International Telecommunication Union

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

X.1158

(11/2014)

SERIES X: DATA NETWORKS, OPEN SYSTEM COMMUNICATIONS AND SECURITY

Secure applications and services – Security protocols

Multi-factor authentication mechanisms using a mobile device

Recommendation ITU-T X.1158

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.1158

Multi-factor authentication mechanisms using a mobile device

Summary

With the wide use of mobile devices, the number of business transactions carried out through these devices is dramatically increasing. However, there are many weaknesses to single-factor authentication when used in the mobile context requiring strong authentication mechanisms to meet requirements for security and convenience. As such, there is a strong need to develop multi-factor authentication mechanisms that are applicable to the mobile context.

Recommendation ITU-T X.1158 provides multi-factor authentication mechanisms using a mobile device. This Recommendation describes the weaknesses of single-factor authentication mechanisms, the need for multi-factor authentication mechanisms, the various combinations of multi-factor authentication mechanisms using a mobile device and the threats for two-factor authentication mechanisms. In addition, security requirements to reduce the threats of single-factor authentication are provided, including potential typical multi-factor authentication mechanisms. This Recommendation assumes the use of a mobile device with subscriber identity module (SIM) card capability, but should not exclude the use of virtual SIM cards. Specifically, this Recommendation is applicable to all applications using mobile devices. This Recommendation is based on the framework described in Recommendation ITU-T X.1154.

History

Edition	Recommendation	Approval	Study Group	Unique ID*
1.0	ITU-T X.1158	2014-11-13	17	11.1002/1000/12341

Keywords

Authentication, authentication factor, mobile device, multi-factor authentication, two-factor authentication.

---

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

FOREWORD

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

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

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

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

NOTE

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

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

INTELLECTUAL PROPERTY RIGHTS

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

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

Table of Contents

Recommendation ITU-T X.1158

Multi-factor authentication mechanisms using a mobile device

1 Scope

This Recommendation provides multi-factor authentication mechanisms using a mobile device. It describes the weakness of a single-factor authentication mechanism, identifies the need for multi-factor authentication, and provides various combinations of multi-factor authentication mechanisms using a mobile device. General security requirements to reduce the threats associated with a single-factor authentication mechanism are provided. In addition, typical multi-factor authentication protocols are given. This Recommendation assumes the use of mobile devices with subscriber identity module (SIM) card capability, but should not exclude the use of virtual SIM card capability. Specifically, this Recommendation is applicable to all applications using mobile devices. This Recommendation is based on the framework described in [ITU-T X.1154].

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 published regularly. A reference to a document within this Recommendation does not give it, as a stand-alone document, the status of a Recommendation.

[ITU-T X.1154] Recommendation ITU-T X.1154 (2013), *General framework of combined authentication on multiple identity service provider environments*.

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

3 Definitions

3.1 Terms defined elsewhere

This Recommendation uses the following terms defined elsewhere:

3.1.1 authentication factor [ITU-T X.1154]: A type of credential; there are three types of authentication factors: ownership factor, knowledge factor and biometric factor.

3.1.2 authentication protocol [ITU-T X.1254]: A defined sequence of messages between an entity and a verifier that enables the verifier to corroborate the entity's identity.

3.1.3 credential [b-ITU-T X.1252]: Set of data presented as evidence of a claimed identity and/or entitlements.

3.1.4 entity authentication assurance (EAA) [ITU-T X.1254]: A degree of confidence reached in the authentication process that the entity is what it is, or is expected to be (this definition is based on the 'authentication assurance' definition given in [b-ITU-T X.1252]).

3.1.5 man-in-the-middle attack [ITU-T X.1254]: Attack in which an attacker is able to read, insert, and modify messages between two parties without their knowledge.

3.1.6 multi-factor authentication [b-ISO/IEC 19790]: Authentication with at least two independent authentication factors.

3.1.7 verifier [b-ITU-T X.1252]: An entity that verifies and validates identity information.

3.2 Terms defined in this Recommendation

This Recommendation defines the following terms:

3.2.1 mobile device: 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.

3.2.2 secure element (SE): A dedicated microprocessor system that contains an operating system, memory, application environment and security protocols intended to be used to store sensitive data and execute sensitive applications.

NOTE – A secure element may reside in a universal subscriber identity module (USIM), a dedicated chip in a phone's motherboard, an external plug in a memory card or as an integrated circuit card.

3.2.3 subscriber identity module (SIM): An integrated chip used mostly in mobile device that operate in the global system for mobile communications (GSM) network.

NOTE – It securely stores the international mobile subscriber identity (IMSI) and the related key used to identify and authenticate subscribers in mobile telephony devices.

3.2.4 verify: Check information by comparing the provided information with previously corroborated information and the binding to the entity.

3.2.5 virtual subscriber identity module (SIM) card: A software application that emulates a SIM card in a mobile device, which does not require a physical SIM card.

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations:

ATM	Automated Teller Machine
CA	Certification Authority
DNA	Deoxyribonucleic Acid
DoS	Denial of Service
EAA	Entity Authentication Assurance
GSM	Global System for Mobile communications
HSM	Hardware Security Module
HTTP	Hypertext Transfer Protocol
IC	Integrated Circuit
IMSI	International Mobile Subscriber Identity
IT	Information Technology
LAN	Local Area Network
MAC	Media Access Control
NFC	Near Field Communication
OOB	Out Of Band
OSP	One-time password Service Provider
OTP	One-Time Password
PC	Personal Computer
PIN	Personal Identification Number

PKI Public Key Infrastructure

RP Relying Party

SE Secure Element

SIM Subscriber Identity Module

SMS Short Message Service

TAN Transaction Authentication Number

TEE Trusted Execution Environment

TPM Trusted Platform Module

USIM Universal Subscriber Identity Module

WiFi Wireless Fidelity

5 Conventions

In this Recommendation:

The keywords "is required to" indicate a requirement which must be strictly followed and from which no deviation is permitted, if conformance to this Recommendation is to be claimed.

The keywords "is recommended" indicate a requirement which is recommended but which is not absolutely required. Thus, this requirement need not be present to claim conformance.

The keywords "is prohibited from" indicate a requirement which must be strictly followed and from which no deviation is permitted, if conformance to this Recommendation is to be claimed.

The keywords "can optionally" indicate an optional requirement which is permissible, without implying any sense of being recommended. This term is not intended to imply that the vendor's implementation must provide the option, and the feature can be optionally enabled by the network operator/service provider. Rather, it means the vendor may optionally provide the feature and still claim conformance with this Recommendation.

6 Overview of multi-factor authentication

6.1 Single-factor authentication

A single-factor authentication is a typical authentication that requires, for example, a user name and password before granting access to the user. Table 1 illustrates typical examples of a single-factor authentication [ITU-T X.1254].

Table 1 – Typical single-factor authentication

Authentication factor	Examples
Something an entity knows (Knowledge factor)	Password, personal identification number (PIN), passphrase, mother's name, phone number.
Something an entity has (Possession factor)	Smart cards, tokens, one-time password (OTP), driver's license, public key infrastructure (PKI) certificate.
Something an entity is (Inherence factor)	Fingerprints, hand geometry, facial image, iris, retina, deoxyribonucleic acid (DNA), voice, signature patterns.
Something an entity does (Behaviour factor)	Behavioural pattern, speed of key input.

In addition, there is location-based authentication, which is used with dial-up remote access as an additional authentication mechanism. For example, it is assumed that an employee can be authorized to work at home using a remote access connection to connect to her office-based resources. The remote access server can be configured such that when the employee calls in and authenticates, the server calls back to the employee's computer at home.

As long as the employee attempts to connect from her home computer, this connection will work. However, if an attacker attempts to impersonate an employee using her username and password, the attacker cannot connect.

6.2 Two-factor authentication

Two-factor authentication is a process that confirms a user's identity using two distinctive factors: something they have and something they know. The two-factor authentication uses a mechanism that implements two authentication factors; it is therefore considered stronger and more secure than the traditionally implemented one-factor authentication system.

Two-factor authentication can provide a significant increase in the security of the authentication system. With two-factor authentication, a password or PIN can be used in conjunction with the use of tokens, smart cards or even biometrics. The combination of multiple factors ensures companies about the authenticity of the users accessing secure systems of an organization.

Two-factor authentication has been introduced to meet the demands of organizations to provide stronger authentication options for their users. In most cases, a hardware token, e.g., an OTP token or a mobile phone, is given to each user for each account. The increasing number of carried tokens and the cost of manufacturing and maintaining them is becoming a burden to both the user and the organization. Today, since many users carry mobile phones at all times, an alternative is to install all the software tokens in the mobile phone. This helps to reduce the manufacturing costs and the number of devices carried by a user.

The following are typical benefits of a two-factor authentication:

- resistant to single-factor attacks including keystroke monitoring, social engineering, man-in-the-middle attacks, network monitoring, password cracking and information technology (IT) staff abuse;
- difficult for a user to deny involvement in a transaction because users are held accountable for all actions resulting from a successful user authentication;
- less likely to lead to fraudulent or unauthorized access to corporate data;
- easy for end users to use; and
- durable and offers a long-term security solution.

The two-factor authentication system also has a number of disadvantages, which include the cost of purchasing, issuing and managing the tokens or cards. From the customer's point of view, using more than one two-factor authentication system requires carrying multiple tokens/cards, which can be lost or stolen.

Two-factor authentication can be regarded as a subtype of the multi-factor authentication, which is authentication with at least two independent authentication factors.

6.3 Multi-factor authentication

In two-factor authentication, the user needs to provide two factors, one of which is typically a physical token, such as a card, and the other is typically something memorized, such as a security code or PIN. Multi-factor authentication is an approach to authentication that requires the presentation of two or more of the three categories of authentication factors: a knowledge factor ("something the user knows"), a possession factor ("something the user has"), and an inherence factor ("something the user is"). The two-factor authentication is a type of multi-factor authentication. A key characteristic of

multi-factor authentication is that the authentication factors must span at least two of the authentication categories. For example, using a smart-card, PIN and fingerprint is a multi-factor authentication mechanism since the three factors are something a user has, something a user knows, and something a user is.

6.4 Combination of multi-factor authentication

Table 2 shows typical combinations used in multi-factor authentication.

Table 2 – Typical combinations used in multi-factor authentication

Type	Combination	Example
Two-factor authentication	Knowledge factor + possession factor	Password + OTP
	Knowledge factor + inherence factor	Password + fingerprint
	Possession factor + inherence factor	OTP + fingerprint
Three-factor authentication	Knowledge factor + possession factor + inherence factor	Password + OTP + fingerprint

6.5 Authentication threats

This clause describes some major threats, which are related to multi-factor authentication. It does not contain a complete set of potential threats.

6.5.1 Key logging attacks

Key logging (more often referred to as *keylogging* or "keyloggers") is the action of recording (or logging) the key strokes on a keyboard, typically in a covert manner so that the person using the keyboard is unaware that their actions are being monitored and recoded. This is sometimes implemented through software that is run on a mobile device.

6.5.2 Lost or stolen mobile device

Mobile devices are becoming a favourite target for theft since they contain credential information that may lead to financial gains. A malicious attacker may be able to steal a user's mobile device and attempt to log in to their various user accounts.

6.5.3 Shoulder surfing

Shoulder surfing is when an attacker obtains all or part of a user's credentials by taking a brief look (typically, over the user's shoulder) at the information provided by the user during authentication.

6.5.4 Denial of service attack

Depending on the method of communication between the mobile device and the personal computer, a denial of service (DoS) attack may be possible.

6.5.5 Online guessing

An attacker performs repeated log-on attempts by guessing possible values of the user’s credentials.

6.5.6 Offline guessing

Secrets associated with credential generation are exposed using analytical methods outside of the authentication transaction. Password cracking often relies upon brute force methods, such as the use of dictionary attacks. With dictionary attacks, an attacker uses a program to iterate through all of the words in a dictionary (or multiple dictionaries in different languages), computes the hash value for each word and checks the resultant hash value against a database.

The use of rainbow tables is another password cracking method. Rainbow tables are pre-computed tables of clear text/hash value pairs. Rainbow tables are quicker than brute-force attacks because they use reduction functions to decrease the search space. Once generated or obtained, rainbow tables can be used repeatedly by an attacker.

6.5.7 Credential duplication

The entity's credential, or the means to generate credentials, has been illegitimately copied. An example would be the unauthorized copying of a private key.

6.5.8 Eavesdropping

An attacker listens passively to the authentication transaction to capture information that can be used in a subsequent active attack to masquerade as the entity.

6.5.9 Replay attack

An attacker is able to replay previously captured messages (between a legitimate entity and a relying party (RP)) to authenticate as that entity to an RP.

6.5.10 Session hijack

An attacker is able to insert himself or herself between an entity and a verifier subsequent to a successful authentication exchange between the latter two parties. The attacker is able to pose as an entity to the RP or vice versa to control session data exchange. An example of this is when an attacker is able to take over an already authenticated session by eavesdropping on or predicting the value of the authentication cookies used to mark the hypertext transfer protocol (HTTP) requests sent by the entity.

In a session hijacking attack, malware or an attacker can take over a session already opened by the user, and use the stored information in the session to perform other transactions or alter the transactions.

6.5.11 Man-in-the-middle

The attacker positions himself or herself between the entity and the RP in order to intercept and alter the content of the authentication protocol messages. Typically, the attacker will simultaneously impersonate the RP to the entity and impersonate the entity to the verifier. Performing an active exchange with both parties simultaneously may allow the attacker to use authentication messages sent by one legitimate party to successfully authenticate to the other.

A man-in-the-middle attack is a special type of social engineering in which the attacker resides in between the user and the intended service provider and attempts to mimic the behaviour of the original service provider in order to fool the user into revealing their required credentials.

6.5.12 Credential theft

A device that generates or contains credentials is stolen by an attacker.

6.5.13 Spoofing and masquerading

Spoofing and masquerading refer to situations in which an attacker impersonates another entity in order to allow the attacker to perform an action they would otherwise not be able to perform (e.g., gain access to an otherwise inaccessible asset). This may be done by making use of the credential(s) of an entity or otherwise posing as an entity (e.g., by forging a credential). Some examples are: when an attacker impersonating an entity spoofs one or more biometric characteristics by creating a "gummy" finger that matches the pattern of the entity, an attacker spoofs a media access control (MAC) address by having its device broadcast a MAC address belonging to another device that has permissions on a particular network, or an attacker poses as a legitimate software publisher responsible for downloading online software applications and/or updates.

6.6 Criteria for selecting a multi-factor authentication method

The following criteria should be used to select the specific type of multi-factor authentication mechanisms used by the RP and the service provider:

- the desired level of entity authentication assurance (EAA);
- the amount of residual risk after applying multi-factor authentication mechanisms;
- the complexity of implementation of authentication mechanisms (e.g., computing power and speed, maturity of technology, scalability of technology);
- the practicability of the multi-factor authentication methods (i.e., difficult update of credential and key distribution);
- the assumption underlying the authentication solution; and
- the authentication failure rates.

6.7 Features of multi-factor authentication mechanisms using a mobile device

In this Recommendation, the mobile device is considered to be one of the authentication factors used in multi-factor authentication mechanisms, where these mechanisms are using the multi-factor authentication methods described in [ITU-T X.1154]. Note that the multi-method authentication and the multiple authentications, also described in [ITU-T X.1154], are not considered in this Recommendation. The considerations on identity management environments in [ITU-T X.1154] can be applied to the mechanisms in this Recommendation.

The purpose of the multi-factor authentication mechanisms in this Recommendation is to provide multiple authentication factors to enhance the security of a service using a mobile device. Multi-factor authentication mechanisms are generally assumed to be secure, since even when one authentication factor is compromised, the other authentication factors still remain secure. Therefore, the multi-factor authentication mechanisms are required to authenticate a user by using two or more authentication factors.

A user holds the authentication information that is used in the form of knowledge-based or inherence-based authentication factors and can transmit the information to the mobile device using a keypad, touchpad, fingerprint recognizer, etc. The mobile device transmits the authentication information to a service provider to be authenticated, or returns the authentication information back to the user by using a display or a sound device. The mobile device or secure elements (SEs) can generate the authentication information that is regarded as a possession-based authentication factor. When the possession-based authentication information is combined by some knowledge or inherence factor, the single use of the combined authentication information can be considered as multi-factor authentication. However, this kind of combined authentication information also can be possibly vulnerable to single authentication threats. Therefore, the generated information from the mobile device or secure elements in this Recommendation would be regarded as single authentication factor that is a possession factor, because the information mainly can prove the possession of the registered mobile device. The service provider receives the authentication information to validate it, or transmits the authentication information including a server's challenge (See Figure 1).

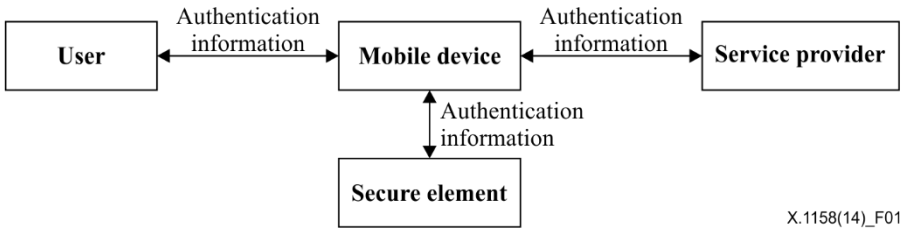


Figure 1 – Overview of multi-factor authentication mechanisms using a mobile device

The authentication mechanisms in this Recommendation, unlike other multi-factor authentication mechanisms, are considered to use a mobile device. Here, the mobile device is used as a possession-based authentication factor. Since the mechanisms are based in mobile devices, at least one mobile device with or without other connected devices is mandatorily used in the mechanisms.

The mobile device is required to be pre-registered with a service provider in order to ensure that the mobile device belongs to the correct user to be authenticated since the mechanisms produce the possession-based authentication information using a mobile device. A mobile device using these mechanisms is able to generate and transmit authentication information. However, the authentication information from the mobile device cannot be trusted when a mobile device has been tampered or affected by malware. Therefore, mechanisms are required to protect the transmission or generation procedures of authentication information from a mobile device.

Multi-factor authentication mechanisms using multiple channels are another alternative to protect the transmission procedure because when an authentication factor transmitted using a specific channel is even compromised, remaining authentication factors transmitted by other channels can still remain secure. Multi-factor authentication mechanisms using secure elements are also effective and more secure to protect the generation procedure because secure elements are tamper resistant and cannot be affected by malware. Therefore, the mechanisms may transmit the authentication information using multiple channels to protect the transmission procedure, or may generate the authentication information using secure elements to protect the generation procedure.

7 Security requirements for multi-factor authentication

7.1 General

– Multi-factor authentication is required to use two or more credentials implementing different authentication factors in the EAA framework, which is described in [ITU-T X.1254].

– Multi-factor authentication is required to be implemented to meet the security requirements for the following phases: a) enrolment (e.g., identity proofing, identity information verification, registration), b) credential management (e.g., credential issuance, credential activation), and c) authentication (see [ITU-T X.1254]).

– The identity of an entity in the multi-factor authentication mechanism is required to be established and managed by an enrolment procedure which consists of four processes: application and initiation, identity proofing, identity verification, and record-keeping/recording (see [ITU-T X.1254]).

– The credentials of each authentication factor in multi-factor authentication is required to be managed securely by the credential management procedure which comprises all processes relevant to the life-cycle management of a credential (see [ITU-T X.1254]).

– Each entity, as an actor in multi-factor authentication, is required to be authenticated during the entity authentication phase where the entity uses its credentials to confirm its identity to a RP (see [ITU-T X.1254]).

– Multi-factor authentication mechanisms are required to provide at least two or more different types of the authentication factor, which are used to authenticate the entity.

– The multi-factor authentication mechanisms in this Recommendation are required to have a capability to generate possession-based authentication information using a mobile device or secure elements in a mobile device, which is valid only once to counter a replay attack.

– Multi-factor authentication mechanisms are required to be resistant to the threats described in clause 6.5.

– Multi-factor authentication mechanisms are recommended to protect the privacy of biometric information which is provided by the user when it is transmitted or stored.

7.2 Mobile device

– The mobile device is required to be identified and registered with a service provider in a secure manner (e.g., online registration with strong authentication or offline registration in office branches) prior to performing the authentication phase so as to prove that the mobile device belongs to the right user.

– The mobile device is required to have a capability to generate the authentication information only after the user has been sufficiently authenticated to check whether the user is entitled to perform the transaction involved, and to provide a notification of the confirmation of the transactions in an explicit way (e.g., using display, ring tone, keypad input validation).

– The mobile device is required to immediately delete any data (e.g., a secret key) that is used during the generation of the authentication information.

– The mobile device is recommended to protect the secure hardware modules inside the mobile device from being infected by malware and to use protection software (e.g., anti-virus vaccines, rooting-detection tools, virtual keypad).

– The mobile device is recommended to provide access control capabilities, such as a finger-print authentication or PIN, to prevent unauthorized access when it is stolen or lost.

– The mobile device is recommended to record data as well as a timestamp for digital forensics, which is supplied from transaction details.

7.3 Secure element

– The secure element with an appropriate access-control capability is required to have a blocking mechanism that can block the authentication process after a number of failed authentication attempts.

– The secure element is required to have a capability to compute session cryptographic keys from the secret key that should not be exposed outside of the secure element. This key is a private key or a pre-shared key between the user and the service provider.

– The secure element is required to have a capability to generate authentication information from an explicit request by the user.

– The virtual secure element (e.g., virtual subscriber identity module (SIM)) is required to be protected from being tampered with by malware in order to maintain the equivalent security strength to that of a dedicated secure element.

7.4 Service provider

– The service provider is required to validate the ownership of the mobile device using the pre-registered user's identity and to verify the origin of the authentication information by checking whether or not it has been transmitted from the pre-registered mobile device.

– The service provider is required to protect the secret key so that it should not be exposed, by using a secure manner such as a hardware security module (HSM).

– The service provider is recommended to notify the user of deletion of information from the mobile device using a kill switch capability, when the mobile device is lost or stolen, and to train the user in the safe use and management of the mobile device.

– To ensure integrity and provide enhanced security of the transaction, it is recommended that the service provider record any data together with a timestamp. The timestamp, which is supplied from the transaction details, can be used for digital forensic analysis.

8 Generic mechanisms

This clause describes the generic mechanisms that are needed to implement the multi-factor authentication service using a mobile device. The generic mechanisms consist of entities, operations, authentication models and protocols.

8.1 Entities

The entities involved in multi-factor authentication mechanisms using a mobile device include the user, the devices and secure elements and the service providers. The details are as follows:

– User: An entity to be authenticated by a service provider through an online-based service. The user has either a knowledge-based authentication factor (e.g., password, PIN) or an inherence authentication factor (e.g., fingerprints, iris scan or footsteps).

– Devices: The set consisting of the mobile device and connected device that generate and transmit the authentication information. The devices in the multi-factor authentication mechanisms using a mobile device are required to include at least one mobile device which is to be used as an authenticator. The devices in the mechanisms are also required to include at least one connected device that is to transmit the authentication information to a service provider. Therefore, the devices are classified into two types: one is the mobile device and the other is the connected device. The mechanisms allow that a single mobile device can also be a connected device.

  • Mobile device: A portable computing device possessed by a user, typically having a display screen with touch input or keypad. Since the mobile device is almost always in the possession of the user, it can be easily used as a possession-based authentication device. It can generate the possession-based authentication information (with or without secure elements), and it can also be used as a connected device to transfer knowledge-based or inherence-based authentication information from a user. Furthermore, a single mobile device can be a connected device when it has the ability for communication (e.g., smart phones, smart watches, smart glasses). A stand-alone mobile device (e.g., OTP tokens, transaction authentication number (TAN) generators) is a dedicated mobile device which includes a feature of the secure element inside and often has limited transmission capability.

  • Connected device: A communication device to access online services offered by a service provider. This may include a personal computer (PC), an automated teller machine (ATM), a mobile phone, etc. Depending on the service model, a connected device can use multiple channels for communication with a service provider.

– Secure elements: A set of secure elements included on a tamper resistant integrated circuit (IC) chip or on-board chip that are activated by the mobile device to securely generate the possession-based authentication information. Secure elements are required to protect a secret key that is pre-shared between a user and a service provider. The secret key is cryptographically calculated to create possession-based authentication information. The secure elements are used in multi-application environments and can be available in multiple form factors such as plastic smart-card; a SIM or universal subscriber identity module (USIM) in a mobile device; a dedicated chip on a phone's motherboard; an external plug-in memory card or an external contactless IC card. In this Recommendation, it is not limited to the use emulated secure elements such as virtual SIMs when they are implemented according to the security requirements described in clause 7.3.

– Service provider: An entity that provides the Internet application service to a user. The service provider has to verify the authentication information transmitted from the user's devices. Verification can be done within an internal authentication server or via an external authentication service provider such as the OTP service provider (OSP) [b-ITU-T X.1153].

8.2 Operations

The multi-factor authentication mechanisms using a mobile device include four operations focused on the authentication information, and these are as follows:

1) Transmit: An operation to deliver the authentication information from, or to, the devices. The authentication information can be transmitted in various ways:
   a) using human intervention methods between the devices and the user (e.g., touch input, display screen);
   b) using near connecting methods between the devices and the secure elements (e.g., data bus, Bluetooth, near field communication (NFC));
   c) using traditional communication methods between the devices and the service provider (e.g., local area network (LAN), wireless fidelity (WiFi)).
2) Activate: An operation to trigger the secure elements to generate the possession-based authentication information. A user can selectively activate the secure elements by providing some authentication information. Although the secure elements are activated by certain authentication information (e.g., password, fingerprints) and transmit only possession-based authentication information to a service provider, they are regarded as a multi-factor authentication mechanism.
3) Generate: An operation to calculate the possession-based authentication information. The mobile device can generate the authentication information, but the security of the information generated from the mobile device is not guaranteed since the mobile device is not tamper resistant when it is affected by malware. The secure elements can also generate the authentication information, and the information from the secure elements cannot be tampered.
4) Verify: An operation to validate the authentication information transmitted by the devices. A service provider can authenticate a user by verifying the multiple authentication information.

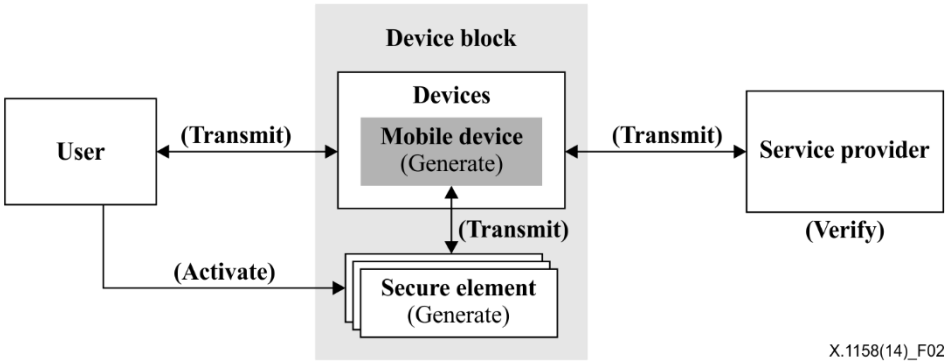


Figure 2 – Operations of the mechanisms

Figure 2 shows the relationships between entities and operations. The device block is a virtual block that includes both devices and secure elements that are often integrated into a mobile device. A user can transmit the authentication information to or from the devices by human intervention methods and the user can activate the secure elements by providing authentication information via the mobile devices. A mobile device and secure elements in a device block are responsible for generating the possession-based authentication information. A connected device in a device block is responsible for transmitting the authentication information to a service provider. The service provider is responsible for transmitting and verifying the authentication information.

8.3 Authentication models

The authentication models represent the relationships and authentication flows among the entities. There are two kinds of authentication models related to multi-factor authentication mechanisms: generic models and hybrid models.

The generic models consist of minimum transactions of authentication information. All generic models are secure and resistant to the authentication threats described in clause 6.5. Therefore, authentication threats cannot compromise the generic models at once because these models are authenticated using multiple authentication information. The hybrid models are combined with multiple generic models to be more easily deployed.

8.3.1 Overview of authentication models

The authentication models in this Recommendation are secure because all the models are required to satisfy the security requirements described in clause 7. All of the models promise that at least one authentication factor will remain secure even in the event that other authentication factors are compromised. The following three principles guarantee the security of the generic models:

1) Transmit by multiple channels: When a mobile device without secure elements generates possession-based authentication information, each of the information is required to be transmitted to a service provider using a different channel. Since the mobile device without secure elements is likely to be tampered with, the possession-based authentication information from the mobile device cannot be guaranteed to be secure. Moreover, multiple information transmitted by single channel is more likely to be compromised altogether by authentication threats. Therefore, a mobile device without secure elements is required to transmit possession-based authentication information independently.

2) Generate by a secure mobile device: When a mobile device with secure elements or a stand-alone mobile device generates possession-based authentication information, all of the information may be transmitted to a service provider using a single channel. Since the secure elements or a stand-alone mobile device are designed to be tamper resistant, the possession-based authentication information from secure elements or a stand-alone mobile device can be transmitted along with other authentication information using the same channel.

   a) Activate by user confirmation: Secure elements in the mobile device (e.g., USIM in a smart phone) are usually passive and should be triggered to interact with the mobile device. As a result, malware installed in a mobile device can possibly activate the secure elements to generate possession-based authentication information without any confirmation by the user. Therefore, passive secure elements that interact with a mobile device are required to block unintended access and be securely activated by the rightful user with full awareness of the intended transaction. The following ways ensure, but are not limited to, the security of activation in the passive mode:

      i) activate by explicit user approval with time-limited credential (e.g., OTP, PIN with time-limit, fingerprint template);

      ii) transaction signing with explicit user confirmation of transaction information.

   b) Segregate from malware: A stand-alone mobile device, or a secure element integrated in a mobile device, is usually designed to be tamper resistant. Since this kind of device is often designed to be segregated from malware, there is no security consideration on the implementation of activation operation. However, the mechanisms using the stand-alone mobile device are required for the connected device to transmit, because the stand-alone mobile device usually has no communication features. There are multiple ways to ensure the segregation from malware, which include but are not limited to:

i) the usage of a stand-alone mobile device (e.g., OTP tokens, TAN generator) that can generate the possession-based authentication information independently, and does not need to interact with other mobile devices;

ii) maintaining the integrity of the generation module with manufacturing supports (e.g., trusted execution environment (TEE), TrustZone, trusted platform module (TPM)) can also assure segregation from malware.

3) Verify multiple authentication factors: In spite of the cost of the authentication information for access control, a service provider is required to verify two or more types of authentication factors to complete the multi-factor authentication mechanisms. When a user activates the secure elements by some authentication information and the secure elements generate possession-based authentication information, this is also regarded as multi-factor authentication since two different types of authentication information are validated. However, the transmission of single authentication information to a service provider after access control is not sufficiently secure because all of the authentication information is transmitted to the same mobile device, which may have been possibly compromised by authentication threats.

Table 3 – Comparison of generic models

Model		**Features**	**Instance of the model**
Using multiple channels	One-directional multiple channels model	The mobile device generates possession-based authentication information, and can be possibly tampered with since the model has no secure elements. Therefore, the model is required to be secured by abiding to the following principles: 1) transmit by multiple channels; 3) verify multiple authentication factors.	Multi-device log-in, Multi-channel, Login
	Bidirectional multiple channels model		SMS OTP, out of band (OOB)
Using a secure mobile device	Mobile device with secure elements model	The secure elements generate possession-based authentication information, and can be possibly activated by un-authorized access since the secure elements are passive, and the mobile device can be possibly tampered with. Therefore, the model is required to be secured by abiding to the following principles: 2) generate with secure elements: 2a) activate by user confirmation; 3) verify multiple authentication factors.	PKI tokens, mobile OTP
	Stand-alone mobile device model	The stand-alone mobile device generates possession-based authentication information and can guarantee segregation from malware, which is specified in clause 8.3.1. The model is required to be secured by abiding to the following principles: 2) generate with secure elements: 2b) segregate from malwares; 3) verify multiple authentication factors.	OTP tokens

Table 3 shows the features and instances of the generic models. The generic models are required to be secured against authentication threats and to reinforce security by multiple authentication

information. To ensure the security of each generic model, there are some constraints to be applied for the devices.

In the one-directional or bidirectional multiple-channels model, the devices are required to transmit the authentication information to a service provider using multiple channels. The service provider is required to verify two or more authentication factors. In the mobile device with the secure elements model, the secure elements are required to be activated by user confirmation and awareness of the transaction details, and to generate the possession-based authentication information. The devices are required to transmit two or more types of authentication information to a service provider, and the service provider is required to verify two or more authentication factors. In the stand-alone mobile device model, the stand-alone mobile device is required to be segregated from other devices or malware, and to generate the possession-based authentication information independently. The connected devices are required to transmit two or more types of authentication information including possession-based authentication information from a stand-alone mobile device, and the service provider is required to verify two or more authentication factors.

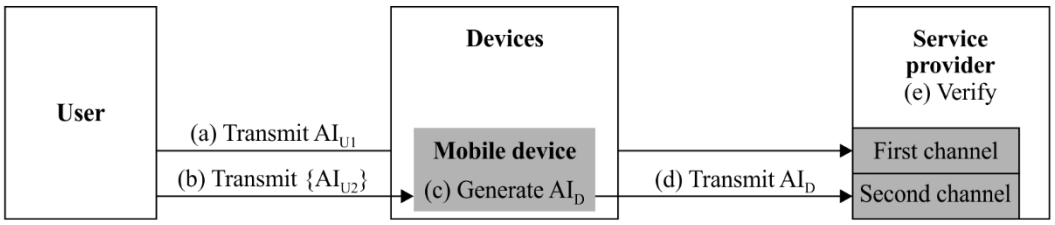
8.3.2 Generic models using multiple channels

The generic models using multiple channels consist of three entities: a user, a service provider and devices excluding secure elements. These models are often implemented by mobile applications in mobile devices that are widely applied in the Internet application service. Since the mobile applications in the mobile device might not be guaranteed from having been tampered, the alternative multiple channels are required to transmit the possession-based authentication information separately from other authentication information.

This model has no limit on the number of devices, but it is required to include at least one mobile device. The mobile device is required to be pre-registered with a service provider to ensure that the user possesses the mobile device. A single mobile device as a connected device can also be applied to this model. The possession-based authentication information from a mobile device can be transmitted in both directions: a user or a service provider. Therefore, this model can be classified into two methods: one-directional and bidirectional transmission.

1) One-directional multiple channels model

The feature of the one-directional multiple channels model is a one-way transmission of the authentication information between the device and the service provider. Examples of this model can be found in multi-device log-ins, multiple channels log-ins in the same device, etc. Figure 3 shows abstract steps of a one-directional multiple channels model.



NOTE – AI_{U1}, AI_{U2}: User's authentication information, AI_D: Device's authentication information, {}: Optional information

X.1158(14)_F03

Figure 3 – One-directional multiple channels model

Step (a): The user holds one or two authentication information (AI_{U1}, AI_{U2}) such as a password, fingerprints, etc. The user transmits one of the authentication information (AI_{U1}) to the first channel of the service provider using a device which would be the mobile device or some connected device.

Step (b): The user can optionally transmit another type of authentication information (AI_{U2}) to the mobile device to get the access rights. This step can be skipped when a mobile device is assumed to be securely managed by the user.

Step (c): The mobile device generates the possession-based authentication information (AI_D), selectively and it checks any additional information (e.g., timestamp).

Step (d): The mobile device transmits the possession-based authentication information (AI_D) to the second channel of the service provider. The first and second channels are required to be different, but not limited to use by the same device.

Step (e): The service provider verifies multiple authentication information (AI_{U1}, AI_D) from multiple channels. In order to achieve multi-factor authentication, all authentication information (AI_{U1}, AI_D) have different authentication factors. After the verification, the service provider allows the user to access the service.

2) Bidirectional multiple channels model

The feature of the bidirectional multiple channels model is a two-way transmission of the authentication information between the device and the service provider. Examples of this model can be found in short message service (SMS), OTP, OOB or e-mail re-confirmation, etc. Figure 4 shows abstract steps of the bidirectional multiple channels model.

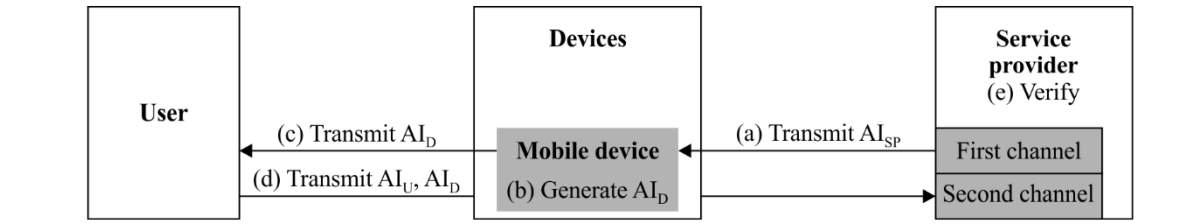


Figure 4 – Bidirectional multiple channels model

Step (a): The service provider generates random nonce value (AI_{SP}) that is valid only for the transaction. The service provider transmits the random nonce value as the authentication information (AI_{SP}) to the mobile device which is pre-registered with the service provider.

Step (b): The mobile device generates the possession-based authentication information (AI_D) by using the authentication information (AI_{SP}) that is transmitted from the service provider. The possession-based authentication information can be the same value with receiving information when the information from the service provider (AI_{SP}) can be guaranteed to be transmitted to a registered mobile device and is valid only for the user.

Step (c): The mobile device transmits the authentication information to the user using human intervention methods (e.g., display screen, sounds). The mobile device can optionally transmit the authentication information directly to the connected device using near connecting methods (e.g., data bus, Bluetooth, NFC).

Step (d): The user holds the authentication information (AI_U) such as a password, fingerprints, etc. The user can transmit the authentication information including the possession-based authentication (AI_U, AI_D) to the second channel of the service provider. The multiple authentication information in the same channel can be secured because the possession-based authentication information (AI_D) is transmitted from the registered mobile device that is certainly possessed by the user.

Step (e): The service provider verifies the user's authentication information (AI_U) and validates the possession-based authentication information (AI_D) by comparing it with the random nonce value (AI_{SP}). In order to achieve the multi-factor authentication, all authentication information (AI_U, AI_D)

have different authentication factors. After the verification, the service provider allows the user to access the service.

8.3.3 Generic models using a secure mobile device

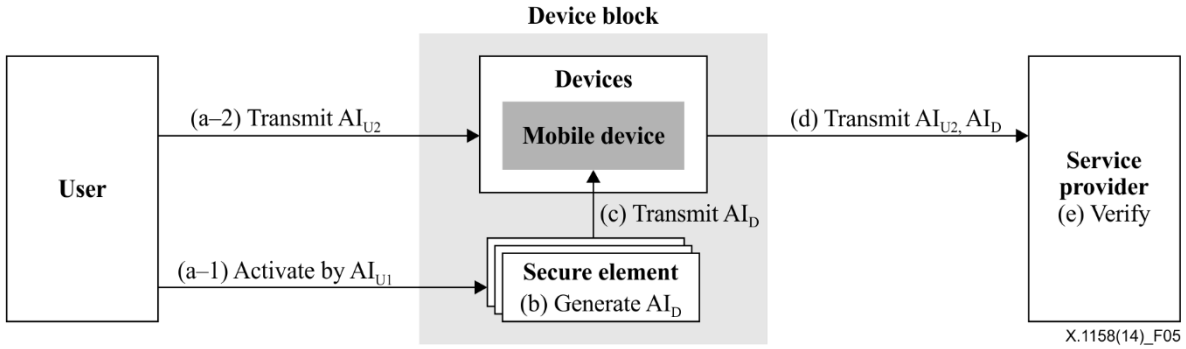
The generic models are able to protect the authentication information using a secure mobile device. There are two ways to use a secure mobile device: a mobile device with secure elements and a stand-alone mobile device.

1) Mobile device with secure elements model

The mobile device with secure elements model consists of four entities: a user, a service provider, devices, and secure elements. This model is often implemented on IC chip or hardware chip. Since the possession-based authentication information from the secure elements has guaranteed the proof of possession, the transmission of multiple authentication information, including the possession-based authentication information, could also be secure. However, passive secure elements can also be activated without any confirmation by the user. Therefore, the passive secure elements are required to be securely activated by the right user.

This model has no limit to the number of devices, but it is required to include at least one mobile device with secure elements. A single mobile device as a connected device can also be applied to this model. The secret key, which stored in the secure elements, is required to be private or pre-shared with the service provider. Moreover, the mobile device is required to be pre-registered with a service provider to confirm that the user possesses the mobile device and secure elements.

Examples of this model can be found in PKI signing tokens in USIM, NFC payment with IC card, etc. Figure 5 shows the abstract steps of the mobile device with secure elements model.



NOTE – *AI_U: User's authentication information*, *AI_D: Device's authentication information*

Figure 5 – Mobile device with secure elements model

Step (a): The user holds multiple authentication information (AI_{U1}, AI_{U2}) such as a password, fingerprints, etc. The user securely activates the secure elements with full awareness of the transactions provided by the authentication information (AI_{U1}). Then the user transmits the other authentication information (AI_{U2}) to a connected device.

Step (b): The secure elements generate the possession-based authentication information (AI_D) by using the secret key which is either a private key or a pre-shared key with the service provider. The possession-based authentication information generated from secure elements (AI_D) guarantees the proof of possession by the user.

Step (c): The secure elements transmit the possession-based authentication information to the mobile device, and the mobile device can optionally deliver the possession-based authentication information directly to the connected device using near connecting methods (e.g., data bus, Bluetooth, NFC).

Step (d): The connected device transmits the multiple authentication information including the possession-based authentication (AI_{U2}, AI_D) to the service provider.

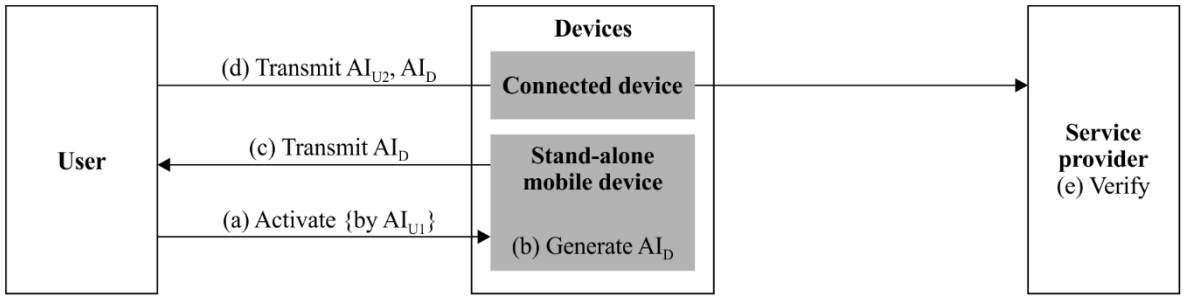
Step (e): The service provider verifies the user's authentication information (AI_{U2}) and validates the possession-based authentication information (AI_D) and it checks the user's secret key or public key. In order to achieve multi-factor authentication, all authentication information (AI_U, AI_D) have different authentication factors. After the verification, the service provider allows the user to access the service.

2) Stand-alone mobile device model

The stand-alone mobile device model consists of three entities: a user, a service provider, and a stand-alone mobile device, which is integrated with a mobile device, and a secure element. The stand-alone mobile device is often implemented in a dedicated hardware token (e.g., an OTP token or a TAN generator), which is tamper resistant. Since the possession-based authentication information from the stand-alone mobile device is guaranteed, the proof of possession and the transmission of multiple authentication information, including the possession-based authentication information, can also be secure. The stand-alone mobile device is secure because it cannot be activated without confirmation by the user.

This model has no limit on the number of devices, but it is required to include at least two devices: one is a stand-alone mobile device and the other is a connected device. The secret key which is stored in the stand-alone mobile device is required to be private or pre-shared with the service provider. Moreover, the stand-alone mobile device is required to be pre-registered with a service provider to ensure the proof of possession by the user.

Examples of this model can be found in OTP token, etc. Figure 6 shows abstract steps of the stand-alone mobile device model.



NOTE – *AI_{U1}, AI_{U2}: User's authentication information, AI_D: Device's authentication information, {}: Optional information*

X.1158(14)_F06

Figure 6 – Stand-alone mobile device model

Step (a): The user holds one or two pieces of authentication information (AI_{U1}, AI_{U2}) such as a password or fingerprints, etc. The user can optionally activate the secure elements by using the authentication information (AI_{U1}). This step can be skipped when a mobile device is assumed to be securely managed by the user.

Step (b): The stand-alone mobile device generates the possession-based authentication information (AI_D) by using the secret key which is either a private key or a pre-shared key with the service provider. The possession-based authentication information generated from the stand-alone mobile device (AI_D) guarantees the proof of possession by the user.

Step (c): The stand-alone mobile device transmits the authentication information to the user using human intervention methods (e.g., display screen, sounds). The stand-alone mobile device can

optionally deliver the possession-based authentication information directly to the connected device using near connecting methods (e.g., data bus, Bluetooth, NFC).

Step (d): The connected device transmits multiple authentication information including the possession-based authentication (AI_{U2}, AI_D) to the service provider.

Step (e): The service provider verifies the user's authentication information (AI_{U2}) and validates the possession-based authentication information (AI_D) by using the user's secret key or public key. In order to achieve multi-factor authentication, all authentication information (AI_U, AI_D) have different authentication factors. After the verification, the service provider allows the user to access the service.

8.3.4 Hybrid models

The generic models shown in clauses 8.3.2 and 8.3.3 are minimized in terms of the transactions of authentication information. The service provider can use the hybrid models combined with multiple generic models to deploy their service easily. There are many applicable scenarios that combine the generic models such as mobile devices with secure elements using multiple channels. This kind of scenario can be found in the authentication service for the financial sector (i.e., mobile OTP token with NFC-enabled IC card). However, the hybrid models cannot always guarantee that they are more secure than the generic models.

8.4 Protocols

Protocols provide guidance on how to implement specific authentication flows of the generic models. All the mechanisms, including the protocols, can be resistant to authentication threats. The protocols can be categorized into four types, and each type is applied to the generic models shown in clause 8.3.2 and 8.3.3. The notation of the protocols is defined as follows:

– AI_{Un} where (n > 1): *n-th* authentication information of the user, which is regarded as knowledge, inherence, or behaviour factor and which often can be submitted by the user. (n is the number of authentication factors that the user holds.) All authentication information is required to include different types of authentication factors.

– AI_D: Authentication information of devices, which is regarded as the possession factor.

– AI_{SP}: Service provider's nonce value.

– ID_U: Identity of the user.

– T_U: Additional text for the transaction (e.g., timestamp or hash value of transaction data). This information can be transmitted from the service provider prior to the authentication procedure.

– T_D: Additional text for the device (e.g., device serial number). This information is required to include a one-time value (e.g., time, event value of accumulated transaction numbers) resistant against replay threats.

– $f(X_1, \ldots, X_n)$ where (n > 1): The generation function which produces the possession-based authentication information using arguments ($X_1, \ldots, X_n$). The arguments are required to be used during the generation when they are provided.

– SK_D: Secret key or private key of the devices.

– { X }: X is optional data and can be simply skipped.

8.4.1 Protocol for the one-directional multiple channels model

The protocol for the one-directional multiple channels model is resistant to authentication threats, since each transmission of the authentication information is separate and independent. In this protocol, the connected device securely transmits the multiple authentication information of the user, which includes knowledge, inherence, or behaviour factor using one channel. In addition, the mobile device transmits the authentication information of the device, which includes the possession-based

factor, using another channel. Figure 7 shows the steps of the protocol for the one-directional multiple channels model.

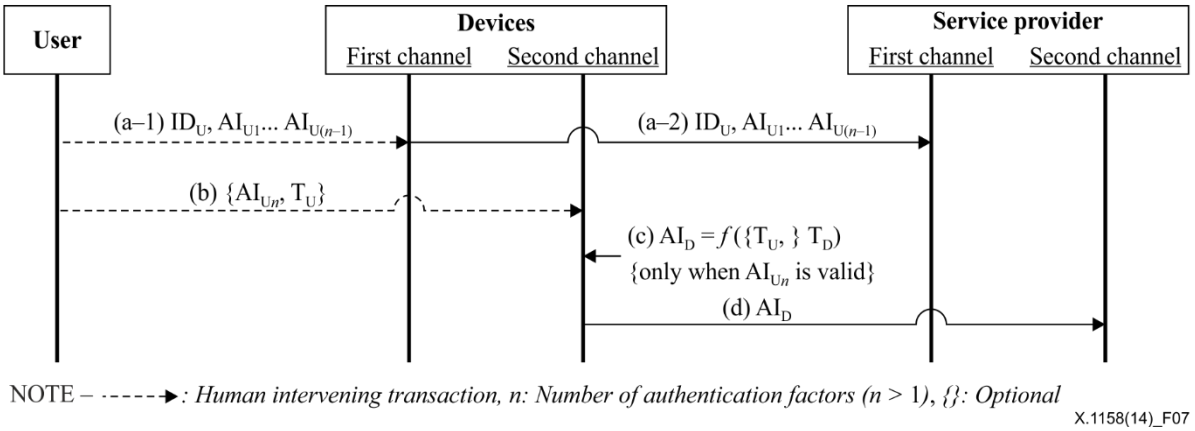


Figure 7 – Protocol for the one-directional multiple channels model

Step (a-1): The user transmits multiple authentication information (AI_{U1} ~ $AI_{U(n-1)}$) with his or her identity (ID_U) to the first channel of the devices. Step (a-2): The device which receives this information has the role of a connected device, and the connected device delivers the transmitted information (ID_U, AI_{U1} ~ $AI_{U(n-1)}$) to the first channel of the service provider. The number of channels and devices are not limited for the transmission of this information.

Step (b): The user can optionally transmit one of the authentication information items (AI_{Un}) with additional text of the transaction (T_U) to the second channel of the devices. The additional text of the transaction (T_U) typically contains the transaction details.

Step (c): The device which uses the second channel would be a mobile device. The mobile device can be activated when the authentication information (AI_{Un}) transmitted from the user is valid. The device can also be activated without any information. When the mobile device is activated, the device generates the possession-based authentication information (AI_D) using the arguments of the additional text for the device (T_D). The additional text of the device (T_D) typically contains the unique value of the mobile device. The additional text of the transaction (T_U) can be selectively used during the generation. A single mobile device can be used as a connected device in this protocol.

Step (d): The mobile device transmits the possession-based authentication information (AI_D) to the service provider.

After the protocol has transmitted all the information, the service provider can identify the user by the user's identity (ID_U), and can also authenticate the user by multiple authentication information such as the user's authentication information (AI_{U1} ~ $AI_{U(n-1)}$) and the possession-based authentication information (AI_D). When each of authentication information has a different factor and includes a possession-based factor, the protocol completes the *n*-factor authentication.

8.4.2 Protocol for the bidirectional multiple channels model

The protocol for the bidirectional multiple channels model has the same features as the previous protocol since the protocol adopts multiple channels for ensuring the security. In this protocol, the service provider securely transmits a nonce value to the specific user's mobile device using one channel. The mobile device generates the possession-based authentication information using the service provider's nonce value. Furthermore, the connected device transmits multiple authentication information, which includes several authentication factors, using another channel. Figure 8 shows the steps of the protocol for the bidirectional multiple channels model.

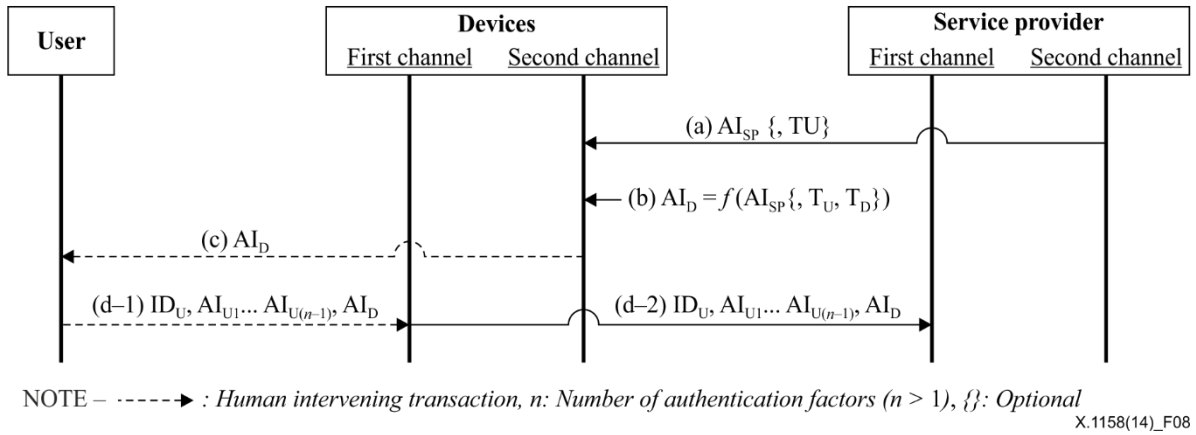


Figure 8 – Protocol for the bidirectional multiple channels model

Step (a): The service provider transmits a nonce value (AI_{SP}) optionally with the additional text of the transaction (T_U) to the second channel of the devices. The additional text of the transaction (T_U) typically contains the transaction details.

Step (b): The device which uses the second channel would be a mobile device. The mobile device can be activated by the user and generates the possession-based authentication information (AI_D) using the arguments of the service provider's value (AI_{SP}), which is a one-time-use value and valid for only the specific user who possesses the mobile device. The additional text of the transaction (T_U) and of the device (T_D) can be selectively used during the generation. There is no limit on the specific implementation of the generation function (*f*). Therefore, when the user is undoubtedly the owner of the mobile device, the function can be a dummy and can generate the possession-based authentication information (AI_D) which has the same value as the service provider's nonce value (AI_{SP}).

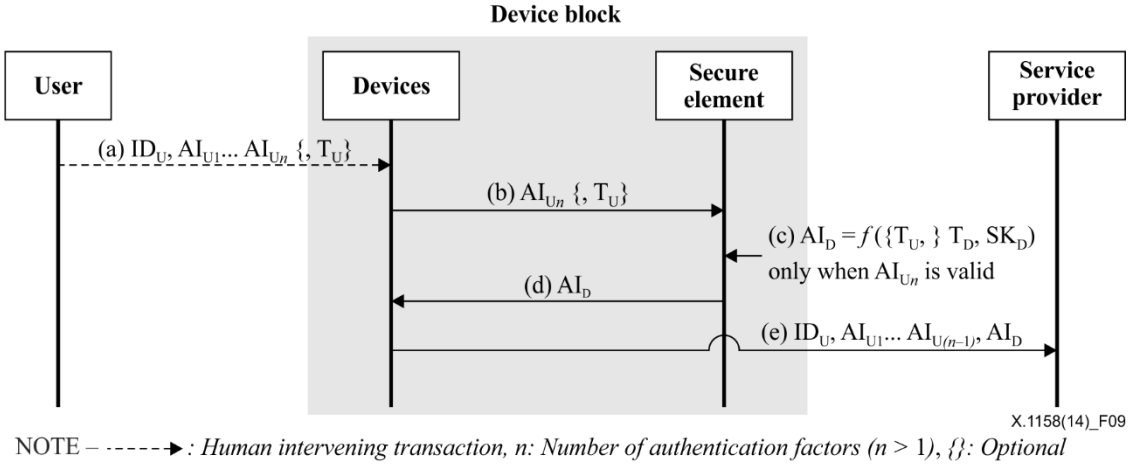
Step (c): The mobile device transmits the possession-based authentication information (AI_D) to the user using a human intervention method (e.g., display screen, voice).

Step (d): The user transmits multiple authentication information (AI_{U1} ~ $AI_{U(n-1)}$) with his or her identity (ID_U) to the first channel of the devices. In addition, the user transmits the possession-based authentication information (AI_D) using the same channel. The device which receives this information has the role of a connected device, and the connected device delivers the transmitted information (ID_U, AI_{U1} ~ $AI_{U(n-1)}$, AI_D) to the first channel of the service provider. The number of channels and devices are not limited to the transmission of this information. Therefore, a single mobile device can be used as a connected device in this protocol.

After the protocol has transmitted all the information, the service provider can identify the user by the user's identity (ID_U), and can also authenticate the user by multiple authentication information such as the user's authentication information (AI_{U1} ~ $AI_{U(n-1)}$) and the possession-based authentication information (AI_D). When each of authentication information has a different factor and includes a possession-based factor, the protocol completes the *n*-factor authentication.

8.4.3 Protocol for the mobile device with secure elements model

The protocol for the mobile device with secure elements model is resistant to authentication threats, since the generation of the possession-based authentication information is separate and independent. In this protocol, the secure element securely generates the possession-based authentication information using a cryptographic key. Furthermore, the mobile device transmits the multiple authentication information to the service provider. Figure 9 shows the steps of the protocol for the mobile device with secure elements model.



NOTE – ------►: *Human intervening transaction, n: Number of authentication factors (n > 1), {}: Optional*

Figure 9 – Protocol for the mobile device with secure elements model

Step (a): The user transmits multiple pieces of authentication information (AI_{U1} ~ AI_{Un}) with his or her identity (ID_U) to the mobile device using a human intervention method (e.g., keypad, touch-screen). The user can optionally transmit the additional text of the transaction (T_U) to the mobile device. The additional text of the transaction (T_U) typically contains the transaction details.

Step (b): The mobile device transmits one piece of authentication information (AI_{Un}) with the additional text of the transaction (T_U) to the secure elements.

Step (c): The secure elements can be activated only when the authentication information (AI_{Un}) transmitted from the user is valid. Otherwise, the authentication protocol would be terminated. When the secure elements are activated, the secure elements generate the possession-based authentication information (AI_D). During the generation, the secret key (SK_D) and the additional text of the device (T_D) are required to be used for ensuring the security. The additional text of the transaction (T_U) can also be optionally used in the generation operation when it is provided. The number of secure elements are not limited to generation. Therefore, one secure element can generate the possession-based authentication information (AI_D) selectively, interacting with the other secure elements.

Step (d): The secure elements transmit the possession-based authentication information (AI_D) back to the mobile device.

Step (e): The mobile device, or the connected device, transmits all the information (ID_U, AI_{U1} ~ $AI_{U(n-1)}$, AI_D) to the service provider. The number of channels and devices are not limited to the transmission of this information. Therefore, a single mobile device can be used as a connected device in this protocol.

After the protocol has transmitted all information, the service provider can identify the user by the user's identity (ID_U), and can also authenticate the user by using multiple authentication information such as the user's authentication information (AI_{U1} ~ $AI_{U(n-1)}$) and the possession-based authentication information (AI_D). This protocol uses (n+1) authentication factors since one of the authentication information (AI_{Un}) has been consumed for activating the secure elements. However, if the authentication information (AI_{Un}) is a possession-based authentication factor, the protocol completes the n-factor authentication since the possession-based authentication information (AI_D) and the authentication information (AI_{Un}) are the same authentication factor.

8.4.4 Protocol for the stand-alone mobile device model

The protocol for the stand-alone mobile device model has the same features as the previous protocol since the protocol adopts the secure generation of possession-based authentication information for ensuring security. In this protocol, the stand-alone mobile device securely generates the possession-based authentication information using a cryptographic key. Furthermore, the connected device

transmits the multiple pieces of authentication information to the service provider. Figure 10 shows the steps of the protocol for the stand-alone mobile device model.

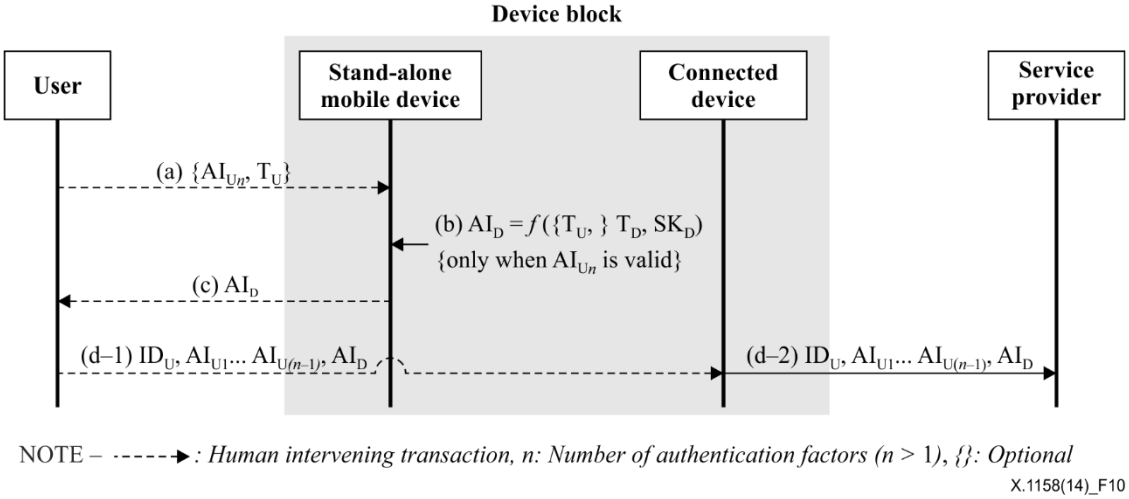


Figure 10 – Protocol for the stand-alone mobile device model

Step (a): The user can optionally transmit one piece of authentication information (AI_{Un}) with the additional text of the transaction (T_U) to the stand-alone devices. The additional text of the transaction (T_U) typically contains the transaction details.

Step (b): The stand-alone mobile device can be activated when the authentication information (AI_{Un}) transmitted from the user is valid. Alternatively the stand-alone mobile device also can be activated without any information. When the stand-alone mobile device is activated, the device generates the possession-based authentication information (AI_D). During the generation, the secret key (SK_D) and the additional text of the device (T_D) are required to be used for ensuring the security. The additional text of the transaction (T_U) can also be optionally used in the generation operation when it is provided.

Step (c): The stand-alone mobile device transmits the possession-based authentication information (AI_D) to the user using a human intervention method (e.g., display screen, voice).

Step (d): The user transmits multiple pieces of authentication information ($AI_{U1} \sim AI_{U(n-1)}$) with his or her identity (ID_U) to the devices. Furthermore, the user transmits the possession-based authentication information (AI_D) to the same device. The stand-alone mobile device typically has no transmission features. Therefore, the device which receives this information has the role of a connected device, and the connected device delivers the transmitted information (ID_U, $AI_{U1} \sim AI_{U(n-1)}$, AI_D) to the service provider. The number of channels and devices are not limited to the transmission of this information. However, at least one stand-alone mobile device and one connected device are required to be used in this protocol.

After the protocol has transmitted all the information, the service provider can identify the user by the user's identity (ID_U), and can also authenticate the user by multiple pieces of authentication information such as the user's authentication information ($AI_{U1} \sim AI_{U(n-1)}$) and the possession-based authentication information (AI_D). This protocol optionally uses (n+1) authentication factors since one piece of the authentication information (AI_{Un}) can be selectively consumed for activating the stand-alone mobile device. However, if the authentication information (AI_{Un}) is a possession-based authentication factor, the protocol completes n-factor authentication since the possession-based authentication information (AI_D) and the authentication information (AI_{Un}) are the same authentication factor.

Appendix I

Typical scenario for two-factor authentication

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

This appendix specifies typical scenarios of a two-factor authentication mechanism using a mobile device. When users want to be authenticated by a web server, they use their password as the first factor and then a one-time password (something the entity has) as the second authentication factor. It is assumed that the client and the server share the secret key, Ks, to compute the second authentication factor.

A typical example of the authentication protocol may comprise the following steps:

1) The client sends to the server a pair of usernames and the hashed password, *h(password)*.

2) The server retrieves the hashed value of the user and compares the received hashed password with the retrieved hashed password. In case of a successful match, it completes one-factor authentication.

3) For the second factor authentication, the client computes Sn, a one-time password at the current session n, from S_{n-1}, a one-time password at the previous session n-1 and the shared secret key, Ks, between the server and the client as follows:

   $Sn = f(\text{Ks}, S_{n-1})$

   The client sends Sn to the server.

4) The server computes Sn' and compares the received Sn and the computed Sn'. In case of a successful match, it completes the second authentication factor.

As long as the token S_{n-1} is adequately secured on the mobile device, proving knowledge of it is sufficient for a second log-in factor (which the client does by checking and providing Sn).

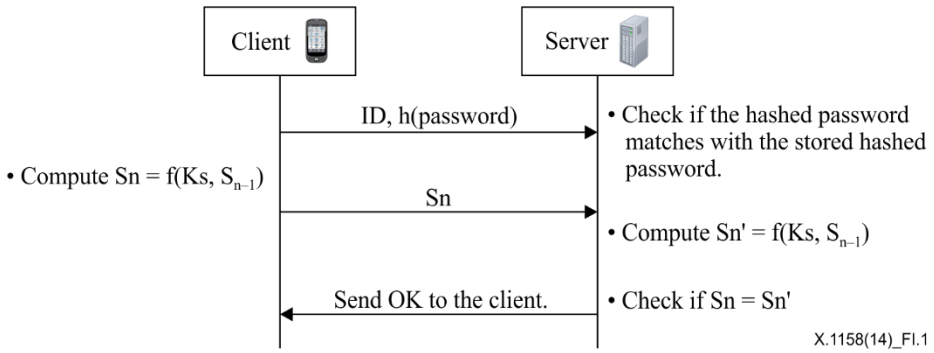


Figure I.1 – Typical two-factor authentication mechanism

Appendix II

Instances of components of multi-factor authentication

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

This appendix describes core instances of components of multi-factor authentication solutions.

II.1 Smart-card

A smart-card is a typical example of a possession factor. A smart-card is one of the most practical and reliable solutions to provide strong authentication of users. A user must possess a smart-card to provide strong authentication. The smart-card may need a second factor such as PIN, a password or even a fingerprint to allow access to the content of the smart-card. The smart-card must require a reading device to communicate with the user. The content in the smart-card cannot be accessed by outsiders unless the value of the second factor is authenticated by the smart-card from the reading device. Specifically, when a user inserts a smart-card into a reading device from a user's computer, the computer reads PIN (or the other second factor) and writes it on the smart-card. Once PIN matches the smart-card, the smart-card will allow the other information it contains to be accessed by the computer. The most important information delivered by the smart-card to the computer is, of course, the identity of the user. When the computer receives that identity, the authentication is complete.

II.2 Digital certificate

One of the core enabling security technologies is the PKI, which is based in digital certificates issued to individuals by a certification authority (CA) through a registration procedure. The validity of the stored information is consistently validated and supported by the PKI. Service providers and financial institutions are increasingly using strong authentication and PKI technology as a key enabler. Digital certificates allow individual users, workstations and servers to identify themselves to each other, by digital signing of e-mail messages, software source files, secure web communications and websites. This key enabling technology allows for a strong authentication [b-ITU-T X.509].

II.3 Biometrics

Biometrics is regarded as an inherence factor. Automated biometrics in general, and fingerprint technology in particular, can provide a much more accurate and reliable user authentication solution. Biometrics is used to identify users based on their physiological or behavioural characteristics. Examples of automated biometrics include fingerprint, face, iris scan, and speech recognition (voice print). As a biometric property is an intrinsic property of an individual, it is difficult to duplicate and nearly impossible to share. A biometric property of an individual can be lost only in the case of a serious accident.

Bibliography

[b-ITU-T X.509] Recommendation ITU-T X.509 (2012), *Information technology – Open Systems Interconnection – The Directory: Public-key and attribute certificate frameworks*.

[b-ITU-T X.1153] Recommendation ITU-T X.1153 (2011), *Management framework of a one time password-based authentication service*.

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

[b-ISO/IEC 19790] ISO/IEC 19790:2012, *Information technology – Security techniques – Security requirements for cryptographic modules*.

SERIES OF ITU-T RECOMMENDATIONS

Series A	Organization of the work of ITU-T
Series D	General tariff principles
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	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	Terminals and subjective and objective assessment methods
Series Q	Switching and signalling
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 and next-generation networks
Series Z	Languages and general software aspects for telecommunication systems

Printed in Switzerland
Geneva, 2015