

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.1127

(09/2017)

SERIES X: DATA NETWORKS, OPEN SYSTEM
COMMUNICATIONS AND SECURITY

Secure applications and services (1) – Mobile security

Functional security requirements and architecture for mobile phone anti-theft measures

Recommendation ITU-T X.1127

ITU-T

ITU-T X-SERIES RECOMMENDATIONS
DATA NETWORKS, OPEN SYSTEM COMMUNICATIONS AND SECURITY

PUBLIC DATA NETWORKS	X.1–X.199
OPEN SYSTEMS INTERCONNECTION	X.200–X.299
INTERWORKING BETWEEN NETWORKS	X.300–X.399
MESSAGE HANDLING SYSTEMS	X.400–X.499
DIRECTORY	X.500–X.599
OSI NETWORKING AND SYSTEM ASPECTS	X.600–X.699
OSI MANAGEMENT	X.700–X.799
SECURITY	X.800–X.849
OSI APPLICATIONS	X.850–X.899
OPEN DISTRIBUTED PROCESSING	X.900–X.999
INFORMATION AND NETWORK SECURITY	
General security aspects	X.1000–X.1029
Network security	X.1030–X.1049
Security management	X.1050–X.1069
Telebiometrics	X.1080–X.1099
SECURE APPLICATIONS AND SERVICES (1)	
Multicast security	X.1100–X.1109
Home network security	X.1110–X.1119
Mobile security	X.1120–X.1139
Web security	X.1140–X.1149
Security protocols (1)	X.1150–X.1159
Peer-to-peer security	X.1160–X.1169
Networked ID security	X.1170–X.1179
IPTV security	X.1180–X.1199
CYBERSPACE SECURITY	
Cybersecurity	X.1200–X.1229
Countering spam	X.1230–X.1249
Identity management	X.1250–X.1279
SECURE APPLICATIONS AND SERVICES (2)	
Emergency communications	X.1300–X.1309
Ubiquitous sensor network security	X.1310–X.1319
Smart grid security	X.1330–X.1339
Certified mail	X.1340–X.1349
Internet of things (IoT) security	X.1360–X.1369
Intelligent transportation system (ITS) security	X.1370–X.1389
Distributed ledger technology security	X.1400–X.1429
Security protocols (2)	X.1450–X.1459
CYBERSECURITY INFORMATION EXCHANGE	
Overview of cybersecurity	X.1500–X.1519
Vulnerability/state exchange	X.1520–X.1539
Event/incident/heuristics exchange	X.1540–X.1549
Exchange of policies	X.1550–X.1559
Heuristics and information request	X.1560–X.1569
Identification and discovery	X.1570–X.1579
Assured exchange	X.1580–X.1589
CLOUD COMPUTING SECURITY	
Overview of cloud computing security	X.1600–X.1601
Cloud computing security design	X.1602–X.1639
Cloud computing security best practices and guidelines	X.1640–X.1659
Cloud computing security implementation	X.1660–X.1679
Other cloud computing security	X.1680–X.1699

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

Recommendation ITU-T X.1127

Functional security requirements and architecture for mobile phone anti-theft measures

Summary

Recommendation ITU-T X.1127 focuses on the functional security requirements and functional architecture for smartphone anti-theft mechanisms based on the general requirements described by the GSMA.

Smartphones are rapidly proliferating and have become a nearly indispensable part of daily life. Unfortunately, many smartphone users have had their phones stolen. A smartphone anti-theft measure, i.e., a kill switch tool, for use in the event it is lost or stolen, should provide the capability to:

- remotely delete the authorized user's data that is on the smartphone;
- render the smartphone inoperable to an unauthorized user;
- prevent reactivation without the authorized user's permission to the extent technologically feasible; and
- reverse the inoperability if the smartphone is recovered by the authorized user, and restore user data on the smartphone to the extent feasible.

History

Edition	Recommendation	Approval	Study Group	Unique ID*
1.0	ITU-T X.1127	2017-09-06	17	11.1002/1000/13259

Keywords

Anti-theft measures, mobile phone, security requirements.

* 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 2017

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 anti-theft measures.....	3
	6.1 Anti-theft measures	3
	6.2 High-level requirements for anti-theft measures	4
7	Functional architecture for mobile phone anti-theft measures	5
	7.1 Threats for mobile phone anti-theft measures	5
	7.2 Key security functions for mobile phone anti-theft measures.....	5
	7.3 Functional architecture for mobile device anti-theft measures	6
	7.4 Mechanisms for mobile phone anti-theft measures.....	7
8	Functional security requirements.....	9
	8.1 Overview	9
	8.2 Functional security requirements for the mobile device owner	9
	8.3 Functional security requirements for the authorized server	10
	8.4 Functional security requirements for the stolen mobile device.....	10
	8.5 Functional security requirements for the backup server.....	10
	Appendix I – General requirements for anti-theft measures.....	12
	I.1 Device owner.....	12
	I.2 Server.....	12
	I.3 Mobile device	13
	I.4 Device manufacture.....	13
	Appendix II – Additional security requirements for anti-theft measures	14
	II.1 Requirements for backup server	14
	Appendix III –.....	15
	III.1 Threats between the Anti-theft specific threats mobile device owner and the authorized server.....	15
	III.2 Threats between the authorized server and the anti-theft disabling agent.....	15
	III.3 Threats between the anti-theft disabling agent and the backup server.....	15
	Appendix IV – Scenario for anti-theft measures	16
	IV.1 Types of disabling features of mobile device.....	16
	IV.2 Enabling for stolen/lost mobile device	16
	IV.3 Disabling scenario for stolen/lost mobile device.....	16

Appendix V TLS profile for anti-theft measures	17
	Page
V.1 TLS protocol requirement	17
V.2 TLS cipher suites for interoperability.....	17
V.3 Digital certificates	17
Appendix VI – Overview of OMA device management	18
VI.1 OMA device management specification	18
Bibliography.....	19

Recommendation ITU-T X.1127

Functional security requirements and architecture for mobile phone anti-theft measures

1 Scope

This Recommendation addresses the functional security requirements and architecture for the smartphone anti-theft measure (i.e., a kill switch), which allows users to remotely delete their personal data or disable stolen or lost smartphone devices.

It is anticipated that functional security requirements and functional architecture identified in this Recommendation can be applicable to smartphones which are able to provide anti-theft measures reflecting the desires of smartphones customers, smartphone manufactures and mobile service operators.

This Recommendation focuses on the functional requirements, functional architecture, and anti-theft mechanisms. It uses a reference model consisting of the device owner, the authorized server, the backup server, and lost or stolen devices. Anti-theft specific threats are described in Appendix III. This Recommendation does not modify the general requirements for smartphone anti-theft features developed by GSMA [b-GSMA].

2 References

The following ITU-T Recommendations and other references contain provisions which, through reference in this text, constitute provisions of this Recommendation. At the time of publication, the editions indicated were valid. All Recommendations and other references are subject to revision; users of this Recommendation are therefore encouraged to investigate the possibility of applying the most recent edition of the Recommendations and other references listed below. A list of the currently valid ITU-T Recommendations is regularly published. The reference to a document within this Recommendation does not give it, as a stand-alone document, the status of a Recommendation.

[ITU-T X.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 data sanitization [b-NIST SP 800-88]: Actions taken to render data written on media unrecoverable by both ordinary and extraordinary means.

3.1.2 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]).

NOTE – The confidence is based on the degree of confidence in the binding between the entity and the identity that is presented.

3.1.3 identity [b-ITU-T X.1250]: The representation of an entity in the form of one or more information elements which allow the entity(s) to be sufficiently distinguished within context. For IdM purposes, the term identity is understood as contextual identity (subset of attributes), i.e., the variety of attributes is limited by a framework with defined boundary conditions (the context) in which the entity exists and interacts.

NOTE – Each entity is represented by one holistic identity, which comprises all possible information elements characterizing such entity (the attributes). However, this holistic identity is a theoretical issue and eludes any description and practical usage because the number of all possible attributes is indefinite.

3.1.4 kill switch [b-GSMA]: A way to disable crucial functions of a mobile device.

NOTE – It is essentially a function within the mobile equipment device, so that if triggered e.g., by a message of some format is sent to it, then the mobile device will cease to operate as it is intended to, and can only be reactivated or reused if the device owner authorizes the reactivation of the device.

3.1.5 mobile phone [b-ITU-T X-Sup.19]: An electronic device used for making phone calls and sending text messages across a wide geographic area through radio access to public mobile networks, while allowing the user to be mobile.

3.1.6 smartphone [b-ITU-T X-Sup.19]: A mobile phone with powerful computing capability, heterogeneous connectivity and advanced operating system providing a platform for third-party applications.

3.1.7 threat [b-ISO/IEC 27000]: potential cause of an unwanted incident, which may result in harm to a system or organization

3.1.8 tunnel [b-ISO/IEC 27033-1]: data path between networked devices which is established across an existing network infrastructure

NOTE – Tunnels can be established using techniques such as protocol encapsulation, label switching, or virtual circuits.

3.2 Terms defined in this Recommendation

This Recommendation defines the following terms:

3.2.1 device hardware: The physical components that together make a functioning mobile device including screen, keys, printed circuit board, chips, SIM card, removable storage, etc.

3.2.2 device software: All software programs on the device and SIM card, including applications, operating system, boot loader, boot-ROM, and firmware.

3.2.3 device user: The authorized user of the mobile device.

3.2.4 secure tunneling: A protocol that allows for the secure transfer of data or message from one network location to another.

NOTE – Secure tunneling generally supports entity authentication, message integrity, and message confidentiality.

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

ATM	Automated Teller Machine
CRL	Certificate Revocation List
DER	Distinguished Encoding Rules
DDoS	Distributed Denial-of-Service
DM	Device Management
EAA	Entity Authentication Assurance
GPS	Global Positioning System
GSMA	Groupe Speciale Mobile Association
HTTP	Hyper-Text Transfer Protocol
LoA	Level of Assurance

MAC	Message Authentication Code
OCSF	Online Certificate Status Protocol
OMA	Open Mobile Alliance
OTP	One-Time Password
PII	Personally Identifiable Information
PKI	Public-Key Infrastructure
SIM	Subscriber Identity Module
SMS-SC	Short Message Service – Service Centre
SSL	Secure Socket Layer
TCP	Transmission Control Protocol
TFA	Three-Factor Authentication
TLS	Transport Layer Security
U	Universal
UICC	Universal Integrated Circuit Card
USSD	Unstructured Supplementary Service Data
2FA	2-Factor Authentication

5 Conventions

This Recommendation applies the following verbal forms for the expression of provisions:

- a) "shall" indicates a requirement
- b) "should" indicates a recommendation
- c) "may" indicates a permission
- d) "can" indicates a possibility and a capability.

6 Overview of anti-theft measures

6.1 Anti-theft measures

Smartphones are rapidly proliferating and have become an indispensable part of daily life. However, millions of smartphone customers have had their phones stolen. A smartphone anti-theft measure, i.e., a kill switch tool, should provide the capability to:

- remotely delete the user's personal data that is on the smartphone in the event it is lost or stolen;
- render the smartphone inoperable to an unauthorized user;
- store user's personal data in the backup server, if necessary, which is operated by cellular service operators or device manufacturers;
- prevent reactivation without the authorized user's permission; and
- reverse the inoperability if the smartphone is recovered by the authorized user and restore user personal data on the smartphone to the extent feasible from the backup server.

Anti-theft software, installed in a mobile device, can disable a stolen or lost handset.

When a device owner becomes aware that their mobile device is lost or stolen, there are two scenarios for initiating execution of disablement features:

- 1) the device owner contacts their cellular service operator, which instructs the mobile device to be disabled; and