Telecommunications Standards Advisory Committee (TSAC)

Technical Specification

Security Requirements for Cellular Devices

Draft IMDA TS CD-SEC
Issue 1, February 2020

Info-communications Media Development Authority
10 Pasir Panjang Road
#03-01 Mapletree Business City
Singapore 117438

Acknowledgement

The Info-communications Media Development Authority (IMDA) and the Telecommunications Standards Advisory Committee (TSAC) would like to acknowledge the following members of the TSAC Focus Area (FA) 7 Secured Devices Task Force (TF) for their invaluable contributions to the preparation of this Technical Specification:

Draft IMDA TS Security Requirements for Cellular Devices Issue 1, February 2020	Technical Specification for Security Requirements for Cellular Devices
Focus Area 7 Chairperson	Mr Lin Yih, Director, Digital Applied Research & Technology
Secured Devices Task Force Chairperson	Mr Daryl Chiam, Director, Singtel Mobile Singapore Pte Ltd
Chief Editor	Dr Guo Huaqun, Senior Scientist and Head of Network Security Unit, Institute for Infocomm Research (I^2R), A*STAR
Editors	Mr Karthikeyan Shanmuganandam, Head of New Businesses and Enterprise, Ericsson Telecommunications Pte Ltd
	Mr Paul Soon, Managing Consultant, Huawei International Pte Ltd
	Mr Bernard Low, Senior Manager, Info-communications Media Development Authority
	Mr Philip Ng, Assistant Director, Info-communications Media Development Authority
	Ms Zhang Keli, Senior Manager, Singtel Mobile Singapore Pte Ltd
Secretary	Ms Kong Pei Wee, Senior Manager, Info-communications Media Development Authority

List of TSAC FA 7 Secured Devices Task Force Members (2018-2021)

S/N	Organisation	Name
1	Association of the Telecommunications Industry of Singapore (ATIS)	Mr Yip Yew Seng, Honorary Secretary and Member
2	Cisco Systems Singapore	Mr Sunil Pereira-Alury, Strategic Account Manager
3	Cisco Systems Singapore	Mr Jason Chao, APJC Head
4	Fortinet Inc.	Mr Robin Liao, Technical Marketing Director
5	M1 Limited	Mr Jeff Chong Kok Vun, Principal Engineer
6	Quectel Wireless Solutions Co. Ltd	Mr Kenny Lau, Overseas Sales Director (South-east Asia)
7	StarHub Ltd	Mr Sudhir Menon, Senior Business Development Director
8	TPG Telecom	Mr Dennis Woo, Core Network Manager

Telecommunications Standards Advisory Committee (TSAC)

The TSAC advises IMDA on the setting of ICT standards as well as on the development and recommendation of specifications, standards, information notes, guidelines and other forms of documentation for adoption and advancement of the standardisation effort of the Singapore ICT industry (hereafter termed "IMDA Standards").

Telecommunications standards-setting in Singapore is achieved with the assistance of TSAC, where professional, trade and consumer interest in telecommunications standards is represented on the TSAC with representatives from network and service operators, equipment suppliers and manufacturers, academia and researchers, professional bodies and other government agencies.

List of TSAC Members (2018-2021)

TSAC Chairman:

Mr Raymond Lee	Director (Infocomm Resource & Technology) Info-communications Media Development Authority

TSAC Members:

Mr Yip Yew Seng	Honorary Secretary Association of Telecommunications Industry of Singapore (ATIS)
Dr Kang Cheng Guan	Senior Director, Security & Emergency Planning Energy Market Authority (EMA)
Mr Jason Tan	Deputy Director Enterprise Singapore (ESG)
Mr Foong Sew Bun	Deputy CE, Services, Governance and Cybersecurity Government Technology Agency (GovTech)
Mr Hong Tse Min	Senior Assistant Director, Infocomm Resource & Technology Infocomm Media Development Authority (IMDA)
Dr Sun Sumei	Department Head, Communications & Network Department Institute for Infocomm Research (I2R)
Mr Peter Quek	Group Director - IT, Cybersecurity & Digital Services Land Transport Authority (LTA)
Mr Denis Seek	CTO M1 Limited
Mr Anil Nihalani	Head, Digital Products & Technology Mediacorp Pte Ltd
Prof Teh Kah Chan	Associate Professor Nanyang Technological University (NTU)
Mr Biplab Sikdar	Associate Professor National University of Singapore (NUS)
Mr Edmund Quek Han Yeow	Director, Radio Network Quality Singapore Telecommunications Ltd (Singtel)
Dr Peter Loh Kok Keong	Associate Professor and Deputy Programme Director, Infocomm Technology Cluster Singapore Institute of Technology (SIT)
Ms Sarah Tay	AVP, Mobile StarHub Ltd
Mr Kenneth Loh	Technical Manager TPG Telecom

This page is intentionally left blank.

Contents

Security Requirements for Cellular Devices

1 Scope

This Specification defines the minimum technical security requirements for the design and management of Devices implemented on cellular networks to better safeguard communication networks from security threats in the area of connection efficiency.

The scope of this IMDA Technical Specification also sets out to minimise the vulnerability of the individual cellular Devices, ensuring that these devices are better protected and secured in the areas of Access Control and Over-The-Air (OTA) updating.

2 References

For the technical requirements captured in this specification, references have been made to the following standards. Where versions are not indicated, implementation of this specification shall be based on current and valid versions of these standards published by the respective Standards Development Organisations.

[1] GSMA TS.34 v5.0: IoT Device Connection Efficiency Guidelines
[2] ENISA, Nov 2017: Baseline Security Recommendations for IoT in the context of Critical Information Infrastructures
[3] GSMA CLP.13: IoT Security Guidelines Endpoint Ecosystem Version 2.0 31 October 2017
[4] ETSI TS 102 226: Remote APDU structure for UICC based applications.
[5] GSMA SGP.02: Remote Provisioning Architecture for Embedded UICC Technical Specification.
[6] GSMA CLP.14: IoT Security Guidelines for Network Operators 2.0 31 October 2017

3 Definitions and Abbreviations

For the purpose of this specification, the following terms and definitions apply.

3.1 Definitions

Access Control	Functions which include identification, authentication, authorisation and accountability.
Device	Devices which are connected via a cellular network.
Network Storms	Network Storms occur when a node sends excessive amount of data in an uncontrolled manner, saturating the network capacity, and consequently causing the network to become unusable for its intended purpose.

3.2 Abbreviations

APDU	Application Protocol Data Unit
DDoS	Distributed Denial of Service
ENISA	European Union Agency for Network and Information Security
ETSI	European Telecommunications Standards Institute
eUICC	Embedded Universal Integrated Circuit Card
GGSN	Gateway GPRS Support Node
GPRS	General Packet Radio Services
GP-TM	Good Practices-Technical Measures
GSM	Global System for Mobile Communications
GSMA	GSM Association
HPLMN	Home PLMN (Public Land Mobile Network)

HLR	Home Location Register
HSS	Home Subscriber Server
IMSI	International Mobile Subscriber Identity
IoT	Internet of things
LTE	Long Term Evolution
MSU	Messaging Signal Units
NFM	Network Friendly Mode
OTA	Over-The-Air
PDP	Packet Data Protocol
SMS	Short Message Service
SMSC	Short Message Service Centre
SMS-MO	SMS- Mobile Originated
UICC	Universal Integrated Circuit Card

This Technical Specification applies the following verbal forms to express requirements:

— The keyword(s) **“shall”** or **"is required to"** indicate a requirement which must be strictly followed and from which no deviation is permitted if conformance to this Specification is to be claimed.

— The keyword(s) **“should”** or **"is recommended"** indicate an optional requirement which is not absolutely required. Thus, this requirement need not be present to claim conformance.

— The keyword **"may"** indicates an optional requirement which is permissible, without implying any sense of being recommended. It means the vendor may optionally provide or not provide the feature and still claim conformance with the Specification.

4 Security Requirements

4.1 Guard against Network Storms

To guard against Network Storms and ensure that the behaviour of Devices does not jeopardise network resilience, Devices in the network shall comply with the Connection Efficiency Requirements defined in section 7 of the GSMA TS.34 [1].

4.1.1 Correct Observation of Cause Codes in Reject Messages

TS.34_7.0_REQ_001 [1]: Devices shall correctly observe cause codes sent in reject messages from the network, and carry out the cause code behaviour as defined in section 7.5 of the GSMA TS.34 [1].

4.1.2 Network Friendly Mode (NFM)

TS.34_7.0_REQ_002 [1]: Devices shall comply with the requirements set out for the Network Friendly Mode (NFM) in section 7.1 of the GSMA TS.34 [1].

NFM is a feature used to regulate the number of times that the communications module in the Device can perform Network signalling requests including IMSI attach, GPRS attach, PDP Context activation and SMS-MO, as well as equivalent LTE signalling requests. This is to regulate and control the amount of Messaging Signal Units (MSU) generated toward network control plane elements such as HLR, HSS, GGSN, SMSC and HPLMN.

As provided for in TS.34_7.1_REQ_001 [1], <NFM Active> shall be set to 1 – Active; and <Start Time Active> shall be set to 1 – Enable Start Timer.

As provided for in TS.34_7.1_REQ_004 [1], Devices should utilise the standard default timeout parameters set out for the NFM iteration intervals.

4.1.3 Back-off Triggers

TS.34_7.0_REQ_003 [1]: Devices shall support Back-Off Triggers defined in section 7.2 of the GSMA TS.34 [1].

If the Device fails to attach to the cellular network, it shall not be allowed to continuously attempt to attach to the network. Continuous requests from a large number of Devices are capable of creating a signalling storm. The frequency of such network signalling re-attempts from the Device, and the duration between the re-attempts shall be controlled. The communications module of the Device shall monitor attempts to attach in a given timeframe and trigger the back-off timer if the number of attempts exceeds the allowable number in that timeframe. Should the number of attempts exceed the limit, back-off will be triggered and the Device shall not send further requests to the network until the back-off time has lapsed.

As provided for in TS.34_7.2_REQ_001 [1], the Back-off Timer Flag shall be enabled when back-off is triggered.

Apart from network attach attempts such as IMSI attach and GPRS attach, similar logic shall apply to other network signalling requests such as PDP Context Activate, SMS MO, and their equivalents.

4.1.4 Back-off Timer

TS.34_7.0_REQ_003 [1]: Devices shall support Back-Off Timer defined in section 7.3 of the GSMA TS.34 [1].

Back-off Timer provides the time-space between consecutive attempts by the Device to attach to the cellular network when its preceding attempt is a failure. The number of successive iterations of attempts shall be counted and stored in a Back-off Iteration Counter. The value of the Back-off Timer should be determined based on the value of Back-off Base

Interval for the given iteration, and a unique time value for that Device, preferably based on IMSI. Successive Back-off Base Interval values for each iteration shall have exponential delay. For example, if the first iteration is 60 seconds, then the second should be 120s, then 240s and so on.

As provided for in TS.34_7.3_REQ_001 [1], the NFM Flag in the communications module shall be set to 1 = Activated.

4.1.5 Logic Flow for Back Off Procedure

TS.34_7.0_REQ_004 [1]: The Device shall support the Logic Flow for Back Off Procedure as shown in section 7.4 of the GSMA TS.34 [1].

4.2 Controlled Access

Devices shall implement technical measures and best practices for controlled access by means of password and proper authentication. The following requirements are typical of industry practice and have been similarly described in ENISA Baseline Security Recommendations for IoT [2] and section 6.9 of the GSMA CLP.13 [3].

4.2.1 Unique Passwords for Device Access Control

Devices with default passwords can be easily compromised allowing an attacker to gain access into the communications module of the Device. The following measures ensure that passwords and authentication mechanisms used in Device access controls are adequately protected.

4.2.1.1 Password Requirements

(a) The length and complexity of the password shall:

i. Consist of 8 or more characters; and
ii. Contain characters from upper case (A through Z), lower case (a through z), digits (0 to 9) and optional special characters (!, $, #, %, etc.).

NOTE: Avoid frequently used dictionary words and their variants that substitute upper or lower case characters with digits and special characters that retains the visual appearance of the dictionary word. For example, "admin", "password", "P@ssw0rd", "Pa$$word123", etc.

(b) Consecutive identical characters in a password should not be used.

(c) Values used in the login ID and password shall not be the same.

(d) The Device should support password aging checks requiring users to change their password after a specified period.

(e) The Device shall not allow the current password to be re-used when changing its password.

(f) The Device should support password history checks requiring a new password be used upon password change and keeping a history of older passwords.

4.2.1.2 Default Password Handling

(a) The default password shall depend on the capability of the Device and the Device can either have:

i. A randomised and unique password for each Device, or
ii. no default password, but the Device must be in disabled state (non-functioning). Upon first use, the Device shall require the user to set a password that meets the password requirements.

(b) The password recovery or reset mechanism shall be protected and shall not supply an attacker with any form of information indicating a valid account (ENISA GP-TM-26 [2]).

4.2.1.3 Authentication Handling

(a) Upon initial setup or first login the default login credentials shall be changed, which include:

i. Password; and
ii. Where applicable, login ID.

(b) Password fields shall protect their contents from being copied.

(c) Password input visibility on the login interface shall follow GSMA CLP.13 [3] Section 6.9. In particular:

i. Passwords shall never be displayed on a user's screen and shall always be hidden with the asterisk character, or another benign glyph.
ii. The Device shall protect itself against brute force and/or other abusive login attempts (ENISA GP-TM-25 [2]). When the number of repeated input errors exceeds the threshold, one or more of the following protection measures can be employed, such as blocking the source IP address, enforcing a pre-configured IP address whitelist, login delay with increasingly prolonged periods after each subsequent attempt, and/or locking out the login account using password authentication.
iii. If the user is locked out, the Device should provide a fall back authentication mechanism to be used for regaining access such as 2FA (two-factor authentication) verification.

(d) Authentication credentials shall be salted, hashed and/or encrypted (ENISA GP-TM-24 [2]).

4.3 Secure over-the-air (OTA) update

The device can be compromised if it is booted up with firmware sent by attackers. Compromised Devices can cause DDoS attacks.

If the OTA application update process is not properly architected, it can result in adversaries remotely injecting executable code into endpoints. If the adversaries have a privileged position on the network, they could potentially affect thousands of endpoints at once. The result of the attack could range from simple code execution, to denial of service (bricking the endpoints), or completely altering the purpose of the endpoint Device.

All software components in the Devices should be securely updateable.

4.3.1 Secure Software/Firmware update over-the-air

Over the air update of Device, if implemented, shall meet the following requirements (ENISA GP-TM-18 [2]):

4.3.1.1 The update file shall not contain sensitive data such as hardcoded credentials, and shall be digitally signed by a trusted entity and transmitted via secure connections.

4.3.1.2 The Device shall verify the signed package before the update process begins.

In addition, section 7.5 of GSMA CLP.13 [3] should be referred to for the implementation of the OTA update process.

4.3.2 Secure UICC/eUICC update over-the-air

Remote management of UICC/eUICC should follow section 5.1.1 of the latest GSMA CLP.14 [6] guidelines.

4.3.2.1 Remote management of the UICC (Over-The-Air, OTA)

To be able to perform changes to the UICC remotely, the network operator or the supplier of UICC typically supports UICC OTA management based on the UICC OTA security mechanisms as described in the latest ETSI TS 102 226 [4] specification.

4.3.2.2 Remote Management of Embedded UICCs (eUICCs)

Devices that may be vulnerable to physical tampering should use eUICCs. The eUICC based Devices shall comply with the OTA security mechanism in the GSMA SGP.02 [5] specifications.

5 Implementation Table

Devices shall be able to support at minimum the features specified in the implementation table given below.

Note: "CR" indicates the "Compliance Requirement".

"M" indicates a Mandatory feature that shall be implemented according to the specified requirements.

"C" indicates that it is Conditional for the feature to be implemented according to the specified requirements, contingent on supplier's claimed capability of that device.

"O" indicates an Optional feature that should be implemented according to the specified requirements.

TS Clause Ref.	Features	CR	Complied with Yes / No	Remarks
4.1.1	Correct Observation of Cause Codes in Reject Messages TS.34_7.0_REQ_001	M		
4.1.2	Network Friendly Mode (NFM) TS.34_7.0_REQ_002	M		
	TS.34_7.1_REQ_001 <NFM Active> shall be set to 1 – Active; and <Start Time Active> shall be set to 1 – Enable Start Timer.	M		
	TS.34_7.1_REQ_002	M		
	TS.34_7.1_REQ_003	M		
	TS.34_7.1_REQ_004 Should utilise the standard default timeout parameters as set out for the NFM iteration intervals	M		
	TS.34_7.1_REQ_005	O		
	TS.34_7.1_REQ_006	M		
	TS.34_7.1_REQ_007	M		
	TS.34_7.1_REQ_008	M		
	TS.34_7.1_REQ_009	M		
	TS.34_7.1_REQ_010	M		
4.1.3	Back-off Triggers TS.34_7.0_REQ_003	M		
	TS.34_7.2_REQ_001 The Back-off Timer Flag shall be enabled when back-off is triggered.	M		
	TS.34_7.2_REQ_002	M		
	TS.34_7.2_REQ_003	M		
	TS.34_7.2_REQ_004	M		
4.1.4	Back-off Timer TS.34_7.0_REQ_003	M		
	TS.34_7.3_REQ_001 The NFM Flag in the Communications Module shall be set to 1 = Activated.	M		

TS Clause Ref.	Features	CR	Complied with Yes / No	Remarks
	TS.34_7.3_REQ_002	M		
	TS.34_7.3_REQ_003	M		
	TS.34_7.3_REQ_004	M		
	TS.34_7.3_REQ_005	M		
	TS.34_7.3_REQ_006	M		
	TS.34_7.3_REQ_007	M		
	TS.34_7.3_REQ_008	M		
	TS.34_7.3_REQ_009	M		
	TS.34_7.3_REQ_010	M		
	TS.34_7.3_REQ_011	O		
	TS.34_7.3_REQ_012	M		
4.1.5	Logic Flow for Back Off Procedure TS.34_7.0_REQ_004	M		
4.2.1	Unique Passwords for Device Access Control Clauses 4.2.1.1 to 4.2.1.3 shall be supported and implemented accordingly, contingent on end-users having access to the communications module of the Device	C		
4.2.1.1	Password Requirements	-		
	4.2.1.1 (a)	M		
	4.2.1.1 (b)	O		
	4.2.1.1 (c)	M		
	4.2.1.1 (d)	O		
	4.2.1.1 (e)	M		
	4.2.1.1 (f)	O		
4.2.1.2	Default Password Handling	-		
	4.2.1.2 (a)	M		
	4.2.1.2 (b)	M		
4.2.1.3	Authentication Handling	-		
	4.2.1.3 (a)	M		
	4.2.1.3 (b)	M		
	4.2.1.3 (c) i	M		
	4.2.1.3 (c) ii	M		
	4.2.1.3 (c) iii	O		
	4.2.1.3 (d)	M		
4.3.1	Secure Software/Firmware update over-the-air If OTA is implemented, it shall be mandatory that the requirements defined in section 4.3.1 are supported.	C		
4.3.2	Secure UICC/eUICC update over-the-air	O		
4.3.2.1	Remote management of the UICC (Over-The-Air, OTA)	O		
4.3.2.2	Remote Management of Embedded UICCs (eUICCs)	O		