Secure Generic Sub-System (SGSS) Version 3.3

Security Policy

Thales e-Security
4th/5th Floors
149 Preston Road
Brighton
BN1 6AS

Tel: +44 (0)1273 384600
Fax: +44 (0)1273 384601

FIPS 140-2 Non-proprietary Security Policy

Contents

1. Glossary

CA	Certificate Authority
EDC	Error Detection Code
FPGA	Field Programmable Gate Array
KAT	Known Answer Test
SGSS	Secure Generic Sub-System

2. Related documents

FIPS140-2	Federal Information Processing Standards Publication, Security Requirements for Cryptographic Modules
FIPS180-1	Secure Hash Standard (SHS)
FIPS186-2	Digital Signature Standard (DSS)
1270A301	SGSS User Guide

3. Introduction

This document is a security policy for the Secure Generic Sub-System (SGSS), version 3.3.

The SGSS module is a multi-chip embedded cryptographic module providing functionality for the secure loading and/or upgrading of applications using the SGSS application. The SGSS is a FIPS 140-2 Security Level 3 module (Ref: FIPS140-2).

The module ensures the integrity of any application that is loaded into itself. It will only allow an application to be loaded if it has been signed by a private key that has been generated by the Certificate Authority (CA). The signature is verified using a FIPS-Approved signature verification algorithm and the public key corresponding to the private key. The Approved algorithm and the public key are securely stored in the module. This procedure ensures that only correctly signed applications can be loaded into the module.

The module implements the following FIPS-Approved algorithms:
DSA (Ref: FIPS186-2)
SHA-1 (Ref: FIPS180-1)

SHA-1 is used as the hash function for the DSA signature verification algorithm.

If a new SGSS bootstrap application is loaded the replacement bootstrap application must be FIPS 140-2 validated. Only bootstrap applications were included in the FIPS 140-2 testing and validation. However loaded, applications that are FIPS 140-2 validated will run in Approved mode.

The SGSS uses only Approved algorithms and does not support non-Approved algorithms. Therefore the SGSS has only an Approved mode of operation.

In normal operation a user of the module need not be aware of the existence of the SGSS bootstrap. The bootstrap is restricted to configuration and maintenance tasks such as reading and updating configuration information and erasing or updating the loaded application.

When an application is present, the SGSS bootstrap will provide basic system initialisation and transfer control to the application. The application is provided with an interface to the bootstrap via the trap 15 instruction.

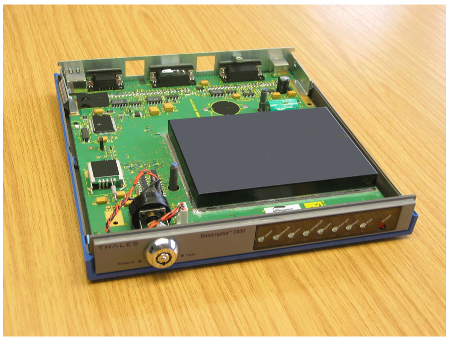
The module is protected by physical security provided by the SGSS tamper resistant alarm circuit and by the external module casing. The circuitry within the module is potted in a hard opaque potting material.

The following page shows the SGSS as a component of the P3™ Cryptographic Module, HSM 8000, WebSentry™ (Ethernet and PCI card versions) and the Datacryptor® 2000. In each photograph the SGSS is the large oblong. It is black in the first four pictures and grey in the fifth. (The external casing of the SGSS module is black for the P3™ Cryptographic Module, HSM 8000, WebSentry™ Ethernet and the Datacryptor® 2000. The external casing is grey for the WebSentry™ PCI card.)

P3™ Cryptographic Module

HSM 8000

WebSentry™ Ethernet



Datacryptor® 2000

THALES e-SECURITY
Model: WebSentry™ PCI
Serial Number:
A3120000010U
Part No: 1600A312
WARNING
This product is tamper resistant. Any attempt to gain access will result in the erasure of its contents and will invalidate all warranties.
Made in the EU
Update: A[ ] B[ ] C[ ] D[ ] E[ ] F[ ]
Label No: 1227B143

WebSentry™ PCI card

4. Identification and Authentication Policy

There are two roles associated with the module. These are the crypto-officer role and the user role. There is no maintenance role associated with the module.

The crypto-officer role involves the loading of a public key certificate into the module at the factory. The public key certificate is used by the module to verify the signature on any application that it loads.

An authorised crypto-officer performs the loading of the public key certificate at the factory.

Once the module is fielded, new applications may be generated at the plant and signed using the private key that is held securely at the factory. (Security at the factory is provided by procedural controls.) In the field the user, acting on behalf of the factory, may load the signed application into the module where the signature is verified using the public key certificate. This is the only cryptographic application offered by the module's software. Details on how to perform the user role securely are contained in the document SGSS User Guide (Ref: 1270A301).

Authentication of the crypto-officer is provided by secure manufacturing procedures at the factory.

The authentication data required of the user is the correctly signed application code. This means that the user's authentication data is effectively the private component of the CA key pair. The authentication data contained in the module will be the corresponding public key and signature algorithm.

The only identity associated with the module is that of the factory. The crypto-officer, acting on behalf of the factory, initialises the module by inserting the public key certificate into the module. The user, also acting on behalf of the factory, loads a signed application in the field. The signature on the application therefore identifies and authenticates the factory.

The corresponding strength of the authentication mechanism depends on the size of the private key space associated with the FIPS-Approved algorithm (DSA using SHA-1) used for generating and verifying the digital signatures. Since the module uses only these FIPS-Approved algorithms (see http://csrc.nist.gov/cryptval/) the size of the key space provides an extremely high level of security for the authentication mechanism. This is shown by the following mathematical argument.

Let x be the size of a private key space used in DSA. Then $x > 2^{159} > 1000000$, so that $1/x < 1/1000000$. It follows that

- the probability that a random attempt to use the authentication mechanism will succeed or that a false acceptance will occur is (significantly) less than one in 1,000,000
- the probability that multiple attempts to use the authentication mechanism during a one-minute period will succeed or that a false acceptance will occur is (significantly) less than one in 100,000.

4.1 Other Security-Relevant Information

FIPS Approved Mode of Operation

The SGSS only has an Approved mode of operation. The following conditions must be satisfied to achieve the FIPS 140-2 Level 3 Approved mode.

FIPS 140-2 Approved security methods are used

The following method must be used:

- DSA/SHA-1 (FIPS Certificate #24)

5. Access Control Policy

5.1 Roles

As already discussed the module supports a crypto-officer and a user role. There is no maintenance role associated with the module.

5.2 Services

The only cryptographic service provided by the module is the loading of signed applications. The user will be able to load an application into the module provided that the application is properly signed and there is sufficient memory space in the SGSS to store the loaded application.

In addition to the loading of signed applications authorised users may also perform the following non-sensitive services:

- Echo (Echoes back an input string)
- Erase application (Erases application)
- Get version (Provides SGSS version number)
- Get CA name (Provides name of CA (factory) which generated public/private key pair)
- Read/Write application configuration (Provides/selects current configuration)
- Reboot unit (Resets the module)
- Set comms baud rate (Sets the communication rate)
- Get date/time (from the real-time clock)
- Read/write to/from unused FLASH (for storage of semi-permanent application data)
- Get CA (read CA properties)

The self-test services provided by the module are an Error Detection Code (EDC) test for validating the bootstrap application, and known answer tests (KATs) on the signature verification algorithm (DSA).

5.3 Cryptographic Keys and Other CSPs

The only cryptographic key directly employed by the module is the public key component of the CA key pair. This is stored in the flash in the SGSS in plaintext form and is protected by the physical security mechanisms associated with the SGSS. This CA public key never leaves the SGSS. Disclosure of the CA public key does not constitute a security risk for the module since possession of the public key would not enable an attacker to sign applications and thereby enter them into the module.

CA private keys are not directly employed by the module. They are used to sign an application that is to be loaded into the module. CA private keys are never loaded into the module and are stored securely with the manufacturer’s factory.

There are no passwords or PINs associated with the operation of the module.

The only other security-relevant data are the Approved signature algorithms used by the module.

These algorithms are publicly available and their disclosure would constitute no threat.

5.4 Services that Operators are Authorised to Perform (within each Role)

The crypto-officer is authorised to load the public key certificate into the module at the factory.

The user is authorised to perform the application-loading service provided by the module.

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

The user is also authorised to perform other services provided by the module (see Section 5.2 above).

6. Physical Security Policy

6.1 Actions Required to Ensure Security is Maintained

The SGSS is a tamper-resistant 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 SGSS is potted with a hard epoxy resin that is opaque within the visible spectrum. The potted module is contained in a hard, solid copper shell. These components provide the module's tamper evidence. The components should be inspected for evidence of tamper. The physical security mechanism described above uses passive techniques and therefore no testing of the mechanism is required.

7. Error Responses

7.1 Power-Up Test Errors

At power-up the SGSS automatically validates the integrity of its application using an EDC algorithm. If the integrity of the application is validated then the SGSS performs a known answer test (KAT) on the signature verification algorithm (DSA).

If the EDC test or either of the KAT tests fails, an error message is logged and then the module reboots itself.

7.2 Conditional Test Errors

When a signed application is loaded then the signature on the application is checked using the signature verification algorithm (DSA). If the verification fails then the application is not loaded into the unit and the SGSS outputs an error message to indicate that the signature verification was unsuccessful.

8. Mitigation of Other Attacks Policy

8.1 Movement, Temperature, Voltage and Intrusion Alarms

The module contains a tamper resistant intrusion detection system that surrounds the secure area. This intrusion detection system is an input to the alarm circuit and cannot be disabled.

The physical security provided by the SGSS operates as a protection mechanism for the RAM, FPGA and Coldfire processor. When there is only a bootstrap present the intrusion detection system serves no useful function. However if a certified application is loaded in the module then the RAM and FPGA are used to contain critical security parameters and as such require protection. The alarm circuit protects the contents of the RAM and cipher FPGA by erasing them if an attempt is made to access the secure area. The contents of the flash are not erased when the alarm is triggered and consequently no sensitive information is stored in flash.

The intrusion detection system consists of two circuits: a continuity circuit and a guard circuit. These two circuits are wrapped around the secure area and then potted in a hard opaque resin.

The alarm is triggered if the continuity circuit is broken or if the two circuits are bridged. Any attempt to access the secure area by cutting or drilling would result in the alarm circuit being triggered by either breaking the continuity circuit or bridging the two circuits. The circuits are bonded to the resin so that any attempt to gain access by forcibly removing the resin will break the continuity circuit and hence trigger the alarm. Any attempt to dissolve the resin will damage the circuits and trigger the alarm.

The alarm circuit is powered from the main power supply when this is available, but if the module is not powered up then it is powered by a battery. The battery is mounted outside the SGSS. If the battery is disconnected or fails the alarm triggers. This ensures that the module’s tamper response and zeroization circuitry is operational at all times.

In addition to the alarm circuit the SGSS has a sensor that detects movement. Any abnormal movement of the module will trigger the motion alarm.

As well as providing tamper resistance the SGSS incorporates environmental failure protection features enabling the module to monitor and respond to fluctuations in the operating temperature and voltage. If the temperature moves outside a predetermined range (-5°C to 60°C) a temperature sensor causes the alarm to be triggered. Similarly if the voltage on the +5v rail surges or is actively driven above the normal level then the alarm is triggered, and if the voltage drops below the normal level then the module shuts down.

In addition to zeroizing all CSPs the effect of triggering the alarm is that the supply rails to the RAM, the cipher FPGA and the ColdFire microprocessor are clamped to ground. This process is much faster than simply removing power from the devices. Additionally the interface lines are disconnected.

If the alarm condition is temporary then the unit will reset itself following removal of the alarm condition. For example if the alarm is triggered by a rise in temperature then the unit will reset itself after the temperature falls.

In some circumstances the triggering of the alarm will be permanent, i.e. the unit will not be able to reset itself due to the persistence of the alarm condition. This would happen, for example, if the alarm circuit were triggered by an intrusion attack. In this case the unit must be returned to the factory for the alarm to be reset.

Both the movement alarm and the temperature alarm can be turned on or off. Before an application has been loaded (i.e. when only the bootstrap application is present) the temperature alarm is enabled and the motion alarm is disabled. The other alarms (i.e. the intrusion detection system and the voltage alarm) are permanently enabled.

The movement alarm and the temperature alarm were not tested as part of the FIPS 140-2 Level 3 validation.

After the security settings have been decided upon (e.g. whether to enable or disable the motion sensor) the physical security mechanisms provided by the SGSS will not require any action on the part of the operator: the module is designed for use in an insecure domain. An attempt to breach security will result in automatic disabling of the module’s functionality.

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 a security policy for the module.

8.2 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 can be enabled or disabled by the user. The user must enable the temperature alarm in order to provide constant protection against a fault induction attack utilising temperature extremes.

The temperature sensor (if enabled) and the outside range voltage sensor will not require any further action on the part of the operator. If either of these alarms is triggered then the module’s functionality will be automatically disabled.

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