

NFC UICC Requirements Specification
Version 5.0
03 August 2014

This is a Non-binding Permanent Reference Document of the GSMA

Security Classification: Non-confidential

Access to and distribution of this document is restricted to the persons permitted by the security classification. This document is confidential to the Association and is subject to copyright protection. This document is to be used only for the purposes for which it has been supplied and information contained in it must not be disclosed or in any other way made available, in whole or in part, to persons other than those permitted under the security classification without the prior written approval of the Association.

Copyright Notice

Copyright © 2014 GSM Association

Disclaimer

The GSM Association ("Association") makes no representation, warranty or undertaking (express or implied) with respect to and does not accept any responsibility for, and hereby disclaims liability for the accuracy or completeness or timeliness of the information contained in this document. The information contained in this document may be subject to change without prior notice.

Antitrust Notice

The information contain herein is in full compliance with the GSM Association's antitrust compliance policy.

Table of Contents

1 Introduction 3
1.1 Overview 3
1.2 Scope 3
1.3 Definition of Terms 3
1.4 Definition 4
2 References 4
2.1 Standard Technical Specifications (Mandatory) 4
2.2 Test Specifications (Mandatory) 5
2.3 Standard Technical Specifications (Conditional) 5
2.4 Standard Technical Specifications (Informative) 5
3 Requirements 5
3.1 Option Description 6
3.1.1 ContactLess Tunnelling, ISO/IEC 14443 Type A 6
3.1.2 Sliding window size of 3 6
3.1.3 HCI as per TS 102 622 6
3.1.4 Support of TERMINAL CAPABILITY 6
3.1.5 Link management gate supported 7
3.1.6 Data link layer specified in TS 102 613 is being used 7
3.1.7 Proactive UICC: ACTIVATE command 7
3.1.8 Support of TS 102 613 indication in ATR Global Interface bytes 7
3.1.9 Cryptographic Algorithm 7
4 Global Platform Requirements 7
4.1 GlobalPlatform Card Specification 2.2 Amendment C Requirements 8
4.2 GlobalPlatform Device Technology Secure Element Access Control 8
5 Remote Application and File Management 8
6 Java Card 8
7 Protection Profile 9
Annex A Applications downloadable in post-issuance phase 2
A.1 Calypso support 2
A.2 MIFARE for Mobile support 2
Annex B Elective Requirements 3
Annex C Elective Requirements for Remote Application Management 4
Annex D Document Management 5
D.1 Document History 5
Other Information 5

1 Introduction

1.1 Overview

With the increasing activity to deploy commercial Near Field Communication (NFC) services in a number of markets around the world, it is important to embrace common standards to promote the global interoperability of services, while maintaining the momentum to meet time-to-market requirements in certain markets.

This document defines a common framework of requirements for UICCs to support UICC-based NFC services, selecting options among those allowed by existing standards to ensure interoperability.

1.2 Scope

This document lists for the NFC UICC a minimum set of requirements and the specification of technical gaps identified to ensure an efficient and consistent development and deployment of NFC services.

In particular this document details:

- References to the standard technical specifications;
- Optional requirements of the referenced standards that shall be implemented in the NFC UICC.

When a standard specification is listed in Section 2.1, Standard Technical Specifications (Mandatory), it is intended to be implemented in all its mandatory parts if not differently specified subsequently in Section 3. This document provides insight into details and descriptions for optional parts of the references that are specified as mandatory in Section 3.

1.3 Definition of Terms

Term	Description
ACP	Access Control Policy
ACT	ACTivation protocol
APDU	Application Protocol Data Unit
API	Application Programming Interface
ATR	Answer To Reset
CASD	Controlling Authority Security Domain
CAT-TP	Card Application Toolkit – Transport Protocol
CLF	Contactless Frontend
CLT	ContactLess Tunnelling
CREL	Contactless Registry Event Listener
CRS	Contactless Registry Services
DAP	Data Authentication Pattern
EAL	Evaluation Assurance Level
HCI	Host Controller Interface

HCP	Host Controller Protocol
MNO	Mobile Network Operator
NFC	Near Field Communication
SD	Security Domain
SHDLC	Simplified High Level Data Link Control
SP	Service Provider
SREJ	Selective REJect
SWP	Single Wire Protocol
UICC	Universal Integrated Circuit Card

1.4 Definition

The definition of the terms SHALL, SHALL NOT, SHOULD, SHOULD NOT and MAY is according with 3GPP TS 21.801 “Specification drafting rules” Annex E” Verbal forms for the expression of provisions”.

2 References

Mandatory references, as defined in section 2.1, are to be implemented in all their mandatory parts, if not differently specified in the document.

Later releases of ETSI-SCP or 3GPP specifications shall be backward compatible. The manufacturer can use Release 9 or a later release of the specifications when explicitly mentioned.

2.1 Standard Technical Specifications (Mandatory)

Term	Description
[1]	ETSI TS 102 221: "Smart Cards; UICC-Terminal interface; Physical and logical characteristics" V9.2.0 (2010-10)[1] or later.
[2]	ETSI TS 102 223: "Smart Cards; Card Application Toolkit (CAT)" V9.4.0 (2012-03) or later.
[3]	ETSI TS 102 225: “Secured packet structure for UICC applications” V.9.2.0 (2012-03) or later.
[4]	ETSI TS 102 226: “Remote APDU Structure for UICC based Applications” V.9.6.0 (2013-01) or later.
[7]	ETSI TS 102 613 Smart Cards; UICC – Contactless Front-end (CLF) Interface; Part 1: Physical and data link layer characteristics V9.3.0 (2012-09) or later.
[8]	ETSI TS 102 622 Smart Cards; UICC – Contactless Front-end (CLF) Interface; Host Controller Interface (HCI) V9.4.0 (2011-09) or later.
[9]	ETSI TS 102 240 Smart Cards; UICC Application Programming Interface and Loader Requirements; Service description; V9.1.0 (2011-12) or later.
[10]	ETSI TS 102 241 Smart Cards; UICC Application Programming Interface (UICC API) for Java Card™ V9.2.0 (2012-03) or later.
[11]	ETSI TS 102 705 Smart Cards; UICC Application Programming Interface for Java Card™ for Contactless Applications V.9.2.0 (2011-04)

[1] USB/IC implementation is not required.

[12]	Java Card™ Platform, Version 3.0.1 Classic Edition
[13]	GlobalPlatform Card Specification Version 2.2.1
[14]	GlobalPlatform Card Specification Version 2.2, Amendment C: Contactless Services Version 1.1 or later
[15]	GlobalPlatform Card UICC Configuration Version 1.0.1
[17]	(U)SIM Java Card Platform Protection Profile (PU-2009-RT-79-2.0.2)
[18]	GlobalPlatform Device Technology Secure Element Access Control v1.0
[25]	3GPP TS 31.111 (Release V9.8.0 or later) Universal Subscriber Identity Module (USIM) Application Toolkit (USAT)
[26]	3GPP TS 31.130 (Release V9.4.0 or later) (U)SIM Application Programming Interface (API); (U)SIM API for Java™ Card
[27]	3GPP TS 31.115 (Release V9.1.1 or later) Secured packet structure for (Universal) Subscriber Identity Module (U)SIM Toolkit applications
[28]	3GPP TS 31.116 (Release V9.4.0 or later) Remote APDU (Application Protocol Data Unit) Structure for (Universal) Subscriber Identity Module (U)SIM Toolkit applications
[29]	GlobalPlatform Card UICC Configuration - Contactless Extension Version 1.0

2.2 Test Specifications (Mandatory)

[19]	Void
[20]	Void

Note: The Test Specifications are now part of the NFC UICC Test Book.

2.3 Standard Technical Specifications (Conditional)

At least one of the two following specifications is Mandatory (see following “Remote Application and File Management” section)**.**

[21]	ETSI TS 102 127: Smart Cards; Transport protocol for CAT applications; Stage 2 (Release 6) V6.13.0 (2009-04) or later.
[22]	GlobalPlatform Card Remote Application Management over HTTP Card Specification v 2.2 - Amendment B Version 1.1.1

2.4 Standard Technical Specifications (Informative)

[5]	ISO/IEC 14443-2: " Identification cards - Contactless integrated circuit(s) cards - Proximity cards - Part 2: Radio frequency power and signal interface"
[6]	ISO/IEC 14443-3: "Identification cards - Contactless integrated circuit(s) cards - Proximity cards - Part 3: Initialization and anti-collision".
[16]	GSMA: NFC Handset APIs & Requirements Version 6.0

3 Requirements

These following features, defined as optional in the standards on section 2.1, shall be implemented in the NFC UICC.

	Option	Mnemonic	Reference
1	CLT, ISO/IEC 14443 Type A	O_CLT_A	[7]
2	Sliding window size of 3	O_WS_3	[7]
3	HCI as per TS 102 622	O_102_622	[8]

4	Support of TERMINAL CAPABILITY	O_TERM_CAP	[1]
5	Link management gate supported	O_LINK_MAN	[8]
6	Data link layer specified in TS 102 613 is being used	O_102_613	[7]
7	Proactive UICC: ACTIVATE command	O_ACTIVATE	[2]
8	Support of TS 102 613 indication in ATR Global Interface bytes	O_ATR	[1]
9	The UICC shall support 3DES cryptographic algorithm	O_ 3DES	[3], [4]
10	The UICC shall support AES cryptographic algorithm	O_AES	[3], [4]

3.1 Option Description

3.1.1 ContactLess Tunnelling, ISO/IEC 14443 Type A

ISO/IEC 14443-2 [5] describes the electrical characteristics of two types (Type A and Type B) of contactless interface between a proximity card and a proximity coupling device.

ISO/IEC 14443-3 [6] describes, for both Type A and Type B, polling for proximity coupling device, the byte format and framing, the initial Request and Answer to Request command content, method to detect and communicate with one proximity card among several proximity card (anti-collision) and other parameters required to initialize communications between a proximity card and a proximity coupling device.

For the purpose of this document only Type A is used over CLT (ContactLess Tunnelling) protocol.

3.1.2 Sliding window size of 3

In SHDLC (Simplified High Level Data Link Control) protocol the concept of a sliding window is used to send multiple frames before receiving confirmation that the first frame has been received correctly. Data may continue to flow when there are long "turnaround" time lags without stopping to wait for an acknowledgement. The sliding window size may be lower than the default value due to limited resources. In consequence, an endpoint may want to ask the other endpoint to lower the sliding window size. The support of this option states that UICC supports a windows size value of 3.

3.1.3 HCI as per TS 102 622

Support of the ETSI TS 102 622 [8] is required.

3.1.4 Support of TERMINAL CAPABILITY

Applications on the UICC requiring more power than the minimum power consumption may use the indication "TERMINAL CAPABILITY is supported" to request the terminal to indicate its capabilities with respect to support of additional power consumption using the TERMINAL CAPABILITY command. The use of this feature is up to the application to specify.

3.1.5 Link management gate supported

A gate provides an entry point to a service that is operated inside a host. The HCP (Host Controller Protocol) enables gates from different hosts to exchange messages. There are two types of gates:

1. Management gates that are needed for the management of the host network;
2. Generic gates that are not related to the management of the host networks.

All hosts may have one link management gate and the host controller shall have one link management gate.

The host controller link management gate provides information about the underlying layer. The registry may not be persistent.

The host link management gate provides access to information related to the link layer. The registry may not be persistent.

For more details see [8] par.7.1.2. *Link management gate*

3.1.6 Data link layer specified in TS 102 613 is being used

Support of ETSI TS 102 613 [7] is required.

3.1.7 Proactive UICC: ACTIVATE command

This proactive command is used to request the terminal to activate a specified interface, e.g. the UICC-CLF interface (if class "l" is supported by the terminal). For more details see [2] par.6.4.40 ACTIVATE.

3.1.8 Support of TS 102 613 indication in ATR Global Interface bytes

The UICC indicates the support of ETSI TS 102 613 [7] inside the Global Interface bytes. This could be useful in order to avoid the Terminal starts ETSI TS 102 613 [7] activation if the UICC doesn't support ETSI TS 102 613[7].

3.1.9 Cryptographic Algorithm

The UICC shall support 3DES cryptographic algorithm with 24 bytes key length.

The UICC shall support AES cryptographic algorithm with 128 and 256 bits key lengths.

4 Global Platform Requirements

The UICC shall support GlobalPlatform Card Specification 2.2.1 [13] in order to allow the Card Content Management in Simple Mode and Delegated Mode. This means that Authorized Management, Delegated Management, Receipt Generation and Token Verification privileges shall be supported. Only the owner of the ISD has the right to assign Authorized Management privileges to a SSD. DAP Verification shall be also supported by the UICC.

The UICC shall be compliant with GlobalPlatform UICC Configuration [15] with the following condition:

If Confidential Setup of Initial Secure Channel Keys is supported, the mechanism defined in the Scenario #2.B (Push Model without Application Provider Certificate) is mandatory. When none of the scenarios for confidential setup of secure channel keys are supported, the CASD (Controlling Authority Security Domain) Capability Information (byte 1) shall indicate that none of the scenarios are supported (i.e. bits b1, b2 and b3 are 0).

The CASD certificate shall be retrieve using the GET DATA command. The GET DATA OTA security details is defined in section 11.5.2 of GlobalPlatform Card Specification Version 2.2, Amendment C GlobalPlatform.

4.1 GlobalPlatform Card Specification 2.2 Amendment C Requirements

The UICC shall support the GlobalPlatform Card Specification Version 2.2, Amendment C [14] with the following additional requirements:

- The interface used by the MNO-Wallet may be the one defined in GlobalPlatform Card Specification Version 2.2, Amendment C [14] for the CRS application.
- The Contactless Self Activation Privilege shall apply as in [14] section 7.2. It is up to the MNO to decide if they want or not to give this privilege during the installation of the application.
- Section 11.5.1 and section 11.6.1 related to the usage of the command GET DATA and STORE DATA for the TLV '5F50' that contain the URL of the Security Domain Manager are not endorsed by this specification.

4.2 GlobalPlatform Device Technology Secure Element Access Control

The interface between the applets ARA-M and ARA-C is not defined in this GlobalPlatform specification [18]. For this reason ARA-C applets may only be used in markets where appropriate interface between ARA-M and ARA-C is available.

5 Remote Application and File Management

Remote Application and File Management as defined in ETSI TS 102 226 [4] and 3GPP TS 31.116 [28] shall be performed using either the CAT-TP mechanism or RAM / RFM over HTTPs mechanism, as defined in ETSI TS 102 225 [3], and 3GPP TS 31.115 [27] for PUSH SMS security and in ETSI TS 102 127 [21].

Use of RAM and RFM over HTTPs shall be as defined in ETSI TS 102 225 [3] , and 3GPP TS 31.115 [27] for PUSH SMS security, ETSI TS 102 226 [4] and GlobalPlatform CS V2.2 Amendment B [22].

Use of CAT-TP or RAM / RFM over HTTPs may differ between regions, for the sake of SP interoperability Annex C defines the respective version used by different MNOs. At least one of the two transport protocols referenced in section 2.3 shall be implemented by the MNOs. For small management operations SMS OTA is still allowed.

6 Java Card

The Integer data type shall be mandatory for the Java Card Virtual Machine and not optional as state in Java Card Platform - Virtual Machine Specification [12] section 2.2.3.1.

7 Protection Profile

The NFC UICC should be compliant with the (U)SIM Java Card Platform Protection Profile [17].

If the NFC UICC needs to be certified at EAL4+, it shall be certified using ISO/IEC 15408 Common Criteria against the (U)SIM Java Card Platform Protection Profile [17].

Annex A Applications downloadable in post-issuance phase

A.1 Calypso support

The UICC will support both ISO 144443 type A and B specifications (references 0 and 0), then if Calypso based application will be required the reference specification of the application that will be OTA downloaded is Calypso 3.1:

[30] ref. 060708-CalypsoAppli "Calypso Specification REV.3 - Portable Object Application" version 3.1 - 10 March 2009;

[31] ref. 090316-MU-CalypsoR3Amd1 "Calypso Specification REV.3 - Amendment 1 to Version 3.1" version 1.0 - 1 June 2010).

A.2 MIFARE for Mobile support

The UICC may support the MIFARE implementation reachable through the MIFARE JavaCard Host Interface API [32]. In this case, the MIFARE for Mobile v2 application framework is required to manage it via OTA:

[32] MIFARE for Mobile v2.1 specifications are available here: http://mifare4mobile.org

This implies that GlobalPlatform Secure Channel Protocol 03 [33] shall be supported.

[33] GlobalPlatform Secure Channel Protocol 03, Card Specification v2.2 – Amendment D version 1.1

Annex B Elective Requirements

Void
Annex B has been voided and the document GlobalPlatform Device Technology Secure Element Access Control [18] has been included in the mandatory standard section.

Annex C Elective Requirements for Remote Application Management

Void.

Annex D Document Management

D.1 Document History

Version	Date	Brief Description of Change	Approval Authority	Editor / Company
1.0	August 2011	First draft for external review	NFC, PSMC	Davide Pratone, Telecom Italia
2.0	November 2011	Second version incorporating feedback received to date approved at PSMC via EX Committee Email approval	PSMC (V2.0 Approved and published)	Davide Pratone, Telecom Italia
3.0	02 July 2012	Version 3 incorporating amended requirements for UICCs submitted to PSMC for approval	NFC, PSMC	Davide Pratone, Telecom Italia
3.0	03 October 2012	Submitted to PSMC for 7 day Committee Email approval	NFC, PSMC	Davide Pratone, Telecom Italia
4.0	15 August 2013	Version 4 incorporating amended UICC requirements submitted to PSMC for approval	NFC, PSMC	Davide Pratone, Telecom Italia
4.0	31 March 2014	Transferred from NFC Fast Track project to SIM Group	SIM group	Davide Pratone, Telecom Italia
5.0	25 June 2014	Version 5 updated by SIM Group and submitted to PSMC for approval	PSMC	Davide Pratone, Telecom Italia

Other Information

It is our intention to provide a quality product for your use. If you find any errors or omissions, please contact us with your comments. You may notify us at prd@gsma.com

Your comments or suggestions & questions are always welcome.