

The ESM-05 Anti-Counterfeiting Embedded Security Module (ESM) is a low gate count, low power identity module that incorporates a unique 256 bit identifier specific to the SoC. The unique identifier is bound to a RSA private key during a user-controlled configuration process to support a variety of identity provisioning schemes. The RSA private key may only be exported as a wrapped key blob using an internal NIST AES key wrap function. Wrapping permanently binds the RSA private key to the module that created it.

Key Features:

- Secure identity module with factory-programmed unique device identifier
- Low active power consumption and auto stand-by mode
- Key import and export functions using NIST AES Key Wrap function
- Internal key generation for symmetric and RSA keys
- Flexible support for Identification and Authentication protocol based on RSA at 1024, 2048 and 3072 bit key sizes
- AMBA/AHB interface

Applications:

- Secure device identifiers
- Identification & Authentication protocol processors
- Cryptographic protocol accelerators
- Secure transaction processing
- Key management systems

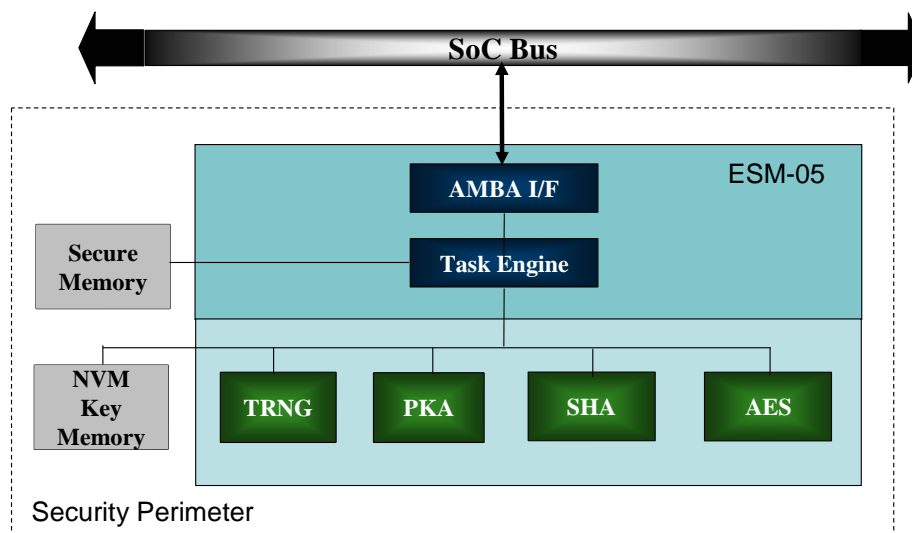


Figure 1 ESM-05 Block Diagram

Description

The ESM-05 anti-counterfeiting embedded security module is a low gate count, low power consumption identity module that incorporates a unique 256 bit identifier specific to the IC. The unique identifier is bound to a RSA private key during a user-controlled configuration process to support a variety of identity provisioning schemes. The RSA private key may only be exported as a wrapped key blob using an internal NIST AES key wrap function. Wrapping permanently binds the RSA private key to the module that created it.

The ESM-05 supports a variety of cryptographic operations including:

- RSA sign message and verify message
- RSA encrypt and decrypt
- Plaintext key import
- Wrapped key import and export
- Generate symmetric key and random number
- Generate RSA key pair

In addition to the internal wrapping key used to bind the ESM-05 to one or more RSA private keys, external wrapping keys may be loaded to the device, allowing wrapped keys created with other systems to be unwrapped with the ESM-05. In addition, multiple RSA private keys may be loaded, including up to three simultaneous keys. Any mix of supported private key sizes is supported by this feature.

The ESM-05 includes numerous high-security features such as protection against side-channel attacks through power or timing analysis. The module includes a zeroize function to support operation at NIST FIPS 140-2 levels 3 and 4. Binding a plaintext key to a module through wrapping using the module's unique identity key is a permanent operation: once bound, keys cannot be unbound or exported in cleartext.

The ESM-05 is targeted at RSA algorithms but can also support Elliptic Curve Cryptography (ECC) with a modified PKA solution and firmware update if required.

Performance

The ESM-05 performance is stated in the specified for RSA operations as indicated in the table on the next page. The performance assumes a 100 MHz core clock. Please note that key generation is not a deterministic process and as such the performance benchmark is stated as a statistical average over many samples. More details on key generation are available under NDA.

Operation	Performance	Conditions
RSA 1024 sign	63 ms	1024 byte payload
RSA 1024 verify	6.5 ms	1024 byte payload
RSA 1024 key generation	8.5 s	Average
RSA 2048 sign	490 ms	1024 byte payload
RSA 2048 verify	50 ms	1024 byte payload
RSA 2048 key generation	115 s	Average
RSA 3072 sign	1640 ms	1024 byte payload
RSA 3072 verify	170 ms	1024 byte payload
RSA 3072 key generation	550 s	Average

Deliverables

With the exception of the TRNG, the ESM-05 is available in soft IP form, either as a Netlist or HDL Source. The deliverables available are:

Netlist Licenses:

- Post synthesis netlist
- Testbench
- Sample simulation script
- Documentation

HDL Source Licenses:

- Verilog HDL
- Testbench
- Sample synthesis script
- Documentation

An FPGA load of the IP can be made available under license for evaluation purposes or the core can be made available on the EVAL-01 evaluation system².

The Ellipsys software required for the ESM-05 is available in object or source code formats.

More information is available by contacting:

Elliptic
62 Steacie Drive, Suite 201
Ottawa, ON, K2K 2A9

Phone: +1 613 254-5456
Fax: +1 613 254-7260
Email: info@ellipticsemi.com