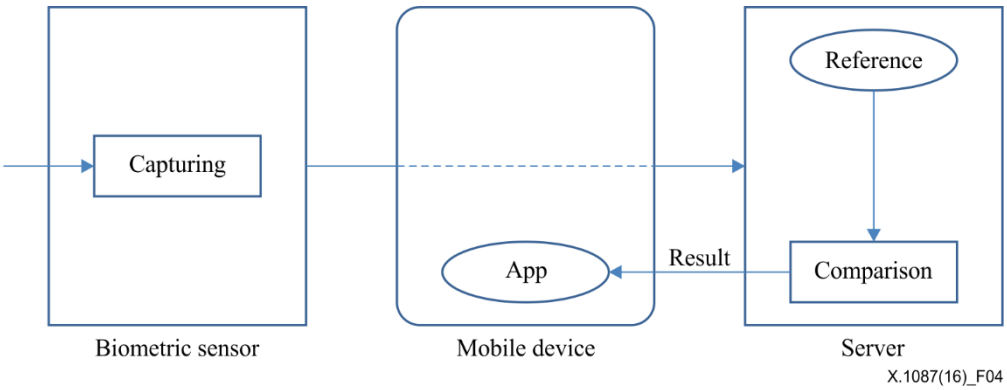

Figure 4 – Model 3

The server requests the sample data required from the biometric sensor for verification, the biometric sensor acquires the sample data and transfers it to the server through the mobile device, and the server finally compares it with the user's template.

For model 3, it is assumed that the mobile device side cannot guarantee sufficient resources in terms of processing power, memory, security, etc. That is the reason why the mobile device is used only for the telecommunication methods. The external biometric sensor communicates with the mobile device using the near field communication when the mobile device cannot support the sensor because of a modality or applicability characteristic.

The user registers their biometric reference in advance with a server that has a trusted biometric reference template.

This model requires that the server trust the data captured from a biometric sensor.

7.5 Model 4

Figure 5 illustrates model 4.

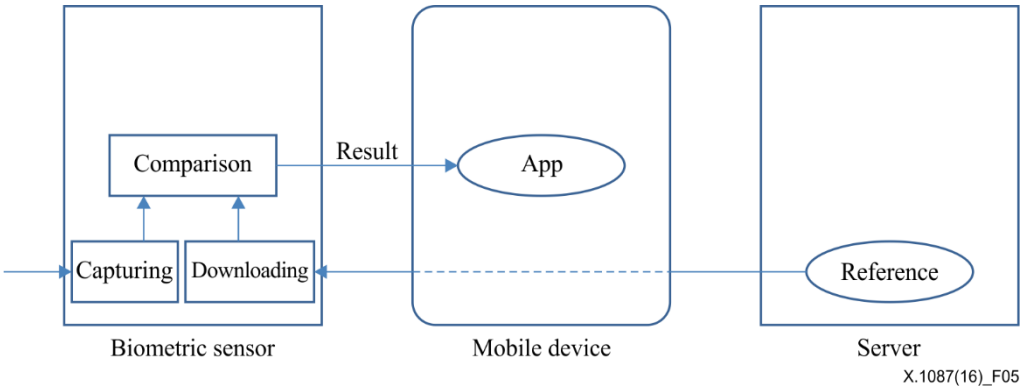

Figure 5 – Model 4

The App requests verification from mobile device, the biometric sensor acquires sample data, and requests the user's template from the server. The biometric sensor then compares the template which is transferred from the server with the captured sample data, and transfers the result data to the mobile device. In this model, the biometric sensors could be hardware security modules. These modules are physical devices that traditionally come in the form of a smartcard or some other universal serial bus (USB) type security token that can provide tamper proof against penetration or modification of an internal operation and/or insertion of active or passive tapping mechanism to disclose secret data or to alter the operation of devices. For model 4, it is assumed that the mobile device side cannot guarantee sufficient resources in terms of processing power, memory, security, etc. That is the reason why the mobile device is used only for the telecommunication methods.

7.6 Model 5

Figure 6 illustrates model 5.

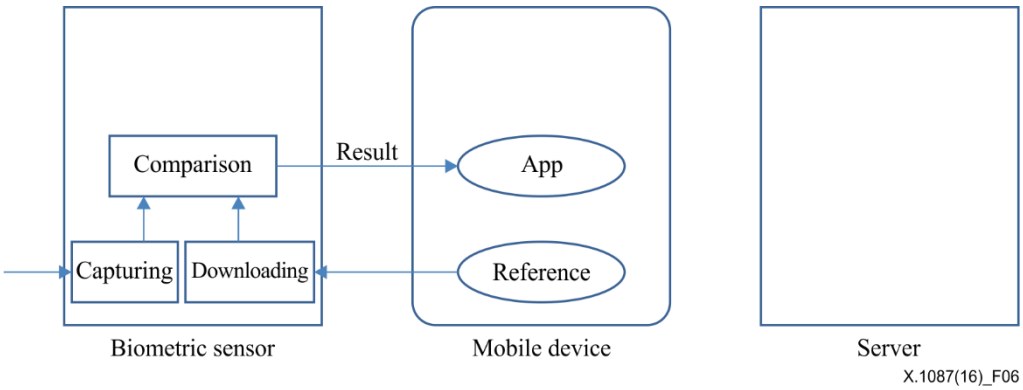

Figure 6 – Model 5

The biometric sensor compares the template which is transferred from the mobile device with the captured sample data, and transfers the result data to the mobile device. Model 5 has the same sequence as Model 4, with the exception of the transfer of the template from the mobile device. In this model, a biometric sensor could be a hardware security module.

For model 5, it is assumed that the mobile device has difficulty to telecommunicate with the server including the wireless environment.

7.7 Model 6

Figure 7 illustrates model 6.

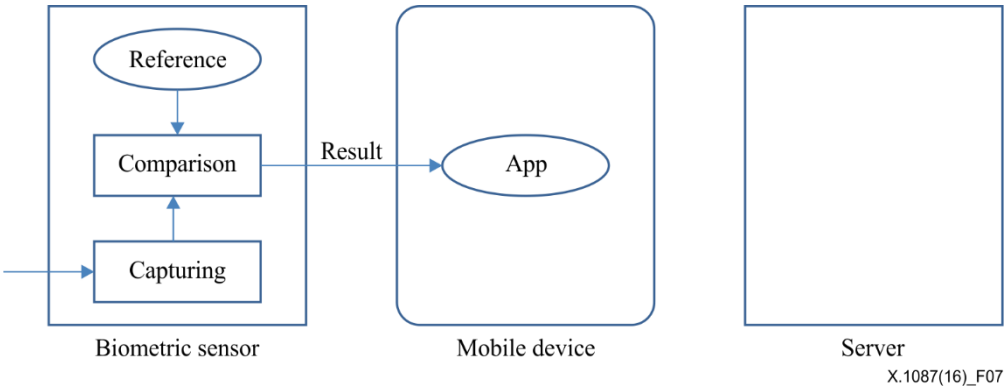

Figure 7 – Model 6

The biometric sensor receives the request from the App; it acquires the sample data, compares it with the registered user's template, and transfers the result to the App.

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

The external biometric sensor communicates with the mobile device using near field communication when the mobile device cannot support the sensor because of a modality or applicability characteristic.

In this model, the biometric sensors could be hardware security modules. These modules are physical devices that traditionally come in the form of a smartcard or some other USB type security token that can provide tamper proof against penetration or modification of an internal operation and/or insertion of active or passive tapping mechanism to disclose secret data or to alter the operation of devices.

For model 6, it is assumed that the mobile device side cannot guarantee security. This is practical when put to use for national infrastructure systems that need a high level of security.

7.8 Model 7

Figure 8 illustrates model 7.

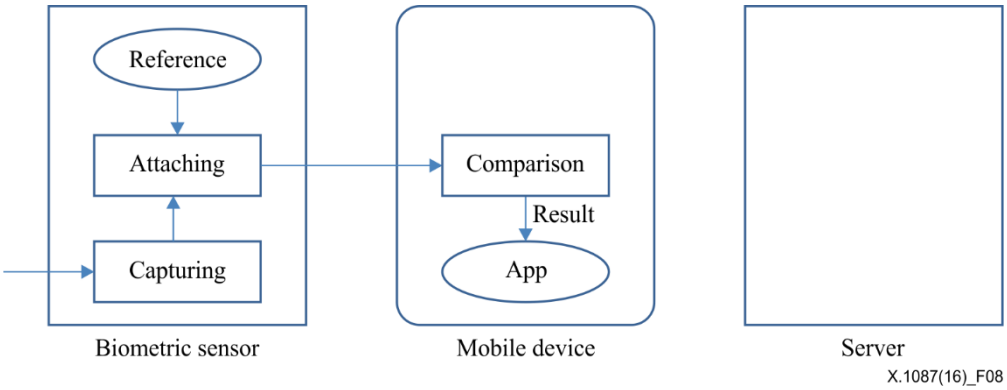

Figure 8 – Model 7

The mobile device requires the comparison function, which is needed for the template and captured sample data. The biometric sensor transfers the acquired sample data and template to the mobile device, and the comparison is ultimately conducted within the mobile device. The mobile device trusts the data captured from a biometric sensor. This is practical for use in credit authorization systems, as a comparison algorithm is not required for the biometric sensor.

7.9 Model 8

Figure 9 illustrates model 8.

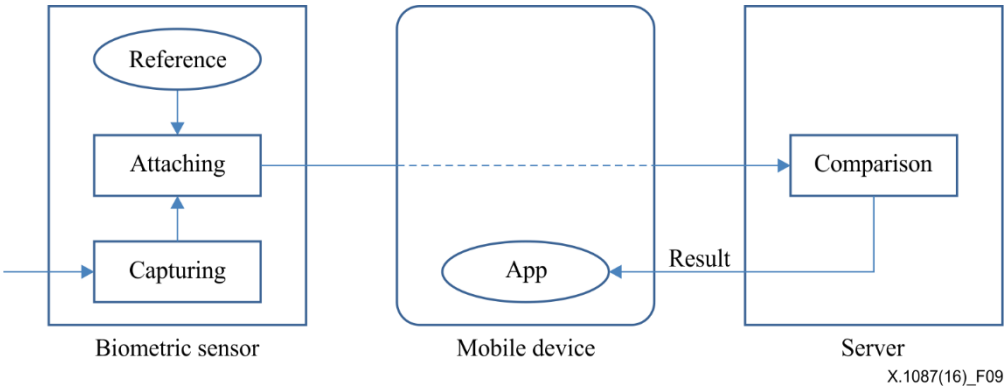

Figure 9 – Model 8

The biometric sensor receives the request from the App, and it acquires the sample data. Model 8 has the same sequence as model 7, excluding the comparison location.

The biometric sensor transfers the acquired sample data and template to the server through the mobile device, and the comparison is ultimately conducted within the server. The mobile device is used only for the telecommunication methods. This model requires that the server trust the data captured from a biometric sensor.

7.10 Model 9

Figure 10 illustrates model 9.

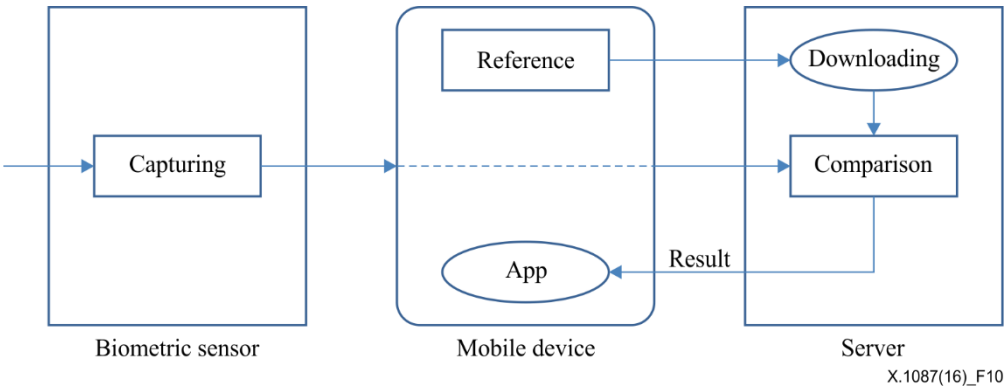

Figure 10 – Model 9

The server requests the sample data from mobile device required for verification, the biometric sensor acquires the sample data and transfers it to the server through the mobile device, and the server finally compares it with the user's template.

This model requires that the server trust the data captured from a biometric sensor.

7.11 Model 10

Figure 11 illustrates model 10.

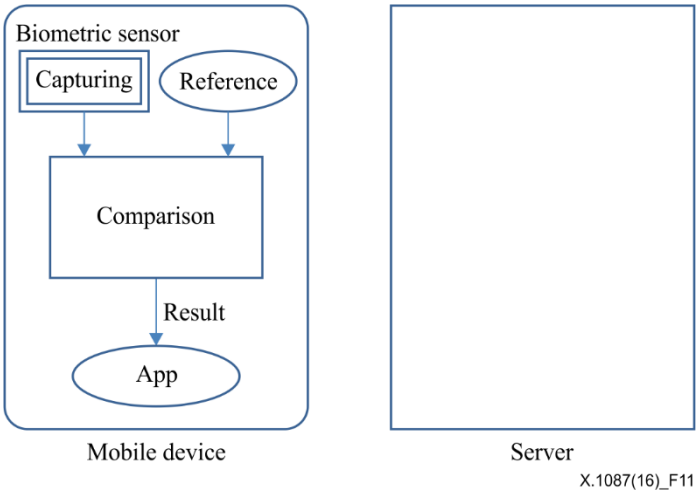

Figure 11 – Model 10

The mobile device acquires the sample data, compares it with the registered user's template, and transfers the result to the App in the mobile device. Template ID information is required, which is the comparison result. For model 10, it is assumed that the mobile device can support the biometric processing load, and the mobile device is given sufficient processing resources. The processing resources must be sufficient to acquire the sample data and to compare it.

7.12 Model 11

Figure 12 illustrates model 11.

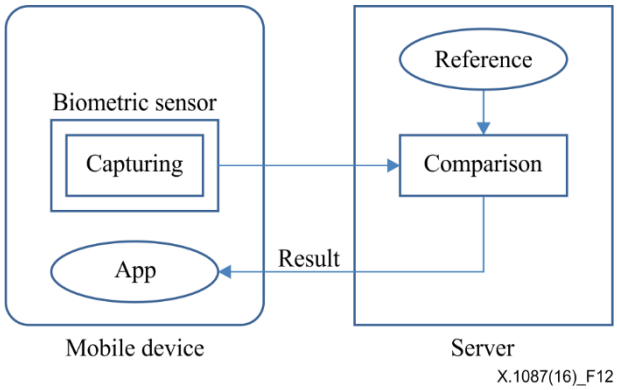

Figure 12 – Model 11

For this model, it is assumed that the mobile device resources, such as memory, disk, etc., are insufficient.

The App requests verification from the mobile device. The mobile device captures the sample data, and requests the verification result from the server with the captured sample data. The server then compares the sample data with the registered user's template, and transfers the result to the App.

Users register in advance their biometric reference template with the server. Template ID information is required in the comparison result.

7.13 Model 12

Figure 13 illustrates model 12.

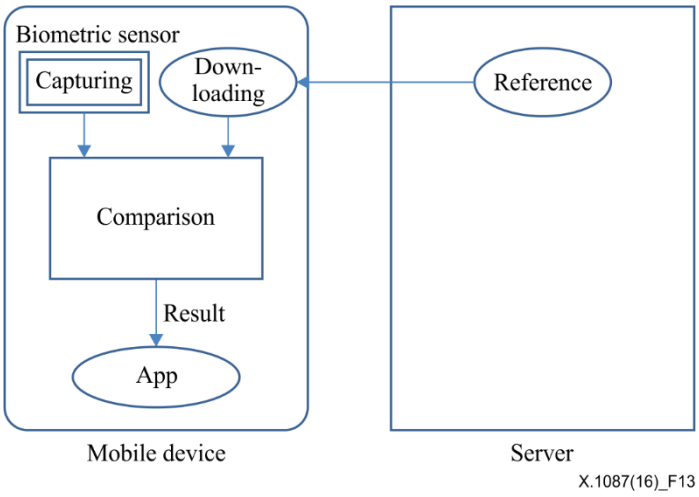

Figure 13 – Model 12

Model 12 has the same sequence as model 10, with the exception of the transfer of the template from the server. Template ID information is required, which is the comparison result.

For model 12, it is assumed that the mobile device can support the biometric processing load, and the mobile device is given sufficient processing resources. The processing resources must be sufficient to acquire the sample data and to compare it.

8 Vulnerabilities of telebiometrics mobile devices

Vulnerabilities mean weaknesses of the mobile devices and their inabilities to withstand hostile environment effects. Attacks are any attempts of unauthorized use, to intentionally destroy, and to maliciously modify or obtain illegally mobile devices assets. In other words, vulnerabilities are the internal attributes of mobile devices, while attacks are the external offensive activities on mobile devices.

8.1 Insufficient application programming interface management

The most distinctive feature of mobile device is the flexible application programming interfaces (APIs), which are mainly used for application development. However, insufficient application programming interface (API) management is responsible for most malicious codes. API management refers to the process of developing, publishing and managing application APIs. Generally, mobile device APIs are classified into open APIs for third-party application developments and controlled APIs for remote maintenances. Controlled APIs generally have superior or particular privileges, which can be used for remote system update, file erasure and information retrieval. If malicious persons obtain controlled APIs, they can initiate negative activities such as backdoor attacks. On the other hand, some open APIs have inappropriate privileges so that they might be utilized to acquire certain privileges and initiate attacks.

8.2 Insecure wireless channels

In wireless environments including cellular networks, user data and control signals transmitted between mobile devices and network devices can be captured as they are transmitted over the air (OTA). If these communication channels are left unprotected or unencrypted, the information will be exposed. In reality, most wireless channels do not have sufficient security protections due to the following reasons:

1) insufficient security protection of protocol stacks;
2) cost considerations due to the high costs of security solutions;
3) Government policies that prevent the implementation of security mechanisms.

Even though security mechanisms, such as authentication, encryption, access control, etc., have been implemented, mobile devices cannot resist some enhanced attacks due to the limited security intensity of the existing security mechanisms.

9 Security threats for each model

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

Table 2 – Security threats for each model

Model	Threats allowing illegal use by unauthorized users	Possible countermeasures
Model 1	– They may replace illegally captured data, such as stolen or altered data. – They may use an illegal biometric reference template data. – They may use an illegal comparison program. – Template can be leaked through the loss of the mobile devices.	– Mutual authentication between sensor and mobile device. – Encryption of the reference data.
Model 2	– They may replace illegally captured data, such as stolen or altered data. – They may alter illegally the data when the captured data is transferred. – They may use an illegal biometric reference template data. – They may use an illegal comparison program. – Leakage of the reference. – They may transfer data to an illegal server. – Template can be leaked through the loss of the mobile device. – Template is leaked by having a central server lost or stolen.	– Authentication of the sensor, mobile device and server. – For example, process key generation and digital signature generation inside of the universal subscriber identity module (USIM) card, when encryption operation is performed. – Encryption of the transmission channel. – Encryption of the reference data. – Encryption of the transmission channel.
Model 3	– They may replace illegally captured data, such as stolen or altered data. – They may alter illegally the data when the captured data is transferred. – They may attack the transmission channels. – They may transfer data to an illegal server. – Template is leaked by having a central server lost or stolen.	– Authentication of the sensor and server. – Encryption of the transmission channel. – Encryption of the transferred data.
Model 4	– They may replace illegally captured data, such as stolen or altered data. – They may use an illegal biometric reference template data. – They may use an illegal comparison program. – Template is leaked by having a sensor lost or stolen. – They may attack the transmission channels. – Template is leaked by having a central server lost or stolen.	– Authentication of the sensor and server. – Encryption of the reference data. – Encryption of the transmission channel. – Encryption of the transferred data.
Model 5	– They may replace illegally captured data, such as stolen or altered data. – They may use an illegal biometric reference template data. – They may use an illegal comparison program. – Template is leaked by having a sensor lost or stolen.	– Authentication of the sensor and mobile device. – Encryption of the reference data.

Table 2 – Security threats for each model

Model	Threats allowing illegal use by unauthorized users	Possible countermeasures
Model 6	– They may replace illegally captured data, such as stolen or altered data. – They may use an illegal biometric reference template data. – They may use an illegal comparison program. – Template is leaked by having a sensor lost or stolen.	– Encryption of the reference data.
Model 7	– They may replace illegally captured data, such as stolen or altered data. – They may alter illegally the data when the captured data is transferred. – They may use an illegal biometric reference template data. – They may use an illegal comparison program. – Template can be leaked through the loss of the mobile device.	– Authentication of the sensor and mobile device. – Encryption of the reference data.
Model 8	– They may replace illegally captured data, such as stolen or altered data. – They may alter illegally the data when the captured data is transferred. – They may attack the transmission channels. – They may transfer data to an illegal server.	– Authentication of the sensor and server. – Encryption of the transmission channel.
Model 9	– Misuse of the sensor (irrelevant App using the sensor). – Irrelevant App attacks on the sensor such as man-in-the-middle attacks; as a result, an irrelevant App uses the captured data. – They may use an illegal biometric reference template data. – They may use an illegal comparison program. – Template can be leaked through the loss of the mobile device.	– Authentication of the sensor and App. – Encryption of the reference data.
Model 10	– Misuse of the sensor (irrelevant App using the sensor). – Irrelevant App attacks on the sensor such as man-in-the-middle attacks; as a result, an irrelevant App uses the captured data. – They may attack the transmission channels. – They may transfer data to an illegal server. – Template is leaked by having a central server lost or stolen.	– Authentication of the sensor and App. – Authentication of the App and server. – Encryption of the transmission channel. – Encryption of the transferred data.

Table 2 – Security threats for each model

Model	Threats allowing illegal use by unauthorized users	Possible countermeasures
Model 11	– Misuse of the sensor (irrelevant App using the sensor). – Irrelevant App attacks on the sensor such as man-in-the-middle attacks; as a result, an irrelevant App uses the captured data. – They may use an illegal biometric reference template data. – They may use an illegal comparison program. – Template can be leaked through the loss of the mobile device. – They may attack the transmission channels. – They may transfer data to an illegal server. – Template is leaked by having a central server lost or stolen.	– Authentication of the sensor and App. – Authentication of the App and server. – Encryption of the reference data. – Encryption of the transmission channel. – Encryption of the transferred data.
Model 12	– Misuse of the sensor (irrelevant App using the sensor). – Irrelevant App attacks on the sensor such as man-in-the-middle attacks; as a result, an irrelevant App uses the captured data. – They may attack the transmission channels. – They may transfer data to an illegal server.	– Authentication of the sensor and App. – Authentication of the App and server. – Encryption of the transmission channel.

Furthermore, Figure 14 illustrates specific threats for the cooperation between the public key infrastructure (PKI) and a biometric authentication, such as the environment of this Recommendation. For a model that incorporates PKI, there remains the threat of a private key leaking out, and that somebody may use it illegally, such as case (a). Even without private key leakages, such as case (b), the relation between the PKI information and the biometric template information may not be guaranteed. Therefore, the biometric template information should require the identification information of the PKI certificate and the validity information for itself. This Recommendation assumes the use of a biometric certificate (BC) of [ITU-T X.1089] as the biometric template.

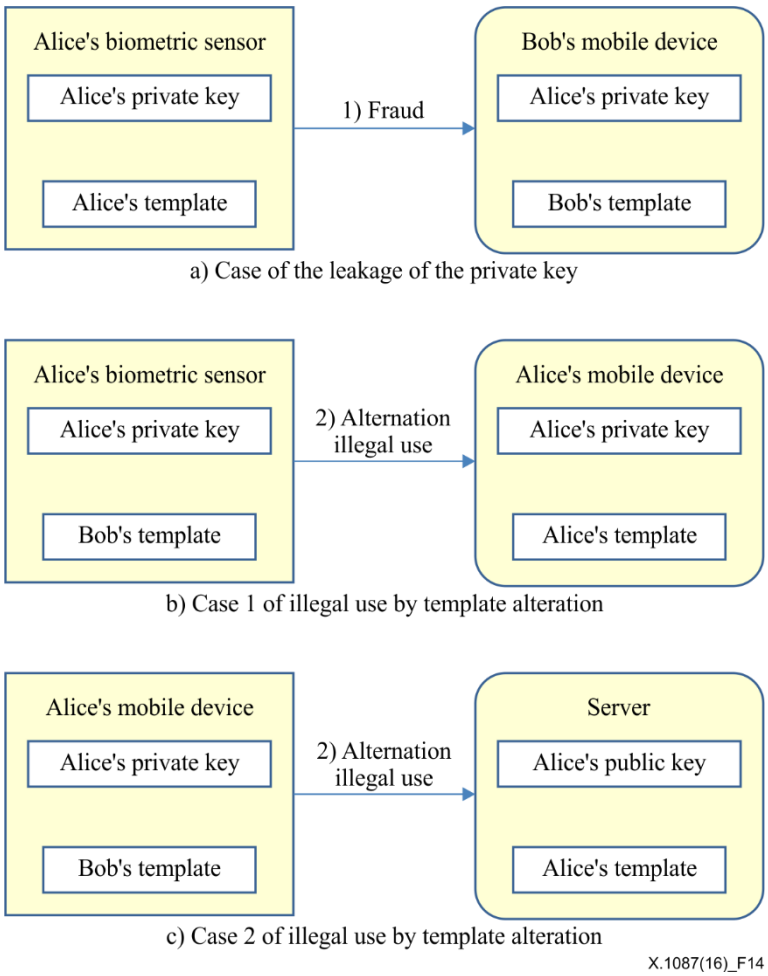

Figure 14 – Risk of illegal use by falsification of the template

Possible threats to private information protection on a sensor, mobile device or a trusted server are listed below:

– Biometric and private information fraud through an illegal sensor.
– Biometric and private information fraud through an illegal mobile device.
– Biometric and private information fraud through an illegal server.
– Biometric and private information fraud through connecting to an illegal network.

Counter measures are listed below:

– Authenticate a sensor using PKI.
– Authenticate a mobile device using PKI.
– Authenticate a trusted server using PKI.
– Encrypt the session key exchange by the use of the transport layer security (TLS) protocol as specified in [IETF RFC 4346].

Appendix I

Use cases

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

The following use case examples illustrate how the concepts discussed throughout this Recommendation can be applied.

I.1 Micro secure digital (SD)-based approach match on card using applet

As defined in model 1, the mobile device receives the request from the App; it acquires sample data, compares it with the registered user's template, and transfers the result to the App. The example application applied model 1 as shown in Figure I.1.

Model 1 that can occur in one way to improve the security vulnerabilities to compare and store in the micro SD match on card (MoC) built into the applet was commissioned. Micro SD has been developed in mobile telebiometrics systems as follows:

1 The biometric sensor captures the user's biometric sample.

2 The biometric sample in the form of a biometric template is converted to a direct wireless fidelity (WiFi) communication that is then delivered to the mobile device.

3 The biometric template that is equipped with a fingerprint authentication applet of the secure element (SE) region of the micro SD fingerprint authentication is sent to the applet.

4 The fingerprint template sent to the applet is registered with micro SD SE to be compared with the biometric reference.

5 User authentication via the mobile app to check the results.

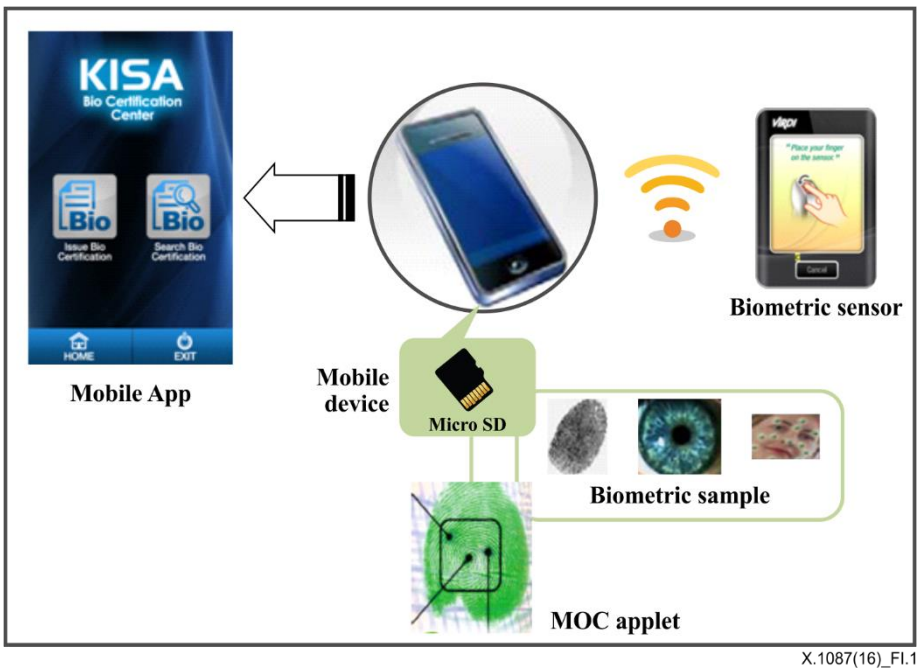

Figure I.1 – Flow of the mobile telebiometrics application system

Comparison and storage of the process of the biometrics mobile device mounted on the micro SD secure element in the applet to block information leakage by performing a security threat can be fundamentally blocked. Figure I.1 illustrates how the concepts discussed throughout this Recommendation can be applied with the following characteristics:

– Fingerprint authentication algorithm and fingerprint information are stored in the micro SD's SE (smartcard).
– Move and mounting are free to the smartphone when changing.
– The independence of the fingerprint authentication applet is ensured regardless of the operating system (OS) and the smartphone model.
– As all stored and matching fingerprint information is in the micro SD, the flow of information is basically cut off; in many cases, it is safe from external security threats.
– Fingerprint applet is executed under the control of Java cards, and real-time environment is verified.
– Support of the encryption of biometric information.

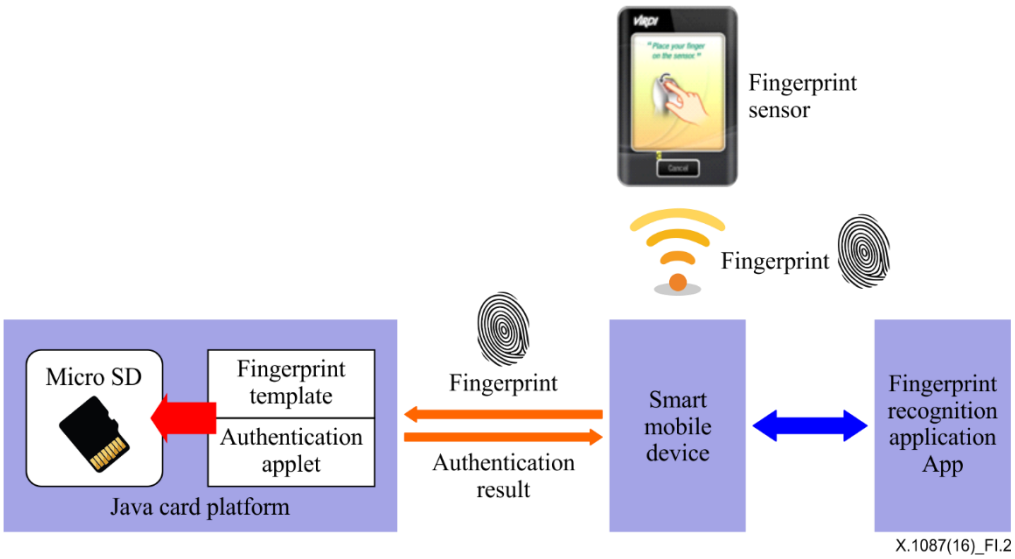

Figure I.2 – Components of the mobile telebiometrics application system

As a secure micro SD's SE maintains the same level of hardware security module, it is possible to save the biometric information to provide a convenient and a high level of security to perform personal authentication, and biometrics information of the mobile device. This is a method suitable for application to implement a solution for the deployment.

Appendix II

Mobile storage study for biometrics

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

This appendix specifies the technological requirements on how to acquire the biometric data for its application in the mobile devices. To perform enrolment, the biometric sample from the user is captured for biometric reference creation, then the user's information are uploaded to the card.

II.1 Off-card comparison

Off-card comparison means the biometric verification is performed on the biometric verification system side. The card acts as a storage device to store the biometric reference(s) of the user. Figure II.1 provides a schematic of the various steps in the process.

To perform verification, the biometric verification system will obtain access to the integrated circuit card (ICC) and read the user's biometric reference. The role of the biometric verification system is to capture the biometric sample and to perform biometric verification. If the biometric verification is successful, the biometric verification system will change its security status. This may include downloading further information from the card for a subsequent transaction. If unsuccessful, further access will be denied.

Cryptography is usually used to mutually authenticate the card and the biometric verification system. To protect the communication between the biometric verification system and the card, a secure channel should be established prior to the transfer of any template or data.

EXAMPLE: Consider a physical access system where the biometric reference and access code is stored on the ICC. The biometric verification system reads the biometric reference from the card, and performs biometric verification. In case of successful verification, it reads the access code from the card and sends it to the back end system that opens the door.

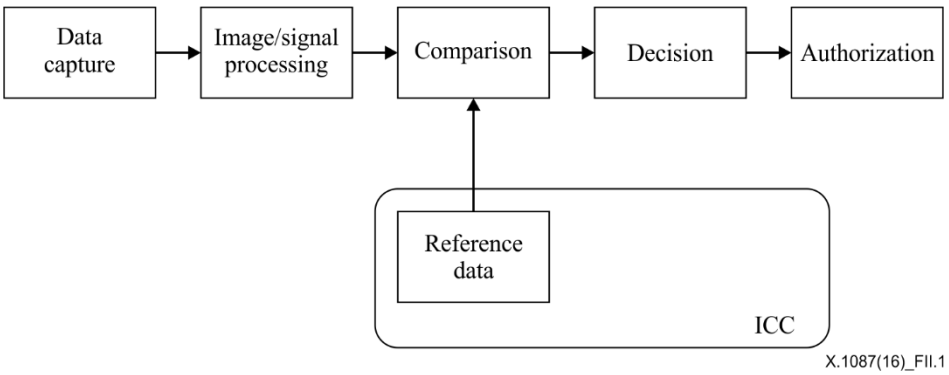

Figure II.1 – General architecture for biometric authentication using off-card matching

II.2 On-card comparison (sensor-off-card)

On-card comparison means the biometric sample verification is performed in the card. The process is schematically represented in Figure II.2. The ICC central processing unit (CPU) should have sufficient processing power to perform the matching. The enrolment process is the same as or similar to that for off-card matching.

To perform on-card comparison, the biometric verification system captures the biometric sample and extracts biometric data. The created biometric data is then uploaded to the card for verification. The verification process is executed on-card. If the biometric verification is successful the card's security state is updated and an appropriate signal sent to the back-end system. In order to protect the

communication between the biometric verification system and the card, a secure and trusted channel is recommended (using Secure Messaging according to [b-ISO/IEC 7816] and mechanisms defined by [b-ISO/IEC 24761] for distributed comparison verification).

EXAMPLE Consider a card with the ability to create digital signatures using a key that never leaves the card. A request sent to the card to initiate the creation of a digital signature receives a response message of security status error. This indicates to the user that verification is required. The user presents the required biometric sample to the biometric verification system for creation of biometric data, which is transmitted to the ICC. The ICC then compares the newly captured biometric data with the stored biometric reference, and in case of successful comparison, ICC updates the security status that subsequently allows the ICC to create digital signature upon receiving the corresponding application protocol data unit (APDU) commands.

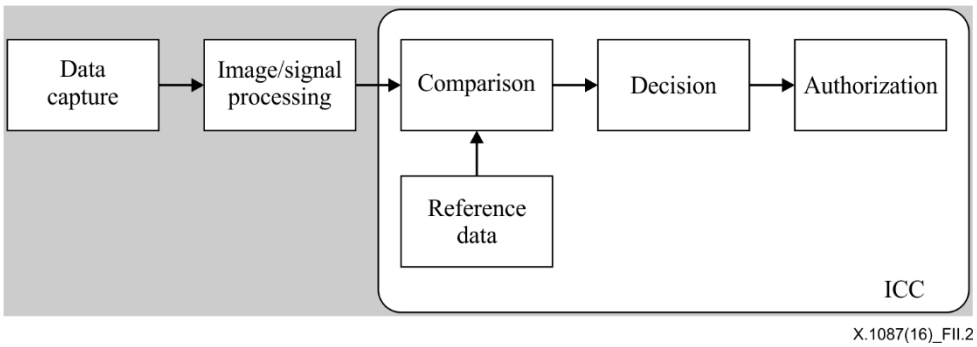

Figure II.2 – General architecture for biometric authentication using on-card matching

II.3 Work-sharing on-card comparison

Work-sharing on-card comparison is similar to on-card comparison except for the comparison procedure. The process is schematically represented in Figure II.3. This type of comparison is designed for an ICC that does not have sufficient processing capability to execute the biometric data comparison. In this case, certain activities that are computationally intensive, for example, a mathematical transformation, are sent to the biometric verification system to perform the calculation. The result of the computation is sent back to the ICC so that the final determination of the matching score is calculated on the card. During the pre-comparison calculation, communication takes place between the card and the biometric verification system. A secure and trusted channel is used to protect the communication between the terminal and the card unless the need for such protection is not explicitly required for a particular operational environment. The final comparison shall be performed in the card.

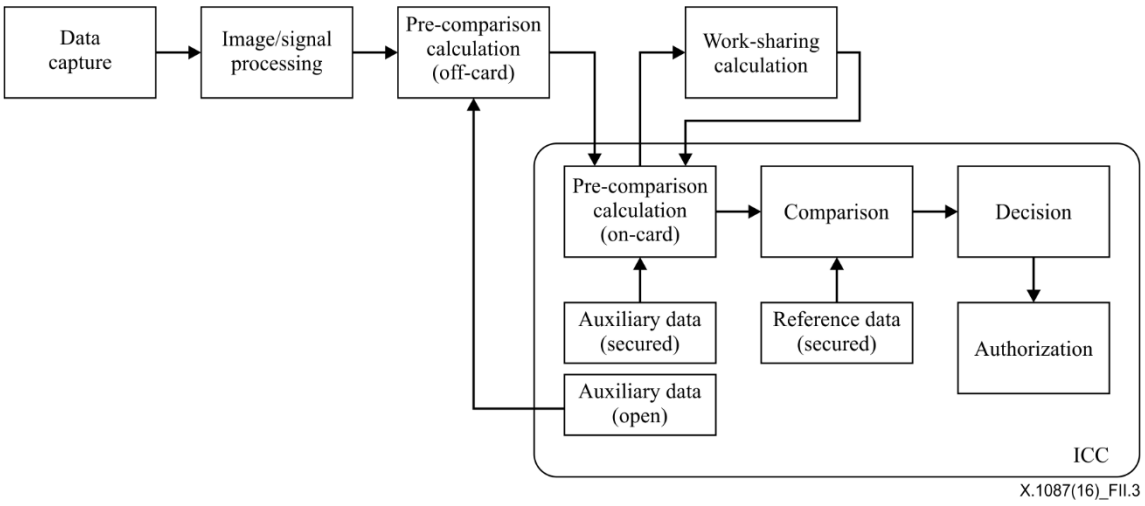

Figure II.3 – General architecture for biometric authentication using work-sharing

NOTE – Work-sharing on-card comparison should only be considered when, with the biometric modality used, the performances of the on-card comparison process are not good enough with regards to the required transaction time for a given application.

II.4 System-on-card comparison

System-on-card comparison means the whole biometric sample verification process is performed on the card. The process is schematically represented in Figure II.4. To perform sensor-on-card comparison, a sensor that is built into the card captures the biometric sample and extracts biometric data. The created biometric data is then used for verification. The verification process is executed on-card. The card's security state is updated once the card finishes the verification. No biometric sample or reference data is transferred to or from the card.

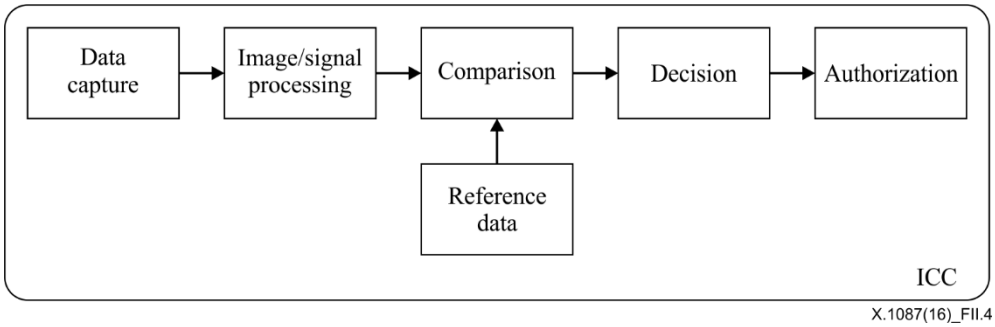

Figure II.4 – General architecture for biometric authentication using system-on-card matching

Appendix III

Use case study for mobile payment services

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

An analysis of the biometrics-based mobile payment environment through a case study on mobile payment environment utilizing biometrics was performed to establish security threats and countermeasures for payment system based on biometrics, such as Type A Pay and Type B Pay.

Those kinds of payment system are applied in model 10 of this Recommendation.

III.1 Type A Pay payment procedure

(Enrolment)

1 Activate payment App

2 Input payment card information (Add Card Menu)

3 Confirm the card enrolment

(Payment) App activation: Progress payment through point of sale (POS) tagging

1 Activate payment app

2 Choose the main card for payment

3 User authentication using fingerprint

4 Check for payment readiness status (blinking green light surrounding payment card)

5 Tagging card to POS (NFC and magnetic are both possible)

6 Confirm the payment information in Type A Pay App

III.2 Type B Pay payment procedure

1 Pay is opened on the smartphone.

2 The NFC tap connection is made between the NFC POS terminal and the smartphone.

3 The NFC POS terminal connects to Pay on the iPhone and selects the card information designated by the buyer. To clarify this point, the authors added, "The actual credit card number is not stored in the phone, rather it is stored as a device account number. During the transaction, that number is combined with a secure transaction code, and must be authorized via the fingerprint scanner on the iPhone 6. (On the iPhone 5, a PIN is used for approval)."

4 The Secure Element chip (part of the phone's NFC hardware) validates the transaction, and the user's authorization is transmitted to the NFC POS terminal.

5 Next, the purchase information moves through the merchant's system, and is forwarded to the acquiring bank.

6 The acquiring bank verifies the merchant and places the transaction data on the payment-processing network.

7 The payment processor (Visa, MasterCard, etc.) matches the transaction data (purchase information and device account number) to the buyer's credit card account.

8 The purchase is processed, and a verification transmitted back through the system to the POS device.

III.3 Type B Pay's built-in security

Put simply, using NFC and a different credit payment methodology made the entire process more secure. The differences are:

- No credit card information is exchanged.
- Each purchase requires a new transaction number.
- No card swiping eliminates bad-guy skimming technology and the infamous memory-scraping malware that afflicted so many Target shoppers.

Type B has potential security issues:

- User authentication: Type B Pay uses biometrics, a logical choice. Yet, it took just two days for attackers to bypass TouchID used on the iPhone 5.
- Validation of mobile application: Enter the user's credit card information into Passbook, by taking a picture or typing, to be a weak link. Malware installed on the iPhone could capture the data and send the information to remote servers under the attacker's control.

Type B Pay works using traditional device-based secure element. Type B does not store the real card or token data in their cloud servers at all. The on-device Secure Element essentially performs card-emulation in addition to secure storage. It sends payment data to the contactless terminal when you Tap & Pay.

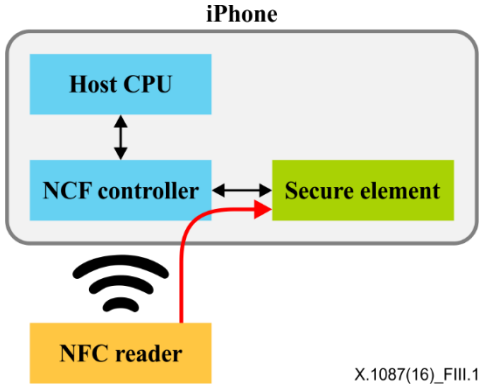

Figure III.1 – Access path for biometric data on mobile devices

First, Type B Pay does not store the real card data inside the SE. Instead, they store a token that conforms to EMVCo tokenization specification. It is this token (along with a cryptogram) that gets sent to the contactless terminal. During the authorization flow, the card network identifies the token, de-tokenizes them into real private access network (PAN) with the help of a token service provider (TSP) and sends the real PAN over to issuer for authorization.

Second, Type B owns and controls the secure element embedded inside the device thereby avoiding unnecessary challenges from the mobile network operators (MNOs).

Finally, Type B significantly simplified the provisioning model. If they had to provision the real card details, they would have to depend on a complex and convoluted process. Fortunately, they provision a token instead and took the opportunity to simplify the process to a bare minimum.

The fast identity on-line (FIDO) Alliance protocols use standard public key cryptography techniques to provide stronger authentication. During registration with an online service, the user's client device creates a new key pair. It retains the private key and registers the public key with the online service. Authentication is done by the client device proving possession of the private key to the service by signing a challenge. The client's private keys can be used only after they are unlocked locally on the device by the user. The local unlock is accomplished by a user-friendly and secure action such as

swiping a finger, entering a PIN, speaking into a microphone, inserting a second-factor device or pressing a button.

The FIDO protocols are designed from the ground up to protect user privacy. The protocols do not provide information that can be used by different online services to collaborate and track a user across the services. Biometric information, if used, never leaves the user's device. Registration process as below:

- User is prompted to choose an available FIDO authenticator that matches the online service's acceptance policy.
- User unlocks the FIDO authenticator using a fingerprint reader, a button on a second-factor device, securely-entered PIN or other method.
- User's device creates a new public/private key pair unique for the local device, online service and user's account.
- Public key is sent to the online service and associated with the user's account. The private key and any information about the local authentication method (such as biometric measurements or templates) never leave the local device.

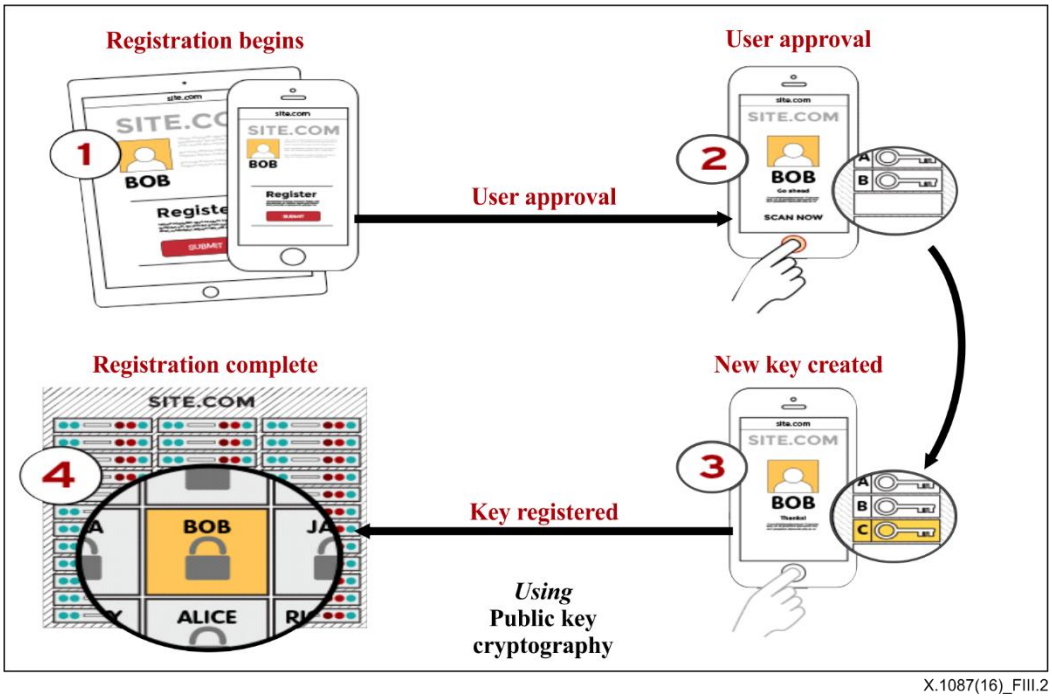

Figure III.2 – Registration process for FIDO

Login procedure is as below:

- Online service challenges the user to login with a previously registered device that matches the service's acceptance policy.
- User unlocks the FIDO authenticator using the same method as at Registration time.
- Device uses the user's account identifier provided by the service to select the correct key and sign the service's challenge.
- Client device sends the signed challenge back to the service, which verifies it with the stored public key and logs in the user.

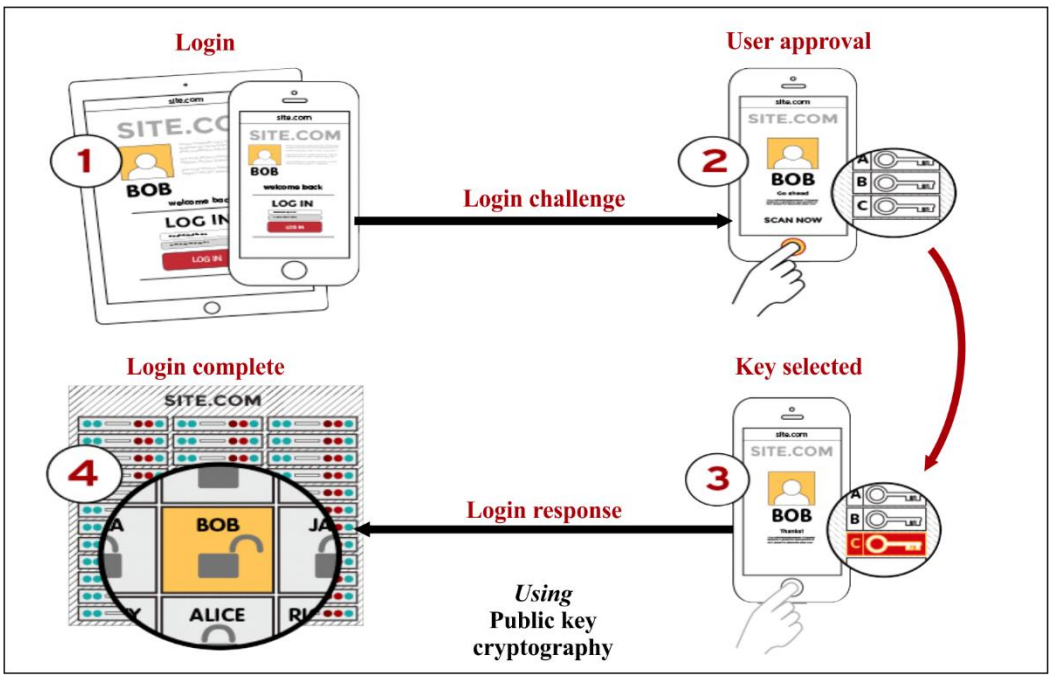

Figure III.3 – Login process for FIDO

Bibliography

[b-ITU-T X.1158] Recommendation ITU-T X.1158 (2014), *Multi-factor authentication mechanisms using a mobile device.*

[b-ISO/IEC 2382] ISO/IEC 2382:2015, *Information technology – Vocabulary*.

[b-ISO/IEC 2382-37] ISO/IEC 2382-37:2012, *Information technology – Vocabulary – Part 37: Biometrics*.

[b-ISO/IEC 7816-15] ISO/IEC 7816-15:2004, *Identification cards – Integrated circuit cards – Part 15: Cryptographic information application.*

[b-ISO/IEC 19784-1] ISO/IEC 19784-1:2006, *Information technology – Biometric application programming interface – Part 1: BioAPI specification*.

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

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, 2017