Kiuru FM Module

Product Fact Sheet v.1.1

Functionality Module (FM) is a custom-developed module for a Hardware Security Module (HSM). FM allows customizing the HSM functionality and to run security-sensitive code inside the tamper-proof environment provided by the HSM.

The Functionality Modules are created using a FM Software Development kit (SDK), and the software package must be signed before it can be loaded into a HSM. Signing the FM ensures that the module cannot be modified by a third party.

Product Description

Alauda PBY protocol is split into two separate components: SRP6 and B17 protocols. SRP6 protocol is used for user's knowledge verification (like PIN) and for data protection key derivation. B17 protocol is used for managing user's key material. Kiuru FM implements the B17 part inside the HSM device.

Kiuru FM is a signed proprietary software module inside a supported HSM device. Kiuru FM communicates with the Alauda PBY (SIC) component on a smartphone by using B17 messaging which is delivered inside the Alauda PBY protocol (Signature Activation Protocol).

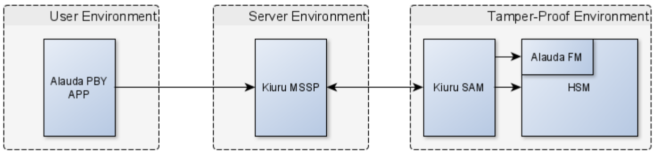

Figure 1: Kiuru FM in a Remote Signature solution.

Product Features

Kiuru FM security improvement focus to the following EN 419241-1 SCAL2 requirements. Kiuru FM improves the standard Kiuru SAM security in the following ways.

1. Smaller SAM attack surface – (I) and (IV)
   - Kiuru FM makes harder for an attacker to forge SAD data when the B17 data computing and handling is done completely in the HSM. (I)
   - Source and verifier of the SAD assertion are the same (IV)
2. HSM enforced signer authentication – (III) and SRA_SAP.1.3, SRA_SAP.1.4
   - The HSM now verifies the authenticity of the B17 data and makes own decisions based on it.
   - B17 material of the SAD is always computed in HSM (V)
3. Signing key activation is split to two components – SAM and HSM – SRA_SAP.1.4
   - SAM takes care of the SRP6 based signer authentication (III) and SAD
   - HSM B17 key material authentication (III)

Security Considerations

The current implementation of the Kiuru SAM product is fully based on General System Security Requirements EN 419241-1 and Protection Profile for QSCD for Server Signing EN 419241-2 . The product has been certified based on the said Protection Profile. Moreover, the SAM server has been separated into a dedicated server, which does not provide any other/unnecessary attack surfaces.process However, if higher security mechanisms than the General System Security Requirements are required, we have designed an optional Kiuru FM model.

The key design principles of the Server Signing have been to enable the sole control of the signer. Moreover, the server signing system components have been defined so that the system consists of SIC, SSA, SAM and HSM modules. SAM and HSM are located in a tamper-proof area.

Tamper-proofing, conceptually, is a methodology used to hinder, deter or detect unauthorized access to a device or circumvention of a security system. Kiuru SAM tamper-proofing concept principle is to minimize SAM server's attack surfaces (hinder), remove all local administrative interfaces (deter) and monitor all changes in mandatory interfaces (detect). Additionally, a privileged user on the SAM server does not have any tools or interfaces to do undetected modifications to Signer's data.

The Kiuru FM model Pros

+ Smaller SAM software attack surface (hindering)
+ HSM enforced signer authentication (detection)
+ Signing key activation is split to two components (hindering)

The Kiuru FM model Cons

- More complicated deployment procedure and system verification
- More complicated key generation and signing flows
- Vendor dependency (vendor specific HSM implementation)

Supported HSM Platforms

+ Thales Luna7
+ Utimaco CP5

Standards

CEN EN 419241-1
CEN EN 419241-2
CEN EN 419241-3

About Methics

Methics Oy is a privately held consulting company specialized in subscriber management and data communication infrastructure development for security, service management and business intelligence. The company offers Java technology based software products under the Kiuru trademark. Kiuru products provide open standard based services for service provisioning and mobile signature services.

Information in this document is provided without warranty.
Product features may change with updates.