



A71CH

Plug & Trust Secure Element

Rev. 1.2 — 27 September 2018
449312

Data sheet
COMPANY PUBLIC

1. Introduction

The A71CH is a ready-to-use solution providing a root of trust at the IC level and proven, chip-to-cloud security right out of the box. It is a platform capable of securely storing and provisioning credentials, securely connecting IoT devices to cloud services and performing cryptographic node authentication.

The A71CH solution provides basic security measures protecting the IC against many physical and logical attacks. It can be used with various host platforms and host operating systems to secure a broad range of applications. It is complemented by a comprehensive product support package, offering easy design-in with plug & play host application code, easy to use development kits, reference designs, and extensive documentation for product evaluation.

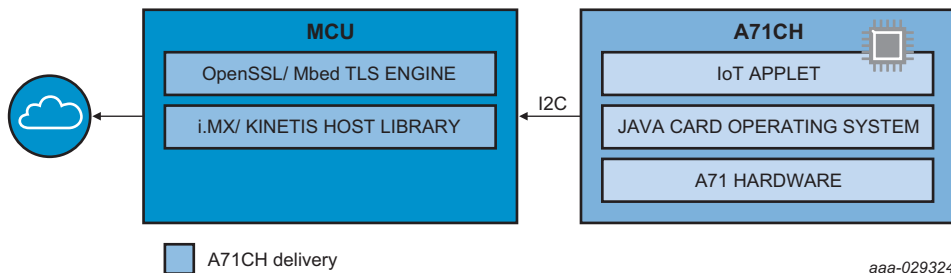


Fig 1. A71CH block diagram



2. General description

2.1 A71CH naming conventions

The following table explains the naming conventions of the commercial product name of the A71CH products. Every A71CH product gets assigned such a commercial name, which includes also customer and application specific data.

The A71CH commercial names have the following format.

A71CHxagpp(p)/mvsrrff

The 'A71CH' is a constant, all other letters are variables, which are explained in [Table 1](#).

Table 1. A71CH commercial name format

| Variable | Meaning | Values | Description |
|----------|---|--------|--|
| x | IC hardware specification code | 1 | standard operational ambient temperature: -25 °C to +85 °C I ² C interface supported |
| | | 2 | standard operational ambient temperature: -40 °C to +90 °C I ² C interface supported |
| a | embedded operating system code | C | Java card operating system |
| g | embedded application firmware (applet) code | H | H is a fixed value = IoT security applet pre installed |
| pp(p) | package type code dd(d)= Delivery Type, TK2= HVSON8 (4x4), UK= WLCSP12 | | |
| m | Manufacturing Site Code | T | |
| v | Silicon Version Code | 0 | |
| s | Silicon Version Subcode | B | |
| rr | ROM Code ID | | |
| ff | FabKey ID | | |

2.2 I²C interface

The A71CH has an I²C interface in slave mode, supporting data rates up to 400 kbit/s operating in Fast-Mode (FM). The I²C interface is using the Smartcard I²C protocol as defined in [Ref. 3](#) which is based on SMBus.

2.3 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.

3. Features and benefits

3.1 Key benefits

- Secure, zero-touch connectivity
- End-to-end security, from chip to edge to cloud
- Secure credential injection for IC-level root of trust
- Fast design-in with complete product support package
- Easy to integrate with different MCU platforms

3.2 Security features

The A71CH security concepts includes many security measures to protect the chip.

The A71CH operates fully autonomously based on an integrated Javacard operating system and applet. Direct memory access is possible by the fixed functionalities of the applet only. With that, the content from the memory is fully isolated from the host system.

Attack protection by integrated design measures in the chip layout, the logic and the functional blocks.

3.3 Cryptography features

The A71CH Secure Element provides the following functionality:

- Protected Access storage, generation, insertion or deletion of 4 key pairs (ECC NIST P-256)
- Systematic enforced authentication
- Secure key management
- Protected Access storage, insertion or deletion of 3 public keys
- Signature generation and verification (ECDSA)
- Shared secret calculation for Key Agreement (ECDH or ECDH-E)
- Protected Access storage and use of 2 monotonic counters (32 bits each)
- Protected Access storage, insertion or deletion of symmetric secrets (8x 128 bits); longer keys can be used by using a ConstructedSecret type
- Content protected access to keys
- A unique chip ID (18 bytes)
- HKDF key derivation using the symmetric secrets as key, Extract & Expand or Expand only modes
- HMAC SHA256 calculation in one shot or sequential
- Freezing of credentials (= OTP behavior)
- Secure channel SCPO3 GP support
- (Optional) trust provisioning of key pairs, public keys, symmetric secrets, etc.
- Possibility to lock the A71CH module as transport lock mechanism

ECC keys and operations support the following ECC curve:

- NIST P-256

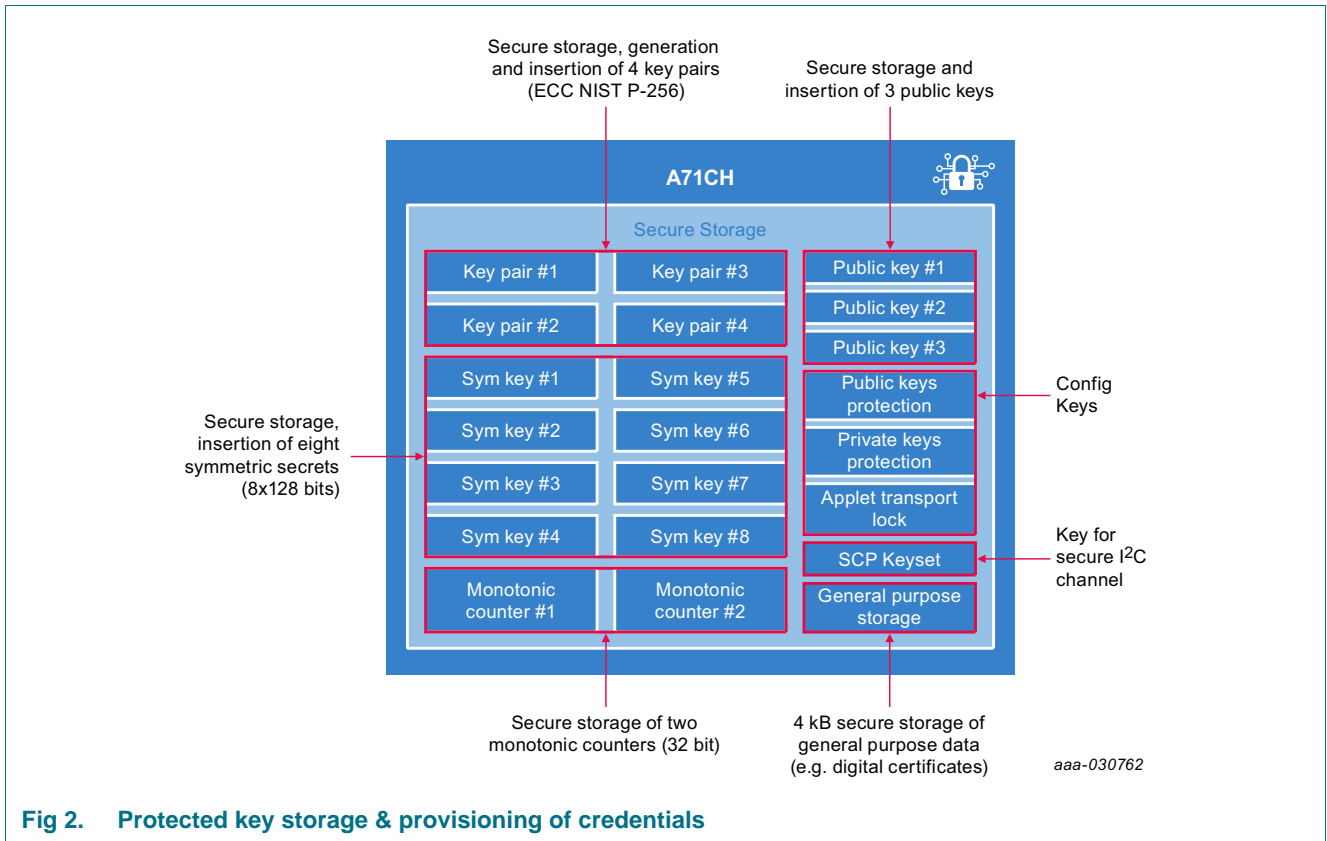


Fig 2. Protected key storage & provisioning of credentials

3.4 Functional features

- Dedicated MX51 security CPU
- 400 kbit/s I²C Fast-mode interface
- -40 °C to +90 °C operational ambient temperature (A7102)
- On-chip Javacard operating system
- 40 μA typical sleep mode current with I²C pads in tristate mode
- 10 μA max deep sleep mode current with I²C pads in tristate mode
- High-performance Public Key Infrastructure (PKI)
- EEPROM with min 500,000 cycles endurance and min 25 years retention time
- HVSON8 package and small WLCSP available

4. Applications

4.1 Use Cases and target applications

- A710xCH EXAMPLE USE CASES
 - ◆ Secure connection to public/private clouds, edge computing platforms, infrastructure
 - ◆ Secure Amazon Web Services-compliant connectivity
 - ◆ Secure commissioning
 - ◆ Device-to-device authentication
 - ◆ Proof of origin / anti-counterfeiting
 - ◆ Key storage and data protection
 - ◆ Secure provisioning of credentials
 - ◆ Ecosystem protection
- A710xCH TARGET APPLICATIONS
 - ◆ Connected industrial devices
 - ◆ Sensor networks
 - ◆ IP cameras
 - ◆ Home gateways
 - ◆ Home appliances

5. Ordering information

5.1 Ordering options

Table 2. Ordering information

| Type number ^[1] | Package | | |
|----------------------------------|---------|---|----------------|
| | Name | Description | Version |
| A7101agTK2/... A7102agTK2/... | HVSON-8 | plastic thermal enhanced very thin small outline package; no leads; 8 terminals; body 4 x 4 x 0.85 mm | SOT909-1 |
| A7101agUK/... A7102agUK/... | WLCSP12 | wafer level chip scale package, 12 bumping, 0.5 mm ball pitch | not applicable |

[1] a = A or C, g = G, C or A, according to the A71CH type classification see [Section 2.1 "A71CH naming conventions"](#)

Table 3. A71CH type table

| 12NC | Type number | Product | Configuration | Package | Orderable part no |
|-------------------|--------------------|-----------|--|---------|--------------------|
| 9353 68 097118 | A7101CHTK2/T0BC2V6 | A71(01)CH | customer programmable | HVSON8 | A7101CHTK2/T0BC2VJ |
| 9353 635 15118 | A7102CHTK2/T0BC2A5 | A71(02)CH | customer programmable | HVSON8 | A7102CHTK2/T0BC2AJ |
| 9353 694 82023 | A7101CHUK/T0BC2HA | A71(01)CH | customer programmable | WLCSP | A7101CHUK/T0BC2HAZ |
| 9353 695 02023 | A7102CHUK/T0BC2VA | A71(02)CH | customer programmable | WLCSP | A7102CHUK/T0BC2VAZ |
| 9353 737 63118 | A7101CHTK2/T0BC2BM | A71(01)CH | Provisioned & Programmable 'Ready for IBM Watson IoT' | HVSON8 | A7101CHTK2/T0BC2BJ |
| 9353 741 46118 | A7102CHTK2/T0BC2CH | A71(02)CH | Provisioned & Programmable 'Ready for IBM Watson IoT' | HVSON8 | A7102CHTK2/T0BC2CJ |

Table 4. A71CH development tools type table

| 12NC | Type number | Development kit | Description |
|--------------|-----------------|-----------------|------------------------------------|
| 935368997598 | OM3710/A71CHARD | OM3710/A71CHARD | Arduino compatible development kit |
| 935369302598 | OM3710/A71CHPCB | OM3710/A71CHPCB | Mini PCB |

[Table 5](#) gives an overview of available A71CH product types.

Table 5. A71CH feature table

| Product type ^[1] | Operational ambient temperature | Interface option |
|-----------------------------|---------------------------------|------------------|
| A7101Cgpp(p) | -25 °C to +85 °C | I ² C |
| A7102Cgpp(p) | -40 °C to +90 °C | |

[1] g = G, C, or A; pp(p) = UA or HN1, according the A71CH type classification see [Section 2.1 "A71CH naming conventions"](#)

5.1.1 Samples and final products

[Section 5.1.2](#), gives details of how to order samples and final products.

5.1.2 Ordering A71CH samples

Samples can be ordered from NXP Semiconductors via nxp.com using the "Buy Direct" button.

Note that NXP Semiconductors can provide up to 5 pieces free of charge. Larger quantities have to be ordered separately.

5.2 Configuration

The A71CH is available in configurations as specified in [Table 3](#). The Configuration defines the default memory and key contents. The table below describes the default configuration "customer programmable". Other configurations will be described in addenda to this data sheet.

Table 6. A71CH type table

| Credential/ State | Amount | Description |
|------------------------|---|------------------------------------|
| Asymmetric Key Pairs | 4 x ECDSA NIST P-256 private + public key | Not set, not locked |
| Asymmetric Public Keys | 3 x ECDSA NIST P-256 public keys | Not set, not locked |
| Config Keys | 3 x AES128 | Not set, cannot be locked |
| Symmetric Secret | 8 x 128 bit key data | Not set, cannot be locked |
| Monotonic Counter | 2 x upcounting counter with 32 bit | Counter set to 0, cannot be locked |
| SCP channel | SCP03 keyset with 3 AES128 keys | Keys not set, SCP03 not active |
| GP Data | 128 segments of 32 bytes each | All bytes set to 0x00 |
| Plain Injection Mode | | Plain secrets can be inserted |
| Debug Mode | | Debug Mode is active |
| TransportLock | | Module can be set to "LOCKED" |

6. Marking

Table 7. Marking codes

| Type number | Marking code |
|----------------|---|
| A710x..TK2/... | Line A: 710* (* = '1' for A7101, '2' for A7102, '3' for A7103) Line B: **** (**** = 4 digit Batch code ^[1]) Line C: ZnD***0 (** = 3 digit Date code ^[2]) Z: diffusion center, SSMC Systems on Silicon Manufacturing (SSMC), Singapore n: assembly center D: code to indicate conformance to RHF-2006 O: Mask version code |

- [1] Batch code: 5 digits available, 2 for DBSN, 2 for ASID: mark "YY ZZ" or 4 digits available, 2 for DBSN, 2 for ASID: mark "YYZZ"

The Assembly Sequence ID (ASID) is a 2-digit indicator that counts the number of assembly batches (transport lots) within one diffusion batch id and one weekly date code. The week start and end dates are defined by the assembly center algorithm. The ASID is assigned sequentially starting with 01 and ranging through 99, then each digit ranges upper case alphabet letters in combination with numeric, then numeric in combination with upper case alphabet letters, then upper case alphabet letters in combination with upper case alphabet letters providing 1175 possible values within a week-code. The numeric zero '0' is only allowed within the sequence of 01 to 99. The alphabet letter 'O' is not allowed to avoid confusion with numeric '0'.

The Diffusion Batch Sequence Number (DBSN) is a 2-digit indicator that counts the number of diffusion batches (DBID) within one Package Type (i.e. HVSON8) and one weekly date code. The DBSN is assigned sequentially starting with 01 and ranging through 99, then each digit ranges upper case alphabet letters in combination with numeric, then numeric in combination with upper case alphabet letters, then upper case alphabet letters in combination with upper case alphabet letters providing 1175 possible values within a week-code. The numeric zero '0' is only allowed within the sequence of 01 to 99. The alphabet letter 'O' is not allowed to avoid confusion with numeric '0'.

- [2] 3 digit Date code: "YWW"

"Y" is a code indicating the year in which the IC is assembled. Examples: for year 1999 is Y = 9, for year 2000 is Y = 0, for year 2001 is Y = 1. "WW" is a code indicating the week in which the IC is assembled. It is determined from the date the assembly transport lot is created or alternately the date die is issued from die stores to assembly start or the date die attach (Diebond) occurs or the date encapsulation occurs.

Examples: for week 01 is WW = 01, for week 52 is WW = 52, for week 53 is WW = 53.

In the case of bumped die (WL-CSP) the code indicates the week in which the IC was bumped.

7. Functional description

7.1 Functional diagram

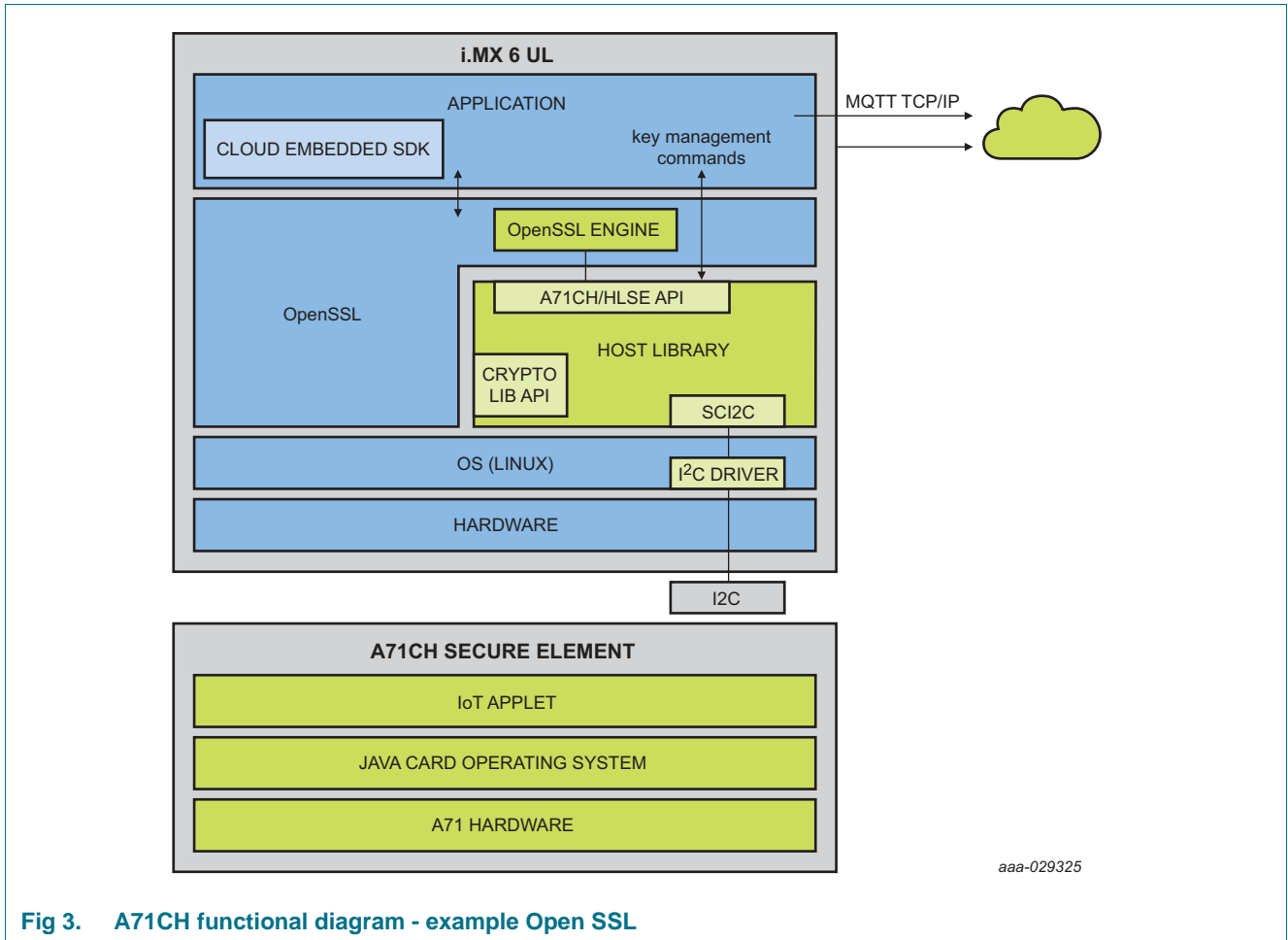


Fig 3. A71CH functional diagram - example Open SSL

The A71CH uses I²C as communication interface as described in the following section. The A71CH commands are wrapped using the Smartcard I² protocol (SCI2C). The detailed documentation for the A71CH commands [ref to APDU Spec] and SCI2C encapsulation (Ref. 3) is available in NXP docstore.”

In order to simplify the product usage a host library was created which takes care for the A71CH commands and SCI2C protocol encapsulation. The host library for various platforms is available for download with complete sources on the A71CH website.

7.2 Credential Storage & Memory

The I²C interface of the A71CH is supporting a Smart Card I²C (SCIIC) Protocol using an Inter-IC (I²C) based physical interface and data link layer using Fast-mode (FM) up to 400 kBit/s, a SMBus based network layer and bus protocol as well as a mapping layer to convey [ISO/IEC 7816-4] based communication. This protocol is specified in [Ref to SCI²C].

- A71CH is compliant to [Ref. 3](#) and implements the following SCIIC protocol options:
 - Usage of the optional error detection code supported
 - CDBMS_MAX of 255 and a CDBSM_MAX of 252
 - Default Frame Waiting Time is 320 ms
 - Protocol binding selection is not supported (not needed as only 7816-4 APDU mapping is supported)
 - The I2C address is 90h (8-bit address) equals 48h (7-bit address) and optional 92h (8-bit address) which equals 49h (7-bit address)

7.3 I²C Interface

The A71CH has an I²C interface in slave mode, supporting data rates up to 400 kbit/s operating in Fast-Mode (FM). The I²C interface is using the Smartcard I²C protocol as defined in [Ref. 3](#) which is based on SMBus. The default I²C address after power-on-reset depends on the bootup condition as shown in [Table 8](#).

7.4 Automatic Communication Mode detection at Power on

The IC configures its interface according to the pin state as shown in the table below. The host system must keep the voltage levels stable at these pins for at least 500 μ s after power-on-reset.

Table 8. I²C address

| IF0 | Value at startup | | | I ² C address | |
|-----|------------------|---------|---------|--------------------------|------|
| | IF1 | I2C_SCL | I2C_SDA | Write | Read |
| 0 | x | 0 | 0 | n.a. | n.a. |
| 1 | 0 | 1 | 1 | 0x90 | 0x91 |
| 1 | 1 | 1 | 1 | 0x92 | 0x93 |

7.5 Power-saving modes

The device provides two power-saving operation modes, the SLEEP mode and the DEEP SLEEP mode. These modes are activated via pad RST_N (DEEP SLEEP mode) or by the device.

7.5.1 SLEEP mode

The SLEEP mode has the following properties:

- all internal clocks are frozen,
- CPU enters power saving mode with program execution being stopped,
- CPU registers keep their contents,
- RAM keeps its contents,

The A71CH enters automatically into SLEEP mode after 312 ms of inactivity on the I²C lines and also wakes up automatically from SLEEP mode. In SLEEP mode, all internal clocks are stopped. The IOs hold the logical states they had at the time IDLE was activated. During SLEEP mode security sensors HVS, LVS, LTS, HTS, Light Sensors, Glitch Sensors and Active Shielding are disabled.

There are two ways to exit from the SLEEP mode:

- A reset signal on RST_N
- An External Interrupt edge triggered by a falling edge on I2C_SDA

7.5.2 DEEP SLEEP mode

The A71CHx provides a special sleep mode offering maximum power saving. It is reached by pulling RST_N to a logic zero level for more than 500 μ s.

While in deep sleep mode the internal power is completely switched off and only the IO pads stay supplied. All digital pads will stay in high-Z mode.

To leave the DEEP SLEEP mode RST_N has to be released and set to a logic „1“ level.

8. Pinning information

8.1 Pinning

8.1.1 Pinning HVSON8

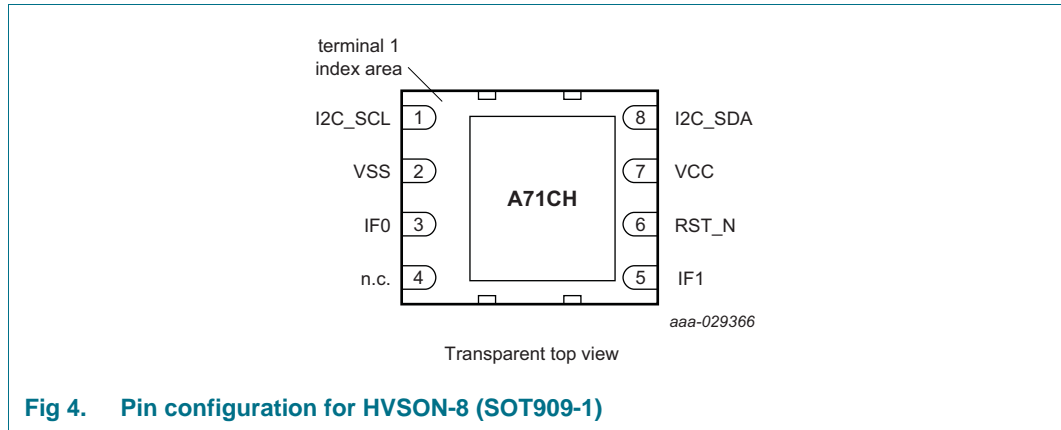
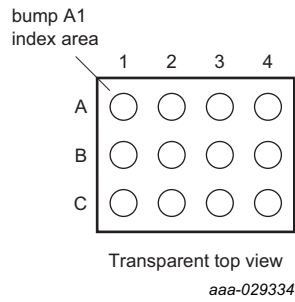


Table 9. Pin description HVSON8

| Symbol | Pin | Description |
|---------|-----|---|
| I2C_SCL | 1 | I ² C clock |
| VSS | 2 | ground |
| IF0 | 3 | interface activation, apply high on startup |
| n.c. | 4 | not connected |
| IF1 | 5 | I ² C address selection |
| RST_N | 6 | reset input, active LOW |
| VCC | 7 | power supply voltage input |
| I2C_SDA | 8 | I ² C data |

The center pad of the IC is not connected, although it is recommended to connect it to ground for thermal reasons.

8.1.2 Pinning WLCSP



| | 1 | 2 | 3 | 4 |
|---|------|------|---------|---------|
| A | n.c. | VSS | I2C_SCL | I2C_SDA |
| B | n.c. | VCC | n.c. | IF1 |
| C | n.c. | i.c. | RST_N | IF0 |

Transparent top view
aaa-029335

Fig 5. Pin configuration for WLCSP12

Fig 6. Ball mapping for WLCSP12

Table 10. Pin description WLCSP

| Symbol | Pin | Description |
|---------|-----|---|
| n.c. | A1 | not connected |
| VSS | A2 | ground |
| I2C_SCL | A3 | I ² C Clock |
| I2C_SDA | A4 | I ² C Data |
| n.c. | B1 | not connected |
| VCC | B2 | Power supply voltage input |
| n.c. | B3 | not connected |
| IF1 | B4 | I ² C address selection |
| n.c. | C1 | not connected |
| i.c. | C2 | internally connected; connect to ground |
| RST_N | C3 | Reset input, active LOW |
| IF0 | C4 | interface activation, apply high on startup |

The pins/balls A1, B1, C1, and B3 are not connected internally. These pins/balls can be used for routing to connect to B2 (VCC) in order to have an easier PCB layout.

9. Package outline

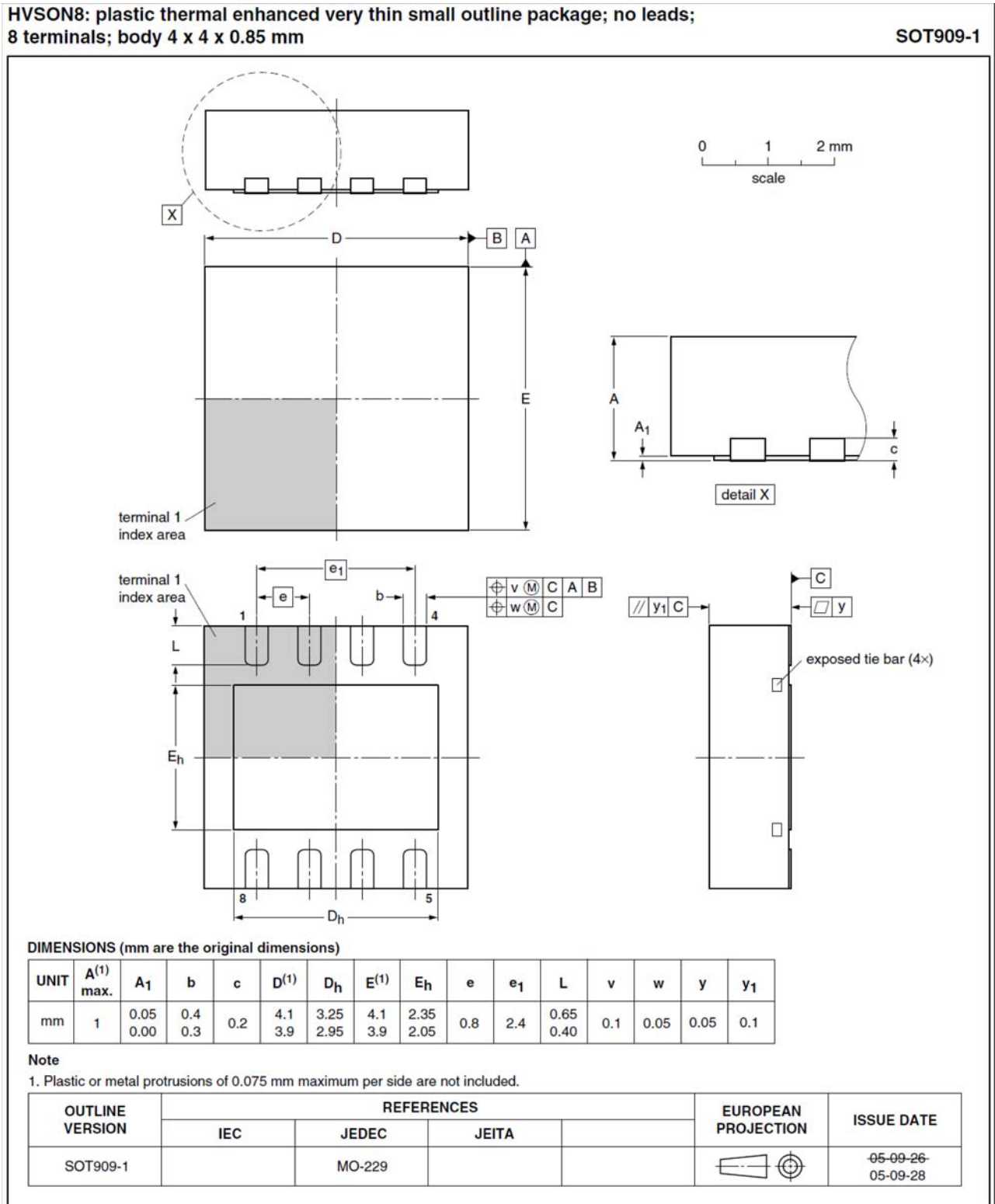


Fig 7. Package outline SOT909-1

WLCSP12 : wafer level chip-size package, 12 bumps, 2.06x2.018x0.6 mm

A7101

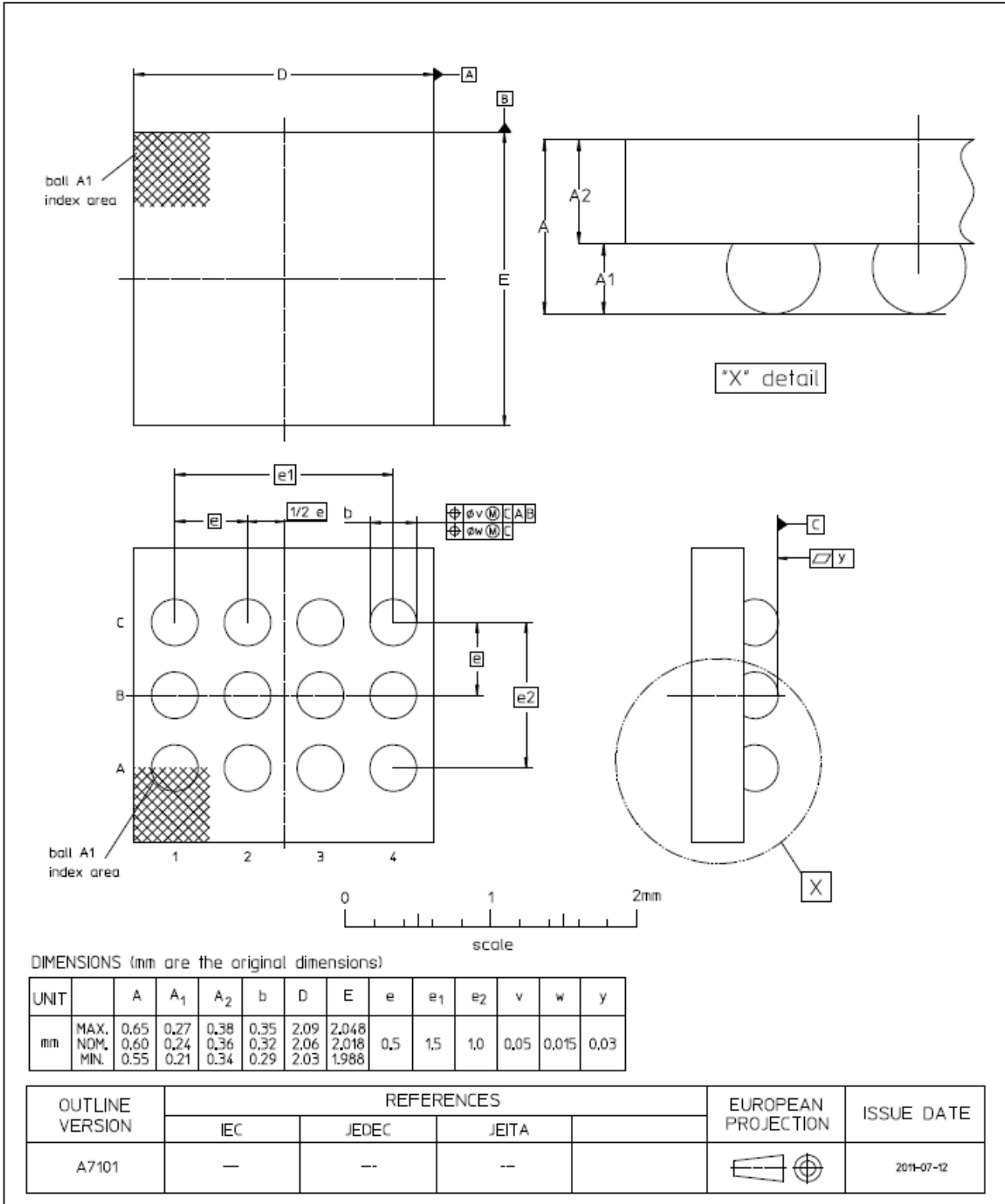


Fig 8. Package outline WLCSP12

10. Packing information

10.1 Reel packing

The A71CH product is available on 7" tape on reel and 13" tape on reel. Details are provided in [Table 11](#).

Table 11. Reel packing options

| Package type | Reel type | Minimum packing quantity |
|--------------|---------------------------------|--------------------------|
| HVSON8 | 7" tape on reel | 1500 |
| HVSON8 | 13" tape on reel ^[1] | 6000 |
| WLCSP12 | 7" tape on reel | 3000 |

[1] For details about packing method, product orientation, tape dimensions and labeling for A71 parts in HVSON8 package having an ordering code (12NC) ending 118 refer to [Ref. 2](#).

11. Electrical and timing characteristics

The electrical interface characteristics of static (DC) and dynamic (AC) parameters for pads and functions used for I²C are in accordance with the NXP I²C specification (see [Ref. 1](#)).

12. Limiting values

Table 12. 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 I2C_SDA, I2C_SCL | - | 10 | mA |
| I _O | output current | pad I2C_SDA, I2C_SCL | - | 10 | mA |
| I _{lu} | latch-up current | V _I < 0 V or V _I > V _{DD} | - | 100 | mA |
| V _{esd_hbm} | electrostatic discharge voltage (Human Body Model) | pads VCC, VSS, RST_N, I2C_SDA, I2C_SCL | ^[1] | ± 2.0 | kV |
| V _{esd_cdm} | electrostatic discharge voltage (Charge Device Model) | pads VCC, VSS, RST_N, I2C_SDA, I2C_SCL | ^[3] | ± 500 | V |
| P _{tot} | Total power dissipation | | ^[2] | 1 | W |
| T _{stg} | Storage temperature | | -55 | +125 | °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.

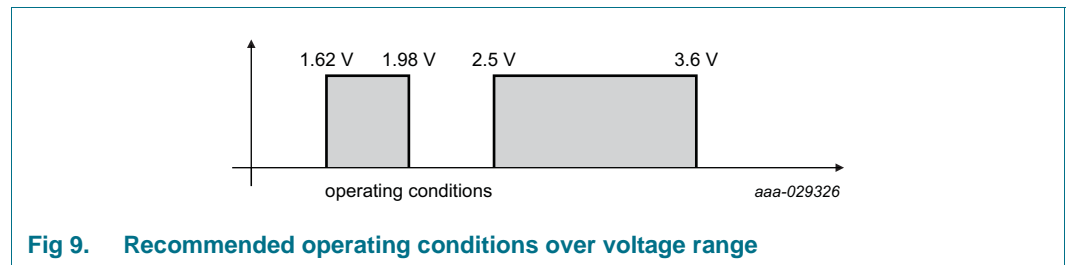
[3] JESD22-C101, JEDEC Standard Field induced charge device model test method.

13. Recommended operating conditions

The A71CH offers two operation modes, the so-called 1V8 mode and the 3V3 mode targeted for battery supplied applications.

Table 13. Recommended operating conditions

| Symbol | Parameter | Conditions | Min | Typ | Max | Unit |
|------------------|--|--|------|-----|------|------|
| V _{DD} | supply voltage range | 3V3 mode range CPU in free runing mode | 2.50 | 3.3 | 3.6 | V |
| | | 1V8 mode | 1.62 | 1.8 | 1.98 | V |
| V _I | DC input voltage on digital I/O pads I2C_SCL, I2C_SDA | 3V3 mode | 0 | | 3.6 | V |
| | | 1V8 mode | 0 | | 3.6 | V |
| V _I | DC input voltage on digital input pad RST_N | 3V3 mode | 0 | | 3.6 | V |
| | | 1V8 mode | 0 | | 3.6 | V |
| T _{amb} | Operating ambient temperature | A7101 | -25 | | +85 | °C |
| | | A7102 | -40 | | +90 | °C |



14. Characteristics

14.1 DC characteristics

Measurement conventions

Testing measurements are performed at the contact pads of the device under test. All voltages are defined with respect to the ground contact pad VSS. All currents flowing into the device are considered positive.

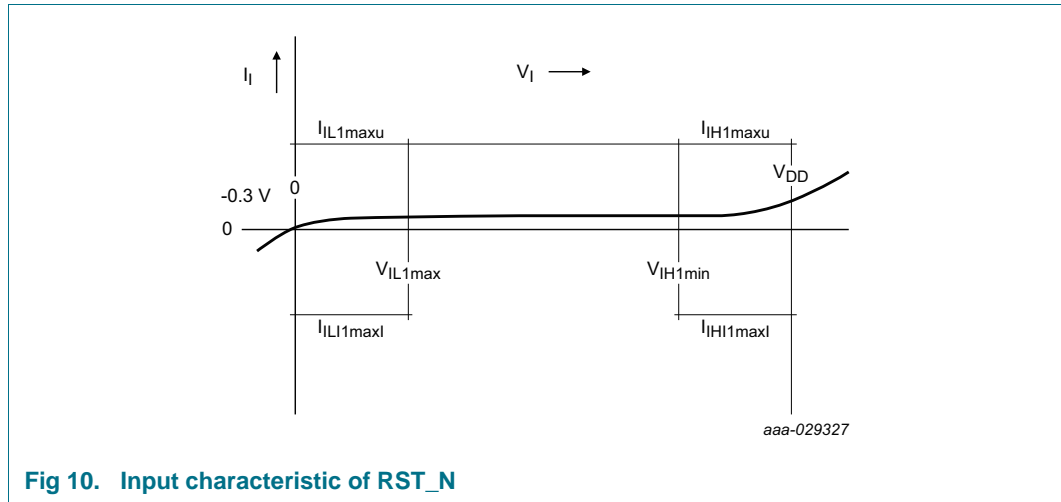
14.1.1 General and I²C I/O interface

Table 14. Electrical DC characteristics of I2C_SCL, I2C_SDA and RST_N

| Symbol | Parameter | Conditions | Min | Typ | Max | Unit |
|--|--|--|---------------------|---------------------|----------------------------------|------|
| Input/Output: I2C_SCL, I2C_SDA in push-pull mode | | | | | | |
| V _{IH} | HIGH level input voltage | | 0.7 V _{DD} | | V _{Imax} ^[1] | V |
| V _{IL} | LOW level input voltage | | -0.5 | | 0.3 V _{DD} | V |
| I _{IH} | HIGH level input current in input mode | V _{IHmin} < V _I < V _{IHmax} | | | ± 10 | μA |
| I _{IL} | LOW level input current | V _{ILmin} < V _I < V _{ILmax} | | | ± 10 | μA |
| V _{OH} | HIGH level output voltage | I _{OH} = -3.0 mA; 3V3 mode | ^[2] | 0.7 V _{DD} | | V |
| | | I _{OH} = -3.0 mA; 1V8 mode | ^[2] | 0.7 V _{DD} | | V |
| V _{OL} | LOW level output voltage | I _{OL} = 3.0 mA 3V3 mode | | | 0.4 | V |
| | | I _{OL} = 2.0 mA 1V8 mode | | | 0.2 V _{DD} | V |
| Input/Output: I2C_SCL, I2C_SDA in open-drain mode | | | | | | |
| V _{IH} | HIGH level input voltage | | 0.7 V _{DD} | | V _{Imax} ^[1] | V |
| V _{IL} | LOW level input voltage | | -0.5 | | 0.3 V _{DD} | V |
| I _{IH} | HIGH level input current in input mode | V _{IHmin} < V _I < V _{IHmax} | | | ± 10 | μA |
| I _{IL} | LOW level input current | V _{ILmin} < V _I < V _{ILmax} | | | ± 10 | μA |
| V _{OL} | LOW level output voltage | I _{OL} = 3.0 mA 3V3 mode | | | 0.4 | V |
| | | I _{OL} = 2.0 mA 1V8 mode | | | 0.2 V _{DD} | V |
| Input: RST_N | | | | | | |
| V _{IH1} | HIGH level input voltage | | 0.7 V _{DD} | | V _{Imax} ^[1] | V |
| V _{IL1} | LOW level input voltage | | -0.3 | | 0.3 V _{DD} | V |
| I _{IH1} | HIGH level RST_N input current | V _{IH1min} ≤ V _I ≤ V _{DD} | ^[3] | | ± 20 | μA |
| I _{IL1} | LOW level RST_N input current | 0 V ≤ V _I ≤ V _{IL1max} | ^[3] | | ± 20 | μA |

[1] Maximum value according to [Table 13 "Recommended operating conditions"](#)

- [2] : External pull-up resistor 20 kΩ to VDD. The worst case test condition for parameter V_{OH} is present at minimum V_{DD} . For class A supply voltage conditions $V_{DD} = 4.5\text{ V}$ is the worst case with respect to the fix specification limit $V_{OHmin} = 3.8\text{ V}$ ($0.844 V_{DD}$). The supply voltage related limit “ $0.7 V_{DD}$ ” is a stricter requirement than the fix value 3.8 V at high V_{DD} ($0.7 V_{DD} = 3.85\text{ V}$ at $V_{DD} = 5.5\text{ V}$). So, in the V_{DD} range 4.5 V to 5.5 V, V_{OHmin} is specified as “the larger value of $0.7 V_{DD}$ and 3.8 V, respectively”.
- [3] The active low RST_N input internally has a resistive pull-down device to VSS. Accordingly a current is flowing into the pad voltages above 0 V. [Figure 10](#) shows the RST_N input characteristic.



14.1.2 I²C interface at 3V3 mode operation^[1]Table 15. Electrical characteristics of IC supply voltage V_{DD} ; $V_{SS} = 0\text{ V}$; $T_{amb} = -40\text{ to }+90\text{ }^{\circ}\text{C}$

| Symbol | Parameter | Conditions | Min | Typ | Max | Unit |
|----------------|--------------------------------|---|------|------|------|---------------|
| Supply | | | | | | |
| V_{DD} | supply voltage range | 3V3 mode range CPU in free running mode | 2.50 | 3.3 | 3.6 | V |
| I_{DD} | no coprocessor active | CPU in free running mode | | 6.3 | 7.0 | mA |
| | EPROM programming in progress | CPU in free running mode | | 7.3 | 8.0 | mA |
| | AES coprocessor active | CPU in free running mode | | 9.3 | 10.3 | mA |
| | ECC coprocessor active | CPU in free running mode | | 13.7 | 15.1 | mA |
| $I_{DD(SLP)}$ | supply current SLEEP mode | $T_{amb} = 25\text{ }^{\circ}\text{C}$ | | 45 | 150 | μA |
| $I_{DD(DSLP)}$ | supply current deep sleep mode | RST_N at 0V, $T_{amb} = 25\text{ }^{\circ}\text{C}$ | | | 10 | μA |
| | | RST_N at 0V, $T_{amb} = 90\text{ }^{\circ}\text{C}$ | | | 10 | μA |

[1] All appropriately marked values are typical values and only referenced for information. They are subject to change without notice.

14.1.3 I²C interface at 1V8 mode operation^[1]

Table 16. Electrical characteristics of IC supply voltage V_{DD}; V_{SS} = 0 V; T_{amb} = -40 to +90 °C

| Symbol | Parameter | Conditions | Min | Typ | Max | Unit |
|-----------------------|--------------------------------|---------------------------------------|------|------|------|------|
| Supply | | | | | | |
| V _{DD} | supply voltage range | 1V8 mode range | 1.62 | 1.8 | 1.98 | V |
| I _{DD} | no coprocessor active | CPU in free running mode | | 2.45 | | mA |
| | AES coprocessor active | CPU in free running mode | | 2.7 | | mA |
| | ECC coprocessor active | CPU in free running mode | | 7.5 | | mA |
| I _{DD(SLP)} | supply current SLEEP mode | T _{amb} = 25 °C | | 40 | 80 | μA |
| I _{DD(DSLP)} | supply current deep sleep mode | RST_N at 0V, T _{amb} = 25 °C | | | 10 | μA |
| | | RST_N at 0V, T _{amb} = 90 °C | | | 10 | μA |

[1] All appropriately marked values are typical values and only referenced for information. They are subject to change without notice.

14.2 AC characteristics

Table 17. Non-volatile memory timing characteristics; V_{DD} = 1.8 V ± 10% or 3 V ± 10% V; V_{SS} = 0 V; T_{amb} = -40 to 90 °C

| Symbol | Parameter | Conditions | Min | Typ | Max | Unit |
|-------------------|---|---------------------------|---------------------|-----|-----|--------|
| t _{EEP} | EEPROM erase + program time | | | 2.7 | | ms |
| t _{EEE} | EEPROM erase time | | | 1.7 | | ms |
| t _{EEW} | EEPROM program time | | | 1.0 | | ms |
| t _{EEER} | EEPROM data retention time | T _{amb} = +55 °C | 25 | | | years |
| N _{EEEC} | EEPROM endurance (number of programming cycles) | | 5 × 10 ⁵ | | | cycles |

Table 18. Electrical AC characteristics of I2C_SDA, I2C_SCL, and RST_N^[1]; V_{DD} = 1.8 V ± 10% or 3 V ± 10% V; V_{SS} = 0 V; T_{amb} = -40 to 90 °C

| Symbol | Parameter | Conditions | Min | Typ | Max | Unit |
|--|--|---|-----|-----|-----|------|
| Input/Output: I2C_SDA, I2C_SCL in open-drain mode | | | | | | |
| t _{rIO} | I/O Input rise time | Input/reception mode | [4] | | 1 | μs |
| t _{fIO} | I/O Input fall time | Input/reception mode | [4] | | 1 | μs |
| t _{fOIO} | I/O Output fall time | Output/transmission mode; C _L = 30 pF | [4] | | 0.3 | μs |
| f _{CLK} | External clock frequency in I ² C applications | t _{CLKW} , T _{amb} and V _{DD} in their spec'd limits | - | | 400 | kHz |
| t _{CLKW} | Clock pulse width i.r.t. clock period (positive pulse duty cycle of CLK) | [3] | 40 | | 60 | % |
| Inputs: RST_N | | | | | | |
| t _{RW} | Reset pulse width (RST_N low) without entering deep sleep mode | | 40 | | 400 | μs |
| t _{RDSLP} | Reset pulse width (RST_N low) to enter deep sleep mode | | 500 | | | μs |
| t _{WKP} | Wake-up time from SLEEP mode | f _{CLKmin} < f _{CLK} < f _{CLKmax} | - | 8 | 10 | μs |

Table 18. Electrical AC characteristics of I2C_SDA, I2C_SCL, and RST_N^[1];
 $V_{DD} = 1.8\text{ V} \pm 10\%$ or $3\text{ V} \pm 10\%$ V; $V_{SS} = 0\text{ V}$; $T_{amb} = -40\text{ to }90\text{ }^\circ\text{C}$

| Symbol | Parameter | Conditions | Min | Typ | Max | Unit |
|--------------|---|---|-----|-----|-----|---------------|
| t_{WKPIO} | Pad LOW time for wake-up from SLEEP mode | level triggered ext.int. | - | 8 | 10 | μs |
| | | edge triggered ext.int. | - | 8 | 10 | μs |
| t_{WKPRST} | RST_N LOW time for wake-up from SLEEP mode | | 40 | | - | μs |
| t_{WKWT} | Time from SLEEP mode wake/up event to I2C_SDA valid | | | 50 | 100 | ns |
| C_{PIN} | Pin capacitances RST_N, I2C_SDA, /I2C_SCL | Test frequency = 1 MHz; $T_{amb} = 25\text{ }^\circ\text{C}$ | - | | 10 | pF |

- [1] All appropriately marked values are typical values and only referenced for information. They are subject to change without notice.
- [2] t_r is defined as rise time between 20% and 80% of the signal amplitude.
 t_f is defined as fall time between 80% and 20% of the signal amplitude.
- [3] During AC testing the inputs RST_N, I2C_SDA, I2C_SCL are driven at 0 V to +0.3 V for a LOW input level and at $V_{DD} - 0.3\text{ V}$ to V_{DD} for a HIGH input level. Clock period and signal pulse (duty cycle) timing is measured at 50% of V_{DD} .
- [4] t_r is defined as rise time between 30% and 70% of the signal amplitude.
 t_f is defined as fall time between 70% and 30% of the signal amplitude.

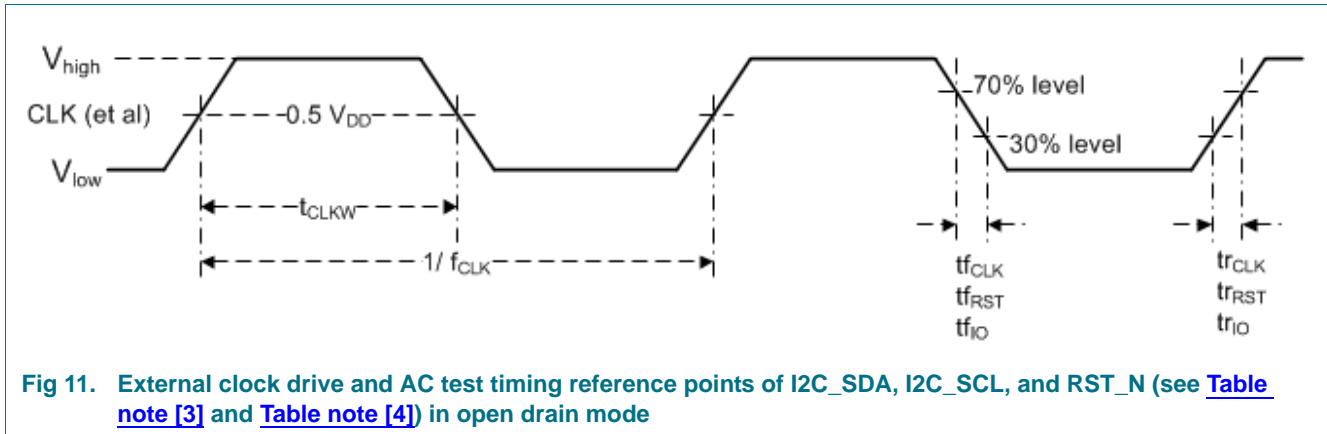


Fig 11. External clock drive and AC test timing reference points of I2C_SDA, I2C_SCL, and RST_N (see [Table note \[3\]](#) and [Table note \[4\]](#)) in open drain mode

14.3 EMC/EMI

EMC and EMI resistance according to IEC 61967-4.

15. Abbreviations

Table 19. Abbreviations

| Acronym | Description |
|----------------|---|
| AES | Advanced Encryption Standard |
| CRC | Cyclic Redundancy Check |
| DES | Digital Encryption Standard |
| DPA | Differential Power Analysis |
| DSS | Digital Signature Standard |
| ECC | Elliptic Curve Cryptography |
| EEPROM | Electrically Erasable Programmable Read-Only Memory |
| I/O | Input/Output |
| MAC | Message Authentication Code |
| OS | Operating System |
| PKI | Public Key Infrastructure |
| SFI | Single Fault Injection |
| SHA | Secure Hash Algorithm |

16. References

- [1] I²C-bus specification and user manual, Rev. 3.0 — June-19-2007, NXP Semiconductors
- [2] SOT909-1; HVSON8; Reel pack; Ordering code (12NC) ending 118; Packing Information; Rev. 2 — 19 April 2013
- [3] Application note SCIIC Protocol Specification, Application note, Rev 1.x, AN12207 (document number an19501x)

17. Revision history

Table 20. Revision history

| Document ID | Release date | Data sheet status | Change notice | Supersedes |
|----------------|--------------|----------------------------|---|------------|
| 449312 | 20180927 | Data sheet | | 449311 |
| Modifications: | | | | |
| | | | <ul style="list-style-type: none"> • Table 1 "A71CH commercial name format": Added WLCSP • Table 3 "A71CH type table": Updated • Section 3.4 "Functional features": Added WLCSP • Section 8.1.1 "Pinning HVSON8": Added paragraph • Section 8.1.2 "Pinning WLCSP": Added section • Figure 5 "Pin configuration for WLCSP12": Added pin configuration • Figure 6 "Ball mapping for WLCSP12": Updated • Table 10 "Pin description WLCSP": Updated • Table 11 "Reel packing options": Added WLCSP | |
| 449311 | 20180801 | Data sheet | | 449310 |
| 449310 | 20180221 | Objective short data sheet | | |
| Modifications: | | | | |
| | | | <ul style="list-style-type: none"> • Initial version | |

18. Legal information

18.1 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>.

18.2 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.

18.3 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.

19. Contact information

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

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

18.4 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.



18.5 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.

20. Tables

| | | | |
|---|----|--|----|
| Table 1. A71CH commercial name format | 2 | I2C_SDA and RST_N | 18 |
| Table 2. Ordering information | 6 | Table 15. Electrical characteristics of IC supply voltage V_{DD} ; $V_{SS} = 0\text{ V}$; $T_{amb} = -40\text{ to }+90\text{ }^{\circ}\text{C}$ | 20 |
| Table 3. A71CH type table | 6 | Table 16. Electrical characteristics of IC supply voltage V_{DD} ; $V_{SS} = 0\text{ V}$; $T_{amb} = -40\text{ to }+90\text{ }^{\circ}\text{C}$ | 21 |
| Table 4. A71CH development tools type table | 6 | Table 17. Non-volatile memory timing characteristics; $V_{DD} = 1.8\text{ V} \pm 10\%$ or $3\text{ V} \pm 10\%$; $V_{SS} = 0\text{ V}$; $T_{amb} = -40\text{ to }90\text{ }^{\circ}\text{C}$ | 21 |
| Table 5. A71CH feature table | 6 | Table 18. Electrical AC characteristics of I2C_SDA, I2C_SCL, and RST_N[1]; $V_{DD} = 1.8\text{ V} \pm 10\%$ or $3\text{ V} \pm 10\%$; $V_{SS} = 0\text{ V}$; $T_{amb} = -40\text{ to }90\text{ }^{\circ}\text{C}$ | 21 |
| Table 6. A71CH type table | 7 | Table 19. Abbreviations | 23 |
| Table 7. Marking codes | 8 | Table 20. Revision history | 25 |
| Table 8. I ² C address | 10 | | |
| Table 9. Pin description HVSON8 | 12 | | |
| Table 10. Pin description WLCSP | 13 | | |
| Table 11. Reel packing options | 16 | | |
| Table 12. Limiting values | 16 | | |
| Table 13. Recommended operating conditions | 17 | | |
| Table 14. Electrical DC characteristics of I2C_SCL, | | | |

21. Figures

| | | | |
|---|----|--|----|
| Fig 1. A71CH block diagram | 1 | Fig 8. Package outline WLCSP12 | 15 |
| Fig 2. Protected key storage & provisioning of credentials 4 | 4 | Fig 9. Recommended operating conditions over voltage range | 17 |
| Fig 3. A71CH functional diagram - example Open SSL | 9 | Fig 10. Input characteristic of RST_N | 19 |
| Fig 4. Pin configuration for HVSON-8 (SOT909-1) | 12 | Fig 11. External clock drive and AC test timing reference points of I2C_SDA, I2C_SCL, and RST_N (see Table note [3] and Table note [4]) in open drain mode | 22 |
| Fig 5. Pin configuration for WLCSP12 | 13 | | |
| Fig 6. Ball mapping for WLCSP12 | 13 | | |
| Fig 7. Package outline SOT909-1 | 14 | | |

22. Contents

| | | | | | |
|----------|---|----------|-----------|---|-----------|
| 1 | Introduction | 1 | 6 | Marking | 8 |
| 2 | General description | 2 | 7 | Functional description | 9 |
| 2.1 | A71CH naming conventions | 2 | 7.1 | Functional diagram | 9 |
| 2.2 | I ² C interface | 2 | 7.2 | Credential Storage & Memory | 9 |
| 2.3 | Security licensing | 2 | 7.3 | I ² C Interface | 10 |
| 3 | Features and benefits | 3 | 7.4 | Automatic Communication Mode detection at Power on | 10 |
| 3.1 | Key benefits | 3 | 7.5 | Power-saving modes | 10 |
| 3.2 | Security features | 3 | 7.5.1 | SLEEP mode | 10 |
| 3.3 | Cryptography features | 3 | 7.5.2 | DEEP SLEEP mode | 11 |
| 3.4 | Functional features | 4 | 8 | Pinning information | 12 |
| 4 | Applications | 5 | 8.1 | Pinning | 12 |
| 4.1 | Use Cases and target applications | 5 | 8.1.1 | Pinning HVSON8 | 12 |
| 5 | Ordering information | 6 | 8.1.2 | Pinning WLCSP | 13 |
| 5.1 | Ordering options | 6 | 9 | Package outline | 14 |
| 5.1.1 | Samples and final products | 6 | 10 | Packing information | 16 |
| 5.1.2 | Ordering A71CH samples | 7 | 10.1 | Reel packing | 16 |
| 5.2 | Configuration | 7 | | | |

continued >>

| | | |
|-----------|--|-----------|
| 11 | Electrical and timing characteristics | 16 |
| 12 | Limiting values. | 16 |
| 13 | Recommended operating conditions. | 17 |
| 14 | Characteristics. | 18 |
| 14.1 | DC characteristics | 18 |
| 14.1.1 | General and I2C I/O interface. | 18 |
| 14.1.2 | I2C interface at 3V3 mode operation ^[1] | 20 |
| 14.1.3 | I2C interface at 1V8 mode operation ^[1] | 21 |
| 14.2 | AC characteristics. | 21 |
| 14.3 | EMC/EMI | 22 |
| 15 | Abbreviations. | 23 |
| 16 | References | 24 |
| 17 | Revision history. | 25 |
| 18 | Legal information. | 26 |
| 18.1 | Data sheet status | 26 |
| 18.2 | Definitions. | 26 |
| 18.3 | Disclaimers | 26 |
| 18.4 | Licenses | 27 |
| 18.5 | Trademarks. | 27 |
| 19 | Contact information. | 27 |
| 20 | Tables | 28 |
| 21 | Figures | 28 |
| 22 | Contents | 28 |

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. 2018.

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: 27 September 2018

449312



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.