A710x family

Secure authentication microcontroller

Rev. 3.5 — 1 November 2013
195735

Product short data sheet
COMPANY PUBLIC

1. General description

1.1 Overview

The A710x 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 had been used in all kind of security applications like bank cards, health insurance cards, electronic passports, pay-tv cards or as embedded secure element in mobile phones. The A710x 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 A710x family supports the following features:

- Dedicated MX51 security CPU
- 400 kbit/s I^2C Fast-mode interface
- Four wire 2 Mbit SPI interface
- 111 kbit/s One-Wire Interface according to Ref. 16 (A7103)
- –40 °C to +90 °C operational ambient temperature (A7102)
- Optional on-chip operating system firmware: JCOP 2.4.2 (A710xC)
- Optional X.509 certificate-based client authentication application pre-installed
- Optional on-chip cryptographic library
- NXP glue logic
- NXP secure fetch technology
- Active shielding technology
- Asynchronous self-timed Handshake Technology
- 20 KB EEPROM for application-code and data
- 40 μA typical sleep mode current with I^2C pads in tristate mode
- 10 μA max deep sleep mode current with I^2C pads in tristate mode
- High-performance secured Public Key Infrastructure (PKI) coprocessor (RSA up to 4096-bit keys, ECC over GF(p) up to 544-bit keys)
- Secured 2-key/3-key triple-DES coprocessor
- Secured AES coprocessor (128-, 192- and 256-bit keys)
- EEPROM with min 500,000 cycles endurance and min 25 years retention time
- Four general-purpose IO ports (partly multiplexed with the I^2C and SPI interface)
- Broad range of tiny package types, i.e. WLCSP

The A710x family key benefits:

- 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 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]:

- Hardware Data Sheet A710x family, Secure authentication microcontroller, Document Number DocID 2164xx[2] (see Ref. 8).

  The hardware data sheet explains the details of the A710x family product from a hardware point of view. It outlines figures like pinning diagram and power consumption but also provides all information needed to develop firmware running on the chip (ROM code).

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

1.2 Cryptographic hardware coprocessors

1.2.1 PKI coprocessor

The approved and modular PKI coprocessor architecture supports the trend of increasing RSA keys with faster execution speeds as well as Elliptic Curve Cryptography (ECC) based on GF(p) or GF(2^n) at best performance. The PKI coprocessor supports RSA with an operand length of up to 8-kbit (up to 4-kbit with intermediate storage in RAM only).

The PKI coprocessor supports 192-bit ECC key length that offers the same level of security as 2048-bit RSA. An ECC GF(2^n) based signature, using a 163-bit key can be executed in less than 30 ms providing a security level comparable to 1024-bit RSA. The operand size for ECC is only limited by the 2.5 KB size of the Crypto-RAM. The PKI coprocessor is easy to use and the flexible interface provides programmers with the flexibility to implement their own cryptography solutions.

1.2.2 Triple-DES coprocessor

The DES widely used for symmetric encryption is supported by a dedicated, high performance, highly attack-resistant hardware coprocessor. Single DES and triple-DES, based on two or three DES keys, can be executed within less than 40 μs. Relevant standards (ISO/IEC, ANSI, FIPS) and Message Authentication Code (MAC) are fully supported.

1.2.3 AES coprocessor

The A710x family secure microcontroller platform provides a dedicated high performance 128-bit parallel processing coprocessor to support secure AES. The implementation is based on FIPS197 as standardized by the National Institute for Standards and Technology (NIST), and supports key lengths of 128-bit, 192-bit, and 256-bit with performance levels comparable to DES. AES is the next generation for symmetric data encryption and recommended successor of DES providing a significantly improved security level.

1.3 I^2C interface

The A710x family has an I^2C interface supporting data rates up to 400 kbit/s operating in Fast-Mode (FM) as specified in Ref. 4. Both operating modes, Master and Slave are supported. The I^2C address is configurable by the embedded firmware.

1.4 SPI interface

The A710x family has a four wire SPI slave interface supporting data rates up to 2 Mbit for full-duplex and synchronous data transfer.

1.5 Universal Asynchronous Receiver/Transmitter (UART)

The A7103 uses a built-in Universal Asynchronous Receiver/Transmitter (UART) to support a Smart Card OneWire (SC1W) Protocol as specified in Ref. 16. The Protocol is using a one-wire based physical interface, a UART-based data link layer, an SMBus based network layer as well as a mapping layer to convey ISO/IEC 7816-4 based communication. The UART is software configurable to use any of the four IO ports.

1.6 General-Purpose IO ports

The A710x family has four general-purpose IO ports (partly multiplexed with the UART, I^2C and SPI interface) which can be used for any purpose.

1.7 Optional on-chip cryptographic library

A secure crypto library providing a broad range of required functions will be available for all A710x devices in order to support customers implementing cryptographic solutions:

- Various algorithms
  - AES encryption and decryption using the AES coprocessor
  - DES and Triple-DES encryption and decryption using the DES coprocessor
  - RSA encryption and decryption, signature generation and verification for straightforward and CRT keys up to 4096-bit
  - RSA key generation
  - ECC over GF(p) signature generation and verification (ECDSA) and Diffie-Hellman key exchange for keys up to 544 bits
  - ECC over GF(p) key generation
  - ECC over GF(2^n) signature generation and verification (ECDSA) and Diffie-Hellman key exchange for keys up to 544-bit
  - ECC over GF(2^n) key generation
  - SHA-1, SHA-224 and SHA-256 hash algorithm
  - Pseudo-Random Number Generator (PRNG)
- Easy to use API for all algorithms
- Latest built-in security features to avoid power (SPA/DPA), timing and fault attacks (DFA)

1.8 Optional on-chip operating system firmware: JCOP 2.4.2 (A710xC)

The A710x family can execute program code from its internal memories. The ROM is used to host program code and data either owned by NXP Semiconductors or provided by third-parties (custom ROM masked product).

NXP Semiconductors offers a Java Card Open Platform operating system called JCOP based on independent, third-party specifications, i.e. by Oracle, the Global Platform consortium, the International Organization for Standards (ISO), EMV (Europay, MasterCard and VISA) and others. The Java Card and GlobalPlatform industry standards together ensure ease of application development and application interoperability for developers. JCOP 2.4.2 compliant to Java Card specification V3.0.1 classic as defined in Ref. 1 JCOP 2.4.2 compliant to Global Platform specification as defined in Ref. 2 and Ref. 3.

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)
- A710xC (JCOP 2.4.2 R1): Support of IO Config and Control API, implementing methods to reconfigure the default I^2C slave address, to configure the GPIO pin as either input or output pin and the read, set or clear the pin.

For more detailed information refer to following documentation[3]:

- User manual JCOP 2.4.2 Revision 1.0, JCOP V2.4.2 Revision 1.0 secure A7 MCU operating system, Document Number 2318xx[4] (see Ref. 10).

  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 A710x family products.
- Administrator manual JCOP 2.4.2 Revision 1.0, JCOP V2.4.2 Revision 1.0 secure A7 MCU operating system, Document Number 2319xx[4] (see Ref. 11).
  The Administrator manual describes JCOP for the administrator of a JCOP operating system. This means it explains the pre-personalization process and its specific commands.
- Hardware Data sheet, A710x family, secure authentication microcontroller, Document Number 2164xx[4] (see Ref. 8).

  The Full data sheet explains the details of the A710x family product from a hardware point of view. It outlines figures like pinning diagram and power consumption.
- A710x family with JCOP 2.4.1R1, secure authentication microcontroller, Document Number 2366xx[4] (see Ref. 9).

  The data sheet explains the details of the A710x family product embedding a JCOP 2.4.2 R1 operating system from a hardware point of view. It outlines figures like pinning diagram and power consumption.

1.9 Optional X509 certificate-based client authentication

In addition to the A710x family secure MCU and the Java Card Open Platform operating system, the total solution includes an X.509 certificate-based client authentication application.

For more detailed information refer to following documentation:

- Application note, Device Authentication APDU Specification, Document Number 2118xx[4] (see Ref. 12).

  The applet user manual contains a detailed description of the authentication application on the A710x family product. It outlines the interface description including the APDU description and a description how to use the applet.

3. These documents are available under NDA
4. Where XX refers to the last version; e.g. 10 refers to version 1.0

1.10 Trust provisioning service

The A710x family is delivered with pre-programmed, die-specific keys and certificates which are being generated and programmed in a certified (Common Criteria) secure NXP Semiconductors internal environment with master keys 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.

1.11 A710x family naming conventions

The following table explains the naming conventions of the commercial product name of the A710x family products. Every A710x family product gets assigned such a commercial name, which includes also customer and application-specific data.

The A710x family commercial names have the following format.

A710xagpp(p)/mvsrrff

The 'A710' is a constant, all other letters are variables, which are explained in the following Table 1.

Table 1. A710x commercial name format

Variable	Meaning	Values	Description
x	IC hardware specification code	1	standard operational ambient temperature: −25 °C to +90 °C I^2C and SPI interface supported
		2	standard operational ambient temperature: −40 °C to +90 °C I^2C and SPI interface supported
		3	standard operational ambient temperature: −25 °C to +90 °C. I^2C and UART interface supported
a	embedded operating system code	A	JCOP V2.4.2 R0.95
		C	JCOP V2.4.2 R1
		Z	Custom ROM coded product
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	

Table 1. A710x commercial name format

Variable	Meaning	Values	Description
s	Silicon Version Subcode	B	
rr	ROM Code ID		
ff	FabKey ID		

1.12 Security features

The A710x family security concept is combining a comprehensive portfolio of NXP Semiconductors security measures which is protecting the chip against all types of attacks. All in all there are more than 100 security features in an NXP Semiconductors 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 counter measures against reverse engineering attacks i.e. the dedicated security CPU designed in asynchronous handshaking circuit technology, the very dense sub-micron 5-metal-layer 0.14 μm technology, the NXP glue logic and active shielding technology are providing highest level of attack resilience which is unique in the market.

Secure Fetch Technology will significantly enhance 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 and against both those with shorter and with longer light pulses; both with single and with 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 A710x 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 1st order DPA, thus equally well resilient against all kinds of leakage attacks.

The A710x 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 sub-micron 5-metal-layer 0.14 μm CMOS technology,
- NXP glue logic
- Active Shielding
- Enhanced security sensors
  - Low and high temperature sensor (for A7101 and A7103 only)
  - Low and high supply voltage sensor
  - Single Fault Injection (SFI) attack detection
  - Light sensors (incl. integrated memory light sensor functionality)

1.13 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.

2. Features and benefits

2.1 Standard family features

- High reliable EEPROM for both data storage and program execution: 20 KB
  - Data retention time: 25 years minimum
  - Endurance: 500,000 cycles minimum
- Dedicated Secure_MX51 MCU (Memory eXtended/enhanced 80C51)
- 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 4096-bit
  - Elliptic Curve over GF(p) Cryptography with key lengths up to 544-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
- On-Chip Key generation
- CRC calculations
- Low-power design using NXP Semiconductors' handshaking technology
- Wake-up from SLEEP mode by any I^2C communication request
- 40 μA typical sleep mode current with I^2C pads operated in tristate mode, don't obstructing the bus lines
- 10 μA maximal deep sleep mode current with I^2C pads operated in tristate mode, don't obstructing the bus lines
- Internally generated CPU clock (typical 31 MHz)
- 1.62 V to 3.6 V operating voltage range
- Broad spectrum of delivery types
  - Wafers
  - WL-CSP package
  - SMD packages

2.2 Product-specific features

- A7101
  - −25 °C to +90 °C operational ambient temperature
  - 400 kbit/s I^2C Fast-mode interface (Master and Slave)
  - 2 Mbit four wire SPI interface (Slave)
- A7102
  - −40 °C to +90 °C operational ambient temperature
  - 400 kbit/s I^2C Fast-mode interface (Master and Slave)
  - 2 Mbit four wire SPI interface (Slave)
- A7103
  - −25 °C to +90 °C operational ambient temperature
  - 111 kbit/s One-Wire Interface according to Ref. 16
  - 400 kbit/s I^2C Fast-mode interface (Master and Slave)

3. Applications

The A710x 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 A710x 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 today's demanding embedded security requirements. The A710x family can be used in various host platforms and host operating systems to secure a broad range of applications.

The A710x 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, SPI and UART interfaces.

The flexibility of the A710x 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	-	3.6	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

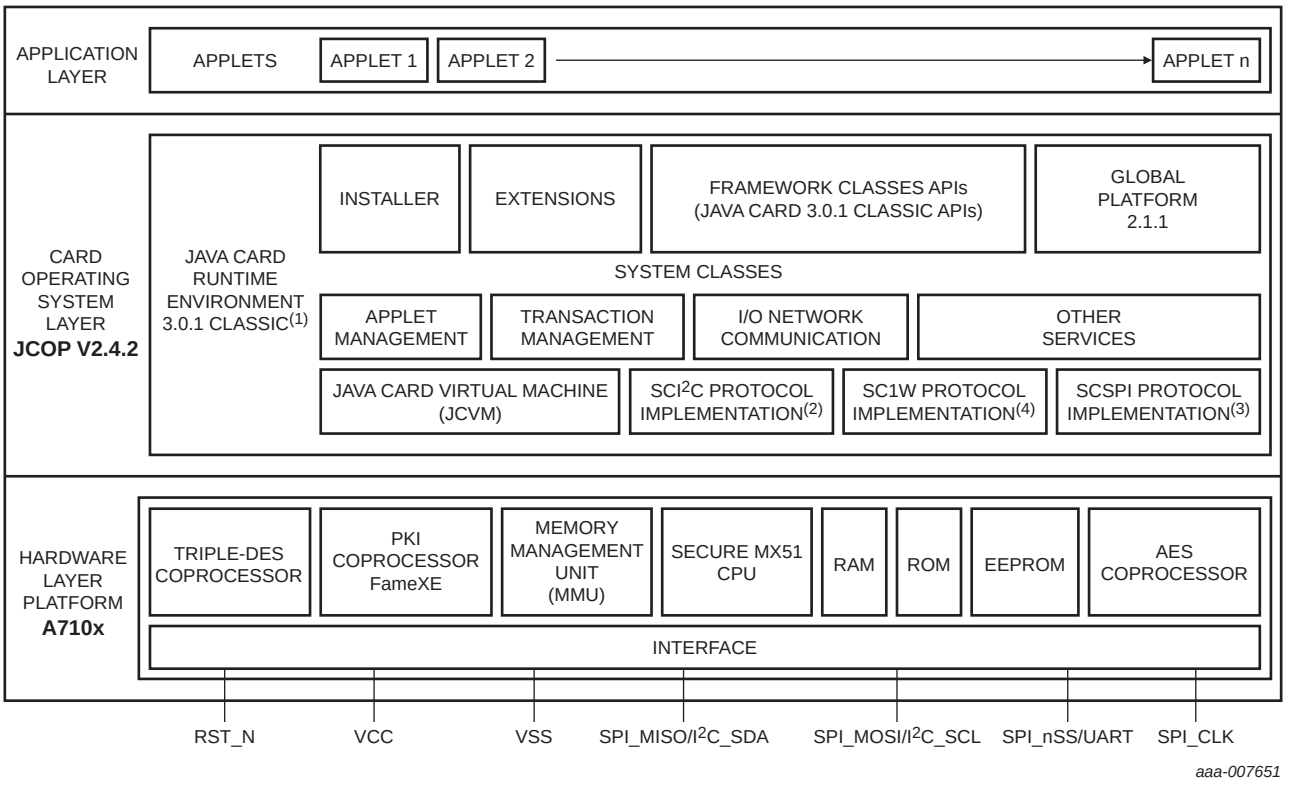
5. Ordering information

Table 3. Ordering information

Type number[1]	Package		
	Name	Description	Version
A7101agUS/...	FFC	8 inch wafer (sawn; 250 μm thickness; on film frame carrier; electronic fail die marking according to SECSII format)	not applicable
A7102agUS/...			
A7103agUS/...			
A7101agUK/...	WLCSP12	wafer level chip scale package, 12 bumping, body 2.1 × 2.1 × 0.6 mm; 0.5 mm ball pitch	not applicable
A7102agUK/...			
A7103agUK/...			
A7101agT1/...	SO-8	plastic small outline package, body 4.9 × 3.9 × 1.75 mm; 1.27 mm pin pitch, 8 leads	SOT096-1
A7102agT1/...			
A7103agT1/...			
A7101agTK2/...	HVSON-8	plastic thermal enhanced very thin small outline package; no leads; 8 terminals; body 4 × 4 × 0.85 mm	SOT909-1
A7102agTK2/...			
A7103agTK2/...			
A7101agHN1/...	HVQFN32	plastic thermal enhanced very thin quad flat package; no leads, 32 terminals; body 5 × 5 × 0.85 mm	SOT617-3
A7102agHN1/...			
A7103agHN1/...			
A7101agHN2/...	HVQFN20	plastic thermal enhanced very thin quad flat package; no leads, 20 terminals; body 4 × 4 × 0.85 mm	SOT917-1
A7102agHN2/...			
A7103agHN2/...			

[1] a = A or C, g = G, C or A, according to the A710x family type classification see Section 1.11 “A710x family naming conventions”

6. Block diagram



(1) For more details see Ref. 5 Figure 3.4 page 36

(2) For more details see Ref. 6

(3) For more details see Ref. 6

(4) For more details see Ref. 16

Fig 1. A710x family block diagram with JCOP OS

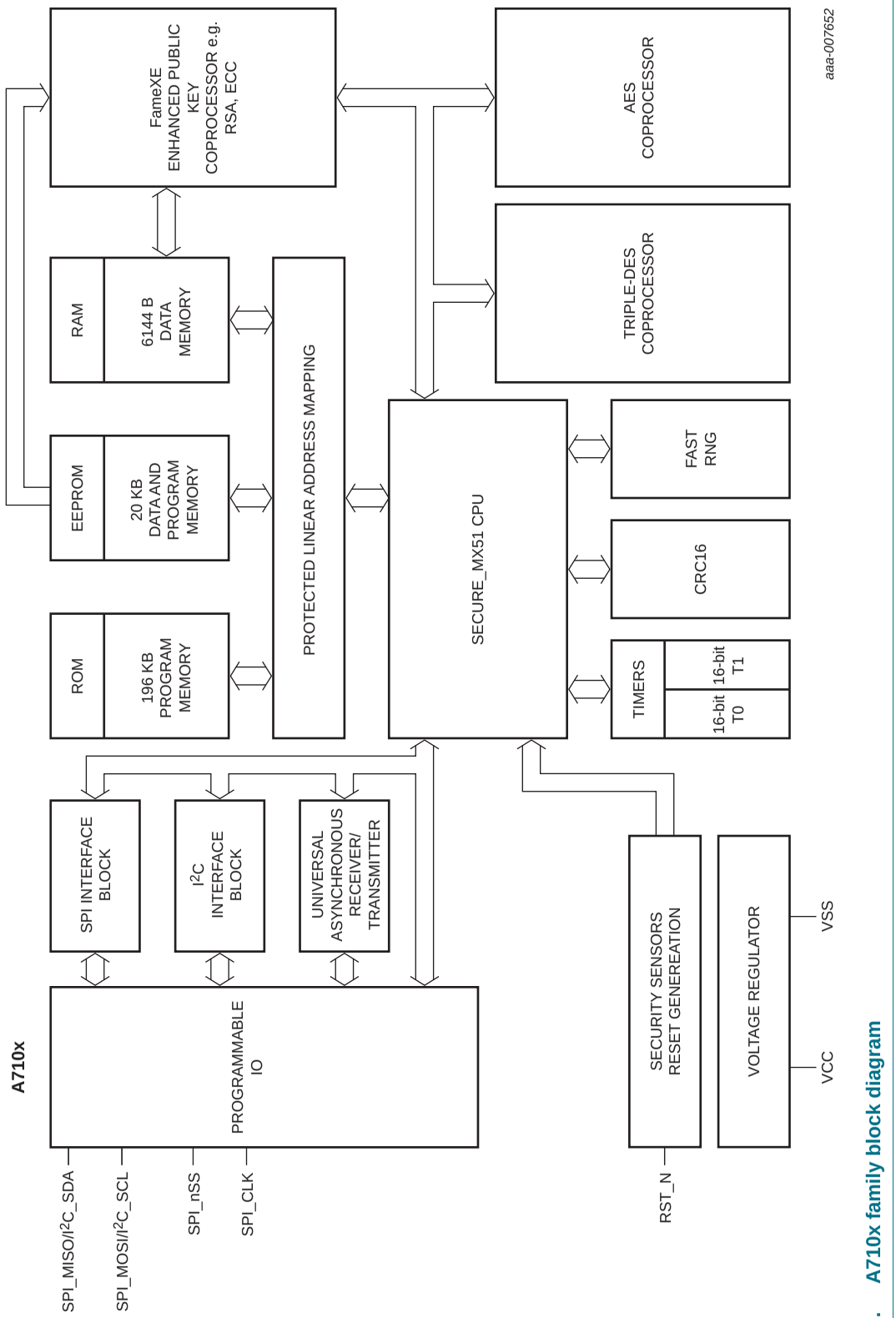


Fig 2. A710x family block diagram

7. Limiting values

Table 4. 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			–0.3	+4.6	V
V_I	input voltage	any signal pad		–0.3	+4.6	V
I_I	input current	pad SPI_nSS/UART_IO, SPI_MISO/I2C_SDA, SPI_CLK, SPI_MOSI/I2C_SCL		-	10	mA
I_O	output current	pad SPI_nSS/UART_IO, SPI_MISO/I2C_SDA, SPI_CLK, SPI_MOSI/I2C_SCL		-	10	mA
I_{lu}	latch-up current	$V_I < 0$ V or $V_I > V_{DD}$		-	100	mA
V_{ESD}	electrostatic discharge voltage	Human Body Model (HBM)	[1][2]		± 2.0	kV
		Charge Device Model (CDM)	[1][3]		± 500	V
P_{tot}	total power dissipation		[4]	-	1	W
T_{stg}	storage temperature			–55	+125	°C

[1] pads VCC, VSS, RST_N, SPI_nSS/UART_IO, SPI_MISO/I2C_SDA, SPI_CLK, SPI_MOSI/I2C_SCL

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

[3] JESD22-C101, JEDEC Standard Field induced charge device model test method.

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

8. Abbreviations

Table 5. 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 CodeBook
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
SPI	Serial Peripheral Interface

9. 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] I^2C-bus specification and user manual, Rev. 0.3 — June-19-2007, NXP Semiconductors

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

[6] SCI^2C Protocol Specification, Rev. 2.0 — Aug-04-2010, NXP Semiconductors

[7] SC-SPI Protocol Specification, Rev. 1.0 — Mar-01-2011, NXP Semiconductors

[8] Hardware Data Sheet A710x family, Secure authentication microcontroller, Document Number DocID 2164xx[5], NXP Semiconductors

[9] A710x family with JCOP 2.4.2 R1, Secure authentication microcontroller, Document Number 2366xx[5], NXP Semiconductors

[10] 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[5], NXP Semiconductors

[11] 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[5], NXP Semiconductors

[12] Application note, Device Authentication APDU Spec - FS1.1, Document Number 2185xx[5], NXP Semiconductors

[13] Application note, Device Authentication Architecture, Application Note for Feature Set FS1.1, Document Number 2154xx[5], NXP Semiconductors

[14] Application note, X.509 Device Certificate Format, Document Number 2119xx[5], NXP Semiconductors

[15] Application note, Device Authentication Host library API, Document Number 2196xx[5], NXP Semiconductors

[16] SC1W Protocol Specification, Rev. 1.1, NXP Semiconductors

[17] SOT909-1; HVSON8; Reel pack; Ordering code (12NC) ending 118; Packing Information; Rev. 2 — 19 April 2013

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

10. Revision history

Table 6. Revision history

Document ID	Release date	Data sheet status	Change notice	Supersedes
A710X_FAM_SDS v.3.5	20131101	Product short data sheet		A710X_FAM_SDS v.3.4
Modifications:	• Updated storage temperature in Table 4 “Limiting values” on page 14			
A710X_FAM_SDS v.3.4	20130809	Product short data sheet		A710X_FAM_SDS v.3.3
Modifications:	• Inserted A7103 product type supporting UART communication • Reference to HVSON8 packing information added • Inserted electrostatic discharge voltage (Charge Device Model) in Table 4 “Limiting values” on page 14			
A710X_FAM_SDS v.3.3	20130315	Product short data sheet		A710X_FAM_SDS v.3.2
Modifications:	• Chapter 7 “Pinning Information” removed from product short data sheet			
A710X_FAM_SDS v.3.2	20130128	Product short data sheet		A710X_FAM_SDS v.3.1
Modifications:	• SO8 pinning figure corrected. See also Figure 8 “Pin configuration for SO-8 (SOT96-1)” on page 16			
A710X_FAM_SDS v.3.1	20121213	Product short data sheet		A710X_FAM_SDS v.3.0
Modifications:	• HVQFN32 pinning corrected. SPI_nSS is connected to pin 3 and pin 2 is not connected. See also Figure 7 “Pin configuration for HVQFN32 (SOT617-3)” on page 15 and Table 7 on page 15 • HVSON8 package (SOT685-1, 5 mm × 6 mm) removed from Table 3 “Ordering information” on page 11 • Footnote about availabilty of HVQFN20 package removed. HVQFN20 package is available. • Defined maximum input and output currents in Table 4 “Limiting values” on page 14			
A710X_FAM_SDS v.3.0	20121024	Product short data sheet		A710X_FAM_SDS v.2.0
Modifications:	• Product version			
A710X_FAM_SDS v.2.0	20111005	Preliminary short data sheet		-
Modifications:	• Initial version			

11. Legal information

11.1 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.

11.2 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.

11.3 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.

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.

11.4 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.

11.5 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.

I^2C-bus — logo is a trademark of NXP B.V.

12. Contact information

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

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

13. Tables

14. Figures

15. Contents

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

Date of release: 1 November 2013
195735