JCOP 4 P71

Short Data Sheet

Rev. 1.0 – 20190327
NXP Doc. No. 432810

Document Information

Info	Content
Keywords	Short Data Sheet, JCOP 4 P71
Abstract	This is the JCOP 4 P71 Short Data Sheet for JCOP 4 P71 on SmartMX3 P71.

Rev	Date	Description
1.0	20190327	Initial release.

1 Introduction

NXP Semiconductors offers a Java Card Operating System (OS) called JCOP. It is based on independent, third-party specifications by Oracle Corporation, the GlobalPlatform consortium, the International Organization for Standardization (ISO), EMVCo, and others. This document gives an overview of the features implemented in JCOP 4 P71.

1.1 Audience

The intended audience for this document are parties interested in JCOP 4 P71. The document gives an at-a-glance overview of NXP's latest Java Card offering.

The following documents contain more detailed information on aspects of JCOP 4 P71:

- JCOP 4 P71 User Guidance and Administrator Manual [12].
- SmartMX3 P71 Family P71D321 Overview, Pinning and Electrical Characteristics Product Short Data Sheet [11].
- SmartMX3 P71 JCOP Delivery Forms and Electrical Characteristics [10].
- NXP Secure Smart Card Controller Antenna Design Guide Application Note [9].

Additional documents are available to registered users on DocStore (http://www.docstore.nxp.com). This includes development guidelines, user guidance manuals and specific NXP application manuals.

Refer to the bibliography for other specifications and documents referenced in this document.

2 Product description

The architecture of JCOP 4 P71 is based on several independent third-party specifications: the Java Card specification from Oracle, the GlobalPlatform specification from the GlobalPlatform consortium, the specifications from International Organization for Standards (ISO), EMV (Europay, MasterCard and VISA), and others.

These industry standards together ensure application interoperability for card issuers as well as application providers. By adhering not just to the standards themselves, but also to their spirit (as evidenced in numerous heritage applications), JCOP 4 P71 ensures large interoperability with third-party applets as well as all existing Smart Card infrastructures. With JCOP 4 P71 the promise of multi-sourcing any component in smart card solutions becomes true. Even in existing infrastructures, JCOP 4 P71 equipped with proper applications can substitute any existing smart card.

Within its targeted segments, the new JCOP 4 P71 platform on SmartMX3 is the most advanced solution available. It combines standard interfaces as defined in Java Card 3.0.5 Classic (see [7], [5], [6]), GlobalPlatform 2.3 (see [2]), and powerful cryptographic capabilities by using coprocessors for public and secret key encryption. The secret key encryption supports Rivest Shamir Adleman asymmetric algorithm (RSA), Elliptic Curve Cryptography (ECC), Advanced Encryption Standard (AES), and Data Encryption Standard with 3 keys (3DES). JCOP does all this within a high security, ultra low power, performance optimized design concept. The platform supports voltage classes “C”, “B”, “extended B”, and “A” (1.62 - 5.5 V) as required by application standards such as the credit/debit card standard (EMV).

2.1 Application options

JCOP 4 P71 is a conversion platform that supports EMV and SECID applications. It can be used for the following applications:

- EMVCo payment card
- Electronic passport (ePP) providing BAC, EACv1 and SAC/PACE support
- European Citizen Card (EN 15480)
- European Health Insurance Card (CDA15974-2009 E)
- Fingerprint Match on Card (ISO 19794) — MINEX III compliant
- International Driving License BAP and EAP (ISO 18013)
- SECID applications such as ePKI, eVR and eRP
- MasterCard, Visa, American Express, Discover and other payment applications

JCOP 4 P71 is highly configurable. The base configuration includes all required functionality for Europay, MasterCard and Visa (EMV) payment cards. The Secure Identification (SECID) configuration adds additional functionality typically required in passport, ID, or similar applications.

Some features are available as add-ons. Add-ons have to be selected when ordering (see Section 4 - Ordering and delivery). Some are included in the main configurations by default, others are selectable only for certain configurations.

2.2 NXP product portfolio

NXP offers JCOP 4 P71 in two different basic OS configurations dedicated for payment and secure ID (eGov) use.

Both basic configuration might be customized by specific OS extensions (add-ons) to add features to the basic configuration. Next to the flexible configuration of the OS itself, applications (applets) can be added when inquiring a specific volume delivery type.

Tab. 2.1: Payment solutions

Available memory	**100**	**150**	**200**
Target applications	Standard payment 1-2 applets (incl. payload)	Multi payment 2-3 applets (incl. payload)	Multi-purpose payment Multiple applets (incl. payload)
Interface	Contact/DIF	DIF	DIF
Type	J2R100/J3R100	J3R150	J3R200
OS add-ons			
Korean SEED	-	Optional	Optional
MoC	-	Optional	Optional
MIFARE Plus EV1	-	Optional	Optional
MIFARE DESFire EV2	-	Optional	Optional

Tab. 2.2: SECID solutions

	Mono	Multi	Convergence
Available memory	110k	150k	180k
Target application	Mono-app	Multi-app	Convergence
Interface	Contact/DIF	Contact/DIF	DIF
Type	J2R110/J3R110	J2R150/J3R150	J3R180
Applet options			
Secure ID applet suites	Optional	Optional	Optional
EMV applets	-	-	Optional
OS add-on			
RSA key gen	Optional	Optional	Optional
MoC ID3/NT	Optional	Optional	Optional
FIPS module	Optional	Optional	Optional
MIFARE Plus EV1	-	-	Optional
MIFARE DESFire EV2	-	-	Optional

- Applets, MIFARE emulations and add-ons, as well as payload memory of the selected applications (incl. MIFARE), need to fit into the selected overall available memory.
- On request, MIFARE emulations and add-ons may be loaded before delivery in the NXP factory to extend the product's base functionality and can be deleted at pre-personalization.
- MIFARE Plus EV1 includes MIFARE Classic and backwards compatibility to MIFARE Plus EV1.
- MIFARE DESFire EV2 is backwards compatible to DESFire EV1.

2.3 Communication interfaces

JCOP 4 P71 provides an interface for the ISO/IEC 7816 [3] communication. If the JCOP hardware supports a contacless communication interface, then ISO/IEC 14443 Type A [4] based communication is also supported.

If the hardware implements two communication interfaces, the current card session uses the interface that received the first clock signal.
The active communication interface can be changed by resetting the card and sending data on the other communication interface.

The rest of this document does not further distinguish between products with one or two hardware communication interfaces. Descriptions for the contactless interface apply only to products with such hardware interface.

JCOP 4 P71 supports the following communication protocols:

- ISO/IEC 7816-3 T=1 direct convention (default),
- ISO/IEC 7816-3 T=0 direct convention,
- ISO/IEC 7816-3 T=1 inverse convention,
- ISO/IEC 7816-3 T=0 inverse convention
- ISO/IEC 14443 Type A T=CL.

On the contact interface, baud rates up to 614kbit/s are supported.
On hte contactless interface, all communication speeds up to 848kbit/s are supported.
Very High Baud Rate (VHBR) is supported for PICC to PCD up to 3.2Mbits/s.

2.4 Integrated MoC

The biometrics algorithm is provided by the JCOP platform as an add-on using Secure Box. Only one MoC library can be active at a time. Decide which library, if any, should be enabled prior to ordering the product (see see Section 4 - Ordering and delivery). For information on how to use the activated library, and details on the exact features available, refer to its user manual.

- Minutiae-based fingerprint comparison algorithm (ISO/IEC 19794-2 compact card format).
- PIV-compliant, certified by NIST in MINEX III program.
- Configurable rotation tolerance up to 180°.
- Maximum number of minutiae: up to 128 (depending on allocated memory).

2.5 Cryptographic algorithms and key sizes

JCOP 4 P71 products support 3DES and AES in Cipher Block Chaining (CBC) and Electronic codebook (ECB) mode, RSA, ECC, and the Korean SEED algorithm. JCOP can generate all RSA and ECC keys on the card for maximum security and supports the hashing methods SHA-1 and SHA-2.
For certified usage JCOP supports the following length of cryptographic keys and Secure Hash Algorithm (SHA) algorithms as defined in the Java Card Application Programming Interface (API) [5]:

- 3DES: 3DES with 2 keys and 3DES with 3 keys
- AES: 128 bits, 192 bits, and 256 bits

- RSA: 512 bits up to 2048 bits in 8-bit steps; optionally (via Order Entry Form) up to 4096 bits in 8-bit steps.

  Note: JCOP supports RSA keys starting at 512 bits. Select a sufficient strength for the intended application.

- ECC: 224 bits up to 521 bits
- SHA: SHA_224, SHA_256, SHA_384, SHA_512

Table 2.2 shows which features are included in which standard configuration, as well as which features are available through add-ons.

2.6 Product customization options

NXP provides a technology process to create transparent blends between JCOP 4 P71 and any set of applets. Standard applications of a particular card issuer as well as native libraries for Secure Box[1] can be put into the Non-Volatile Memory (NVM) during the chip production.

For details of available memory configurations in JCOP products, see Section 2.7 - Available memory.

Note: The memory footprint of an applet installed as part of the customization process may vary from the numbers reported by CAP File Converter. The difference is due to how data structures are handled.

The customization process does not impact the JCOP OS platform's functionality, performance, or security. This process can be used to pre-load applets and Secure Box native libraries.
The customization process also has no impact on a certificate which may have been issued for a particular version of JCOP.

2.7 Available memory

The available PHEAP space can be increased by deleting any preloaded item. Below are several typical configurations with the Config Module present.

Typical config (no applets)	Available persistent memory	Available transient memory
Base OS EMV (A1F3)	217 944 bytes	4 192 bytes
Base OS + MIFARE DESFire EV2 8k (A1BB)	128 844 bytes	3 312 bytes
Base OS + MIFARE Plus EV1 4k (A1C0)	142 820 bytes	3 264 bytes
SECID basic (A1C1)	175 280 bytes	4 192 bytes
SECID full (A1C2)	157 524 bytes	4 192 bytes

Note: The Config Module requires space until it is deleted.

[1] The Secure Box feature allows third-party libraries to be securely loaded and accessed. It is described in a separate manual.

Note: The amount of free memory depends on which add-ons (made up by one or more modules) and applets are installed on the card. To estimate the size available for a configuration, start with the card memory size and subtract module and applet sizes. For module sizes, see JCOP 4 P71 UGM [12]. For application sizes, refer to the user manual for the individual applet.

2.8 Designed-in support

NXP provides the following support:

- Development environment
  - JCOP Eclipse Generic Plugin
  - JCOP Eclipse Target Pack
  - Secure Box Development Framework
  - JCShell Standalone
  - SCCommUI (Smart Card Communication User Interface):
    - A graphical user interface for smart card operating systems
- NXP Semiconductors Customer Application Support (CAS)
- JCOP 4 P71 sample modules or cards

3 Standard features

This chapter lists features which are available to all JCOP 4 P71 products.

3.1 JCOP 4 P71 product family features

- Java Card 3.0.5 Classic
- GlobalPlatform 2.3 ([2]) (CI v2.0, see [1])
- GlobalPlatform Mapping Guidelines
- GlobalPlatform Secure Channel Protocol 01, 02 and 03
- GlobalPlatform Delegated Management, DAP and Authorized Management
- Data Encryption Standard (DES) and dual/triple key DES via coprocessor
- AES via coprocessor
- RSA via coprocessor
- ECC via coprocessor
- Other cryptographic support such as SHA-1, SHA-224, SHA-256, SHA-384, SHA-512 and CRC support
- Contact interface with T=0 and T=1 protocols according to ISO/IEC 7816-3
- Contactless interface with T=CL protocol according to ISO/IEC 14443 Type A
- FIPS certified
- Additional JCOP 4 P71 APIs .
- DRG.3 compliant pseudo-random number generator. Random numbers requested by a function call to the `RandomData` class are acquired from this random number generator. This includes the random challenge values used in the SCP protocols as defined by GlobalPlatform. DRG.3 is the default RNG setting.

3.2 Java Card 3.0.5 Classic

JCOP 4 P71 implements Java Card 3.0.5 Classic (API [5], Runtime Environnment [6] and Virtual Machine [7]).

All mandatory Java Card APIs defined in [5] can be invoked by an applet. However, some of these APIs provide restricted functionality or no functionality at all.

4 Ordering and delivery

4.1 Key exchange

The Transport Key will be specified by NXP and delivered to the customer as explained below.

To get access to the Transport Key of a JCOP 4 P71 product, send a request to retrieve this key to the email address **fabkey.bli@nxp.com**. In order to properly process this request, the FabKey Help Desk needs to identify the product of your request either by your Order Entry Form number or with the complete output of the IDENTIFY command.

The request will be processed by the FabKey Help Desk. Be aware that the response containing the transport key needs to be sent encrypted. Therefore the GPG key needs to be exchanged with the FabKey Help Desk before, where the Help Desk is required to verify the GPG fingerprint. This fingerprint needs to be submitted via a different communication channel from the GPG key itself.

The response from the Help Desk is confidential and needs to be handled under security and export control rules of the product and its documentation.

Note that individual Transport Keys are defined for different products.

NXP Semiconductors can only accept requests for Transport Keys after the customer has already received products of that type number.

4.2 Product delivery

This section describes the measures that are needed to ensure secure delivery of a JCOP product. For details see the wafer and delivery specification of the hardware [8].

NXP offers two ways of delivery of the product:

1. The customer collects the product at the NXP site (“Collection”).
2. The product is sent by NXP to the customer. To guarantee that the product is not manipulated during the delivery, the product is delivered in parcels sealed with special tape. The tape is printed with consecutive numbers and has special adhesive features which make any manipulation visible. NXP encloses a form in the parcel which the customer is asked to return. By this NXP is informed that the customer has received the undamaged parcel (“Shipment”).

Both methods guarantee that the customer gets authentic products. Additionally the customer can use the Transport Key to authenticate the chip.

5 Appendix

5.1 Performance figures

In the absence of standard performance tests, typical cryptographic operations are timed. The protocol used is T=1, direct convention, Fi/Di='11' with BWI=4. The reader clock rate is 4.8 MHz. Power Class A (5 V) is used.

To avoid measuring communication and other overhead, the execution time is calculated as difference between the times measured for an Application Protocol Data Unit as defined in ISO/IEC 7816 (APDU) which executes the operation mentioned in the table and an APDU which does not execute the operation. The Java Card applet which was loaded onto the card for the performance measurements uses RAM for the output buffer.

The execution times below are typical values but cannot be guaranteed.

Tab. 5.1: AES, standard API

Operation	Cipher	Data length	Execution time
Encrypt 128 bit AES Key	ALG_AES_BLOCK_128_CBC_NOPAD	128 Byte	1.67 ms
Decrypt 128 bit AES Key	ALG_AES_BLOCK_128_CBC_NOPAD	128 Byte	1.71 ms
Encrypt 128 bit AES Key	ALG_AES_BLOCK_128_CBC_NOPAD	512 Byte	2.00 ms
Decrypt 128 bit AES Key	ALG_AES_BLOCK_128_CBC_NOPAD	512 Byte	2.00 ms

Tab. 5.2: AES, CryptoBaseX

Operation	Cipher	Data length	Execution time
Encrypt 128 bit AES_X Key (CryptoBaseX)	ALG_AES_BLOCK_128_CBC_NOPAD	128 Byte	2.00 ms
Decrypt 128 bit AES_X Key (CryptoBaseX)	ALG_AES_BLOCK_128_CBC_NOPAD	128 Byte	2.00 ms
Encrypt 128 bit AES_X Key (CryptoBaseX)	ALG_AES_BLOCK_128_CBC_NOPAD	512 Byte	3.00 ms
Decrypt 128 bit AES_X Key (CryptoBaseX)	ALG_AES_BLOCK_128_CBC_NOPAD	512 Byte	3.00 ms

Tab. 5.3: DES, standard API

Operation	Cipher	Data length	Execution time
Encrypt 3KEY 3DES	ALG_DES_CBC_NOPAD	128 Byte	1.68 ms
Decrypt 3KEY 3DES	ALG_DES_CBC_NOPAD	128 Byte	1.77 ms
Encrypt 3KEY 3DES	ALG_DES_CBC_NOPAD	512 Byte	2.20 ms
Decrypt 3KEY 3DES	ALG_DES_CBC_NOPAD	512 Byte	2.50 ms

Tab. 5.4: DES, CryptoBaseX

Operation	Cipher	Data length	Execution time
Encrypt 3KEY 3DES (CryptoBaseX)	ALG_DES_CBC_NOPAD	128 Byte	1.79 ms
Decrypt 3KEY 3DES (CryptoBaseX)	ALG_DES_CBC_NOPAD	128 Byte	1.89 ms
Encrypt 3KEY 3DES (CryptoBaseX)	ALG_DES_CBC_NOPAD	512 Byte	2.30 ms
Decrypt 3KEY 3DES (CryptoBaseX)	ALG_DES_CBC_NOPAD	512 Byte	2.60 ms

6 Supported specifications

6.1 Applet specifications

- EMV Card Personalization Specification, Version 1.1, July 2007
- EMV Common Payment Application Specification, Version 1.0, December 2005
- M/Chip Multi-application Requirements, Multiple M/Chip Instances on a Single Card, 30 June 2016
- M/Chip Advance Card Application Specification Payment & Data Storage Version 1.2.1, August 2016
- Multiple M/Chip Instances - MCADS Personalization Profiles Add-On for IAT version 1.02, November 2016
- PKI Specifications (PKCS#11, PKCS#15) — middleware for Windows, Linux and Mac also available
- Visa Integrated Circuit Card Specification (VIS) 1.6
- Visa Contactless Payment Specification (VCPS) 2.2

6.2 Operating system specifications

- EMV Integrated Circuit Card Specifications for Payment Systems, Book 1 through 4, version 4.3, EMVCo, November 2011.
- EMV Contactless Specification for Payment Systems, Book A through D, version 2.6, EMVCo, August 2016.
- GlobalPlatform 2.2.1 ID Configuration:
  - Multi-application environment, post issuance loading, delegated management and lifecycle management.
  - Secure Channel Protocol (SCP) 01, 02 and 03.
- GlobalPlatform Card Specification 2.3, GlobalPlatform, December 2016.
- EMV 4.3, EMVCo, November 2011.
- EMV Contactless 2.6, EMVCo, 2016.
- 3.0.4 Classic, Oracle Corporation, September 2011.
- 3.0.5 Classic, Oracle Corporation, June 2015. Memory management and garbage collection are supported.
- ISO 7816 (contact)
- ISO 14443 (contactless)

- PUF: interface to the physical unclonable function provided by the hardware.
- Secure Box: interface that allows native libraries to be stored and securely used on the hardware.

7 Contents

8 Bibliography

[1] GlobalPlatform Inc. GlobalPlatform Card Common Implementation Configuration 2.0, December 2015.

[2] GlobalPlatform Inc. GlobalPlatform Card Specification 2.3, December 2015.

[3] ISO. ISO 7816-3: Part 3: Cards with contacts - Electrical interface and transmission protocols, November 2006.

[4] ISO/IEC. ISO/IEC 14443 Proximity Cards - Part 4: Transmission protocol - ISO/IEC 14443-2:2008.

[5] Oracle. Java Card 3 Platform, Application Programming Interface, Classic Edition, Version 3.0.5, May 2015.

[6] Oracle. Java Card 3 Platform, Runtime Environment Specification, Classic Edition, Version 3.0.5, May 2015.

[7] Oracle. Java Card 3 Platform, Virtual Machine Specification, Classic Edition, Version 3.0.5, May 2015.

[8] NXP Semiconductors. SmartMX3 family N7121 - Wafer and Delivery Specification, Rev. 1.0, August 29 2017.

[9] NXP Semiconductors. NXP Secure Smart Card Controller Antenna Design Guide Application Note, rev. 3.0, doc. no. 497630, November 23 2018.

[10] NXP Semiconductors. SmartMX3 Family P71D321 - Delivery forms and electrical characteristics, doc. no. 458010, January 19 2018.

[11] NXP Semiconductors. SmartMX3 Family P71D321 Overview, Pinning and Electrical Characteristics Product Short Data Sheet, rev. 3.0, doc. no. 412530, November 23 2018.

[12] NXP Semiconductors. JCOP 4 P71D321 User Guidance and Administrator Manual, doc. no. 496535, March 22 2019.

9 Legal information

9.1 Definitions

Draft – The document is a draft version only. The content is still under internal review and subject to formal approval, which may result in modifications or additions. NXP Semiconductors does not give any representations or warranties as to the accuracy or completeness of information included herein and shall have no liability for the consequences of use of such information.

9.2 Disclaimers

Limited warranty and liability – Information in this document is believed to be accurate and reliable. However, NXP Semiconductors does not give any representations or warranties, expressed or implied, as to the accuracy or completeness of such information and shall have no liability for the consequences of use of such information.

In no event shall NXP Semiconductors be liable for any indirect, incidental, punitive, special or consequential damages (including - without limitation - lost profits, lost savings, business interruption, costs related to the removal or replacement of any products or rework charges) whether or not such damages are based on tort (including negligence), warranty, breach of contract or any other legal theory.

Notwithstanding any damages that customer might incur for any reason whatsoever, NXP Semiconductors' aggregate and cumulative liability towards customer for the products described herein shall be limited in accordance with the Terms and conditions of commercial sale of NXP Semiconductors.

Right to make changes – NXP Semiconductors reserves the right to make changes to information published in this document, including without limitation specifications and product descriptions, at any time and without notice. This document supersedes and replaces all information supplied prior to the publication hereof.

Suitability for use – NXP Semiconductors products are not designed, authorized or warranted to be suitable for use in life support, life-critical or safety-critical systems or equipment, nor in applications where failure or malfunction of an NXP Semiconductors product can reasonably be expected to result in personal injury, death or severe property or environmental damage. NXP Semiconductors accepts no liability for inclusion and/or use of NXP Semiconductors products in such equipment or applications and therefore such inclusion and/or use is at the customer's own risk.

Applications – Applications that are described herein for any of these products are for illustrative purposes only. NXP Semiconductors makes no representation or warranty that such applications will be suitable for the specified use without further testing or modification.

Customers are responsible for the design and operation of their applications and products using NXP Semiconductors products, and NXP Semiconductors accepts no liability for any assistance with applications or customer product design. It is customer's sole responsibility to determine whether the NXP Semiconductors product is suitable and fit for the customer's applications and products planned, as well as for the planned application and use of customer's third party customer(s). Customers should provide appropriate design and operating safeguards to minimize the risks associated with their applications and products.

NXP Semiconductors does not accept any liability related to any default, damage, costs or problem which is based on any weakness or default in the customer's applications or products, or the application or use by customer's third party customer(s). Customer is responsible for doing all necessary testing for the customer's applications and products using NXP Semiconductors products in order to avoid a default of the applications and the products or of the application or use by customer's third party customer(s). NXP does not accept any liability in this respect.

Export control – This document as well as the item(s) described herein may be subject to export control regulations. Export might require a prior authorization from competent authorities.

Evaluation products – This product is provided on an "as is" and "with all faults" basis for evaluation purposes only. NXP Semiconductors, its affiliates and their suppliers expressly disclaim all warranties, whether express, implied or statutory, including but not limited to the implied warranties of non-infringement, merchantability and fitness for a particular purpose. The entire risk as to the quality, or arising out of the use or performance, of this product remains with customer.

In no event shall NXP Semiconductors, its affiliates or their suppliers be liable to customer for any special, indirect, consequential, punitive or incidental damages (including without limitation damages for loss of business, business interruption, loss of use, loss of data or information, and the like) arising out the use of or inability to use the product, whether or not based on tort (including negligence), strict liability, breach of contract, breach of warranty or any other theory, even if advised of the possibility of such damages.

Notwithstanding any damages that customer might incur for any reason whatsoever (including without limitation, all damages referenced above and all direct or general damages), the entire liability of NXP Semiconductors, its affiliates and their suppliers and customer's exclusive remedy for all of the foregoing shall be limited to actual damages incurred by customer based on reasonable reliance up to the greater of the amount actually paid by customer for the product or five dollars (US$5.00). The foregoing limitations, exclusions and disclaimers shall apply to the maximum extent permitted by applicable law, even if any remedy fails of its essential purpose.

9.3 Licenses

ICs with DPA Countermeasures functionality

NXP ICs containing functionality implementing countermeasures to Differential Power Analysis and Simple Power Analysis are produced and sold under applicable license from Cryptography Research, Inc.

9.4 Patents

Notice is herewith given that the subject device uses one or more of the following patents and that each of these patents may have corresponding patents in other jurisdictions.
<Patent ID> – owned by <Company name>

9.5 Trademarks

Notice: All referenced brands, product names, service names and trademarks are property of their respective owners.

MIFARE – is a trademark of NXP B.V.

For more information, please visit: http://www.nxp.com
For sales office addresses, please send an email to: salesaddresses@nxp.com

Date of release: 20190327

Document identifier: NXP Doc. No. 432810