JCOP21sim Technical Brief

Overview: *This document contains a simple overview about the technical capabilities of the first GSM SIM member of the JCOP card OS family. Requests for further information may be directed at javacard@zurich.ibm.com.*

1. Basic specifications

JCOP is an IBM BlueZ implementation of the basic specifications [1] and [2] including refinements from Visa International set in the Visa OpenPlatform Card Implementation Guides (http://www.visa.com/nt/suppliers/vendor). All necessary clarifications from ISO7816 and EMV 2000 are also incorporated into the implementation where required by [1] and [2].

JCOP21sim is the first GSM SIM member of this family. It adds GSM SIM and WAP WIM capabilities according to [3-9] to the ones listed in JCOP20.

JCOP21sim can also be configured to be fully compliant to EMV for use as a banking card if the GSM/WAP functionality is not activated.

2 Communications

2.1 Supported protocols

ISO7816 T=0 direct convention [default][1]

ISO7816 T=0 inverse convention[1]

2.2 Supported speeds

At the default clock rate of 3.57 MHz, the following communication speeds can be attained:

9600 bit/sec [default]

19200 bit/sec

38400 bit/sec

57600 bit/sec

115200 bit/sec

[1] The contact protocols of JCOP can be configured to support the clock-stop feature of certain terminals to save power consumption (typically done in mobile phones).

3 Memory availability for applications

3.1 EEPROM

3.1.1 Persistent Java heap

Used for allocating persistent objects, applets, and storage of post-issuance loaded applet code (aka packages).

Size: 14/30kB* (without custom ROM applets).

3.1.2 Transaction buffer

Used to save data written transactional (e.g. all persistent byte and short stores) as well as persistent parameters to Util.arrayCopy; see [1].

Size: 512 bytes

3.2 RAM

3.2.1 Transient Java heap

Used for allocating transient objects and arrays of type CLEAR_ON_RESET and CLEAR_ON_DESELECT.

Size: 512 bytes

3.2.2 APDU buffer

Used to hold incoming and outgoing communications data.

Size: 261 bytes

3.2.3 Java stack

Used to hold call parameters, local variables, and stack frames of the VM.

Size: 200 bytes

3.3 ROM

8/40kB* free for applications

* Depending on hardware configurations (see section 5)

4 Supported optional features

Certain features listed in the standards implemented are not defined to be mandatory. The ones implemented in JCOP are listed below.

4.1 JavaCard

4.1.1 Garbage Collection

Fully implemented: Deleted objects, applets, and packages are fully reclaimed and the space can be used for other purposes after deletion.

4.1.2 Standard Cryptographic Algorithms

JCOP21sim has the ability to generate RSA keys on the card. The following JavaCard API constants (see [1]) are implemented by this version of JCOP:

Ciphers:

ALG_DES_CBC_NOPAD

ALG_DES_CBC_ISO9797_M1

ALG_DES_CBC_ISO9797_M2

ALG_DES_ECB_NOPAD

ALG_DES_ECB_ISO9797_M1

ALG_DES_ECB_ISO9797_M2

ALG_RSA_PKCS1

ALG_RSA_NOPAD

Signatures:

ALG_DES_MAC8_NOPAD

ALG_DES_MAC8_ISO9797_M1

ALG_DES_MAC8_ISO9797_M2

ALG_RSA_SHA_ISO9796

ALG_RSA_SHA_PKCS1

ALG_RSA_MD5_PKCS1

MessageDigest:

ALG_SHA

ALG_MD5

RandomData:

ALG_SECURE_RANDOM

KeyTypes:

LENGTH_DES

LENGTH_DES3_2KEY

LENGTH_RSA_2048[1]

LENGTH_RSA_1024[1]

LENGTH_RSA_768[1]

LENGTH_RSA_512[1]

TYPE_DES_TRANSIENT_RESET

TYPE_DES_TRANSIENT_DESELECT

TYPE_DES

TYPE_RSA_PUBLIC

TYPE_RSA_PRIVATE[2]

TYPE_RSA_CRT_PRIVATE

KeyPair:

ALG_RSA_CRT

4.2 OpenPlatform

4.2.1 Global PIN

Fully implemented: All described APDU and API interfaces for this feature are present.

4.2.2 Security Domains/DAP

JCOP21sim allows the installation of multiple Security Domains as well as Mandated DAP verification.

4.3 GSM

JCOP21sim fully implements the GSM SIM functionality as defined in [3], [4] and [6]. Furthermore, it provides the SIM API for Java Card [5], which allows the installation of SIM Toolkit applications written in Java. Also, the security mechanisms defined in [7] are fully

[1] All multiples of 32 (bit) are supported as valid RSA key lengths. Thus, key length values such as 736 (bits) can be passed as parameters to the respective functions.

[2] Private Keys must be loaded with key material. On-card key generation is only supported for RSA keys in CRT format.

implemented allowing over-the-air loading of Java applications as well as remote file-system management.

By default JCOP21sim supports the COMP128 (version 1 and 2) cryptographic algorithm for GSM authentication. Other algorithms can be integrated on demand.

4.4 WAP

The JCOP21sim system provides a built-in WAP 2.0 WIM application [8], which can be optionally installed when the SIM functionality is activated. This allows configuring JCOP21sim as SIM-only or as SWIM card. The WIM application supports application-level signatures as well as WTLS security based on 1024-bit RSA operations and the WTLS SHA-1 pseudo-random function as defined in [9].

5 Supported Hardware

The identical JCOP mask can run on these platforms and automatically make use of their resources, i.e., create a bigger persistent Java heap, and make more ROM memory available for ROMed applets*.

5.1 Philips P8WE5017

64 kB ROM → 8kB free for ROM'd applets in Custom Mask Process

16 kB EEPROM

2300 Bytes RAM

Triple-DES coprocessor

FameX RSA coprocessor

5.2 Philips P8WE5033

96 kB ROM → 40kB free for ROM'd applets in Custom Mask Process

32 kB EEPROM

2300 Bytes RAM

Triple-DES coprocessor

FameX RSA coprocessor

* Custom applets may be submitted to Philips for inclusion into a ROM mask. The maximum package size is 16kB.

A Revision History

1.0	Initial document
1.1	Corrected free ROM memory sizes (3.3)
1.2	Specification amendment on RSA keys (4.1.2); Free ROM applet size clarified (5)
1.3	Added comment on clock-stop feature (2.1)

B References

[1] Sun Microsystems: JavaCard 2.1.1 http://java.sun.com/products/javacard

[2] Global Platform Consortium: OpenPlatform 2.0.1' http://www.globalplatform.org/

[3] GSM 11.11: Specification of the Subscriber Identity Module 8.0.3

[4] 3GPP TS 11.14: Specification of the SIM Application Toolkit 8.5.0

[5] 3GPP TS 03.19: Subscriber Identity Module API for JavaCard 8.3.0

[6] GSM 03.40: Technical Realization of the Short Message Service (SMS) 7.4.0

[7] 3GPP TS 03.48: Security Mechanisms for SIM Application Toolkit 8.8.0

[8] WAP-260-WIM-20010712-a: Wireless Application Protocol, Wireless Identity Module

[9] WAP-261-WTLS-20010406-a: Wireless Application Protocol, Wireless Transport Layer Security