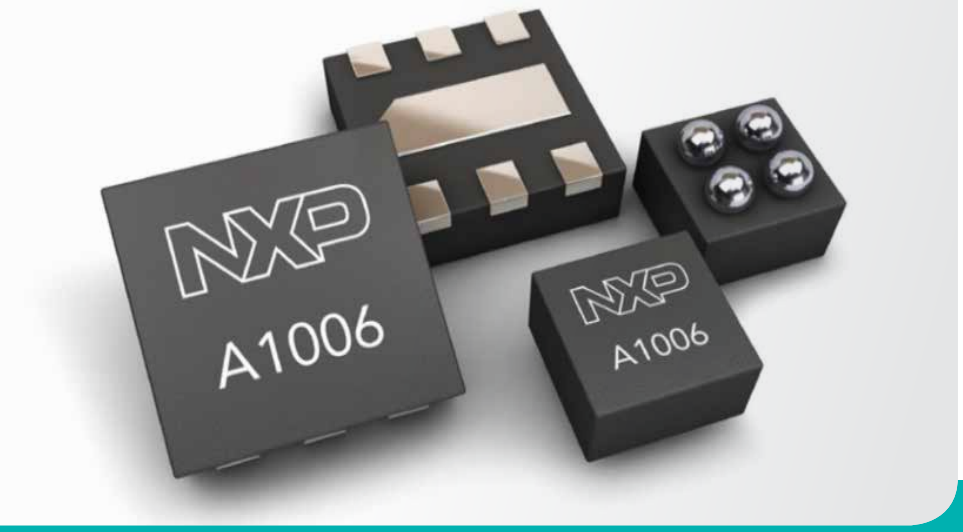

A1006 Secure Authenticator for anti-counterfeit applications

Complete secure solution for brand protection, revenue protection, and customer safety

Brand owners are facing increasing threats from counterfeits of their own products. The A1006 Secure Authenticator from NXP provides a robust security solution to prevent counterfeits. With low power consumption, small footprint, and flexible interfaces, the A1006 offers superior security that is easy to integrate into a range of electronic devices that are common targets of electronic counterfeiters.

KEY BENEFITS

- Targeted for anti-counterfeit applications providing a strong asymmetric cryptographic solution coupled with NXP security technology and services
- Highly secure solution with industry leading tamper resistance and countermeasures against various invasive and non-invasive attacks
- Unique public and private key per chip preventing scalable attacks
- Industry's smallest Secure Authenticator, with solutions as small as 1 mm2
- Industry's lowest power Secure Authenticator solution
- No secure element needed in the host, lowering the total system cost
- Complete solution with the Secure IC, reference host software, demo board and development kit, supported by industry leading security experts for ease of integration and faster time-to-market
- Trust provisioning services to securely generate die individual keys and certificates and injection in a common criteria certified secure NXP internal environment

KEY FEATURES

- Strong authentication using asymmetric authentication protocol based on NIST B-163 elliptic curve
- Digitally signed certificates using 224-bit ECDSA and SHA-224 digest hash
- Industry leading advanced security features include: TRNG, active shielding, security sensors, and many more
- 4 Kbit EEPROM supports two certificates, system memory, and user needs
- Flexible interfaces: 400 kbps I^2C or a 100 Kbps bus powered one wired interface with 8kV IEC61000-4-2 ESD protection
- Power supply range from 1.8 V to 3.3 V
- Very low power consumption (50 µA typ, 550 µA max) and a deep sleep mode with power consumption < 1 µA at 1.8 V power supply
- Industry's smallest footprint — as small as 1 mm2, also available in 2 x 2 mm plastic package

- Product life cycle management with secure provisioning and non-reversible user mode

APPLICATIONS

- Counterfeit protection of hardware and software
  - Anti-cloning and brand integrity of original goods
- Profile of service
  - Conditional access to software, content, and features
- Electronic consumables
  - Batteries
  - Printer cartridges
  - Medical devices
  - Electronic cigarettes
- Electronic accessories
  - Power adapters
  - Power banks
  - Keyboards
  - Mobile device accessories
  - Licensable accessories

A COMPREHENSIVE SECURE SOLUTION

The A1006 Secure Authenticator offers a true end-to-end secure solution. The A1006 Secure Authenticator IC is built with strong protection against various invasive and non-invasive attacks. The IC is manufactured in NXP's certified secure manufacturing facilities to prevent key leakage during the fabrication process and certified secure HSMs are used to create and provision die individual keys and certificates. The solution also includes the host reference software, evaluation boards and the support of a best in class customer applications team with security experts, to ease the integration into the target customer applications.

NXP TRUST PROVISIONING SERVICES

NXP's trust provisioning services is a unique value add to the customer as a part of the A1006 Secure authenticator solution. Each A1006 IC comes with an NXP cryptographically signed X.509 certificate and an optional user certificate. The certificate contains information regarding the IC, a unique identifier, other customer information as well as a public key. The private key corresponding to the public key is stored in the IC and never leaves the IC.

The trust provisioning services offered by NXP include creation of die individual private/public key pairs, certificates and other personalized data in CC EAL5+ certified Hardware Secure Modules (HSM), and only these HSMs have access to master secrets and other unencrypted cryptographic objects. The data generated by the HSMs are inserted into each chip during production flow in our secure manufacturing facilities.

SUMMARY

A1006 Secure Authenticator solution — A complete solution, offering a one-stop shop for building authenticated devices and deterring even the most persistent counterfeiters

For more details, visit: **nxp.com/authentication**

www.nxp.com

Document Number: A1006FS REV 0