THALES

Thales Advanced Security Platform (TASP)

Non-Proprietary Security Policy FIPS 140-2 Level 3

Copyright

Date	February 24, 2021
Doc. No	TesUSA-DDQ-000058-EN
Doc Version	1.5

Contents

Tables

Figure

1. Abbreviations

Approved	FIPS-Approved
ECDSA	Elliptic Curve Digital Signature Algorithm
Flash	Electrically erasable non-volatile memory
FIPS	Federal Information Processing Standard
FIPS 140-2	FIPS PUB 140-2 (Ref: FIPS 140-2)
FPGA	Field Programmable Gate Array
KAT	Known Answer Test
PCIe	Peripheral Component Interconnect Express
RAM	Random Access Memory
SHA	Secure Hash Algorithm
SHA-512	SHA producing a 512-bit message digest
SSD	Solid State Drive
TASP	Thales Advanced Security Platform (multi-chip embedded cryptographic module)

2. Reference Documents

FIPS 140-2	Federal Information Processing Standards Publication, Security Requirements for Cryptographic Modules, FIPS PUB 140-2 (latest release 12/03/2002)
FIPS 180-4	Federal Information Processing Standards Publication, Secure Hash Standard, FIPS PUB 180-4 (latest release 08/04/2015), which defines the SHA-512 hash, used by ECDSA in the Digital Signature Standard (Ref: FIPS 186-4)
FIPS 186-4	Federal Information Processing Standards Publication, Digital Signature Standard, FIPS PUB 186-4, which defines ECDSA (Elliptic Curve Digital Signature Algorithm) (latest release 07/19/2013)

3. Introduction

3.1 Purpose

This document is the Thales Group (Thales) Security Policy for the Thales Advanced Security Platform (TASP), which is a FIPS 140-2 defined multi-chip embedded cryptographic module. The TASP provides functionality for the secure loading and/or upgrading of applications used in a range of Thales products. The TASP's FIPS 140-2 validation does not extend to the module's operations after an application is successfully loaded or upgraded.

The module ensures that only applications that have been cryptographically signed by Thales can be loaded into the module. The module ensures the integrity of any application that is loaded into it. It will only allow an application to be loaded if it has been signed by a private key that has been generated by the vendor and in possession of the vendor. The signature is verified using a FIPS Approved signature verification algorithm and a public key corresponding to the vendor's private key (see Section 4). This Approved algorithm and the hash of the public keys are securely stored in the module.

Hardware Version	Firmware Version	Overall FIPS Level
TASP 1.0, P/N: FIPS Rev: 1.1	Bootstrap Version 1.1.22, 1.1.29 and 1.1.40	Level 3

Table 1 - Product References

The module implements the following FIPS Approved algorithms:

- ECDSA P-521 (Ref: FIPS 186-4)
- SHA-512 (Ref: FIPS 180-4)

The FIPS validation includes the integrity check on the bootstrap itself using SHA-512 and the digital verification on the signed application using ECDSA p521/SHA-512 as represented in the Figure below.

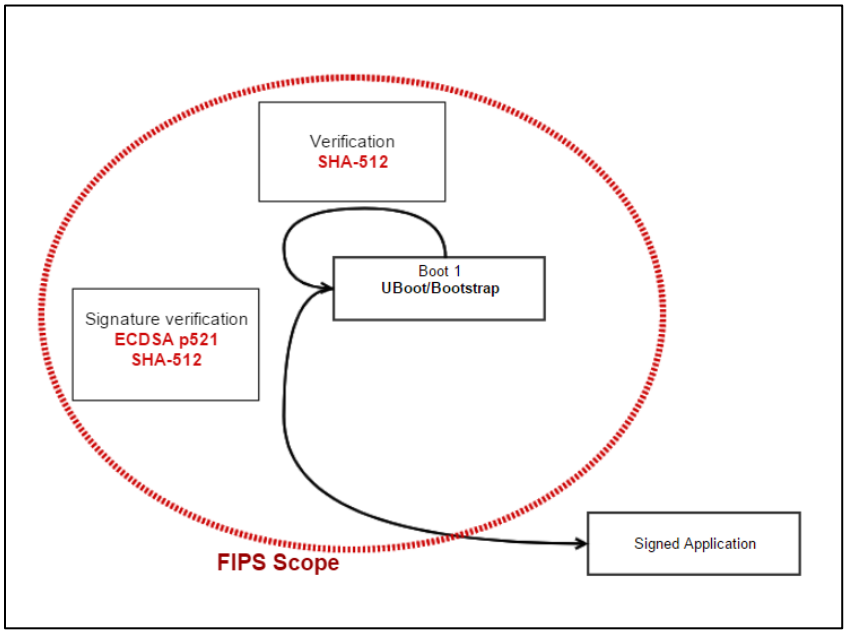

Figure 1 - Bootstrap

The circuitry that include all the security components within the module's cryptographic boundary is protected by hard, production-grade metal covers.

TASP contains a protected non-volatile memory that can be used by applications to contain confidential key material.

The figure below shows the TASP in the form in which it can be embedded in Thales products.

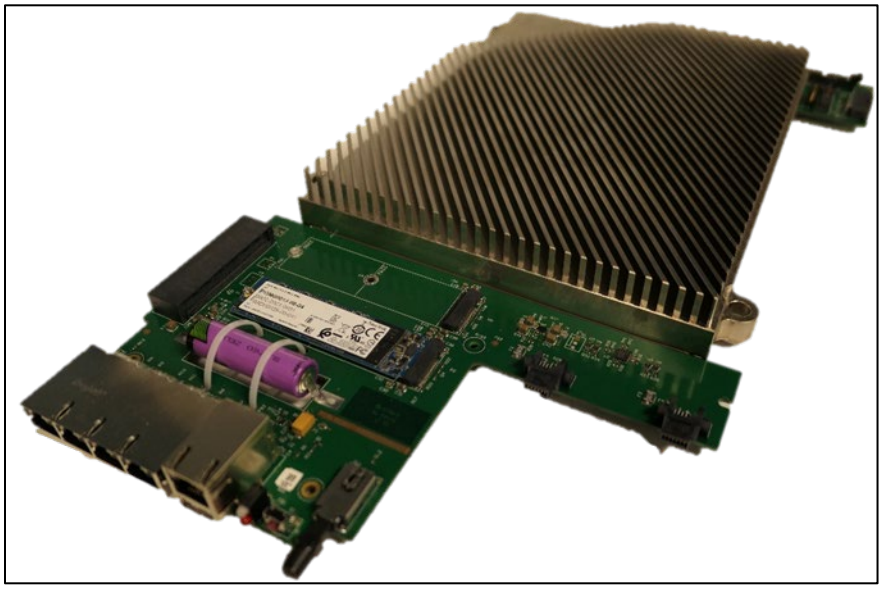

Figure 2 - TASP

The cryptographic boundary of the TASP is physically contiguous and is defined by the two-piece metal enclosure covering all critical components on the top and underside of the module, and the PCB as shown in Figure 2.

The figure below shows the TASP embedded in a Thales product. The blue line shows the TASP's boundary.

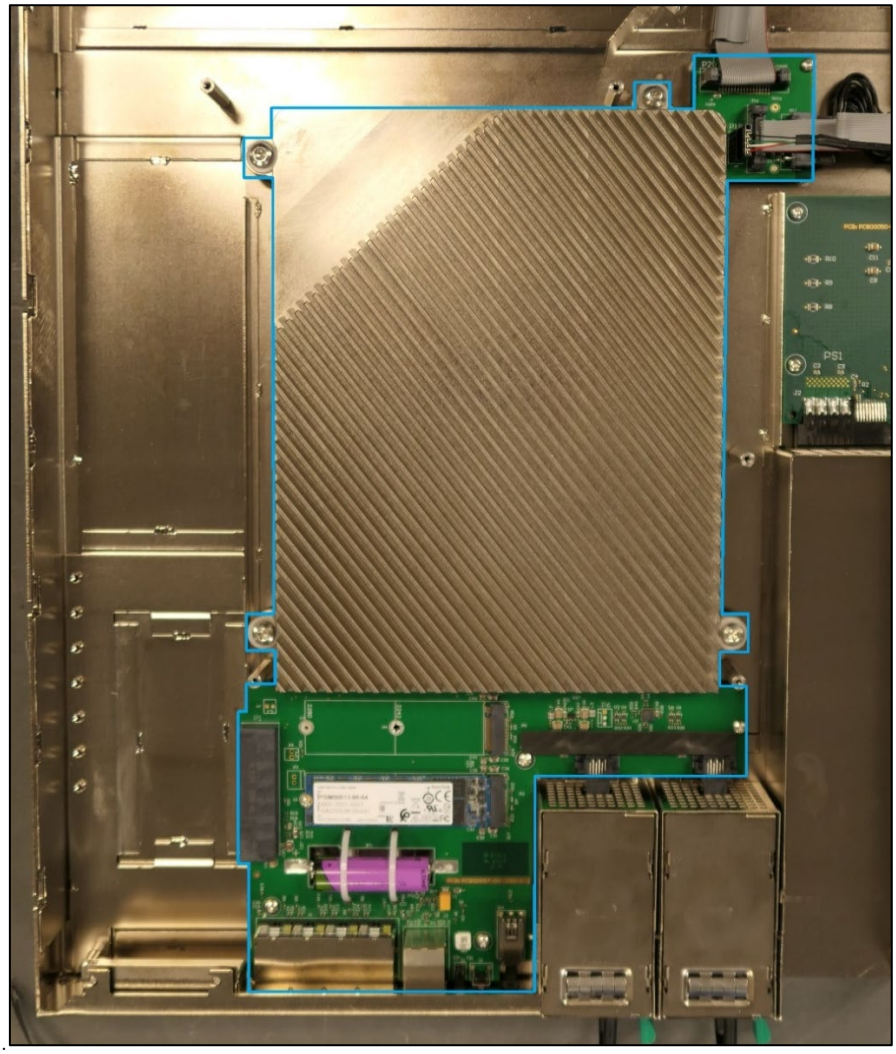

Figure 3 - TASP within a Thales Product

As shown in Figure 3, the TASP's boundary is represented as:

- A large rectangular grey metallic area in the centre of the photograph – which is the top security cover. A similar cover is fitted to the underside of the board.
- Excluded circuitry outside of the security covers performs no sensitive operations and consists of power supplies and interfacing electronics for use by a loaded application.[1]

The module always operates in the FIPS Approved mode of Operation. Its status is indicated by toggling a GPIO line to either the active, or inactive state.

[1] *"The following observable, non-security-relevant components are excluded from FIPS 140-2 requirements: Molex Headers connectors, RJ45 connector, USB connector, PCIe connector, M.2 Application Memory Connectors, M.2 NVMe Memory module (application loaded within this space is out of validation scope), USB 2.0 conditioner, supportive Passive components, Diodes, PTC Fuses, Power Distribution ICs and Battery, DC/DC Converters , Foam pad, Cable Ties, M.2 standoff, M2 screw and switch cap."*

3.2 Overall FIPS Level 3

The FIPS 140-2 security levels for the module in overall FIPS level 3 configuration are as follows:

Security Requirement	Security level
Cryptographic Module Specification	3
Cryptographic Module Ports and Interfaces	3
Roles, Service and Authentication	3
Finite State Model	3
Physical Security	3
Operational Environment	N/A
Cryptographic Key Management	3
EMI/EMC	3
Self-Tests	3
Design Assurance	3
Mitigation of Other Attacks	3
Overall FIPS level	3

Table 2 - Security Level of Security Requirements

3.3 Ports and Interfaces

The TASP interfaces are physically capable of both data input and data output, or for conveying control and status to and from the module.

The figure below shows the bootstrap part of the main Processor with the main hardware component and interfaces. The red dotted line represents the TASP's cryptographic boundary.

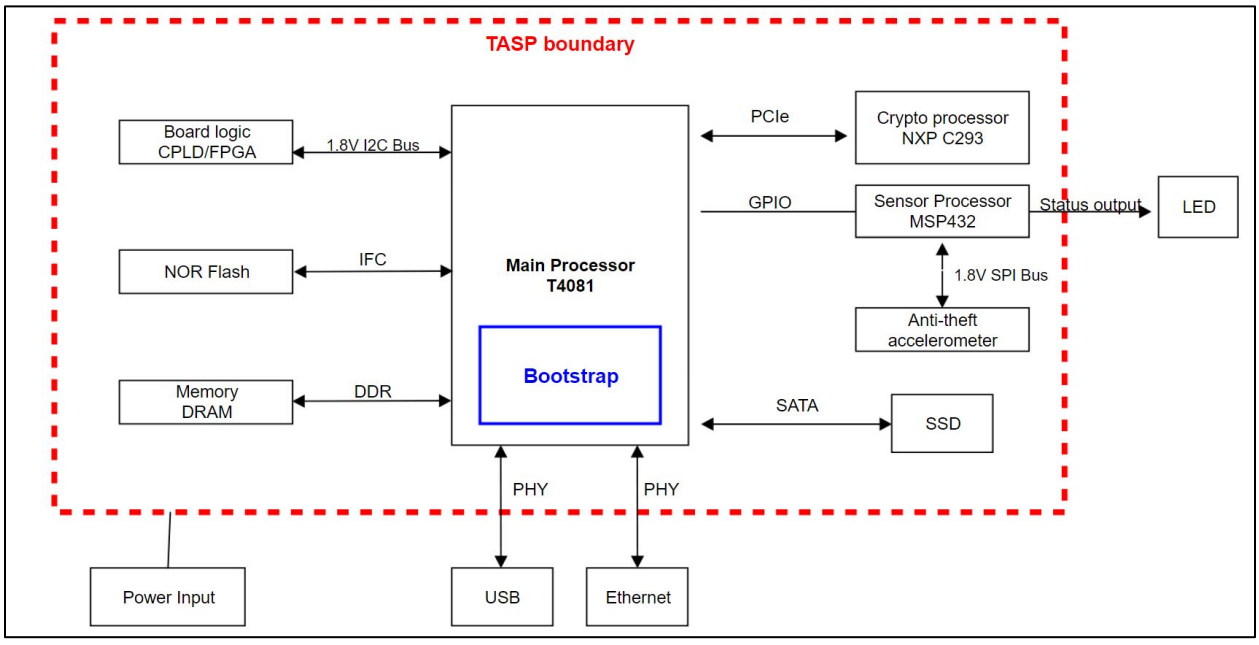

Figure 4 - Hardware Design with Bootstrap

Please see Table 3 for more details on Ports and Interfaces.

Physical Port	Qty	Logical Interface Definition	Technical Specification
USB	3	N/A	Available for use by loaded applications. Not used by TASP Bootstrap.
Ethernet	5	N/A	Available for use by loaded applications. Not used by TASP Bootstrap.
PCI Express	5	N/A	Available for use by loaded applications. Not used by TASP Bootstrap.
Board Logic	1	NA	Available for use by loaded applications. Not used by TASP Bootstrap.
Power	1	Control input Power in	Turn on/off payShield 10000. This is control input interface of the module.
GPIO	1	Status output	Provide status of the module. *

Table 3 - Ports and Interfaces Description*

*Control in, data in, and data out are available to loaded applications, but not applicable for this module.-

4. Identification and Authentication Policy

The TASP contains the Bootstrap Authentication public key, and its hash, and the hash of the Application Authentication public key. These are loaded into the module during manufacture. One key is used to authenticate the bootstrap image itself and one is used to authenticate the application image.

Authentication of public keys is provided by the secure manufacturing procedures of the vendor.

The authentication data required of the operators is their correctly signed code. This means that the authentication process is the verification of the signature on the code presented to the module (i.e., after it has been signed by the private component of the vendor's key pair). The authentication data contained in the module will be the corresponding public key and signature.

With the vendor's public key of 521 bits ECDSA key size, ECDSA with SHA-512 has an equivalent security strength of 256 bits. The possibility that a random attempt to directly use the authentication mechanism of TASP will succeed, or that a false acceptance will occur, is 1/2^256, which is significantly less than one in 1,000,000 as required by FIPS 140-2. The module supports a maximum of 20 attempts per minute using the authentication system. The probability that multiple random attempts to use the authentication mechanism during a one-minute period will succeed or that a false acceptance will occur is 20 * 1 / 2 ^256 = 20 / 2^256. This is significantly less than one in 100,000 as required by FIPS 140-2. Therefore, the authentication mechanism within the TASP is significantly stronger than the minimum required for FIPS 140-2 validation.

Other Security-Relevant Information

All aspects of the TASP's design are controlled by Thales' configuration management system.

TASP only has a FIPS Approved mode of operation. TASP uses only FIPS Approved algorithms and it does not support non-FIPS Approved algorithms. Unauthenticated firmware cannot be loaded into the module.

TASP's bootstrap is restricted to loading an application. When an application is present to be loaded, TASP's bootstrap will normally provide basic system checks and initialization, and then transfer control to the application.

The application itself, and any other firmware loaded into this module, is out of the scope of this validation and requires a separate FIPS -140-2 validation.

5. Access Control Policy

5.1 Roles

The module supports a crypto-officer role and a user role. There is no maintenance role associated with the module. The types of each Role identified for TASP are shown in the table below.

Role	Type of Authentication	Authentication Data
Crypto-Officer	Identity based	Signature Verification
User	Identity based	Signature Verification

Table 4 - Roles and Required Identification and Authentication

The strength of authentication is described in Section 4, “Identification and Authentication Policy”.

5.2 Services

The services provided by the module are described in the table below

Service	Service Input	Service Output	Description
Show Status	Perform self-tests Perform loading of signed application.	Output the status of the module	Output status of the cryptographic module: output indication whether or not the module has passed the power-up self-test, is in an error state, and whether or not the firmware load authentication was successful (see Section 5.4)
Perform Self-Tests	No input (self-test run automatically once power on).	Show status	Initiate (by power cycling) and run the self-tests (see Section 8). This service uses the ‘Bootstrap Authentication Key’ defined in section 6.1
Perform Loading of Signed Application	Once "Perform self-tests" has passed and signed application is sent to the module	Show status	Perform loading of signed applications. The FIPS authenticated firmware for loading of signed applications is normally referred to as a “bootstrap”. If an attempt is made to load an application into the module, that application must have been properly signed and there must be sufficient memory space within the TASP to store the loaded application. This service uses the ‘Application Authentication Key’ defined in section 6.1.

Table 5 – Services Provided

5.3 Services vs Roles

The module supports two types of operators: “Crypto-Officer” and “User”.

The operator will have access to the signed application that is to be loaded into the module. Procedures should be implemented to ensure that only authorized operators are allowed to access the signed application. However, the operator will not have direct access to the particular private key that has been used to sign the application. This means that the operator would not be able to sign another application and load it into the module. The signing of the application must be authorized by the vendor.

The table below describes the services and the associated roles in which the services can be performed.

Services/Roles	Crypto-Officer or User
Show Status	x
Perform Self-Tests	x
Perform Loading of Signed Application	x

Table 6 – Services and Associated Roles

In addition, the Crypto-Officer installs the module and performs the inspection (see Section 7).
TASP does not support concurrent operators. An operator cannot change roles without re-authenticating.

5.4 Module Status

The module can only be in FIPS approved mode (see Section 4). However, the module generates signal output via GPIO indicating its status.

During execution of all power on self-tests and self-authentication, and prior to bootstrap exiting after loading and verifying the next system component, a specific GPIO signal is sent as described below:

- Flashing signal to indicate booting
- Solid signal on successful completion of bootloader

The solid signal is considered as the FIPS mode "success" indicator.

If the bootloader fails:

- The module enters the error state, the solid signal is not sent, and the module sends a dual flashing signal on the GPIO.
- Depending of the type of the error, the module will either reboot or enter a hard error state. The hard error state renders the module unusable and it must be returned for service.

6. Cryptographic Functionality

6.1 Critical Security Parameters

The only cryptographic keys directly employed by the module are the public keys component of the vendor's key pairs. Disclosure of the vendor's public keys does not constitute a security risk for the module since possession of these public keys would not enable an attacker to sign applications, and thereby enter them into any TASP module.

Public Keys	Description	Size	Generation/Established	Storage	Zeroization*
Bootstrap Authentication Key	The public key, and its hash, of the key pair used for self-authentication of the bootstrap at boot time	521	Generated externally and loaded as part of the manufacturing process.	Non-volatile memory – Flash	Non-Applicable
Application Authentication Key	The public key, and its hash of the key pair used to authenticate applications loaded into the module.	521	Generated externally and loaded as part of the manufacturing process.	Non-volatile memory – Flash	Non-Applicable

Table 7 - Security Parameters

There are no passwords or PINs associated with the operation of the module.
The only other security-relevant data are the signature algorithms used by the module. These algorithms are publicly available and their disclosure would constitute no threat.
*Zeroization occurs when the key is replaced by a subsequent key.

6.2 FIPS Approved Algorithms

CAVP #	Algorithm	Standard	Details
Boot Loader			
#1156	ECDSA	FIPS 186-4	**SigVer**: CURVES (P-521: (SHA-512)) **SHS:** Val# 3829
#3829	SHA	FIPS 180-4	**SHA-512** (BYTE-only)

Table 8 - Overview of FIPS Approved Algorithms

The module does not support any non-FIPS approved or non-allowed algorithms.

7. Physical Security

7.1 Actions Required to Ensure Security is Maintained

The TASP is a multiple-chip embedded cryptographic module consisting of production grade components intended to meet FIPS 140-2 Level 3. It does not support a maintenance role and therefore security concerns arising from such a role are not relevant.

The cryptographic boundary of the TASP is physically contiguous and is defined by the two-piece metal enclosure covering all critical components on the top and underside of the module. Attempts to remove the metal enclosure result in the module becoming non-functional.

7.2 Tamper-Evident Seals

TASP's metal covers are screwed together from the underside using eight (8) screws: one in each corner, and one in each side. The heads of the four (4) screws near the edges of the bottom cover are covered by four (4) tamper-evident seals with each seal protecting one screw head. The seals are applied by the vendor during the manufacturing process. The seals are also serialized; the vendor maintains a record of the association between numbered seals and modules.

The figure below shows the correct locations for the four (4) seals on the bottom cover.

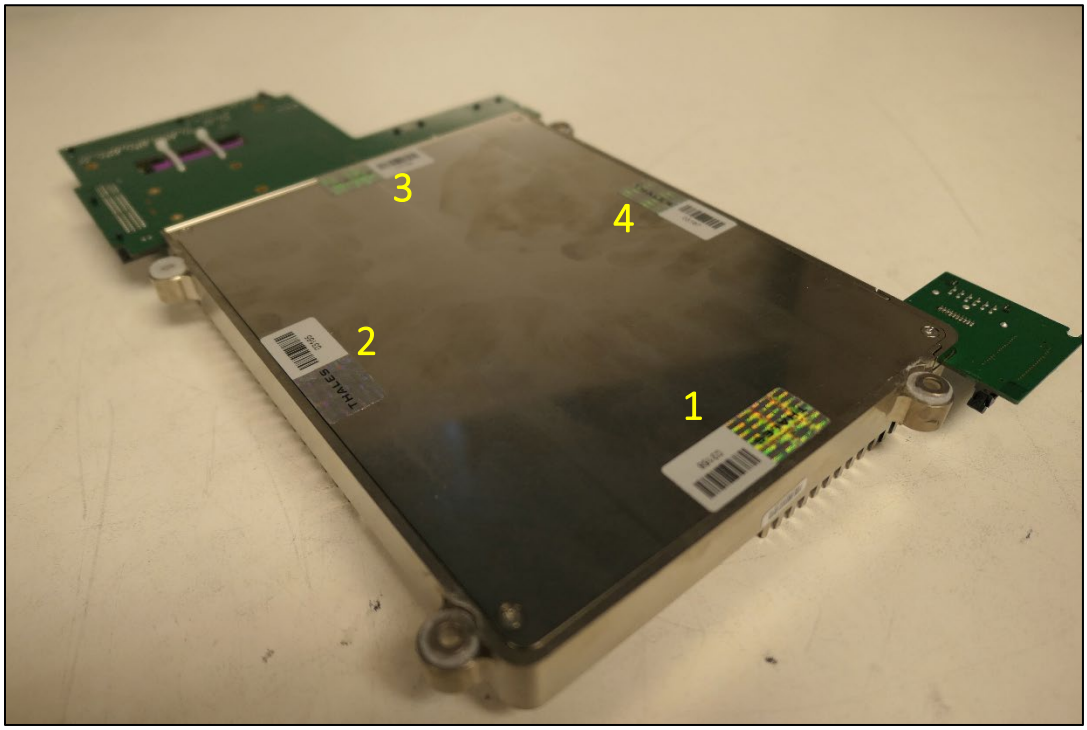

Figure 5 - Tamper-Evident Seals on Underside Bottom Cover of TASP

Each seal is fitted at the edge of the metal cover but does not overlap the outside metal part as shown in the picture below.

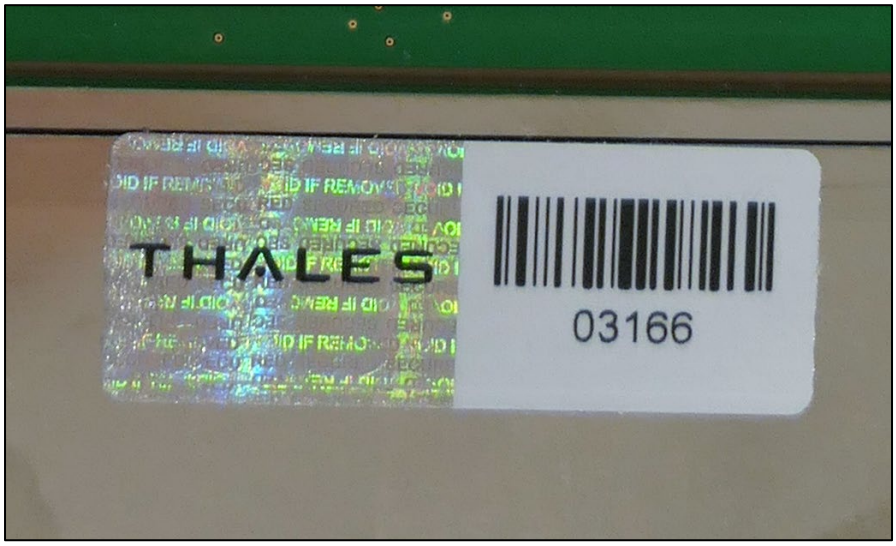

Figure 6 - Position of the Tamper-Evident Seal on Edge of TASP

Note that the above tamper-evident seal has rounded corners and has a holographic background image. If there is an attempt to remove the seal from the metal cover, the surface of the seal will discolor; and, in the darkening color, the word "VOID" will appear and will remain visible even if the seal is pressed back to the surface of the cover. Any significant damage to any seal directly above the protected screw heads may indicate attempts at tampering with the module.

The seals are designed and intended to stay in place and intact for the entire life of the module.

These seals are not the module's only system for tamper-evidence. Operators can maintain the integrity of the module by adhering to the inspection instructions of the product in which the module is embedded – which typically involves a routine annual inspection of physical integrity.

Attempting to penetrate the security cover will result in visible damage to the security cover.

If tampering is detected, the module should be returned to the manufacturer.

8. Self-Tests

8.1 Self-Tests

There is a self-test service provided by the module, which is an ECDSA test for verifying the authenticity of the bootstrap when it is loaded. This firmware integrity test is performed at start-up and can be performed on demand (i.e., during start-up after a service request to reboot the unit).

Known Answer Tests (KAT) on the elliptic curve signature verification algorithm (ECDSA) using SHA-512 is performed at power up.

8.2 Power up Test Errors

If there is an integrity test failure or KAT test failure, 1) the GPIO continuously sends the flashing signal, 2) the module enters in the error state, 3) the application won't be loaded, and 4) the system will reboot or enter in the hard error state.

8.3 Conditional Test Errors

When a signed application is sent to the module, the signature on the application is checked using the signature verification algorithm (ECDSA). If the signature verification fails, then the application is not executed, and the module enters in error state. TASP will attempt to verify a backup image, if this also fails, then TASP enters in hard error state.

9. Mitigation of Other Attacks Policy

9.1 Intrusion, Movement, Temperature and Voltage

The module contains a tamper-detection and response system. The tamper-response can be triggered by a variety of sources.

The physical security provided by the TASP operates primarily as a protection mechanism for its battery-backed RAM. If a signed application is loaded by the module, then this RAM is typically used to contain and protect that application's critical security parameters. The tamper-response protects the contents of the RAM by quickly erasing them. The module also contains non-volatile flash memory. The contents of the flash are not erased when the response is triggered, and consequently no sensitive information is stored in flash in plaintext.

Opening TASP's metal covers will produce a tamper-response. This system also includes additional facilities for other sources, external to TASP, to trigger the erasure of the contents of the battery-backed RAM and thus secure the module by deleting its non-volatile sensitive plaintext data.

The tamper-detection and response system is powered from the main power supply when this is available; but when the module is not powered this way, the system can be powered by a battery. If all power is removed, the tamper-response is triggered.

The TASP has a sensor that can detect movement. Whilst the TASP's motion detector is enabled, any significant tilting of the module is liable to trigger its tamper-response.

The TASP incorporates features enabling the module to monitor and respond to fluctuations in the operating temperature and voltage. If the internal temperature of the monitored components inside the module exceeds the predetermined range, this will trigger the tamper-response.

If any of the voltage sources supplied within the TASP surges or is actively driven above a threshold voltage level, then the tamper-response is triggered. If the voltage from the main power supply drops below the normal range, it will trigger a tamper-response. If voltage drops too low to complete power loss, the system will enter in hard error state.

NOTE: If the environmental condition that triggers the tamper-response is temporary, then the unit will reset itself following the return to the normal environmental condition. For example, if the tamper-response is triggered by a rise in temperature, then the unit will reset itself after the temperature falls. This should allow the module to function normally again; but it cannot restore the former contents of the battery-backed RAM that were erased when the tamper-response was triggered.

Moreover, beyond certain thresholds, the unit will block operation and require return to the manufacturer.

The motion detector can be either turned on or turned off and ignored as a potential trigger for the tamper-response. Other sources for triggering the tamper-response (e.g., the intrusion detection system) are permanently enabled.

When the module has been loaded with an application, it will be necessary to ensure that it is subject to appropriate protection against unauthorised use. However, such protection measures would form part of the security policy for the loaded application rather than the module itself and are therefore outside the scope of this validation.

The module also features hardware integrity and functional checks that also trigger the tamper-response when a failure is detected. These fail-safe design features are also intended to provide mitigation of attacks designed to selectively disable the module's tamper-detection and response system.

9.2 Fault Induction Attacks

Fault induction attacks make use of fluctuations in external forces to cause processing errors within a module.

The module provides protection against certain types of fault induction attack. The module contains a temperature sensor and a mechanism to detect abnormal voltage variations.

The temperature sensor and the abnormal voltage detection mechanism will not require any further action on the part of the user or crypto-officer. If either of these sources triggers a tamper-response, then the module will automatically protect the contents of the battery-backed RAM by quickly erasing them.

There are no conditions under which the temperature and abnormal voltage detection mechanisms are known to be ineffective.

Addresses

Americas

900 South Pine Island Road, Suite 710, Plantation, Florida 33324, USA
Tel: +1 888 744 4976 or + 1 954 888 6200
sales@thalesesec.com

Europe, Middle East, Africa

Meadow View House, Long Crendon, Aylesbury, Buckingamshire HP18 9EQ, UK
Tel: + 44 (0)1844 201800
emea.sales@thales-esecurity.com

Asia Pacific

Units 4101, 41/F. 248 Queen's Road East, Wanchai, Hong Kong, PRC
Tel: + 852 2815 8633
asia.sales@thales-esecurity.com

Internet Addresses

Website:	https://www.thalesgroup.com/
Support:	https://www.thalesesecurity.com/services/support
Online documentation:	https://www.thalesesecurity.com/resources