GLOBALPLATFORM

THE STANDARD FOR MANAGING APPLICATIONS ON SECURE CHIP TECHNOLOGY

GlobalPlatform Card

UICC Configuration – Contactless Extension

Version 1.0

Member Release

February 2012

Document Reference: GPC_GUI_035

This document is provided as a member benefit to GlobalPlatform members only.
Please help us maintain the value of your membership and encourage recruitment by observing this restriction.

Contents

1 Introduction 5
1.1 Audience 5
1.2 IPR Disclaimer 5
1.3 Normative References 5
1.4 Terminology and Definitions 6
1.5 Abbreviations and Notations 6
1.6 Revision History 6
2 User Interaction Management 7
2.1 General 7
2.2 GlobalPlatform CRS Application GET STATUS Command 7
2.2.1 Command Message 7
3 Contactless Protocol Management 8
4 Communication Interface Access Configuration 9
5 Application Selection 10
6 Contactless Privilege 11
7 Application Availability on the Contactless Interface 12
8 Security Domain APDU Commands 13
8.1 INSTALL Command 13
8.1.1 INSTALL [for registry update] Command 13
8.1.2 INSTALL Parameters 14
8.2 DELETE Command 16
8.3 GET STATUS Command 16
Annex A Application Programming Interfaces 17
A.1 Standard Java Card API 17
A.2 GlobalPlatform Java Card API 17

Tables

Table 1-1: Normative References 5
Table 1-2: Terminology and Definitions 6
Table 1-3: Abbreviations 6
Table 1-4: Revision History 6
Table 3-1: Default OPEN Protocol Data for Type A 8
Table 3-2: Default OPEN Protocol Data for Type B 8
Table 4-1: ISD Default Values 9
Table 5-1: OPEN – Continuous Processing Initial Value 10
Table 8-1: Supported System Specific Parameters 14
Table 8-2: Optionally Supported System Specific Parameters 14
Table 8-3: Contactless Protocol Parameters 14
Table 8-4: User Interaction Parameters 15
Table 8-5: DELETE Error Conditions 16
Table 8-6: GET STATUS Error Conditions 16

1 Introduction

This document defines an extension of the GlobalPlatform UICC Configuration [UICC] for UICCs equipped with contactless functionality. It specifies configuration requirements for implementing GlobalPlatform Card Specification Amendment C [AmdC] on the UICC. This document may define behaviors contradicting those described in [UICC].

1.1 Audience

This document is intended primarily for card manufacturers and application developers developing GlobalPlatform implementations on a UICC.

It is assumed that the reader is familiar with smart cards, and in particular familiar with GlobalPlatform Card Specification Amendment C: Contactless Services [AmdC].

1.2 IPR Disclaimer

GlobalPlatform draws attention to the fact that claims that compliance with this specification may involve the use of a patent or other intellectual property right (collectively, “IPR”) concerning this specification may be published at https://www.globalplatform.org/specificationsipdisclaimers.asp. GlobalPlatform takes no position concerning the evidence, validity, and scope of these IPR claims.

1.3 Normative References

Table 1-1: Normative References

Standard / Specification	Description	Ref
GlobalPlatform Card Specification	GlobalPlatform Card Specification v2.2.1	[GPCS]
GlobalPlatform Card Specification Amendment C	GlobalPlatform Card Specification v2.2 – Amendment C v1.0.1, Contactless Services	[AmdC]
GlobalPlatform UICC Configuration	GlobalPlatform Card – UICC Configuration v1.0.1	[UICC]
ISO/IEC 14443-3	Identification cards – Contactless integrated circuit cards – Proximity cards – Part 3: Initialization and anti-collision	[14443-3]
Java Card API	Application Programming Interface, Java Card™ Platform, v3.0.1, Classic Edition	[JCAPI]

1.4 Terminology and Definitions

Table 1-2 defines the expressions used within this Specification that use an upper case first letter in each word of the expression. Expressions within this document that use a lower case first letter in each word take the common sense meaning. (Tagged data elements are also given an upper case first letter in each word of their names.)

Table 1-2: Terminology and Definitions

Term	Definition
Contactless Application	Applications that are explicitly or implicitly configured to be usable on a contactless interface (e.g. based on ISO/IEC 14443 [14443-3]) are referred to as “Contactless Applications”.
Contactless Session	A contactless session starts when the card enters the RF field and ends when the card leaves the RF field.

1.5 Abbreviations and Notations

Table 1-3: Abbreviations

Abbreviation	Meaning
AID	Application Identifier
AFI	Application Family Indicator
APDU	Application Protocol Data Unit
API	Application Programming Interface
BER-TLV	Basic Encoding Rules – Tag, Length, Value
CRS	Contactless Registry Services
CREL	Contactless Registry Event Listener
ISD	Issuer Security Domain
OPEN	GlobalPlatform Environment
RF	Radio Frequency
TLV	Tag, Length, Value
UICC	Universal Integrated Circuit Card

1.6 Revision History

Table 1-4: Revision History

Date	Version	Description
February 2012	1.0	Initial release.

2 User Interaction Management

2.1 General

All of the parameters and mechanisms described in [AmdC] – Chapter 3 “User Interaction Management” shall be supported, with the following precisions:

- Application Group (see section 3.7 of [AmdC]): The card may require that an Application Group be created, i.e. that the Head Application for that Application Group be installed, before an Application can request joining that group. In such a case, if an Application requests joining an Application Group that does not yet exist, a status word of '6985' shall be returned.
- CRS Application (see section 3.9 of [AmdC]): The presence on the card of a CRS Application, i.e. an Application with the Contactless Activation Privilege, is optional.
- GlobalPlatform CRS Application (see section 3.11 of [AmdC]): The presence on the card of the GlobalPlatform CRS Load File (with standard AID) is optional. It shall be possible to load the GlobalPlatform CRS Load File (with standard AID) if it is not initially present on the card.

2.2 GlobalPlatform CRS Application GET STATUS Command

The GET STATUS command shall be supported.

2.2.1 Command Message

Reference Control Parameter P2

The CRS Application may optionally check that Search Criteria and Filter Criteria sent in mode First Occurrence and mode Next Occurrence are the same. If it does check consistency between the two modes and the criteria are different, then a response of '6A80' shall be returned. If it does not check consistency between the two modes, then the new criteria sent in mode Next Occurrence shall apply.

3 Contactless Protocol Management

All of the parameters and mechanisms described in [AmdC] – Chapter 4 “Contactless Protocol Management” shall be supported, with the following precisions:

- The Protocol Parameters for Type A and Type B shall be supported. The Default Protocol Parameter values shall always exist for protocols Type A and Type B.

Table 3-1 and Table 3-2, below, define the default protocol parameters for use by the OPEN for Type A and Type B, respectively.

Table 3-1: Default OPEN Protocol Data for Type A

T	**L**	**Value Description**		
'A0'	Var	Protocol Parameter Data		
		T	**L**	**Unique Identifier**
		'80'	1	LV: '00'
		T	**L**	**SAK**
		'81'	1	'xx1xxxxx' (b6 is set)
		T	**L**	**ATQA**
		'82'	2	'0400'
		T	**L**	**APPLICATION_DATA (ATS)**
		'83'	1	LV: '00'
		T	**L**	**FWI,SFGI**
		'84'	1	'78'
		T	**L**	**CID**
		'85'	1	'01'
		T	**L**	**DATA_RATE_MAX**
		'86'	3	'000001'

Table 3-2: Default OPEN Protocol Data for Type B

T	**L**	**Value Description**		
'A0'	Var	Protocol Parameter Data		
		T	**L**	**PUPI**
		'80'	1	LV: '00'
		T	**L**	**AFI**
		'81'	1	'00' (all)
		T	**L**	**ATQB**
		'82'	4	'00000071'
		T	**L**	**Higher Level Response in response to ATTRIB**
		'83'	1	LV: '00'
		T	**L**	**DATA_RATE_MAX**
		'84'	3	'000001'

4 Communication Interface Access Configuration

All of the parameters and mechanisms described in [AmdC] – Chapter 5 “Communication Interface Access Configuration” shall be supported, with the following precisions:

- For the ISD, the default values of the Communication Interface Access Configuration Parameters are described below in Table 4-1:

Table 4-1: ISD Default Values

Length	**Value Description**		
Var	Communication Interface Access Configuration		
	Tag	**Length**	**Value**
	'80'	1	'C0'
	'81'	1	'80'
	'82'	1	'80'

5 Application Selection

All the parameters and mechanisms described in [AmdC] – Chapter 6 “Application Selection” shall be supported, with the following precisions:

- Only the ISD shall be able to set up the timeout for Continuous Processing. For the OPEN, the initial timeout value is fixed to 0, meaning that there is no continuous processing:

Table 5-1: OPEN – Continuous Processing Initial Value

Length	Value Description
2	'0000'

- The String Recognition Algorithm shall be supported. The Bitmap Recognition Algorithm is optionally supported.

6 Contactless Privilege

All of the privileges and mechanisms described in [AmdC] – Chapter 7 “Contactless Privilege” shall be supported.

7 Application Availability on the Contactless Interface

All the parameters and mechanisms described in [AmdC] – Chapter 8 “Application Availability on the Contactless Interface” shall be supported, with the following precisions:

- The default value of the “Initial Contactless Activation State” parameter of the OPEN is '01', meaning Applications are installed in the ACTIVATED state if they have access to the contactless interface (see Chapter 4) and do not explicitly specify their Initial Contactless Activation State.
- The initial value of the Contactless Interface Availability is ON.

8 Security Domain APDU Commands

8.1 INSTALL Command

8.1.1 INSTALL [for registry update] Command

The INSTALL [for registry update] command shall be supported to update the system parameters of Applications according to the following rules:

- When the Application AID field is not present, the command is used to request updates to OPEN system parameters. The Security Domain processing the command shall be the ISD. Otherwise the command shall be rejected with a status word of '6985'. Notice that requesting updates to OPEN system parameters is not the same as requesting updates to ISD system parameters (i.e. by explicitly specifying the AID of the ISD in the command).
- When the Application AID field is present, the command is used to request updates to the system parameters of an Application. With respect to the identified Application, the Security Domain processing the command shall be an ancestor SD with the AM privilege, or a SD with DM privilege under an ancestor SD with AM privilege. Otherwise the command shall be rejected with a status word of '6985'. An exception to this rule is that the ISD is also able to update the system parameters of any Security Domain that is extradited to itself (i.e. at the top of an independent hierarchy).
- Only the ISD is able to update its own system parameters. A Supplementary Security Domain (even with the AM or DM privilege) cannot update its own system parameters.

Updating the privileges of an Application using the INSTALL [for registry update] command is not supported. If the Privileges field is present, then the command shall be rejected with a status word of '6A80'.

Extradition of an application using the INSTALL [for registry update] command shall be supported, and accepted according to the same rules as the INSTALL [for extradition] command.

The following sections describe the system parameters that shall be supported within the INSTALL [for install] and INSTALL [for install & make selectable] commands, and also indicate which system parameters can be updated using an INSTALL [for registry update] command.

For the purpose of clarification, it is recalled here that the INSTALL [for registry update] cannot be used to update Application Specific Install Parameters (tag 'C9').

8.1.2 INSTALL Parameters

8.1.2.1 System Specific Parameters

Table 8-1 lists the system specific parameters that shall be supported by the platform and may be used within the INSTALL [for install], INSTALL [for install & make selectable], and INSTALL [for registry update] command (according to the rules described in section 8.1.1):

Table 8-1: Supported System Specific Parameters

Tag	Length	Value Description
…	..	Other parameters as defined in GlobalPlatform Card Specification [GPCS]
'A0'	var	Contactless Protocol Parameters
'A1'	var	User Interaction Parameters

Tag 'B0' is reserved for, and shall be supported as defined by the ETSI.

Table 8-2 lists the system specific parameters that are optionally supported by the platform within the INSTALL [for install], INSTALL [for install & make selectable], and INSTALL [for registry update] command (according to the rules described in section 8.1.1):

Table 8-2: Optionally Supported System Specific Parameters

Tag	Length	Value Description
'82'	2 or 4	Cumulative Granted Volatile Memory
'83'	2 or 4	Cumulative Granted Non Volatile Memory

If a parameter is not supported by the platform, then the corresponding TLV shall be ignored.

8.1.2.2 Contactless Protocol Parameters

Table 8-3 lists the Contactless Protocol Parameters that shall be supported by the platform and may be used within the INSTALL [for install], INSTALL [for install & make selectable], and the INSTALL [for registry update] command (according to the rules described in section 8.1.1):

Table 8-3: Contactless Protocol Parameters

Tag	Length	Value Description
'80'	var	Assigned Protocols for implicit selection
'81'	1	Initial Contactless Activation.
'A2'	var	Contactless Protocol Parameters Profile.
'83'	var	Pattern Recognition Algorithm.
'84'	1-2	Continuous Processing.
'A5'	var	Communication Interface Access Parameters.
'86'	var	Protocol Data Type A (Card Emulation Mode).
'87'	var	Protocol Data Type B (Card Emulation Mode).

8.1.2.3 User Interaction Parameters

Table 8-4 lists the User Interaction Parameters that shall be supported by the platform and may be used within the INSTALL [for install], INSTALL [for install & make selectable], and the INSTALL [for registry update] command (according to the rules described in section 8.1.1):

Table 8-4: User Interaction Parameters

Tag	Length	Name
'7F20'	var	Display Control Template
'A0'	var	Head Application
'A1'	var	Add to the Group Authorization List
'A2'	var	Remove from the Group Authorization List (see note below)
'A3'	var	Add to the CREL List
'A4'	var	Remove from the CREL List
'A5'	Var	Policy Restricted Applications
'A6'	Var	Application discretionary data
'87'	1	Application Family
'88'	1	Display Required Indicator

Note: The support for tag 'A2' (Remove from the Group Authorization List) is mandatory within the INSTALL [for registry update] command, and only optional within the INSTALL [for install] and INSTALL [for install & make selectable] commands. If it is not supported, then tag 'A2' shall be ignored.

8.2 DELETE Command

Processing State Returned in the Response Message

A successful execution of the command shall be indicated by status bytes '90' '00'.

This command may either return an error condition as listed in [GPCS] or the following error conditions:

Table 8-5: DELETE Error Conditions

SW1	SW2	Meaning
'6A'	'86'	If the UICC does not support Cumulative Deletion

8.3 GET STATUS Command

The Filter Criterion Tag List and the Response Message format shall be supported.

If the Filter Criterion request for Cumulative Granted Memory information and Cumulative Granted Memory is not supported then the UICC shall ignore such criterion and no error shall be returned.

Reference Control Parameter P2

The Security Domain may check or not that Search Criteria and Filter Criteria sent in mode First Occurrence and mode Next Occurrence are the same. If it does check consistency between the two modes and the criteria are different, then a response of '6A80' shall be returned. If it does not check consistency between the two modes, then the new criteria sent in mode Next Occurrence shall apply.

Processing State Returned in the Response Message

A successful execution of the command shall be indicated by status bytes '90' '00'.

This command may either return an error condition as listed in [GPCS] or the following error conditions:

Table 8-6: GET STATUS Error Conditions

SW1	SW2	Meaning
'6A'	'86'	If the UICC does not support Cumulative Deletion and P1 indicates “Logically Deleted With References”

Annex A Application Programming Interfaces

A.1 Standard Java Card API

This section provides some precisions on the implementation of the standard Java Card API [JCAPI]:

This configuration assumes that several communication interfaces may be available (e.g. contact and contactless). The card shall be able to receive APDU commands and send APDU responses, as specified in ISO 7816-4, on any of these communication interfaces. The card shall always be able to know on which communication interface a specific APDU command has been received.

Therefore, the `APDU.getProtocol()` method shall return:

- For a communication originated over the contactless IO interface, depending on the protocol, one of the following:[1]
  - `(PROTOCOL_MEDIA_CONTACTLESS_TYPE_A | PROTOCOL T1)`
  - `(PROTOCOL_MEDIA_CONTACTLESS_TYPE_B | PROTOCOL T1)`
- For a communication originated over the contact interface, depending on the protocol, one of the following:
  - `PROTOCOL_T0`
  - `PROTOCOL_T1`

The following behavior is required in the case the communication interface on which the APDU command currently being processed was received would become unavailable:

If any of the following methods is invoked, and the communication interface on which the APDU command currently being processed was received is not available anymore, then an `APDUException` shall be thrown with a reason code `APDUException.IO_ERROR`:

- `APDU.setOutgoing()`
- `APDU.setOutgoingNoChaining()`
- `APDU.setOugoingLength()`
- `APDU.sendBytes()`
- `APDU.sendBytesLong()`
- `APDU.setOutgoingAndSend()`

A.2 GlobalPlatform Java Card API

The `org.globalplatform` shall be supported with version 1.5 or above, with the following precisions:

- The object returned by the `GPSystem.getSecureChannel()` method shall implement the `SecureChannelx2` interface.
- The object returned by the `GPSystem.getSecureChannel()` method may optionally implement the `SecureChannelx` interface.

The `org.globalplatform.contactless` shall be supported with version 1.1 or above.

[1] As defined in [JCAPI], "PROTOCOL_T1" denotes the T=CL variant for contactless cards defined in ISO 14443-4 [14443-3].