International Telecommunication Union

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

X.1279

(09/2020)

SERIES X: DATA NETWORKS, OPEN SYSTEM COMMUNICATIONS AND SECURITY

Cyberspace security – Identity management

Framework of enhanced authentication using telebiometrics with anti-spoofing detection mechanisms

Recommendation ITU-T X.1279

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
QUANTUM COMMUNICATION	
Terminologies	X.1700–X.1701
Quantum random number generator	X.1702–X.1709
Framework of QKDN security	X.1710–X.1711
Security design for QKDN	X.1712–X.1719
Security techniques for QKDN	X.1720–X.1729
DATA SECURITY	
Big Data Security	X.1750–X.1759
5G SECURITY	X.1800–X.1819

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

Recommendation ITU-T X.1279

Framework of enhanced authentication using telebiometrics with anti-spoofing detection mechanisms

Summary

Recommendation ITU-T X.1279 provides an architectural framework of enhanced authentication using telebiometrics with anti-spoofing detection. This Recommendation analyses threats to traditional telebiometric authentication solutions and specifies an architectural framework, authentication process flows and security considerations for enhanced authentication using telebiometrics with anti-spoofing detection mechanisms.

History

Edition	Recommendation	Approval	Study Group	Unique ID*
1.0	ITU-T X.1279	2020-09-03	17	11.1002/1000/14261

Keywords

Anti-spoofing detection, enhanced authentication, 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

Introduction

Telebiometric authentication technology is frequently used in various areas that require a high level of reliability such as e-banking and procurement services. Efforts must be made to develop a security system that can pre-emptively cope with potential security threats for the purpose of ensuring telebiometric data security.

This Recommendation analyses threats to traditional telebiometric authentication solutions and proposes a framework of enhanced authentication using telebiometrics with anti-spoofing detection (ASD). Anti-spoofing detection aims to determine that the user who sends the telebiometric authentication request is the active person who owns the biometric data. Anti-spoofing detection can be used together with telebiometric verification to enhance security and avoid fake biometric situations. Anti-spoofing detection functionality can be designed to enhance security and avoid the biometric data leakage.

Recommendation ITU-T X.1279

Framework of enhanced authentication using telebiometrics with anti-spoofing detection mechanisms

1 Scope

This Recommendation provides an architectural framework of enhanced authentication using telebiometrics with the capabilities of anti-spoofing detection. This Recommendation analyses threats to traditional telebiometric authentication solutions and specifies an architectural framework, authentication process flows and security considerations for enhanced authentication using telebiometrics with anti-spoofing detection mechanisms.

The architectural framework specified in this Recommendation can be used as guidance to help in the deployments of enhanced telebiometric authentication solutions using anti-spoofing detection functionalities.

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.1086] Recommendation ITU-T X.1086 (2008), *Telebiometrics protection procedures – Part 1: A guideline to technical and managerial countermeasures for biometric data security.*

[ITU-T X.1087] Recommendation ITU-T X.1087 (2016), *Technical and operational countermeasures for telebiometric applications using mobile devices*.

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

3 Definitions

3.1 Terms defined elsewhere

This Recommendation uses the following terms defined elsewhere:

3.1.1 authentication [b-ISO/IEC 2382-37]: The act of proving or showing to be of undisputed.

3.1.2 biometric (adjective) [b-ISO/IEC 2382]: Pertaining to the field of biometrics.

3.1.3 biometric capture [b-ISO/IEC 2382-37]: Obtain and record, in a retrievable form, signal(s) of biometric characteristic(s) directly from individual(s), or from representation(s) of biometric characteristic(s).

3.1.4 biometric characteristic [b-ISO/IEC 2382-37]: Biological and behavioural characteristic of an individual from which distinguishing, repeatable biometric features can be extracted for the purpose of biometric recognition.

3.1.5 biometric data [b-ISO/IEC 2382-37]: Biometric sample or aggregation of biometric samples at any stage of processing, e.g., biometric reference, biometric probe, biometric feature r biometric property.

3.1.6 biometric feature [b-ISO/IEC 2382-37]: Numbers or labels extracted from biometric samples and used for comparison.

3.1.7 biometric recognition/biometrics [b-ISO/IEC 2382-37]: Automated recognition of individuals based on their biological and behavioral characteristics.

3.1.8 biometric reference database [b-ISO/IEC 2382-37]: Database of biometric reference data records.

3.1.9 biometric template [b-ISO/IEC 19784-1]: Set of stored biometric features comparable directly to biometric features of a recognition biometric sample.

3.1.10 biometric verification [b-ISO/IEC 2382-37]: Process of confirming a biometric claim through biometric comparison.

3.1.11 comparison (match/matching) [b-ISO/IEC 19784-1]: Estimation, calculation or measurement of similarity or dissimilarity between recognition biometric sample(s)/biometric features/biometric models and biometric reference(s).

3.1.12 comparison decision [b-ISO/IEC 19784-1]: Determination of whether the recognition biometric sample(s) and biometric reference(s) have the same biometric source, based on a comparison score(s), a decision policy(ies) including a threshold, and possibly other inputs.

3.1.13 mobile device [b-ISO 18461]: portable computing device, typically having a display screen with touch, pen and/or keyboard input and Internet connection.

3.1.14 user [b-ISO/IEC 2382-37]: Any person or organization interacting in any way with a biometric system.

3.1.15 telebiometrics [b-ITU-T X.1081]: The application of biometrics to telecommunications.

3.2 Terms defined in this Recommendation

This Recommendation defines the following terms:

3.2.1 anti-spoofing detection: A process of detecting and preventing spoofing of a biometric system through illegitimate actions.

3.2.2 obfuscation: A deliberate act of creating source or machine code that is difficult for humans to understand. This technique relies on a collection of transformations that change the apparent operation of the software without changing the results. An obfuscated program should produce exactly the same results as a non-obfuscated program.

NOTE – Obfuscation is a technique that is normally used to hide the meaning of some software by rearranging the operations, but it can also be used to add weak watermarks to the code. In both cases, the algorithms rely on a collection of transformations that change the apparent operation of the software without changing the results. An obfuscated program should produce exactly the same results as a non-obfuscated program. [b-Disappearing Cryptography]

3.2.3 quality detection: A measure of fitness of a biometric sample to accomplish or fulfil the biometric comparison decision.

3.2.4 spoofing: The pretense assumed by an entity to be a different entity, by presenting a recorded image or other biometric data sample, or an artificially derived biometric characteristic, in order to impersonate an individual.

NOTE – This definition has been adapted from [b-ITU M.3016.0].

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms

ASD Anti-Spoofing Detection

PII Personally Identifiable Information

PKI Public Key Infrastructure

SMS Short Messaging Service

SRP Secure Remote Password

5 Conventions

None.

6 Security threats to telebiometric authentication and countermeasures

6.1 Background

With the emergence of Internet services, authentication mechanisms based on traditional password can no longer satisfy requirements of user experiences and security capabilities; telebiometric authentication mechanisms are more commonly used now for reasons of convenience and security.

However there are challenges and risks in biometric authentication mechanisms, for example, attackers may use a photo, or a computer generated picture, or a face in the screen for facial recognition authentication, or a user may use a copy of a telebiometric sample (e.g., a fingerprint, iris or voiceprint) for telebiometric authentication.

6.2 Reference authentication modes

For telebiometric authentication on mobile devices, there are two basic reference authentication modes:

1) Local authentication mode: The biometric data is stored on a mobile device and telebiometric verification is done on the mobile device side. The telebiometric verification result is sent to the server side.
2) Remote authentication mode: The biometric data is stored on the server and telebiometric verification is done on the server side.

This Recommendation focuses on remote authentication mode.

6.3 Security threats

6.3.1 Security threats on the client side

Telebiometric authentication encounters the following security threats on the client side:

– The client is a faked agent or is modified with malicious code.
– Attackers try to disrupt the availability and integrity of the client.
– Attackers try to steal or modify the captured biometric data of the client.
– Attackers may use a photo, or a computer-generated picture, or a face in the screen for facial recognition authentication.
– Attackers may use a copy of biometric data (e.g., fingerprint, iris or voiceprint) for telebiometric authentication.

6.3.2 Security threats on the server side

Telebiometric authentication encounters the following security threats on the server side:

– Attackers may intrude on the server to disrupt the server database or server application.

– Captured biometric data or template data may be replaced illegally or leaked, as altered or stolen data.

– Captured biometric data or template data may be altered illegally, when the captured data is transferred.

– An illegal comparison program may be used.

6.3.3 Security threats to the transmission channel between client and server

Telebiometric authentication has the following security threats to the transmission channel between client and server:

– Attacks may eavesdrop or modify the messages between client and server.

– The biometric data may be stolen or modified during the transmission from the client to the server.

6.4 Countermeasures

To mitigate these threats to telebiometric authentication, anti-spoofing detection (ASD) is usually used together with telebiometric verification for authentication.

ASD should be implemented in a telebiometric authentication framework. ASD functionality can be used to determine that the user who sends the telebiometric authentication request is the active person who owns the biometric data. This can avoid the situation where an illegal user may use fake or copied biometric data for telebiometric authentication.

ASD can be used together with telebiometric verification to enhance security and avoid fake biometric situations. For example, a mobile application may ask the user to nod, shake heads, blink, open mouth, etc., to validate that the user is the actual person who made the authentication request.

Additional security threats and countermeasures are provided in [ITU-T X.1086] and [ITU-T X.1087].

7 Architectural framework

7.1 Architectural diagram

The architectural diagram of enhanced authentication using telebiometrics with ASD mechanisms is shown in Figure 1.

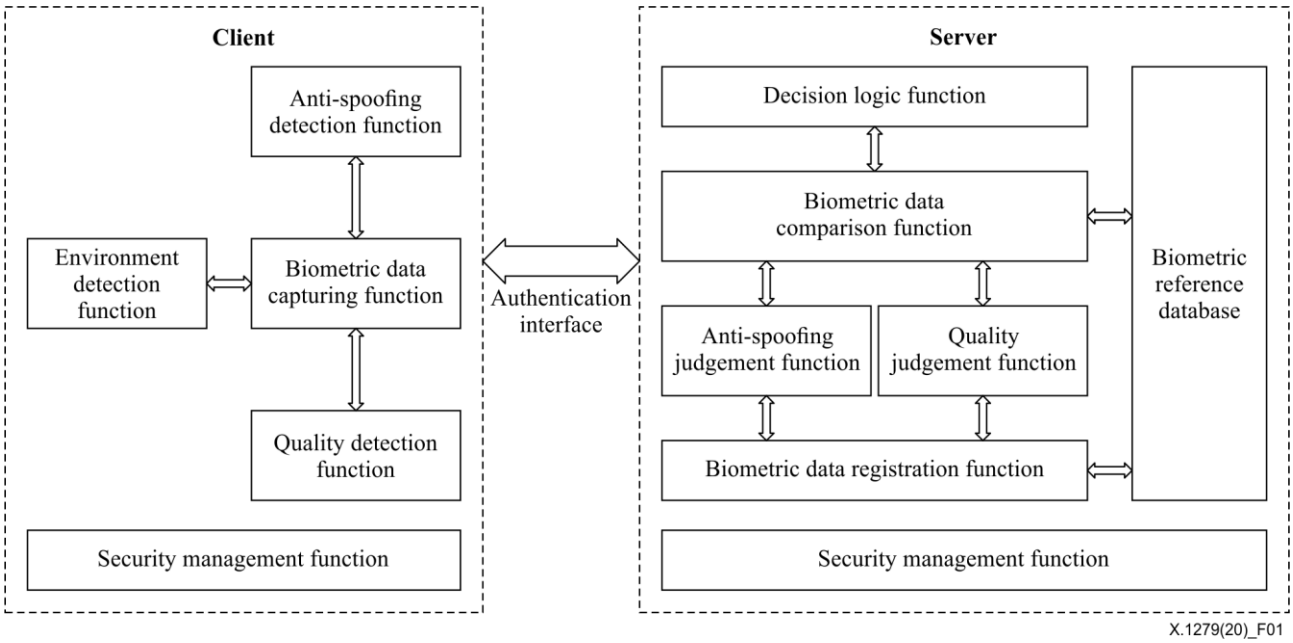

Figure 1 – Architectural diagram of enhanced authentication using telebiometrics with ASD mechanisms

The detailed description of functions in this architectural diagram is given in clauses 7.2 and 7.3.

7.2 Client side functionalities

7.2.1 Environment detection function

This function is responsible for recognizing and detecting the biometric characteristics and environment conditions. For example, it judges whether or not the facial characteristics satisfy collection conditions, whether or not the environment satisfies data collection conditions.

7.2.2 Biometric data capturing function

This function is used to capture end users' biometric data and then send the biometric data to a local quality detection function and ASD function for processing, and after that send the biometric data to the server through authentication interface for remote authentication.

7.2.3 ASD detection function

This function is used to detect the expected movements according to the server's strategies or policies, such as nodding, shaking heads, blinking, opening mouth, etc.

Although many methods can be used for ASD, liveness detection is much more suitable for telebiometric authentication on mobile devices. Challenge-response can be used as a tool for determining if a subject's presentation has liveness properties exhibited in the biometric data capture subsystem's acquisition. For example, the live human iris is expected to respond to changes in visible light illumination (the challenge) with changes in pupil size (the expected response if alive).

Liveness detection may be performed in the following steps that are similar to the biometric recognition processes:

– capture raw data for ASD from a subject using the biometric data capture subsystem,

– extract features from the ASD data, and

– compare the ASD features with the criteria.

7.2.4 Quality detection function

This function is used to preliminarily judge the quality of the biometric data according to the server's strategies or policies. The quality detection function performs quality evaluation on the collected biometric data, and extracts the biometric characteristics. Usually, this function is used together with the ASD function and biometric data capturing function, to output the best biometric data for biometric data modeling and judgment.

7.2.5 Security management function

The security management function on the client side is responsible for credential management, trusted environment, etc.

7.3 Server side functionalities

7.3.1 Biometric data registration function

This function is responsible for handling biometric data registration. Biometric data registration can be collected from a client, batch imported directly or collected from other channels such as a national identity database. This can be achieved from a biometric data registration template.

7.3.2 Anti-spoofing judgement function

This function is used to judge if the biometric data is fake or copied. The server will perform deep anti-spoofing judgement based on the preliminary detection result from client side and the server's strategies and policies.

The server can indicate the client to detect the expected movements according to the server's strategies or policies, such as nodding, shaking heads, blinking, opening mouth, etc. The server receives the extracted biometric characteristic data from the client, and uses its biometric reference and the pre-defined strategy to judge if a subject's presentation has liveness properties.

7.3.3 Quality judgement function

This function is used to judge the quality of the biometric data based on the preliminary detection result from client side and the server's strategies and policies. The quality judgment function performs a quality evaluation on the received biometric data. If the quality does not reach the required threshold, the server will reject the received biometric data and ask the client to capture the biometric data again. If the quality matches the required threshold, the biometric data will be sent to the biometric data comparison function to compare.

Biometric data capturing capability may be different for different device types. The quality of biometric data can be improved based on different device types. The server may ask the user to use multiple devices to capture the biometric data to improve the quality. If the biometric reference is captured from different device types, the server should store and use the different biometric references for different device types.

7.3.4 Biometric data comparison function

This function supports the comparison and verification between extracted biometric features from a client and biometric references stored on the server side. The biometric references stored in a biometric reference database are generated from the biometric data registration process.

7.3.5 Decision logic function

This function contains decision logics to run different authentication processes and feedback the related instructions to the client to execute the different authentication processes. The decision is made based on the risk management data, including software and hardware information of the mobile device and the user's profile. For example, according to data analysis, if the end user is high risk, a

decision logic function asks the client to execute ASD in addition to the basic biometric capture and comparison.

7.3.6 Biometric reference database

Biometric reference database is used to store biometric data, risk management data, user name, identity, etc.

7.3.7 Security management function

This function is used to guarantee the secure execution of the server functionalities and the secure storage of the biometric reference database, to avoid tampering or theft of the biometric data or template.

8 Authentication process flows

8.1 Message types

In the protocol stack of telebiometric authentication on mobile devices, there are at least three types of messages in different stages:

– Registration: a server records a user's registration information and authentication type according to a negotiation between the user and the server.

– Authentication: a server compares a received biometric data against a registered biometric reference;

– Deregistration: a user deregisters from a server. The server deletes the registration data of the user.

NOTE – This Recommendation focuses on remote verification. The client registers a biometric reference to the server. After receiving the verification request, the server compares the received biometric data against registered biometric reference.

8.2 Process flows

8.2.1 Registration process flows

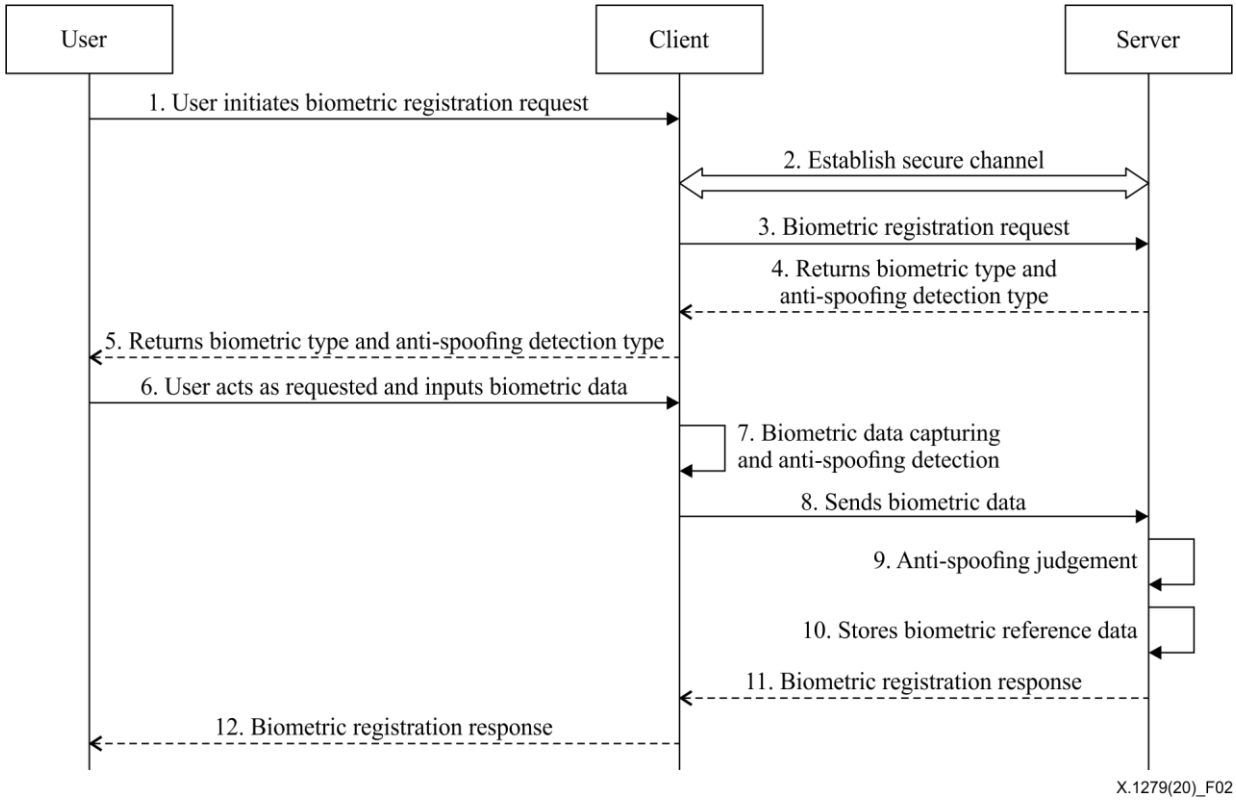

Figure 2 – Registration process flows

Figure 2 shows the registration process flows. The detailed flows are described below:

Pre-condition: The user authenticates with the server successfully through other authentication mechanisms, e.g., user account identifier/password, and short messaging service (SMS) verification code.

1. User uses account identifier/password to log in and initiates biometric registration request to the client;
2. Client establishes a secure channel with the server to protect the session and data transmission, for example, by using secure remote password (SRP) protocol;
3. Client sends biometric registration request together with user account identifier and risk management data to the server;
4. Decision logic function in the server returns the right biometric type and ASD type to the client based on the analysis of risk management data and business logic;
5. Client asks user to perform the specified actions to capture biometric data;
6. User acts as requested and inputs biometric data from the client;
7. Biometric data capturing function in the client captures the biometric data, and ASD detects the expected movements of user;
8. Client extracts biometric features and sends the features to the server as a biometric reference in the established secure channel;
9. Server binds the biometric data with the user account identifier, and performs ASD;
10. Server stores the received biometric reference in the biometric reference database;
11. Server returns biometric registration results to the client;
12. Client informs user the biometric registration result.

8.2.2 Authentication process flows

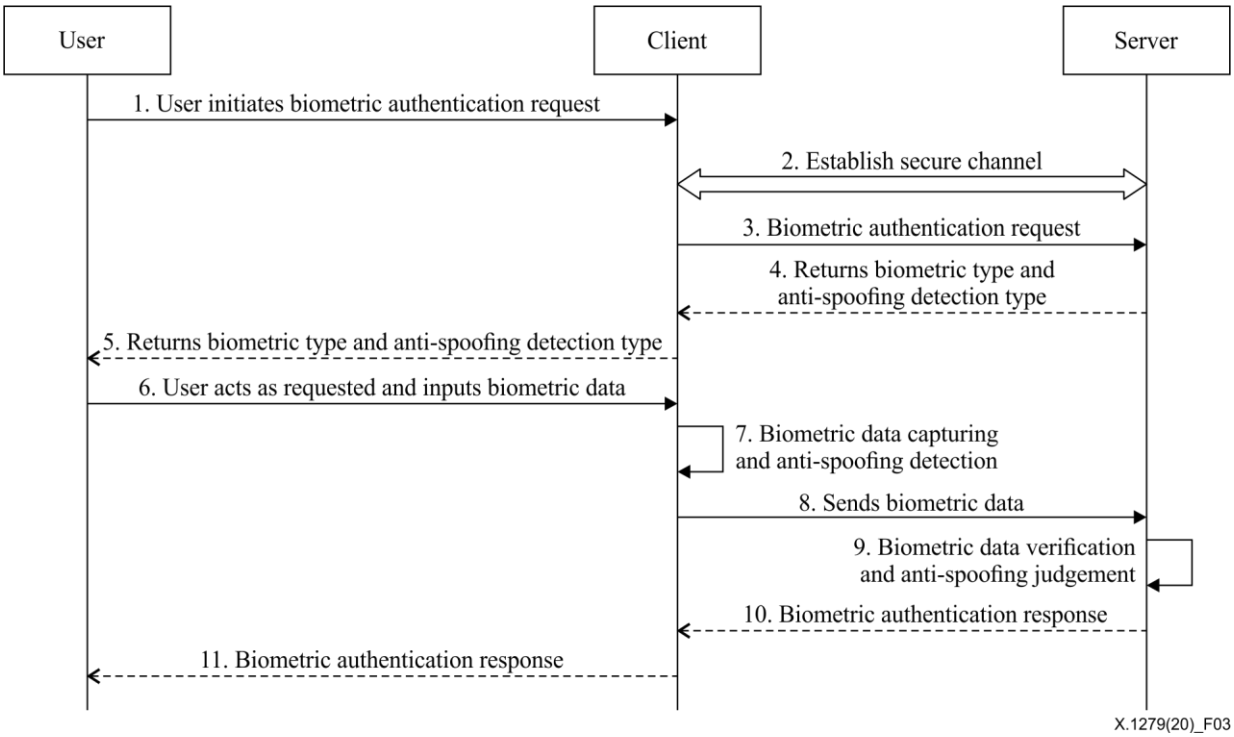

Figure 3 – Authentication process flows

Figure 3 shows the authentication process flows. The detailed flows are described below:

1. User initiates biometric authentication request to the client, together with the user account identifier;
2. Client establishes a secure channel with the server to protect the session and data transmission, for example, by using secure remote password (SRP) protocol;
3. Client sends biometric authentication request together with the user account identifier and risk management data to the server;
4. Decision logic function in the server returns the right biometric type and ASD type to the client based on the analysis of risk management data and business logic;
5. Client asks user to perform the specified actions to capture biometric data;
6. User acts as requested and inputs biometric data from the client;
7. Biometric data capturing function in the client captures the biometric data, and ASD function detects the expected movements of user;
8. Client sends extracted biometric feature data to the server in the established secure channel;
9. Server makes biometric data verification between the extracted biometric feature and biometric reference, and performs ASD;
10. Server returns biometric authentication result to the client;
11. Client informs user of the biometric authentication result.

8.2.3 Deregistration process flows

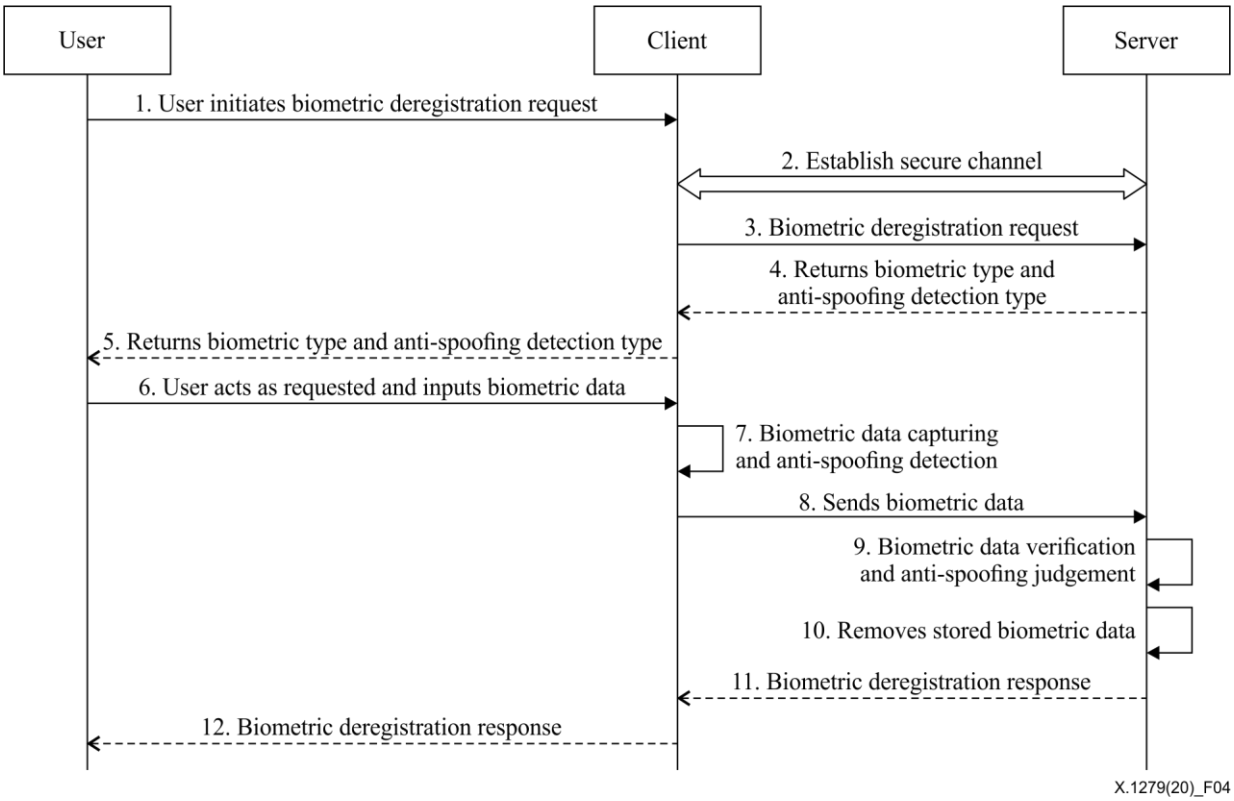

Figure 4 – Deregistration process flows

Figure 4 shows the deregistration process flows. The detailed flows are described below:

Pre-condition: user authenticates with server successfully through other authentication mechanisms, e.g., user account identifier/password, and SMS verification code.

1. User uses account identifier/password to log in and initiates biometric deregistration request to the client;
2. Client establishes a secure channel with the server to protect the session and data transmission, for example, by using SRP protocol;
3. Client sends biometric deregistration request together with user account identifier and risk management data to the server;
4. Decision logic function in the server returns the right biometric type and ASD type to the client based on the analysis of risk management data and business logic;
5. Client asks user to perform the specified actions to capture biometric data;
6. User acts as requested and inputs biometric data from the client;
7. Biometric data capturing function in the client captures the biometric data, and ASD function detects the expected movements of user;
8. Client sends extracted biometric feature data to the server in the established secure channel;
9. Server makes biometric data verification between the extracted biometric feature and stored biometric reference, and performs ASD;
10. Server removes user's biometric reference from the biometric reference database;
11. Server sends biometric deregistration result to the client;
12. Client informs user of biometric deregistration result.

9 Security guidelines

9.1 Client security

The mobile device operating system should be updated to the latest secure version in time.

The client should be signed to identify the source of client.

The client should be protected against unauthorized modification or update.

Code and data protection should be enhanced against reverse engineering in the client, e.g., obfuscation.

The data acquisition in the client should be implemented in a trusted environment to ensure the confidentiality and integrity of the collected data.

9.2 Server security

Strict access control policy should be implemented in the server, any operation to the server should be authenticated and authorized first.

The server should have the ability to identify the identity of the client.

The communication between server and client should be protected against reply attack, e.g., using dynamic data in messages such as nonce, challenge or timestamp.

Logs should be maintained for the operations on the server, and the integrity of logs should be protected.

9.3 Storage security

ITU-T X.509 certificates and private keys should be stored securely, and a strict access control policy should be set.

Private keys should be stored in cipher text, and the encryption algorithm should be at a high security level to prevent cracking.

Biometric data stored in the server should be encrypted, and the encryption algorithm should be at a high security level to prevent cracking.

Biometric data stored in the server should be an extracted biometric feature, and cannot be restored to the original data.

More details of storage security should conform to the requirements in [ISO/IEC 24745].

9.4 Communication security

Before any communication between the client and server, a secure channel should be established, e.g., https is suitable for the purposes of communication security.

The mechanism of secure key exchange in the authentication between client and server should be provided, e.g., SRP can be used as the mechanism of secure key exchange.

The key used for negotiating the secure channel should be prevented from being intercepted, e.g., SRP can be used to negotiate the secure channel without key transportation.

The information such as processed biometric data and the result of the decision component should be encoded for transmission, and their integrity should be verified by a one-way function, such as a hash function or the public key infrastructure (PKI), which prohibits any alteration of the data during transmission.

Processed biometric data should be desensitized and encrypted for transmission, and the encryption key should be different with a different client, the server uses the matched decryption key to decrypt.

More details of communication security should conform to the requirements in [ISO/IEC 24745].

9.5 Other security considerations

Besides storage security and communication security, there are many other aspects of security that need to be considered, such as processing security, personally identifiable information (PII) protection and so on. More details of security techniques of biometric information protection should conform to the requirements in [ISO/IEC 24745].

Appendix I

Use cases and scenarios

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

I.1 Use case study for mobile payment services

Alice is a user who uses an application called ‘mobile wallet’ for mobile payments. The procedure is described as follows:

1) At the first time, Alice uses her username and password to log onto the mobile wallet application. She does not want to have to input her password every time she makes a payment, and also she is afraid of forgetting her password. So she clicks a button "Facial verification payment registration" in the mobile wallet application.
2) The mobile wallet application asks Alice to open the camera, and nod in the camera.
3) Alice receives a notice from the mobile wallet application: "You have registered successfully".
4) Alice buys a cup of coffee in Starbuck's shop, and uses the mobile wallet application to pay. Alice opens the mobile wallet application, and gets ready to pay. The mobile application asks Alice to open the camera and nod in the camera. Alice quite enjoys this experience.
5) Alice gets notification from mobile wallet application: "You have paid successfully, thank you!".
6) After some time, Alice no longer wants to use this function anymore and so she clicks a button to close this payment method option.

I.2 Use case study for e-commerce services

Bob owns a shop selling clothes and he wants to open an online shop on an e-commerce platform. The procedure is described as follows:

1) At the first time, Bob registers himself on the e-commerce platform and applies to open a new shop. Bob sets his username and password on the e-commerce platform from an e-commerce application on his mobile device.
2) The e-commerce application on his mobile device asks Bob to open the camera and perform several actions in sequence, e.g., open mouth, shake head, blink eyes and nod in the camera.
3) Bob receives a notice from the e-commerce mobile application: "You have registered successfully".
4) After some time, Bob wants to publish some clothes from his shop. The e-commerce platform asks Bob to open the camera, and perform several actions in sequence, e.g., shake head, blink eyes, open mouth and nod in the camera.
5) Bob gets notification from the e-commerce platform: "You have logged in successfully."
6) After some time, Bob does not want to use this function again, and he clicks a button to close this authentication option.

Appendix II

Secure remote password (SRP)

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

SRP is a password-based identity authentication and key exchange protocol. The advantage of SRP is that the key plaintext is not a transfer phenomenon in the process of authentication, users only need to hold the password. In addition, the server does not store users' passwords, but does store the relevant information, even if the server is captured by an adversary; the adversary cannot forge a legitimate client (as the password cannot be obtained).

The details of SRP protocol can be found in [b-RFC 2945].

The SRP protocol can be used to establish secure channels between client and server in the biometric registration process, biometric authentication process and biometric deregistration process. SRP protocol can be used to negotiate secure connections using a user-supplied password, while eliminating the security problems traditionally associated with reusable passwords. SRP protocol can also be used to perform a secure key exchange in the authentication process, allowing security layers (privacy and/or integrity protection) to be enabled during the session.

Appendix III

Examples of how a server performs ASD in face recognition

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

Examples of how a server performs ASD in face recognition include but not limited to:

1) Following some hints or instructions from the server, the user can perform a specified action and the server detects the action from the face image.
2) The server should have the ability to detect the angle of face and camera, and detect the living body through the change of the face angle in the process.
3) The server should have the ability to detect the continuity of face action, prevent slide play and prevent people from changing in the process.
4) The server should have the ability to detect the replay of the face action video.
5) The server should have the ability to prevent face picture attack.
6) The server should have the ability to detect the use of 3D face models produced by computer graphics technology.

Bibliography

[b-ITU-T M.3016.0] Recommendation ITU-T M.3016.0 (2005), *Security for the management plane: Overview.*

[b-ITU-T X.509] Recommendation ITU-T X.509 (2019), *Information technology – Open Systems Interconnection – The Directory: Public-key and attribute certificate frameworks.*

[b-ITU-T X.1081] Recommendation ITU-T X.1081 (2011), *The telebiometric multimodal model - A framework for the specification of security and safety aspects of telebiometrics*.

[b-ITU-T X.1085] Recommendation ITU-T X.1085 (2016) | ISO/IEC 17922:2017, *Information technology - Security techniques – Telebiometric authentication framework using biometric hardware security module.*

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

[b-ITU-T X.1252] Recommendation ITU-T X.1252 (2010), *Baseline identity management terms and definitions.*

[b-ITU-T X.1254] Recommendation ITU-T X.1254 (2012), *Entity authentication assurance framework.*

[b-ISO 18461] ISO 18461:2016, *International museum statistics.*

[b-ISO/IEC 19784-1] ISO/IEC 19784-1:2018, *Information technology –Biometric application programming interface – Part 1: BioAPI specification*

[b-ISO/IEC 19792] ISO/IEC 19792:2009, *Security evaluation of biometrics.*

[b-ISO/IEC 19989] ISO/IEC 19989, *Evaluation of presentation attack detection for biometrics.*

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

[b-ISO/IEC 2382-37] ISO/IEC 2382-37:2017, *Information technology – Vocabulary – Part 37: Biometrics*

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

[b-ISO/IEC 30107] ISO/IEC 30107:2017, *Information technology – Biometric presentation attack detection.*

[b-ISO/IEC 30125] ISO/IEC 30125:2016, *Biometrics – Biometrics used with mobile devices.*

[b-RFC 2945] RFC 2945, *The SRP Authentication and Key Exchange System*

[b-Disappearing Cryptography] Disappearing Cryptography (Third Edition), 2009, Pages 355-364.

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, 2020