HARDWARE SECURITY MODULE AS A SERVICE (HSMAAS) - EXECUTIVE SUMMARY REPORT

Prepared by	HSMAAS Team
Document Type	ESR
Reference	ESA-DOPS-STU-ESR-0001
Issue/Revision	1 / 2
Date of Issue	2023-12-04
Status	FINAL

APPROVAL

Title Hardware Security Module as a Service (HSMaaS) - Executive Summary Report	
Issue 1	**Revision** 2
Author HSMAAS Team	**Date** 2023-12-04
Approved by . . .	**Date** 2023-12-04

CHANGE LOG

Reason for change	**Issue**	**Revision**	**Date**
MO FR	0	1	2023-07-27
MO 1.0.0, HSM 1.0.0	1	0	2023-11-10
MO 1.0.1, HSM 1.0.1	1	1	2023-11-22
HSM 1.0.2	1	2	2023-12-04

CHANGE RECORD

Issue 1	**Revision** 2		
Reason for change	**Date**	**Pages**	**Paragraph(s)**
MO FR	2023-07-27	All	All
MO 1.0.0, HSM 1.0.0	2023-11-10	All	All
MO 1.0.1, HSM 1.0.1	2023-11-22	All	AR RID fixes
HSM 1.0.2	2023-12-04	All	3.2

DISTRIBUTION

-

Table of Contents

1. INTRODUCTION

This document is the Executive Summary Report for the ESA activity "AO/1-10814/21/NL/GLC". The contract was performed by CGI and Skudo. The work produced two independent products (MO and HSM) with full documentation stacks that were combined into one demo, as outlined in the table below. Demo1 was a joint demonstration of CGI and Skudo.

Demo	Demo description	Company	Product and document stack	Product description
Demo1	Encryption in MO framework supported by PKI. Demonstrated in OPS-SAT experiment 146. Onboard cryptogrphy support by Skudo HSM/FPGA.	CGI	MO/PKI	Automatic handshaking with mutual authentication and symmetric encryption in MAL messages. Implemented in a "Secure MAL" plugin component. Supported by Public Key Infrastructure.
		Skudo	HSM	Integration of the HSM onto the on-board MitySOM FPGA hardware, PKCS#11 SW library and interface; I/O memory mapped interface (pkcs/FPGA) for I/O and storage.

Table 1: Demo and products overview

The MO activity (CGI) creates a Public Key (PK) cryptography-based security solution for CCSDS MO infrastructure. It implements a simplified TLS in the CCSDS MO/MAL protocol (Transport layer). In the demo the OPS-SAT MO infrastructure is updated with the security solution and its operation is demonstrated on Flatsat and OPS-SAT, where the MO infrastructure performs handshakes and exchanges encrypted data between ground and space.

The HSM activity (Skudo) ports Skudo's proprietary HSM to OPS-SAT Cyclone-V FPGA and exposes PKCS#11 interface. The interface makes the the HSM usable for MO.

The rest of the document describes the joint demo and the software that was developed.

2. TERMS, DEFINITIONS AND ABBREVIATED TERMS

2.1. Terms

Security Module - SSM or HSM, depending on context. This document uses the term SM to reference cryptography support. From Java perspective the use of SSM and HSM is interchangeable, since they are implementations of the PKCS#11 interface. SSM in this activity is a software implementation of a generic cryptographic device with a PKCS#11 interface.

Key Agreement - In cryptography, a key-agreement protocol is a protocol whereby two or more parties can agree on a key in such a way that both influence the outcome. If properly done, this precludes undesired third parties from forcing a key choice on the agreeing parties.

Secure Session, Session - The consumer and provider have established a key agreement. The derived symmetric data encryption keys have been created on SM and are ready for encryption and decryption.

2.2. Abbreviated Terms

CA - Certificate Authority

CCSDS - Consultative Committee for Space Data Systems

CTT - Consumer Test Tool

FPGA - Field Programmable Gate Array

HSM - Hardware Security Module

MAL - Message Abstraction Layer

MO - Mission Operations

NMF - NanoSat MO Framework

OCSP - Online Certificate Status Protocol

OSI - Open Systems Interconnection

PKCS - Public-Key Cryptography Standards

PKI - Public Key Infrastructure

SM - Security Module

SSM - Software Security Module

TCP/IP - Transmission Control Protocol / Internet Protocol

TLS - Transport Layer Security

3. DEMO1

The Demo1 diagram below shows the converted OPS-SAT MO system, where the MAL message bodies are encrypted. The system has the following components:

- Consumer Test Tool is a generic MO services client.
- Ground MO Proxy is a protocol bridge from TCP/IP to SPP, and a synchronized onboard archive mirror.
- NanoSat MO Framework is onboard MO applications environment.
- PKI is deployed on ground and consists of Certificate Authority and OCSP Responder.
- SoftHSMv2 is a PKCS#11 compliant security module that offers cryptography functions for ground MO components.
- Skudo HSM is a PKCS#11 compliant product described in section 2.2.

The MO components communicate using MAL messages, that are transmitted over TCP/IP and SPP transports. The transports are changed in the Ground MO Proxy protocol bridge. With the applied changes the MAL message encryption is not removed in the protocol bridge.

The green arrows on the diagram show the MAL message channels between applications. The software developed in this activity encrypts those messages using the idea of TLS. The first message to be sent detects the absence of a "secure session" (there is no session key on security module) and initiates a handshake. Part of handshake is mutual authentication using X.509 public key certificates. The ground certificates are OCSP stapled so that onboard can verify it without extra ground communication. After the handshake completes the end nodes shall have derived secret material on their security modules, which is used for symmetric encryption of the MAL messages.

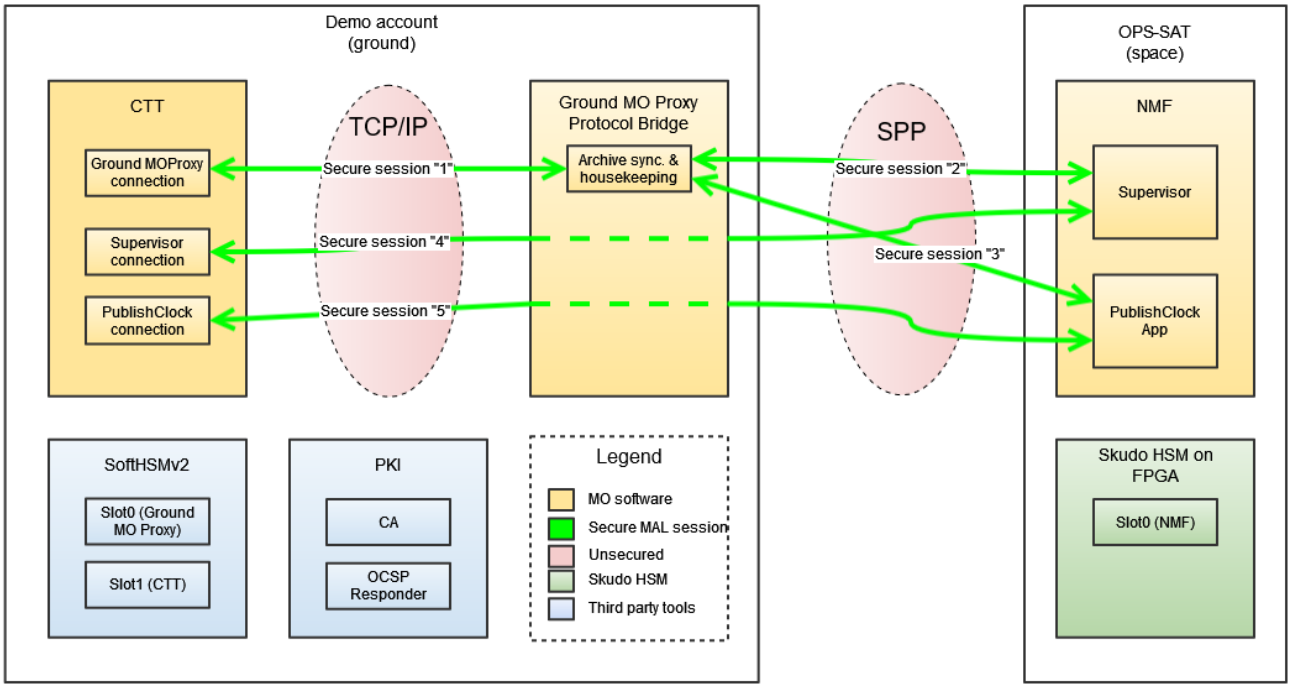

Figure 1: Demo1 OPS-SAT MO system

3.1. Developed software: MO encryption

The developed software is a "Secure MAL" dependency for MO applications. It performs handshake, if needed, and encrypts MAL message bodies. The software is packaged as a JAR. The software can be used in MO consumer and provider applications, Consumer Test Tool, Ground MO Proxy, and NMF Supervisor and its MO applications. The following applies to MO software using the "Secure MAL":

- Key agreement and session
    - The consumer end initiates key agreement automatically, using asymmetric cryptography.
    - The key agreement and encryption algorithms (including X25519), and key lengths are configurable.
    - The key agreement uses mutual authentication using the X.509 public key certificates.
    - The secure session is between MO applications. A MO application may use several MO services.

    - The secure session has a configurable validity period. Note! In implementation the secure session does not expire.
    - The consumer end initiates an automatic reconnect on session expiry. Note! In implementation reconnect on server encryption errors, e.g. missing secure session.

- Encryption
    - The encryption (AES-GCM) is applied to MAL message bodies in the MAL layer.
    - The session data is encrypted using symmetric cryptography.
    - The secret material is kept on third party security modules that use the PKCS#11 interface.
- System and PKI
    - The supporting PKI is deployed on ground.
    - The consumer end is on the ground and the provider end can be onboard (both ends cannot be in space).
    - The consumer X.509 public key certificates are OCSP stapled.
    - Each MO node has its identity certificate and a copy of CA and OCSP Responder certificates.
    - Each MO node can specify its own PKCS#11 security module implementation, such as SoftHSMv2, Skudo HSM, or BouncyCastle for testing.
    - The system can be configured to bypass encryption by MO area. This is used for demo purposes to limit logging to relevant services.
    - The handshaking and data exchange is conducted over MO Security Service, specified in this activity.

3.2. Developed software: HSM

The SKUDO-HSM project was initiated in response to the growing complexities in securing satellite communication and the limitations of existing software-based security solutions (due to larger attack surfaces offered by all software-based technologies). The project aimed to develop a hardware-based security approach by creating an Hardware Security Module (HSM) and interface specifically planned for satellite applications.

Requirements & Design
The project was built on defined requirements to address the specific needs of satellite operations. It featured three main components: a PKCS#11 module, an HSM cryptographic

module, and a storage module. The project involved transitioning from the MAX10 FPGA to the Cyclone-V FPGA with the goal to provide cryptographic functions to an NMF app, a process that included the development of a new PKCS#11 software interface and a memory-mapped I/O interface to facilitate communication between the modules.

Testing & Validation

Two sets of tests were conducted using a Flatsat, replicating the OPS-SAT environment. The first test (successfully completed) focused on the successful porting of the Verilog HSM to the Cyclone-V FPGA and testing all functions via a standard PKCS#11 interface. The second test (not successfully executed) involved validating the integration of the system with the CGI NMF application, ensuring that the HSM correctly processed all encryption requests from the Flatsat and the satellite.

Achievements & Milestones

The project achieved significant technical milestones, notably the successful porting of the HSM system to the Cyclone-V FPGA architectures (as on the FlatSAT and OPS-SAT), the implementation of a memory mapped I/O interface and the integration with a PKCS#11 standard library.

Conclusion

The SKUDO-HSM project has contributed to the field of satellite cybersecurity. It shows potential in using hardware-based security measures for space operations. The project reflects a commitment to enhancing satellite security and marks a step forward in cybersecurity technology for possible space applications.