

---

# HSM Proxy Security Analysis

Version 0.5.1

Frank Cornelis

Copyright © 2013 FedICT

## Abstract

This document delivers the result of a security analysis on the HSM Proxy product. Although we don't declare any Commons Criteria [CCPART1] conformance, we use the CC terminology and methodology for the security analysis of the HSM Proxy product.

1. Security Target .....	2
1.1. Security Target Introduction (ASE_INT) .....	2
1.2. Conformance claims .....	2
1.3. Security Problem Definition (ASE_SPD) .....	2
1.4. Security Objectives (ASE_OBJ) .....	4
1.5. Extended Components Definition (ASE_ECD) .....	6
1.6. Security Requirements (ASE_REQ) .....	6
1.7. TOE Summary Specification .....	9
2. Security Target Evaluation .....	11
2.1. Introduction .....	11
2.2. Evaluation .....	11
2.3. Results of the evaluation .....	12
2.4. Conclusions and recommendations .....	12
2.5. List of evaluation evidence .....	12
3. TOE Evaluation .....	12
3.1. Introduction .....	13
3.2. Architectural description of the TOE .....	13
3.3. Evaluation .....	13
3.4. Results of the evaluation .....	13
3.5. Conclusions and recommendations .....	13
3.6. List of evaluation evidence .....	13
A. References .....	13
B. HSM Proxy Security Analysis License .....	13
C. HSM Proxy Project License .....	13



## Work in progress

Please notice that this security analysis is not yet complete.

# 1. Security Target

This Security Target is compliant with [CCPART1] and [CCPART2] .

## 1.1. Security Target Introduction (ASE\_INT)

This document is the Security Target (ST) for the HSM Proxy version 0.5.1 product.

### 1.1.1. ST Reference

HSM Proxy 0.5.1 Security Target

### 1.1.2. Target Of Evaluation (TOE) Reference

HSM Proxy 0.5.1 product.

### 1.1.3. TOE Overview

See HSM Proxy Product Overview document [HSM-OVERVIEW] .

### 1.1.4. TOE Description

TOE type: Hardware Security Module

The HSM Proxy offers two interfaces:

- Via the Administrator portal, administrators can configure the HSM Proxy. Only authorized administrators can utilize this portal.
- Via the web service, applications can connect to the HSM Proxy and create signatures using their assigned (HSM) keys. Only authenticated and authorized applications can create signatures via the HSM Proxy web service.

Non-TOE hardware/software/firmware requirements by the TOE as well as the physical scope can be found in [HSM-INSTALL] .

## 1.2. Conformance claims

This Security Target is CC Part 2 [CCPART2] conformant and CC Part 3 [CCPART3] conformant for EAL1.

No conformance claim to a Protection Profile is made of the HSM Proxy product.

## 1.3. Security Problem Definition (ASE\_SPD)

This part of the ST provides the security problem definition, which defines the security problem the TOE and its operational environment is intended to address. This this end, it specifies:

- the threats that the TOE and its operational environment must counter,

- the assumptions made about the operational environment.

### 1.3.1. Threats

This section defines the threats, along with the threat agents.

T.DATA	Unauthorized Access to Resources. A user obtains unauthorized access to data resources via the web service interface of the TOE.
T.RESIDUAL_DATA	A user may gain unauthorized access to data through reconfiguration of Security Attributes.
T.ACCESS	Unauthorized Access to Security Attributes. A user obtains unauthorized access to security attributes via the web service interface of the TOE.
T.ATTACK	Undetected Attack. An undetected compromise of IT assets occurs as a result of an attacker attempting to perform actions, which the individual is not authorized to perform, via the web service interface of the TOE.
T.INTEGRITY	Modification of data in transit. An attacker modifies data in transit between a user and the TOE.
T.UNKNOWN_STATE	When the TOE is initially started or restarted after a failure, the security state of the TOE may be unknown.

In addition, the following threats are countered by the Operational Environment.

TE.OPERATE	Insecure Operation. Compromise may occur because of improper configuration and/or administration.
------------	---

### 1.3.2. Organizational Security Policies

There are no organizational security policies with which the TOE must comply.

### 1.3.3. Assumptions

This part of the security problem definition scopes the security problem by identifying what aspects of the operational environment are taken to be axiomatic.

A.TOE.CONFIG	The TOE is installed, configured, and managed in accordance with its evaluated configuration described in.
A.PHYSICAL	It is assumed that the IT environment provides the TOE with appropriate physical security, commensurate with the value of the IT assets protected by the TOE.
A.HTTPS	The underlying system ensures that only appropriately encrypted communications reach the TOE from the user community.

A.NETWORK                      The security-critical software of the TOE and the underlying system (including network services) are logically protected using firewall technology which prevent unauthorized network access.

### 1.4. Security Objectives (ASE\_OBJ)

This part of the ST defines the security objectives that the TOE and its operational environment must achieve in order to fully solve the security problem defined in [Section 1.3, “Security Problem Definition \(ASE\\_SPD\)”](#).

#### 1.4.1. Security Objectives for the TOE

This section defines the security objectives that the TOE is expected to achieve, in order to solve its part of the security problem.

O.I&A	The TOE must uniquely identify all users, and must authenticate the claimed identity before granting the user access to the system.
O.ACCESS	The TOE must prevent unauthorized access to resources and security attributes protected by the product.
O.ADMIN	The TOE must provide functionality which enabled an authorized administrator to effectively manage access to the TOE and its data, and will ensure that only authorized Administrators are able to access such functionality.
O.CRYPTO	The TOE must protect communications between itself and the users so that data in transit is not eavesdropped, modified, or replayed.
O.AUDIT	The TOE must provide the means of generating records of security relevant events in sufficient detail to help an administrator of the TOE to detect user queries that subvert the configured TOE security policy.

#### 1.4.2. Security Objectives for the operational environment

This section defines the security objectives that the operational environment is expected to achieve, in order to solve its part of the security problem.

OE.ADMIN	The underlying system must provide functions to enable an authorized administrator to effectively manage the TOE and its security functions, ensuring that only authorized Administrators can access such functionality.
OE.PORTS	The underlying system is locked down such that only necessary logical access points to its constituent components are exposed.

OE.NETWORK	The underlying system provides firewall technology where necessary to ensure that direct network attack on the TOE is prevented.
OE.SSL	The underlying system provides SSL where necessary to ensure that communications with the TOE are encrypted.
OE.INSTALL	The TOE is delivered, installed, managed and operated in accordance with the operational documentation of the TOE.
OE.PHYSICAL	Those responsible for the TOE must ensure that those parts of the TOE and the underlying system that are critical to the security policy are protected from physical attack.
OE.TRUST	Those responsible for the TOE must ensure that only users, who can be trusted to perform administrative duties with integrity, have privileges to do so.

### 1.4.3. Security Objectives Rationale

This section contains the security objectives rationale demonstrating that, if all the security objectives stated in [Section 1.4, “Security Objectives \(ASE\\_OBJ\)”](#) are achieved, the security problem as defined in [Section 1.3, “Security Problem Definition \(ASE\\_SPD\)”](#) is solved.

The [Table 1, “Suitability to counter the threats”](#) demonstrates that the TOE security objectives, in conjunction with the security objectives for the environment, are suitable to counter each of the threats.

**Table 1. Suitability to counter the threats**

Threat	Objective	Justification
T.DATA	O.I&A	Prevents unauthorized users from accessing the TOE.
	O.ACCESS	Prevents unauthorized access to security attributes that protect and resources that store TOE assets.
T.RESIDUAL_DATA	O.ACCESS	Changed security attributes should instantly reflect in assigned user authorizations.
T.ACCESS	O.I&A	Prevents unauthorized access to security attributes that protect the TOE assets.
	O.ACCESS	Prevents unauthorized access to security attributes that protect and resources that store TOE assets.
	O.ADMIN	Administrators must be able to configure the security attributes.

Threat	Objective	Justification
T.ATTACK	O.AUDIT	Provides user accountability by storing information about security events pertinent to attack detection.
T.INTEGRITY	O.CRYPTO	Protects data in transit from unauthorized modification.
	OE.SSL	Protects data in transit from unauthorized modification.
T.UNKNOWN_STATE	OE.INSTALL	Administrator trust booting must be performed as described in the TOE documentation.
TE.OPERATE	OE.INSTALL	Ensures that the underlying system is securely configured.

The [Table 2, “Suitability to uphold the assumptions”](#) demonstrates that the security objectives for the operational environment are suitable to uphold each of the assumptions.

**Table 2. Suitability to uphold the assumptions**

Assumption	Objective	Justification
A.TOE.CONFIG	OE.ADMIN	Underlying system enables only Administrators to install and configure the TOE.
	OE.INSTALL	Self evident
	OE.TRUST	Self evident
A.PHYSICAL	OE.PHYSICAL	Self evident
A.HTTPS	OE.SSL	Self evident
A.NETWORK	OE.NETWORK	Self evident
	OE.PORTS	Self evident

## 1.5. Extended Components Definition (ASE\_ECD)

## 1.6. Security Requirements (ASE\_REQ)

This part of the ST defines the security requirements that the TOE must meet in order to achieve the corresponding TOE security objectives defined in [Section 1.4, “Security Objectives \(ASE\\_OBJ\)”](#). The Security Requirements are divided in to Security Functional Requirements (SFRs) and Security Assurance Requirements (SARs).

### 1.6.1. Security Functional Requirements (SFRs)

This section contains the Security Functional Requirements (SFRs). As required by the CC these are constructed, where possible, using the security functional components as defined in [CCPART2]. In the instantiation of these functional components we use the following convention:

- **Assignment:** indicated with bold text
- Selection: indicated with underlined text
- *Refinement:* additions indicated with italic, deletions indicated with ~~strike-through~~ .
- Iteration: indicated with typical CC requirement naming followed by a lower case letter for each iteration.

### 1.6.1.1. Class FAU: Security Audit

#### 1.6.1.1.1. FAU\_GEN.1: Audit data generation

FAU\_GEN.1.1                      The TSF shall be able to generate an audit record of the following auditable events:

- Start-up and shutdown of the audit functions;
- All auditable events for the minimum level of audit; and

FAU\_GEN.1.2                      The TSF shall record within each audit record at least the following information:

- Date and time of the event, type of event, subject identity (if applicable), and the outcome (success or failure) of the event; and
- For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST, **unsuccessful use of the authentication mechanism (as required by FIA\_UAU.2)** .

#### 1.6.1.1.2. FAU\_GEN.2: User identity association

FAU\_GEN.2.1                      For audit events resulting from actions of identified users, the TSF shall be able to associate each auditable event with the identity of the user that caused the event.

### 1.6.1.2. Class FDP: User data protection

#### 1.6.1.2.1. Application Access Policy

FDP\_ACC.1.1a                      The TSF shall enforce the **Application Access Policy** on

- **all applications;**
- **the private keys; and**

	<ul style="list-style-type: none"><li>• the usage of these private keys for signing purposes.</li></ul>
FDP_ACF.1.1a	<p>The TSF shall enforce the <b>Application Access Policy</b> to objects based on the following:</p> <ul style="list-style-type: none"><li>• the authorized application identity;</li><li>• access permission associated with the application</li></ul>
FDP_ACF.1.2a	<p>The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed:</p> <ul style="list-style-type: none"><li>• if the application requesting access is denied access, then access is denied;</li><li>• if the application requesting access has no permission to use the requested application key, then access is denied.</li></ul>
FDP_ACF.1.3a	<p>The TSF shall explicitly authorise access of subjects to objects based on the following additional rules:</p> <ul style="list-style-type: none"><li>• if the application has permissions to use the requested application key.</li></ul>
FDP_ACF.1.4a	<p>The TSF shall explicitly deny access of subjects to objects based on the following additional rules:</p> <ul style="list-style-type: none"><li>• TODO</li></ul>

### 1.6.1.2.2. Administrator Access Policy

FDP_ACC.2.1b	<p>The TSF shall enforce the <b>Administrator Access Policy</b> on</p> <ul style="list-style-type: none"><li>• web users; and</li><li>• web server content.</li></ul> <p>and all operations among subjects and objects covered by the SFP.</p>
FDP_ACC.2.2b	<p>The TSF shall ensure that all operations between any subject controlled by the TSF and any object controlled by the TSF are covered by an access control SFP.</p>



### 1.6.1.3. Class FIA: Identification and authentication

#### 1.6.1.3.1. FIA\_UAU.2: User authentication before any action

FIA\_UAU.2.1                      The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.

#### 1.6.1.3.2. FIA\_UID.2: User identification before any action

FIA\_UID.2.1                      The TSF shall require each user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user.

#### 1.6.1.4. FPT\_STM.1: Reliable time stamps

FPT\_STM.1.1                      The TSF shall be able to provide reliable time stamps.

### 1.6.2. Security Assurance Requirements (SARs)

The target evaluation assurance level for the product is not yet determined.

### 1.6.3. Security Requirements Rationale

This section demonstrates that, if the TOE meets all the stated SFRs, then all TOE security objectives will be achieved.

**Table 3. Suitability to achieve the security objectives**

Objective	SFR(s)	Justification
O.I&A	FIA_UAU.2	Requires successful authentication before allowing TOE access to users.
	FIA_UID.2	Requires successful identification before allowing TOE access to users.
O.ACCESS	FAU_GEN.1	Ensures that an audit record is generated for each detection of a possible security breach.
O.AUDIT	FAU_GEN.2	Ensures that users are held accountable for their actions.
	FPT_STM.1	Provides a trusted source of time for auditing purposes.

## 1.7. TOE Summary Specification

### 1.7.1. TOE Security Functions

Listed below are the Security Functions provided by the TOE (TSFs). These TOE Security Functions are grouped in three categories:

- Identification and Authentication
- Discretionary Access Control
- Accountability and Audit

### 1.7.1.1. Identification and Authentication

#### 1.7.1.1.1. Web service identification and authentication (SF.I&A.1)

The HSM Proxy version 0.5.1 web service provides identification and authentication of the connecting application instances.

The web service has been secured as specified in [HSM-WS-SPECS] .

#### 1.7.1.1.2. Administrator portal identification and authentication (SF.I&A.2)

The HSM Proxy version 0.5.1 administrator portal provides identification and authentication of the connecting users using the Belgian eID card.

### 1.7.1.2. Accountability and Audit

#### 1.7.1.2.1. Audit (SF.AUDIT)

The HSM Proxy version 0.5.1 provides security audit functionality. Start-up and shutdown of the audit functions generates audit records. An unsuccessful authentication of applications or administrators generates an audit record. The Administrator can view the security audit.

## 1.7.2. TOE Security Functions Rationale

This section demonstrates the suitability of the TOE Security Functions to address the Security Functional Requirements.

**Table 4. SFR to SF Rationale**

SFR		TSF	Rationale
FIA_UAU.2	FIA_UAU.2.1	SF.I&A.1, SF.I&A.2	SF.I&A.1 fully implements this SFR for the web service interface. SF.I&A.2 fully implements this SFR for the administrator portal interface.
FIA_UID.2	FIA_UID.2.1	SF.I&A.1, SF.I&A.2	SF.I&A.1 fully implements this SFR for the web service interface. SF.I&A.2 fully implements this SFR for the administrator portal interface.
FAU_GEN.1	FAU_GEN.1.1	SF.AUDIT	SF.AUDIT implements start-up and shutdown audit recording of the audit system. SF.AUDIT implements audit generation of unsuccessful authentication attempts.

SFR		TSF	Rationale
FAU_GEN.2	FAU_GEN.2.1	SF.AUDIT	SF.AUDIT implements accountability of user actions.

## 2. Security Target Evaluation

This part contains the Evaluation Technical Report (ETR) of the Security Target according to [CCCEM] .



### Non-compliant CC evaluation

Although we use the same terminology and structure as set by [CCCEM] , please keep in mind that the evaluation has not been performed by a compliant evaluation facility.

### 2.1. Introduction

Evaluated Security Target: [Section 1, “Security Target”](#) .

ETR configuration control identifier: HSM Proxy ST Evaluation 0.5.1.

Identity of the developer: FedICT

Identity of the sponsor: FedICT

Identity of the evaluator: FedICT

### 2.2. Evaluation

The evaluation methodology in this section is based on chapter 10 of [CCCEM] .

#### 2.2.1. ST introduction (ASE\_INT)

**Table 5. Evaluation results**

Assurance Component	Action	Result
ASE_INT.1	ASE_INT.1.1E	PASS
	ASE_INT.1.2E	PASS

#### 2.2.2. Conformance claims (ASE\_CCL)

**Table 6. Evaluation results**

Assurance Component	Action	Result
ASE_CCL.1	ASE_CCL.1.1E	FAIL. Cannot claim conformance.

### 2.2.3. Security problem definition (ASE\_SPD)

**Table 7. Evaluation results**

Assurance Component	Action	Result
ASE_SPD.1	ASE_SPD.1.1E	PASS

### 2.2.4. Security objectives (ASE\_OBJ)

**Table 8. Evaluation results**

Assurance Component	Action	Result
ASE_OBJ.1	ASE_OBJ.1.1E	PASS
ASE_OBJ.2	ASE_OBJ.2.1E	PASS

### 2.2.5. Extended components definition (ASE\_ECD)

**Table 9. Evaluation results**

Assurance Component	Action	Result
ASE_ECD.1	ASE_ECD.1.1E	?
	ASE_ECD.1.2E	?

### 2.2.6. Security requirements (ASE\_REQ)

**Table 10. Evaluation results**

Assurance Component	Action	Result
ASE_REQ.1	ASE_REQ.1.1E	FAIL
ASE_REQ.2	ASE_REQ.2.1E	FAIL

## 2.3. Results of the evaluation

FAIL

## 2.4. Conclusions and recommendations

## 2.5. List of evaluation evidence

## 3. TOE Evaluation

This part contains the Evaluation Technical Report (ETR) of the TOE according to [CCCEM] .

### 3.1. Introduction

### 3.2. Architectural description of the TOE

### 3.3. Evaluation

### 3.4. Results of the evaluation

FAIL

### 3.5. Conclusions and recommendations

### 3.6. List of evaluation evidence

## A. References

[CCPART1] *Common Criteria for Information Technology Security Evaluation - Part 1: Introduction and general model* . Version 3.1, Revision 4.

[CCPART2] *Common Criteria for Information Technology Security Evaluation - Part 2: Security functional components* . Version 3.1, Revision 4.

[CCPART3] *Common Criteria for Information Technology Security Evaluation - Part 3: Security assurance components* . Version 3.1, Revision 4.

[CCCEM] *Common Criteria for Information Technology Security Evaluation - Evaluation methodology* . Version 3.1, Revision 4.

[HSM-OVERVIEW] *HSM Proxy Product Overview* . Version 0.5.1 .

[HSM-INSTALL] *HSM Proxy Installation Manual* . Version 0.5.1 .

[HSM-ADMIN] *HSM Proxy Administrator Manual* . Version 0.5.1 .

[HSM-WS-SPECS] *HSM Proxy Web Service Specifications* . Version 0.5.1 .

## B. HSM Proxy Security Analysis License



This document has been released under the [Creative Commons 3.0](http://creativecommons.org/licenses/by-nc-nd/3.0/) [http://creativecommons.org/licenses/by-nc-nd/3.0/] license.

## C. HSM Proxy Project License

The HSM Proxy Project source code has been released under the GNU LGPL version 3.0.

This is free software; you can redistribute it and/or modify it under the terms of the GNU Lesser General Public License version 3.0 as published by the Free Software Foundation.

This software is distributed in the hope that it will be useful, but WITHOUT ANY WARRANTY; without even the implied warranty of MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the GNU Lesser General Public License for more details.

You should have received a copy of the GNU Lesser General Public License along with this software; if not, see <http://www.gnu.org/licenses/>.