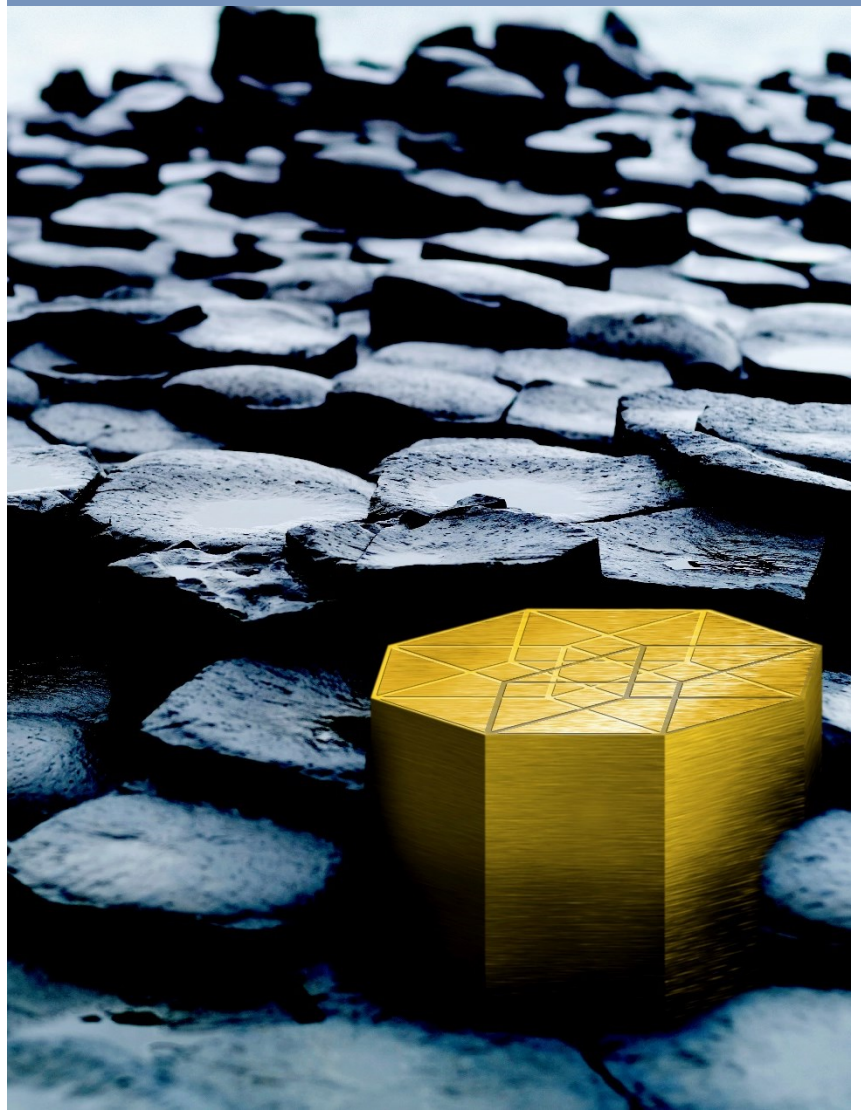
CRYPTOMATHIC



Server Signing QSCD Protection Profile

Jan Kjaersgaard

CEN TC224 WG17

Editor prPP 419 241-2

CRYPTOMATHIC

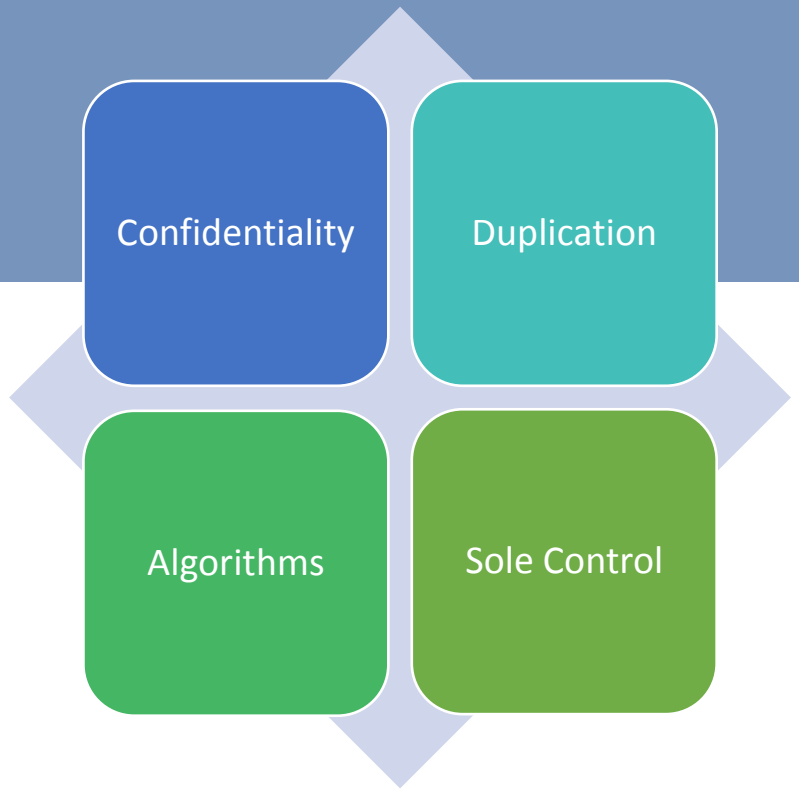
Agenda

- eIDAS abouts QSCDs
- What does PP contains
- Standards
- Signature Activation
- User Authentication
- Architecture deployments
- Status

CRYPTOMATHIC

eIDAS about QSCDs

- **Article 3:**
  - Qualified electronic signature requires a qualified electronic signature creation device
- **Article 29:**
  - Meet the requirements in Annex II
- **Article 30:**
  - Must be certified
  - The EC must publish standards for security assessment

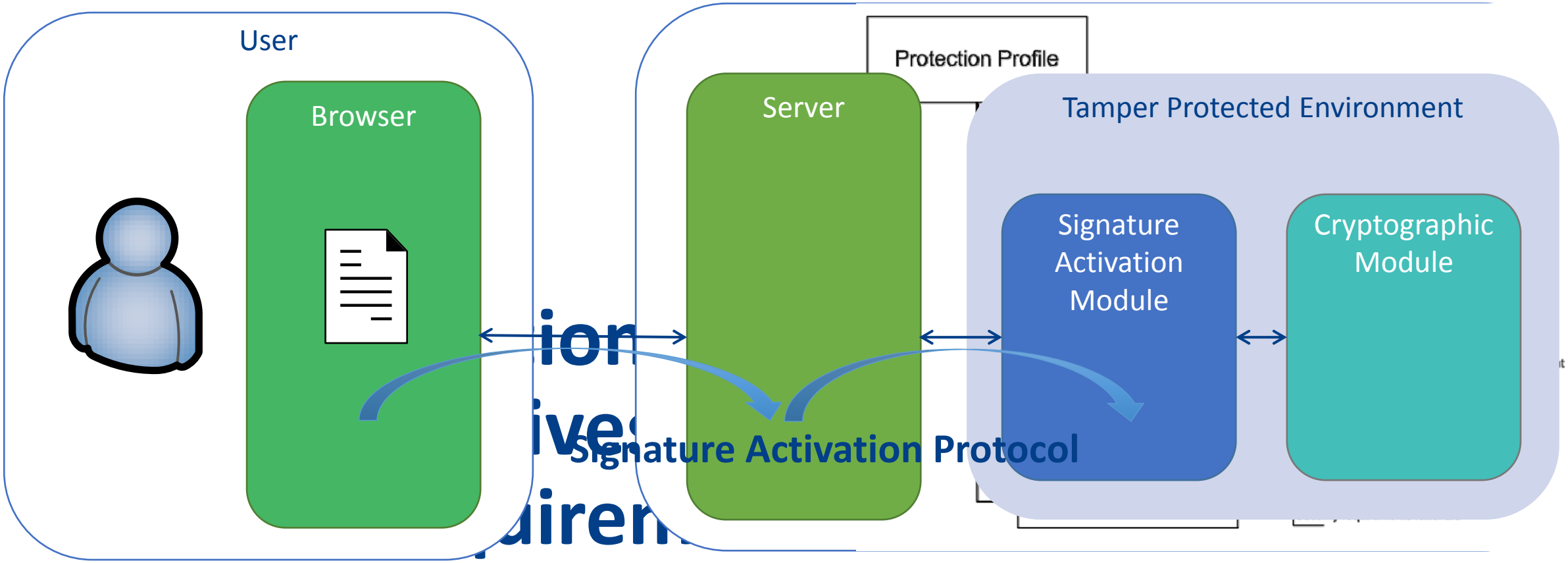


Implementing Decision 2016/650

- Common Criteria is now mandatory
- Smart card standards
- Nothing yet for remote signing

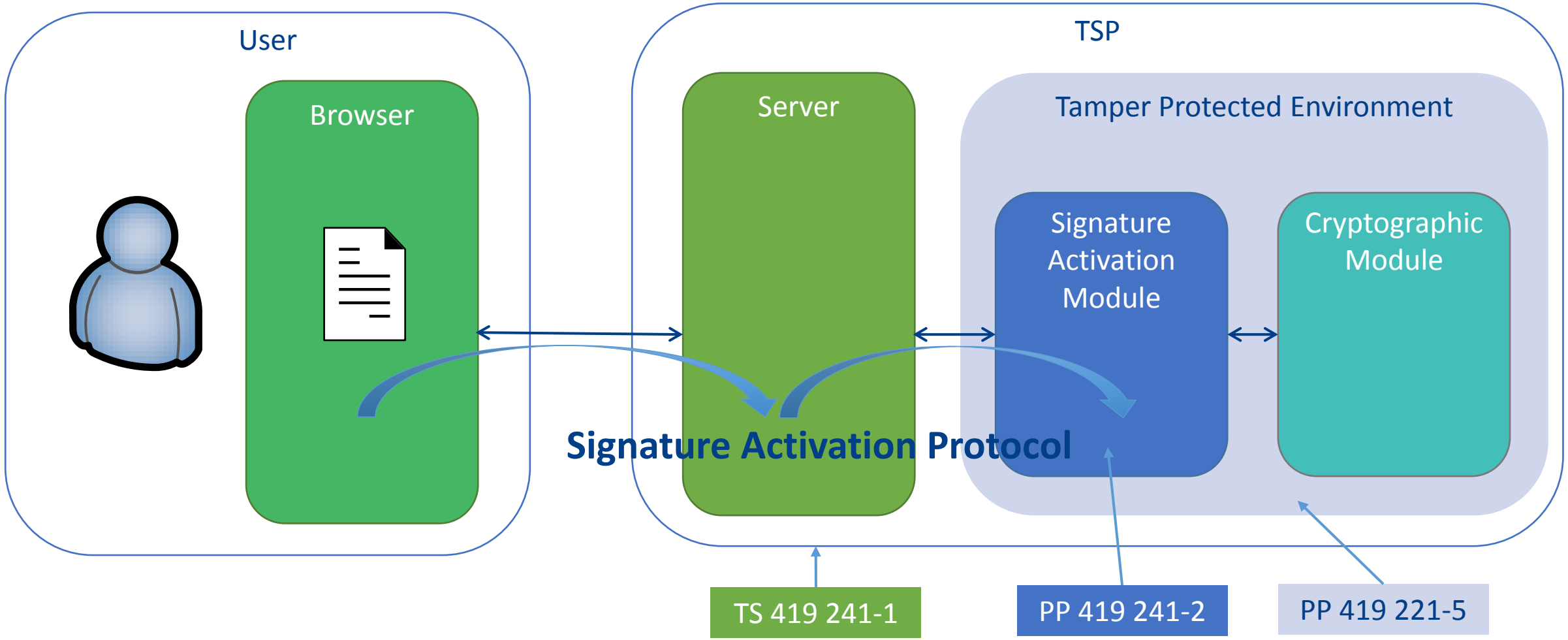
CRYPTOMATHIC

What does the PP contain?



CRYPTOMATHIC

Standards



CRYPTOMATHIC

Signature Activation

Signature Activation Protocol

- Transmits SAD in a secure way to the Signature Activation Module

Signature Activation Data (SAD)

- User is authenticated
- Document hash
- Key identifier

Signature Activation Module

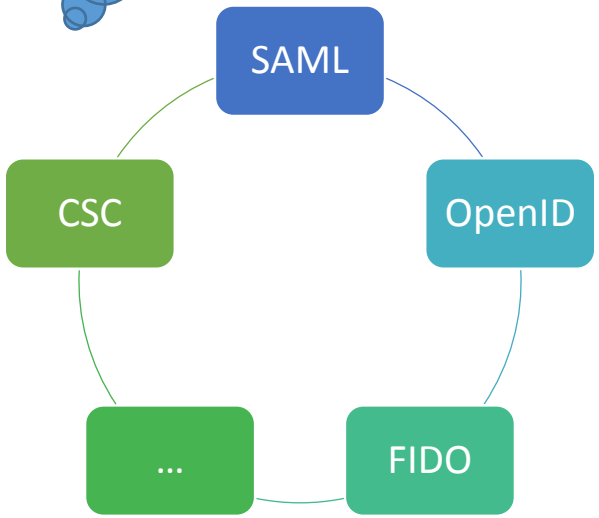
- Verifies SAD
- Uses the Cryptographic Module for the signature creation

User Authentication

Authentication mechanism with assurance level substantial

Signature Activation Data:
- User is authenticated
- Document hash
- Key identifier

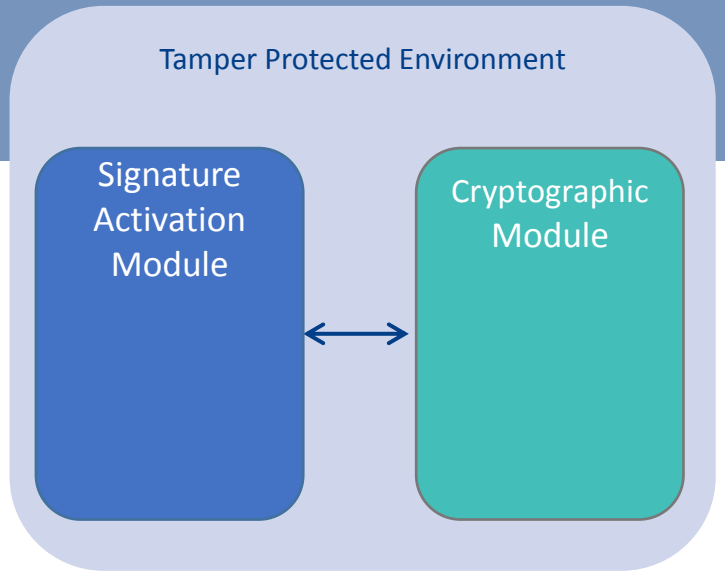
- **Directly by the SAM**
  - The SAM verifies all authentication factors
- **Indirectly by the SAM**
  - An external system verifies the authentication factors
  - Can be part of the TSP or a notified scheme
  - It shall provide an assertion, which must be verified by the SAM
- **Directly and indirectly**



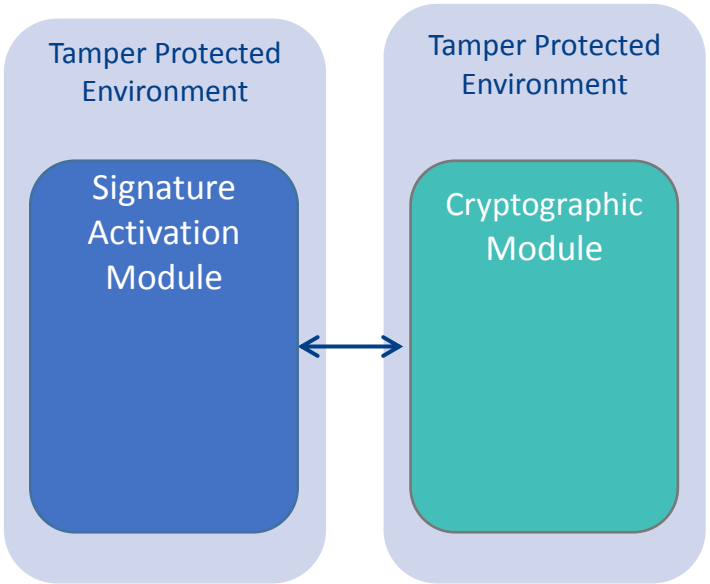
CRYPTOMATHIC

SAM deployments

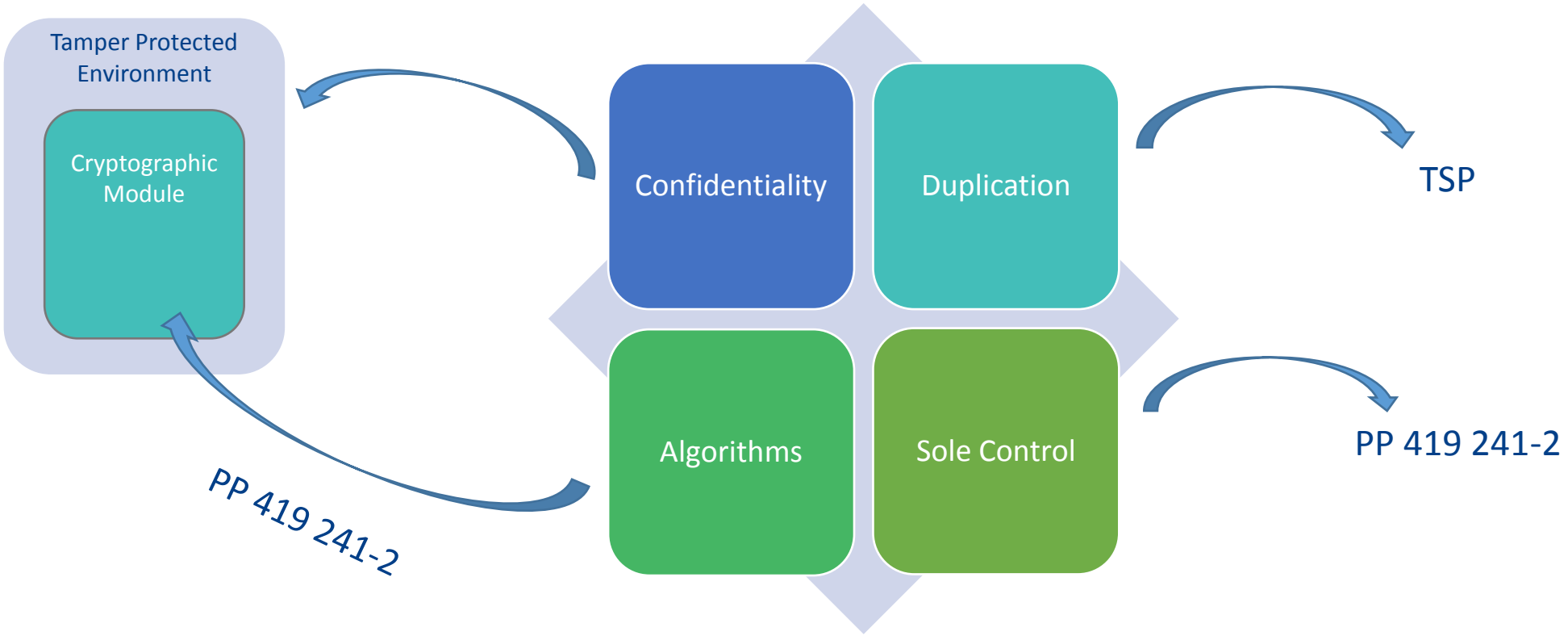
- **Common tamper protected environment**
  - Benefits from HSM certification



- **Seperate tamper proteced environment**
  - Certification must cover
    - Random Number Generation
    - Communication with Cryptographic Module
    - Physical Protection



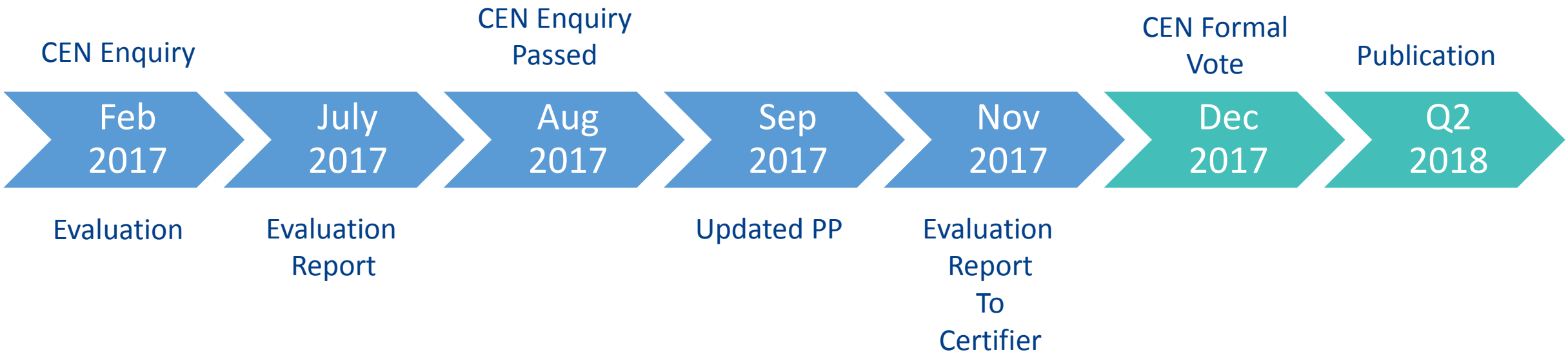
Do we meet the QSCD requirements?



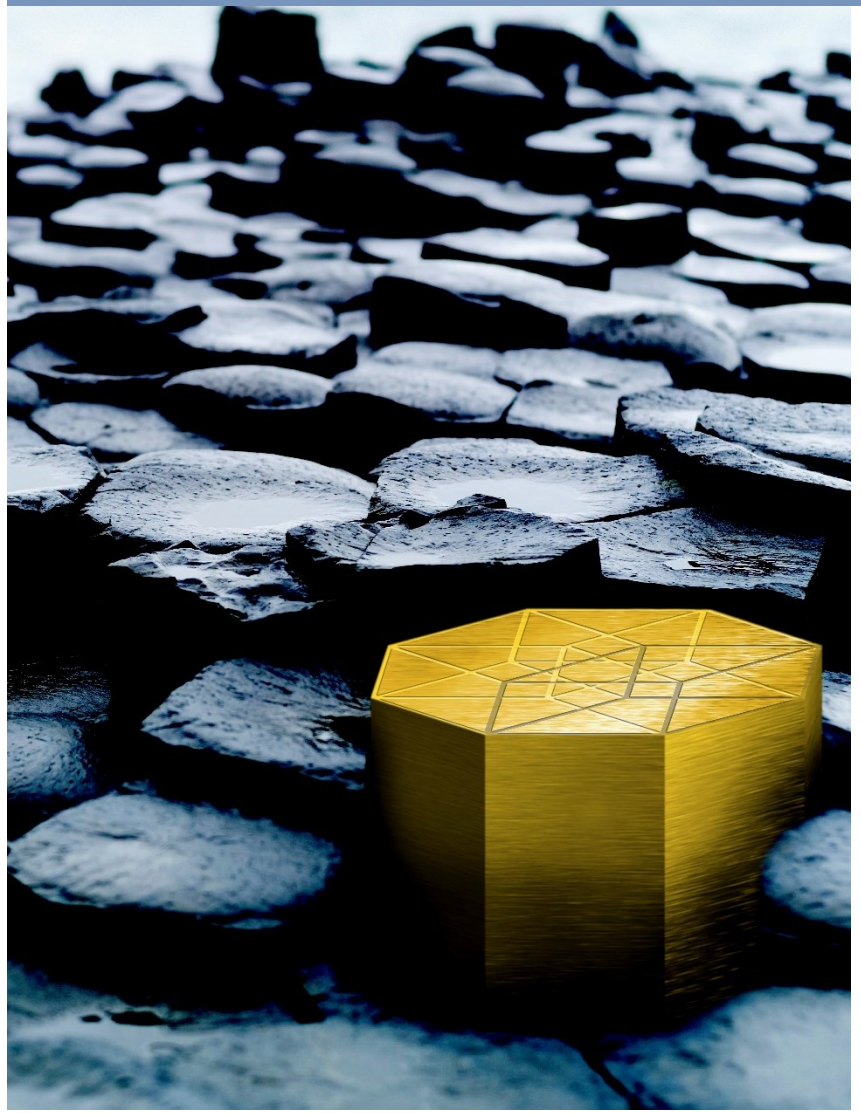
CRYPTOMATHIC

Status

- **CEN Process towards being a EU norm**
- **Evaluation for correctness**



CRYPTOMATHIC



Server Signing QSCD Protection Profile

CEN TC224 WG17 prPP 419 241-2

Jan Kjaersgaard

+45 90707665

Jan.Kjaersgaard@cryptomathic.com