UNIVERSIDAD DE CHILE

System for secure electronic communications through HSM bases on threshold cryptography.

University of Chile has generated a distributed system that uses threshold cryptography capable of simulating an HSM without expensive hardware and maintaining high security.

THE CHALLENGE

Currently there are HSM's based on hardware and software. The hardware offers prices between US $ 50 and US $ 50,000, but accessing a low-cost one implies a highly vulnerable level of security. There are also low-cost software, but they present greater security vulnerability than those based on hardware. In addition, there are services in the cloud (Cloud Computing) with lower average prices for hardware and with greater flexibility, but involves trusting the information to an external company.

The solution proposed consists of a fault tolerant system, since it distributes the keys on a set of internal nodes, and in addition it would be necessary to take control of half plus one of the machines to expose the keys.

THE TECHNOLOGY

This technology consists of simulating an HSM, which uses threshold cryptography in order to distribute the keys over a set of internal nodes.

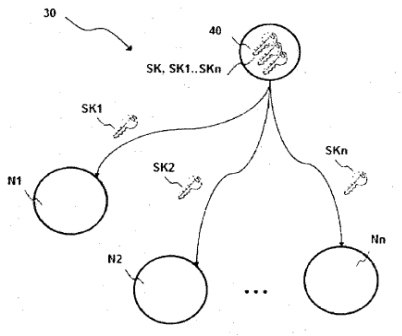
The digital signature process involves the steps of: 1) the signing agent receives a document to be signed and the alias of the key with which the document will be signed; 2) the signing agent puts the document in the queue of requests; 3) the active nodes get the request from the queue: 4) each node signs the request with its piece of code; 5) each node puts its partial signature on (to answer queue; 6) the signing agent receives the partial signatures and verifies them; 7) if at least k> n / 2 valid partial signatures are received, the signature is validated and delivered to the client. Otherwise, it generates an error message.

STAGE OF DEVELOPMENT

- Laboratory tests.
- Currently working on an implementation model for the NIC Chile.

COMPETITIVE ADVANTAGES

- Low cost technology, maintaining a good level of security.
- It has greater robustness and tolerance than some HSM software, because it distributes the key in different geographical locations.



Schematic representation of the initiation process.

APPLICATIONS

- Informatic security.
- Banking industry.
- IoT and Smartcity.
- Electronic signatures (Documents).

OPPORTUNITY

Available for **out-licensing.**

INTELLECTUAL PROPERTY/REFERENCES

- Patent Applications US 16/067,307, CL 2015-03766.

VID INVESTIGACIÓN INNOVACIÓN CREACIÓN ARTÍSTICA
Vicerrectoría de Investigación y Desarrollo
UNIVERSIDAD DE CHILE

CONTACT: **Alexander Ibarra**
Technology Manager
alexander.ibarra@uchile.cl
+56 (2) 29782411