A700x family

Secure authentication microcontroller

Rev. 3.1 — 5 July 2013
202031

Product short data sheet

1. General description

1.1 Overview

The A700x family is a tamper resistant secure Micro Controller Unit (MCU) family using a dedicated security hardened MX51CPU. NXP Semiconductors has a long track record in security MCUs. NXP ICs have been used in all types of security applications such as bank cards, health insurance cards, electronic passports, and pay-TV cards. They have also been used as embedded secure element in mobile phones. The A700x family features a significantly enhanced secure microcontroller architecture. Extended instructions for Java and C code, linear addressing and high speed at low power are among many other improvements added to the classic 80C51 core architecture.

The A700x family supports the following features:

- Dedicated MX51 security CPU
- 100 kbit/s I^2C slave interface
- ISO/IEC 7816 interface (optional)
- ISO/IEC14443 interface (optional)
- –40 °C to +90 °C operational ambient temperature (optional)
- On-chip operating system firmware: JCOP 2.4.2
- X.509 certificate-based client authentication application pre-installed
- Secure generation and insertion of key and certificate data, individualized for each die (optional)
- NXP glue logic
- NXP secure fetch technology
- Active shielding technology
- Asynchronous self-timed Handshake Technology
- Up to 76 kB EEPROM for application-code and data
- 40 μA typical sleep mode current with I^2C pads operated in weak pull-up mode, do not obstruct the bus lines
- High-performance secured Public Key Infrastructure (PKI) coprocessor (RSA up to 2048-bit keys, ECC over GF(p) up to 320-bit keys)
- Secured 2-key/3-key triple-DES coprocessor
- Secured AES coprocessor (128-, 192- and 256-bit keys)
- Compliant to Java Card specification V3.0.1 classic as defined in Ref. 1
- Compliant to Global Platform specification as defined in Ref. 2 and Ref. 3

The A700x family runs a Java Card Open Platform operating system named JCOP. It is based on independent, third-party specifications such as Oracle, Global Platform consortium, International Organization for Standards (ISO), and EMV (Europay, MasterCard and VISA). The Java Card and Global Platform industry standards combined ensure ease of application development and application interoperability for developers.

The A700x family key benefits are:

- Complete security platform enabling customized solutions.
- Field and silicon proven solutions- deployed in numerous devices and environments.
- Ensures trust to drive applications in open and closed systems where a high level of security is needed.
- Full solution, ease to integrate, ensuring lower total cost of ownership.
- Robust cryptographic core, countermeasures and protection of device assets.
- Powerful cryptographic coprocessors for public and secret key encryption within a low power, performance optimized design based on NXP Semiconductors handshaking technology.

For more detailed information refer to following documentation[1]:

- User manual JCOP 2.4.2 R1 for A7 family, JCOP V2.4.2 Revision 1.0 secure embedded MCU operating system, Document Number 2318xx[2] (see Ref. 16).

  The User manual describes JCOP for the applet developer. It outlines the features available through the Java Card API. Also it explains any additional functionality at the Java layer. Also, this User manual contains the information on how to order A700x family products.
- Admin manual JCOP 2.4.2 R1 for A7 family, JCOP V2.4.2 Revision 1.0 secure embedded MCU operating system, Document Number 2319xx2 (see Ref. 17). The Administrator manual describes JCOP for the administrator of a JCOP operating system. This manual explains the pre-personalization process and its specific commands.
- Full data sheet, A700x family, secure authentication microcontroller, Document Number 2066xx[2] (see Ref. 15).

  The Full data sheet explains the details of the A700x family product from a hardware point of view. It outlines figures like pinning diagram and power consumption.
- Application note, Device Authentication APDU Specification, Document Number 2118xx[2] (see Ref. 18).

  The applet user manual contains a detailed description of the authentication application on the A700x family product. It outlines the interface description including the APDU description and a description how to use the applet.

1. These documents are available under NDA
2. where XX refers to the last version; e.g. 10 refers to version 1.0

All information provided in this document is subject to legal disclaimers.

© NXP B.V. 2013. All rights reserved.

1.2 A700x family naming conventions

The following table explains the naming conventions of the commercial product name of the A700x family products. Every A700x family product gets assigned such a commercial name, which includes also customer and application-specific data.

The A700x family commercial names have the following format.

A700xagpp(p)/mvsrrff

The '**A700**' is a constant, all other letters are variables, which are explained in Table 1.

Table 1. JCOP V2.4.2 commercial name format

Variable	Meaning	Values	Description
	IC hardware specification code	see Table 4	
a	embedded operating system code	A	JCOP V2.4.2 R0.9
		C	JCOP V2.4.2 R1
g	embedded application firmware (applet) code	G	Generic, no application layer firmware (i.e. JCOP applets) pre-installed
		C	Customized, customer Applet pre-installed in ROM or EEPROM
		A	Application firmware implementing generic X509 based client authentication
pp(p)	package type code	see Table 3	
m	Manufacturing Site Code	T	
v	Silicon Version Code	0	
s	Silicon Version Subcode	B	
rr	ROM Code ID		
ff	FabKey ID		

1.3 X509 certificate-based client authentication

In addition to the A700x family secure MCU and the Java Card Open Platform operating system, the total solution includes an X.509 certificate-based client authentication application.

1.4 Trust provisioning service

The A700x family is delivered with pre-programmed, die-specific keys and certificates which are being generated and programmed in a certified (Common Criteria) secure NXP internal environment. The master keys are securely stored in HSMs (Hardware Secure Modules). Additional authentication software for the host (host-MCU or remote server) can also be included as part of the solution.

NXP Semiconductors offers a pre-personalizations service where customer-specific initialization data can be preprogrammed. This data can be die-individual card manager keys, symmetric DES-or AES keys, random data, X509 certificates, RSA signing keys or any other constant data like application code.

All information provided in this document is subject to legal disclaimers.

© NXP B.V. 2013. All rights reserved.

1.5 JCOPX - Additional Application Programming Interface (APIs) features

JCOP provides extended support for several industry-specific requirements. This support is given with the JCOPX API that comprises following functionality:

- Extended cryptography support (several algorithms and methods not specified in Java Card v3.0.1 classic (see Ref. 1)
- Secure Box feature supporting execution of native customer code in user mode out of Java Application
- A700xC (JCOP 2.4.2 R1): Support of IO configuration and control API, implementing methods to reconfigure the default I2C slave address. To configure the GPIO pin as either input or output pin and the read, set or clear the pin.
- MIFARE FleX support

More details about the JCOPX API can be found in JCOP User Manual (see Ref. 16).

1.6 Security features

The A700x family security concept is combining a comprehensive portfolio of NXP security measures which is protecting the chip against all types of attacks. Summarizing, there are more than 100 security features in an NXP security chip to protect against attacks from outside. NXP Semiconductors apply their extensive knowledge of chip security to harden the chip against any kinds of attacks.

The following features provide the highest level of attack resilience, which is unique in the market.

- counter measures against reverse engineering attacks provided by the dedicated security CPU designed in asynchronous handshaking circuit technology
- very dense submicron 5-metal-layer 0.14 μm technology
- NXP glue logic and active shielding technology

Secure Fetch Technology significantly enhances the chip hardware security for a certain class of light and laser attacks to the chip hardware. More specifically, Secure Fetch offers increased protection against attacks with higher spatial resolution. It also protects against attacks with both shorter and longer light pulses, and with both single and multiple pulses. It protects both the device memory and code fetching operations from ROM, RAM and EEPROM, greatly increasing the probability that fault injection attacks are detected. This unique security technology offers increased protection against future attack scenarios with light and laser sources, facilitating the development of highly secure software applications for customers.

The A700x family security concept includes dedicated HW measures to protect against any kind of leakage attacks. The Triple-DES coprocessor provides a high level of leak-resistance to first-order DPA, thus equally resilient against all kinds of leakage attacks.

All information provided in this document is subject to legal disclaimers.

© NXP B.V. 2013. All rights reserved.

The A700x family incorporates inherent and OS controlled security features:

- Secure Fetch Technology, protecting code fetches from ROM, RAM and EEPROM
- Dedicated security CPU designed in asynchronous handshaking circuit technology
- High dense submicron 5-metal-layer 0.14 μm CMOS technology,
- NXP glue logic
- Enhanced security sensors
  - Low and high temperature sensor (for A7001/3/5 only)
  - Low and high supply voltage sensor
  - Single Fault Injection (SFI) attack detection
  - Light sensors (incl. integrated memory light sensor functionality)

1.7 Security licensing

NXP Semiconductors has obtained a patent license for SPA and DPA countermeasures from Cryptography Research Incorporated (CRI). This license covers both hardware and software countermeasures. It is important to customers that countermeasures within the operation system are covered under this license agreement with CRI. Further details can be obtained on request.

All information provided in this document is subject to legal disclaimers.

© NXP B.V. 2013. All rights reserved.

2. Features and benefits

2.1 Standard family features

- High reliable EEPROM for both data storage and program execution: 80 kB
  - Data retention time: 25 years minimum
  - Endurance: 500,000 cycles minimum
- Dedicated Secure_MX51 MCU (Memory eXtended/enhanced 80C51)
- 100 kbit/s I^2C slave interface
- Optional ISO/IEC 7816 contact interface
- Optional ISO/IEC 14443 A Contactless Interface Unit (CIU)
- Public Key Cryptography (PKC) coprocessor supporting RSA, Elgamal, DSS, Diffie-Hellman, Guillou-Quisquater, Fiat-Shamir and Elliptic Curves
  - RSA support for the key lengths up to 2048 bit
  - Elliptic Curve over GF(p) Cryptography with key lengths up to 320 bit
- Single DES (56 bit) and Triple DES with 2 or 3 Keys (112 bit or 168 bit), encryption and decryption in ECB, CBC and CBC-MAC mode
- High-speed AES coprocessor (128-bit parallel processing AES engine)
- Low-power True Random Number Generator (TRNG) in hardware, AIS-31 compliant
- SHA1, SHA-224 and SHA-256
- SEED algorithm
- MD5
- On-Chip Key generation
- CRC calculations
- Data Authentication Pattern (DAP) for the Supplementary Security Domains
- Low power and low voltage design using NXP Semiconductors handshaking technology
- Power-saving SLEEP mode
- Wake-up from SLEEP mode by any I^2C communication request
- 40 μA typical sleep mode current with I^2C pads operated in weak pull-up mode, do not obstruct the bus lines
- Internally generated CPU clock (typical 62 MHz)
- 1.62 V to 5.5 V operating voltage range

2.2 Product-specific features

- A7001
  - −25 °C to +85 °C operational ambient temperature
- A7002
  - −40 °C to +90 °C operational ambient temperature
- A7003
  - −25 °C to +85 °C operational ambient temperature
  - ISO/IEC 7816 contact interface
- A7004
  - −40 °C to +90 °C operational ambient temperature
  - ISO/IEC 7816 contact interface

All information provided in this document is subject to legal disclaimers.

© NXP B.V. 2013. All rights reserved.

- A7005
  - –25 °C to +85 °C operational ambient temperature
  - ISO/IEC 7816 contact interface
  - ISO/IEC 14443 A Contactless Interface Unit (CIU)
  - Factory configurable input capacitance to match smaller loop antennas
  - MIFARE reader infrastructure compatibility via optional MIFARE 1K, 4K or FleX implementation including built-in anticollision support
- A7006
  - –40 °C to +90 °C operational ambient temperature
  - ISO/IEC 7816 contact interface
  - ISO/IEC 14443 A Contactless Interface Unit (CIU)
  - Factory configurable input capacitance to match smaller loop antennas
  - MIFARE reader infrastructure compatibility via optional MIFARE 1K, 4K or FleX implementation including built-in anticollision support

All information provided in this document is subject to legal disclaimers.

© NXP B.V. 2013. All rights reserved.

3. Applications

The A700x family is a complete embedded security platform for mobile phones, portable devices, computing and consumer electronic devices, and embedded systems where a strong security infrastructure is required. The A700x family provides an outstanding level of security, while overcoming the challenges of performance, power consumption and solution footprint. Its flexible architecture offers brand owners and device manufacturers a robust solution that can be tailored to meet the demanding embedded security requirements of today. The A700x family can be used in various host platforms and host operating systems to secure a broad range of applications.

The A700x family is offered as a turnkey solution that provides customers easy integration of authentication solutions into their end products. Minimal impact on the performance of end-products is achieved through high-speed, low power consumption ICs that feature the industry standard I^2C interface.

The flexibility of the A700x family solution allows for fast and convenient customization of specific solutions or implementations.

3.1 Application areas

- Embedded Security
- Counterfeit protection of hardware and software
  - Anti-cloning
  - Brand integrity of original goods
- Profile of service
  - Conditional access to software, content and features
  - Secure access to online services
- Device identity
  - Signing transactions
  - Secure machine to machine (M2M) communication

4. Quick reference data

Table 2. Quick reference data

Symbol	Parameter	Conditions	Min	Typ	Max	Unit
V_{DD}	supply voltage		1.62	-	5.5	V
EEPROM						
t_{ret}	retention time	T_{amb} = +55 °C	25	-	-	years
$N_{endu(W)}$	write endurance	under all operating conditions	5×10^5	-	-	cycles

All information provided in this document is subject to legal disclaimers.

© NXP B.V. 2013. All rights reserved.

5. Ordering information

Table 3. Ordering information

Type number[1]	Package		
	Name	Description	Version
A7001agUA/...	FFC	8 inch wafer (sawn; 150 μm thickness; on film frame carrier; electronic fail die marking according to SECSII format)	not applicable
A7002agUA/...			
A7003agUA/...			
A7004agUA/...			
A7005agUA/...			
A7006agUA/...			
A7001agHN1/...	HVQFN32	plastic thermal enhanced very thin quad flat package; no leads, 32 terminals; body 5 × 5 × 0.85 mm	SOT617-1
A7002agHN1/...			
A7003agHN1/...			
A7004agHN1/...			
A7005agHN1/...			
A7006agHN1/...			

[1] a = A or C, g = G, C or A, according to the A700x family type classification, see Section 1.2 “A700x family naming conventions”

5.1 Ordering options

Table 4 gives an overview of available A700x family product types

Table 5. shows JCOP features.

Table 4. A700x family feature table

Product type[1]	Operational ambient temperature	Free EEPROM data space	Transient Heap (RAM)	Embedded OS	Interface option
A7001Cgpp(p)	–25 °C to +85 °C	76.4 kB	3.2 kB	JCOP 2.4.2 R1	I^2C
A7002Cgpp(p)	–40 °C to +90 °C	76.4 kB	3.2 kB	JCOP 2.4.2 R1	I^2C
A7003Cgpp(p)	–25 °C to +85 °C	76.4 kB	3.2 kB	JCOP 2.4.2 R1	I^2C, ISO/IEC 7816
A7004Cgpp(p)	–40 °C to +90 °C	76.4 kB	3.2 kB	JCOP 2.4.2 R1	I^2C, ISO/IEC 7816
A7005Cgpp(p)	–25 °C to +85 °C	76.4 kB (MIFARE Config A)	3.2 kB	JCOP 2.4.2 R1	I^2C
		75.4 kB (MIFARE Config B1)			ISO/IEC 7816
		72.4 kB (MIFARE Config B2)			ISO/IEC 14443 A
A7006Cgpp(p)	–40 °C to +90 °C	76.4 kB (MIFARE Config A)	3.2 kB	JCOP 2.4.2 R1	I^2C
		75.4 kB (MIFARE Config B1)			ISO/IEC 7816
		72.4 kB (MIFARE Config B2)			ISO/IEC 14443 A

[1] g = G, C, or A; pp(p) = UA or HN1, according to the A700x family type classification, see Section 1.2 “A700x family naming conventions”

All information provided in this document is subject to legal disclaimers.

© NXP B.V. 2013. All rights reserved.

Table 5. JCOP V2.4.2 feature table

Product type	Java Card	Global Platform	VGP configurable 1, 2, 3	Applet backward compatible VGP 2.0.1 [1]	Applet loading	APDU Buffer	IO configure and control API
JCOP V2.4.2 R1	3.0.1	2.1.1	3	yes	yes	1462 bytes	

[1] To configure JCOP V2.4.2 R1 to be application backward compatible contact NXP Semiconductors Customer Application Support (CAS).

5.1.1 Samples and final products

Section 5.1.2, Section 5.1.3 and Section 5.1.4 give details of how to order samples and final products.

5.1.2 Ordering A700x family samples

Samples in HVQFN32 package can be ordered from NXP Semiconductors.

Note that NXP Semiconductors can provide up to 10 pieces free of charge. Larger quantities have to be ordered separately. Valid NDA has to be in place before samples are shipped.

Contact your local NXP Semiconductors representative for further information.

5.1.3 Ordering JCOP products

NXP Semiconductors has created various product configurations which are available for ordering. For a complete list of orderable A700x product types and part numbers, contact your local NXP Semiconductors representative.

5.1.4 JCOP tools

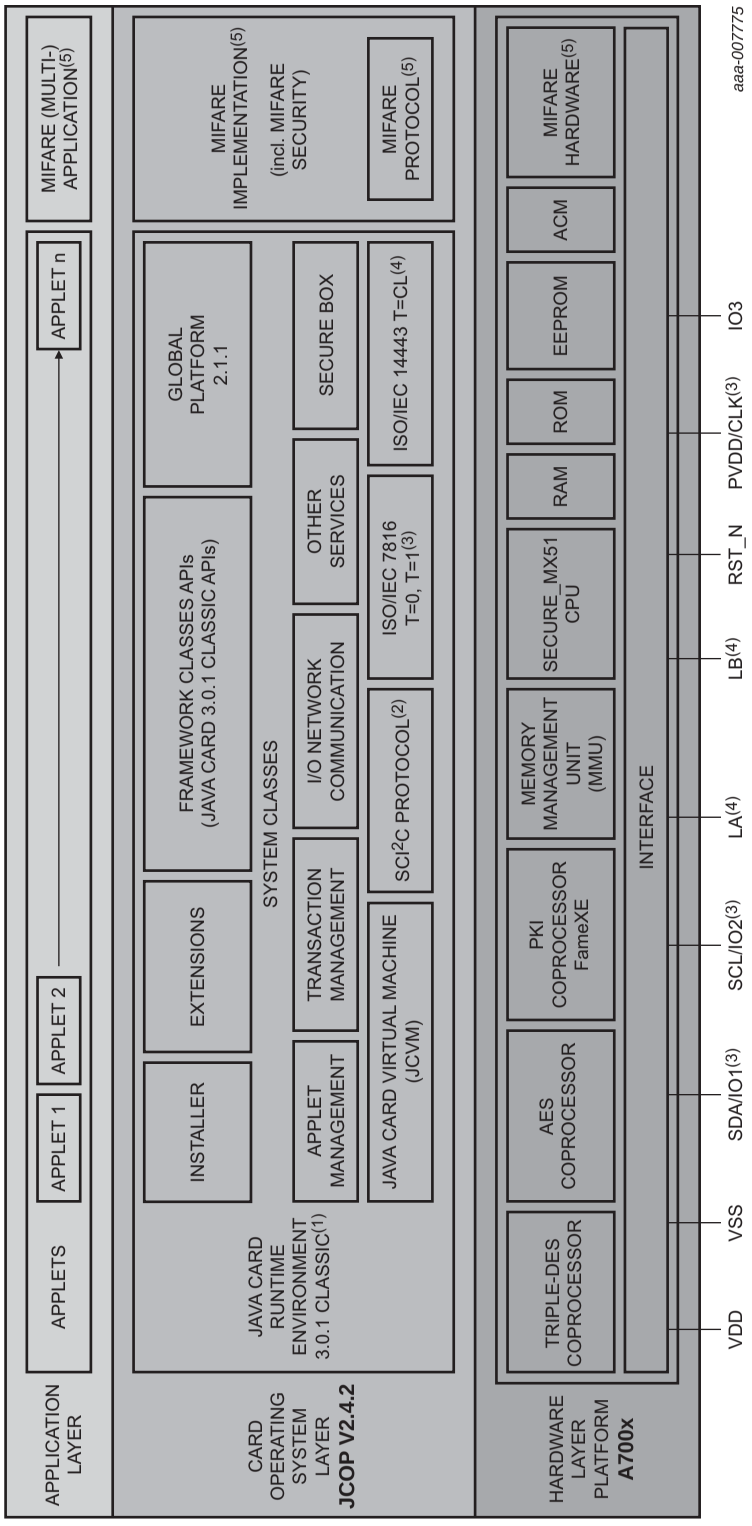
JCOP tools provide Integrated Development Environment (IDE) based on the ECLIPSE framework and specific JCOP product family through the JCOP tools plug-in.

Contact your local NXP Semiconductors representative for further information on JCOP tools (plug-in) availability.

All information provided in this document is subject to legal disclaimers.

© NXP B.V. 2013. All rights reserved.

6. Block diagram



(1) For more details, see Ref. 4

(2) For more details, see Ref. 5

(3) ISO/IEC 7816 interface not available on A7001/2

(4) ISO/IEC 14443 A interface only available on A7005/6

(5) Depends on configuration of JCOP 2.4.2 R1

Fig 1. A700x family block diagram

All information provided in this document is subject to legal disclaimers.

© NXP B.V. 2013. All rights reserved.

7. Limiting values

Table 6. Limiting values

In accordance with the Absolute Maximum Rating System (IEC 60134). Voltages are referenced to VSS (ground = 0 V).

Symbol	Parameter	Conditions		Min	Max	Unit
V_{DD}	supply voltage			−0.5	+6.0	V
V_I	input voltage	any signal pad		−0.5	V_{DD} + 0.5	V
I_I	input current	pad SDA, SCL or IO3		-	±15.0	mA
I_O	output current	pad SDA, SCL or IO3		-	±15.0	mA
I_{lu}	latch-up current	V_I < 0 V or V_I > V_{DD}		-	±100	mA
V_{ESD}	electrostatic discharge voltage	pads VDD, VSS, SDA, SCL, IO3	[1]	-	±4.0	kV
P_{tot}	total power dissipation		[2]	-	1	W
T_{stg}	storage temperature		[3]	-	-	°C

[1] MIL Standard 883-D method 3015; human body model; C = 100 pF, R = 1.5 kΩ; T_{amb} = −25 °C to +85 °C.

[2] Depending on appropriate thermal resistance of the package.

[3] Depending on delivery type, refer to *NXP Semiconductors General Specification for 8" Wafers* and to *NXP Semiconductors Contact & Dual Interface Chip Card Module Specification*.

8. Application information

Figure 2 shows a typical application diagram. It shows how the pins of the A700x family are applied to operate the IC in an I^2C system as an I^2C slave device. In this system, an individual reset control is not supported. The hardware reset is executed at power-up time (power-on reset).

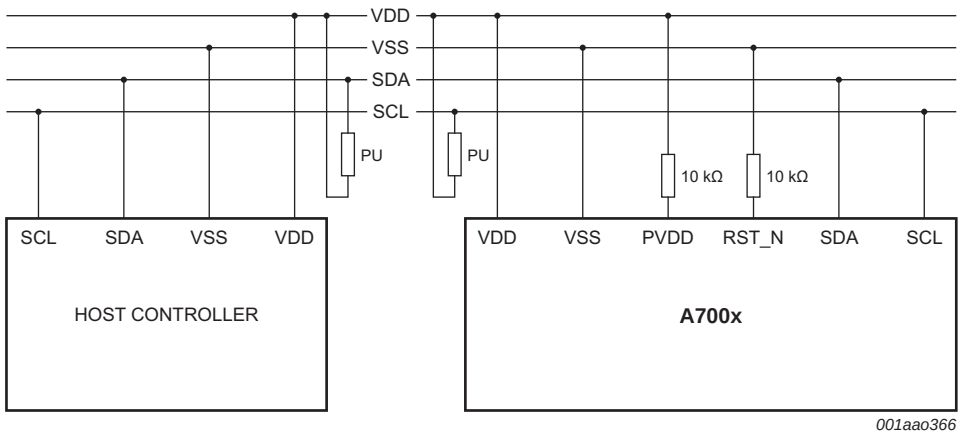


Fig 2. System overview supporting Power-on Reset

All information provided in this document is subject to legal disclaimers.

© NXP B.V. 2013. All rights reserved.

9. Abbreviations

Table 7. Abbreviations

Acronym	Description
AES	Advanced Encryption Standard
API	Application Programming Interface
CBC	Cipher-Block Chaining
CRC	Cyclic Redundancy Check
DES	Digital Encryption Standard
DPA	Differential Power Analysis
DSS	Digital Signature Standard
ECB	Electronic Code Book
ECC	Elliptic Curve Cryptography
EEPROM	Electrically Erasable Programmable Read-Only Memory
GF	Galois Function
I/O	Input/Output
MAC	Message Authentication Code
MD5	Message-Digest algorithm 5
MMU	Memory Management Unit
OS	Operating System
PKC	Public Key Cryptography
PKI	Public Key Infrastructure
RSA	Rivest, Shamir and Adleman
SFI	Single Fault Injection
SHA	Secure Hash Algorithm
SMD	Surface Mounted Device
SPA	Simple Power Analysis

All information provided in this document is subject to legal disclaimers.

© NXP B.V. 2013. All rights reserved.

10. References

[1] Oracle Java Card 3.0.1 classic: http://www.oracle.com/technetwork/java/javacard/overview/index.html

[2] Global Platform Consortium: GlobalPlatform Card Specification 2.1.1, March 2003: http://www.globalplatform.org/

[3] GlobalPlatform Consortium: GlobalPlatform; Card Specification 2.1.1 Amendment A, March 2004

[4] Java Card Technology for Smart Cards, Zhiqun Chen, ISBN 0-201-70329-7

[5] SCI^{2}C Protocol Specification, Rev. 1.2 — Apr-26-2012, NXP Semiconductors

[6] ISO/IEC International Standard 14443: “Identification cards - Contactless integrated circuit(s) cards - Proximity cards - Part 1: Physical characteristics”, 2000

[7] ISO/IEC International Standard 14443: “Identification cards - Contact less integrated circuit(s) cards - Proximity cards - Part 2: Radio frequency power and signal interface”, 2000

[8] ISO/IEC International Standard 14443: “Identification cards - Contact less integrated circuit(s) cards - Proximity cards - Part 3: Initialization and anticollision”, 2000

[9] ISO/IEC International Standard 14443: “Identification cards - Contact less integrated circuit(s) cards - Proximity cards- Part 4: Transmission protocol”, 2000

[10] ISO/IEC International Standard 7816: “Identification cards - Integrated circuit(s) cards with contacts - Part 3: Electrical interface and transmission protocol”, 2006

[11] ISO/IEC International Standard 7816: “Identification cards - Integrated circuit(s) cards with contacts - Part 4: Interindustry commands for interchange”, 2005

[12] ISO/IEC International Standard 7816: “Identification cards - Integrated circuit(s) cards with contacts - Part 5: Registration of application providers”, 2005

[13] ISO/IEC International Standard 7816: “Identification cards - Integrated circuit(s) cards with contacts - Part 8: Security related interindustry commands”, 2004

[14] Application Design Guide A7001, AN195112, NXP Semiconductors

[15] A700x, Secure authentication microcontroller, Document Number 2066xx[3], NXP Semiconductors

[16] User manual JCOP 2.4.2 R1 for A7 family, JCOP V2.4.2 Revision 1.0 secure embedded MCU operating system, Document Number 2318xx[3], NXP Semiconductors

[17] Admin manual JCOP 2.4.2 R1 for A7 family, JCOP V2.4.2 Revision 1.0 secure embedded MCU operating system, Document Number 2319xx[3], NXP Semiconductors

[18] Application note, APDU Specification - Authentication Device, Document Number 2185xx[3], NXP Semiconductors

3. Where XX refers to the last version; e.g. 10 refers to version 1.0.

All information provided in this document is subject to legal disclaimers.

© NXP B.V. 2013. All rights reserved.

11. Revision history

Table 8. Revision history

Document ID	Release date	Data sheet status	Change notice	Supersedes
A700X_FAM_SDS v.3.1	20130705	Product short data sheet	-	A700X_FAM_SDS v.3.0
Modifications:	• Removed chapter “Pinning Information”. • Corrected a number of details throughout the data sheet.			
A700X_FAM_SDS v.3.0	20130128	Product short data sheet	-	A700X_FAM_SDS v.2.2
Modifications:	• Document status promoted from Preliminary status to Product status. • HVSON8 package (SOT685-1, 5 mm × 6 mm) removed from Table 3 “Ordering information” on page 9.			
A700X_FAM_SDS v.2.2	20120521	Preliminary short data sheet	-	A700X_FAM_SDS v.2.1
Modifications:	• Text errors corrected.			
A700X_FAM_SDS v.2.1	20120217	Preliminary short data sheet	-	A700X_FAM_SDS v.2.0
Modifications:	• New product type A7003/4 supporting ISO/IEC 7816 contact interface. • New product type A7005/6 supporting ISO/IEC 7816 contact interface and ISO/IEC 14443 A contactless interface. • New product types upgraded to JCOP 2.4.2 R1 with IO Configuration and Control API support.			
A700X_FAM_SDS v.2.0	20110825	Preliminary short data sheet	-	A7001AG_SDS v.1.1
Modifications:	• New product type A7002 supporting −40 °C to +90 °C operational ambient temperature range. • Sleep mode current reduced from 50 μA (typical) to 40 μA (typical).			
A7001AG_SDS v.1.1	20110318	Preliminary short data sheet	-	A7001AG_SDS v.1.0
Modifications:	• Product naming updated.			
A7001AG_SDS v.1.0	20110211	Preliminary short data sheet	-	-
Modifications:	• Initial version.			

All information provided in this document is subject to legal disclaimers.

© NXP B.V. 2013. All rights reserved.

12. Legal information

12.1 Data sheet status

Document status[1][2]	Product status[3]	Definition
Objective [short] data sheet	Development	This document contains data from the objective specification for product development.
Preliminary [short] data sheet	Qualification	This document contains data from the preliminary specification.
Product [short] data sheet	Production	This document contains the product specification.

[1] Please consult the most recently issued document before initiating or completing a design.

[2] The term 'short data sheet' is explained in section "Definitions".

[3] The product status of device(s) described in this document may have changed since this document was published and may differ in case of multiple devices. The latest product status information is available on the Internet at URL http://www.nxp.com.

12.2 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.

Short data sheet — A short data sheet is an extract from a full data sheet with the same product type number(s) and title. A short data sheet is intended for quick reference only and should not be relied upon to contain detailed and full information. For detailed and full information see the relevant full data sheet, which is available on request via the local NXP Semiconductors sales office. In case of any inconsistency or conflict with the short data sheet, the full data sheet shall prevail.

Product specification — The information and data provided in a Product data sheet shall define the specification of the product as agreed between NXP Semiconductors and its customer, unless NXP Semiconductors and customer have explicitly agreed otherwise in writing. In no event however, shall an agreement be valid in which the NXP Semiconductors product is deemed to offer functions and qualities beyond those described in the Product data sheet.

12.3 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. NXP Semiconductors takes no responsibility for the content in this document if provided by an information source outside of NXP Semiconductors.

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 and its suppliers accept 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.

Limiting values — Stress above one or more limiting values (as defined in the Absolute Maximum Ratings System of IEC 60134) will cause permanent damage to the device. Limiting values are stress ratings only and (proper) operation of the device at these or any other conditions above those given in the Recommended operating conditions section (if present) or the Characteristics sections of this document is not warranted. Constant or repeated exposure to limiting values will permanently and irreversibly affect the quality and reliability of the device.

Terms and conditions of commercial sale — NXP Semiconductors products are sold subject to the general terms and conditions of commercial sale, as published at http://www.nxp.com/profile/terms, unless otherwise agreed in a valid written individual agreement. In case an individual agreement is concluded only the terms and conditions of the respective agreement shall apply. NXP Semiconductors hereby expressly objects to applying the customer's general terms and conditions with regard to the purchase of NXP Semiconductors products by customer.

No offer to sell or license — Nothing in this document may be interpreted or construed as an offer to sell products that is open for acceptance or the grant, conveyance or implication of any license under any copyrights, patents or other industrial or intellectual property rights.

All information provided in this document is subject to legal disclaimers.

© NXP B.V. 2013. All rights reserved.

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.

Quick reference data — The Quick reference data is an extract of the product data given in the Limiting values and Characteristics sections of this document, and as such is not complete, exhaustive or legally binding.

Non-automotive qualified products — Unless this data sheet expressly states that this specific NXP Semiconductors product is automotive qualified, the product is not suitable for automotive use. It is neither qualified nor tested in accordance with automotive testing or application requirements. NXP Semiconductors accepts no liability for inclusion and/or use of non-automotive qualified products in automotive equipment or applications.

In the event that customer uses the product for design-in and use in automotive applications to automotive specifications and standards, customer (a) shall use the product without NXP Semiconductors' warranty of the product for such automotive applications, use and specifications, and (b) whenever customer uses the product for automotive applications beyond NXP Semiconductors' specifications such use shall be solely at customer's own risk, and (c) customer fully indemnifies NXP Semiconductors for any liability, damages or failed product claims resulting from customer design and use of the product for automotive applications beyond NXP Semiconductors' standard warranty and NXP Semiconductors' product specifications.

Translations — A non-English (translated) version of a document is for reference only. The English version shall prevail in case of any discrepancy between the translated and English versions.

12.4 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.

12.5 Trademarks

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

FabKey — is a trademark of NXP B.V.

I²C-bus — logo is a trademark of NXP B.V.

13. Contact information

For more information, please visit: **http://www.nxp.com**

For sales office addresses, please send an email to: **salesaddresses@nxp.com**

All information provided in this document is subject to legal disclaimers.

© NXP B.V. 2013. All rights reserved.

14. Tables

Table 1. JCOP V2.4.2 commercial name format 3
Table 2. Quick reference data 8
Table 3. Ordering information 9
Table 4. A700x family feature table 9
Table 5. JCOP V2.4.2 feature table 10
Table 6. Limiting values 12
Table 7. Abbreviations 13
Table 8. Revision history 15

15. Figures

Fig 1. A700x family block diagram 11
Fig 2. System overview supporting Power-on Reset . . 12

16. Contents

1 General description 1
1.1 Overview 1
1.2 A700x family naming conventions 3
1.3 X509 certificate-based client authentication . . . 3
1.4 Trust provisioning service 3
1.5 JCOPX - Additional Application Programming Interface (APIs) features 4
1.6 Security features 4
1.7 Security licensing 5
2 Features and benefits 6
2.1 Standard family features 6
2.2 Product-specific features 6
3 Applications 8
3.1 Application areas 8
4 Quick reference data 8
5 Ordering information 9
5.1 Ordering options 9
5.1.1 Samples and final products 10
5.1.2 Ordering A700x family samples 10
5.1.3 Ordering JCOP products 10
5.1.4 JCOP tools 10
6 Block diagram 11
7 Limiting values 12
8 Application information 12
9 Abbreviations 13
10 References 14
11 Revision history 15
12 Legal information 16
12.1 Data sheet status 16
12.2 Definitions 16
12.3 Disclaimers 16
12.4 Licenses 17
12.5 Trademarks 17
13 Contact information 17
14 Tables 18
15 Figures 18
16 Contents 18

Please be aware that important notices concerning this document and the product(s) described herein, have been included in section 'Legal information'.

© NXP B.V. 2013. All rights reserved.

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

Date of release: 5 July 2013
202031

Document identifier: A700X_FAM_SDS

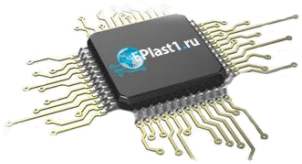
Компания «ЭлектроПласт» предлагает заключение долгосрочных отношений при поставках импортных электронных компонентов на взаимовыгодных условиях!

Наши преимущества:

- Оперативные поставки широкого спектра электронных компонентов отечественного и импортного производства напрямую от производителей и с крупнейших мировых складов;
- Поставка более 17-ти миллионов наименований электронных компонентов;
- Поставка сложных, дефицитных, либо снятых с производства позиций;
- Оперативные сроки поставки под заказ (от 5 рабочих дней);
- Экспресс доставка в любую точку России;
- Техническая поддержка проекта, помощь в подборе аналогов, поставка прототипов;
- Система менеджмента качества сертифицирована по Международному стандарту ISO 9001;
- Лицензия ФСБ на осуществление работ с использованием сведений, составляющих государственную тайну;
- Поставка специализированных компонентов (Xilinx, Altera, Analog Devices, Intersil, Interpoint, Microsemi, Aeroflex, Peregrine, Syfer, Eurofarad, Texas Instrument, Miteq, Cobham, E2V, MA-COM, Hittite, Mini-Circuits,General Dynamics и др.);

Помимо этого, одним из направлений компании «ЭлектроПласт» является направление «Источники питания». Мы предлагаем Вам помощь Конструкторского отдела:

- Подбор оптимального решения, техническое обоснование при выборе компонента;
- Подбор аналогов;
- Консультации по применению компонента;
- Поставка образцов и прототипов;
- Техническая поддержка проекта;
- Защита от снятия компонента с производства.



Как с нами связаться

Телефон: 8 (812) 309 58 32 (многоканальный)
Факс: 8 (812) 320-02-42
Электронная почта: org@eplast1.ru
Адрес: 198099, г. Санкт-Петербург, ул. Калинина, дом 2, корпус 4, литера А.