Security Selection Guide

EBV Elektronik
I An Avnet Company I

Security Selection Guide

FOREWORD

Authentication in the Smart Grid, Anti-Counterfeit protection for products, Safety in Industry 4.0 and Securing Car to Car communication are just some examples of the needs which are currently coming up in the IoT market.

All these applications have something in common: they are supported by an overall concept for various hardware components and software. EBV with its considerable product portfolio and an extensive network of partners can fulfill an important role here. Our EBV specialists can assist in determining the whole potential of Security, especially by helping with the selection of the right components in order to develop a tailored system solution for our customers. EBV's international presence in EMEA is important in this respect, as it enables the selection of the right products and partners even beyond national boundaries. Our ID specialists receive on-going trainings and have access to the expertise of our partners, component manufacturers and systems vendors. We want to make the introduction of Security & Identification as simple as possible. Together with our suppliers and partner network, EBV is able to offer a comprehensive solution. For our customers this means to have a single point of contact, starting from the design-in phase up to the rollout of a product or installation.

Christian Krieber
Director Segment Security & Identification

WHY DO WE NEED SECURITY?

In a world where not only computers are connected, but also any kind of devices, it is becoming more and more important to protect communications channels from being spied out or to securely authenticate the devices communicating to each other by proven techniques. Self-made algorithms as well as not securely stored crypto keys (like in software) lead to hacks which we are currently seeing on the market. Hacked cars which are controlled from outside, printers sending information to an external server, TV cameras giving access to private lives or attacked industrial plants are just some examples what we have seen in the media over the last month. Therefore, it is important to already add security on a board level.

Security is a Journey, Not a Destination

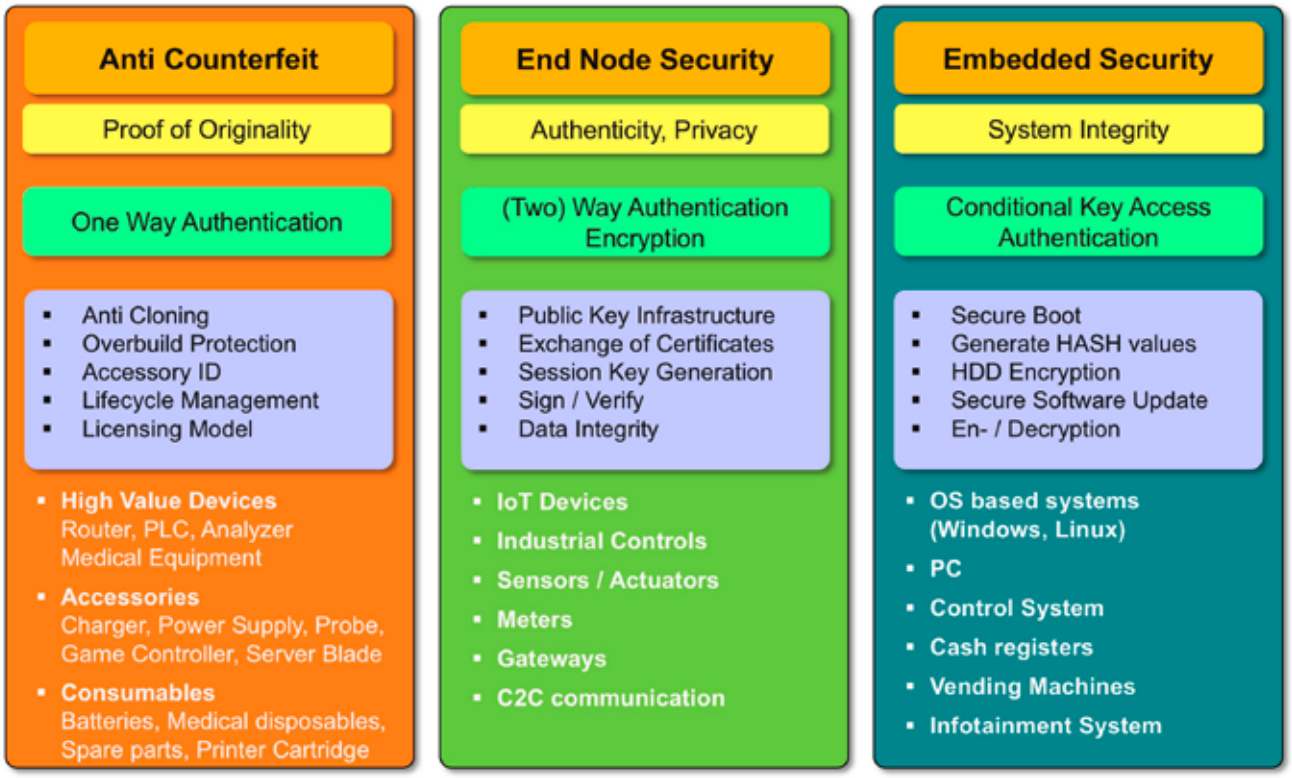
Kerckhoffs's law (from the 19th century)

A cryptosystem should be secure even if everything about the system, except the key, is public knowledge.

PRINCIPALS AND BEST PRACTICES

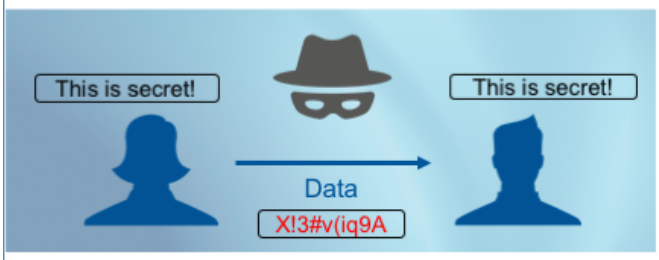
- Security by **design**
  - Think about security from the beginning
  - Adding it later is often difficult and expensive
  - Use proven, established algorithms / tools / hardware
  - Do it regularly (audit)
- Security is a **process**
  - Mechanisms come and go
  - Very active field of research
  - Reviewed by scientific community
  - Competitions for new algorithmslike SHA-3, CAESAR, eSTREAM, ...
  - Open-source implementation
- Security consist of **layers**
  - Not one perfect mechanism/solution
  - Effort increases with number of layers
  - Multiple mechanisms to enforce a policy

SECURITY MEASURES



SECURITY OBJECTIVES

In principal, all security objectives can be tailored down to three fundamental cryptographic objectives.



Confidentiality: Eavesdropping possible?

Solution: Encryption / Decryption
Symmetric, (Asymmetric)

Integrity: Code or message modified?

Solution: Checksum
Hash (e.g. memory content)
MAC (e.g data stream)
Digital Signature

Authenticity: Device original?

Solution: Challenge & Response
MAC (symmetric)
Sign – Verify (asymmetric)

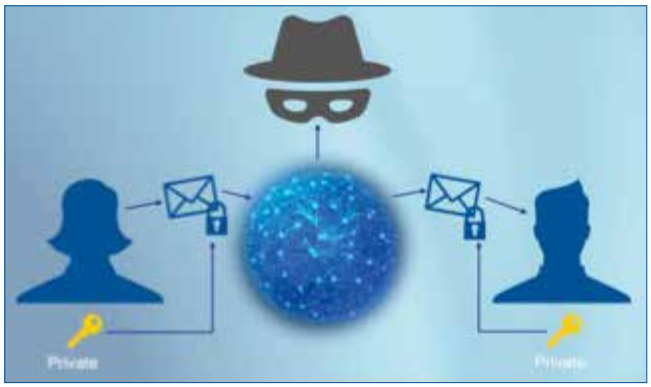
SECURITY FUNDAMENTALS

Symmetric Encryption

The easiest way to scramble information is to use a symmetric crypto algorithm. Doing this, two parties, like a host and a client, are using the same key to encrypt and decrypt information. This secret key has to be stored in a secured way (crypto hardware) and shall never be disclosed. A symmetric algorithm is very fast and easy to implement and, therefore, already existing in many microcontrollers. The main challenge for using symmetric encryption is the key exchange of the symmetric keys. In order to avoid that the same key is used in a larger system where there is an increased risk to break this system, it is common to generate symmetric session keys (one time use only) for the encryption itself and to use an asymmetric algorithm based process to exchange or generate these keys before the symmetric encryption.

Typical Usage
- Data Encryption / Decryption
- Scrambling of Software

Typical Algorithms
- AES 128, AES 256
- Not recommended: DES, 3DES

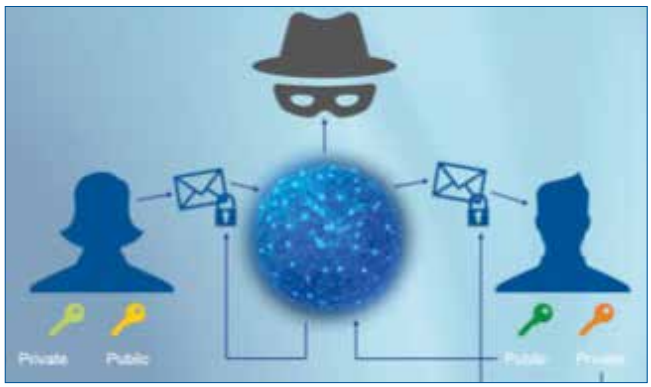


Asymmetric Encryption

Whereas symmetric algorithms are used for encrypting/ decrypting data, the strength of asymmetric encryption is in the area of authenticating a device in a system. Instead of using the same key for the host and the client, now all devices own a key-pair, which is mathematically linked and only these two keys can work together. One key is called the private key and should be stored in a secured way (crypto hardware). This key may never be disclosed to anybody. The corresponding second key is called the public key and can be distributed to everybody in the system. Depending on the use case, asymmetric encryption is either used to sign any kind of data for later authentication (using one's own private key) or to encrypt information (using someone else's public key).

Typical Usage
- Session Key Generation
- Sign / Verify
- Certificates

Typical Algorithms
- RSA-3072
- ECC-256

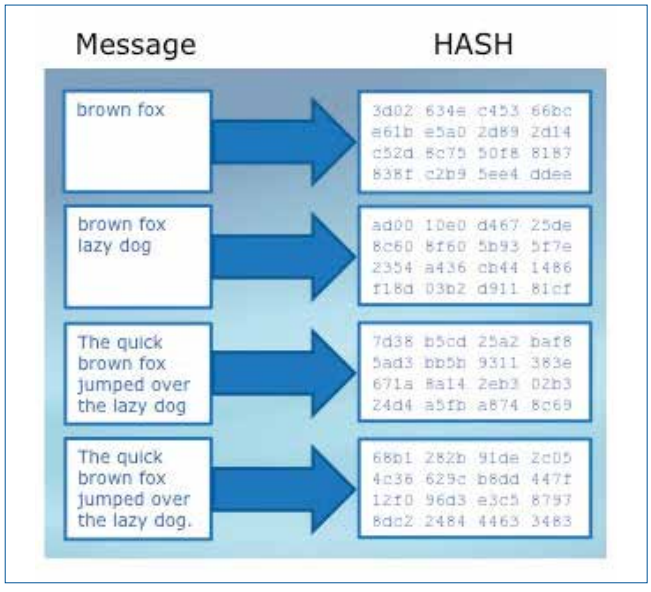


HASH

A HASH function is used as a kind of checksum in order to verify if data has been changed or manipulated. Any input data stream with a variable length is processed with a standardized proven algorithm and the result is a HASH value with a fixed length of bytes. Since the calculation is one way, there is no chance to compute the original message just from the HASH value. Also a minor change on the input side will result in a big change on the output side.

Typical Usage
- Software / Data Integrity Check
- Password Storage
- Pseudo- Random Generator

Typical Algorithms
- SHA-256, SHA3-256
- Not recommended: MD5, SHA1



Certificates

Like an ID card in real life, a certificate is used to assure the authenticity of data or a device. Depending on the use case, a company can either sign the certificate on its own – to check the authenticity of e.g. spare parts, or if a company wants to show authenticity to the outside world, get certificate data signed by an external Certification Authority (CA).

Content of a Certificate:

- Technical Data (Serial Number, Validity Date, Issuer …)
- Personal/Device Data (Web Address, Device ID, Product Part Number …)
- Public Key (Device Public Key)
- Signature (HASH value signed with the issuer's private key)

"TECHNICAL DATA"

```
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            17:90:60:e1:cc:00:93
    Signature Algorithm: sha256WithRSAEncryption
        Issuer: C=DE, O=DFN-Verein, OU=DFN-PKI, CN=DFN-Verein PCA Global - G01
        Validity
            Not Before: May 12 15:05:53 2014 GMT
            Not After : Jul  9 23:59:00 2019 GMT
```

"PERSONAL DATA"

```
Subject: C=DE, O=RWTH Aachen, CN=RWTH Aachen CA/emailAddress=ca@rwth-aachen.de
```

"PUBLIC KEY"

```
Subject Public Key Info:
    Public Key Algorithm: rsaEncryption
        Public-Key: (2048 bit)
        Modulus:
            00:b8:30:08:64:e3:c8:dc:7a:52:df:35:42:39:92:
            f3:2f:f8:21:79:e3:12:67:2f:8c:7f:70:94:27:37:
            63:48:77:a0:89:dd:fa:ac:d2:c8:8e:d9:ec:48:00:
            […]
            52:7b:01:51:89:27:10:52:53:30:e7:d3:19:03:2d:
            8b:d9:c2:a6:9e:62:48:fc:90:30:76:a1:27:91:c9:
            f1:a3
        Exponent: 65537 (0x10001)
```

"SIGNATURE"

```
Signature Algorithm: sha256WithRSAEncryption
     6e:e1:13:2c:20:8c:c8:38:1a:e4:af:3e:65:a1:03:a6:a1:9b:
     87:7a:40:7b:2c:69:58:06:2a:2e:ed:84:ea:8d:63:9a:03:15:
     06:2f:9c:5f:d8:bf:6a:a3:64:27:c5:e1:61:59:49:c3:20:7b:
     […]
     da:9d:d2:f2:ab:b3:e1:47:f3:da:59:a8:c9:67:a1:ea:df:48:
     aa:db:0d:f6:ce:11:40:82:1a:93:8c:93:0f:24:28:14:ef:c3:
     1e:84:a4:b9:41:d5:42:15:f2:2b:e3:12:40:f8:ee:ec:af:59:
     21:dd:e6:2e
```

OPTIGA™ - EASY TO USE, RELIABLE EMBEDDED SECURITY SOLUTIONS FOR IoT APPLICATIONS

Infineon`s OPTIGA™ family of security solutions is designed for easy integration into embedded systems to protect the confidentiality, integrity and authenticity of information and devices. These hardware-based security solutions scale from basic authentication chips to sophisticated implementations and are used in a wide range of embedded applications ranging from consumer to industrial applications. Designed by the leading provider of embedded security solutions, Infineon`s OPTIGA™ combines sophisticated and strong security with ease of use and wide range implementation support for the customer. With OPTIGA™ customers get the full package consisting of the security chips with an operating system as well as libraries for the host controller which makes it easy to get started with IoT security right away. Additionally, customized implementation consulting and dedicated security concepts for specific applications is available through the Infineon Security Partner Network (ISPN).

OPTIGA™ TPM FAMILY – SLB 96XX

Key Features

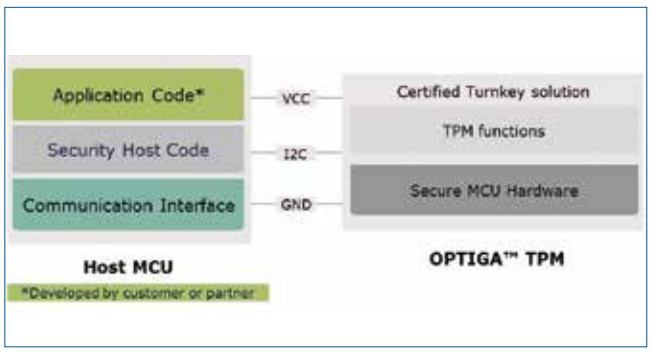
- Standardized security controller
- TCG certified products
- Products with TPM 1.2 and 2.0
- Standard & extended temperature range (-40...85°C)
- Firmware upgrade capability
- SPI, I²C & LPC interface
- VQFN-32 & TSSOP-28 package
- CC and FIPS certification

Customer Values

- Innovative security solutions provided by the market leader
- High confidence level based on Common Criteria certification
- Easy integration based on standardization

Applications

- Notebooks/PCs/tablets/severs
- Network systems and boards
- Industrial automation
- Home automation
- Automotive



OPTIGA™ TRUST B SLE95250

Key features

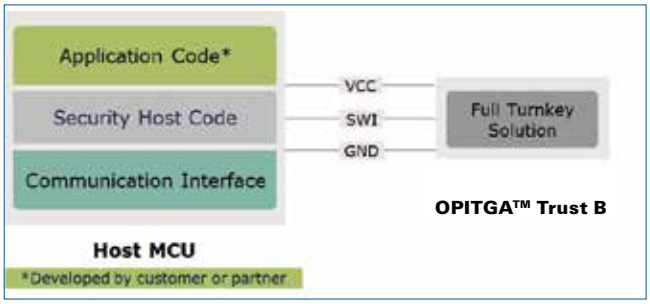
- Strong cost efficient asymmetric cryptography with ECC 131-bit key length
- Turnkey solution including host-side software for easy integration
- 512 bit user NVM
- Easy-to-implement single-wire host interface
- Life span counter for original parts
- OPTIGA™ Digital Certificate (ODC) with device personalization (unique key pair per chip)
- Size-optimized TSNP-6-9 package (1.1 x 1.5 mm)

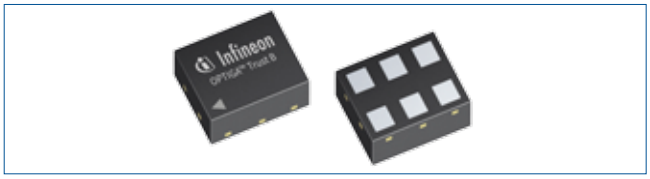
Customer value

- Lower system costs due to single-chip solution
- Increased security with asymmetric cryptography and chip-individual keys
- Easy integration thanks to full turnkey design

Applications

- Battery authentication
- IoT edge devices
- IP & PCB design protection
- Consumer accessories
- Original replacement parts
- Medical & diagnostic equipment



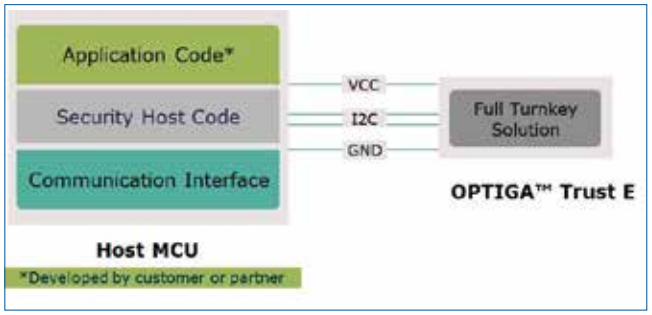


OPTIGA™ TRUST E SLS 32AIA

Key features
- Advanced security controller
- Turnkey solution
- Full system integration support
- PC interface
- Up to 3 Kbyte user memory
- ECC 256 bit, SHA-256
- Compliant with new USB Type-C standard
- Standard & extended temperature range (-40...85 °C)
- USON-10 package (3 x 3 mm)

Customer values
- Protection of IP and data
- Protection of business cases
- Protection of company image
- Safeguarding of quality and safety

Applications
- Internet of things (IoT)
- Industrial control and automation
- Medical devices
- Consumer electronics
- Smart home
- PKI networks

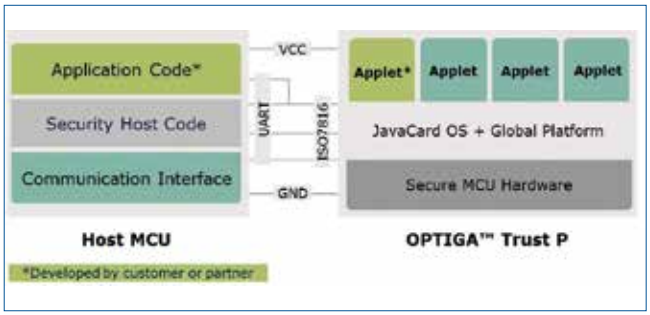


OPTIGA™ TRUST P SLJ 52ACA

Key features
- High-end security controller with advanced cryptographic algorithms implemented in hardware (ECC521, RSA2048, TDES, AES)
- Common Criteria EAL 5+ (high) certification
- Programmable Java Card operating system with reference applets for a variety of use cases and host-side support
- 150 KB user memory
- Small footprint VQFN-32 SMD package (5 x 5 mm)
- ISO 7816 UART interface

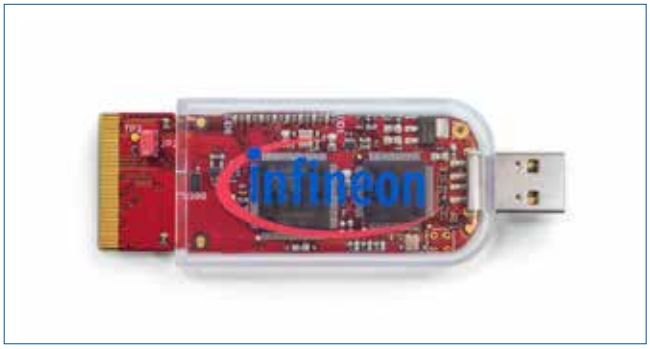
Customer value
- Confidence in a secured and certified solution
- Increased flexibility based on programmable solution with reference applets to simplify customization and integration
- Protection of system integrity, communication and data

Applications
- Industrial control system
- Energy generation & distribution systems
- Healthcare equipment & networks
- Consumer electronics
- Home security & automation
- Network applications



OPTIGA™ TRUST B EVALUATION BOARD

- Based on Infineon XMC4500 microcontroller
- USB: Simulated Host for demo purpose
- Windows based GUI for demo purpose
- Support of multiple devices by single-wire host interface (SWI)
- Non-volatile memory with read and write capability



SP no: SP001675878

OPTIGA™ TRUST E EVALUATION KIT

- XMC4500 Relax Kit with Extension Board incl. OPTIGA™ Trust E
- Easy to use GUI for demo purpose
- Intuitive Getting started guide with step by step descriptions
- Incl. all required Cables, Software and Documentation

SP no: SP001398818

OPTIGA™ TRUST P DEMO KIT

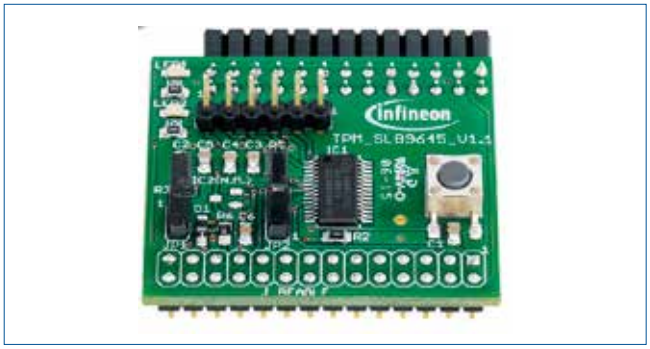
- OPTIGA™ Trust P Board
- Host Controller Board
- Connection Cables
- Demo Utility Software (PC)
- Demo System User Guide
- Demonstrates Functionality of OPTIGA™ Trust P
- Expandable to Full Development Kit with Software Download

SP no: SP001220816

OPTIGA™ TPM SLB9645 (I²C) SUPPORT – EVAL BOARD

- Plug-In Board (IRIDIUM) for the
  - RaspberryPi
  - Beagle Board-xM

- Documentation - Application note describing how to setup authentication and secure communication including:
  - Linux setup and driver
  - Software Stack
  - TPM Initialization
  - OpenSSL/GnuTLS



SP no: SP001265088

OPTIGA™ TPM AND OPTIGA™ TRUST PRODUCT FAMILY OVERVIEW

Sales code	Interface	Temperature range	Package	Common Criteria certified	Typical / recommended use s code
OPTIGA™ TPM SLB 9645					
SLB 9645TT1.2	I²C	-20 ... +85	TSSOP-28		Notebook, desktops, tablets, mobile computing on non x86
SLB 9645XQ1.2	I²C	-40 ... +85	VQFN-32		Industrial embedded computing on non x86
SLB 9645XT1.2	I²C	-40 ... +85	TSSOP-28		Industrial embedded computing on non x86
OPTIGA™ TPM SLB 9660					
SLB 9660TT1.2	LPC	-20 ... +85	TSSOP-28	√	Notebook, desktops, tablets on x86 & embedded computing
SLB 9660VQ1.2	LPC	-20 ... +85	VQFN-32	√	Notebook, desktops, tablets on x86 & embedded computing
SLB 9660XT1.2	LPC	-40 ... +85	TSSOP-28	√	Industrial embedded computing on x86
SLB 9660XQ1.2	LPC	-40 ... +85	VQFN-32	√	Industrial embedded computing on x86
OPTIGA™ TPM SLB 9665					
SLB 9665TT2.0	LPC	-20 ... +85	TSSOP-28	√	Notebook, desktops, tablets on x86/x64 & embedded computing
SLB 9665VQ2.0	LPC	-20 ... +85	VQFN-32	√	Notebook, desktops, tablets on x86/x64 & embedded computing
SLB 9665XT2.0	LPC	-40 ... +85	TSSOP-28	√	Industrial embedded computing on x86/x64
SLB 9665XQ2.0	LPC	-40 ... +85	VQFN-32	√	Industrial embedded computing on x86/x64
OPTIGA™ TPM SLB 9670					
SLB 9670VQ1.2	SPI	-20 ... +85	VQFN-32	√	All architectures
SLB 9670XQ1.2	SPI	-40 ... +85	VQFN-32	√	All architectures
SLB 9670VQ2.0	SPI	-20 ... +85	VQFN-32	√	All architectures
SLB 9670XQ2.0	SPI	-40 ... +85	VQFN-32	√	All architectures
OPTIGA™ Trust					
OPTIGA™ Trust B SLE95250	SWI	-25 ... +85	TSNP-6		
OPTIGA™ Trust E SLS 32AIA	I²C	-40 ... +85	USON-10		
OPTIGA™ Trust P SLS 52ACA	ISO 7816 UART	-25 ... +85	VQFN-32	√	

www.ebv.com/optiga

DRIVING INTEROPERABILITY, SECURITY AND CONVENIENCE THROUGH CIPURSE™ OPEN STANDARD FOR SERVICES IN SMART CITIES

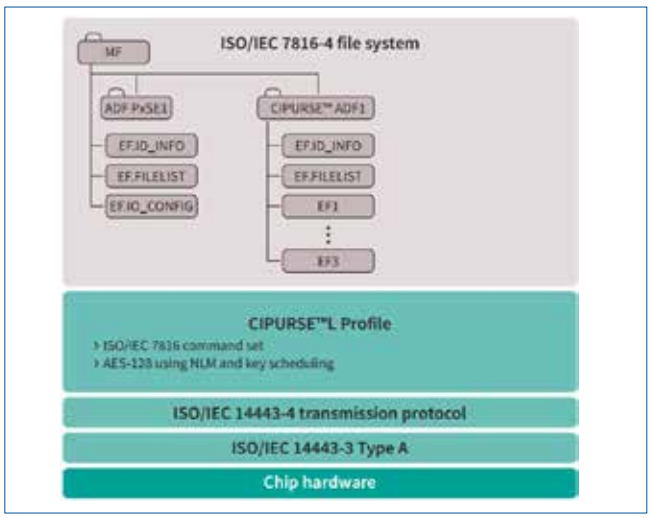
At Infineon, we understand the market need for open, non-proprietary, interoperable, secure and competitive solutions capable of spanning ticketing, identification, micropayment and access management. CIPURSE™ is the only global open standard for secure, cost-effective and flexible fare collection, identification and access management solutions. All of our contactless platforms are available with CIPURSE™ compliance.

Supported by a global, multi-provider community, CIPURSE™

- Provides a secure and flexible solution for smart city application, such as for public transport, access, loyalty and micropayment
- Protects investments
- Is non-discriminatory and compliant with public procurement rules
- Utilizes the advanced AES 128 encryption algorithm, which enables fast and secure transactions

CIPURSE™ MOVE – SLM 10TLC002L

The CIPURSE™ move is a ready-to-use cost optimized contactless security product and offers secure storage of AES-128 keys in hardware for 3-pass mutual authentication and communication. It targets single application and provides 304 Byte of user memory for application data storage. It is the ideal product to support migration from existing nonsecure or systems using Mifare compatible technology towards a more advanced, state-of-the-art and future proven security architecture such as the Open Standard CIPURSE™.



Memory & Block diagram

Key Features

- ISO/IEC 14443-3 Type A contactless interface
- CIPURSE™ L Profile compliant
- 304 Byte (2.4 kbit) user memory
- One application configurable
- Limited Refund feature
- NFC Forum Type 4 support
- Secure storage of AES-128 keys
- Secured 3 pass mutual authentication using AES-128
- Secured communication using AES-128 and session key derivation mechanism
- Data exchange protocol inherently DPA and DFA resistant

Customer Values

- Secured transaction (< 100 ms)
- Ready-to-use for personalization
- Future proven cost effective solution for single application
- CIPURSE™ certified

Applications

- Public Transport Ticketing
- Limited Use Ticket, Limited Use Card
- Account based Ticket, Single Ride Ticket
- Event Ticket
- Access management, hospitality
- Loyalty and identification
- Closed-loop payment

CIPURSE™4MOVE – SLS 32TLC00XS(M)

The CIPURSE™4move is a ready-to-use cost optimized contactless security controller. It targets multi-applications and is available with 2 and 4 kByte user memory for application data storage of up to 8 custom applications. It is the ideal product to support the upgrade from existing nonsecure or systems using Mifare compatible technology towards a more advanced, state-of-the art and future proven security architecture such as the Open Standard CIPURSE™.

Key Features

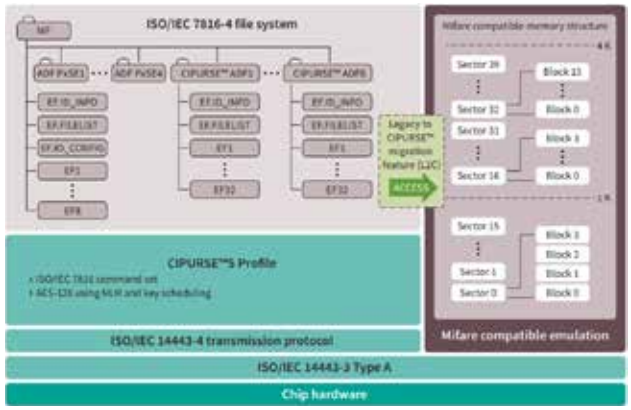
- ISO/IEC 14443-3 Type A contactless interface
- CIPURSE™ S Profile compliant
- 2 kByte and 4 kByte user memory
- Up to 8 applications configurable
- Optional support of 1 kByte or 4 kByte Mifare compatible emulation
- Legacy to CIPURSE™ migration feature
- Limited refund feature
- NFC Forum Type 4 Tag support
- Data rates up to 848 kbit/s
- Secured communication using AES-128 and session key derivation mechanism
- Data exchange protocol inherently DPA and DFA resistant

Customer Values

- Secured transaction (< 100 ms)
- Ready-to-use for personalization
- Future proven cost effective solution for multi-application
- CIPURSE™ certified
- CC EAL 5+ (high) for HW and SW

Applications

- Public Transport Ticketing
- Event Ticket
- Access management, hospitality
- Loyalty and identification
- Closed-loop payment



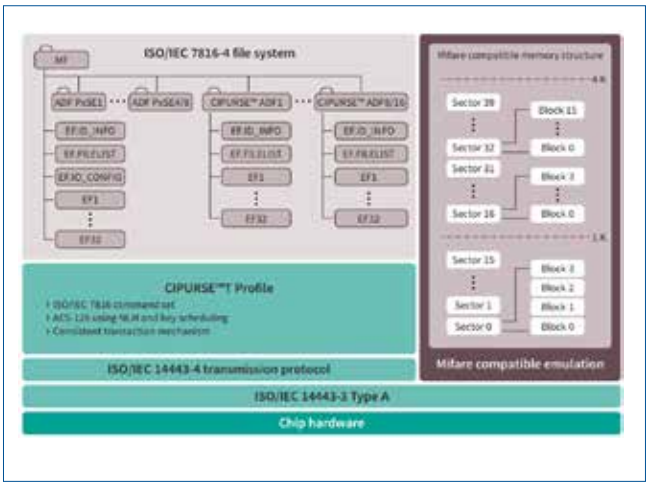
Memory & Block diagram

CIPURSE™ SECURITY CONTROLLER – SLS 32TLC100(M)

The CIPURSE™ Security Controller is a ready-to-use cost optimized contactless security controller. It targets multi-applications and is available with 8 kByte user memory for application data storage of up to 8/16 custom applications. It is the ideal product to support the upgrade from existing nonsecure or systems using Mifare compatible technology towards a more advanced, state-of-the-art and future proven security architecture such as the Open Standard CIPURSE™.

Key Features

- ISO/IEC 14443-3 Type A contactless interface
- CIPURSE™ T Profile compliant
- 8 kByte user memory
- Up to 8/16 applications configurable
- Optional support of 1 kByte or 4 kByte Mifare compatible emulation
- Limited refund feature
- NFC Forum Type 4 Tag support
- Data rates up to 848 kbit/s
- Secured communication using AES-128 and session key derivation mechanism
- Data exchange protocol inherently DPA and DFA resistant



Memory & Block diagram

Customer Values

- Secured transaction (< 100 ms)
- Ready-to-use for personalization
- Future proven cost effective solution for multi-application
- CIPURSE™ certified
- CC EAL 5+ (high) for HW and SW
- Security attack preventions for all critical operations using both hardware and software countermeasures

Applications

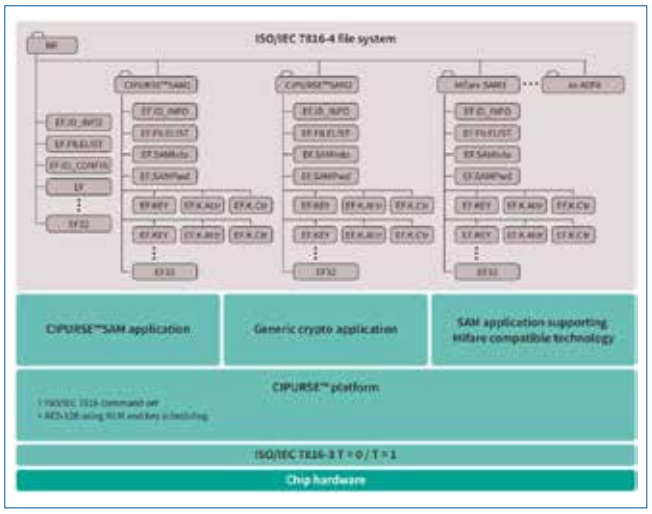
- Public Transport Ticketing
- Event Ticket
- Access management, hospitality
- Loyalty and identification
- Closed-loop payment

CIPURSE™SAM – SLF 9630

The CIPURSE™SAM is a ready-to-use Secure Access Module and offers secure storage of keys in hardware for 3-pass mutual authentication and communication. It offers a dedicated key management system with flexible key diversification and secured key loading for user card authentication, personalization and SAM administration. Commands and transmitted data can be secured using the CIPURSE™ Cryptographic Protocol which is inherently resistant against physical attacks like DPA and DFA and was honored in 2012 with the German IT Security Award.

Key Features

- Enables secured authentication between a reader and CIPURSE™ smart cards using AES-128 based authentication schemes or cards using Mifare compatible technology
- Dedicated key management system including key derivation and key upload
- Online and offline modes
- Up to 8 SAM applications (ADF) configurable
- Up to 512 reloadable 128-bit keys across all key files for SAM operations
- Secure storage of keys
- Secured 3 pass mutual authentication
- Secured communication using AES-128 and session key derivation mechanism
- Data exchange protocol inherently DPA and DFA resistant



Memory & Block diagram

Customer Values

- Secured transaction (< 100 ms)
- Ready-to-use for personalization
- Future proven cost effective solution for security application
- CIPURSE™ certified
- CC EAL 6+ (high) for HW

Applications

- Public Transport Ticketing
- Event Ticket
- Access management, hospitality
- Loyalty and identification
- Closed-loop Micropayment

CIPURSE™ EVALUATION & DEVELOPMENT KIT

The CIPURSE™ Evaluation & Development Kit enables communication with CIPURSE™ compliant smart cards and Secure Access Module (SAM). The kit supports plain-text as well as CIPURSE™ AES-128 based cryptography protected communication. You can develop and load state of the art security applications onto a CIPURSE™ card or SAM without a need for additional tools or equipment.

Key Features

- CIPURSE™ Explorer
  - Graphical user interface for user-friendly interfacing to CIPURSE™ based products
  - Script execution
  - Detailed User Manual
- Sample Scripts
  - Scripts for CIPURSE™ SAM personalization & key distribution
  - Scripts for card personalization & operation
  - Scripts for NFC Type 4 Tag configuration
- CIPURSE™ sample cards
  - CIPURSE™ move SLM 10TLC002L
  - CIPURSE™ 4move SLS 32TLC00xS(M)
  - CIPURSE™ Security Controller SLS 32TLC100(M)
  - CIPURSE™ SAM SLF 9630

SP Number: SP000942974

Customer Values

- State-of-the art JavaScript execution environment with built-in libraries implementing CIPURSE™ command set and CIPURSE™ cryptography
- Support of Infineon's CIPURSE™ products
- Interfacing to PC/SC smart card readers
- For implementation into terminals source code modules are provided to ease realization of CIPURSE™ relevant functionality: CIPURSE™ Terminal Secure Messaging Application Note, CIPURSE™ Command Library

Sales code	Interface	Temperature range	Package	Common Criteria certified	Typical applications
my-d™ move					
SLE 66R01P	ISO/ IEC 14443-3 Type A, NFC Forum Type 2 Tag operation	-25 °C … +70 °C	C, NB		Public Transport, Ticketing, Access Management
SLE 66R01L	ISO/ IEC 14443-3 Type A, NFC Forum Type 2 Tag operation	-25 °C … +70 °C	C, NB		Public Transport, Ticketing, Access Management
Mifare compatible SLE 66R35					
SLE 66R35I	ISO/IEC 14443-3 Type A	-25 °C … +70 °C	C, NB, MCC2, MCC8		Public Transport, Ticketing, Access Management
SLE 66R35R	ISO/IEC 14443-3 Type A	-25 °C … +70 °C	C, NB, MCC2, MCC8		Public Transport, Ticketing, Access Management
SLE 66R35E7	ISO/IEC 14443-3 Type A	-25 °C … +70 °C	C, NB, MCC2, MCC8		Public Transport, Ticketing, Access Management
CIPURSE™move					
SLM 10TLC002L	ISO/IEC 14443-3 Type A, ISO/IEC 14443-4 Transmission Protocol, NFC Forum Type 4 Tag configurable	-25 °C … +70 °C	C, NB, MCC8		Public Transport, Ticketing, Access Management, Micropayment
CIPURSE™4move					
SLS 32TLC002S	ISO/IEC 14443-3 Type A, ISO/IEC 14443-4 Transmission Protocol, NFC Forum Type 4 Tag configurable	-25 °C … +85 °C	C, NB, MCC8	√	Public Transport, Ticketing, Access Management, Micropayment
SLS 32TLC002S1	ISO/IEC 14443-3 Type A, ISO/IEC 14443-4 Transmission Protocol, Mifare 1kB compatibility, NFC Forum Type 4 Tag configurable	-25 °C … +85 °C	C, NB, MCC8	√	Public Transport, Ticketing, Access Management, Micropayment
SLS 32TLC002S4	ISO/IEC 14443-3 Type A, ISO/IEC 14443-4 Transmission Protocol, Mifare 4kB compatibility, NFC Forum Type 4 Tag configurable	-25 °C … +85 °C	C, NB, MCC8	√	Public Transport, Ticketing, Access Management, Micropayment
SLS 32TLC004S	ISO/IEC 14443-3 Type A, ISO/IEC 14443-4 Transmission Protocol, NFC Forum Type 4 Tag configurable	-25 °C … +85 °C	C, NB, MCC8	√	Public Transport, Ticketing, Access Management, Micropayment
SLS 32TLC004S1	ISO/IEC 14443-3 Type A, ISO/IEC 14443-4 Transmission Protocol, Mifare 1kB compatibility, NFC Forum Type 4 Tag configurable	-25 °C … +85 °C	C, NB, MCC8	√	Public Transport, Ticketing, Access Management, Micropayment
SLS 32TLC004S4	ISO/IEC 14443-3 Type A, ISO/IEC 14443-4 Transmission Protocol, Mifare 4kB compatibility, NFC Forum Type 4 Tag configurable	-25 °C … +85 °C	C, NB, MCC8	√	Public Transport, Ticketing, Access Management, Micropayment
CIPURSE™Security Controller					
SLS 32TLC100	ISO/IEC 14443-3 Type A, ISO/IEC 14443-4 Transmission Protocol, NFC Forum Type 4 Tag configurable	-25 °C … +85 °C	C, NB, MCC8, MCS8	√	Public Transport, Ticketing, Access Management, Micropayment, Smart Cities
SLS 32TLC100M1	ISO/IEC 14443-3 Type A, ISO/IEC 14443-4 Transmission Protocol, Mifare 1kB compatibility, NFC Forum Type 4 Tag configurable	-25 °C … +85 °C	C, NB, MCC8, MCS8	√	Public Transport, Ticketing, Access Management, Micropayment, Smart Cities
SLS 32TLC100M4	ISO/IEC 14443-3 Type A, ISO/IEC 14443-4 Transmission Protocol, Mifare 4kB compatibility, NFC Forum Type 4 Tag configurable	-25 °C … +85 °C	C, NB, MCC8, MCS8	√	Public Transport, Ticketing, Access Management, Micropayment, Smart Cities
CIPURSE™SAM					
SLF 9630	ISO/ IEC 7816-3 T=1	-25 ... +85	ID-1/ID-000 card, VQFN-8	√	Security applications with key based authentication, Public Transport, Ticketing, Access Management, Micropayment

MAXIM'S HISTORY OF SECURITY

We have the underlying technology to bring increasing levels of connectivity to our world. But this push for connectivity will only thrive if users can trust the connected objects and their underlying infrastructure. Contrary to what many believe, software alone is insufficient to protect connected, embedded devices from attack. Hardware-based security is the key. Maxim has built a proven portfolio of embedded security ICs that protect against malicious attacks for a broad array of applications. Our line of security managers, secure authenticators and microcontrollers, and resources including reference schematics, drivers, middleware, communication stacks, and support make it easier and faster for you to safeguard your designs.

Figure 1. The Technology Foundation of DeepCover Security

DEEPCOVER SOLUTIONS FOR EMBEDDED SECURITY

Embedded systems are susceptible to numerous threats, including:

- Counterfeiting
- Hardware or software IP reverse engineering
- Malware injection or firmware substitution
- Eavesdropping
- Identity theft
- Unauthorized network connection
- Unauthorized re-use

Secure device authentication, secure boot, and encryption are the answers to these attacks. DeepCover® Secure Authenticators and DeepCover Secure Microcontrollers incorporate these techniques to ensure your platforms are trustworthy.

Trusted platforms, IP protection, secure download, and secure communication are the most frequent requirements for IoT node security. Table 1 maps our DeepCover solutions to common IoT needs.

DEEPCOVER SECURE AUTHENTICATORS

Secure Authenticators provide a core set of fixed-function crypto operations, secure key storage, and numerous supplemental feature options including: secure download/boot processing, protected nonvolatile memory for end application use, secure GPIO, decrement-only counters, session key generation, true random number source, and encrypted R/W of stored data. In addition to cryptographic strength, all devices provide advanced physical protection to address malicious die-level security attacks. As the inventor of the revolutionary 1-Wire® interface, Maxim is a leader in the development of devices that connect to nontraditional form-factors such as printer cartridges, medical disposables and battery packs.

Requirements		DeepCover Secure Authentication ICs		DeepCover Secure Microcontrollers
		SHA-Based	ECDSA-Based	
Trust	Device authentication	•	•	•
	Usage control/features enablement	•	•	•
	Secure boot/download		•	•
IP Protection	Hardware and firmware anticloning	•	•	•
	Firmware encryption			•
Secure Communications	Certificate distribution and verification		•	•
	Packet encryption	•	•	•
	Full TLS support			•
	Small message encryption	•	•	•

Table 1. DeepCover Security Solutions for IoT Security Needs

Secure Authenticator Applications
Maxim's secure authentication solutions solve a wide range of security issues including:

Common Application Requirements
- Product Quality/Safety
- Counterfeit Prevention
- Secure Download/Boot
- Use/Feature Control
- IoT Device Integrity/Authenticity

Solved with Targeted Product Features
- Bidirectional Authentication
- Secure System Data Storage
- Secure Use Counting
- System Session Key Generation
- Secure Memory Settings
- Secure GPIO
- Random Number Source
- IoT Device Integrity/Authenticity

ECDSA AUTHENTICATORS

The **DS28C36** and companion **DS2476** provide a core set of asymmetric-key and symmetric-key cryptographic tools in a compact, low-cost solution. Asymmetric public-key features are supported with the FIPS 186 P256-based elliptic-curve (ECC) algorithm and symmetric secret-key with FIPS 180/198 SHA-256 HMAC. The devices are fully flexible in terms of operational configuration and public-key vs. secret-key feature usage. End application use cases include bidirectional authentication, secure storage of system data (for example, system crypto keys), secure verification of system-critical data, secure boot, and secure use control. Additionally, two pins of GPIO are provided with optional secure state control and level sensing.

The **DS2476** is a companion coprocessor to the **DS28C36** for applications where the host system microcontroller has insufficient computing resources for ECC algorithms or lacks the required secure storage for a ECDSA private key or SHA-256 system secret, when used.

The DS28E35 and companion DS2475 are ECDSA authenticators with a reduced feature set for applications that do not require the full functionality of the DS28C36.

Table 2 lists our DeepCover ECDSA authenticators and companion coprocessors.

SHA-256 AUTHENTICATORS

The **DS28E15**/**DS28E22**/**DS28E25** family of devices operate with the 1-Wire interface and offer several options for user-memory size and operating voltage. The **DS2465** is a companion coprocessor with integrated 1-Wire line driver which provides secure storage for a system SHA-256 key. All devices provide a FIPS 180 based bidirectional authentication capability. The **DS28C22** offers the SHA-256 functionality with an I²C interface.

The **MAX66240**/**MAX66242** are NFC/RFID transponders with SHA-256 bidirectional authentication. The MAX66242 expands this functionality with an option for RF energy harvesting, an I²C interface that can be configured as master or slave, and one GPIO pin. The **MAX66300** is a host system NFC transceiver and companion SHA-256 coprocessor to the transponders and provides secure storage for SHA-256 system keys.

Table 3 lists our DeepCover SHA-256 authentication ICs, companion co-processors, transceivers, and responders.

Part Number	Type	Operating Voltage	Interface	User EEPROM	Package Option
DS28C36	Authenticator	3.3 V	I²C	4kb	TDFN
DS2476	Coprocessor			4kb	TDFN
DS28E35	Authenticator	3.3 V	1-Wire	1kb	TSOC, TDFN
DS2475	Coprocessor		I²C/1-Wire	-	SOT

Table 2. DeepCover ECDSA Authentication Devices

Part Number	Type	Operating Voltage	Interface	User EEPROM	Package Option
DS28C22	Authenticator	3.3 V	I²C	3 kb	TDFN
DS2465	Coprocessor	3.3 V	I²C/1-Wire	0.5 kb	TSOC
DS28E15	Authenticator	3.3 V	1-Wire	0.5 kb	SFN, TSOC, TDFN
DS28E22				2 kb	TSOC, TDFN
DS28E25				4 kb	SFN, TO92, TSOC, TDFN
DS24L65	Coprocessor	1.8 V	I²C/1-Wire	0.5 kb	TSOC
DS28EL15	Authenticator		1-Wire	0.5 kb	SFN, TDFN
DS28EL22				2 kb	TDFN
DS28EL25				4 kb	TDFN
MAX66240	Authenticator Transponder	Passive	NFC	4 kb	SOIC, TDFN, 8-Bump WLP
MAX66242		Passive (optional 3.3 V)	NFC /I²C		
MAX66300	Coprocessor Transceiver	3.3 V, 5 V	NFC/UART/SPI	1 kb	TQFN

Table 3. DeepCover SHA-256 Authentication Devices

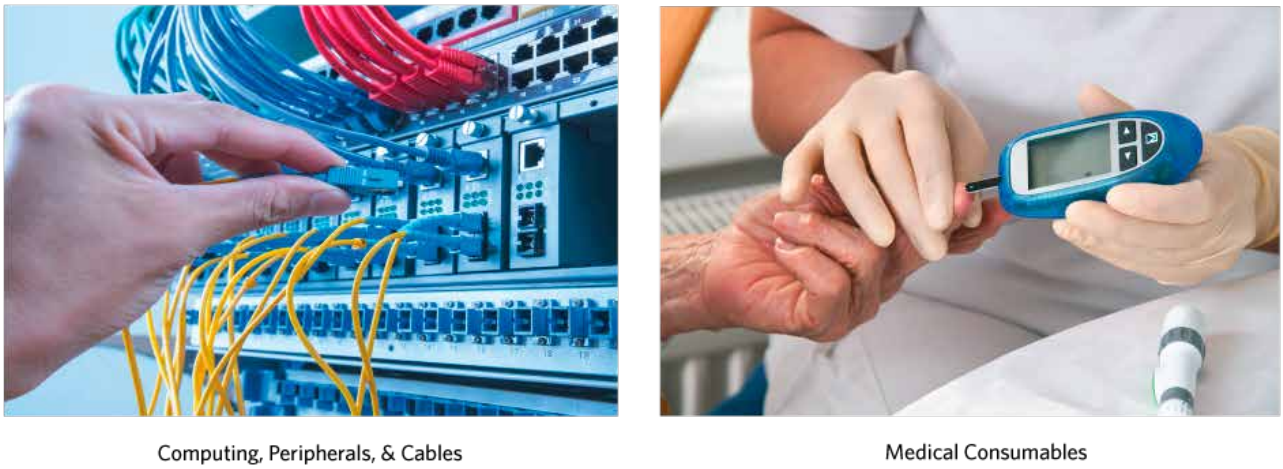


Figure 2. Secure Authentication Applications Made Possible by 1-Wire

THE 1-WIRE INTERFACE

Maxim's 1-Wire interface solution provides a versatile, rugged and very reliable interconnect method for secure authentication in areas not previously possible. This is of particular value when there is a contact limited interconnect to the subassembly that needs authentication. In addition to IoT nodes, examples include medical sensors and tools, pluggable modules, industrial controllers, authentication for printer cartridges and general IP protection. Figure 2 provides examples of end applications that 1-Wire enables.

1-Wire Product Features:

- Single Contact Sufficient for Control and Operation
- Power Derived from the 1-Wire Bus ("Parasite Power")
- Unique ID Factory-Programmed into Each Device
- Multidrop Capable: Supports Multiple Devices on a Single Line
- Exceptional ESD Performance, typically 8kV HBM

TOOLS AND SERVICES FOR SECURE AUTHENTICATORS

Reference Designs:

- **MAXREFDES155**: Embedded Security in IoT - Public-Key Secured Data Paths with ECDSA (Figure 3)
- **MAXREFDES143**: IoT Authenticated Sensing and Notification with SHA-256
- **MAXREFDES43**: Xilinx® Zynq™ ZedBoard™ Authentication with DS28C22 SHA-256
- **MAXREFDES44**: Xilinx Zynq MicroZed Authentication with DS28E35 ECDSA
- **MAXREFDES34**: Xilinx Spartan-6 Authentication with DS28E15 SHA-256

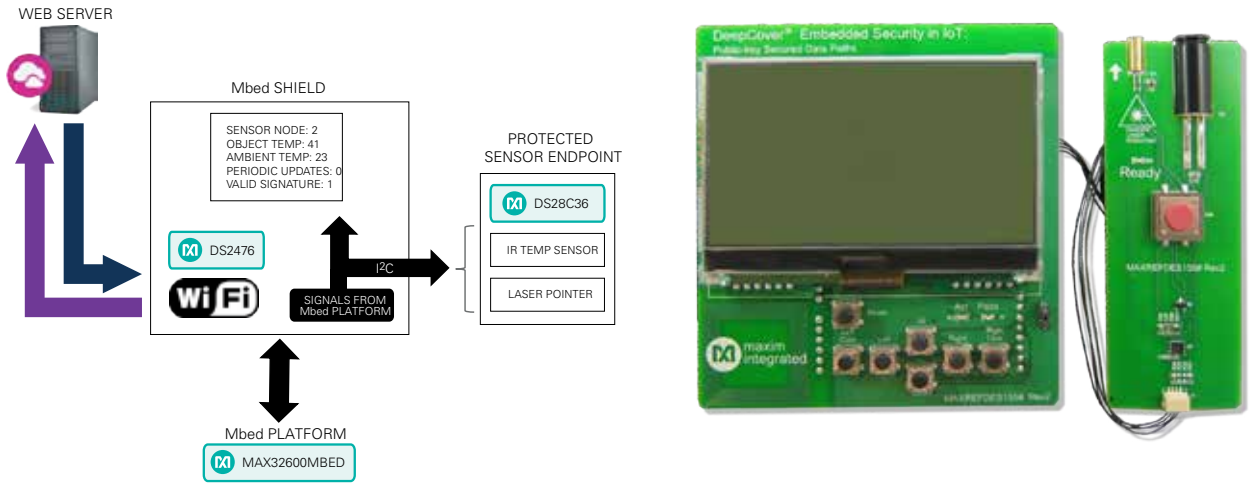


Figure 3. MAXREFDES155 Reference Design

A FACTORY KEY MANAGEMENT SERVICE FOR SECURE AUTHENTICATORS

A fundamental cryptosystem principle regarding keys that was introduced in 1883 by Dutch cryptographer Auguste Kerckhoffs applies equally today:

"A cryptosystem should be secure even if everything about the system, except the key, is public knowledge."

With this in mind, OEMs that use secure authenticators in their end applications must ensure that their keys are programmed prior to equipment being delivered to end customers and that the keys are not compromised at any point in the supply chain. As a value-add option to OEMs, Maxim offers a key management and programming service to securely install keys, certificates, and application data prior to product shipment. Our secure process for transferring your data to our factory includes an encrypted file transfer of device settings from your computer to our production environment. You can be assured that the secret or private key is not compromised during manufacturing or at any point in the supply chain. Contact EBV for additional information.

SECURE AUTHENTICATOR EVALUATION KITS

Table 4 lists the evaluation kits for each secure authenticator device.

SECURE MULTI-DEVICE PROGRAMMER

Although factory, OEM and distributor programming services are geared towards high-volume production builds, there is also a need for security when building prototypes and for low-volume applications.

The DS9488-GP8 multi-device programming system securely install keys, data, and device configuration settings for a variety of our 1-Wire® and I²C interfaced products. The system optionally enables encrypted programming files to be securely moved from one programmer to another to support development at one location and programming at another, if needed. Socket adapters are available for most device packages.

Part Number	Evaluation Kit
DS28C36 DS2476	DS28C36EVKIT
DS28E35 DS2475	DS28E35EVKIT
MAX66242 MAX66240 MAX66300	MAX66300-24XEVKIT
DS28C22	DS28C22EVKIT

Table 4. Secure Authenticator Evaluation Kits

Part Number	Evaluation Kit
DS28E15	DS28E15EVKIT
DS28E22	DS28E22EVKIT
DS28E25	DS28E25EVKIT
DS2465	See note
DS28EL15	DS28EL15EVKIT
DS28EL22	DS28EL22EVKIT
DS28EL25	DS28EL25EVKIT
DS24L65	See note

Note: The DS2465 and DS24L65 are included in the evaluation kits for DS28E15/DS28C22/DS28E25 and DS28EL15/DS28EL22/DS28EL25

DEEPCOVER SECURE MICROCONTROLLERS FOR EMBEDDED SECURITY

Maxim pioneered active tamper reaction technology, which instantaneously wipes out the keys and secrets of devices during attempted tampering, enabling a security level of FIPS 140-2 level 3 or 4.

Active tamper reaction technology requires a battery to operate. For end-products and applications that cannot accommodate a battery, we developed the DeepCover secure cryptographic controller, **MAXQ1061**, which is based on tamper-proof EEPROM and does not require a battery (Figure 4). Table 5 lists DeepCover secure microcontrollers designed specifically for embedded security applications.

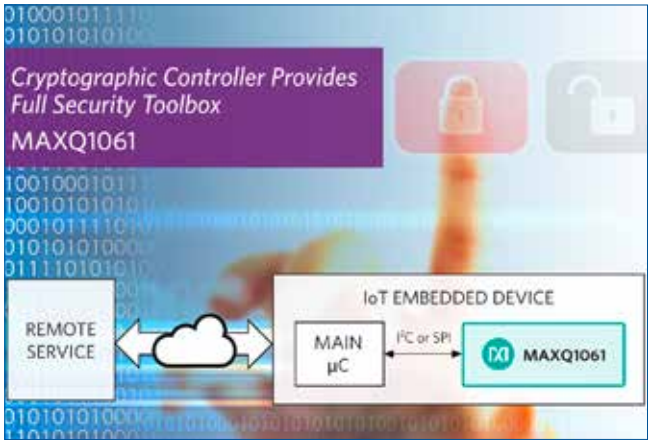


Figure 4. MAXQ1061

MAXQ1061: DEEPCOVER SECURE CRYPTOGRAPHIC CONTROLLER

The MAXQ1061 protects the confidentiality, authenticity and integrity of software IP, communication and revenue models. It is ideal for IoT nodes, connected embedded devices, industrial networking, PLC, and network appliances.

The embedded, comprehensive cryptographic toolbox provides key generation and storage up to full SSL/TLS/DTLS support. It handles encryption, ECDSA digital signature computation, and verification. It can also serve as a secure bootloader for an external generic microcontroller.

Key Features:

- Advanced Cryptographic Tool Box Seamlessly Supports Highly Secure Key Storage
- Make Certificates Distribution Easy
- High-Level Functions Simplify SSL/TLS/DTLS Implementations
- Multiple Communication Interface Options for Simpler Connection to a Host Processor
- Comprehensive Host Software Libraries are Provided
- Extensive Host/System Services Increase Flexibility and
- Reduce System Cost
- Fast AES Engine for Bulk Encryption
- No Firmware Development Required

Part Number	Core	Frequency	Key Storage	USB	I²C	SPI	Symmetric Crypto	Asymmetric Crypto	Hash Algorithms
MAXQ1061	Built-in Firmware		Tamperproof EEPROM		•	•	AES 128, 256	ECDSA P-256, P-384, P-521 ECDH	SHA-256, SHA-384, SHA-512
MAX32555	Cortex® M3	60 MHz	Active tamper reaction	•	•	•	AES 128, 192, 256 3DES	RSA 1024, 2048 ECDSA P-256, P-384, P-521 ECDH	SHA-224, SHA-256, SHA-384, SHA-512
MAXQ1050	MAXQ30	20 MHz	Active tamper reaction	•		•	AES 128, 192, 256	RSA 1024, 2048 ECDSA P-192, P-256	SHA-224, SHA-256

Table 5. DeepCover Secure Microcontrollers for Embedded Security Applications

DEEPCOVER SECURE MICROCONTROLLERS FOR FINANCIAL TRANSACTIONS

Consumer payment habits are changing: chip cards are replacing magnetic stripe cards, contactless payment is now supported either by smartcards or smartphones, mobile POS terminals enable card acceptance for small merchants or home services, and countertop POS systems are adopting the tablet form factor. In the meantime, standards and payment schemes require even greater security. Supporting the increased flexibility expected by consumers, while at the same time guaranteeing the security of transactions, has become a permanent challenge for financial transaction systems designers. Maxim's expertise in this field has enabled the development of a wide range of secure microcontrollers supporting these trends.

For example, the **MAX32560** secure microcontroller (Figure 5) integrates an EMV-compliant integrated contactless reader interface that makes this device the first secure microcontroller to support PCI-PTS security and contactless payments.

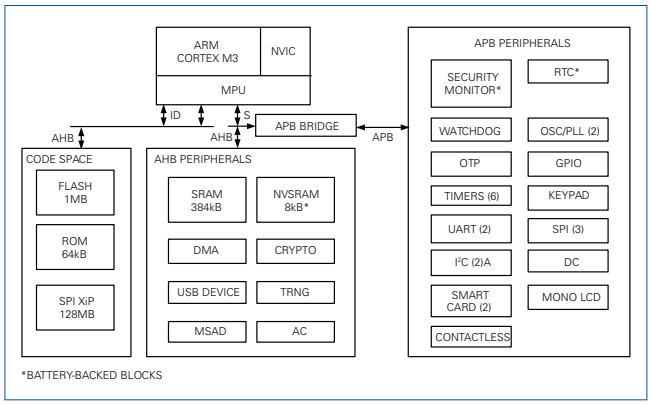


Figure 5. MAX32560 Block Diagram

Our secure microcontrollers feature:

- Active tamper reaction
- Hardware crypto accelerators
- Dedicated integrated analog interfaces for financial transactions
  - EMV-compliant smartcard PHY
  - Magnetic stripe card reader
  - EMV contactless
- Internal security monitors
- Advanced sensors for external tamper detection

Our expertise also goes beyond silicon. In addition to delivering secure microcontrollers with the latest security features, we also provide:

- EMV software stacks
- PCI-PTS evaluation reports
- Crypto libraries
- Full Linux BSP and PCI-PTS-compliant Linux code for **MAX32590**
- Support for PCI-PTS and EMV certifications

Secure Arm-Based Microcontrollers

Our Arm®-based secure microcontrollers (Figure 6) were designed to be used either as main processors or coprocessors for POS or mobile POS systems, pin pads or encrypted pin pads. While these products offer a wide variety of tools, libraries and operating systems, they also provide advanced security features compliant with the latest standards. This unique combination accelerates time to market and leads to first-pass certification success. Table 6 lists DeepCover secure microcontrollers that support financial transaction applications.

Figure 6. MAX32560 Evaluation Kit

SECURE MICROCONTROLLERS FOR MAGNETIC HEADS

The PIN Transaction Security (PCI-PTS) standard demands increasing levels of cardholder data protection, requiring magnetic card data to be highly protected in financial terminals. For this reason, we have designed microcontrollers (Figure 7) that can read and decode 3 tracks of magnetic stripe data and encrypt them before they are transmitted to the application processor, saving the implementation of costly physical protections. Table 7 and Figure 8 depict secure microcontrollers designed for magnetic head applications.

Figure 7. MAXQ1744 Evaluation Board

	MAX32590	MAX32550	MAX32552	MAX32560	MAX32555
Core	ARM 926EJ-S	Cortex-M3	Cortex-M3	Cortex-M3	Cortex-M3
Flash/SRAM	—/384KB	1MB/256KB	1MB/384KB	1MB/384KB	512KB/96KB
Contactless Interface	—	—	—	—	—
TFT Controller/Mono LCD	Yes/Yes	Yes/Yes	No/Yes	No/Yes	No/Yes
Clock Speed	384MHz	108MHz	108MHz	108MHz	60MHz
AES Encrypted NVSRAM	24KB	8KB	8KB	8KB	8KB
Dynamic Sensor Pairs	6	6	6	6	4
OTP	2KB	4KB	4KB	4KB	4KB
MSR Decoder/Smartcard UART/Smartcard PHY	—/2/—	1/1/1	1/2/1	1/2/2	1/1/2
ADC	3-channel 10-bit	2-channel 10-bit	2-channel 10-bit	2-channel 10-bit	6-channel 10-bit
DAC	—	1-channel 10-bit	1-channel 8-bit	1-channel 8-bit	1-channel 8-bit
USB device/SPI/UART/I²C	1/5/3/1	1/3/2/1	1/3/2/1	1/3/2/1	1/3/3/1
Ethernet MAC	Yes	—	—	—	—
USB Host	1	—	—	—	—
External Memories	NAND/NOR Flash Encrypted LPDDR	—	Quad SPI with XiP	Quad SPI with XiP	—
Timers	3	6	6	6	8
GPIO	160	70	69	69	70
Package	BGA324	BGA121	BGA121	BGA144	BGA121

Table 6. DeepCover Secure Microcontrollers for Financial Transaction Applications

	Core/Frequency	Memories	Interface	Crypto	Others
MAXQ1741	MAXQ20 at 12MHz	16kB Flash 1kB SRAM	1 UART 2 SPI 1 I²C	AES	—
MAXQ1743 MAXQ1744	Turnkey embedded firmware provided by Maxim		1 I²C 1 SPI	AES, 3DES	— Ultra-low power: 450µA during card reading

Table 7. DeepCover Secure Microcontrollers for Magnetic Head Applications

SECURE MICROCONTROLLER TOOL SETS

Our secure microcontroller development boards embed a comprehensive set of interfaces. They feature the most common payment-dedicated interfaces such as smartcard connectors, magnetic stripe heads, keyboards and displays.

Our Arm-based secure microcontroller development tools are based on popular open-source IDE, compilers, and debuggers. By leveraging the Arm core they reduce development times and accelerate time to market.

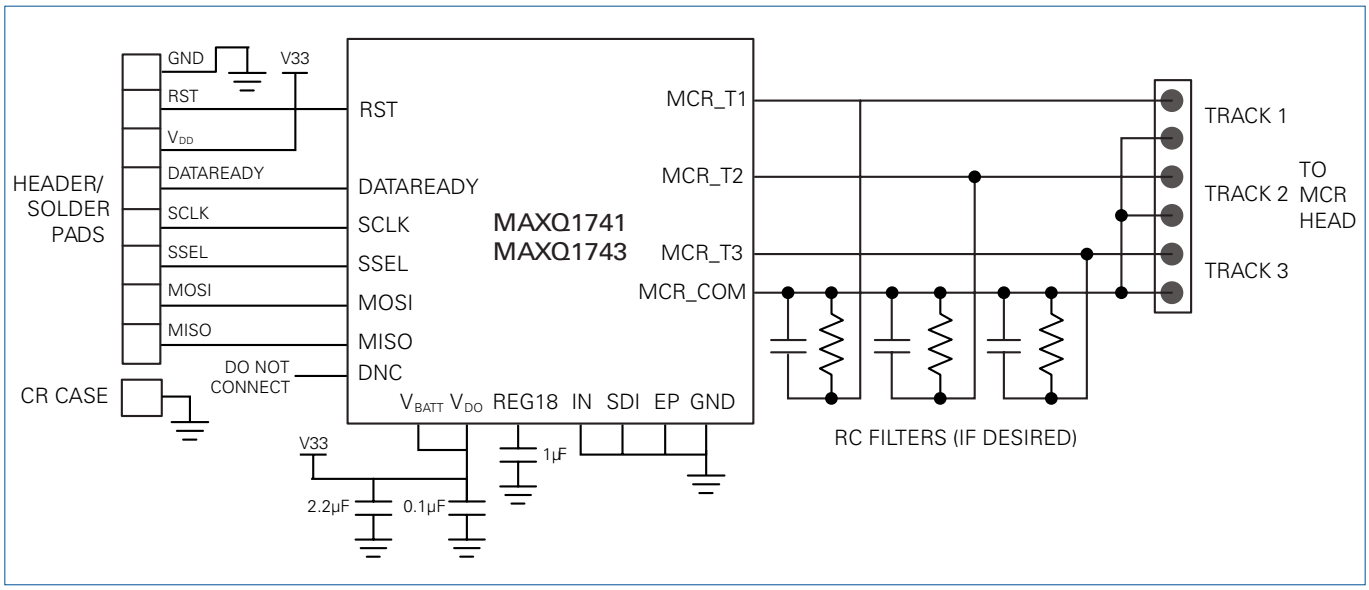


Figure 8. MAXQ1741/MAXQ1743

DeepCover - DeepCover is a registered trademark of Maxim Integrated Products, Inc.
1-Wire - 1-Wire is a registered trademark of Maxim Integrated Products, Inc.

MICROCHIP – SECURE PRODUCTS

World-class embedded security solutions ensures trust for every system design

Trust is what security is really all about today. Microchip security products make "trust" easy to embed in any system. Flexibility, advanced features, innovative cost effective architectures, and ultra-secure hardware defense mechanisms make Microchip hardware-based security devices an ideal way to add trust, by design.

- Microchip CryptoAuthentication™ – Offers product designers an extremely cost-effective, easy to design, tiny, and ultra-secure hardware authentication capability
- Trusted Platform Module – The Microchip Trusted Platform Module (TPM) provides strong hardware-based public key (RSA) security on a single device for personal and tablet computers as well as embedded processor based systems

CRYPTOAUTHENTICATION FAMILY

A Crypto Element Device Family with Ultra-secure Hardware-based Key Storage

CryptoAuthentication Devices Keep it Real

Microchip CryptoAuthentication crypto element devices with hardware-based key storage ensure that a product, consumables it uses, firmware it runs, accessories that support it, and the network nodes it connects to are not cloned, counterfeited, or tampered with. Keeping products real helps maintain an OEM revenue flow by ensuring that only legitimate products can work in the host system and not used beyond their expiration.

Microchip offers the industry's widest selection of authentication devices featuring hardware-based key storage and cryptographic countermeasures that can fight off even the most aggressive attacks. Because attackers cannot see secret keys that are stored in protected hardware, they cannot attack.

CryptoAuthentication Devices Make It Easy

CryptoAuthentication devices support modern cryptographic standards. They work with any MCU, are extremely cost-effective, require only a single GPIO, and use very little power. Additionally, they operate over a wide voltage range and come in exceptionally small packages. Advanced protocols like ECDSA sign-verify (asymmetric authentication) and ECDH (key agreement in encryption/decryption settings) are built-in which makes adding sophisticated security easy.

CryptoAuthentication Devices Make it "Real Easy"

Cryptography is mathematically complex and highly detailed with many standards, algorithms, processes, definitions, and methodologies. Since Microchip does the hard cryptographic engineering there is no need to be a crypto expert. As a result, it is real easy to add robust security to digital systems.

CryptoAuthentication Use

- Secure Download and Boot – Authenticate and protect code in-transit
- Ecosystem Control – Ensure only authorized OEM and licensed nodes
- Anti-cloning – Prevent identical BOM and stolen codes
- Message Security – Authentication, data integrity, and confidentiality of network / IoT nodes

ECC-BASED CRYPTO ELEMENTS

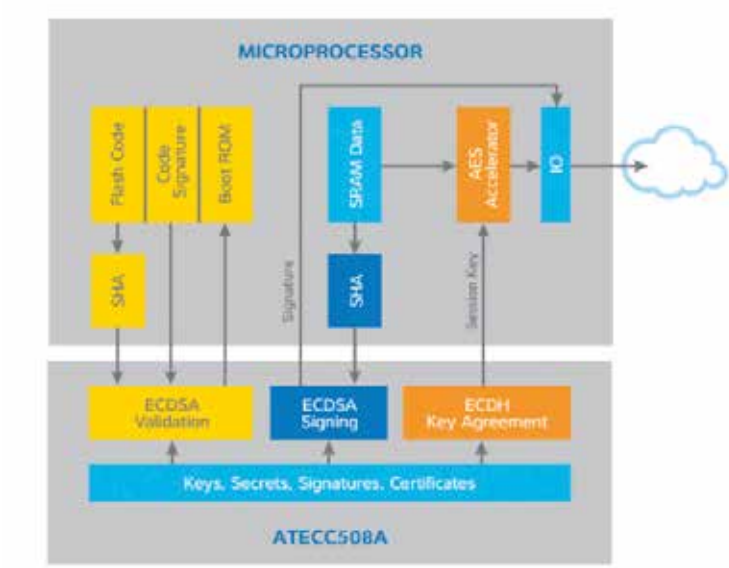
ECC-based Crypto Elements are ideal for emerging Internet of Things (IoT) and traditional applications because ECDH key agreement enables confidentiality when users employ it with microprocessors running encryption/decryption algorithms, such as AES (Advanced Encryption Standard). Built-in ECDH eases key agreement and increases security between network nodes and host/ client applications. This Crypto Elements addresses market segments such as home automation, industrial networking, accessory and consumable authentication, medical, mobile, and others.

- Easy way to run ECDSA and ECDH Key Agreement
- ECDH key agreement makes encryption/decryption easy
- Ideal for IoT node security
- Authentication without the need for secure storage in the host
- No requirement for high-speed computing in client devices

ATECC508A

The Microchip ATECC508A integrates ECDH (Elliptic Curve Diffie–Hellman) security protocol—an ultra-secure method to provide key agreement for encryption/decryption, along with ECDSA (Elliptic Curve Digital Signature Algorithm) sign-verify authentication—for the Internet of Things (IoT) market including home automation, industrial networking, accessory and consumable authentication, medical, mobile and more. With ECDH and ECDSA being built right in, this device is ideal for the rapidly growing IoT market by easily supplying the full range of security such as confidentiality, data integrity, and authentication to systems with MCU or MPUs running encryption/decryption algorithms (i.e. AES). Similar to all Microchip CryptoAuthentication products, the new ATECC508A employs ultra-secure hardware-based cryptographic key storage and cryptographic countermeasures which are more secure than software-based key storage.

The device is compatible with any microprocessor (MPU) or microcontroller (MCU) including Microchip | SMART and Microchip AVR MCUs or MPUs. As with all CryptoAuthentication devices, the ATECCC508A delivers extremely low-power consumption, requires only a single GPIO over a wide voltage range, and has a tiny form factor making it ideal for a variety of applications that require longer battery life and flexible form factors.



Key Features

- Crypto Element Device with Secure Hardware-based Key Storage
- Performs High-Speed Public Key Algorithms (PKI): ECDSA and ECDH
- NIST Standard P256 Elliptic Curve Support
- SHA-256 Hash Algorithm with HMAC Option
- Host and Client Operations
- Two High-endurance Monotonic Counters
- Guaranteed Unique 72-bit Serial Number
- Internal High-quality FIPS Random Number Generator (RNG)
- Storage for up to 16 Keys
- Multiple Options for Consumption Logging and One Time Write Information
- Intrusion Latch for External Tamper Switch or Power-on Chip Enablement
- 2.0...5.5 V Supply Voltage Range, 1.8...5.5 V IO Levels
- <150 nA Sleep Current
- 8-pad UDFN, 8-lead SOIC, and 3-lead CONTACT Packages
- Single-wire; I²C
- Temp. Range (deg C): -40...85

Microchip Ordering Code	Package	Interface Configuration
ATECC508A-SSHCZ-T	8-lead SOIC, Tape and Reel(2)	Single-Wire
ATECC508A-SSHCZ-B	8-lead SOIC, Bulk in Tubes(1)	Single-Wire
ATECC508A-SSHDA-T	8-lead SOIC, Tape and Reel(2)	I²C
ATECC508A-SSHDA-B	8-lead SOIC, Bulk in Tubes(1)	I²C
ATECC508A-MAHCZ-T	8-pad UDFN, Tape and Reel(2)	Single-Wire
ATECC508A-MAHDA-T	8-pad UDFN, Tape and Reel(2)	I²C
ATECC508A-MAHCZ-S	8-pad UDFN, Tape and Reel(3)	Single-Wire
ATECC508A-MAHDA-S	8-pad UDFN, Tape and Reel(3)	I²C
ATECC508A-RBHCZ-T(4)	3-lead CONTACT, Tape and Reel(2)	Single-Wire

B = Bulk
T = Tape and Reel
SOIC = 4,000 units per reel
UDFN = 15,000 units per reel
RBH = 5,000 units per reel
S = Tape and Reel
UDFN = 3,000 units per reel

SHA BASED: FAST, SECURE, AND COST EFFECTIVE SYMMETRIC AUTHENTICATION

The Microchip SHA-based CryptoAuthentication crypto element devices have been architected to provide flexible user-configured security to enable a wide range of authentication models. The ATSHA204A is the first device in the SHA device group. The ATECC108A and ATECC508A are supersets of the ATSHA204A and thus upward compatible. As with all CryptoAuthentication devices, the ATSHA204A is easy to design in with no crypto expertise required.

Secure Hash Algorithm (SHA) algorithms are widely used in most cryptographic systems and remain an important component in most modern authentication protocols. These devices support the SHA-256 standard. The ATSHA204A is the most cost-effective solution in the Microchip CryptoAuthentication portfolio. It integrates the SHA-256 hash algorithm with a 4.5 Kb EEPROM and provides robust hardware authentication using secure key/data storage. The tiny packaging and a single-wire interface make the device ideal for handheld electronic systems and any space-constrained embedded system.

CryptoAuthentication devices in the SHA mode include client and host security capabilities that offload key storage and algorithm execution from the microcontroller, significantly reducing system cost and complexity. SHA based symmetric authentication is fast relative to asymmetric approaches, making the ATSHA204A a good choice with speed (and/or cost) are important considerations. CryptoAuthentication devices have full metal shields over all of the internal circuitry, so that if an attacker cuts or short circuits any trace in the shield, the product stops functioning. Additional security features include internal clocks and voltage generation, encrypted memories, tamper detection, and fully secure production test methodologies. With the ATSHA204A implementing host-side security to provide a full system solution is now easier than ever.

Benefits

- Cost-effective Symmetric Authentication Solution
- Fast Authentication
- Easy Key Management

ATSHA204A

The Microchip® ATSHA204A is a full turnkey security device. It includes a 4.5 Kb EEPROM divided into 16 slots. This array can be used for storage of keys, miscellaneous read/write, read-only, password or secret data, and consumption tracking. Access to the various sections of memory can be restricted in a variety of ways and then the configuration locked to prevent changes.

Access to the chip is through a standard I²C interface at speeds up to 1Mb/sec. The chip also supports a single-wire interface that can reduce the number of GPIOs required on the system processor and/or reduce the number of pins on connectors. It is compatible with most UART or serial I/O controllers. System integration is eased with a wide supply voltage range and an ultra-low sleep current of less than 100 nA.

Key Features

- Crypto Element Device with Secure Hardware-based Key Storage
- SHA-256 Hash Algorithm with HMAC Option
- Host and Client Operations
- Guaranteed Unique 72-bit Serial Number
- Internal High-quality FIPS Random Number Generator (RNG)
- Storage for up to 16 Keys
- Multiple Options for Consumption Logging and One Time Write Information
- 2.0...5.5 V Supply Voltage Range
- <150 nA Sleep Current
- 8-pad UDFN, 8-lead SOIC, and 3-lead CONTACT Packages
- Single-wire; I²C
- Temp. Range (deg C): -40...85

Microchip Ordering Code	Package	Delivery	Type Interface Configuration
ATSHA204A-MAHCZ-T	8-pad UDFN	Tape and Reel	Single-Wire
ATSHA204A-MAHDA-T	8-pad UDFN	Tape and Reel	I²C
ATSHA204A-MAHCZ-S	8-pad UDFN	Tape and Reel	Single-Wire
ATSHA204A-MAHDA-S	8-pad UDFN	Tape and Reel	I²C
ATSHA204A-SSHCZ-T	8-lead SOIC	Tape and Reel	Single-Wire
ATSHA204A-SSHDA-T	8-lead SOIC	Tape and Reel	I²C
ATSHA204A-SSHDA-B	8-lead SOIC	Bulk in Tubes	I²C
ATSHA204A-RBHCZ-T	3-lead Contact	Tape and Reel	Single-Wire

B = Bulk
T = Tape and Reel
SOIC = 4,000 units per reel
UDFN = 15,000 units per reel
RBH = 5,000 units per reel
S = Tape and Reel
UDFN = 3,000 units per reel

AES BASED: AUTHORIZATION, KEY MANAGEMENT, AND MEMORY ENCRYPTION

The first device in the AES family, the ATAES132A, is a high-speed, high-security, 32 K Serial EEPROM that enables authentication and confidential nonvolatile data storage. It is a direct drop-in for industry standard Serial EEPROMS and is an easy way to add security to a system. The ATES132A includes a high-quality hardware Random Number Generator (RNG) paired with a Federal Information Processing Standards (FIPS) Deterministic Random Bit Generator (DRBG) to prevent replay attacks.

Data encryption and decryption can be easily performed for both internally stored data or for small external data packets (depending upon the configuration). Data encrypted by one AES device can be decrypted by another, and vice versa. The secure Serial EEPROM architecture of the ATAES132A and packages compatible with standard SPI and I²C EEPROM footprints allow direct insertion into many existing Serial EEPROM applications.

Benefits

- Drop-in upgrade for existing sockets for high security applications
- Single protocol authentication and encryption
- Securely tracks events which is useful in evaluating warranty claims

ATAES132A

The ATAES132A crypto element with hardware-based key storage is a very fast high-security serial 32K EEPROM device that enables authentication and confidential nonvolatile data storage. It is a direct drop-in for industry standard Serial EEPROMS, and supports the Advanced Encryption Standard (AES) cryptography standard.

The AES-128 cryptographic engine operates in AES-CCM mode to provide authentication, stored data encryption/decryption, and Message Authentication Codes (MACs). Data encryption/decryption can be performed for internally stored data or for small external data packets depending upon the configuration. Data encrypted by one ATAES132A device can be decrypted by another, and vice versa. Extended security functions are accessed by sending command packets to the ATAES132 using standard write instructions and reading responses using standard read instructions. The device incorporates multiple physical security mechanisms to prevent release of the internally stored secrets.

The device's secure Serial EEPROM architecture and packages compatible with standard SPI and I²C EEPROM footprints allow insertion into many existing Serial EEPROM applications. Like all Microchip CryptoAuthentication devices the ATAES132A stores keys and other secret data in hardware protected by a range of physical and cryptographic countermeasures, making it far more secure than software or unprotected hardware storage mechanisms.

Benefits

- Easily Add Security by Replacing Existing Serial EEPROM
- Authenticate Consumables, Components, and Network Access
- Protect Sensitive Firmware
- Securely Store Sensitive Data and Enable Paid-for Features
- Prevent Contract Manufacturers from Overbuilding
- Manage Warranty Claims
- Securely Store Identity Data (i.e. Fingerprints and Pictures)

Key Features

- 32 Kb Standard Serial EEPROM User Memory (16 User Zones of 2 Kb)
- AES Algorithm with 128-bit Keys
- AES-CCM for Authentication
- Secure Storage for 16 and 128 bit Keys
- Encrypted User Memory Read and Write
- FIPS Random Number Generator (RNG)
- 16 High-Endurance Monotonic EEPROM Counters
- Authentication Prior to Zone Access
- Read/Write, Encrypted, or Read-only User Zone Options
- SPI and I²C Interface Options
- 2.5...5.5 V Supply, <250 nA Sleep

Serial EEPROM Compatible Pinout (SOIC, SOP, or UDFN)

Microchip Ordering Code	Package	Delivery	Interface Configuration
ATAES132A-SHEQ	SOIC	Bulk	SPI
ATAES132A-SHER	SOIC	Bulk	I²C
ATAES132A-SHEQ-T	SOIC	Tape and Reel	SPI
ATAES132A-SHER-T	SOIC	Tape and Reel	I²C
ATAES132A-MAHEQ-T	UDFN	Tape and Reel	SPI
ATAES132A-MAHER-T	UDFN	Tape and Reel	I²C

T = Tape and Reel
SOIC = 4,000 units per reel
UDFN = 15,000 units per reel
RBH = 5,000 units per reel

CryptoAuthentication and TPM Kits

Ordering Code	Supported Devices	Description
Evaluation Kits		
ATCRYPTOAUTH-XPRO	ATECC508A ATSHA204A ATAES132A	For Microchip MCU Eval Kits
AT88CK590	ATECC508A ATSHA204A ATAES132A	Standalone evaluation kit via USB
Development Kits		
AT88CK101SK-MAH-XPRO	ATECC508A ATSHA204A ATAES132A	UDFN
AT88CK101SK-SSH-XPRO	ATECC508A ATSHA204A ATAES132A	SOIC-8
AT88CK101SK-RBH	ATECC508A ATSHA204A	3-lead CONTACT
Personalization Kit		
AT88CK9000-xx	ATSHA204A ATAES132A	Standalone personalization kit. For different packages available
Provisioning Kits		
AT88CKECCROOT	ATECC508A	Root Module Kit
AT88CKECCSIGNER	ATECC508A	Signer Module Kit
AT88CKECCPROVISION	ATECC508A	Root + Signer Module Kit
TPM Development Kits		
AT97SC3205P-SDK2	AT97SC3205	SPI TPM Kit
AT97SC3205T-SDK2	AT97SC3205T	I²C TPM Kit

Standalone personalization kit. For different packages availableProvisioning

PROVISIONING

Provisioning Kits

- Root Module Kit (AT88CKECCROOT) – This module is used to securely create and store a root key in protected hardware. Each kit contains three USB Root Modules that can be used to create the primary root key and two backups
- Signer Module Kit (AT88CKECCSIGNER) – This module is used to create signing keys using the root module. It can be used in the customer's production platform to sign and load the crypto element's device certificates. Each kit contains three Signer Modules to provide a primary Signer Module and two secure backups
- Provisioning Starter Kit (AT88CKECCPROVISION) – This module is a provisioning starter kit containing three USB Root Modules and three USB Signer Modules. It takes the place of one AT88CKECCROOT and one AT88CKECCSIGNER Module Kits

All the steps are simple and spelled out in detail making it easy to seamlessly providing devices at production. Microchip provides the embedded system firmware and PC software necessary to implement the steps.

Root Module Kit

SOFTWARE AND LIBRARY SUPPORT

CryptoAuthLib

CryptoAuthLib is a software support library for the Microchip ATSHA204A, ATECC108A and ATECC508A CryptoAuthentication devices written in C. It is a portable, extensible, powerful, and easy-to-use library for working with the ATSHA and ATECC family devices. Example code and application notes for various use cases demonstrate how to use CryptoAuthLib to develop powerful crypto-authentication applications.

Key Features

- Ease of Use – A Basic API serves the needs of most applications
- Powerful – For sophisticated applications and developers, the full power of the device is available through a core API
- Portable – Runs on small processors and desktop systems alike
- Extensible – Is architected to easily support new MCU platforms or protocols
- X.509 Certificate Support – Has an API for storing, retrieving, and manipulating X.509 certificates
- TLS Integration APIs

http://www.atmel.com/tools/CryptoAuthLib.aspx

MICROCHIP CRYPTO EVALUATION STUDIO (ACES)

The ACES package is a suite of software tools to configure and demonstrate the Microchip CryptoAuthentication Family of devices using various evaluation kits.

ACES was designed to minimize the learning curve for using the Microchip CryptoAuthentication Family of devices in your application. The package includes the ACES Configuration Environment (ACES CE) and a comprehensive help system.

The ACES package also includes support for the AT88CK9000 programmer board.

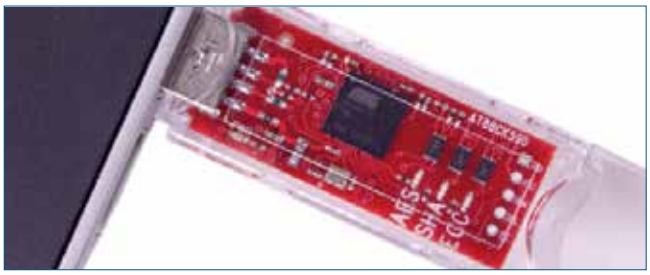
http://www.atmel.com/tools/ATMELCRYPTOEVALUATIONSTUDIO_ACES.aspx

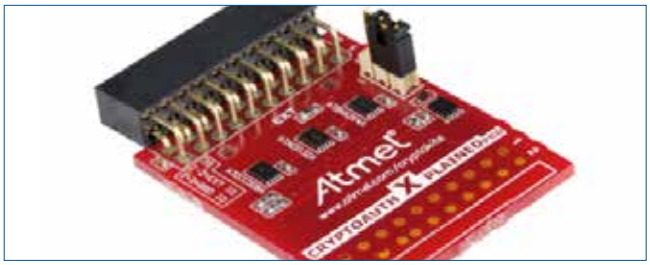
MICROCHIP HARDWARE-TLS PLATFORM

The Microchip Hardware-TLS platform provides an interface between software TLS packages and the ATECC508A cryptographic co-processor. wolfSSL and OpenSSL implementations can now utilize hardware-based secure storage for private keys and authentication data and also allow resource-constrained IoT nodes to implement full elliptic curve authentication and Diffie-Hellman key agreement and session key derivation. With Microchip HW-TLS, TLS communications links can have hardened security even out to the smallest IoT edge node.

Key Features

- Elliptic Curve Cryptography (ECC) hardware acceleration for resource-constrained IoT nodes – ECDSA authentication for node identification. ECDH Key Agreement for data encryption. Minimizes code and processing in the main device controller. Rapid execution of ECC processes even on M0-class processors
- Tamper-resistant secure storage of private keys, certificates and other sensitive data
- Internal private key generation – Private keys are never accessible external to the device
- Microchip Certified-ID Support – DIY secure certificate signing and provisioning
- Low power consumption for battery operated IoT products
- Flexible application for authentication on multiple network layers: Application, Transport, Link





TPM - TRUSTED PLATFORM MODULE

Complete Security for PCs and Embedded Systems

The Microchip FIPS 140-2 Certified Trusted Platform Module (TPM) provides strong hardware-based public key (RSA) security for both personal computers and embedded processors on a single chip. It is a complete turnkey system that integrates industry-leading Microchip AVR® microcontroller architecture, Microchip EEPROM technology, and Microchip security technology. Implementing version 1.2 of the Trusted Computing Group (TCG) specification for TPMs, the chip supports secure boot via platform integrity measurements, intellectual property protection, authentication, and secure communications. The AT97SC* series is offered in three different interfaces: SPI, LPC, and I²C. All revisions are supported in both Commercial and Industrial Grades. The Trusted Platform Module Embedded Development Kit received a 2008 Readers Tech Choice Award from eg3, an independent news source devoted to electronic design.

Key Features

- Turnkey solution – The TPM includes integrated, protected nonvolatile storage for cryptographic keys, secrets, and authorization information
- Full TCG compliance – According to TCG, applications based on the trusted computing infrastructure exhibit superior security governance and risk management
- Hardware security – The TPM includes a high-quality hardware random number generator, active shielding, and a variety of tamper-detection and response circuits
- High performance – The TPM's cryptographic accelerator can compute a 2048-bit RSA signature in 200 ms
- Energy savings – The TPM supports SIRQ for interrupts and CLKRUN to permit clock stopping for power savings in mobile computers
- Software support – BIOS and hardware drivers are available for both Windows and Linux; third-party system and application software is also available
- Three interfaces – There is a 45 MHz SPI, 33 MHz LPC interface for PC integration and a 2-wire interface available
- Certifications - FIPS 140-2 & CC EAL 4+

TCG VERSION 1.2

The Microchip Trusted Platform Module is a fully integrated security module designed to be integrated into computer systems and other embedded systems. The TPM conforms to TCG v1.2 specifications and includes a cryptographic accelerator capable of computing a 2048-bit RSA signature (key generation, signing, and verification) in 200ms. Performance of the SHA-1 accelerator is 20µs per 64-byte block. The AT97SC3204T version complies with the TWI I²C 2-wire protocol.

Key Parameters

Parameter	Value
Operating Voltage (Vcc):	3.3
Interface Type:	AT97SC3205: SPI / AT97SC3205: I²C
Max. Operating Freq. (MHz):	45 MHz SPI / 0.4 MHz I²C
Algorithm Type:	RSA / SHA-1 / SHA-2 (Sign/Verify Sign)
Key Size:	UP TO 2048
Temp. Range (deg C):	-40...85 or 0...70

Ordering Codes see TPM Part Number Selection Guide

http://www.atmel.com/Images/Atmel-8965-TPM-Part-No-Selection-Guide-ApplicationNote.pdf

The EBV IoT

Smart, Secure, Connected – Everywhere

For years, EBV has been supporting customers' end products across EMEA which are called today – the Internet of Things (IoT). The EBV sales teams together with our technology and market segments enable customers to develop their IoT programs and add new functionalities such as security and wireless. In addition, the EBVchips program can offer new innovative solutions for white spots that have yet to be covered. For all information around IoT, please contact your EBV partner and visit us at ebv.com/iot.

Distribution is today. Tomorrow is EBV!

www.ebv.com

EBVElektronik
I An Avnet Company I

NXP - SECURE CONNECTIONS FOR A SMARTER WORLD

Security is a race in the internet of things (IoT) and staying ahead is a major challenge. We know security is an increasingly critical part of the connected solutions you use and design. Identity theft is at an all-time high. Data privacy concerns are arising on pace with the growth of connected devices. And newly-connected command and control systems present attractive targets for hackers.

We're here to help you. NXP is the global leader in security solutions for personal identification, contactless payment, authentication, data transport and application processing. Our secure element – a specific integrated circuit for handling and storing secured data – features non-volatile memory, a security CPU and crypto coprocessor, and additional security measures, to offer you the ultimate protection against tampering and attack.

Secure designs – from the end node to the network to the cloud

We secure more types of end equipment than any other company in the world. From the edge of the network to the gateway to the cloud, our broad portfolio of secure microcontrollers, high-performance multicore communications processors, applications processors, middleware and software ensures the devices you design and use are protected. Our decades-long investment and expertise in security make us the partner of choice for determining the security requirements of your next project.

How NXP helps you with your security and privacy needs

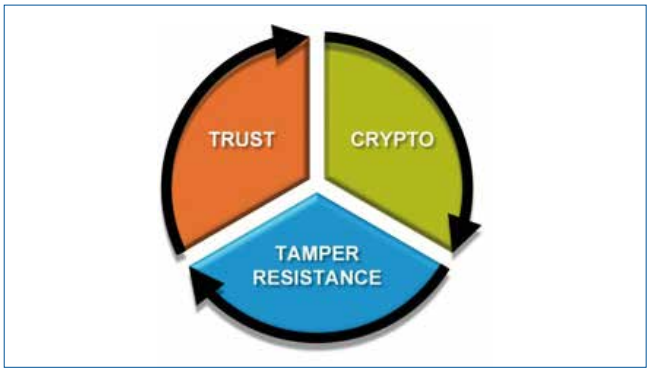
You don't have to sacrifice performance to add security, either. Our QorIQ processors integrate crypto acceleration that allows you to develop secure connections without a performance penalty for the world's new virtualized networks – ranging from the wireless infrastructure to the smart grid to the home.

And as the leader in security ICs, we allow you to choose from a complete range of ICs for smart cards, tags, labels and readers featuring many coprocessor, security, memory and interface options. We address all your needs, from low-cost smart label ICs for high-volume supply chain management applications through to our next generation 32-bit-smart-computing platform for powerful multi-application smart cards.

NXP'S PILLARS OF SECURITY

Trust - The assurance that only access from a reliable source will occur

- Code I/P Protection
  - Internal Memory Protection
  - External Memory Protection
- Debug Port Protection
- Authentication
  - Software Updates
  - Device Verification
- Secure Boot



Cryptography - The science of protecting data through encoding and decoding

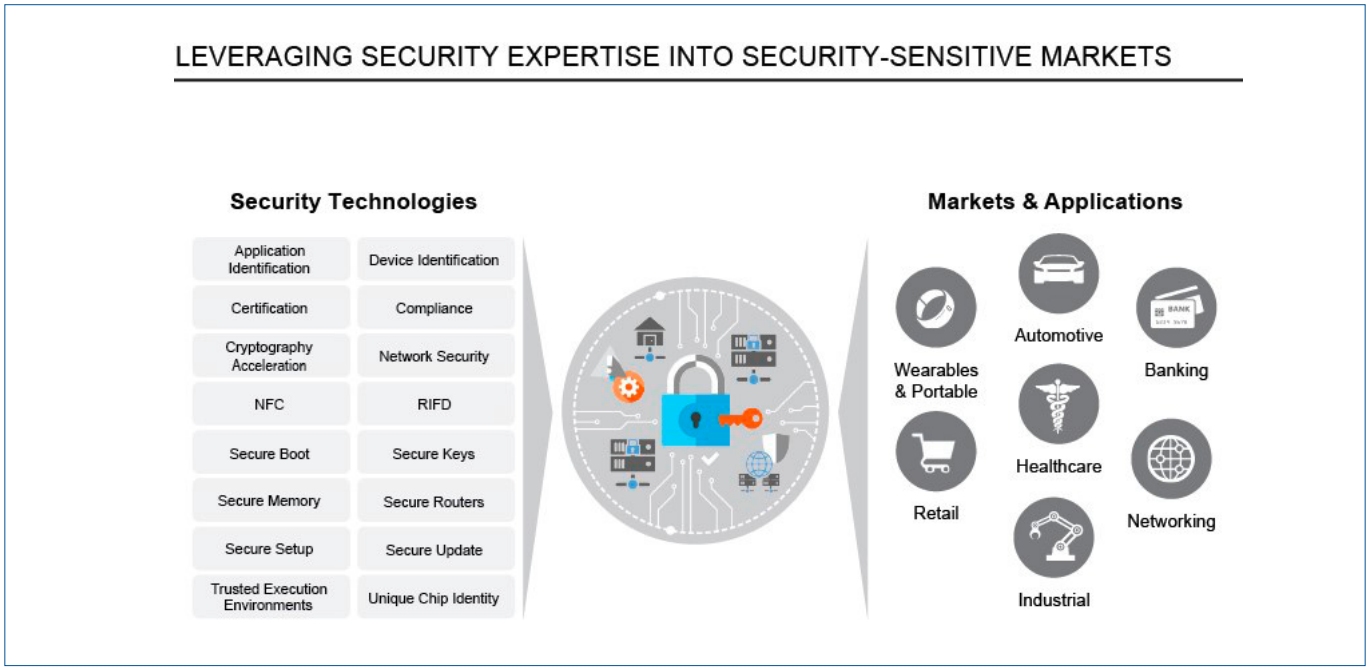
- Symmetric Encryption
  - DES/DES3, AES
- Asymmetric Encryption
  - RSA, ECC
- Hashing
  - CRC, MD5, SHA
- True Random Number Generation
- Security Protocols
  - SSL, HomeKit, Thread

Tamper Resistance - Proactive monitoring of physical and environmental system attacks

- Tamper Detection
  - Physical
    - Enclosure Intrusion
    - Drilling and Probing
  - Environmental
    - Voltage
    - Temperature
    - Frequency
- Secure Storage

NXP PRODUCTS FOR SECURITY – MODULES SUPPORTING THE PILLARS OF SECURITY

Hardware support for		Secure Elements	Kinetis	LPC	i.MX	QorIQ	C29x	Auto
Trust	Code I/P Protection	√	OTFAD	√	BEE	√	CCSR	CSE
	Debug Port Protection		√	√	√	√	√	√
	Authentication	√	Unique ID	Unique ID	Unique ID	Unique ID	Unique ID	CSE
	Secure Boot	√	√	√	HAB	√	√	√
Cryptography	Symmetric Encryption	√	mmCAU LTC	√	CAAM BEE	SEC	SEC	CSE HSM
	Asymmetric Encryption	√	LTC		CAAM	SEC	SEC	
	Hashing		LTC		CAAM	SEC PME	SEC	
	TRNG	√	√	√	√	SEC	SEC	CSE
	Security Protocols	√	LTC		CAAM	SEC PME	SEC	HSM
Tamper	Physical	√	DryIce		SNVS	Secure Monitor	√	√
	Environmental	√	DryIce		SNVS	Secure Monitor	√	√
	Secure Storage	√	DryIce	√	SNVS	Secure Monitor	√	√



SECURE ELEMENTS

Value proposition

Best in class anti-counterfeiting/anti-hacking technology

- Strongest levels of market-proven and certified security
- End to end security includes common criteria certified design environment, production facilities and secure personalization/key insertion per chip

Lowest power, smallest footprint, high performance

- Solutions as small as 1mm²
- Power consumption as low as 500 uA full-on, 50 uA typ, < 1 uA deep sleep
- Full certificate validation plus ECC challenge-response in ~50 ms

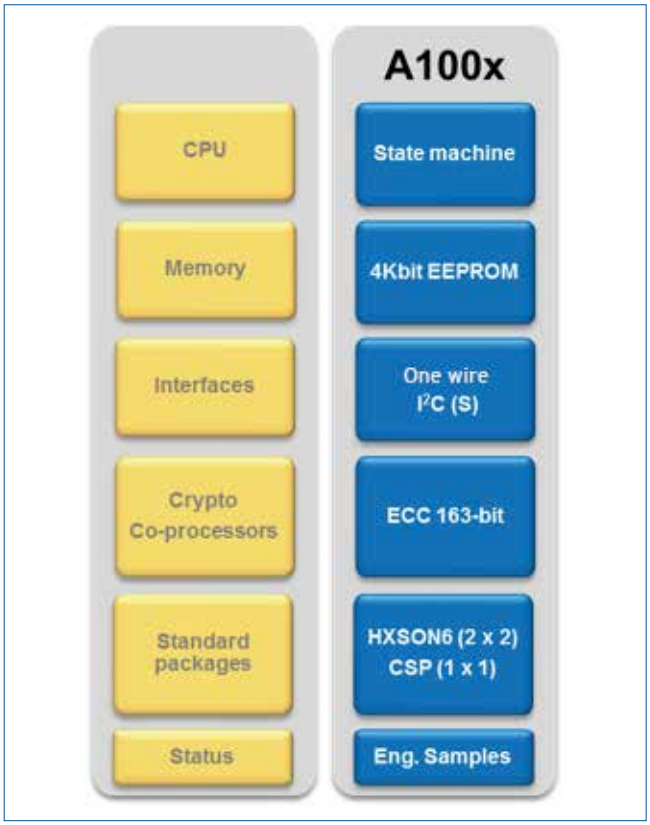
Ease of system integration

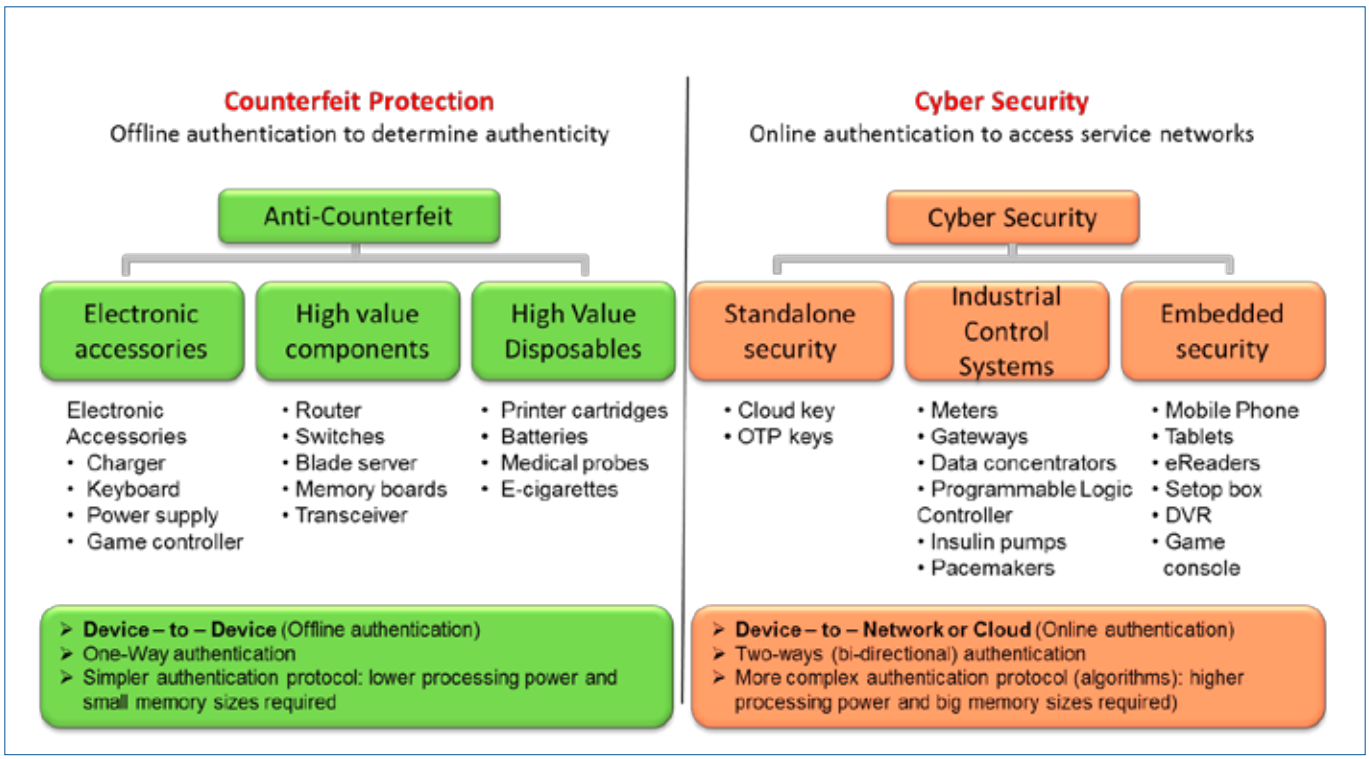
- Bus-powered one wire interface
- 8kV IEC61000-4-2 contact ESD protection
- Demo board and host demo software available
- Applications support team includes security experts

Portfolio Overview

Options for flexibility vs. cost & size:

- CPU: from simple state machine to secure micros with range of supported clock rates
- Memory: EEPROM and/or RAM in various sizes
- Interfaces: I²C slave only, I²C/SPI master and slave
- Crypto-Coprocessor: ECC only; PKI (RSA, ECC), 3-DES, AES
- Packages: HVSON, HVQFN, CSP





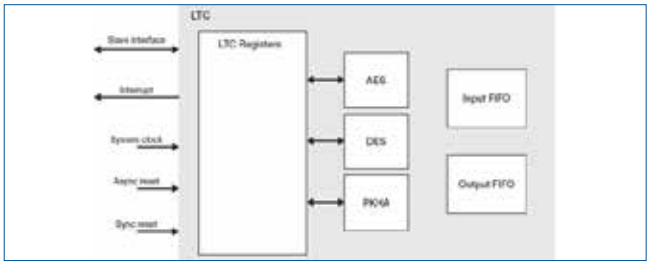
KINETIS MICROCONTROLLER WITH ADVANCED SECURITY

NXP provides the broadest portfolio of energy efficient, 32-bit microcontroller (MCU) products for low-power applications enabling the Internet of Things. The Kinetis MCU portfolio includes devices based on the ARM®Cortex®-M0+, Cortex-M4 and Cortex-M7 core. The scalability offered by the Kinetis MCU portfolio enables a range of low-power MCUs from the high performance Kinetis K series to the ultra-low power Kinetis L series, providing industry-leading energy efficiency. The Kinetis MCU portfolio is supported by the most comprehensive set of development tools and software.

Low-power Trusted Crypto Engine (LTC)

LTC features

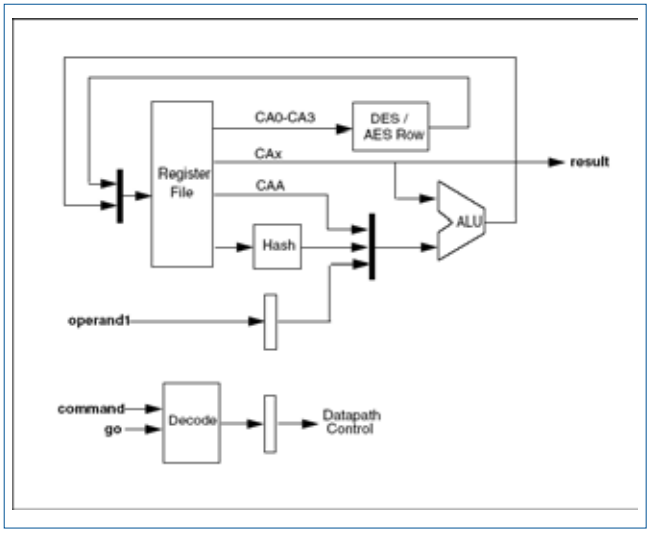
- AES128 and AES256 support
- Single- and triple-DES
- Public key hardware accelerator capable
- The LTC driver is provided in the Kinetis SDK
  - Support for symmetric and asymmetric modes
  - Public key cryptography support - RSA, ECDSA, ECDH



Memory-Mapped Cryptographic Acceleration Unit (mmCAU)

CAU features

- Data Encryption Standard (DES)
  - DES, 3DES
  - Two key (K1, K2, K1) or three key (K1, K2, K3)
  - ECB and CBC modes
- Advanced Encryption Standard (AES)
  - Key lengths of 128, 192, and 256 bits
  - ECB, CBC, CTR, CCM modes
- Message Digest (MD)
  - SHA-1 160-bit digest
  - SHA-2 256-bit digest
  - MD5 128-bit digest
- Hardware Random Number Generator (RNG)
  - FIPS compliant (with appropriate software)

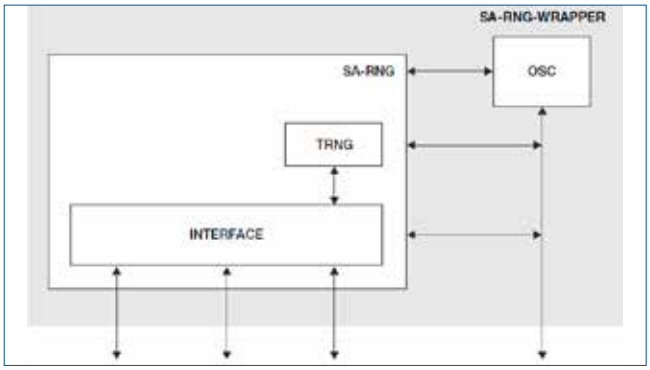


Standalone True Random Number Generator (SA-TRNG)

TRNG is based on collecting bits from a random noise source. This random noise source is a ring oscillator that is sensitive to random noise (temperature variations, voltage variations, cross-talk and other random noise) within the device in which the TRNG is used.

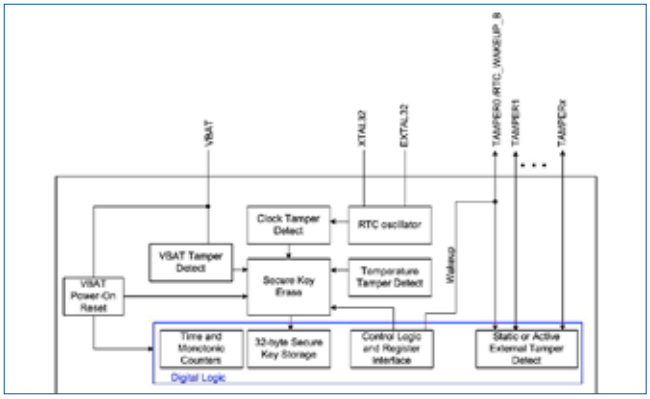
The SA-TRNG is hardware accelerator module that generates a 512-bit entropy as needed by an entropy consuming module or by other post processing functions.

For hardware or software based implementation of a DRBG defined by SP800-90.



DryICE – Tamper Detection Module

- 256-bit Secure Key Register
  - Erased on tamper
  - RAM – powered from VBAT
  - DRY_SKR[0:7]
- Tamper Detection
  - Hardware GPIO
  - Voltage & temperature
  - Clock frequency
- Secure Real-time Clock
  - Timestamps tamper events
  - bIndependant VBAT, power-on reset and 32kHz osc



LPC MICROCONTROLLER WITH ADVANCED SECURITY

LPC microcontrollers based on the ARM Cortex-M cores offer the highest clock speeds, highest levels of system integration, exceptional power efficiency, as well as reduced system design cost and complexity. Some utilize a Cortex-M4 processor with a built-in floating-point unit. The LPC portfolio includes three series based on the Cortex-M4 cores, including single-core and multi-core architectures that allow efficient application partitioning and/or scalable power performance:

LPC Security features (LPCxxSxx devices only)

- AES-128 encryption engine
- True random number generator (TRNG)
- OTP key storage
- Code read protection (CRP)

I.MX APPLICATION PROCESSORS

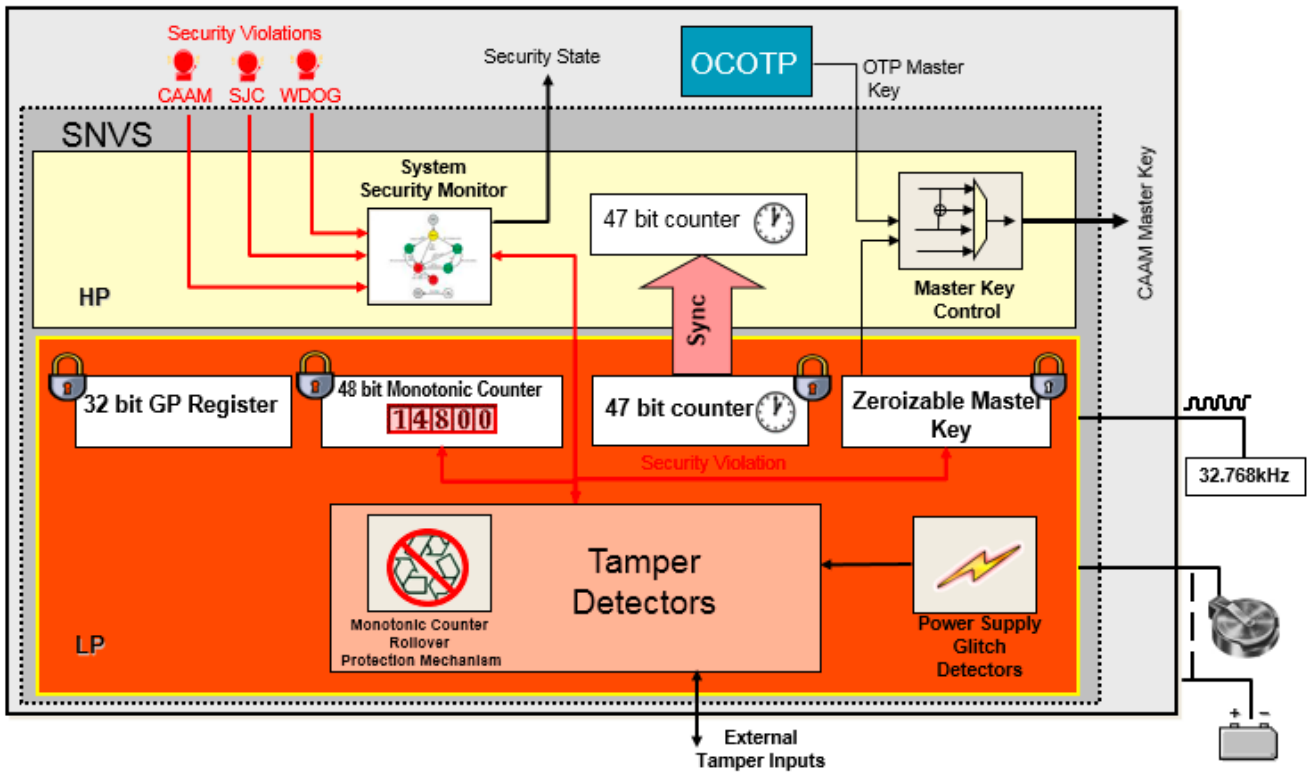
The i.MX series of applications processors is a feature and performance scalable multicore platform that includes single-, dual- and quad-core families based on the ARM®Cortex® architecture, including Cortex-A9, combined Cortex-A9 + Cortex-M4 and Cortex-A7 based solutions up to 1.2 GHz.

Targeting consumer, industrial and automotive applications, the i.MX 6 series combines broad levels of integration and power-efficient processing capabilities all the way up to bleeding edge 3D and 2D graphics, as well as high-definition video, to provide a new level of multimedia performance for an unbounded next-generation user experience. The i.MX 6 series is supported by our proprietary companion power management integrated circuits (PMICs).

High Assurance Boot (HAB)

Feature	HAB4	Comments
Image authentication	Yes	Yes
Super Root Key	Multiple, revocable	Fused Hash
Public key type	RSA-4096 (max)	128-bit security achieved with RSA-3072
Certificate format	X.509v3	Tools support
CMS (PKCS#1)	CMS (PKCS#1)	Tools support
Hash algorithm	SHA-256	NIST recommended
Image Encryption	Yes	
Wrapped key format	CAAM blob	Secret keys stored in secure RAM partition on i.MX6 Dual/Quad
Secret key type	AES-128/192/256	
Decryption algorithm	AES-CCM	Authenticated decryption
Device configuration commands	▸Write value ▸Set/clear bitmask ▸Wait on bitmask	Provides flexible device configuration
Unlock commands	▸Field Return fuse ▸Revocation fuses ▸Secure JTAG ▸CAAM/SNVS	Secure by default

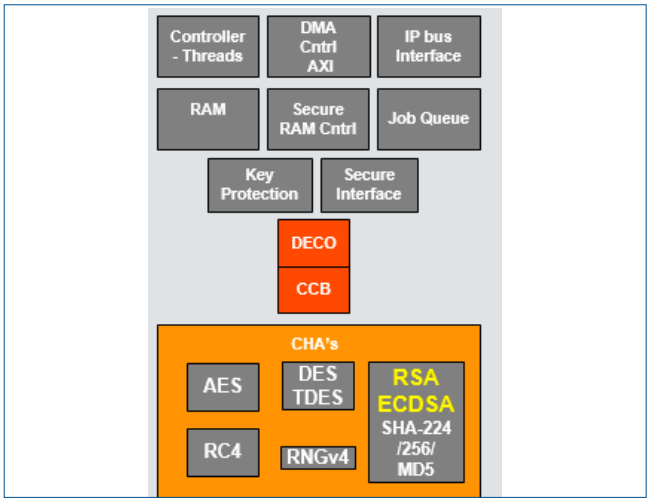
Secure Non-Volatile Storage (SNVS)

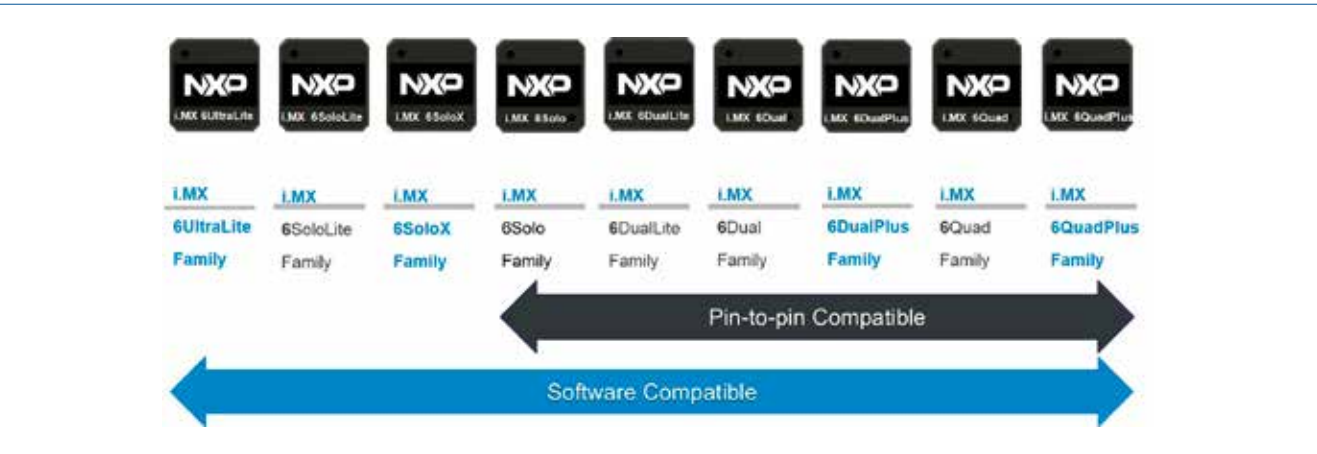


Crypto Acceleration & Assurance Module (CAAM) – Asymmetric Crypto Acceleration

CAAM Features

- Secure Boot
- RNG
- tamper detection
- secure storage
- AES-128, DES 3DES, ARC4, MD5, SHA-1, SHA-224, SHA-256
- 16 KB Secure RAM
- tamper-resistant RTC
- secure debug
- OTP Space
- OTF Encryption/Decryption
- digital rights management (DRM),



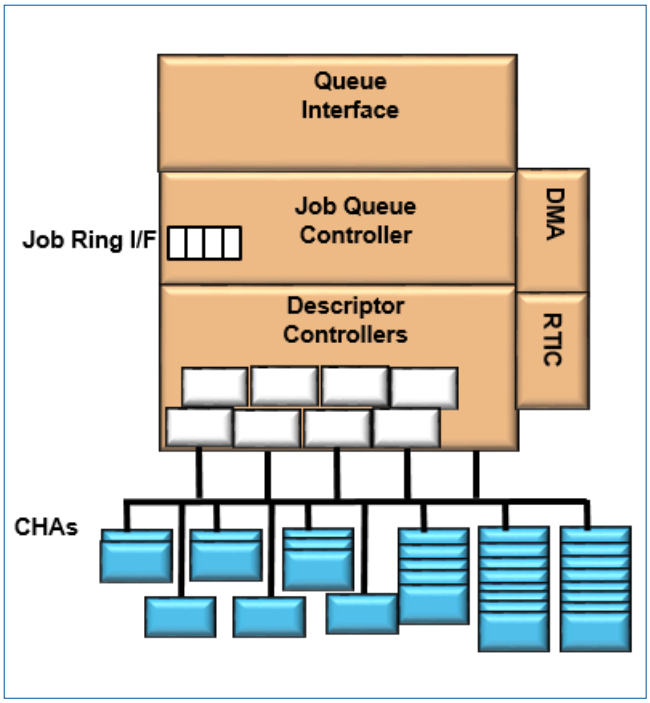


QorIQ PROCESSING PLATFORMS: MULTICORE SoCs

Whether it's for the world's new virtualized networks, the mobile wireless infrastructure, the smart home, the smart grid, the automated factory, the intelligent hospital or aerospace and defense—get your high-performance communications, base stations and computing systems to market easier with our advanced QorIQ platforms.

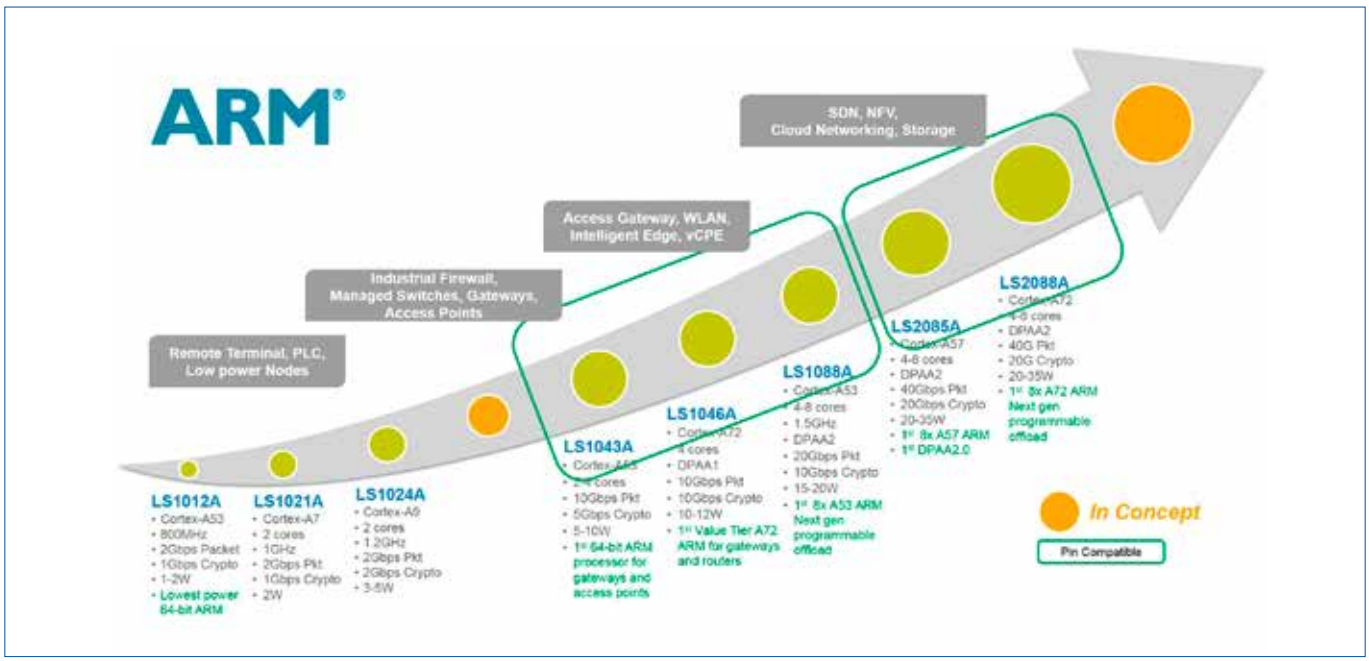
SEC Features

- Public Key Hardware Accelerators (PKHA) ~25K RSA Ops/sec (1024b)
  - RSA and Diffie-Hellman (to 4096b)
  - Elliptic curve cryptography (1023b)
- Data Encryption Standard Accelerators (DESA) ~15Gbps
  - DES, 3DES (2K, 3K)
  - ECB, CBC, OFB modes
- Advanced Encryption Standard Accelerators (AESA) ~40Gbps
  - Key lengths of 128-, 192-, and 256-bit
  - ECB, CBC, CTR, CCM, GCM, CMAC,
  - OFB, CFB, and XTS
- ARC Four Hardware Accelerators (AFHA) ~7.5Gbps
  - Compatible with RC4 algorithm
- Message Digest Hardware Accelerators (MDHA) ~40Gbps
  - SHA-1, SHA-2 256,384,512-bit digests
  - MD5 128-bit digest
  - HMAC with all algorithms
- Kasumi/F8 Hardware Accelerators (KFHA) ~9Gbps
  - F8 , F9 as required for 3GPP
  - A5/3 for GSM and EDGE
  - GEA-3 for GPRS
- Snow 3G Hardware Accelerators (STHA) ~12Gbps
  - Implements Snow 3.0
- ZUC Hardware Accelerators (ZHA) ~14Gbps
  - Implements 128-EEA3 & 128-EIA3
  - CRC Unit~40Gbps
  - Standard and user defined polynomials
- Random Number Generator, random IV generation

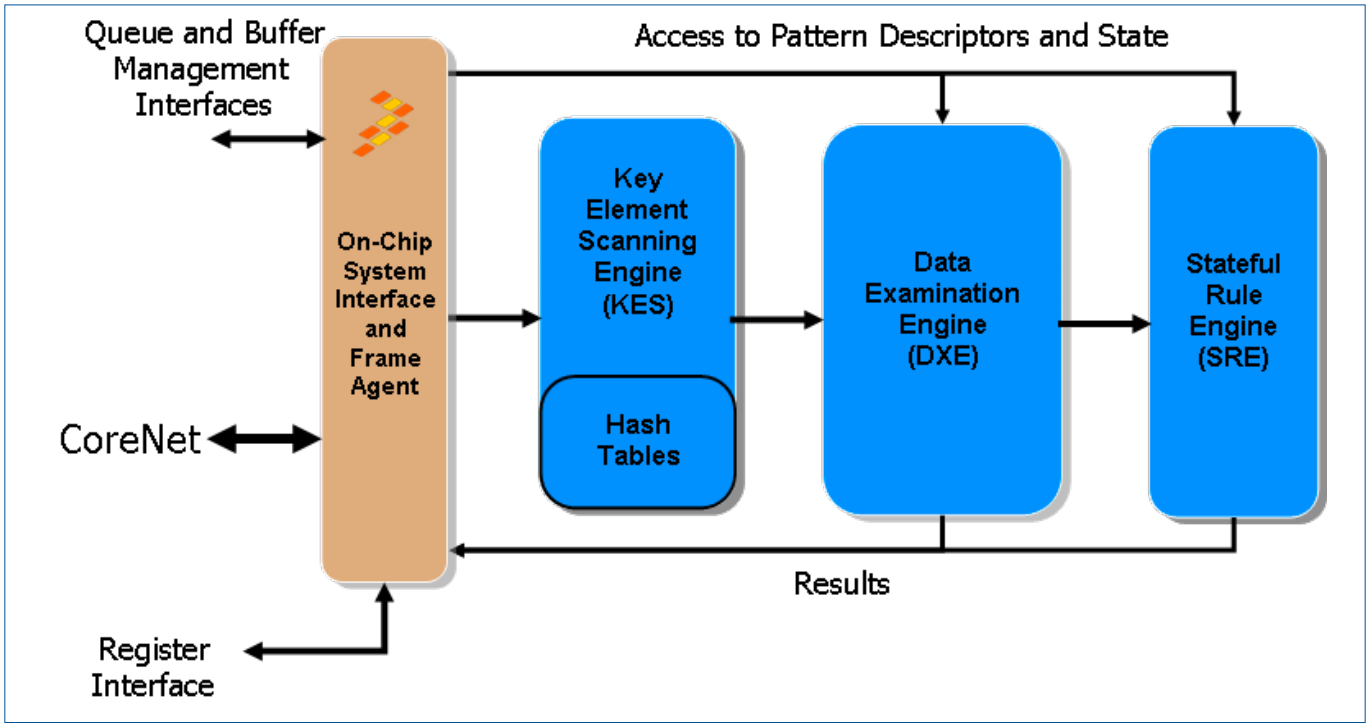


Supports protocol processing for the following:

- IPSec
- 802.1ae (MACSEC)
- SSL/TLS/DTLS
- 3GPP RLC
- LTE PDCP
- SRTP
- 802.11i (WiFi)
- 802.16e (WiMax)



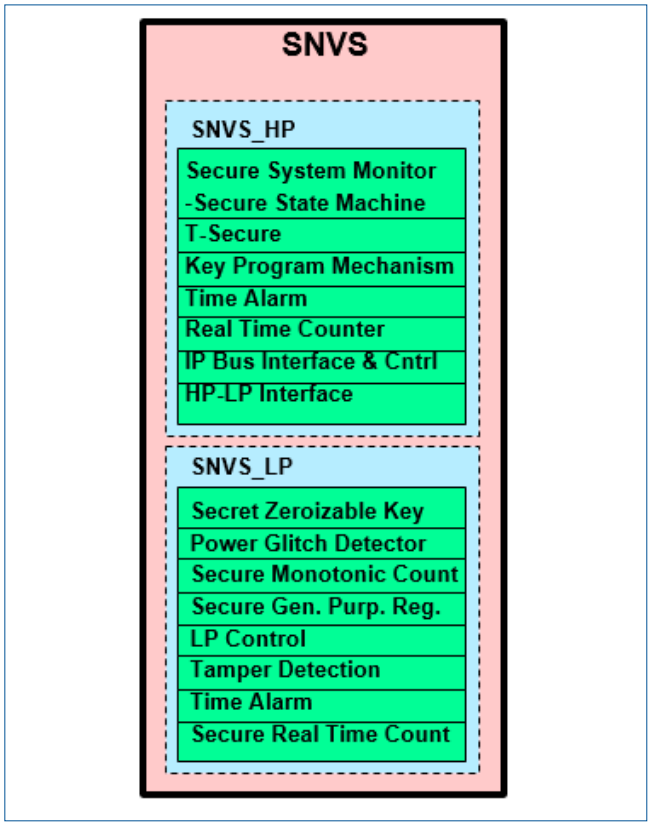
Pattern Matching Engine (PME 2.0)



PME Features

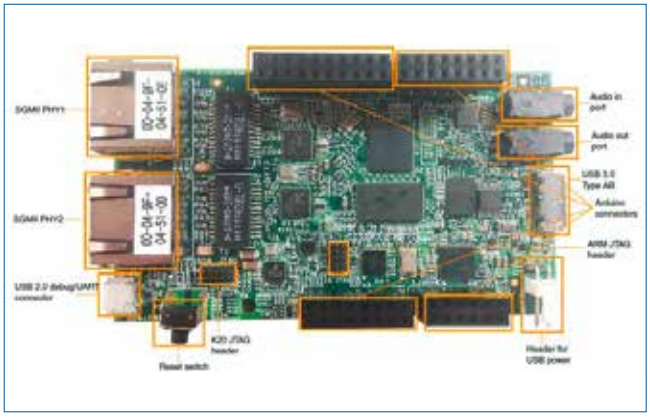
- Full-featured regular expression pattern matching accelerator
- Multi-Gbps performance with regular DDR SDRAM memory
- Pattern matches can be further qualified with stateful rules

Secure Non-Volatile Storage (SNVS)



SNVS Features

- SNVS_HP – System Power Domain
  - System Security Monitor
  - Zeroizable Master Key Programming Mechanism
  - Master Key Control block
  - Non-Secure Real Time Counter with Alarm
- SNVS_LP – Dedicated Power Domain
  - Zeroizable Master Key
  - Secure Non-Rollover Real Time Counter with Alarm
  - Non-Rollover Monotonic Counter
  - Power Glitch Detector
  - General Purpose Register
  - Tamper Detection Monitor



C29X: CRYPTO COPROCESSOR

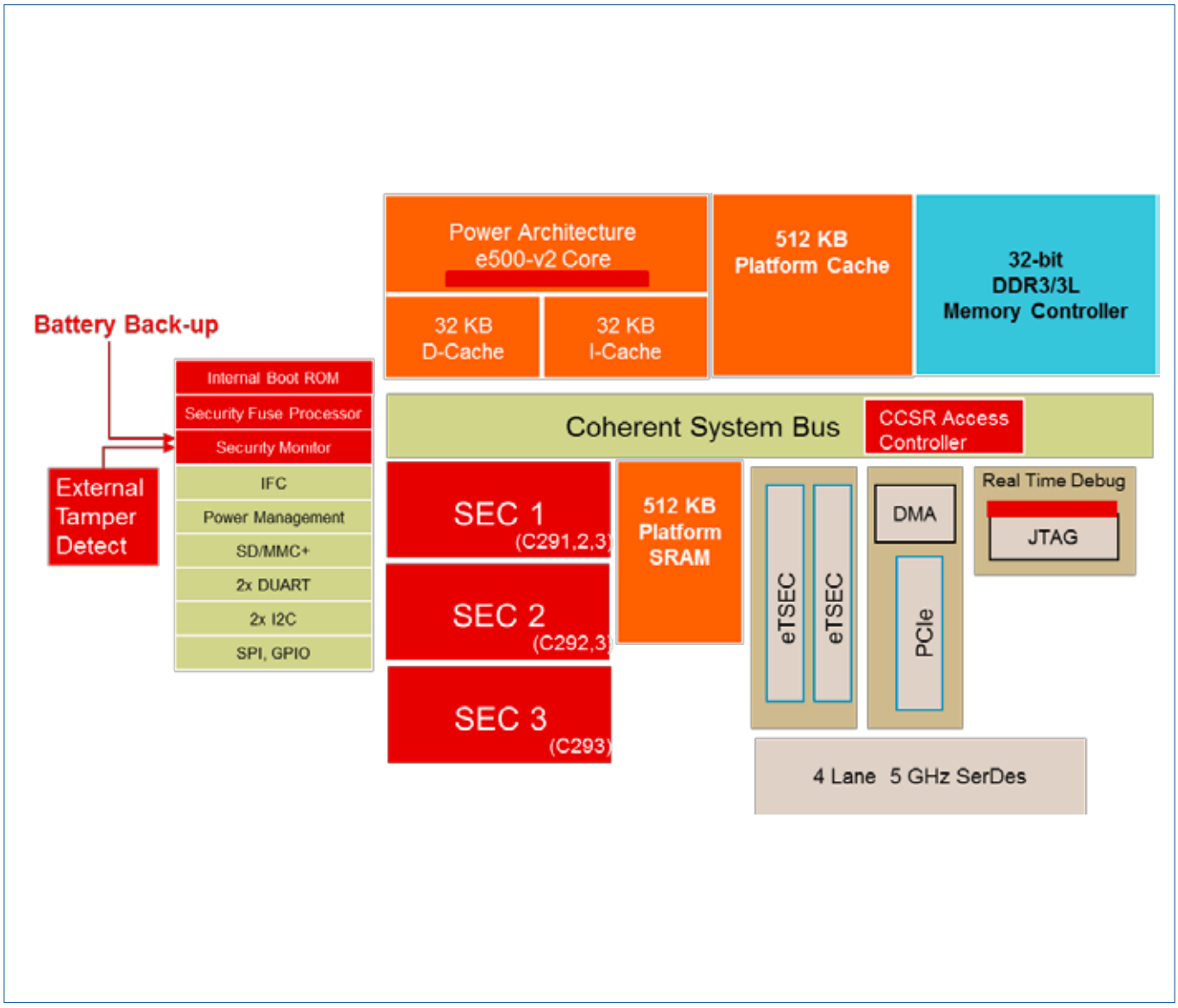
The NXP C29x crypto coprocessor family consists of three high performance crypto coprocessors – the C291, C292 and C293 – which are optimized for public key operations targeting network infrastructure across the enterprise and the data center.

Public key algorithms such as RSA, Diffie Hellman and Elliptic Curve Cryptography (ECC) are the basis of digital signature and key exchange protocols that make secure transactions possible. By providing public key acceleration, the C29x family enables networks to efficiently scale with the increase in SSL and IPsec traffic that require public key. Scaling with secure transactions is difficult because performing public key math in software can quickly saturate today's general purpose processors.

While optimized around public key, the C29x family can also accelerate AES-HMAC-SHA-1 bulk encryption. The three devices offer scalable, pin-compatible performance and range from one to three security engines (SEC) – the C291 features one SEC, the C292 features two SECs, C293 features three SECs.

Security Features

- Up to 32k of RSA 2048-bit private key performance (C293)
- Up to 12Gbps AES-HMAC-SHA-1 bulk encryption (system throughput)
- Power as low as five watts (C291)
- Support of dual use cases:
  - Public key offload – no external memory required
  - Secure key management – act as offload accelerator or stand alone
- NXP trust architecture:
  - Secure boot
  - Tamper detection
  - Optional battery backed secret key



MICROCONTROLLERS AND PROCESSORS FOR AUTOMOTIVE

NXP offers the broadest portfolio of single–, dual– and multicore processors built on ARM Cortex or Power Architecture® technology, providing exceptional performance and superb reliability. Whether you're designing a high–end networking application or an automotive system, you'll find the integration expertise and comprehensive ecosystem you need with NXP's automotive processor families.

The safety and security features enable its use in airbag applications as well as in immobilizers where secure communication and integrity of the system is required.

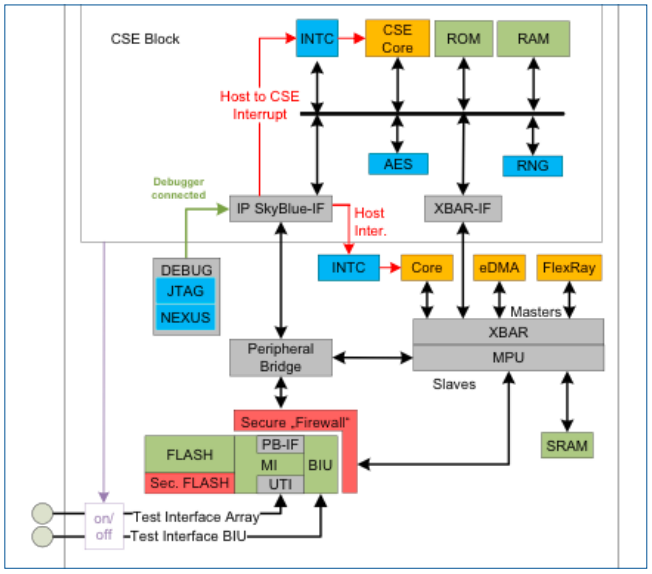
Cryptography Service Engine (CSE)

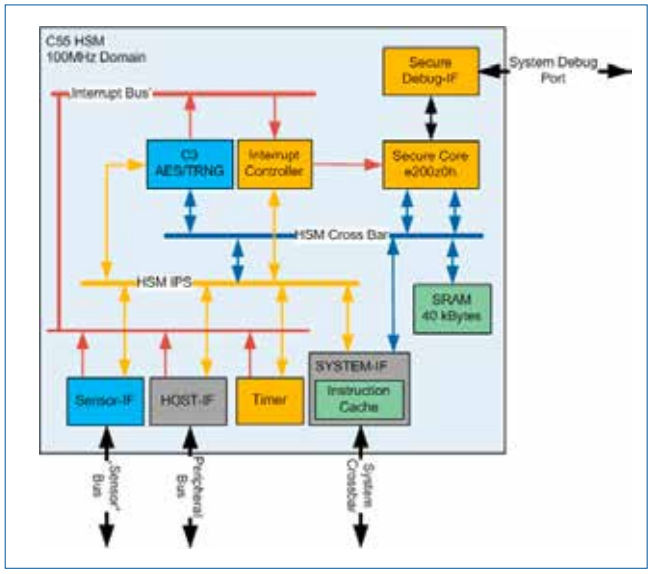
Moves the crypto keys from public memory into the secure memory. Only the CSE can access the keys.

- 32-bit secure core up to 133 MHz
- AES-128
- 120-bit Unique ID
- Secure Boot support
- Secure flash blocks assigned to CSE
- No other masters can access this memory
- PRNG seed generation via TRNG

Hardware Security Module (HSM)

- The HSM is a programmable security module. Customers are able to implement their own security algorithm and communication layers
- e200z0h core with up to 100MHz clock
- 4Kbytes instruction cache
- Secure Debugger Interface
- Cryptographic Modules with AES-128,
- Random Number Generator, DMA
- Sensor Interface – monitor for voltage,
- temperature and clock





ST SECURITY SOLUTION FOR INTERNET OF THINGS

The authentication market is currently expanding from largely deployed brand protection, IT security and TPM solutions to now include the Internet of Things market.

Data issued from Objects involved in smart grids, smart cities, smart homes, smart industry, with Industry 4.0 initiative, must be trusted, and more and more connected devices are now adopting solutions based on secure elements similar to those used in printers, PCs, game controllers, phone accessories, batteries, and luxury goods."

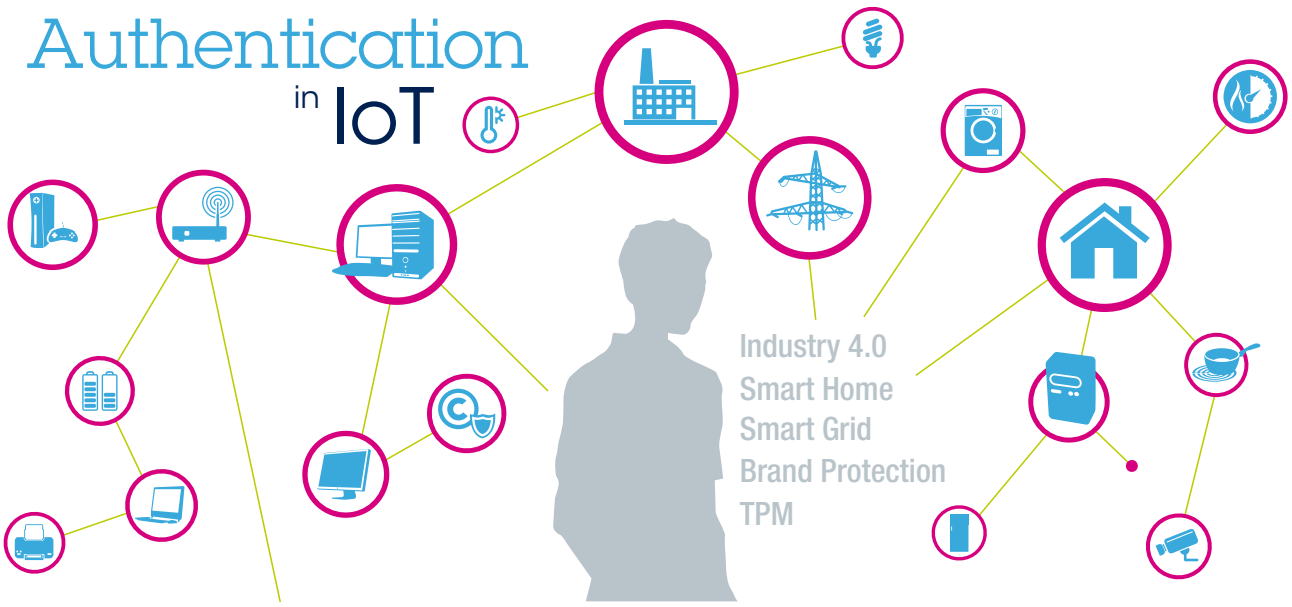
ST offers a full ecosystem with ready-to-use turnkey solutions to ensure device identity, systems and network integrity, for customers cautious about their brand, or willing to rely on a safe and secure IoT. These solutions may be used as standalone chips in consumables like ink cartridges or in conjunction with an application MCU - like STM32 - or MPU.

ST secure element STSAFE family ranges from optimized to flexible Java based and TCG compliant TPM solutions. Relying on EAL5+ Common Criteria certified chips on top of which runs an ST developed secure operating system, ST's solutions ensure state-of-the-art security for the protection of objects and IoT networks against:

- Device counterfeiting
- User data corruption
- Device malfunction
- Service & network access corruption

Developers benefit from a comprehensive set of development tools and services:

- Expansion board based compatible with STM32 Nucleo and Arduino xxx
- Example codes and libraries to be embedded in the application microcontrollers (authentication, TLS)
- Personalization services for trusted secrets storage



STSAFE-TPM standardized

- Platform integrity
- Compliant and certified TPM 1.2 & 2.0 TCG standard
- Boot securization,
- EAL4+ Common Criteria certified

STSAFE-J flexible

- Flexible Java based crypto services
- Authentication, encryption, signature
- Secure channel (flexible)
- Secure firmware upgrade
- High memory key storage
- EAL4+ Common Criteria / BSI certified

STSAFE-A optimized

- optimized crypto services
- Authentication, Encryption, signature
- Secure channel (TLS)
- Secure firmware upgrade
- Hardware EAL5+ Common Criteria certified

STSAFE-A

STSAFE-A is an optimized secure solution providing authentication and data management services to a local or remote host. Its command set is tailored to address strong authentication, establish a secure channel in the scope of a TLS session, verify signatures, and offer secure storage as well as decrement counters for usage monitoring.

EAL5+ Common Criteria certified, STSAFE-A is a highly secure authentication solution whose security is certified by independent parties. It is particularly well suited for applications heavily exposed to fraud and counterfeiting attacks, such as printers, game controllers, phone accessories, and IoT networks. STSAFE-A is the ideal solution for customers wishing to build an ecosystem around their brand.

STSAFE-J

With a flexible Global Platform and Java 3.0.4 compliant command set, STSAFE-J is the new generation of KERKEY™ versatile secure solution offering a wide range of cryptographic and secure services for applications which need to comply with a pre-established schemes. Moreover, its EAL4+ Common Criteria certificate enables it to serve the smart grid market as well as those requiring strong security in concentrators, gateways, and IoT devices.

STSAFE-TPM

STSAFE-TPM, ST's Trusted Platform Module, is an EAL4+ Common Criteriacertified solution compliant and certified TPM 1.2 & 2.0 TCG (Trusted Computing Group) standard, which protects users' assets by monitoring platform integrity from the boot phase.

Used in devices where firmware integrity is a must, TPMs are largely deployed in desktops, notebooks, tablets, and servers and continue to spread into today's connected world, expanding from PCs to phones to home gateways to cars to infrastructures and more.

STSAFE-A100 FEATURES

- Authentication (of peripherals, IoT and USB Type-C devices)
- Secure channel establishment with remote host including transport layer security (TLS) handshake
- Signature verification service (secure boot and firmware upgrade)
- Usage monitoring with secure counters
- Pairing and secure channel with host application processor
- Wrapping and unwrapping of local or remote host envelopes
- On-chip key pair generation

Security features

- Latest generation of highly secure MCUs
  - EAL5+ AVA_VAN5 Common Criteria certified
  - Active shield
  - Monitoring of environmental parameters
  - Protection mechanism against faults
  - Unique serial number on each die
  - Protection against side-channel attacks
- Advanced asymmetric cryptography
  - Elliptic curve cryptography (ECC) with NIST or Brainpool 256-bit and 384-bit curves
  - Elliptic curve digital signature algorithm (ECDSA) with SHA-256 and SHA-384 for digital signature generation and verification
  - Elliptic curve Diffie-Hellman (ECDH) for key establishment
- Advanced symmetric cryptography
  - Key wrapping and unwrapping using AES- 128/AES-256
  - Secure channel protocols using AES-128
- Secure operating system
  - Secure STSAFE-A100 kernel for authentication and data management
  - Protection against logical and physical attacks

Hardware features

- Highly secure MCU platform
- 6 Kbytes of configurable non-volatile memory
  - Highly reliable CMOS EEPROM technology
  - 30 years' data retention at 25 °C
  - 500 000 erase/program cycles endurance at 25 °C
  - 1.62...5.5 V continuous supply voltage
- Operating temperature: -40...95 °C

Protocol

- I²C-bus slave interface
  - Up to 400 Kbps transmission speed (Fast mode) and true open-drain pads
  - 7-bit addressing

Packages

- ECOPACK®-compliant SO8N 8-lead plastic small outline and UFDFPN 8-lead ultra-thin profile fine pitch dual flat packages

Tools and services:

- X-NUCLEO-STSA100 expansion shield compatible with STM32 Nucleo board (support of Morpho and Arduino connectors)
- Comprehensive set of software libraries, STM32 Cube compliant or ARM® mbed™ compliant
- Reference code examples for main use cases
- Personalization services for storing customer confidential datas

Figure 1. Authentication to a remote server (IoT device case)

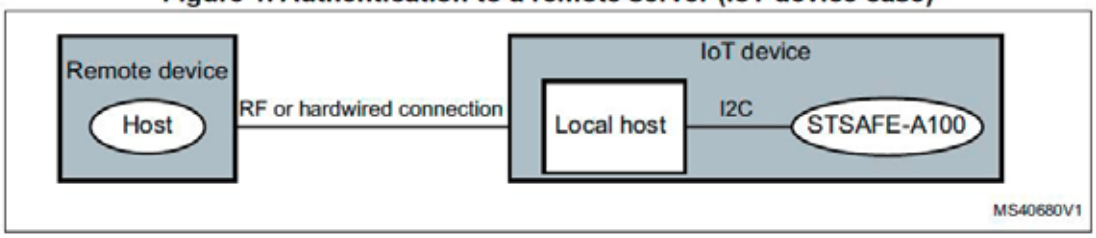
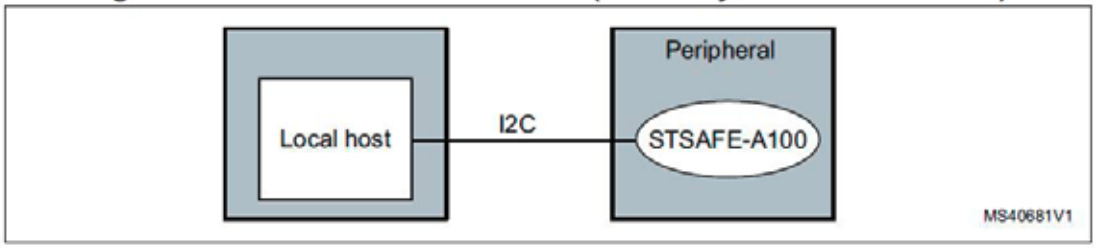


Figure 2. Authentication to a local host (accessory or consumable case)



STSAFE-J
FEATURES

Key Features

- ECC support for NIST-P-256 and other curves are supported depending on the product
- Digital signature generation and verification with ECDSA
- Key agreement with Diffie-Hellman (ECKA-ECDH) and El Gamal (ECKA-EG)
- ECDH-GM primitive for PACE protocol
- On-chip RSA and ECC key pair generation
- Key pair, public key and PIN objects
- Up to 80 Kbytes of user memory
- Extended length APDUs
- In house personalization services
- Full ecosystem with expansion board and middleware
- Supports specific application loading
- Different ST applets available for preloading

Platform

- Java Card™ 3.0.4 Classic Edition
- GlobalPlatform™ 2.1.1
- ISO/IEC 7816 T=0 and T=1 contact protocols
- Standard I²C communication up to 100 kHz
- Java Card Closed Protection Profile, v3.0
- Candidate to CC Certification EAL5+

Hardware

- ARM® SecurCore® SC000™ 32-bit RISC core 30-year data retention at 25°C & 500 000 erase/write cycles at 25 °C
- Operating temperature: -25 to +85 °C
- Enhanced NESCRYPT cryptoprocessor for public key cryptography
- Contact assignment compatible with ISO/IEC 7816-3 standards
- Asynchronous receiver transmitter (IART) for high speed serial data support (ISO/IEC 7816-3 and EMV® compliant)
- ESD protection greater then 6 kV (HBM) for contacts pads
- 1.62 V to 5.5 V supply voltages
- Common Criteria (EAL5+) certification
- ECOPACK® 32-lead VFQFPN 5x5 mm (0.5 mm pitch)

Security

- AIS-31 class PTG.2 compliant true random number generator (TRNG)
- AIS-20/31 class DRG.3 deterministic number generator (DRNG)
- Enhanced cryptographic algorithms: DES/3DES, ECC and AESSHA-1, SHA-256, MD5 and CRC16
- Generic Mapping primitive for Password Authenticated Connection Establishment (PACE) protocol
- Hardware security enhanced DES accelerator
- Hardware Security Enhanced AES
- Differential power analysis (DPA) and differential fault analysis (DFA) countermeasures against side channel attacks
- Active shield
- Unique serial number on each die

STSAFE-TPM FEATURES

- Flash based Trusted Platform Module (TPM)
- Supporting 2 modes exclusively with either the TPM1.2 or the TPM2.0 command set
- Supporting dynamic switch from one mode to another and capability to lock irreversibly one mode
- For TPM1.2, compliant with Trusted Computing Group (TCG) Trusted Platform Module (TPM) Main specifications 1.2, Level 2, Revision 116 and TCG PC Client Specific TPM Interface Specifications 1.3
- For TPM2.0, compliant with Trusted Computing Group (TCG) Trusted Platform Module (TPM) Library specifications 2.0, Level 0, Revision 116 and TCG PC Client Specific TPM Platform Specifications 0.43
- TPM firmware code can be upgraded thanks to a persistent Application Flash Loader to support new standard evolutions
- Targeting Common Criteria certificate according to the TPM 1.2 and TPM 2.0 protection profiles at EAL4+
- Targeting FIPS 140-2 certification
- SPI support up to 33 MHz
- Support for software and hardware physical presence for TPM1.2

Hardware features

- ARM® SecurCore® SC300™ 32-bit RISC core
- Highly reliable Flash memory technology
- Temperature ranges:
  - Standard: -25 °C to +85 °C
  - Extended: -40 °C to +105 °C
- ESD protection up to 4 kV (HBM)
- 1.8 V or 3.3 V supply voltage range
- 28-lead thin shrink small outline and 32-lead very thin fine pitch quad flat pack ECOPACK® packages

Security features

- Active shield and environmental sensors
- Memory protection unit (MPU) used to segregate TPM assets between TPM1.2 and TPM2.0 modes
- Monitoring of environmental parameters (power and clock)
- Hardware and software protection against fault injection
- FIPS compliant RNG built on an SP800-90A compliant SHA256 DRBG and an AIS-31 Class PTG2 compliant true random number generator (TRNG)
- Cryptographic algorithms: – RSA key generation (1024 or 2048 bits)
  - RSA signature and encryption
  - HMAC SHA-1 & SHA-256
  - AES-128-192-256
  - ECC 224 & 256 bits

Product compliance

- Compliant with Microsoft® Windows® 7, Windows 8.1 and Windows 10
- Compliant with Intel® TXT for TPM1.2 and TPM2.0
- TPM 1.2 and TPM 2.0 compliant with the respective TCG test suites

SUMMARY COMPARISON

	STSAFE-A100	STSAFE-J	STSAFE-TPM
Typical applications	• Printers, mobile accessories, play station accessories • meters, gateways, Smart home devices, Smart city devices • USB-C authentication	• Gateways	• Computers • Gateways • Servers
Features	• Generic & USB-C Authentications • Signature verification • Secure channel establishment with distant server (TLS) • Decrement counter • Secure data storage	• Flexible crypto services (Java + GP + applet)	• TCG compliant TPM 1.2 & 2.0
Personalization service at ST	Yes	Yes	Yes
Certification	CC EAL5+ HW	CCEAL5+ HW CC EAL4+ Platform	CCEAL4+ & TCG
Crypto	ECC, AES	RSA, AES, ECC, SHA	AES, 3DES, RSA, SHA-1, SHA-256, ECC
T° range	-40°C - 95°C	-40°C - 85°C	-40°C - 105°C
Package	SO8N DFN 2x3	VQFN 32 DFN8 4*4.2	TSSOP28 VQFN32
Comm. I/F	I^2C	I^2C	SPI, I^2C

NOTES

ABOUT EBV ELEKTRONIK

EBV Elektronik, an Avnet (NYSE:AVT) company, was founded in 1969 and is the leading specialist in EMEA semiconductor distribution. EBV maintains its successful strategy of personal commitment to customers and excellent services. 230 Technical Sales Specialists provide a strong focus on a selected group of long-term manufacturing partners. 110 continuously trained Application Specialists offer extensive application know-how and design expertise. With the EBVchips Program, EBV, together with its customers, defines and develops new semiconductor products. Targeted customers in selected growth markets will be supported by the Vertical Sales Segments. Warehouse operations, complete logistics solutions and value-added services such as programming, taping & reeling and laser marking are fulfilled by Avnet Logistics, EBV's logistical backbone and Europe's largest service centre. EBV operates from 64 offices in 29 countries throughout EMEA (Europe – Middle East – Africa). For more information about EBV Elektronik, please visit ***www.ebv.com****.*

Follow EBV on ***Facebook****,* ***LinkedIn****,* ***Twitter*** *and* ***YouTube****.*

EBV EUROPEAN HEADQUARTERS

EBV Elektronik GmbH & Co. KG I DE-85586 Poing | Im Technologiepark 2-8 | Phone: +49 8121 774 0 | www.ebv.com

EBV REGIONAL OFFICES | Status October 2017

AUSTRIA
AT-1120 Wien
Grünbergstraße 15 / Stiege 1 / 7. OG
Phone: +43 1 89152 0
Fax: +43 1 89152 30

BELGIUM
BE-1831 Diegem
Kouterveldstraat 20
Phone: +32 2 716001 0
Fax: +32 2 72081 52

BULGARIA
BG-1505 Sofia
48 Sitnyakovo Blvd., Serdika offices,10th floor, Unit 1006
Phone: +359 2 9264 337
Fax: +359 2 9264 133

CZECH REPUBLIC
Amazon Court
Karolinska 661/4
CZ-18600 Prague
Czech Republic
Phone: +420 2 34091 011
Fax: +420 2 34091 010

DENMARK
DK-8230 Åbyhøj
Ved Lunden 10-12, 1. sal
Phone: +45 8 6250 466
Fax: +45 8 6250 660

DK-2730 Herlev
Lyskær 9, 1. sal
Phone: +45 39 6905 11
Fax: +45 39 6905 04

ESTONIA
EE-10414 Tallinn
Niine 11
Phone: +372 62 5799 0
Fax: +372 62 5799 5
Cell. +372 513 2232

FINLAND
FI-02240 Espoo
Pihatörmä 1 a
Phone: +358 9 2705279 0
Fax: +358 9 27095498

FI-90100 Oulu
Nahkatehtaankatu 2
Phone: +358 8 4152627 0
Fax: +358 8 4152627 5

FRANCE
FR-13856 Aix-en-Provence
1330 Rue G.G. de la Lauziere
Europarc Pichaury, Bâtiment A2
Phone: +33 442 3965 40
Fax: +33 442 3965 50

FR-92184 Antony Cedex (Paris)
2-6 Place Du General De Gaulle - CS70046
Phone: +33 1 409630 00
Fax: +33 1 409630 30

FR-35510 Cesson Sévigné (Rennes)
35, av. des Peupliers
Phone: +33 2 998300 50
Fax: +33 2 998300 60

FR-67400 Illkirch Graffenstaden
35 Rue Gruninger
Phone: +33 3 904005 92
Fax: +33 3 886511 25

FR-31500 Toulouse
8 chemin de la terrasse
Parc de la plaine
Phone: +33 5 610084 61
Fax: +33 5 610084 74

FR-69693 Venissieux (Lyon)
Parc Club du Moulin à Vent
33, Av. du Dr. Georges Lévy
Phone: +33 4 727802 78
Fax: +33 4 780080 81

GERMANY
DE-85609 Aschheim-Dornach
Einsteinring 1
Phone: +49 89 38882 351
Fax: +49 89 38882 444

DE-10587 Berlin
Englische Straße 28
Phone: +49 30 747005 0
Fax: +49 30 747005 55

DE-30938 Burgwedel
Burgdorfer Straße 2
Phone: +49 5139 8087 0
Fax: +49 5139 8087 70

DE-59439 Holzwickede
Wilhelmstraße 1
Phone: +49 2301 94390 0
Fax: +49 2301 94390 30

DE-41564 Kaarst
An der Gümpgesbrücke 7
Phone: +49 2131 9677 0
Fax: +49 2131 9677 30

DE-71229 Leonberg
Neue Ramtelstraße 4
Phone: +49 7152 3009 0
Fax: +49 7152 759 58

DE-90471 Nürnberg
Lina-Ammon-Straße 19B
Phone: +49 911 817669 0
Fax: +49 911 817669 20

DE-04435 Schkeuditz
Airport Business Center Leipzig
Frankfurter Straße 2
Phone: +49 34204 4511 0
Fax: +49 34204 4511 99

DE-78048 VS-Villingen
Marie-Curie-Straße 14
Phone: +49 7721 99857 0
Fax: +49 7721 99857 70

DE-65205 Wiesbaden
Borsigstraße 36
Phone: +49 6122 8088 0
Fax: +49 6122 8088 99

HUNGARY
HU-1117 Budapest
Budafoki út 91-93, West Irodahaz
Phone: +36 1 43672 29
Fax: +36 1 43672 20

IRELAND
IE-Dublin 12
Calmount Business Park
Unit 7, Block C
Phone: +353 1 40978 02
Fax: +353 1 45685 44

ISRAEL
IL-40600 Tel Mond
Drorrim South Commercial Center
P.O. Box 149
Phone: +972 9 77802 60
Fax: +972 3 76011 15

ITALY
IT-20092 Cinisello Balsamo (MI)
Via C. Frova, 34
Phone: +39 02 660962 90
Fax: +39 02 660170 20

IT-50019 Sesto Fiorentino (FI)
EBV Elektronik Srl
Via Lucchese, 84/B
Phone: +39 05 543693 07
Fax: +39 05 542652 40

IT-41126 Modena (MO)
Via Scaglia Est, 33
Phone: +39 059 292 4211
Fax: +39 059 292 9486

IT-80128 Napoli (NA)
Via G. Capaldo, 10
Phone: +39 081 193016 03
Fax: +39 081 198061 24
Cell. +39 335 83905 31

IT-00155 Roma (RM)
Via Edoardo D'Onofrio 212
Phone: +39 06 4063 665/789
Fax: +39 06 4063 777

IT-35030 Sarmeola di Rubano (PD)
Piazza Adelaide Lonigo, 8/11
Phone: +39 049 89747 01
Fax: +39 049 89747 26

IT-10144 Torino (TO)
Via Treviso, 16
Phone: +39 011 26256 90
Fax: +39 011 26256 91

NETHERLANDS
NL-3606 AK Maarssenbroek
Planetenbaan 116
Phone: +31 346 5830 10
Fax: +31 346 5830 25

NORWAY
Postboks 101, Manglerud
Ryensvingen 3B
NO-0681 Oslo
Phone: +47 22 67178 0
Fax: +47 22 67178 9

POLAND
PL-80-838 Gdansk
Targ Rybny 11/12
Phone: +48 58 30781 00

PL-02-674 Warszawa
Ul. Marynarska 11
Phone: +48 22 25747 06

PL-50-062 Wroclaw
Pl. Solny 16
Phone: +48 71 34229 44
Fax: +48 71 34229 10

PORTUGAL
Unipessoal LDA
Edifício Tower Plaza
Rotunda Eng.º Edgar Cardoso, 23 - 14ºG
PT-4400-676 Vila Nova de Gaia
Phone: +351 22 092026 0
Fax: +351 22 092026 1

ROMANIA
4C Gara Herastrau Street
Building B, 2nd Floor - 2nd District
Bucharest
RO-014472
Phone: +40 21 52816 12
Fax: +40 21 52816 01

RUSSIA
RU-620028 Ekaterinburg
Tatischeva Street 49A
Phone: +7 343 31140 4
Fax: +7 343 31140 46

RU-127486 Moscow
Korovinskoye Shosse 10,
Build 2, Off.28
Phone: +7 495 730317 0
Fax: +7 495 730317 1

RU-195197 St. Petersburg
Polustrovsky Prospect 43,
Office 421
Phone: +7 812 635706 3
Fax: +7 812 635706 4

SERBIA
Balkanska 2
XS-11000 Belgrade
Phone: +381 11 40499 01
Fax: +381 11 40499 00
Mobile: +381 63 204506
Mobile: +381 62 780012

SLOVAKIA
SK-82109 Bratislava
Turčianska 2
Green Point Offices
Phone: +421 2 3211114 1
Fax: +421 2 3211114 0

SLOVENIA
SI-1000 Ljubljana
Dunajska 167
Phone: +386 1 5609 778
Fax: +386 1 5609 877

SOUTH AFRICA
ZA-8001 Foreshore, Cape Town
1 Mediterranean Street
5th Floor MSC House
Phone: +27 21 402194 0
Fax: +27 21 4196256

ZA-3629 Westville
Forest Square,11 Derby Place
Suite 4, Bauhinia Building
Phone: +27 31 27926 00
Fax: +27 31 27926 24

ZA-2157 Woodmead,
Johannesburg
Woodlands Office Park
141 Western Service Road
Building 14-2nd Floor
Phone: +27 11 23619 00
Fax: +27 11 23619 13

SPAIN
ES-08014 Barcelona
c/Tarragona 149 - 157 Planta 19 1°
Phone: +34 93 47332 00
Fax: +34 93 47363 89

ES-39005 Santander (Cantabria)
Racing nº 5 bajo
Phone: +34 94 22367 55
Phone: +34 94 23745 81

ES-28760 Tres Cantos (Madrid)
Centro Empresarial Euronova
C/Ronda de Poniente, 4
Phone: +34 91 80432 56
Fax: +34 91 80441 03

SWEDEN
SE-191 62 Sollentuna
Glimmervägen 14, 7 tr
Phone: +46 859 47023 0
Fax: +46 859 47023 1

SWITZERLAND
CH-8953 Dietikon
Bernstrasse 394
Phone: +41 44 74561 61
Fax: +41 44 74561 00

CH-1010 Lausanne
Av. des Boveresses 52
Phone: +41 216 5401 01
Fax: +41 216 5401 00

TURKEY
Canan Residence
Hendem Cad. No: 54 Ofis A2
Serifali Umraniye
TR-34775 Istanbul
Phone: +90 216 528831 0
Fax: +90 216 528831 1

Armada Is Merkezi
Eskisehir Yolu No: 6 , Kat: 14
Ofis No: 1406
Sogutozu
TR-06520 Ankara
Phone: +90 312 2956 361
Fax: +90 312 2956 200

UKRAINE
UA-03040 Kiev
Vasilovskaya str. 14
off. 422-423
Phone: +380 44 496222 6
Fax: +380 44 496222 7

UNITED KINGDOM
South East
2, The Switchback
Gardner Road
Maidenhead
GB-Berkshire, SL6 7RJ
Phone: +44 16 28778556
Fax: +44 16 28783811

South West & Wales
12 Interface Business Park
Bincknoll Lane
Royal Wootton Bassett
GB-Wiltshire, SN4 8SY
Phone: +44 17 93849933
Fax: +44 17 93859555

North
Manchester International
Office Centre, Suite 3E (MIOC)
Styal Road
GB-Manchester, M22 5WB
Phone: +44 16 149934 34
Fax: +44 16 149934 74

Scotland
1st Floor
180 St. Vincent Street
GB-Glasgow, G2 5SG
Phone: +44 141 242482 0
Fax: +44 141 2211916

Distribution is today. Tomorrow is EBV!
www.ebv.com

EBV Elektronik
An Avnet Company