



CEN/TC224/WG17

server signing activities

- **Response to the EC standardization needs on eIDAS interoperability framework and level of assurance**

- **Series of standard to define:**

⊖ 419 241 Part 1: General System Security Requirements

⊖ 419 241 Part 2: Protection Profile for QSCD for Server Signing

SERVER SIGNING SCOPE

- The purpose of the trustworthy system (TW4S) is to create a digital signature under sole control of a natural person, or under control of a legal person which may be incorporated into an electronic signature or an electronic seal as defined in the eIDAS Regulation.
- SCOPE:
 - ⊖ provides commonly recognized functional models of TW4S;
 - ⊖ specifies overall requirements that apply across all of the services identified in the functional model;
 - ⊖ specifies security requirements for each of the services identified in the TW4S;
 - ⊖ specifies security requirements for sensitive system components which may be used by the TW4S.



SERVER SIGNING OBJECTIVES

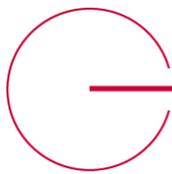
The objectives is to define requirements on the same scope as for a local signing device (pin/key/hash), but used remotely.

- **Defines requirements to :**

- ↳ the signing key protection and signing key usage;

- ↳ the signer authentication means and mechanisms;

- ↳ the link between the authenticated signer and the DTBS/R (hash);



SOLE CONTROL ASSURANCE LEVEL

In order to fit to many scenarios as eSign/eSeal or simple/advanced/qualified, the server signing standard defines 2 levels of sole control.

- **Sole control assurance level 1 (SCAL1):**

- ⊖ The signing keys are used, with a low level of confidence, under the sole control of the signer;
- ⊖ The authorised signer's use of its key for signing is enforced by the SSA which authenticates the signer.

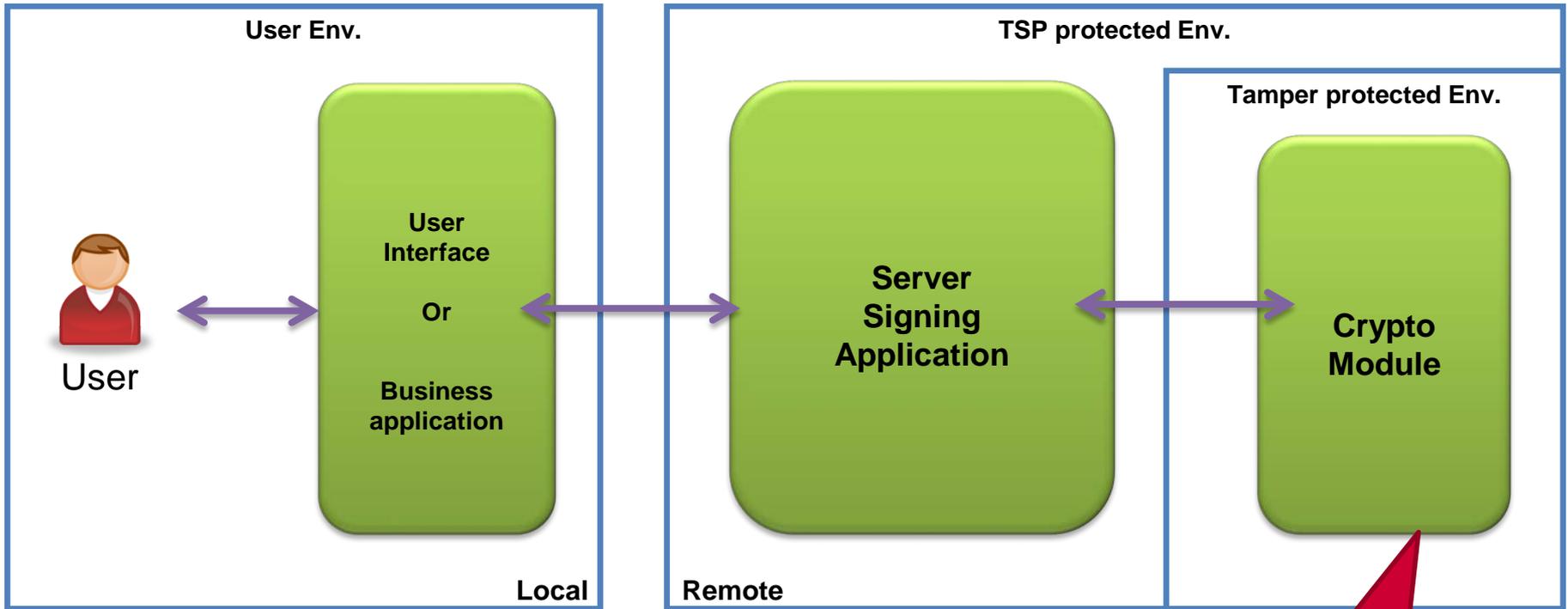
- **Sole control assurance level 2 (SCAL2):**

- ⊖ The signing keys are used, with a high level of confidence, under the sole control of the signer;
- ⊖ The authorised signer's use of its key for signing is enforced by the SAM [...], in order to enable the use of the corresponding signing key

REMOTE SIGNING OVERVIEW

Sole control Assurance Level 1

419 241-1
level1



SCAL1 components

→ Data communications

PP-Crypto
419 221-5



SIGNATURE ACTIVATION (SCAL2)

The goal for SCAL 2 is to provide the same level of security as provided by a smartcard. But the standard doesn't define an activation process, only security requirements on that process.

- **Signature Activation Protocol (SAP):**

- ⊖ The set of the necessary steps in order to create a signature;
- ⊖ Shall generate an 'activation data'.

- **Signature Activation Data (SAD):**

- ⊖ Shall be linked to the authenticated signer; (substantial level)
- ⊖ Shall be linked to the DTBS/R; (to protect from replay attack)
- ⊖ Shall be generated under sole control of the signer.

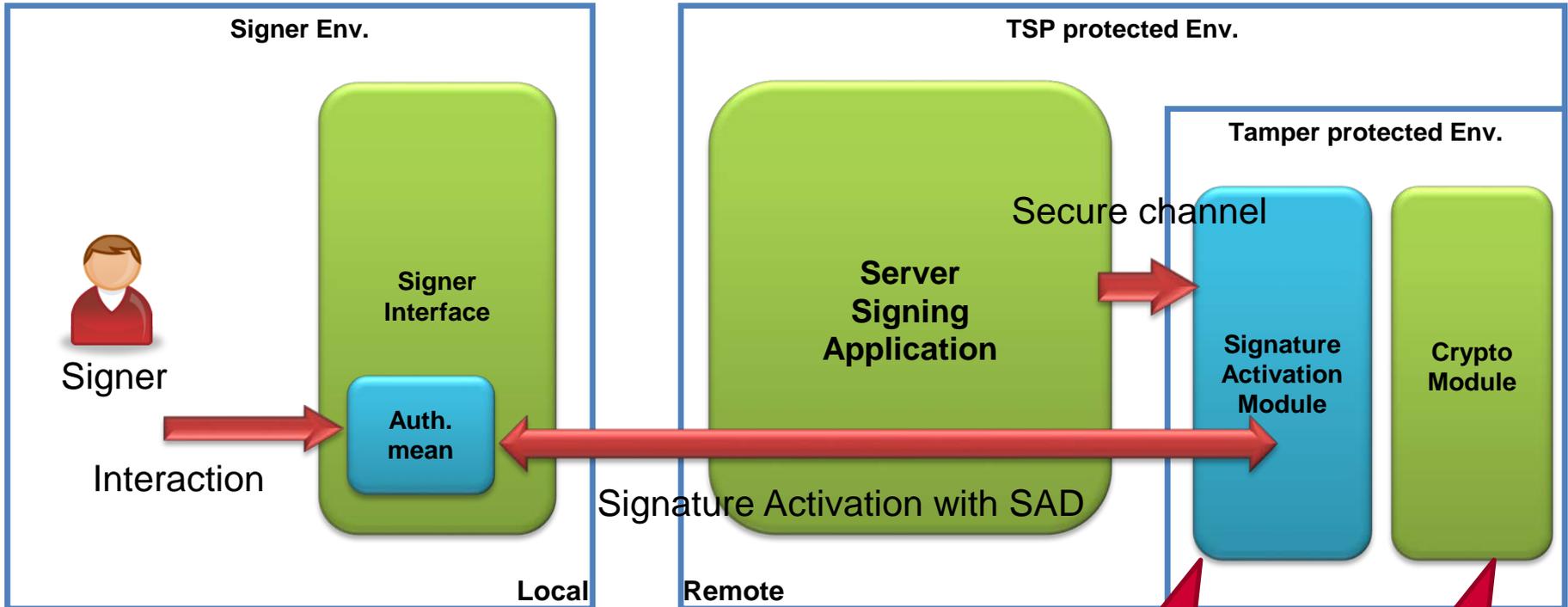
- **Signature Activation Module (SAM):**

- ⊖ Piece of software protected by an HSM;
- ⊖ Checks the validity of the SAD in order to activate the signing key.

REMOTE SIGNING OVERVIEW

Sole control Assurance Level 2

419 241-1
Level 2



SCAL1 components

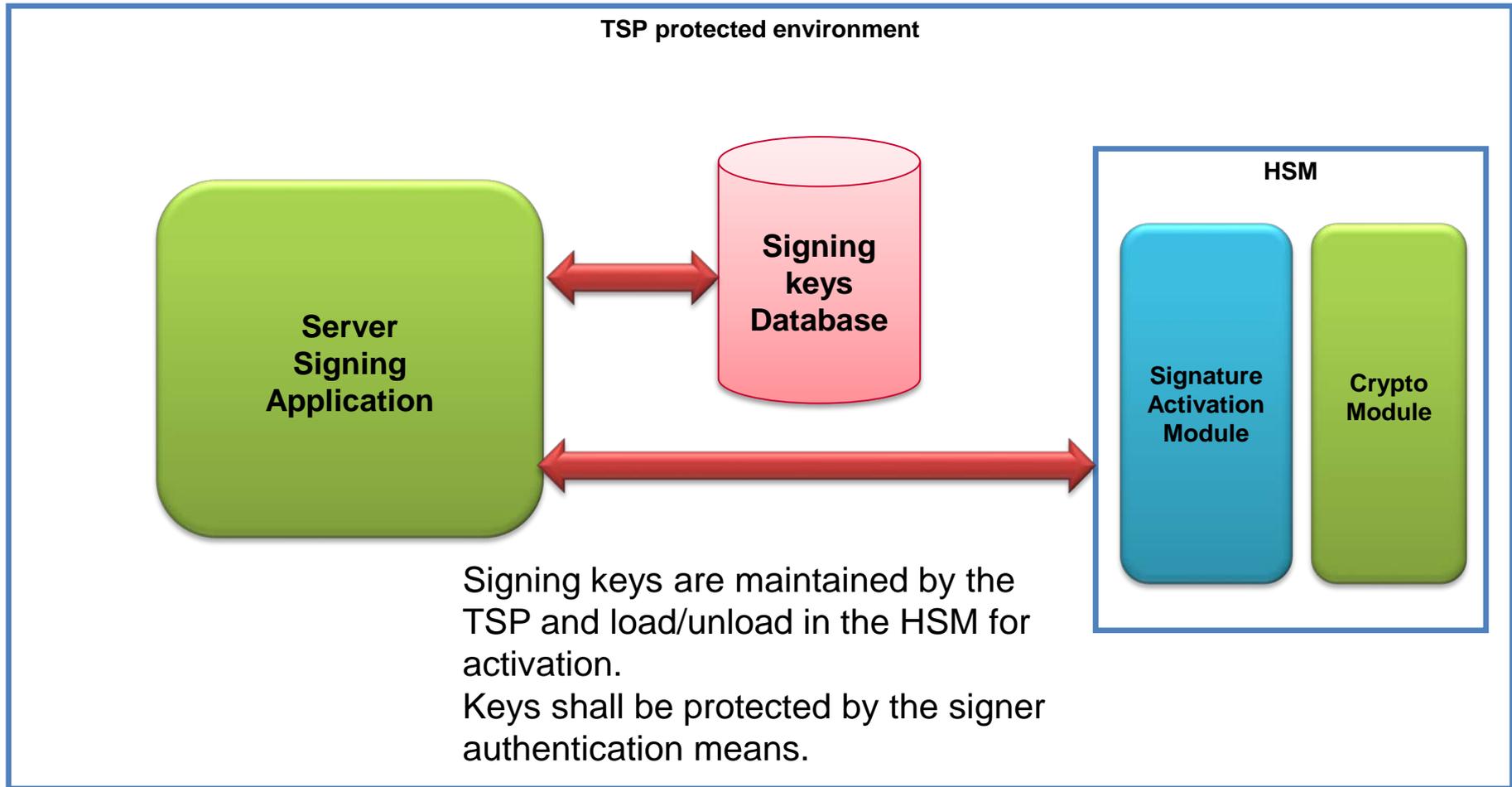
SCAL2 components

PP-SAP/SAD
419 241-2

PP-Crypto
419 221-5

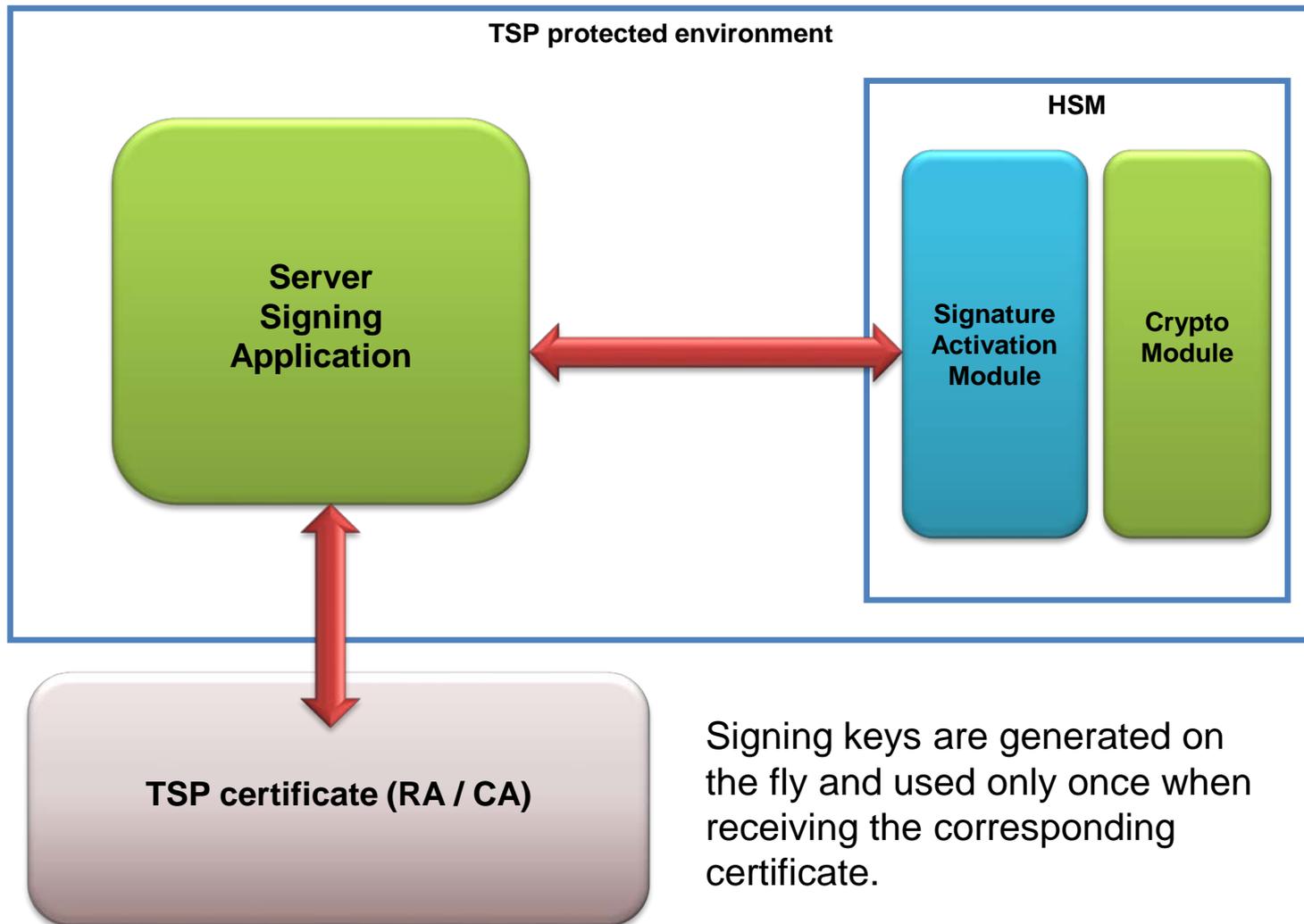
REMOTE SIGNING EXAMPLE

Long lived keys



REMOTE SIGNING EXAMPLE

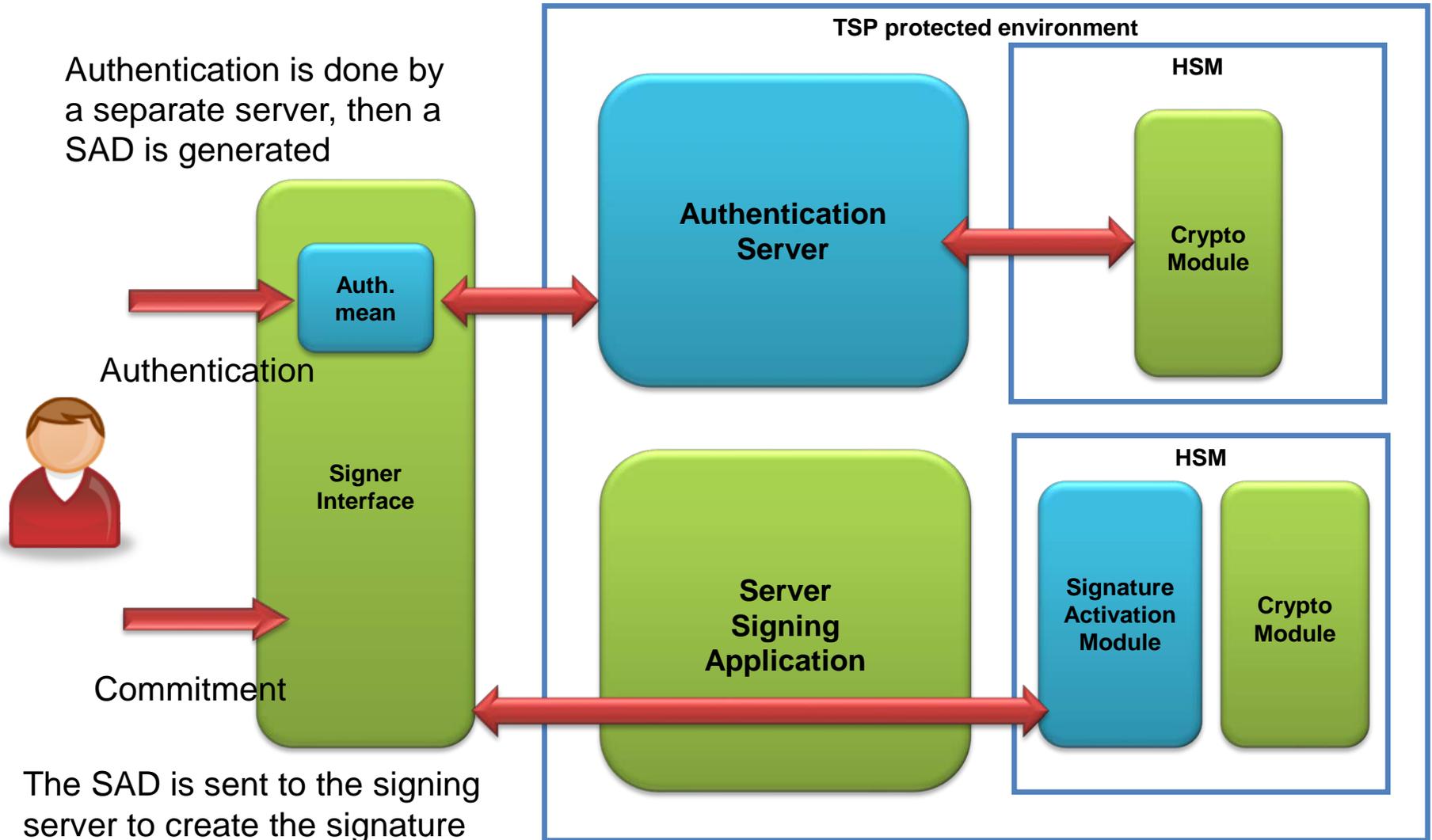
Short term keys



Signing keys are generated on the fly and used only once when receiving the corresponding certificate.

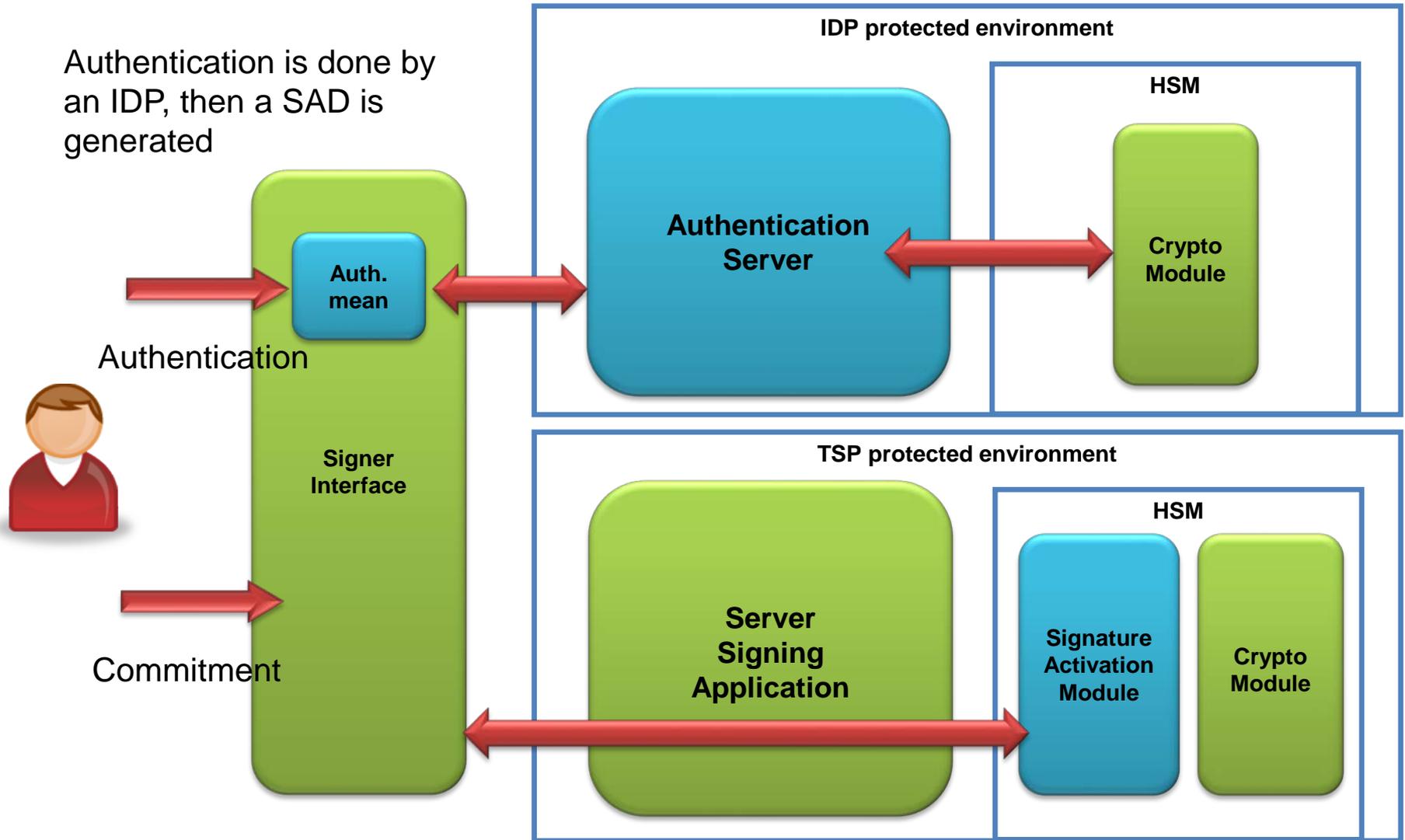
REMOTE SIGNING EXAMPLE

Segregation of authentication and signing HSM



REMOTE SIGNING EXAMPLE

Delegation of authentication to an IDP



Questions ?

Contact details:

Franck Leroy
franck.leroy@docapost.fr

CEN TC 224 / WG 17