

I n t e r n a t i o n a l T e l e c o m m u n i c a t i o n U n i o n

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

ITU-T X-SERIES RECOMMENDATIONS

DATA NETWORKS, OPEN SYSTEM COMMUNICATIONS AND SECURITY

PUBLIC DATA 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/>.

© ITU 2015

All rights reserved. No part of this publication may be reproduced, by any means whatsoever, without the prior written permission of ITU.

Table of Contents

		Page
1	Scope.....	1
2	References.....	1
3	Definitions	1
	3.1 Terms defined elsewhere	1
	3.2 Terms defined in this Recommendation.....	2
4	Abbreviations and acronyms	2
5	Conventions	3
6	Overview of multi-factor authentication	3
	6.1 Single-factor authentication.....	3
	6.2 Two-factor authentication	4
	6.3 Multi-factor authentication.....	4
	6.4 Combination of multi-factor authentication	5
	6.5 Authentication threats.....	5
	6.6 Criteria for selecting a multi-factor authentication method	7
	6.7 Features of multi-factor authentication mechanisms using a mobile device..	7
7	Security requirements for multi-factor authentication.....	8
	7.1 General	8
	7.2 Mobile device	9
	7.3 Secure element.....	9
	7.4 Service provider.....	9
8	Generic mechanisms	10
	8.1 Entities.....	10
	8.2 Operations.....	11
	8.3 Authentication models.....	12
	8.4 Protocols	18
	Appendix I – Typical scenario for two-factor authentication	23
	Appendix II – Instances of components of multi-factor authentication.....	24
	II.1 Smart-card	24
	II.2 Digital certificate	24
	II.3 Biometrics.....	24
	Bibliography.....	25

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.