SAFRAN

IDENTITY & SECURITY

TINYSE+
CSPN SECURITY TARGET

Reference: SEC135 rev 5

Issue Date: 2017-03-30

0 Table Of Content

1 TSE+ Reference (Identification)

Product Vendor: Safran Identity & Security

Product Vendor website: http://www.morpho.com/

The Target of evaluation (TSE+) is the TinySE+ version 1 (**TSE+ rev 1**).

Reference and version is obtained using Get Info command (Cf. [TEP078] For details.)

2 TSE+ Description

2.1 TSE+ General Description

The **TinySE+ (TSE+) rev 1** is an embedded secure element designed for IoT market. It is made of a hardware (HW) part and an embedded software (ES) part:

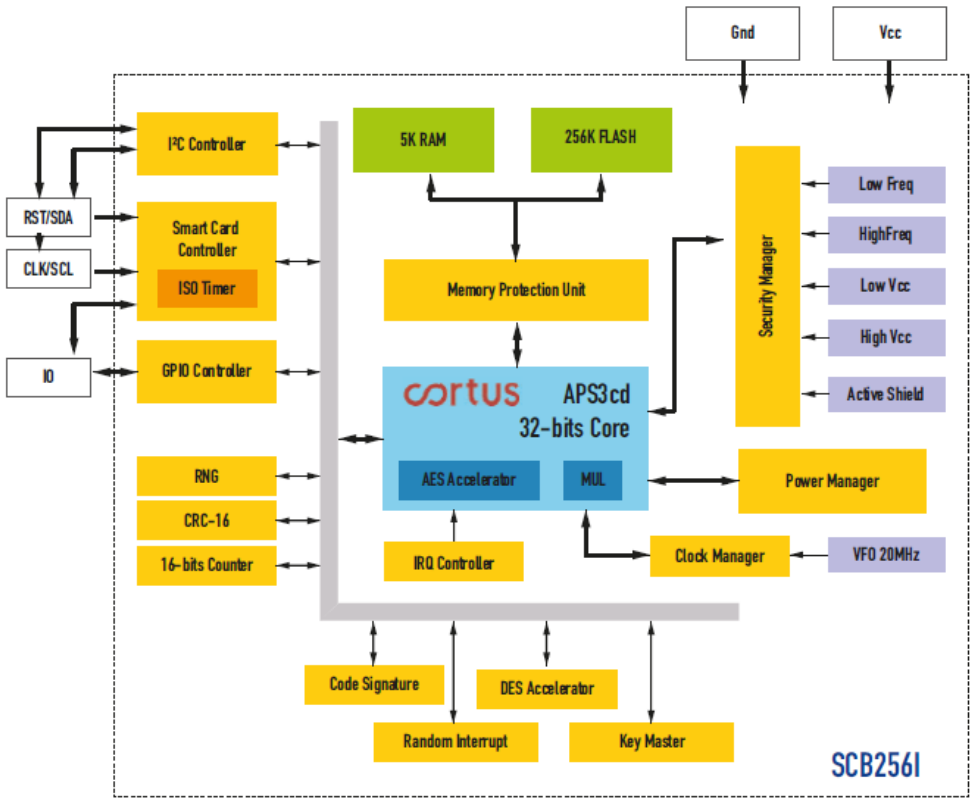
- HW: SCB256I rev A *obtained using "Read OTP" command [TEP078]*
- SW: IOTOS - ES version 1.1.1 *obtained using "Read TinySE+ Info" command [TEP078]*

The TSE+ is a product that provides "security functions" designed to be embedded in any "IoT" device.

The TSE+ provides the following functions:

- mutual authentication (with diversified secrets for each TSE+)
- MAC command (Message Authentication Calculation of any message sent to the TSE+)

HW overview:



ES overview:

The TSE+ answers to the following commands:

- Get Info / Get OTP
- Initialize update
- External Auth
- Message MAC (conditioned to External Auth success)

2.2 TSE+ Usage mode

The TSE+ is embedded in an IoT device. It is used as a “slave” by the main application processor (main CPU) of the IoT device.

Commands are sent by the IoT host device main CPU using the physical I2C interface.

The TSE+ has its own unique serial number.

2.3 TSE+ Operational environment

The TSE+ contains secrets that allows a trusted entity (such as a remote server) to check that it is genuine. The secrets are shared with the trusted entity and loaded into the TSE+ during production with a secured provisioning flow.

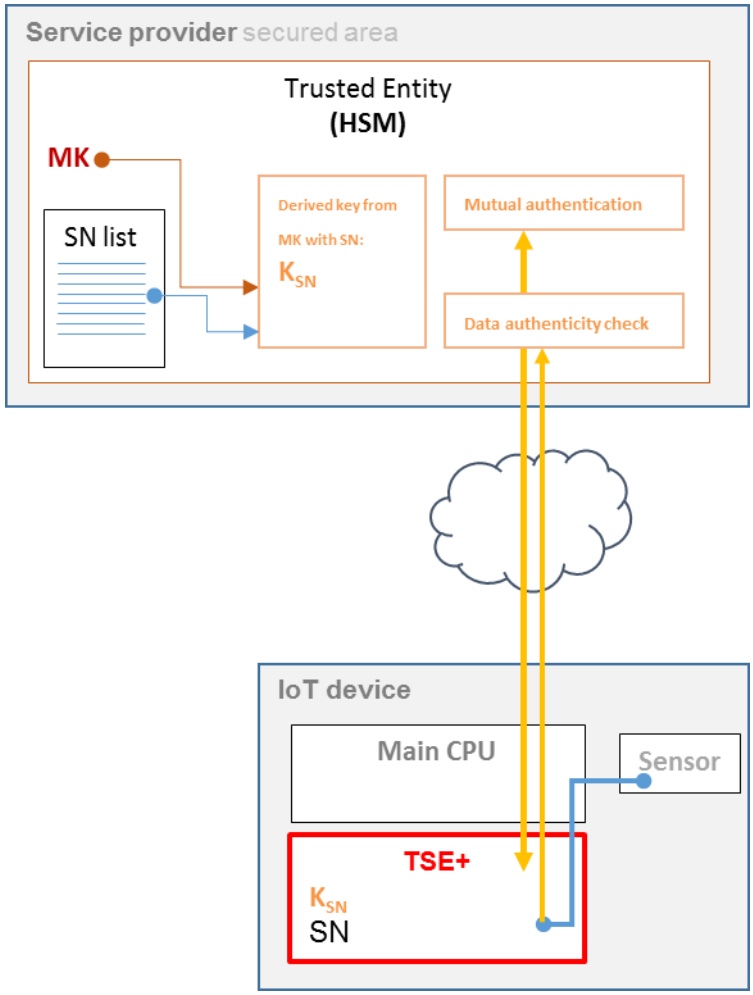


Figure: overall view of the Tiny SE+L (in red) in its operational environments

The remote trusted entity has a list of TSE+ serial numbers SN and knows the master keys. Please refer to [TEP078] for a detailed keys description.

The remote trusted entity can request a mutual authentication using the TSE+ unique key (obtained using SN and the relevant key).

The remote trusted entity can request a message MAC from the TSE+ using the TSE+ unique key (obtained using SN and the relevant key).

2.4 Assumptions on TSE+ Operational environment

2.4.1 Definitions

Trusted entity (or remote trusted entity)

The trusted entity is responsible of operating the technical system capable of remotely using the TSE+. It manages the secrets (and all related operations) required to authenticate the TSE+ and their data.

Manufacturer:

This is the generic term for the entity in charge of producing the TSE+. The manufacturer is in charge of:

- Loading the embedded software
- Inserting the secrets inside the TSE+
- Securely exchanging the secrets with the remote trusted entity

HSM:

Hardware security module, “state of the art” equipment used to generate/store/securely share the secrets

IoT device:

This is the technical system the TSE+ is embedded on.

Main CPU:

This is the “core” of the IoT device that manages functions of the IoT devices, network connections and exchanges with the trusted entity and exchanges with the TSE+.

2.4.2 Assumption

Trusted entity

The remote trusted entity is using state of the art equipment to receive, store and manage the secrets.

Provisioning

The diversified secrets are loaded in each TSE+ using a secured trusted flow.

The master secrets and serial numbers are securely shared between the Manufacturer HSM and the trusted remote entity.

TSE+ end of life

The remote trusted entity can manage a list of revoked TSE+ (using their SNs).

3 TSE+ Technical operational environment

The TSE+ is directly managed by the main CPU of the device/object it is embedded on. Thanks to this main CPU, the communication between the TSE+ and the remote trusted entity is possible.

4 TSE+ Assets

The TSE+ must protect the following assets:

Kauth: Unique Authentication Key ➔ confidentiality

Kmac: Unique MAC Key ➔ confidentiality

5 Threats on TSE+

5.1 The threat agents are:

Agent 1:

A threat agent, with a physical access to the TSE+, trying to forge a single or several genuine TSE+.

Agent 2:

A threat agent, with a logical remote access to the TSE+ (through IoT device interfaces), trying to manipulate the TSE+ in order to forge a single or several genuine TSE+.

Agent 3:

A threat agent, with a logical remote access to the TSE+ (through IoT device interfaces), trying to manipulate the communication between the TSE+ and the trusted entity.

5.2 Threat definition

Threat 1 description:

An attacker by using physical/logical/software means, obtains the secret Kauth/Kmac in order to make a clone or a counterfeit of the TSE+.

Related threat agent: Agent 1 or 2

Threat 2 description:

An attacker by using side channel means, obtains the secret Kauth/Kmac in order to make a clone or a counterfeit of the TSE+.

Related threat agent: Agent 1

Threat 3 description:

An attacker uses replay attacks (replay of a recorded valid transaction) to perform an authentication to the remote trusted entity without a genuine TSE+.

Related threat agent: Agent 3

6 Security functions of the TSE+

The TSE+ provides the external user with some functions (named actions) made available through the TSE+ external interfaces (Cf. [TEP078] for details):

- Actions related to **Get Info / Get OTP**

  Provide the user with hardware and software identification means necessary for authenticity checks. Without this it is not possible to perform the authentication (Initialize Update).

  And of course, it also provides the user with the mean to identify the TSE+.

- Actions related to **Initialize update**

  Allows the external user to authenticate the TSE+ (by using the Kauth key). This key is securely stored and used by the TSE+.

  This authentication function is protected against replay attacks.

- Actions related to **External Auth** (Also Implemented for future extensions)

  Perform an authentication of the external user by the TSE+ (by using the Kauth key). This key is securely stored and used by the TSE+.

  This authentication function is protected against replay attacks.

- Actions related to **Message MAC** (conditioned to External Auth success)

  Perform an MAC calculation on a message submitted by the external user (by using the Kmac key). This key is securely stored and used by the TSE+.

Important note regarding “Message MAC” function:

This function mitigates threats where the threat agent acts remotely.

In case of a physical access to the IoT device, the threat agent could attack the message before submission to the TSE+ “Message MAC” function.

Attacks made (even remotely) on the main CPU are also not covered.

7 Referenced documents

[TEP078] TinySE+ User Manual
[TEP063] SCB256I Technical Datasheet
[TEP072] SCB256I Errata Sheet