A1006

Secure Authenticator IC

Rev. 1 — 25 July 2018 **Product short data sheet**

1. Introduction

The A1006 Secure Authenticator IC is a secure, easy to use authentication IC for use in electronic accessories such as AC/DC adapters, cables, keyboards, docking stations, batteries, digital headsets, electronic cigarettes etc., for authentication and anti-counterfeiting purposes.

NXP Semiconductors has a long track record and extensive portfolio of security ICs. NXP security ICs have been used in many high security applications including bank cards, health insurance cards, and electronic passports. They are also being used as embedded secure elements in mobile phones.

The A1006 secure authentication IC extends this portfolio for applications requiring tamper-resistant, secure, one-way authentication.

The A1006 authentication IC is a secure solution built with many tamper resistant features and security countermeasures to deter common invasive and non-invasive attacks.

2. General description

The A1006 Secure Authenticator Solution is a complete embedded security platform for electronic accessories, mobile phones, portable devices, computing and consumer electronic devices, and embedded systems where a strong security infrastructure is required for authentication and counterfeit detection and prevention. The A1006 provides an outstanding level of security, while overcoming the challenges of performance, power consumption and solution footprint.

The A1006 security solution is based on industry standard asymmetric cryptographic challenge-response protocols, using NIST approved elliptic curves, Elliptic Curve Diffie-Hellman challenge response (ECDH), and customizable X.509 certificates signed using the Elliptic Curve Digital Signature Algorithm (ECDSA). Advanced anti-tampering countermeasures are incorporated into the A1006 to prevent various attacks and minimize the scalability of any attempts to clone the A1006.

The A1006 is offered as a turnkey solution that provides customers easy integration into their end products. A 400 kbps I^2C-bus interface along with a one-wire interface provide simple options for interfacing to most embedded systems. A reference host library is provided to simplify host code implementation, and keys and certificates can be programmed in NXP's secure manufacturing facilities, eliminating the need for creating and managing private key insertion and certificate signing in the system designer's supply chain.

3. Features and benefits

- Advanced security using unique asymmetrical public/private key based Diffie-Hellman authentication protocol based on ECC (Elliptic Curve Cryptography) with a NIST B-163 bit strong binary field curve
- Authentication time (on-chip calculations) < 50 milliseconds
- Each A1006 is provisioned with a fixed unique Private Key and a corresponding Public Key in a certificate that contains the Public Key and additional information including a unique identifier and the customizable product-specific fields.
- A1006 certificates are digitally signed using ECDSA (Elliptic Curve Digital Signature Algorithm) based on the NIST P-224 curve and the SHA-224 digest hash, with the customer's desired certificate authority key
- Non-Volatile Memory (NVM) for storage of device behavior, usage data, logistic information or any other arbitrary data
- Protection against Simple Power Analysis (SPA), Differential Power Analysis (DPA) and fault attacks
- One-Wire Interface (OWI) at 125 kbps, with ability to support bus-powered operation
- 400 Kbps I^2C Fast-mode interface
- Power consumption: Maximum of 550 µA active
- Deep Sleep mode with very low power consumption of less than 3.3 µA at 3.3 V and < 1 µA at 1.8 V
- Entry to and exit from the Deep Sleep mode through I^2C/OWI interface[1]
- ESD protection 8kV IEC61000-4-2 contact discharge (on OWI pin)
- EEPROM sections (4 Kbit total)
  - 2 Kbit certificates (2 × 1 Kbit)
  - 1 Kbit user memory
  - 1 Kbit system memory
- Minimum 10 years memory retention at 85 °C
- 500,000 write/erase endurance
- Multiple Package options available
  - HXSON6: Plastic thermal enhanced extremely thin small outline package, no leads
  - WLCSP4: 4 bump Wafer Level Chip Scale Package
- Maximum height 0.5 mm
- Operating temperature range –40 °C to 85 °C

3.1 Trust provisioning service

The A1006 can be delivered with pre-programmed, device-specific keys and certificates that are generated and programmed in a secure NXP internal environment with master keys securely stored in HSMs (Hardware Secure Modules).

1. Separate wakeup pin to wake up from deep sleep state in HXSON6 package

3.2 Security features

The A1006 secure authentication IC incorporates an extensive set of security measures from NXP Semiconductor's portfolio of such measures. The countermeasures against invasive and non-invasive attacks provide a high level of attack resilience. The A1006 countermeasures, including glue logic, active and passive shielding, memory scrambling and encryption, and other security features provide a unique level of security for this class of authentication devices.

The A1006 includes dedicated HW to protect against reverse engineering attacks, fault attacks and leakage attacks.

The A1006 incorporates many security countermeasures, including:

- Mathematically proven design that offers protection against logical and messaging attacks
- Use of active and passive shielding to protect against probe attacks
- EEPROM data encryption and address scrambling with random data placement
- Simple Power Analysis (SPA)/ Differential Power Analysis (DPA) protected calculation of ECC point multiplication
- Proprietary glue logic to thwart circuit analysis
- Enhanced security sensors
  - Low and high supply voltage sensors

4. Applications

- Embedded Security
- Counterfeit protection of hardware and software
  - Anti-cloning
  - Brand integrity of original goods
  - Accessories like speakers, docking stations, batteries, chargers, printer cartridges, e-cigarettes and other high value disposables
- Profile of service
  - Conditional access to software, content and features
  - Secure access to online services
- Secure Device identity

5. Quick reference data

Table 1. Quick reference data

Symbol	Parameter	Conditions	Min	Typ	Max	Unit
V_{DD}	Supply Voltage		1.62[1]	1.8	3.6	V
EEPROM						
t_{ret}	retention time	T_{amb} = +85 °C	10	-	-	years
$N_{endu(W)}$	write endurance	under all operating conditions	5×10^5	-	-	cycles

[1] minimum supply voltage related to the pull-up resistor values. In case of a single A1006 device, this is in the 200 to 500 Ohm range.

6. Ordering information

6.1 A1006 naming conventions

The following table explains the naming conventions of the commercial product name of the A1006 products. Every A1006 product gets assigned such a commercial name, which includes also customer and application specific data.

The A1006 commercial names have the following format.

A1006pp

The ‘A1006’ is a constant, all other letters are variables, which are explained in Table 2.

Table 2. A1006 commercial type name format

Variable	Meaning	Values	Description
pp	package type code	see Table 4	

The following table explains the naming conventions used for A1006 products.

A1006pp/mvsrr

The 'A1006' is the base device part number. The variable letters and digits are explained in Table 3.

Table 3. Naming conventions

Variable	Meaning	Values
pp	package type code	see Table 4
m	manufacturing site code	T
v	silicon version code	A
s	silicon subversion code	1
rr	Fabkey number	Refer to Fabkey chapter for more details

Table 4. Base product types

Type number	Package		
	Name	Description	Version
A1006TL	HXSON6	plastic, thermal enhanced extremely thin small outline package; no leads; 6 terminals; body 2.0 x 2.0 x 0.5 mm	SOT1348-1
A1006UK	WLCSP4	wafer level chip-scale package; 4 bumps; 1.03 x 0.94 x 0.5 mm	SOT1375-4

6.2 Ordering options

Table 5. Ordering options

Type number	Orderable part number	Package	Packing method	Minimum order quantity	Temperature
A1006TL	A1006TL/TA1NXZ[1]	HXSON6	7-inch reel	4000	T_{amb} = –40 °C to +85 °C
A1006TL	A1006TL/TA1rrZ[2]	HXSON6	13-inch reel	75000	T_{amb} = –40 °C to +85 °C
A1006UK	A1006UK/TA1NXZ[1]	WLCSP4	7-inch reel	4000	T_{amb} = –40 °C to +85 °C
A1006UK	A1006UK/TA1rrZ[2]	WLCSP4	13-inch reel	75000	T_{amb} = –40 °C to +85 °C

[1] NX (fixed) - standard certificate

[2] Variable, <>NX - custom certificate, code assigned after certificate verification

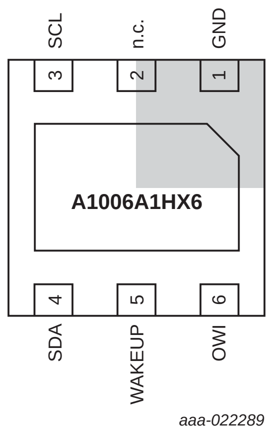
7. Marking

Table 6. Marking codes

Type number	Marking code
A1006UK/TA1…	Line A: .(DOT)A1 (A1 Product Family) Line B: ddd (Last 3 digits of diffusion #) Line C: d|| (d – last 1 digit of diffusion # || - Wafer ID)
A1006TL/TA1....	Line A: A 1 6 Line B: XXY XX = ASID Y: weekly rotating 1-5

8. Pinning information

8.1 Pinning



(1) The center pad is attached internally to the substrate using non-conductive die attach material. It can be externally connected to ground or treated as a no connect.

Fig 1. Pin configuration for HXSON6 (top view)

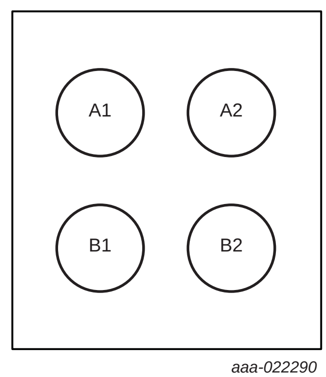


Fig 2. Ball layout for WLCSP4 (top view)

8.2 Pin description

Table 7. Pin description

Symbol	Pin		Description
	HXSON6	WLCSP4	
GND	1	A2	ground (0 V)
n.c.	2	-	connect to ground
SCL	3	B2	I^2C clock
SDA	4	B1	I^2C data
WAKEUP	5	-	wakeup from Deep-sleep mode
OWI	6	A1	One-Wire Interface. Power pin as well as communication channel if OWI mode is used; I^2C VDD supply voltage if I^2C-bus interface is used

9. Functional description

9.1 External interfaces

The A1006 supports both an I^2C and an OWI. After boot phase, both the interfaces are active. The first valid command at any interface decides which interface will stay active. With the SoftReset command, it is possible to activate both interfaces again.

9.2 OWI

The A1006 Secure Authenticator IC implements the proprietary OWI protocol of NXP. This interface provides both data and power, eliminating the need for an extra supply pin and no external components except pull-up (like a cap). The A1006 implements a half duplex master/slave communication protocol that can easily be controlled via a microcontroller's GPIO. The OWI is capable of up to 125 kbps data transmission.

9.3 I^2C-bus interface

The A1006 supports the I^2C-bus protocol at a data rate of up to 400 kbps. Any device that sends data to the bus is defined to be a transmitter, and any device that reads the data to be a receiver. The device that controls the data transfer is known as the bus master and the other as the slave device. A data transfer can only be initiated by the bus master, which also provides the serial clock for synchronization. The A1006 is always a slave in all communications. In the following description, the Master device refers to the host, and the slave device refers to the A1006.

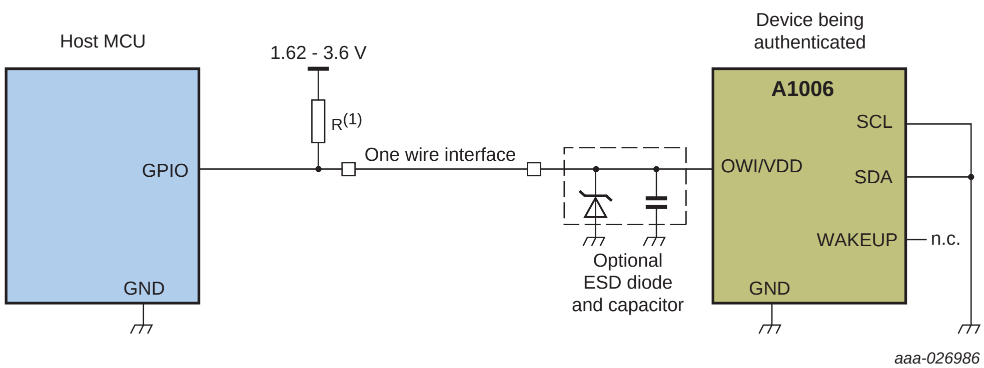
9.4 Deep-sleep mode

The A1006 supports a deep sleep mode where it consumes extremely low power but it can also be woken up in case further operations with the IC are necessary.

10. Application information

10.1 One Wire Interface

Figure 3 shows A1006 powered by a host microcontroller using the OWI interface to communicate with A1006.

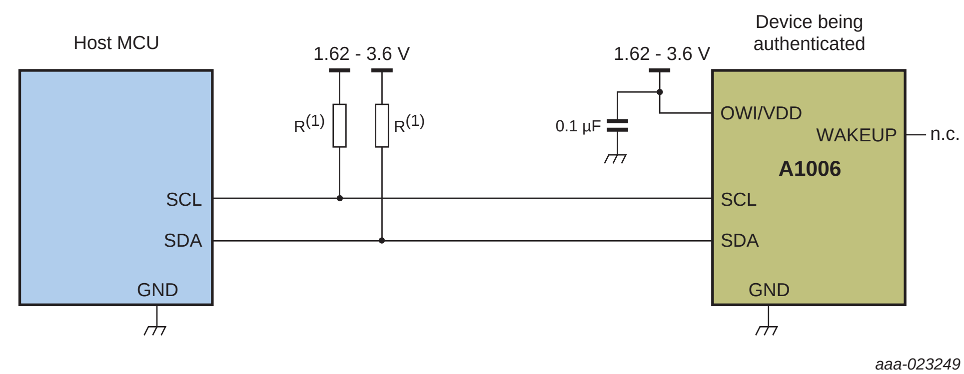


(1) 200Ω to 500Ω recommended for VDD = 1.8 V. Higher values up to 1.2kΩ may be used with VDD = 3.3 V.

Fig 3. Application diagram for OWI

10.2 I^{2}C interface

Figure 4 shows A1006 connected to a host microcontroller via I^{2}C interface.



(1) Typically 900Ω for VDD = 1.8 V and 1.1kΩ for 3.3 V

Fig 4. Application diagram for using I^{2}C-bus interface

10.3 Authentication

Figure 5 shows authentication flow at a high level. Please refer to A1006 user guide for details.

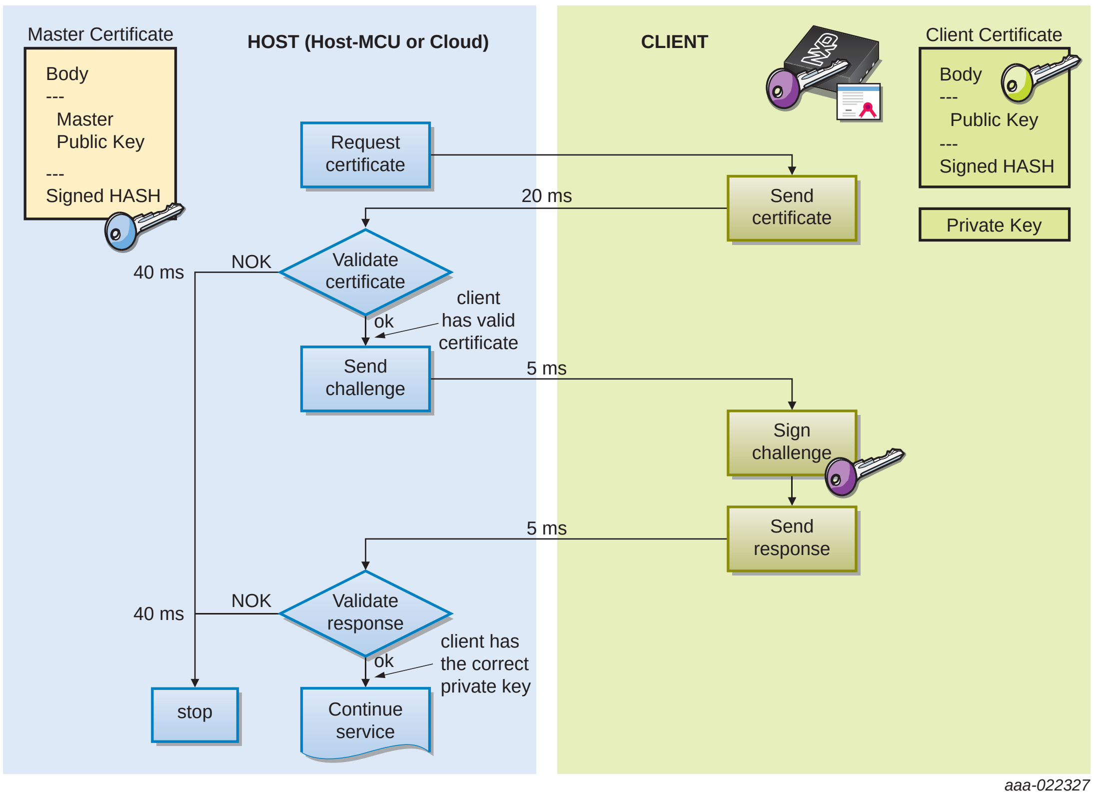


Fig 5. Authentication flow

To prove its authenticity the A1006 supports a public/private key Diffie-Hellman authentication protocol based on ECC (Elliptic Curve Cryptography) with a 163 bit strong binary field curve. The implementation uses a standard curve NIST B-163.

The protocol is a two-pass challenge-response protocol where the host can verify the authenticity of the A1006. The host chooses random number r, multiplies “basepoint” G by this random number to get point rG. The host sends the point rG to the A1006. The A1006 stores a private key q and public key Q (=qG). This public key Q is embedded in a certificate cert(Q) and stored in the A1006. The A1006 computes q(rG) and returns the result to the host. The host verifies that cert(Q) is valid, extracts the public key Q from the certificate and verifies that q(rG) received from the A1006 equals rQ (i.e. r(qG)).

If both checks are valid, the A1006 has proven its authenticity.

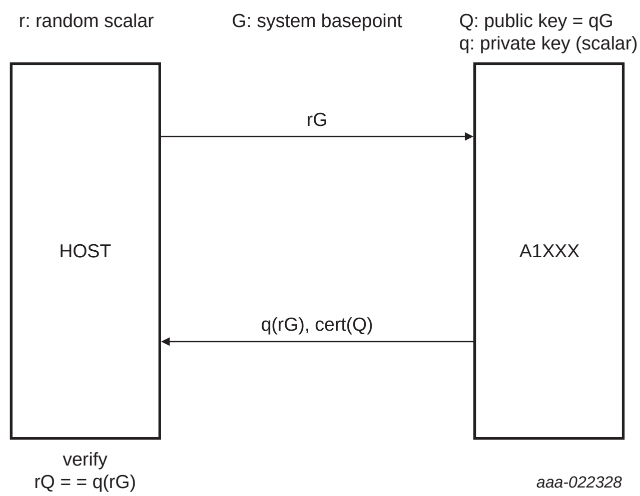


Fig 6. Authentication protocol

11. Limiting values

Table 8. Limiting values

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

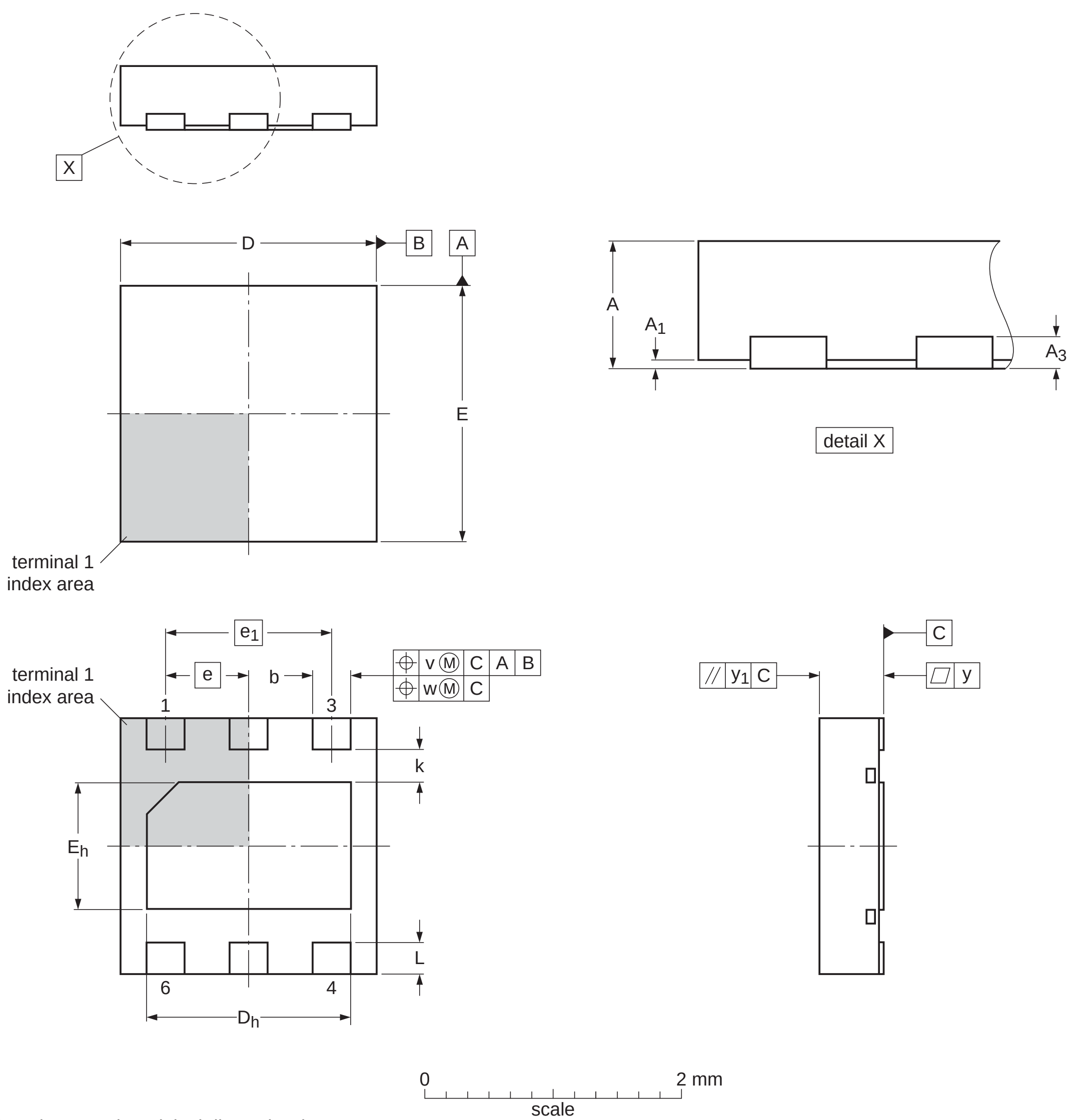
Symbol	Parameter	Conditions	Min	Max	Unit
$V_{DD,OWI}$	supply voltage		–0.5	+4.6	V
V_I	I/O voltage	on pins SCL, SDA, WAKEUP	–0.5	+4.6	V
I_{IL}	latch-up current	$V_I < 0$ V or $V_I > V_{OWI}$	-	100	mA
V_{esd}	electrostatic discharge voltage	[1]	-	8.0	kV
P_{tot}	total power dissipation	[2]	-	2.0	mW
T_{stg}	storage temperature		–65	+150	°C
T_J	junction temperature		–40	+85	°C
t_{ret}	retention time	T_{amb} = +85 °C	10	-	years
$N_{endu(W)}$	write endurance	under all operating conditions	5×10^5	-	cycles

[1] IEC61000-4-2; contact discharge only on the OWI pin, all other pins support 2 kV HBM

[2] Depending on appropriate thermal resistance of the package

12. Package outline

HXSON6: plastic, thermal enhanced extremely thin small outline package; no leads; 6 terminals; body 2.0 x 2.0 x 0.5 mm **SOT1348-1**



Dimensions (mm are the original dimensions)

Unit		A	A_1	A_3	b	D(1)	D_h	E(1)	E_h	e	e_1	k	L	v	w	y	y_1
mm	max	0.5	0.05		0.35	2.1	1.7	2.1	1.1				0.30				
	nom			0.127	0.30	2.0	1.6	2.0	1.0	0.65	1.3		0.25	0.1	0.05	0.05	0.05
	min		0.00		0.25	1.9	1.5	1.9	0.9			0.2	0.20				

Note

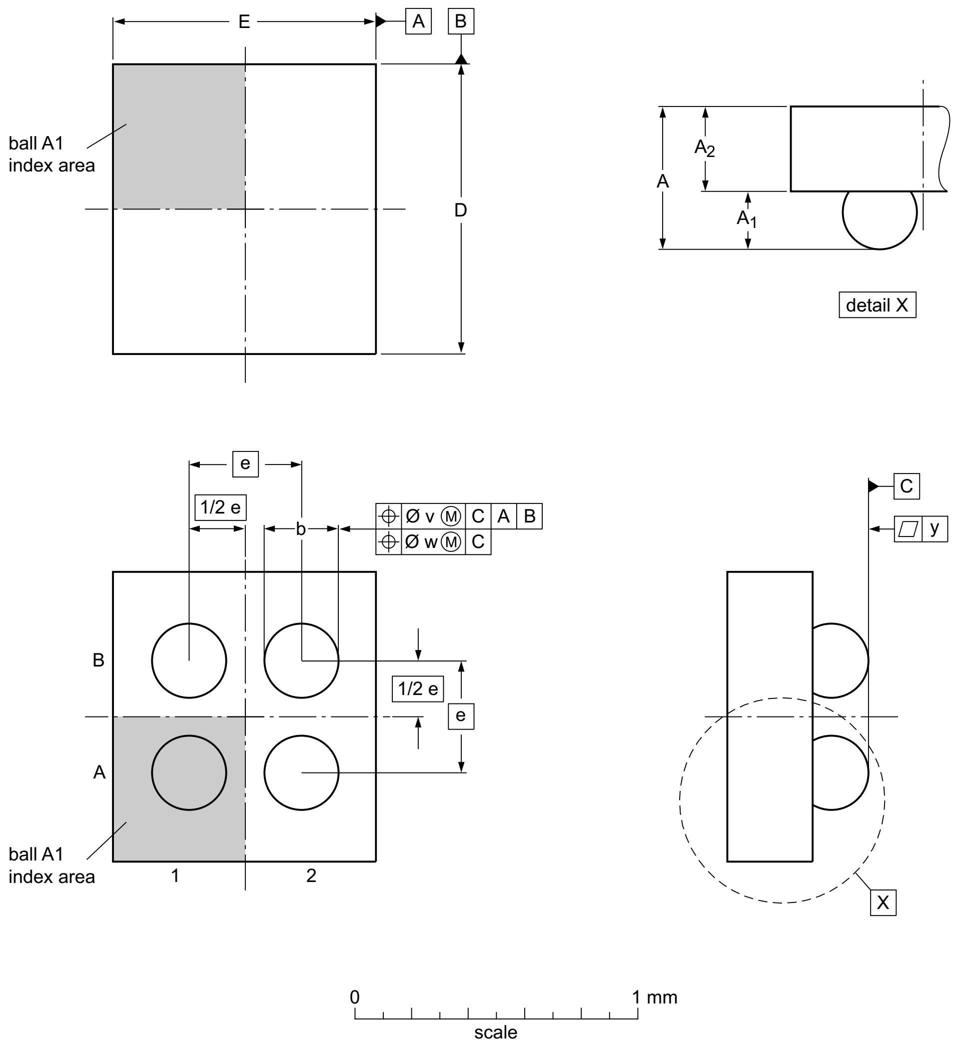
1. Plastic or metal protrusions of 0.075 mm maximum per side are not included.

sot1348-1_po

Outline version	References				European projection	Issue date
	IEC	JEDEC	JEITA			
SOT1348-1	- - -	- - -	- - -			~~13-09-04~~ 15-05-08

Fig 7. Package outline SOT1348-1 (HXSON6)

WLCSP4: wafer level chip-scale package; 4 bumps; 1.03 x 0.94 x 0.5 mm **SOT1375-4**



Dimensions (mm are the original dimensions)

Unit		A	A_1	A_2	b	D	E	e	v	w	y
mm	max	0.54	0.23	0.325	0.29	1.06	0.97				
	nom	0.50	0.20	0.300	0.26	1.03	0.94	0.4	0.05	0.015	0.03
	min	0.46	0.17	0.275	0.23	1.00	0.91				

sot1375-4_po

Outline version	References				European projection	Issue date
	IEC	JEDEC	JEITA			
SOT1375-4						~~16-04-06~~ 16-12-05

Fig 8. Package outline SOT1375-4 (WLCSP4)

13. Abbreviations

Table 9. Abbreviations

Acronym	Description
OWI	One-Wire Interface

14. Revision history

Table 10. Revision history

Document ID	Release date	Data sheet status	Change notice	Supersedes
A1006_SDS	20180725	Product short data sheet	-	-

15. Legal information

15.1 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.

15.2 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.

15.3 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.

15.4 Licenses

ICs with DPA Countermeasures functionality	
LICENSED DPA COUNTERMEASURES™	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.

15.5 Trademarks

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

16. Contact information

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

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

17. Contents

Date of release: 25 July 2018
Document identifier: A1006_SDS