NXP A7001 dedicated high-security microcontroller for device authentication solutions

Secure device identification and brand protection against counterfeits

Brand owners are facing ever more challenges to protect their intellectual property and products from counterfeits. NXP, the company that created MIFARE™ contactless platforms and SmartMX™ microcontrollers, and co-invented NFC technology, now leverages its heritage and expertise in secure solutions for dedicated authentication products. The first product in our dedicated authentication family, the A7001, is a tamper resistant and secure MCU solution, for counterfeit protection, profile of service, and secure machine-to-machine communication.

Key benefits

- High security and physical tamper resistance with MX51 security CPU
- Speed and performance with multiple crypto-coprocessors
- Turnkey solution with dedicated authentication firmware (host and client)
- Easy integration with industry-standard I²C interface
- Optional key/certificate generation and loading

Key features

- Dedicated secure MX51 CPU with 80 KB EEPROM secure user memory
- High-performance secure Public Key Infrastructure (PKI) coprocessor (RSA, ECC)
- Secure 3-DES coprocessor
- Secure AES coprocessor (128-, 192- and 256-bit keys)
- I²C interface
- Low-power standby mode
- NXP patented glue-logic™ security feature

Applications

- 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

Security

The A7000 product family provides protection against light attacks, invasive fault attacks and side-channel attacks. The A7001 also has a built-in Memory Management Unit (MMU) to support strong firewalls and enhance security levels within a multi-application set-up.

All relevant cryptographic algorithms are supported with 'hardened' IC blocks equipped with unique features. Cryptographic coprocessors support public key algorithms and optimized, certified crypto libraries are available for interfacing the coprocessors and simplifying development of a secure OS. The A7001 product comes with a CRI license for improved DPA/SPA attack resistance features.

Convenience and performance

The NXP's dedicated authentication family 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 secure MCU, the total solution includes MCU firmware and an X.509 certificate authentication application, as well as loading of keys/certificates. These keys and certificates are generated and programmed in a certified (Common Criteria) secure NXP internal environment. The master keys are 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 A7001 solution allows for fast and convenient customization of specific solutions or implementations.

A7001 product characteristics

- Total solution
  - Secure MCU
  - Firmware
  - X.509 Certificate authentication application (Secure MCU + Host)
  - Generation, signing and loading of keys/certificates in a certified secure environment
- Secure MX51 CPU (Memory eXtended/enhanced 80C51)
- 80 KB EEPROM
  - Data retention time: 25 years
  - Endurance: 500 000 cycles minimum
- I^2C interface
- Supports voltage 1.62 to 5.5 V
- Memory Management Unit (MMU)
- High-speed 3-DES coprocessor (64-bit parallel)
- High-speed AES coprocessor (128-bit parallel)
- PKI (RSA, ECC) coprocessor FameXE (32-bit parallel)

Date of release: March 2011
Document order number: 9397 750 17096
Printed in the Netherlands