Online services and brand owners are facing ever increasing challenges in efforts to protect their intellectual property and products from counterfeiting, intrusion and theft. NXP introduces the A71 strong authentication microcontroller family; a tamper resistant secure MCU solution, dedicated to meet the market needs for counterfeit protection and cyber security.

**Key benefits**
- High security and physical tamper resistance
- Speed and performance with multiple crypto-coprocessors
- Optimized for power efficiency in sleep and operational modes
- Minimal total solution size through tiny wafer level chip scale package
- Multiple package options to fit the needs of individual applications
- Turnkey solution with dedicated embedded authentication firmware (host and client)
- Easy integration with industry standard 400 kbit I²C and 2 Mbit SPI interface
- Ready to use product with factory inserted key and certificate data (individualized for each die)

**Applications**
- Counterfeit protection of hardware and software - Anti-cloning - Brand integrity of original goods
- Cyber Security and device Identity - Conditional access to software and content - Secure access to online services - Ability to sign transactions and manage signed transactions - Secure machine to machine (M2M) communication

**Key features**
- Dedicated secure MX51 CPU with 20 KB EEPROM secure user memory
- -40 °C to +90 °C operational ambient temperature range (A7102)
- 15 uA (max) deep sleep mode current
- High-performance secure Public Key Infrastructure (PKI) coprocessor (RSA, ECC)
- Secure dual/triple-DES coprocessor
- Secure AES coprocessor (128-, 192- and 256-bit keys)
- Available in broad range of packages, i.e. tiny wafer level chip scale package
- 400 kbit I²C interface
Security

The A71 product family provides protection against light attacks, invasive fault attacks and side-channel attacks. All relevant cryptographic algorithms are supported with 'hardened' IC blocks equipped with unique features. Cryptographic coprocessors support public key algorithms. Optimized, certified crypto libraries, that make use of the coprocessors for faster performance are available. These capabilities simplify the development of a secure OS. The A71 products come with a CRI license delivering DPA/SPA attack resistance criteria.

Convenience and performance

NXP's dedicated A71 authentication family is offered as a turnkey solution that provides customers easy integration of authentication solutions. Minimal impact on the performance of end-products is achieved through high speed, low power consumption ICs that feature the desirable I2C and SPI interface.

In addition to the secure MCU, the total solution includes MCU firmware, an X.509 certificate based authentication application, as well as factory inserted keys and certificates. Key or certificate provisioning is done in a certified (Common Criteria) secure NXP internal environment with master keys securely stored in HSMs (Hardware Secure Modules). And authentication software for the host (host-MCU or remote server) can also be included as part of the solution.

A71 family product characteristics

- Total solution
  - Secure MCU
  - Embedded firmware
  - X.509 certificate based authentication application
    (Secure MCU + Host)
  - Generation, signing and loading of keys and certificates in a certified secure environment
- Secure MX51 CPU (Memory eXtended/enhanced 80C51)
- 20 KB EEPROM
  - Data retention time: 25 years
  - Endurance: 500 000 cycles minimum
- 400 kbit I2C fast mode interface
- Four wire 2 MBit SPI interface
- NXP patented glue logic™
- NXP secure fetch technology™
- 1.8 V to 3.6 V operating voltage range
- 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)