| Resumen | | | | | |
| --- | --- | --- | --- | --- | --- |
|  | | | | | |
| Registro de modificaciones | | | | | |
| Versión | Descripción | Autor | Fecha creación | Aprobado por | Fecha aprobación |
| 1.0 | Versión inicial | IVM | 16/08/17 |  |  |
|  |  |  |  |  |  |

Contenido

[1. Everilion HSM 3](#_Toc491083441)

[2. References 4](#_Toc491083442)

[3. Questions for EESTI project 5](#_Toc491083443)

# Everilion HSM

Everilion is working with HSM devices from 2012.

Our company is using HSM for 2 different purposes:

1. Usual payment solutions: here we have been using ADYTON for the banking industry and for Retail where a typical payment transaction is taking place and PCI requirements must be achieved.
2. New areas where security is an asset: As an example, we are using  ADYTON in the public sector and health industry for cyphering and secure documents that must not be share, used and seen by anyone except for its owners and a selected group of authorized users.

We offer consultancy services in payment and security applications, definition of HSM API and layer of services for integration with HSM and development of that layer of services.

# References

Those are our main references regarding integratin with HSM

* Inwallet
  + Design, development and deployment of the Inditex wallet
  + Registration and storage of cards in PCI plataform
  + Use of those cards for bank payment
* Sergas
  + Design, development and deployment of cyphering of documents for public competition
* Banco Popular – TPIN
  + Storage of keys for PIN management
  + Translation of PIN block encryption from one kind of key to another
  + Integration with HSM API and development of layer of services to costumer
* Banco Popular – Hub Digital
  + Storage of keys
  + Ciphering and deciphering of XML and MAC computation
  + Integration with HSM and development of layer of services to costumer
* Banco Popular – HCE
  + Storage of keys
  + Ciphering and deciphering of XML and MAC computation
  + Integration with HSM and development of layer of services to costumer

# Questions for EESTI project

The following questions are leaded in order to have knowledge of the scope of the integration with HSM

* Has the API of the HSM already defined or should be necessary consultancy issues for define it?

- Is not defined so far. It could be necessary consultancy.

* Has the API for the application costumer already defined or should be necessary consultancy issues for define it?

- Is not defined so far. It could be necessary consultancy.

* Which is the way of integration with HSM? Sockets with HSM proprietary protocol? Webservices? Other? (Could we have access to HSM API documentation?)

- Integration with HSM could be done through Unix domain socket on Unix or named pipes or TCP/IP sockets on Windows.

* Is it necessary some kind of login/password for have access to HSM functionality in integration mode?

- It could be. Not sure at this point. Why is this important?

* Which is the aim of the integration layer, just only expose methods for costumer to have access to HSM services or it should develop also some logical of application?

- For now just develop methods to be used by NLS Services.

* How many different HSM functionalities is expected to be developed?  
  - All those necessary to run the business requirements, including basic management functionalities for keys: load, store, delete. Probably some others, but we can’t define at this point, since deep analysis haven’t been performed so far.
* Is expected that the layer of integration should storage data (for configuration, key identificators, etc)? That is, should the database have a database?

- It could be possible, depends on the development and the necessary flows.