NXP IoT security IC A71CH for cloud connections

Plug & Trust: The fast and easy way to deploy secure IoT connections

This ready-to-use solution provides a root of trust at the IC level and delivers proven, chip-to-cloud security right out of the box, so you can connect to IoT clouds and services, including AWS, IBM Watson IoT Platform and Google Cloud IoT Core, without writing security code or exposing keys.

KEY BENEFITS

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

KEY SECURITY FEATURES

- Protected access to credentials
- Encrypted/authenticated interface to host processor
- Certificate-based TLS set-up (ECC NIST P-256)
- TLS set-up using pre-shared secret (TLS-PSK)
- Connectionless message authentication (HMAC)
- ECC key generation & signature verification
- Symmetric key derivation
- Secure vault for product master secrets (key wrapping, derivation, locking)
- Encrypted key injection
- Optional trust provisioning by NXP and qualified partners

KEY HARDWARE FEATURES

- Easy access to any MCU/MPU with I^{2}C 400 kbps slave interface
- Standard (-25 to +85 °C, A7101CH) and extended (-40 to +90 °C, A7102CH) temperature ranges
- HVSON8 (4x4 mm) and WLCSP (2x2 mm) package

The arrival of subscription-based cloud connectivity using clouds, such as Amazon Web Services (AWS), IBM Watson IoT Platform and Google Cloud IoT Core, makes the Internet of Things (IoT) more accessible to everyday products, and is expanding the range of IoT-driven services.

When deploying cloud services, security is always a concern, since every device needs to be protected from hacking, data breaches, botnet attacks, and other dangers lurking in the IoT. The keys and certificates used to authenticate the cloud connection need to remain securely hidden, and any data transmitted by the IoT device needs to remain safe and secure while in transit. What's more, the security mechanisms need to be scalable, so they can be deployed efficiently on a large scale, even when manufactured by different OEMs.

To meet this need, NXP now offers the A71CH, a security IC that delivers high-end security to IoT deployments of any size. As a ready-to-use, plug & trust solution that works with public and private clouds, the A71CH offers zero-touch secure connectivity with proven, hardware-based security algorithms.

The pre-integrated connectivity applet means there's no need to write security code, and the ready-to-deploy host software is easy to integrate with different MCU and MPU platforms.

Designed with built-in security measures and optimized for secure connectivity, the A71CH supports key insertion at the IC level and delivers trusted security right out of the box.

PROVEN PERFORMANCE

The A71CH builds on NXP's leadership in some of the world's most demanding security applications, such as payment and logical and physical access, as well as identification, including electronic passports.

Purpose-built to bring security to the IoT, the A71CH protects essential device functions, including object authentication, data protection, and cloud access, supports software integrity and roll-back protection, and safeguards service integrity and ecosystems. It also provides a platform for new business models.

The A71CH supports industrial applications with an optional extended temperature range (-40 to +90 °C), and is designed for longevity, with up to 25 years minimum data retention in general-purpose storage and 500,000 cycles minimum endurance.

LIFECYCLE PROTECTION

NXP fosters trust throughout the product lifecycle, from production to the field. Die-individual keys and certificates can be injected by NXP at their certified-secure manufacturing facilities, or by a qualified partner, so as to create a silicon-based root of trust.

As a result, IoT devices that use the A71CH can incorporate security from the start, not as a bolt-on or afterthought.

COMPLETE PRODUCT SUPPORT PACKAGE

Delivered as a ready-to-use solution, the A71CH includes a complete product support package that simplifies design-in and reduces time-to-market. NXP eases the overall design process in several ways. For example, the use of an OpenSSL engine and integration into mbedTLS, both part of the host software package, makes it easier to work with connectivity stacks. NXP also offers time-saving design tools like sample code for major use cases, extensive application notes, and compatible development kits for i.MX and Kinetis microcontrollers, which accelerate the final system integration.

A71CH USE CASES

- Secure connection to cloud services, edge computing platforms, infrastructure
- Device-to-device authentication
- Proof of origin / anti-counterfeiting
- Secure key storage
- Secure management of credentials
- Secure data protection
- Secure commissioning support
- Ecosystem protection

A71CH TARGET APPLICATIONS

- Connected industrial devices
- Security systems and sensor networks
- Gateways
- Smart Cities
- Smart Home

Configuration	Orderable Part Number	Description	Package	12NC
Customer programmable	A7101CHTK2/T0BC2VJ	Security IC with standard temp range (-25 to +85 °C)	HVSON8, Reel	9353 680 97118
Customer programmable	A7102CHTK2/T0BC2AJ	Security IC with extended temp range (-40 to +90 °C)	HVSON8, Reel	9353 635 15118
Customer programmable	A7101CHUK/T0BC2HAZ	Security IC with standard temp range (-25 to +85 °C)	WLCSP, Reel	9353 694 82023
Customer programmable	A7102CHUK/T0BC2VAZ	Security IC with extended temp range (-40 to +90 °C)	WLCSP, Reel	9353 695 02023
Provisioned & Programmable	A7101CHTK2/T0BC2BJ	Security IC with standard temp range (-25 to +85 °C) Ready for IBM Watson IoT	HVSON8, Reel	9353 737 63118
Provisioned & Programmable	A7102CHTK2/T0BC2CJ	Security IC with extended temp range (-40 to +90 °C) Ready for IBM Watson IoT	HVSON8, Reel	9353 741 46118

Item	Description	12NC
OM3710/A71CHARD	A71CH Arduino-compatible development kit	9353 689 97598

Find all information on **www.nxp.com/A71CH**