

OpenHSM: An Open key life cycle protocol for Public Key Infrastructure's Hardware Security Modules

Jean Everson Martina
University of Cambridge/UK

Tulio Cicero Salvaro de Souza
Ricardo Felipe Custodio
Federal University of Santa Catarina/Brazil

EUROPKI'07
Fourth European PKI Workshop
Theory and Practice
28-30 June, 2007, Mallorca, Balearic Islands, Spain

ICP-EDU Project

- Project from Brazilian Research Network(RNP)
- PKI to be deployed in research centers and universities in Brazil
- Part I – Certificate Management System
- Part II – “Affordable” HSM for PKI
- PoC – Test of policies and practices for the PKI
- Part III – Applications Integration and user protection

ICP-EDU Definitions/Problems

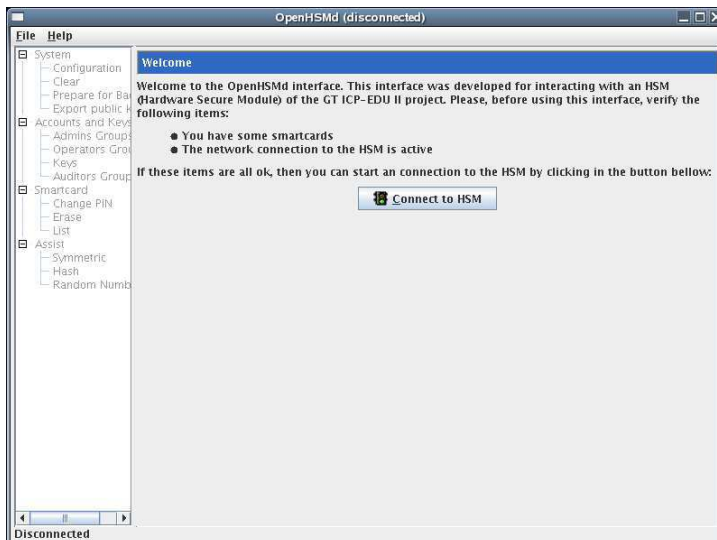
- Each institution is responsible by its CA's private keys.
- Each institution can define its own Certification Hierarchy
- Security by strict auditing
- HSMs are work as black boxes(in terms of internal protocols)- **Inacceptable**
- PKI HSMs must be built for PKI not adapted from other applications(Banks)

OpenHSM objectives

- Easy of integration/understanding (uses a PKI to control the keys inside it)
- Create discussion on the topic of a HSM built for PKI
- Propose a protocol to manage keys inside a HSM (or not!)
- Create a low cost solution (Brazilian Reality)

Prototyping Platform

- Intel Based
- True Random Number Generator
- Security Unit
- Anti Tampering System
- Separate Crypto Unit
- Connected via Ethernet
- External Card Reader
- Free Software Based (Free/Open Implementation)
- Standard Connection Interfaces (OpenSSL,PKCS#11)

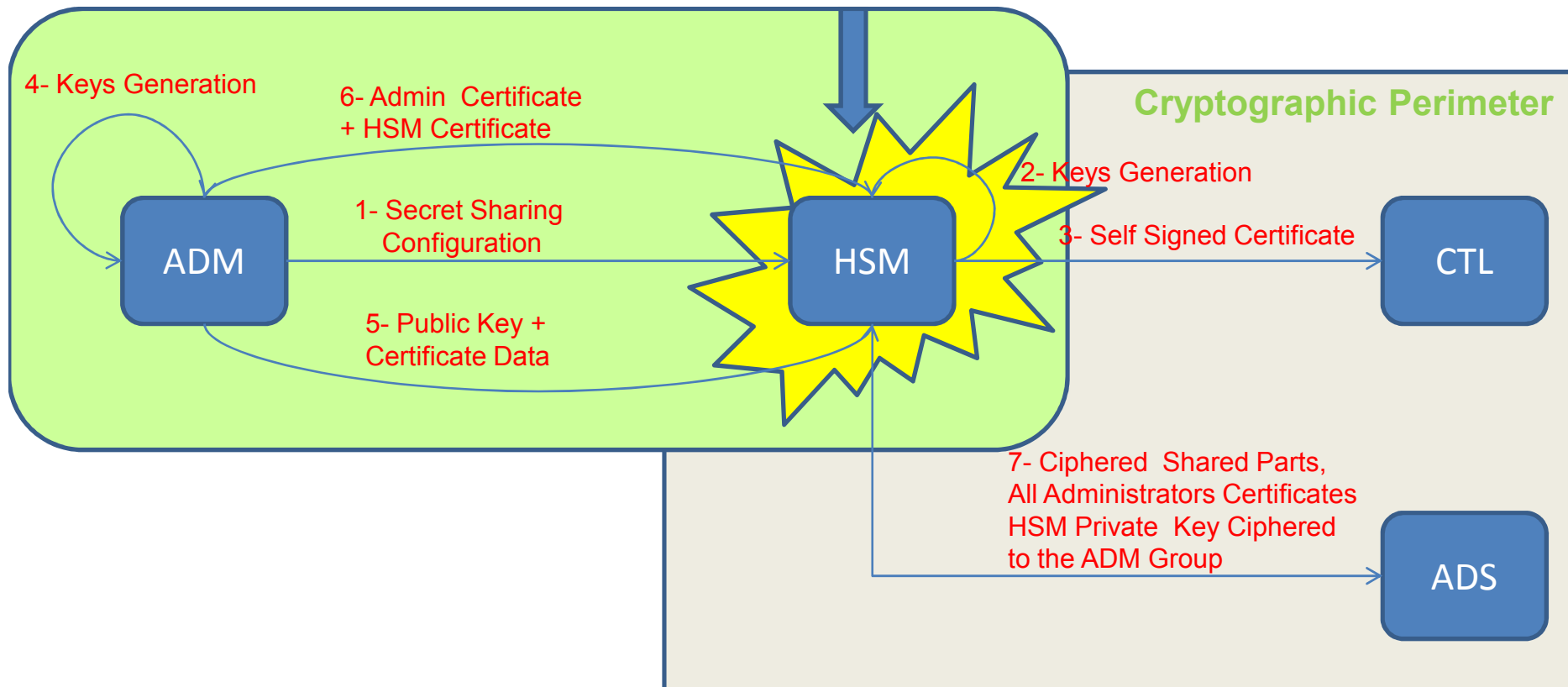


Protocol Premises

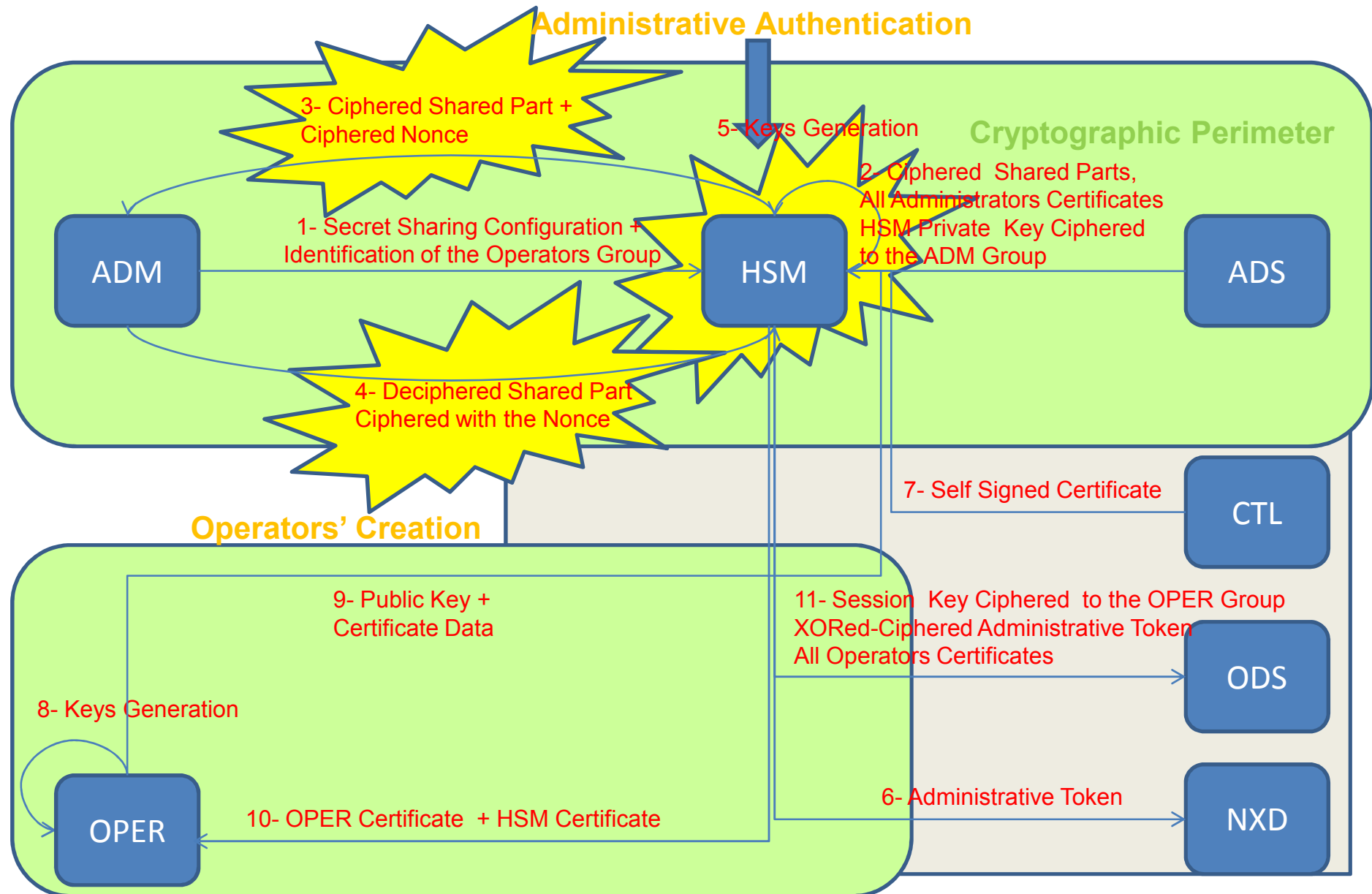
- Each principal holds securely its private keys
- RNGs works perfectly and true randomly
- NXD is flushed on a pre-established basis
- All data storages store data as it was sent to them
- The secret sharing scheme works perfectly
- Principals cannot retain data between runs, except storage principals
- All certificates are securely verified before use

Initialisation and Creation of Administrator Group

Administrators' Creation

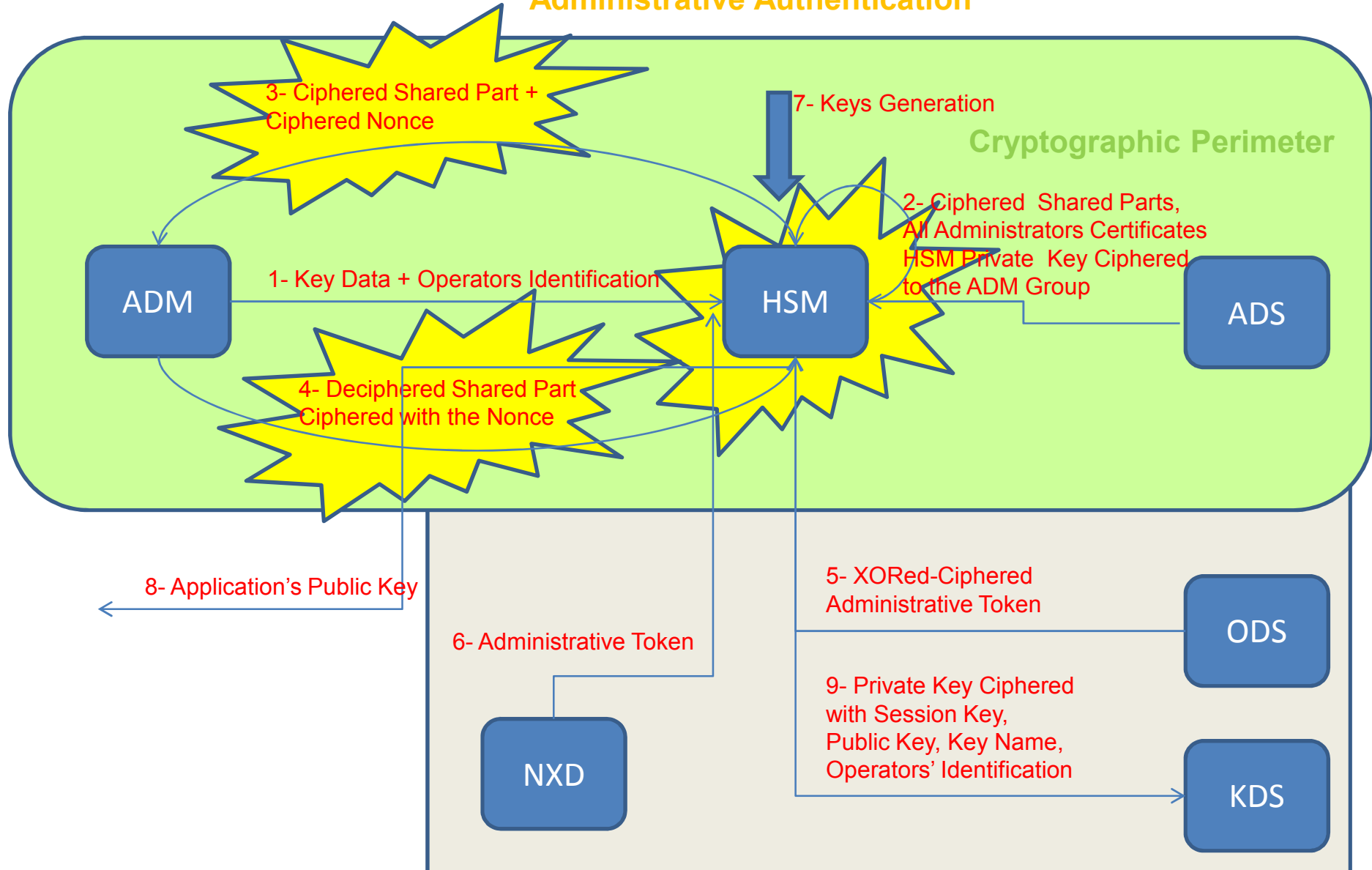


Creation of Operators Group



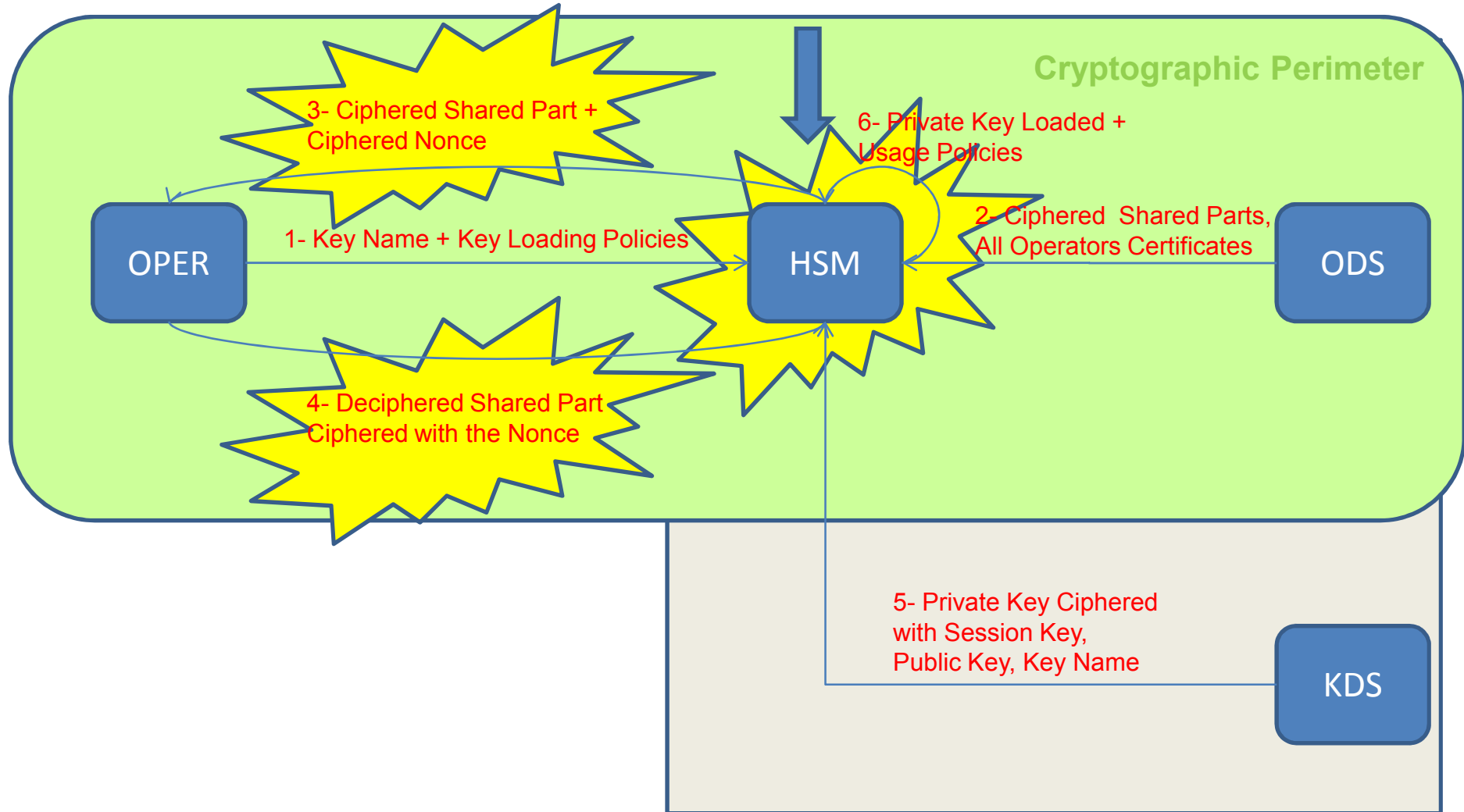
Application's Asymmetric Key Generation

Administrative Authentication



Application's Asymmetric Key Usage

Operative Authentication



Conclusions

- The protocol is already in its 3rd version (bugs and errors may happen)
- We have the complete set of protocols (18: group changes, backup, auditing, etc)
- It proved viable to implement
- Enabled us to debug better CMS, by strict auditing(not showed here)
- It is intended to be a kick-start to the community

Present/Future Work

- Bug search in the protocol using ATPs (finished with simplistic models)
- Proof of the security proprieties using Inductive Modelling, developed by Paulson and Bella
- Work on the hardware development targeting international certification (RNP)

Questions:

More information on the project development

<http://www.icpedu.labsec.ufsc.br>

<http://projetos.labsec.ufsc.br/icpedu>