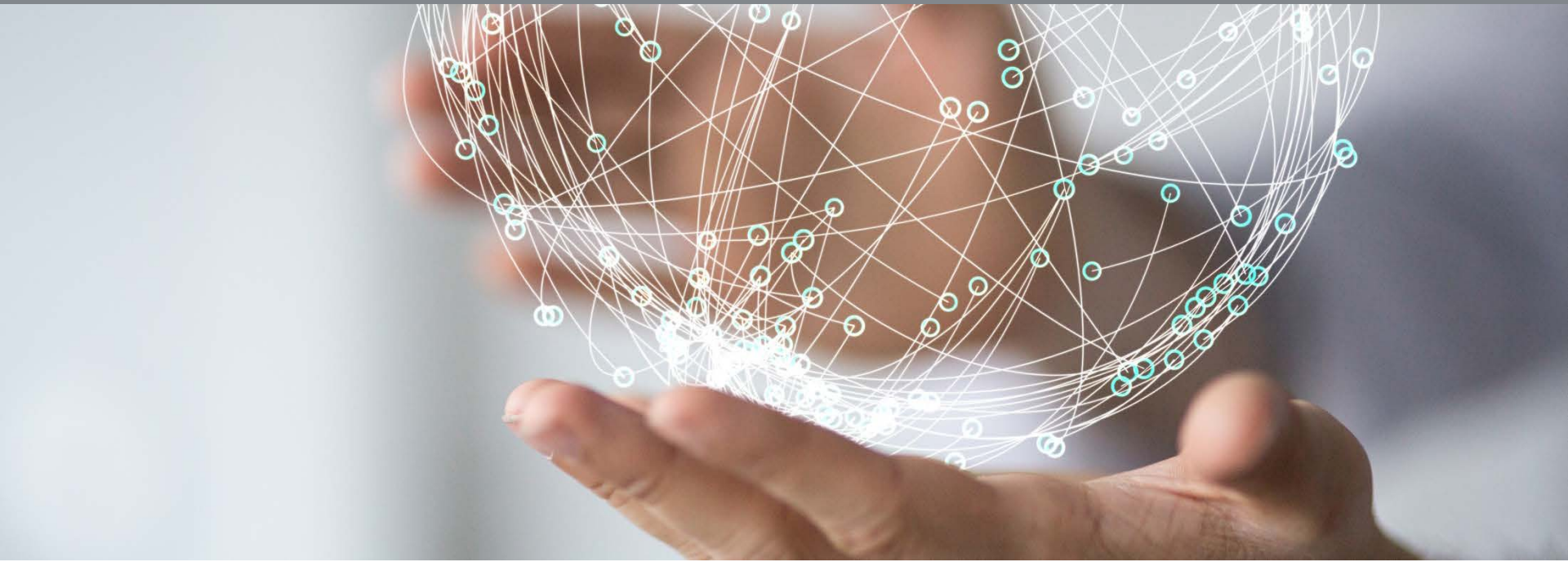


CEN Standardisation Activities for eIDAS (Regulation (EU) No 910/2014)

7. CA day (TSP compliance info day on eIDAS, ETSI, application services and CA/B-Forum requirements)

TÜViT / Bundesdruckerei, Berlin 2016-09-19

Dr. Christoph Sutter

TÜV NORD GROUP

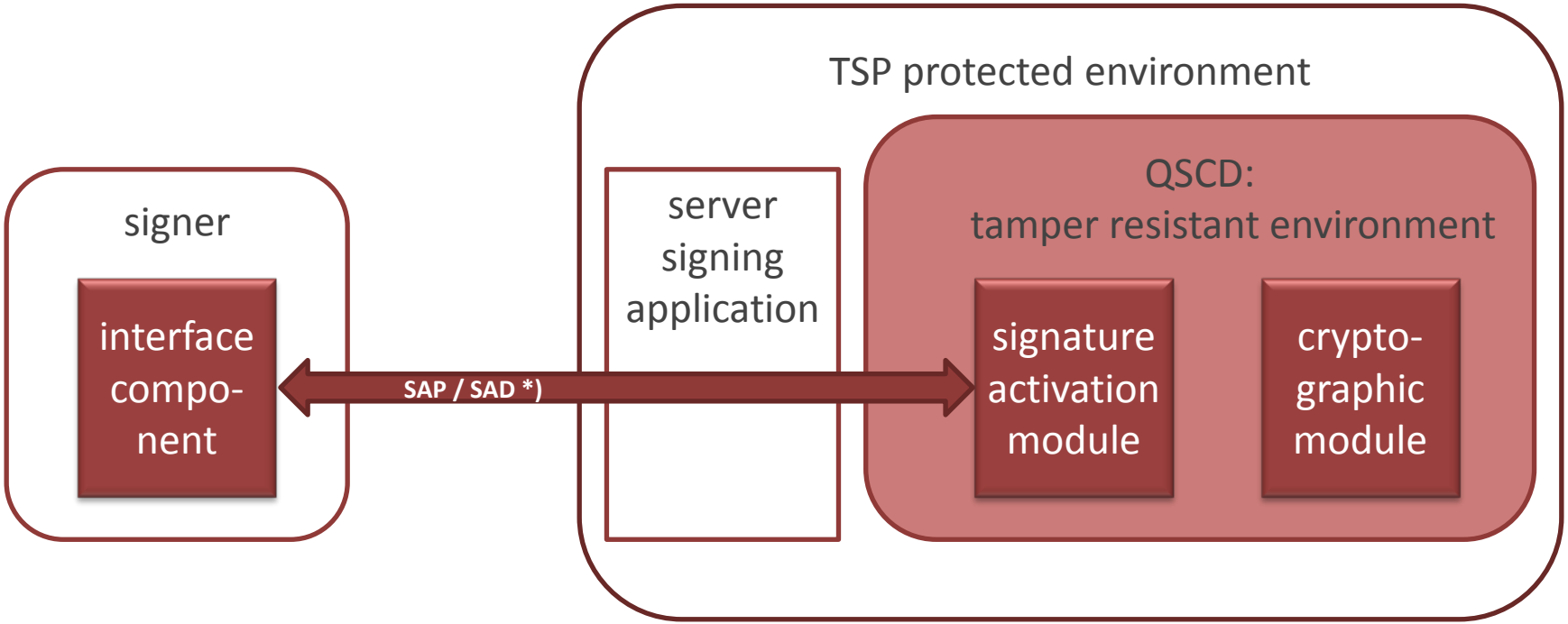
OVERVIEW

1. Remote electronic signatures
    - architecture for server signing
    - qualified electronic signature / seal creation devices (QSCD)
    - sole control on the use of the signature key
2. Status of current work items of CEN TC224 WG17 with relation to eIDAS
    - EN 419221-5 (cryptographic module)
    - EN 419241-1,-2,-3 (remote signatures)
    - EN 419231 (time stamping)
3. Summary

REMOTE ELECTRONIC SIGNATURES ACCORDING TO eIDAS

are explicitly permitted	•(because of) multiple economic benefits (recitals 51, 52) •condition: appropriate mechanisms and procedures to ensure sole control of the signatory on key usage
QSCD managed by qualified TSP	•qualified TSP for key generation and management (on behalf of the signatory) mandatory (annex II.3) •regular audit of the QSCD environment •supervision by supervisory body
QSCD-certification mandatory	•through notified (certification) public / private bodies •against requirements of annex II •security evaluation process with comparable level as ISO/IEC 15408 (Art. 30.3 (b) and Com. Imp. Decision (EU) 2016/650)

REMOTE ELECTRONIC SIGNATURE – SCHEME FROM CEN STANDARDS



*) SAP: Signature-Activation-Protocol
SAD: Signature-Activation-Data

SAD & SAP – SOLE CONTROL ON SIGNING KEY USAGE

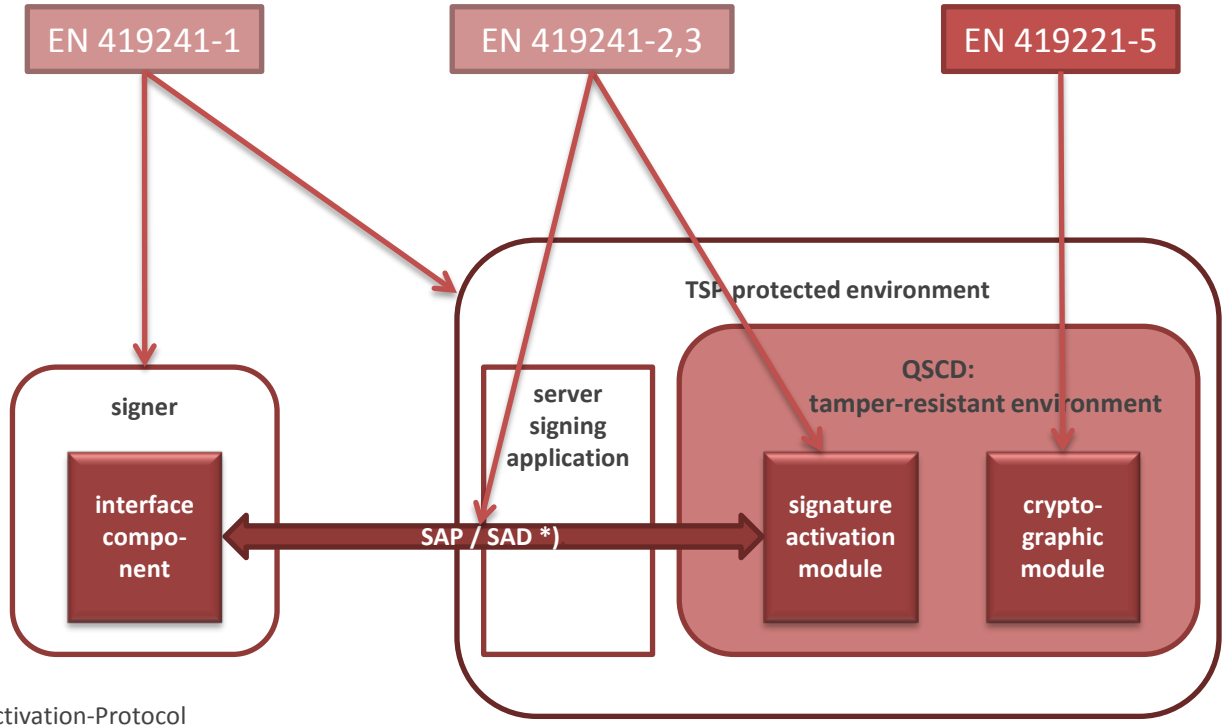
Signature Activation Data (SAD):

- under sole control of the signer
- binds signer authentication to
  - data to be signed and
  - signature key (signature creation data)
- verification in signature activation module within tamper resistant QSCD environment
- signature creation
  - after successful verification of the SAD and
  - within the QSCD cryptographic module

Signature Activation Protocol (SAP):

- ensures secure SAD transmission between signer interface component to signature activation module
- controls signature creation on data to be signed (one or more documents / data sets)
- ensures secure usage of the signature key through verification of signer's authentication

REMOTE SIGNATURES – CEN STANDARDS



*) SAP: Signature-Activation-Protocol
SAD: Signature-Activation-Data

STATUS OF CURRENT STANDARDS OF CEN TC224 WG17

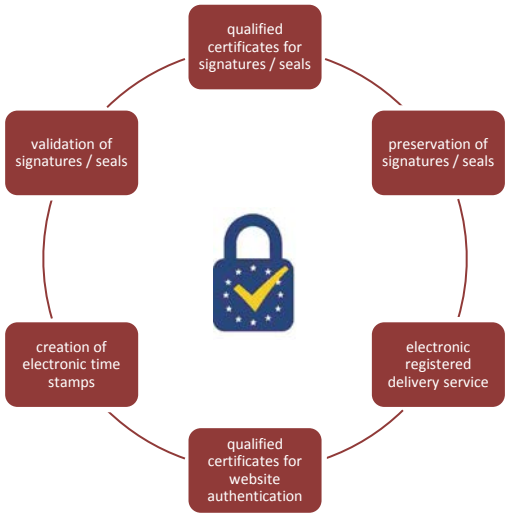
no	name (short)	CB	status	publication
EN 419 2**2**1-5	Crypto module for Trust Services	ANSSI, FR	@ ANSSI for certification	~Q3'2017
EN 419 2**3**1	time stamping	ANSSI (FR)	@ ANSSI for certification	~Q3'2017
EN 419 2**4**1-1	general req. for server signing	none	stable draft	~Q3'2017
EN 419 2**4**1-2,-3	QSCD for server signing	ANSSI (FR)	working draft under discussion	~Q**4**'2017

STATUS OF PUBLISHED STANDARDS OF CEN TC224 WG17

no	name (short)	CB	type of standard	publication
EN 419 2**1**1 (1-6)	SSCD	BSI (DE)	certified PP	2013, 2014
TS 419 2**2**1 (1-4)	Crypto module	ANSSI (FR)	certified PP	2016
EN 419 2**5**1 (1-3)	Authentication Device	none	non-certified PP	2013
TS 419 2**6**1	TWS for TSPs (certs, time-stamps)	none	no PP	2015

SUMMARY / OUTLOOK

- QSCD / eIDAS-relevant standards in scope of CEN TC224 WG17:
  - PP for cryptographic module (draft EN 419221-5)
  - PP for QSCDs for remote signatures (draft EN 419241-1,-2,-3)
  - PP for time-stamping (draft EN 419231)
- Standards will (presumably) published in 2017:
  - 419221-5 to be used to certify QSCD for TSP Operation
  - 419241-2/3 together with 419221-5 to be used to certify QSCDs for remote signing services (TSP managed)
  - 419231 could be used to certify TWS for time-stamping services
- Commission Implementing Decision (EU) 2016/650 could be amended:
  - EN 419221-5 as first standard for QSCDs operated in protected TSP environment
  - EN 419241-2/3 and EN 419221-5 as first standards for remoted (TSP managed) QSCDs
  - (besides CEN EN 419211 for user managed QSCDs)



Thank you very much for your attention!

Your contact

Dr. Christoph Sutter

Head of the Certification Body
TÜV Informationstechnik GmbH
IT Infrastructure
+49 201 8999-582
C.Sutter@tuvit.de

TÜV NORD GROUP