International Telecommunication Union

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 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 legder 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/.

Table of Contents

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
OCSP	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

2) the device owner runs an application on another mobile device, or accesses a disabling tool that renders the lost/stolen mobile device inoperable.

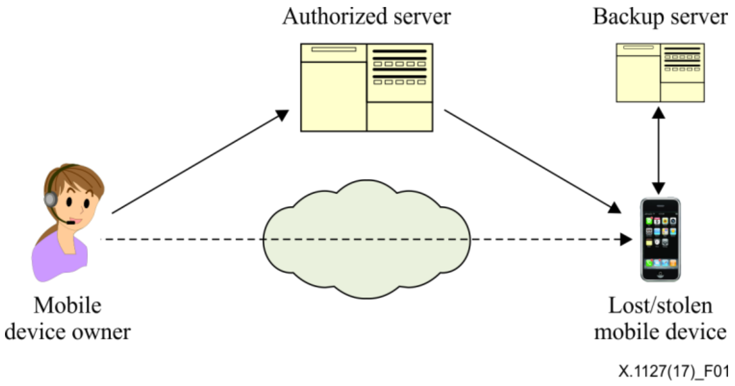


Figure 1 – Reference model for anti-theft measures

Figure 1 describes the reference model for anti-theft measures for mobile devices. The authorized server supports the disabling function for mobile devices, stolen or lost, and is operated by cellular service providers or device manufacturers. The authorized server sends the disabling instruction to the stolen/lost mobile device. The backup server restores the mobile device's personal data at the request of the device owner.

The communication between the lost/stolen mobile device and the authorized server should be protected using a secure tunnel (for example, secure socket layer (SSL)). In addition, the communication between the lost/stolen mobile device and the backup server should be protected using a secure tunnel (e.g., SSL).

This Recommendation is built on the entity authentication assurance (EAA) framework for managing EAA described in [ITU-T X.1254]. This EAA framework defines four levels of assurance (LoA) for entity authentication. Each LoA describes the degree of confidence in the processes leading up to and including the authentication process itself, thus providing assurance that the entity that uses a particular identity is, in fact, the entity to which that identity was assigned.

Some jurisdictions may request that anti-theft software should be installed or available for download. For example, in the United States, California is mandating that anti-theft software be installed on new phones but users will have the ability to disable the feature, although it will be enabled by default. By having the anti-theft feature be opt-out rather than opt-in, it is expected that many more customers will use the anti-theft measures and thus, the possibility that any given mobile device will be protected will be much higher.

6.2 High-level requirements for anti-theft measures

The high-level security requirements for anti-theft measures when transferring anti-theft messages from the authorized server to the mobile device are:

- entity authentication;
- message integrity;
- replay detection and sequence integrity;
- proof of receipt and proof of execution;
- message confidentiality; and
- indication of the security mechanisms used.

7 Functional architecture for mobile phone anti-theft measures

7.1 Threats for mobile phone anti-theft measures

This clause describes a set of identified security threats which are addressed by some requirements or mechanisms of this Recommendation. The security threat model and other fundamental materials have been addressed according to the following ITU-T Recommendations:

– [b-ITU-T X.800] defines the general security-related architectural elements that can be applied appropriately under the circumstances wherein the protection of communication between open systems is required.

– [b-ITU-T X.805] defines the network security architecture for providing end-to-end network security.

[b-ITU-T X.800] and [b-ITU-T X.805] identify the following security threats to the networks:

– destruction of information and/or other resources;

– corruption or modification of information;

– theft, removal, or loss of information and/or other resources;

– disclosure of information;

– interruption of services.

This Recommendation identifies the following threats specific to mobile phone anti-theft measures:

– unauthorized request to delete data on a disabled mobile phone;

– unauthorized request to disable the mobile phone;

– unauthorized disclosure of sensitive data on a mobile phone;

– loss of user data on a mobile phone;

– unauthorized access and/or modification to the functions of, or data on, a disabled device;

– unauthorized disclosure of user data and software exchanged between device and network operator and/or disabling tool for anti-theft measure;

The risks are as follows:

– hackers could find a way to hijack, disable instructions and turn off the mobile device;

– the personal data stored in the backup server or in transit between the mobile device and the backup server could be disclosed.

7.2 Key security functions for mobile phone anti-theft measures

The functions to disable a mobile device shall only be executed from an authorized server or a disabling tool supporting the disable function. In order to fulfil this requirement, the following five functions are required:

1) a secure communication connection between the device and server;

2) entity authentication by the server of the device;

3) entity authentication by the device of the server and the server being authorized to perform the function;

4) location tracking of the stolen mobile device; and

5) secure backup/deletion of data on a disabled mobile phone.

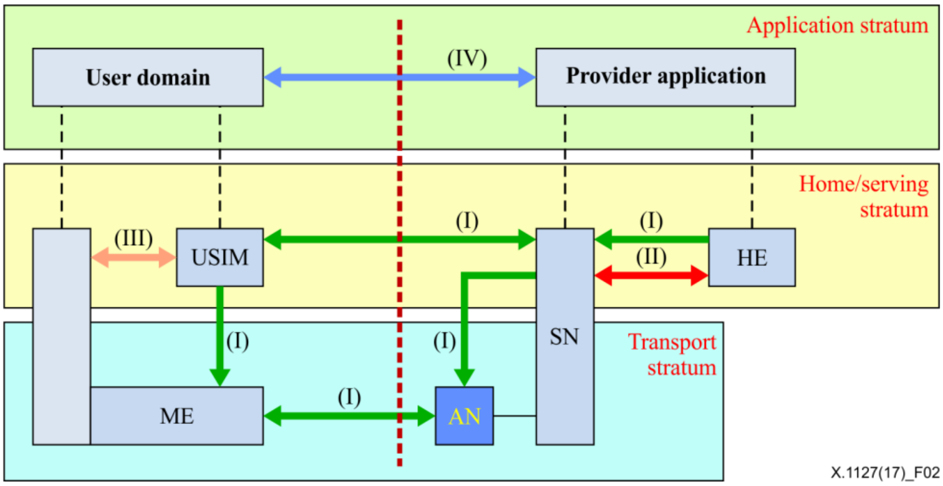
A mechanism should be provided through the personal website to allow device owners to manage personally identifiable information (PII) to be stored by the device owner. The application installed in the mobile device may be provided to the device owner. The anti-theft application may allow device owners to select data including PII for anti-theft and involve automatic backups of data including PII to a cloud-based storage solution. The procedure for this management consists of the following three steps:

1) installation of applications on the mobile device;
2) registration to the website by mobile service providers or device manufacturers;
3) management (i.e., deletion, downloading, uploading) of PII stored in the backup server through the personal website.

7.3 Functional architecture for mobile device anti-theft measures

The functional architecture for mobile device anti-theft measures is based on the security architecture described in [b-3GPP TS 33.102]. Figure 2 describes the security architecture consisting of five security groups as follows:

1) network access security (I): The set of security features that provide users with secure access to 3G services, and which in particular protect against attacks on the (radio) access link;
2) network domain security (II): The set of security features that enable nodes in the provider domain to securely exchange signalling data, and protect against attacks on the wireline network;
3) user domain security (III): The set of security features that secure access to mobile stations;
4) application domain security (IV): The set of security features that enable applications in the user and in the provider domain to securely exchange messages;
5) visibility and configurability of security (V): The set of features that enable the user to be informed of whether a security feature is in operation or not and whether the use and provision of services should depend on the security feature.



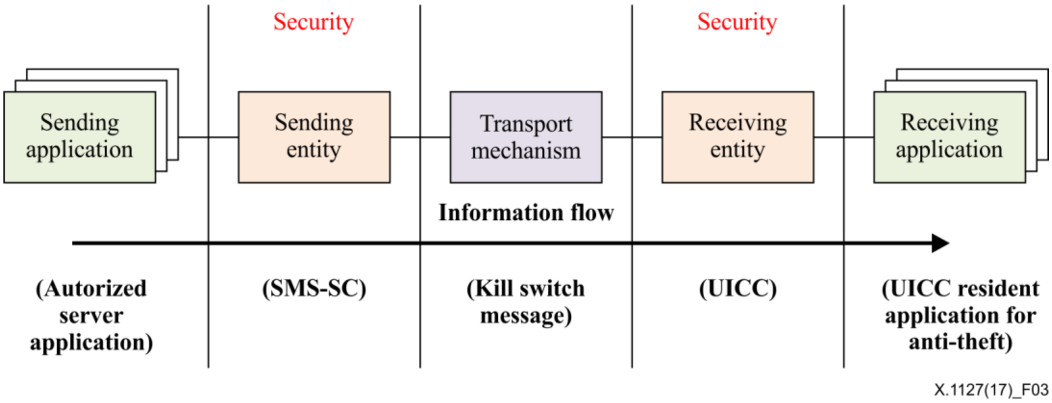
NOTE – Figure 2 is taken from [b-3GPP TS 33.102].

Figure 2 – Security architecture

The application for anti-theft measures in the mobile device is part of the set of applications which reside in the user domain, while the anti-theft function in the service provider is part of the set of applications residing in the provider application.

The security reference model for anti-theft measures is based on one described in [b-3GPP TS 22.048]. The sending application is an entity generating an application message to be sent, while the sending entity is the entity from which the secured packet originates (e.g., short message service – service centre (SMS-SC), universal integrated circuit card (UICC), unstructured supplementary service data (USSD) entry point, or dedicated universal (U) subscriber identity module (SIM) toolkit server) and where the security mechanisms are invoked. The sending entity generates the secured packets to be sent. Secured packets are transmitted through the transport-level secure tunnel or application-level secure tunnel.

The receiving application is the entity to which the application message is destined while the receiving entity is the entity where the secured packet is received (e.g., SMS-SC, UICC, USSD entry point, or dedicated (U)SIM toolkit.



NOTE – Figure 3 is taken from [b-3GPP TS 22.048].

Figure 3 – Security reference model

In this Recommendation, the security architecture is based on the reference model in Figure 1, the security architecture in Figure 2 and the security reference model in Figure 3.

7.4 Mechanisms for mobile phone anti-theft measures

7.4.1 Mechanisms for secure communication

The lost or stolen device should act as an authentication server, a client of secure tunnel.

The communication channel between the client and server should meet the following six security requirements:

1) confidentiality: The secure tunnel should ensure that data cannot be read by unauthorized entities. This is accomplished by encrypting data using a cryptographic algorithm and a secret key – a value known only to the two entities exchanging data. Data can only be decrypted by an entity who has the secret key.

2) integrity: The secure tunnel should determine if data have been changed (intentionally or unintentionally) during transit. The integrity of data shall be assured by generating a message authentication code (MAC) value, which is a keyed cryptographic checksum of the data. If data are altered and the MAC is recalculated, the old and new MACs will differ.

3) peer authentication: Each endpoint shall confirm the identity of the other endpoint with which it wishes to communicate, ensuring that the network traffic and data are being sent from the expected host. Secure tunnel authentication is typically performed one-way, authenticating the server to the client; however, a secure tunnel requires authentication for both endpoints.

4) replay protection: The same data shall not be delivered multiple times, and data shall not be delivered grossly out of order. A sequence number or a counter could be used at the source of a message. The source or the message adds a sequence number to its packet starting at 0 and increments every time it sends another message.

5) traffic analysis protection: A person monitoring network traffic shall not determine the content of the network traffic or how much information is being exchanged. A secure tunnel can also conceal which parties are communicating, whereas SSL leaves this information

exposed. Frequency of communication may also be protected depending on implementation. Nevertheless, the number of packets being exchanged can be counted.

6) access control: The endpoints of the secure tunnel shall perform filtering to ensure that only authorized users can access particular network resources. The endpoints of the secure tunnel may also allow or block certain types of network traffic, such as allowing web server access but denying file sharing.

To meet the above requirements, the use of transport layer security (TLS) for securing communication between the mobile device and the authorized server is recommended. TLS is a protocol that provides a secure communication tunnel over networks. It allows client/server applications to communicate in a way that is designed to prevent eavesdropping, tampering, or message forgery. TLS is positioned on top of reliable transport protocols (e.g., transmission control protocol (TCP)), and is used for encapsulation of various higher-level protocols (e.g., hyper-text transfer protocol (HTTP)).

TLS consists of three basic phases:

1) peer negotiation for algorithm support;

2) key exchange and authentication;

3) symmetric cipher encryption and message authentication.

The detailed profile for TLS is given in Appendix V.

In addition, this Recommendation also recommends the use of the secure communication channel based on the Open Mobile Alliance (OMA) protocol.

7.4.2 Mechanisms for mutual authentication

Authentication serves to confirm the identities of communicating entities. There are three types of authentication factors:

1) knowledge factor ("something only a user knows"), such as passwords;

2) possession factor ("something only a user has"), such as automated teller machine (ATM) cards; and

3) inherence factor ("something only a user is"), such as biometrics.

[b-ITU-T X.1158] describes three types of authentication methods:

1) single-factor authentication (SFA) is the traditional method that requires only a username and password before granting access to the user;

2) two-factor authentication (2FA) is based on using the combination of two different authentication factors. These factors may be something that a user knows, something that a user has or something that a user is. A good example, from everyday life, is that when a user wants to withdraw money from a cash machine, only the correct combination of a bank card (something that a user has) and a personal identification number (PIN), i.e., something that a user knows, allows the transaction to be conducted;

3) three-factor authentication (TFA) is based on using the combination of three independent different factors: what a user knows (password), what a user has (security token) and what a user is (biometric verification).

Multi-factor authentication is based on using a combination of two or more independent different factors. Two-factor authentication and TFA are a part of multi-factor authentication.

7.4.3 Mechanisms for secure data deletion

Sanitization refers to a process that renders access to target data on the media infeasible for a given level of effort [b-NIST SP 800-88]. [b-NIST SP 800-88] provides three categories of sanitization as follows:

1) clear operation: Applies logical techniques to sanitize data in all user-addressable storage locations for protection against simple non-invasive data recovery techniques; typically applied through the standard Read and Write commands to the storage device, such as by rewriting with a new value or using a menu option to reset the device to the factory state (where rewriting is not supported);
2) purge operation: Applies physical or logical techniques that render target data recovery infeasible using state of the art laboratory techniques;
3) destroy operation: Renders target data recovery infeasible using state of the art laboratory techniques and results in the subsequent inability to use the media for storage of data.

The Clear operation overwrites media by using organizationally approved software and performs verification on the overwritten data. The Clear pattern should be at least a single write pass with a fixed data value, such as all zeros. Multiple write passes or more complex values may optionally be used.

8 Functional security requirements

8.1 Overview

- the functional architecture is required to be built on the EAA framework described in [ITU-T X.1254];
- the functional architecture is required to provide a secure tunnel (for example, TLS described in [b-IETF RFC 6460] or secure communication channel based on the OMA protocol) for communication between components;
- the functional architecture is required to provide a secure key management (for example, based on public-key infrastructure (PKI) described in [b-ITU-T X.509]) for supporting secure tunnels;
- the functional architecture is required to support at least LoA 2 entity authentication mechanism described in [ITU-T X.1254];
- the functional architecture is required to support at least LoA 2 entity enrolment described in [ITU-T X.1254];
- the functional architecture is required to support at least LoA 2 entity credential management described in [ITU-T X.1254];
- the functional architecture is required to support message authentication for messages transferred;
- the functional architecture is required to support anti-replay attack for messages transferred;
- the functional architecture is required to support capability to backup device data to the secure network server;
- the functional architecture is required to provide a strong authorization (access control);
- the functional architecture is required to support security mechanisms described in [b-3GPP TS 22.048];
- the functional architecture is required to provide identity management for the mobile device owner, authorized server and mobile devices stolen.

8.2 Functional security requirements for the mobile device owner

- the mobile device owner is required to be authenticated to the authorized server based on at least 2FA (for example, ID/PW and one-time password (OTP) described in [ITU-T X.1254]);

- the mobile device owner is required to be identified using at least LoA 2 entity enrolment procedure described in [ITU-T X.1254];
- the functional architecture of the device owner is required to authenticate the authorization server using at least LoA 2 authentication mechanism described in [ITU-T X.1254];
- the functional architecture of the device owner is required to support a secure tunnel (for example, TLS described in [b-IETF RFC 6460] or secure communication channel based on OMA protocol) for communication of transferred message with the authorized server.

8.3 Functional security requirements for the authorized server

- the functional architecture of the authorized server is required to authenticate the device owner using at least a 2FA mechanism (for example, LoA 3 authentications described in [ITU-T X.1254]);
- the functional architecture of the authorized server is required to be authenticated by the mobile device stolen using at least a 2FA mechanism (for example, LoA 3 authentications described in [ITU-T X.1254]);
- the functional architecture of the authorized server is required to support a secure tunnel (for example, TLS described in [b-IETF RFC 6460] or secure communication channel based on OMA protocol) for communication of message with the mobile device owner;
- the functional architecture of the authorized server is required to support secure tunnel for communication of transferred message with the mobile device stolen.

8.4 Functional security requirements for the stolen mobile device

- the functional architecture of the stolen mobile device is required to support a secure tunnel (for example, TLS described in [b-IETF RFC 6460] or secure communication channel based on the OMA protocol) for communication of transferred message with the authorized server;
- the functional architecture of the stolen mobile device is required to be authenticated to the authorized server using at least a 2FA mechanism (for example, LoA 3 authentications described in [ITU-T X.1254];
- the functional architecture of the stolen mobile device is required to authenticate the authorized server using at least a 2FA mechanism (for example, LoA 3 authentications described in [ITU-T X.1254];
- the functional architecture of the stolen mobile device is required to invoke a feature to backup all device data that belongs to the owner to a secure network server;
- the functional architecture of the stolen mobile device is required to implement the access control mechanisms for launching instructions received from the authorized server;
- the functional architecture of the stolen mobile device is required to protect data or functions from access and use by unauthorized entity;
- the functional architecture of the stolen mobile device is required to support the clear operation for secure data deletion described in clause 7.4.3 once it receives the instruction to delete data in the mobile device from the authorized server.

8.5 Functional security requirements for the backup server

- the functional architecture of the backup server is required to support a secure tunnel for transferring messages with the mobile device;
- the functional architecture of the backup server is required to authenticate the mobile device using a robust authentication mechanism, which is to backup device data, if necessary;
- the functional architecture of the backup server is required to be authenticated by the mobile device using a robust authentication mechanism;

- the functional architecture of the backup server is required to support capability to backup appropriate device data from the mobile device;
- the functional architecture of the backup server is required to provide sufficient resources (i.e., storage) to the mobile device.

Appendix I

General requirements for anti-theft measures

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

[b-GSMA] provides general requirements for information for anti-theft measures. This appendix describes these requirements.

I.1 Device owner

- to confirm that the device has been irretrievably lost or stolen (e.g., global positioning system (GPS) coordinates show the device in a location unknown by the owner), the owner is required to start the procedure to disable service, after conducting the following:
  - signalling the device to emit a loud tone for a prolonged period (30 seconds to 3 minutes) to allow the owner an opportunity to locate the device, assuming it is within earshot,
  - displaying a message on the device lock/home screen asking for return of the device,
  - finding the location of the device using GPS (or any other location technology if this feature is supported by the device) and showing the location on a map;
- the owner is required to explicitly be 'opted-out' of the device-disabling feature but is required to be 'opted-in' as a default;
- on initial start-up and set-up of the mobile device, a short tutorial is recommended to be shown to the owner to educate them on general safe behaviour when using and storing the new device. Completion of the tutorial should be necessary before service activation;
- the device owner is recommended to be able to access and invoke a device-disabling function via the use of self-service capabilities, without needing to involve the network operator;
- a device owner is recommended to be unable to re-enable a device if it was disabled by the operator;
- the owner may invoke a feature to backup all device data that belongs to the owner (personal data), to a secure network server;
- the owner is required to have the ability to remotely render all device data inaccessible;
- the owner is required to have the ability to remotely delete user data (e.g., pictures, videos, phonebook, e-mails) from the device. If user data is strongly encrypted, then wiping the encryption key from the device is sufficient;
- for lost or stolen devices registered on a visited network (roaming), the owner may be advised of any additional costs when attempting to invoke functions to backup data, disable the device, or to restore the device;
- an unauthorized user is required to be unable to access the functions of, or data on, a disabled device;
- a function to display a custom message on the home/lock screen of the device when the device is not in the owner’s possession should be made available to the owner.

I.2 Server

- a network operator is required to authenticate a request from a device owner to initiate disabling a device;
- an owner request to disable a device is required to be authenticated and is only required to control the device which is registered to that owner;
- the location and access to servers supporting the disable feature is required to be secure;

- only authorized personnel with sufficient training are recommended to be allowed to access and invoke the disabling functions;
- the server is required to generate and retain logs of all disable requests received;
- when restoring service to a re-enabled device that was previously disabled, the owner's backed-up data and applications are required to be restored to the device;
- owner data that have been backed-up are required to be stored securely and the confidentiality and integrity of the data guaranteed;
- once an owner has requested their device to be disabled, they can expect the function to complete execution in less than 15 minutes, if the device can be successfully authenticated;
- factory reset cannot be used as a means to bypass anti-theft measures.

I.3 Mobile device

- the request to disable a device is required to be verified as authentic before proceeding to the next steps toward device disablement;
- the mechanism to disable a mobile device is required to be executed from an authorized server supporting the disable function. In order to fulfil this requirement, the following is needed:
  - a secure connection between the device and server;
  - authentication by the server of the device;
  - authentication by the device of the server and the server being authorized to perform the function;
- the mobile device, on initial start-up and setup is required to explicitly guide the owner through the setup of anti-theft features and any other relevant security features such as device access control mechanisms;
- the device is required to have the capability to have service re-enabled by the legitimate owner after it has been disabled. It is required not to be capable of being re-enabled by anyone who is not the rightful owner;
- the device disable function is recommended to be operable when a device is not connected to a public land mobile network but is connected to the Internet;
- for lost or stolen devices registered on a visited network (roaming), all functions for backing-up data, disabling the device and restoring the device is required to function successfully.

I.4 Device manufacture

- device manufacturers are recommended to continue to implement and evolve measures to deter and prevent the unauthorized re-initialization of a lost or stolen device to a state where it can be used by someone other than the owner.

Appendix II

Additional security requirements for anti-theft measures

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

II.1 Requirements for backup server

– the mechanism is required to be executed from a backup server supporting storing PII of the stolen/lost mobile devices. In order to fulfil this requirement, the following is needed:

  - a secure connection between the device and backup server;
  - authentication by the backup server of the mobile device;
  - authentication by the device of the backup server.

Appendix III

Anti-theft specific threats

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

III.1 Threats between the mobile device owner and the authorized server

- impersonation of device owner. An improper disable instruction is delivered to the authorized server by an attacker that is impersonating the device owner. The attack which exploits this threat can cause innocent mobile devices to be disabled;
- tampering/eavesdropping/replaying of a message. An improper disable instruction is delivered to the authorized server; the content of the instruction message is revealed to the attacker who is able to eavesdrop on the communication; or enormous traffic is sent resulting in distributed denial-of-service (DDoS) attacks to the authorized server;
- impersonation of authorized server. Either authentication credential of the legitimate device owner is revealed or disabling instruction of the legitimate device owner is delivered to the impersonated authorized server. The attack which exploits this threat can cause innocent mobile devices to be disabled.

III.2 Threats between the authorized server and the anti-theft disabling agent

- impersonation of authentication server. An improper disable instruction is delivered to the stolen mobile device;
- tampering/eavesdropping/replaying of a message. An improper disable instruction is delivered to the anti-theft disabling agent; the content of the instruction message is revealed to the attacker which is able to eavesdrop on the communication; or enormous traffic is sent resulting in DDoS attacks to the disabling agent;
- impersonation of disabling agent. Either authentication credential of the legitimate authorized server is revealed to, or a disable instruction of the legitimate device owner is delivered to the impersonated disabling agent.

III.3 Threats between the anti-theft disabling agent and the backup server

- impersonation of anti-theft disabling agent. The backup message stored in the backup server is revealed to the impersonated disabling agent;
- tampering/eavesdropping/replaying of a message. The backup information is altered and revealed to the attacker which is able to eavesdrop on the communication;
- impersonation of backup server. The backup information is revealed to the impersonated backup server.

Appendix IV

Scenario for anti-theft measures

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

IV.1 Types of disabling features of mobile device

There are two types of disabling features:

1) a "hard" disabling feature which renders a stolen mobile device permanently unusable;

2) a "soft" disabling feature which only makes a mobile device unusable to "an unauthorized user".

IV.2 Enabling for stolen/lost mobile device

Anti-theft features require active involvement of the mobile device owner. When a device owner purchases a new mobile device, and subscribes to a cellular provider, they should configure the mobile device to enable the anti-theft feature.

IV.3 Disabling scenario for stolen/lost mobile device

If a mobile phone is stolen or lost, the device owner contacts their cellular service provider or uses a website operated by the cellular operator, known as an authorized server, to send a "device disabling" instruction to the mobile device. This instruction will lock the mobile device and, if the device owner chooses, could also erase some personal data from the mobile device or allow the backup server to store some personal data.

The device disabling instruction will render the device inoperable on the network of any provider of commercial mobile services or commercial mobile data service globally, even if the device is turned off or has the data storage medium removed.

The only way to restore a locked device will be with a password supplied by the phone's owner.

Appendix V

TLS profile for anti-theft measures

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

This appendix provides a minimum TLS profile for anti-theft measures. The typical example of the TLS profile is given in [b-IETF RFC 6460] and [b-ISO/IEC 20648].

V.1 TLS protocol requirement

– the anti-theft scheme acting as a server is recommended to implement the TLS protocol; however, its use by clients is optional. TLS version 1.2 (specified in [b-IETF RFC 5246]) or later is required to be implemented.

V.2 TLS cipher suites for interoperability

– the anti-theft scheme shall not use MD5 or SHA-1 as the default keyed-hash message authentication code (HMAC);

– the anti-theft scheme shall not use RC4 as the default cryptographic algorithm;

NOTE – [b-IETF RFC 7465] bans the use of RC4.

– the anti-theft scheme is required to support: selection and use of signature/hash algorithm pairs, using the signature algorithms supported in TLS 1.2 and use of SHA-256 or greater strength hashes;

– the anti-theft scheme is required to use cipher suites that have at least 112 bits of security strength. In addition, the following cipher suites is required to be supported:

- TLS_RSA_WITH_AES_128_CBC_SHA256 {0x00, 0x3C}.

V.3 Digital certificates

The anti-theft scheme is required to support [b-ITU-T X.509] version 3 public key certificates that are conformant with the Certificate and Certificate Extension Profile defined in section 4 of [b-IETF RFC 5280].

– the TLS server in the anti-theft scheme is required to support server certificates;

– the TLS client in the anti-theft scheme is recommended to support client certificates;

– the anti-theft scheme is required to support key sizes of 2048 bits or greater, for RSA/DSA server [b-ITU-T X.509] certificates;

– the anti-theft scheme is required to support distinguished encoding rules (DER) encoded [b-ITU-T X.509], Base64 encoded [b-ITU-T X.509], and PKCS#12 [b-IETF RFC 7292] certificate formats;

– the anti-theft scheme is required to support certificate validation as described in section 6 of [IETF RFC 5280], which are presented a digital certificate. In addition, one of the following approaches shall be used to determine whether a certificate has been revoked:

- option 1: use of certificate revocation lists (CRLs): supported CRLs in the DER encoded [b-ITU-T X.509] or the Base64 encoded [b-ITU-T X.509] formats and valid CRLs stored locally (distribution out of scope for this standard) or retrieved from an external source (e.g., a CRL distribution point (CRLDP)),

- option 2: use of a certificate-status protocol such as online certificate status protocol (OCSP) in one of the following ways: directly use the OCSP as described [b-IETF RFC 6960] and indirectly using OCSP through the certificate status request extension to TLS described in section 8 of [b-IETF RFC 6066].

Appendix VI

Overview of OMA device management

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

This appendix provides an overview of device management (DM) protocol defined by OMA [b-OMA-DM].

VI.1 OMA device management specification

OMA DM specification is designed for management of mobile devices such as mobile phones, PDAs, and tablet computers. Device management is intended to support the following uses:

- provisioning: Configuration of the device (including first-time use), enabling and disabling features;
- device configuration: Allow changes to settings and parameters of the device;
- software upgrades: Provide for new software and/or bug fixes to be loaded on the device, including applications and system software;
- fault management: Report errors from the device, query about status of device.

All of the above functions are supported by the OMA DM specification, and a device may optionally implement all or a subset of these features. Since the OMA DM specification is aimed at mobile devices, it is designed with sensitivity to the following:

- small footprint devices, where memory and storage space may be limited;
- constraint on bandwidth of communication, such as in wireless connectivity;
- tight security, as the devices are vulnerable to software attacks; authentication and challenges are made part of the specifications.

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.800] Recommendation ITU-T X.800 (1991), *Security architecture for Open Systems Interconnection for CCITT applications*.

[b-ITU-T X.805] Recommendation ITU-T X.805 (2003), *Security architecture for systems providing end-to-end communications*.

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

[b-ITU-T X.1250] Recommendation ITU-T X.1250 (2009), *Baseline capabilities for enhanced global identity management and interoperability*.

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

[b-ITU-T X-Sup.19] ITU-T X-series Recommendations – Supplement 19 (2013), *Supplement on security aspects of smartphones*.

[b-ISO/IEC 20648] ISO/IEC 20648:2016, *Information technology – TLS specification for storage systems*.

[b-ISO/IEC 27000] ISO/IEC 27000:2016, *Information technology – Security techniques – Information security management systems – Overview and vocabulary*.

[b-ISO/IEC 27033-1] ISO/IEC 27033-1:2009, *Information technology – Security techniques – Network security – Part 1: Overview and concepts*.

[b-3GPP TS 22.048] 3GPP TS 22.048 (2003), *Security mechanisms for the (U)SIM Application Toolkit*, June 2003.

[b-3GPP TS 33.102] 3GPP TS 33.102 (2009), *3G Security; Security architecture (Release 9)*, December 2009.

[b-IETF RFC 5246] IETF RFC 5246 (2008), *The Transport Layer Security (TLS) Protocol Version 1.2*.

[b-IETF RFC 5280] IETF RFC 5280 (2008), *Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile*.

[b-IETF RFC 6066] IETF RFC 6066 (2011), *Transport Layer Security (TLS) Extensions: Extension Definitions*.

[b-IETF RFC 6460] IETF RFC 6460 (2012), *Suite B Profile for Transport Layer Security (TLS).*

[b-IETF RFC 6960] IETF RFC 6960 (2013), *ITU-T X.509 Internet Public Key Infrastructure Online Certificate Status Protocol – OCSP*.

[b-IETF RFC 7292] IETF RFC 7292 (2015), *PKCS #12 Personal Information Exchange Syntax v1.1*.

[b-IETF RFC 7465] IETF RFC 7465 (2015), *Prohibiting RC4 Cipher Suites*.

[b-GSMA] GSMA, *SG.24 Anti-Theft Device Feature Requirements v3.0*, 17 May 2016.

[b-OMA-DM] Open Mobile Alliance, *OMA Device Management V1.2*, April 2013.

[b-NIST SP 800-88] NIST, *NIST Special Publication 800-88 Revision 1: Guidelines for Media Sanitization*, December 2014.

SERIES OF ITU-T RECOMMENDATIONS

Series A	Organization of the work of ITU-T
Series D	Tariff and accounting principles and international telecommunication/ICT economic and policy issues
Series E	Overall network operation, telephone service, service operation and human factors
Series F	Non-telephone telecommunication services
Series G	Transmission systems and media, digital systems and networks
Series H	Audiovisual and multimedia systems
Series I	Integrated services digital network
Series J	Cable networks and transmission of television, sound programme and other multimedia signals
Series K	Protection against interference
Series L	Environment and ICTs, climate change, e-waste, energy efficiency; construction, installation and protection of cables and other elements of outside plant
Series M	Telecommunication management, including TMN and network maintenance
Series N	Maintenance: international sound programme and television transmission circuits
Series O	Specifications of measuring equipment
Series P	Telephone transmission quality, telephone installations, local line networks
Series Q	Switching and signalling, and associated measurements and tests
Series R	Telegraph transmission
Series S	Telegraph services terminal equipment
Series T	Terminals for telematic services
Series U	Telegraph switching
Series V	Data communication over the telephone network
Series X	**Data networks, open system communications and security**
Series Y	Global information infrastructure, Internet protocol aspects, next-generation networks, Internet of Things and smart cities
Series Z	Languages and general software aspects for telecommunication systems

Printed in Switzerland
Geneva, 2017