Giving confidence in Server Signing for eIDAS using Common Criteria evaluation

30th June 2015

Eurosmart

Agenda

- Article 30 of eIDAS & CC unique Framework
- Common Criteria advantages
- QSCD : evaluation based on Protection Profiles
- QSCD architecture
- Threat model for Server Signing
- QSCD key features
- Conclusion

Article 30 of eIDAS

- Article 30: rules for Certification of Qualified electronic Signature Creation Devices

QSCD requires Security Certification based on

a) a security evaluation process carried out in accordance with one of the standards for the security assessment of information technology products

b) or may use alternative only in the absence of standards

c) or when a security evaluation process referred to in point (a) is ongoing.

Common Criteria : the **only standard** security certification scheme **widely recognized to provide high level of confidence**

CC Evaluation / Certification means to reach Confidence

Confidence comes from evaluation driven by :
Assurance * Resistance * Expertise

Confidence comes from certification driven by :
Relevance * Independency * Recognition

QSCD : evaluation based on Protection Profiles

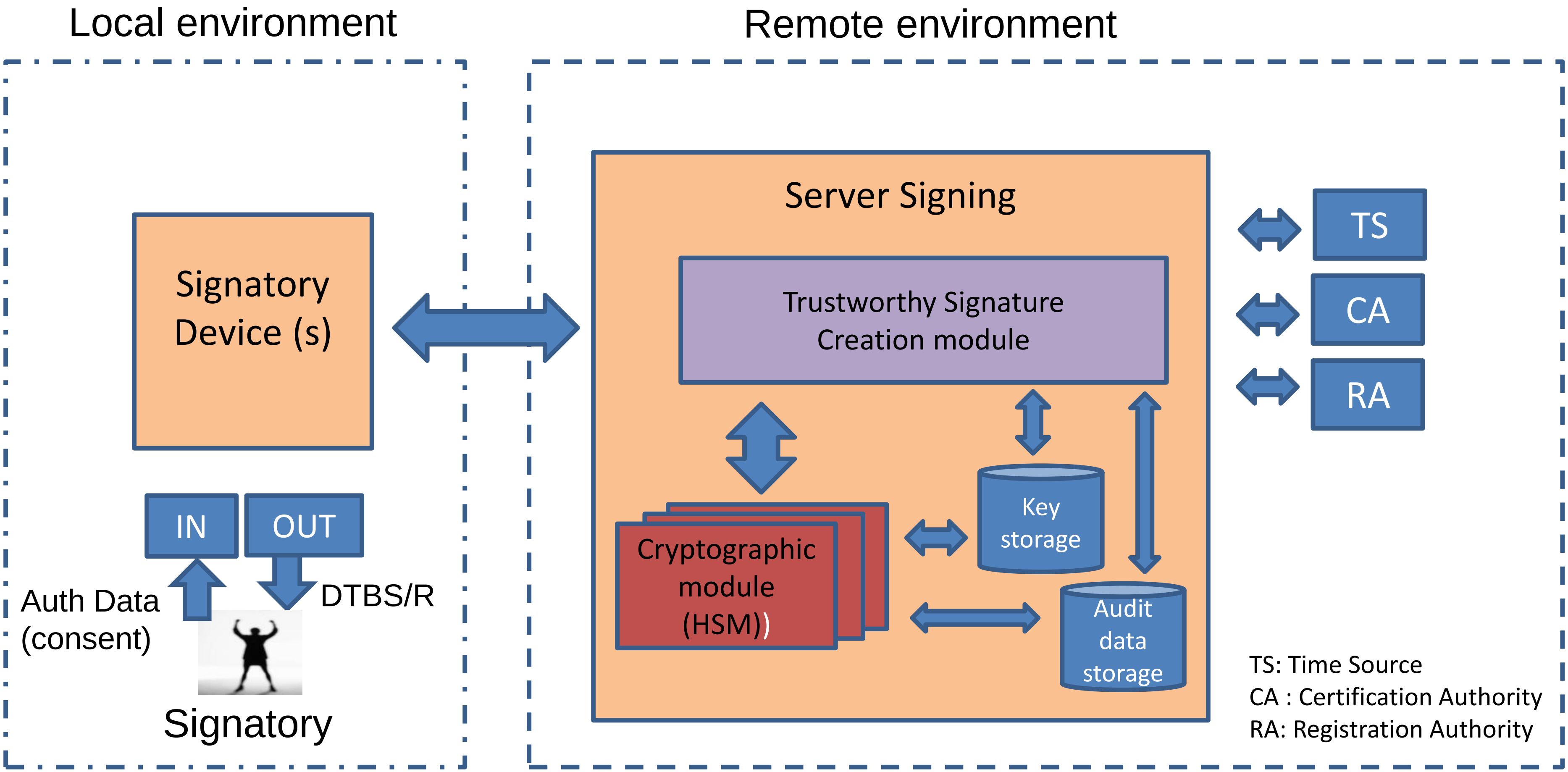
Protection Profiles in Common Criteria allows to define accurately

- Generic Security Problem definition (Technology neutral) => Scope
- Security Objectives for Server Signing system and its environment => Purpose
- Functional requirements (What to evaluate) => Features
- Assurance requirements (How to evaluate) => Method, Rigor, Depth

Allowing :

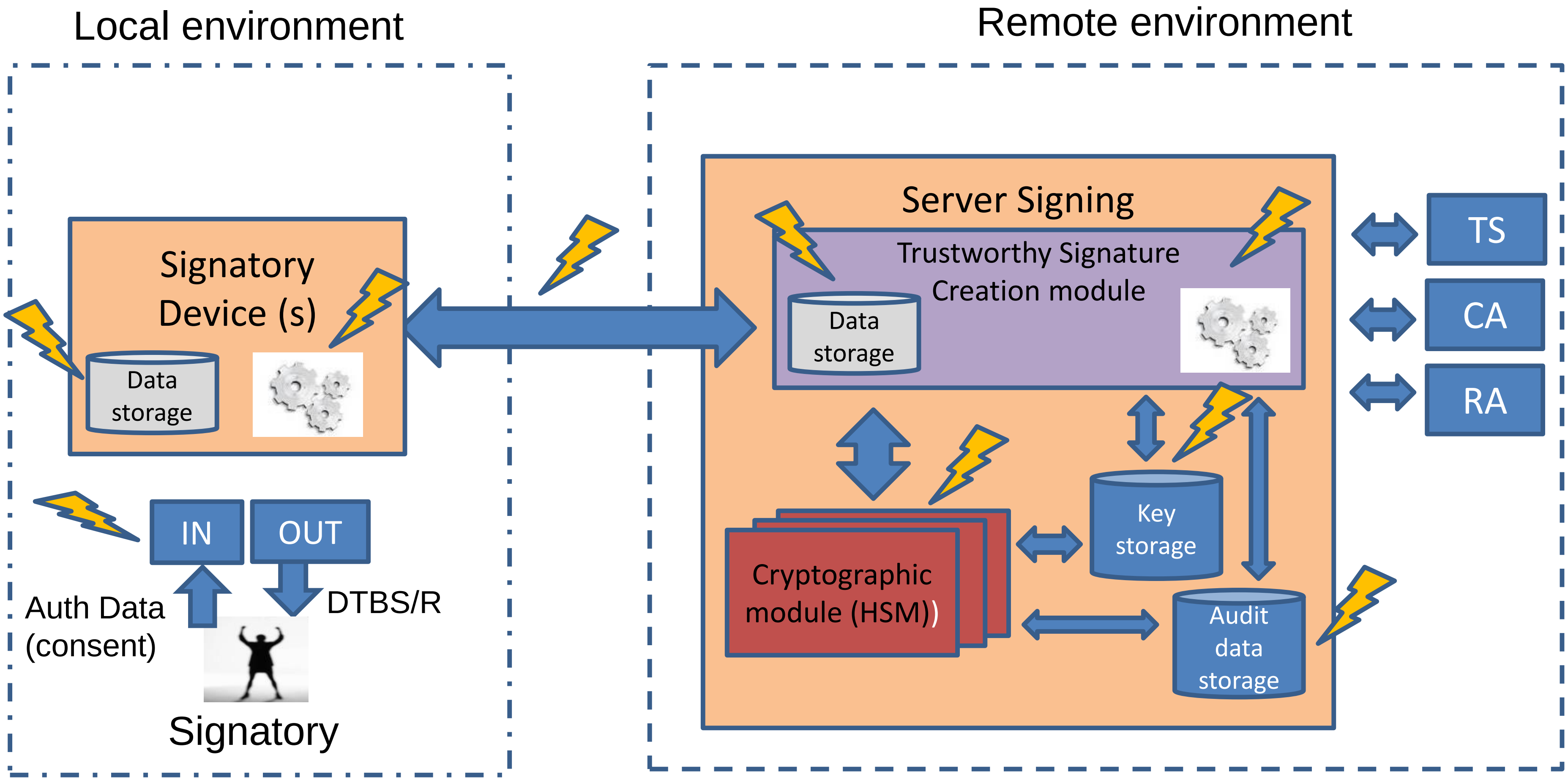
- Evaluation can be reproduced
- Evaluation results can be compared

Architecture for Server Signing



How to provide to Signatory Sole Control to signature operation for a given DTBS and a SCD when it is done by HSM on its behalf ?

Threat model for Server Signing



Threats

ABUSE OF SIGNATORY SOLE CONTROL
(bypass authentication or signature activation protocol)

INVALID SIGNATURE with WRONG DTBS, KEY, IDENTITY
(bypass of access control or MIB or MIM)

SIGNATURE done WITH WEAK KEY
(weak key generation and binding to usage or identity)

UNAUTHORIZED SIGNATURE with different DTBS, KEY, IDENTITY

Not Qualified SIGNATURE transformed in Qualified (No valid Certificate, no use of QSCD)

QSCD key features

- **Signatory Enrolment**
  - Signatory identity check and unique identifier creation
  - Signatory authentication mean creation and distribution

- **Signature Key Management**
  - Unicity of SCD
  - SCD/SVD generation and binding
  - Key export and import from cryptographic module
  - Key back-up outside CM

- **Signature Authorization**
  - Signatory consent linked to DTBS
  - Signatory authentication
  - Signature authorization method linked to DTBSR, SCD.ID and SIGN.ID

- **Signature Generation**
  - DTBSR secure transfer (Confidentiality & Integrity protection)
  - Secure crypto operation
  - Secure usage of SCD (C&I protection, key selection & usage)

QSCD features
(other things to consider)

- **Signature request and DTBS confidentiality**
  - Protection of DTBS and Signature request is often a MUST

- **Signature operation privacy**
  - Link between Signature request and Signatory Identity

- **Certificate Management**
  - Certificate generation & import request
  - Certificate validity check
  - SCD activation only for valid certificate

- **We recommend these QSCD features to be implemented even if there are not clearly written in eIDAS**

eIDAS and CC Protection Profiles

Article 30 of eIDAS requiring qualification of QSCD will be applied thanks to certification using Common Criteria protection profiles.

Writing and evaluation of Protection Profiles for each item included in QSCD are in progress under ANSSI certification scheme.

THANK YOU FOR YOUR ATTENTION

FRANCOIS GUERIN
www.eurosmart.com