winbond

SESIP Protection Profile for Secure External Memories Presented by Winbond

Ilia Stolov | Center Head of Secure Solutions

April 2022

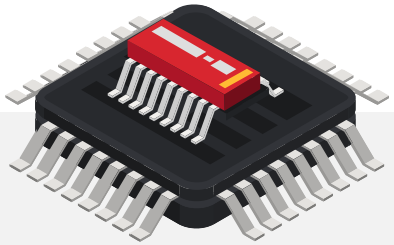
EXTERNAL MEMORY EVOLUTION

Before 2000

Stand Alone

Embedded platforms were based on a subsystem made of separate CPU, memories and peripherals

EXTERNAL MEMORY EVOLUTION



2000-2015

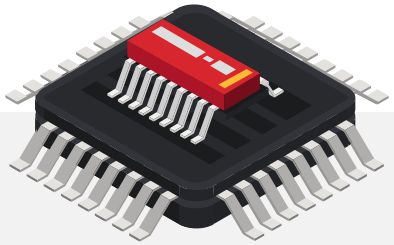
MCUs – On chip flash

CPU, memories and peripherals were made monolithically on the same die or in the same packaged device. It enabled security to be incorporated easily into the MCU e.g. Smart cards, Secure Elements, Hardware Security Modules

Advanced and diverse needs led to system integrators usage of external non-volatile memories to store critical platform assets such as:

- Code
- Private Data of End Users
- Platform Private Keys
- Platform Credentials

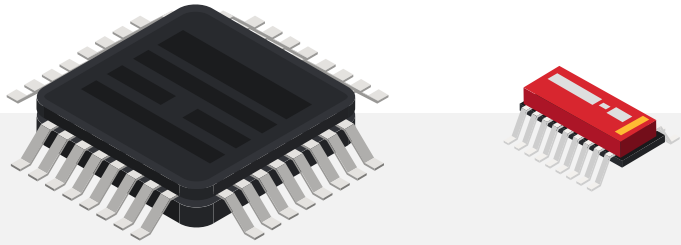
EXTERNAL MEMORY EVOLUTION



2000-2015

MCUs – On chip flash

CPU, memories and peripherals were made monolithically on the same die or in the same packaged device. It enabled security to be incorporated easily into the MCU e.g. Smart cards, Secure Elements, Hardware Security Modules



FinFET

Separated Again

WHY DO WE NEED SECURE STORAGE?

VULNERABILITY

- Eavesdropping
- Unauthorized data read
- Unauthorized data/code manipulation
- Attacking memory interface

NO SECURITY MECHANISMS

Standard memory devices have no security mechanisms. For most use cases, security must be extended from MCU to include the storage device (not rely only on MCU)

WHAT IS “A SECURE STORAGE”?

The system needs
A secure storage device

- The storage needs to be as reliable as an embedded storage
- The data stored inside the secure storage should be accessible only to authorized entities
- The stored data can only be modified by authorized entities
- System should keep track of changes made to the stored data and alert if outdated data is found

These storage devices must meet certification requirements
(SESIP, Common Criteria)

WHY SESIP PROFILE FOR SECURE EXTERNAL MEMORIES ?

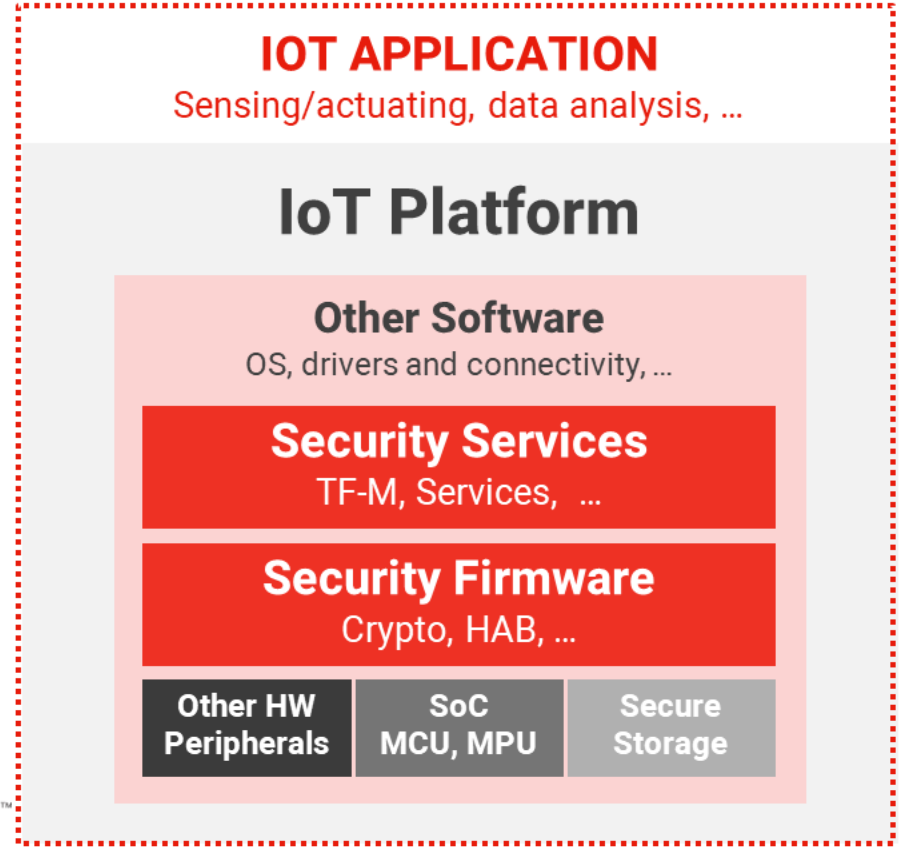
Memories are key components in the system, holding code and vendor/platform/user sensitive data

Clear security requirements for external memories

- Security Functional Requirements (which security features)
- Security Assurance Requirements (which evaluation activities)

Allow the reuse of evaluation results for entire system SESIP evaluation

SESIP™



SESIP PROFILE APPROACH
FOR SECURE EXTERNAL MEMORIES

Evaluate a memory device as a “stand alone” component without relying on the security capabilities of the SoC/MCU

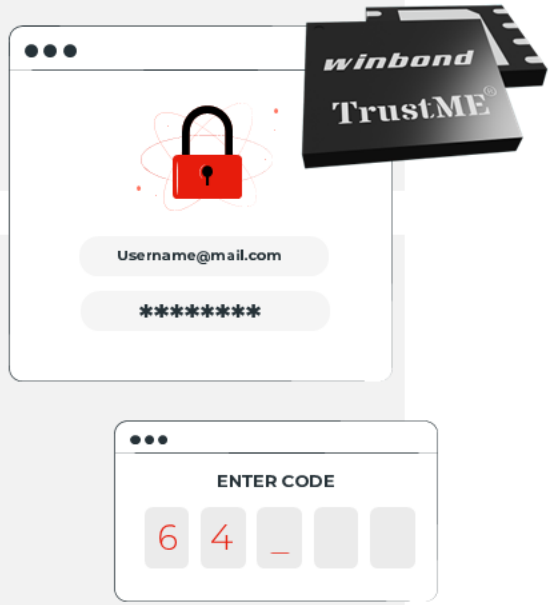
- This allows composition certification and creates a minimal baseline for what a Certified Secure Memory needs to be

The following main security features were listed:

- Data is protected for integrity and authenticity
- Communication with the secure memory is protected
- Freshness of the memory content is guaranteed
- Physical attacker resistance is required

“SECURE STORAGE”
SECURITY FUNCTIONAL REQUIREMENTS

All data stored in the secure memory (expect for a predefined list of data) is protected to ensure authenticity and integrity using a key of predefined length



This SFR guarantees that data read from the secure memory has not been modified by an adversary and that it is complete, just as it was stored in the secure memory.

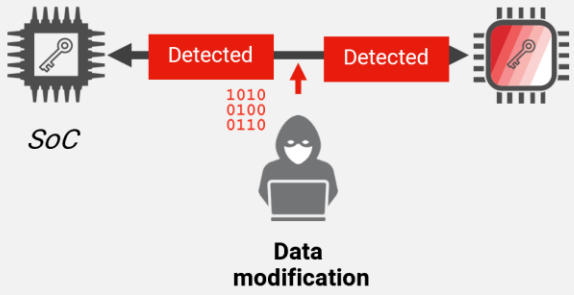
- For code stored in the secure memory, it guarantees the code is genuine and has not been even partially modified or replaced
- For data stored in the secure memory, it guarantees that the code and overall application can rely on it to be genuine and complete

"SECURE COMMUNICATIONS"
SECURITY FUNCTIONAL REQUIREMENTS

This SFR requires that the secure memory provides at least one communication channel for the host to communicate with the secure memory in a way that is protected from:

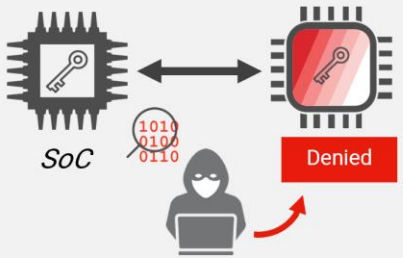
1. Modification

Adversary cannot change the data going from or to the secure flash without this change being detectable



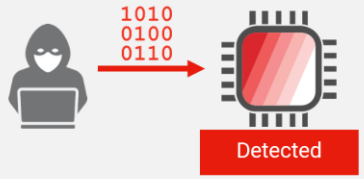
2. Replay

Adversary cannot record and resend old, genuine communications in an effort to trick the system into using that old genuine information as legitimate information



3. Impersonation

An adversary cannot create genuine communications with the memory device without knowledge of the secret communications key



“RELIABLE INDEX”
SECURITY FUNCTIONAL REQUIREMENTS

This SFR requires that the secure memory provides a strictly increasing function (e.g. monotonic counter).

The reliable index allows the memory to guarantee the **freshness** of the information stored in it so that an adversary cannot write genuine, yet outdated information to the memory.

This SFR prevents **roll-back** attacks on code and data and guarantees the system is always up-to-date with the latest information written to it.

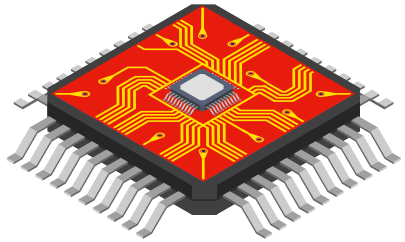
PHYSICAL ATTACKER RESISTANCE

The physical attacker resistance applies in both identification and exploitation phases

For SESIP2 level
an AVA_VAN.2
(15 points) protection
is sufficient

For SESIP3 level
an AVA_VAN.3
(20 points)
protection is needed

For SESIP5 level
AVA_VAN.5
(30 points and up)
protection is mandatory



BENEFITS OF SESIP

USER
Undisrupted and reliable service IoT security adapted to use-cases, trusted services and privacy

SOFTWARE DEVELOPERS
Reduces vendors security NRE Reduces vendors manufacturing and operational costs
Reduces vendors time to market Helps protect vendors against expensive recalls and lawsuits

OEMS AND SERVICE PROVIDERS
Helps meet compliance
Reduces service operational costs Significantly reduces cyber disaster impact and recovery

CHIPMAKERS
Increases the overall value of the product
Reduces operational costs
Clear market differentiator

winbond

THANK YOU

Website: www.winbond.com

E-mail: trustme@winbond.com