floor51

EXCEPTIONAL::SOFTWARE

Get In Touch

+44 (0) 7956 308115

enquiries@floor51.com

www.floor51.com

Imagine a secure and efficient place to lock away business logic along with keys and algorithms in a tamper proofed unit.

INTRODUCING HSIM-51 FROM FLOOR 51

Product Features

floor51 provides customised firmware for popular HSMs containing a variety of additional features, all accessible from vendor neutral APIs:

Secured Business logic

- HSS eKi decryption for use with Milenage, all contained within the HSM so that the Ki is never used in an unencrypted form externally
- SIM provisioning credentials generation and transport encryption, from Ki to PIN/PUKs generation, all in one request
- SIM OTA secured payload assembly for both UICCs and eUICCs

Mobile algorithms

- Milenage AES+XOR, f1 to f5 functions, c1 to c5 and r1 to r5 values
- COMP-128 variants per operator
- TUAK
- SIM and Remote SIM OTA custom key derivation algorithms per operator

Platform Availability

SafeNet ProtectServer Now

Utimaco SecurityServer 2018

Enterprise Grade Appliance

floor51 can assemble enterprise ready HSM appliances supporting:

- RAID
- iLO
- Redundant power
- Dual ethernet with network card bonding
- Nagios and SNMP

Business Critical Use Cases

HSS authentication

Traditional SIM provisioning

SIM management OTA

Remote SIM provisioning and management OTA

Custom Algorithms

Custom algorithms can be implemented on a case by case basis per operator including:

- COMP128 variants
- SIM OTA algorithms for the generation of derived keys

In all cases a preconfigured build system can be provided so that a C implementation of the algorithm can be inserted without needing to share it with floor51

Technical Standards

3GPP 35.206 Specification of the MILENAGE Algorithm Set

GSMA SG.03 Rules for the Management and Distribution of the COMP128 Family of Example A3 and A8 Algorithms

3GPP 35.231 Specification of the TUAK Algorithm Set

3GPP 23.048 Security Mechanisms for the (U) SIM Application Toolkit

GSMA SGP.22 RSP Technical Specification

SIMAlliance eUICC Profile Package Interoperable Format 2.1

SECURED BUSINESS LOGIC

Custom business logic can be migrated into the HSM environment. This provides tamper proofing and portability for software at the heart of business critical systems

floor51's vendor neutral APIs mean that an alternative HSM provider can be swapped in without needing to change any client code. Equally, customers can migrate to new client systems without needing to change the HSM or the business logic within it

floor51 can share the source code for algorithm implementations resident inside the HSM with the customer, so that their integrity can be checked

By implementing business logic within the HSM it is possible to generate data that is never held in the client machine's memory. For example, during the provisioning process the HSM can generate a Ki and OPc, then produce the eKi for the HSS, and then a version for the SIM manufacturer without ever needing to return the Ki in an unencrypted form. Using just the algorithms alone would mean having to retain the Ki in client memory

floor51's APIs are provided as C libraries that can be exported to a variety of languages using SWIG including Java, Python, C#, PHP, JavaScript and more