Security Products

Glossary of Terms

World-Class Embedded Security Solutions Ensure 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. In addition to using security solutions to prevent malicious attacks on and through your products, you can also use cryptography and authentication to improve customer experience, protect your brand and even revenue stream by preventing cloning of your products. Flexibility, advanced features, innovative cost-effective architectures, and ultra-secure hardware defense mechanisms make Microchip's hardware-based security devices an ideal way to add trust by design.

Microchip offers a variety of solutions from hardware-based crypto companions to microcontrollers and microprocessors with integrated security components.

- **CryptoAuthentication™ Libraries** — Offer you 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.
- **CryptoMemory® ICs** — The Microchip CryptoMemory IC family offers a range of cost-efficient, high-security electrically erasable programmable read-only memory chips (EEPROMs) and host-side security for applications requiring comprehensive data protection.
- **CryptoRF® Devices** — Microchip's 13.56 MHz RFID CryptoRF device family employs a 64-bit embedded hardware encryption engine, mutual authentication, and up to 64 Kbits of user memory.
- **Secure Boot for Application Processors** — Designed for securing the boot of applications processors, the CEC1302 and CEC1702 are full-featured ARM® Cortex®-M4-based microcontrollers with complete hardware cryptography accelerators enabled solutions in a single package. These products can also be used as the standalone MCU in embedded applications.
- **Secure SAMA5D2 MPU** — Secure by design, the SAMA5D2 MPU family sets the standard for securing embedded applications. ARM TrustZone®, hardware cryptography, secure memories and multiple monitoring mechanisms detect or prevent intrusion attempts. With PCI pre-certification, it is the solution of choice for financial transactions, such as POS terminals.

Term	Definition
Advanced Encryption Standard (AES)	A fast-symmetric key algorithm with a 128-bit block and keys of lengths 128-, 192- and 256-bits based on a substitution-permutation network.
Alice, Bob and Eve	Alice is the name given to the first user, Bob is the name of the second user and Eve is the name given to the eavesdropper (hacker).
ARM® TrustZone	Circuitry embedded in the ARM Cortex®-A processors since ARMV6 architecture and in the ARM Cortex-M processors since ARMV8M architecture allowing to split the software into a trusted world and a normal world.
Asymmetric Key Algorithm	A cryptographic algorithm that uses a private and a public key for encryption and decryption operations.
Asymmetric Key Cryptography	Cryptography employing one key to sign or encrypt and a different key to verify or decrypt.
Attack	Attempt to break the cryptographic methods implemented in a security service. This includes a brute force, man-in-the-middle and plaintext attacks.
Attack Surface	A potentially exploitable vulnerability of a system
Authentication	Assures that something is what it claims to be. For example, this confirms that the origin of the message came from the specific sender.
Block Cipher	A symmetric key algorithm that encrypts a message by breaking it down into fixed size blocks and encrypting each block.
Brute Force Attack	Attack characterized by methodically guessing each key and using those keys to decipher ciphertext. The attack becomes increasingly time and power consuming with increasing key size.
Certificate Authority (CA)	An entity that issues digital certificates and provides a “trust anchor” or “root of trust” in a “chain of trust.”
Chain of Trust	A structure of certificates or signatures that allows a “trust anchor” to assure the trustworthiness of other members in the structure. It is called a “chain” because the trustworthiness of each layer is guaranteed by the one before, back to the trust anchor.
Checksum	A value that is assigned to a file that is tested later to confirm that there were not any malicious changes made to the original file.
Cipher	An encryption-decryption algorithm. Plaintext passed through the cipher becomes ciphertext.
Cipher Block Chaining (CBC)	Block cipher mode of operation where each ciphertext depends upon the previous ciphertext. An Initialization Vector (IV) is used on the first block to ensure that each message is unique.
Curve25519	A specific elliptical curve designed to be used with ECDH, offers 128 bits of security and is one of the fastest ECC curves. Also known as ED25519 and Edwards Curve.
Data Encryption Standard (DES)	A symmetric encryption algorithm with a 56-bit key. Triple DES (3DES) applies DES to each block three times. 3DES is more secure because three different keys are used, providing a 168-bit key.
Decryption	The transformation of ciphertext back into original data (plaintext).
Diffie-Hellman	An asymmetric key agreement algorithm. Typically, two entities exchange some public information, then combine them via a secure mathematical algorithm with their own private keys to generate a shared session key.
Digital Certificate	An electronic document binding some pieces of information together, such as a user's identity, a public key and/or digital signature.
Digital Signature	Asymmetric key algorithm that associates a calculated number to a message and a signer. Depending on the algorithm, the calculated number permits authentication, integrity and non-repudiation of the message by the signer.
Digital Signature Algorithm (DSA)	An asymmetric key algorithm that creates a digital signature using the private key of a public/private key pair. The signature is verified by the associated public key.
Electronic Code Book (ECB)	A block cipher mode of encryption where each block of plaintext is individually encrypted to a block of ciphertext.
Elliptic Curve	Mathematical construct that satisfies this equation with x and y as variables and a and b as constants: $y^2 = x^3 + ax + b$ in field GF(p) and $y^2 + xy = x^3 + ax^2 + b$ in field GF(2^n).
Elliptic Curve Cryptography (ECC)	An asymmetric key algorithm based upon elliptical curve constraints. Often combined with Diffie-Hellman (ECDH) and DSA (ECDSA).
Elliptical Curve Diffie-Hellman (ECDH)	Combination of Elliptical curve cryptography and Diffie-Hellman key exchange to generate a shared secret.
Elliptical Curve Diffie-Hellman Ephemeral (ECDHE)	ECDH done with ephemeral (temporary) keys. After the secret is used, it is destroyed, along with the temporary key pairs. This type of fleeting secret is fundamental to achieving Perfect Forward Secrecy.

Term	Definition
Elliptical Curve Digital Signature Algorithm (ECDSA)	Combination of ECC and DSA.
Encryption	The use of an algorithm to transform original data (plaintext) into incomprehensible data (ciphertext).
Entropy	A profound lack of order. Random numbers used in cryptography require a very high degree of entropy.
Federal Information Processing Standards (FIPS)	Standards set by the US government regarding data protection.
Hacker	A person who tries to overcome data security measures.
Hash Function	Often referred to as a Message Digest Algorithm. An algorithm that produces message digests. Common hash functions include MD2, MD4, and SHA.
HMAC	Key-based hashing for Message Authentication Codes.
Identification	A process through which one user identifies the other user.
Initialization Vector (IV)	An initial block of data used to prime the symmetric cypher pump as to now always begin the actual encryption from the exact same state.
Key	A parameter used in cryptographic functions. Types of keys include private keys, public keys, secret keys and session keys.
Key Agreement	A process by which two entities in a system agree on a common key.
Key Functions	Common functions regarding keys include expansion, generation, management, recovery and revocation.
Key Pair	Pair of corresponding public and private keys. Always present in Asymmetric Key Cryptography.
Key Schedule	An algorithm that creates subkeys in a cipher block within a key space.
Key Space	Collection of all possible keys in a cryptosystem.
Message Authentication Code (MAC)	A transformation of plaintext using a MAC algorithm and symmetric key that provides authentication and data integrity. Also called MIC.
MAC Algorithm	An algorithm that produces a MAC. Common algorithms are HMAC-MD5, HMAC-SHA-1 and HMAC-SHA-512.
Man-in-the-Middle Attack	An attack where a hacker sits in the middle of the communicating parties and collects all the data.
Message Digest	Transformation that provides data integrity. Created by using a hash. The algorithm takes variable-length data and transforms it to a fixed-length piece of data. Also called a fingerprint.
National Institute of Standards and Technology (NIST)	Division of the US Government that produces safety standards for cryptography.
Nonce	Number used once. A nonce is used to assure the uniqueness of an operation. This uniqueness thwarts replay attacks and makes backwards calculation of keys infeasible.
One Time Pad	Also called the perfect cipher, is a crypto algorithm where a plaintext message is combined with a secret key of equal length. Commonly used with the XOR function. It is the only existing cipher considered to be mathematically unbreakable.
Perfect Forward Secrecy	Protects past sessions against future compromises of secret keys or passwords. AKA: Forward Secrecy.
Plaintext	Data transferred without any cryptographic protection. Also called cleartext.
Private Key	This term depends on context. If discussing symmetric cryptography, the private key is synonymous with the secret key (shared key). In asymmetric cryptography, the private key is the secret half of the public/private key pair.
Pseudo Random Number (PRN)	Numbers that seem random but are actually determined by specific function and seed value. PRNs are created by a PRNG (PRN Generator).
Public Key	Universal key in asymmetric cryptography.
Public Key Infrastructure (PKI)	A set of roles, policies, and procedures needed to create, manage, distribute, use, store, and revoke digital certificates and manage public-key encryption.
Random Number	A number that cannot be reasonably predicted better than by chance. Generated by a Random Number Generator (RNG).

Term	Definition
Root of Trust	An authoritative entity for which trust is assumed and not derived. Also called Trust Anchor.
RSA	Asymmetric Key Algorithm that can encrypt data and create and confirm digital signatures.
Salt	A string of random or pseudo random bits added to keys to complicate attacks.
Secret Key	A shared key used for encryption and decryption in symmetric cryptography.
Secret Sharing	Splitting a secret key in many pieces so that the user needs all pieces to utilize the secret key.
Secure Boot	The process that verifies that a certain piece of hardware boots up using only trusted firmware.
Secure Remote Password (SRP)	A security protocol that makes an eavesdropper unable to brute force guess a password without the other parties getting involved.
Seed	A random sequence of numbers used to derive more random numbers.
Session Key	A key used only for the duration of communication between users.
Secure Hash Algorithm (SHA)	A message digest algorithm that creates a unique hash value for each input.
SHA-1	A type of SHA that is no longer considered strong enough against modern hackers. The hash function uses a 160-bit hash value.
SHA-2	Superseded SHA-1. This hash algorithm works in the same way but produces a longer and stronger hash. There are four main variants: SHA-224, SHA-256, SHA-384 and SHA-512. The numbers at the end of the acronym are the bit size of the resulting hash.
SHA-3	Most recent version of SHA series. Unlike SHA-1 and SHA-2, it uses a new structure called the sponge construction, in which data is “absorbed” into the sponge, and then the result is “squeezed” out. The result is a permutation-based hash.
Shared Key	The secret key users share in symmetric key cryptography.
Shared Secret	A piece of data known only two the parties communicating.
Side Channel Attack	Any attack based on the information of the physical implementation of the cryptosystem. Information that could be used against a system includes timing information, power consumption and electromagnetic leaks.
Sign/Verify	See Digital Signature Algorithm.
Symmetric Key Algorithm	A cryptographic algorithm that uses a secret key which is shared between entities in the system.
Symmetric Key Cryptography	Cryptography employing symmetric key algorithms.
Tamper Resistant	Hardware devices that are impossible or almost impossible to extract information from.
Transport Layer Security (TLS)	Standard security technology creating an encrypted link between a web server and a browser. Its predecessor is known as Secure Sockets Layer (SSL).
Trust Anchor	A trust anchor is an authoritative entity for which trust is assumed and not derived. AKA: Root of Trust.
Trusted Platform Module	International standard set by the Trusted Computing Group for microcontrollers with integrated graphic keys.
Verification	A sub-process of authentication where one user verifies that the other user is who it claims to be.

The Microchip name and logo, the Microchip logo, CryptoMemory and CryptoRF are registered trademarks and CryptoAuthentication is a trademark of Microchip Technology Incorporated in the U.S.A. and other countries. ARM and Cortex are registered trademarks of ARM Limited (or its subsidiaries) in the EU and other countries. © 2017, Microchip Technology Inc. All Rights Reserved. 7/17.
DS00002493A