A7001AG

Secure authentication microcontroller

Rev. 1.1 — 18 March 2011
202011

Preliminary short data sheet
COMPANY PUBLIC

1. General description

1.1 Overview

The A7001AG is a tamper resistant secure Micro Controller Unit (MCU) 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 A7001AG 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 A7001AG supports the following features:

- 100 kbit/s I^2C slave interface
- NXP patented glue logic™
- NXP secure fetch technology™
- Active shielding technology
- Asynchronous self-timed Handshake Technology
- Dedicated MX51 security CPU
- 72 KB EEPROM for application-code and data
- 50 μA typical sleep mode current with I^2C pads operated in weak pull-up mode, don't obstructing 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)
- EEPROM with minimum 500 000 cycles endurance and minimum 25 years retention time
- On-chip operating system firmware: JCOP 2.4.2 R1
- 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 A7001AG runs 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.

The A7001AG 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]:

- Administrator manual, A7001AG, Doc.No. 1887xx[2]
- User manual, A7001AG, Doc.No. 18821xx
- Hardware data sheet, A7001AG, secure smart card controller, Doc.No. xx

The Administrator manual describes JCOP for the administrator of a JCOP secure element. This means it explains the pre-personalisation process and its specific commands.

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 A7001AG products.

The Hardware data sheet explains the details of the A7001AG product from a hardware point of view. It outlines figures like pinning diagram and power consumption.

1.2 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

More details about the JCOPX API can be found in JCOP User Manual.

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

1.3 Security features

The A7001AG security concept is combining a comprehensive portfolio of NXP 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 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 patented 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 A7001AG security concept includes dedicated HW measures to protect against any kind of leakage attacks. The Triple-DES coprocessor is mathematically proven leak-resistance to 1st order DPA, thus equally well resilient against all kinds of leakage attacks.

The A7001AG 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 patented glue logic™
- Enhanced security sensors
  - Low and high temperature sensor
  - Low and high supply voltage sensor
  - Single Fault Injection (SFI) attack detection
  - Light sensors (incl. integrated memory light sensor functionality)

1.4 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 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
- 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
- 50 μA typical sleep mode current with I^2C pads operated in weak pull-up mode, don't obstructing the bus lines
- Internally generated CPU clock (typical 62 MHz)
- 1.62 V to 5.5 V operating voltage range
- −25 °C to +85 °C operational ambient temperature

3. Applications

The A7001AG 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 A7001AG 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 A7001AG can be used in various host platforms and host operating systems to secure a broad range of applications.

The A7001AG 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.

In addition to the A7001AG secure MCU, the total solution includes MCU firmware and an X.509 certificate authentication application. The A7001AG 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 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.

The flexibility of the A7001AG 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 1. 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

5. Ordering information

Table 2. Ordering information

Type number	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
A7001AGHN3/...	HVSON-8	plastic thermal enhanced very thin small outline package; no leads; 8 terminals; body 6 × 5 × 0.85 mm	SOT685-1
A7001AGHN1/...	HVQFN32	plastic thermal enhanced very thin quad flat package; no leads, 32 terminals; body 5 × 5 × 0.85 mm	SOT617-1

5.1 Ordering options

The following sections describe information how to order samples and final products.

5.1.1 Ordering A7001AG samples

Samples in HVQFN32 package can be ordered from NXP Semiconductors.

Note that NXP Semiconductors can provide up to 10 pcs 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.

5.1.2 Ordering JCOP products

NXP Semiconductors has created a generic product type that is available for ordering.

This product will have one card manager authentication key for all parts.

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 applet code.

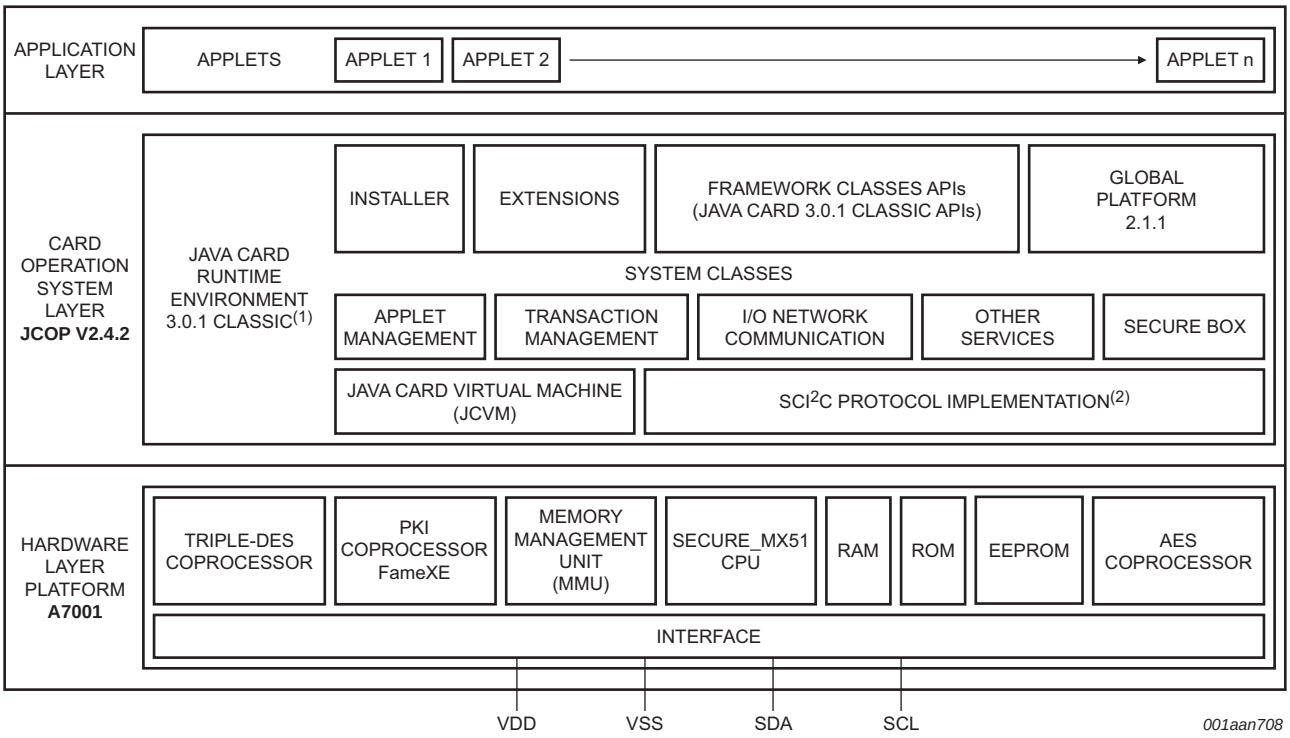
Contact your local NXP Semiconductors representative for further information.

5.1.3 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.

6. Block diagram



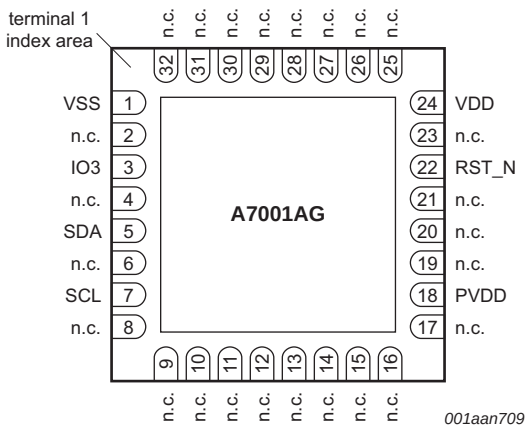
(1) For more details see Ref. 4 Figure 3.4 page 36

(2) For more details see Ref. 5

Fig 1. A7001AG block diagram

7. Pinning information

7.1 Pinning



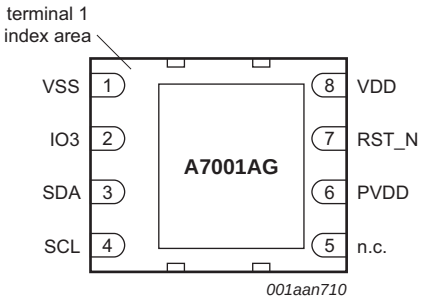
Transparent top view

n.c. = not connected / reserved = not to be connected

Fig 2. Pin configuration HVQFN32 (SOT617-3)

Table 3. Pin description

Symbol	Pin	Description
VSS	1	Ground supply voltage
N.C.	2	not connected
IO3	3	Input/Output #3 for serial data, not used by embedded firmware, set to TriState High Z Input
N.C.	4	not connected
SDA	5	I^2C Data
N.C.	6	not connected
SCL	7	I^2C Clock
N.C.	8 to 17	not connected
PVDD	18	Requires connection via pull-up resistor to VDD
N.C.	19 to 21	not connected
RST_N	22	Reset input, active LOW
N.C.	23	not connected
VDD	24	Supply voltage
N.C.	25 to 32	not connected



Transparent top view

Fig 3. Pin configuration for HVSON-8 (SOT685-1)

Table 4. Pin description

Symbol	Pin	Description
VSS	1	Ground supply voltage
IO3	2	Input/Output #3 for serial data, not used by embedded firmware, set to TriState High Z Input
SDA	3	I^2C Data
SCL	4	I^2C Clock
N.C.	5	Not connected
PVDD	6	Requires connection via pull-up resistor to VDD
RST_N	7	Reset input, active LOW
VDD	8	Supply voltage

8. Memory

8.1 Available memory space

Table 5. A7001AG Memory Map

Product type	Transient Heap (RAM)	Persistent Heap (EEPROM)	Free ROM for Applets	APDU Buffer
A7001AG	3550 bytes	79900 bytes	133648 bytes	1462 bytes

8.2 Garbage collection

Garbage collection is fully implemented (see Ref. 1): Deleted objects, applets, and packages are fully reclaimed (incl. compactification) and the space can be used for other purposes after deletion.

9. 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 IO1, IO2 or IO3		-	±15.0	mA
I_O	output current	pad IO1, IO2 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, CLK, RST_N, IO1, IO2, IO3	[1]	-	±4.0	kV
		pads LA, LB	[1]	-	±2.0	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*.

10. Application information

Figure 4 shows a typical application diagram. It shows how the pins of the A7001AG shall be applied in order to operate the IC in an I^2C system as I^2C slave device. In this system an individual reset control is not supported. The hardware reset will be executed at power-up time (power-on reset).

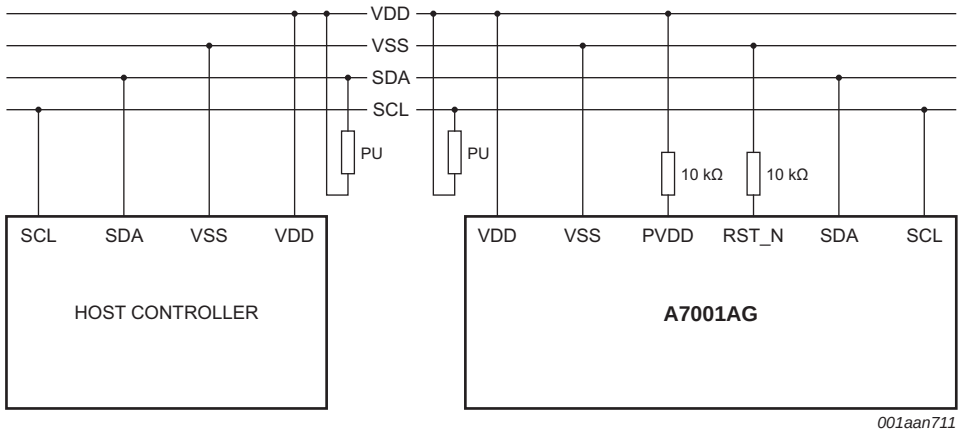


Fig 4. System overview supporting Power-on Reset

11. 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 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

12. 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] SCI²C Protocol Specification, Rev. 2.0 — Aug-04-2010, NXP Semiconductors

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

13. Revision history

Table 8. Revision history

Document ID	Release date	Data sheet status	Change notice	Supersedes
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-			

14. Legal information

14.1 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.

14.2 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.

14.3 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.

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.

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 national 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.

14.4 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.

14.5 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.

15. Contact information

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

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

16. Tables

17. Figures

18. 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: 18 March 2011
202011