



Protection Profiles for Secure Signature-Creation Devices as European Standards

Dr. Susanne Pingel (Federal Office for Information Security)

Wolfgang Killmann (T-Systems GEI GmbH)

11. ICCC September 21st-23rd 2010, Antalya



Agenda

- ❑ Demand for Standards
- ❑ Definition of Secure Signature-Creation Device
- ❑ Scope of Standard
- ❑ Structure of Standard
- ❑ Contents of Standard
- ❑ Comparison with former Standard
- ❑ Status and Time Schedule



Demand for Standards (I)

DIRECTIVE 1999/93/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 13 December 1999 on a Community framework for electronic signatures

Article 3, §5: The Commission may, in accordance with the procedure laid down in Article 9, establish and publish reference numbers of generally recognised standards for electronic-signature products in the *Official Journal of the European Communities*.



Demand for Standards (II)

COMMISSION DECISION of 14 July 2003

A. List of the generally recognised standards ... Annex II

CWA 14167-2 (March 2002): security requirements for trustworthy systems managing certificates for electronic signatures — Part 2: cryptographic module for CSP signing operations — Protection Profile (CMSO-PP)

B. List of the generally recognised standards ... Annex III

CWA 14169 (March 2002): secure signature-creation devices



Definition of SSCD (I)

- ❑ **‘Secure Signature-Creation Device’ (SSCD)** means configured software or hardware used to implement the signature-creation data and the signature generation function (according to Annex III)
- ❑ Typical devices: smartcards, cryptomodules
- ❑ EU Directive, Annex III:
 - ❑ covers requirements for secure signature-creation devices to ensure the functionality of advanced electronic signatures
 - ❑ not covered: the entire system environment in which such devices operate



Definition of SSCD (II)

EU Directive, Annex III: Requirements for SSCDs

1. SSCDs must, by appropriate technical and procedural means, ensure at the least that:
 - (a) the signature-creation-data (SCD) used for signature generation can practically occur only once, and that their secrecy is reasonably assured;
 - (b) the SCD used for signature generation cannot, with reasonable assurance, be derived and the signature is protected against forgery using currently available technology;
 - (c) the SCD used for signature generation can be reliably protected by the legitimate signatory against the use of others.
2. SSCDs must not alter the data to be signed or prevent such data from being presented to the signatory prior to the signature process.



Scope of SSCD Standard (I)

- ❑ set-up as European standard (CEN EN 14169)
- ❑ issued by the European Committee for Standardization, Information Society Standardization System (CEN/ISSS)
- ❑ developed by the Technical Committee CEN/TC 224 “Personal identification, electronic signature and cards and their related systems and operations” and its Working Group WG 17
- ❑ fulfils the requirements of the EU Directive 1999/93/EC
- ❑ in accordance with article 3 and 9 of this European Directive these standards can be notified by the European Commission in the Official Journal of the European Communities as generally recognised standards for electronic-signature products



Scope of SSCD Standard (II)

- ❑ standard covers several documents specifying a suite of Protection Profiles (PPs) for SSCDs
- ❑ target of evaluation (TOE) for these PPs: SSCD (in different variants)
- ❑ PPs formally specify the security-functional and assurance requirements for SSCDs as defined in the EU Directive, Annex III
- ❑ CC certification of these PPs is intended (CC EAL 4+)
- ❑ for electronic signature products evaluated according to Common Criteria V 3.1 with a conformance claim to one or more of these PPs it is implied that the EU Member States shall presume compliance with the requirements in the EU Directive, Annex III for such products



Scope of SSCD Standard (III)

- this European standard:
 - specifies terms used in defining PPs for SSCDs
 - specifies functional and operational requirements for SSCDs
 - describes the target of evaluation (TOE) for these PPs
- covers an update of BSI-PP-0006-2002 and BSI-PP-0005-2002 resp. of the Electronic Signatures (E-SIGN) CEN/ISSS workshop agreement (CWA) 14169:2002, Annex C on the protection profile secure signature-creation devices, "EAL 4+"
- supersedes as well CWA 14168:2002



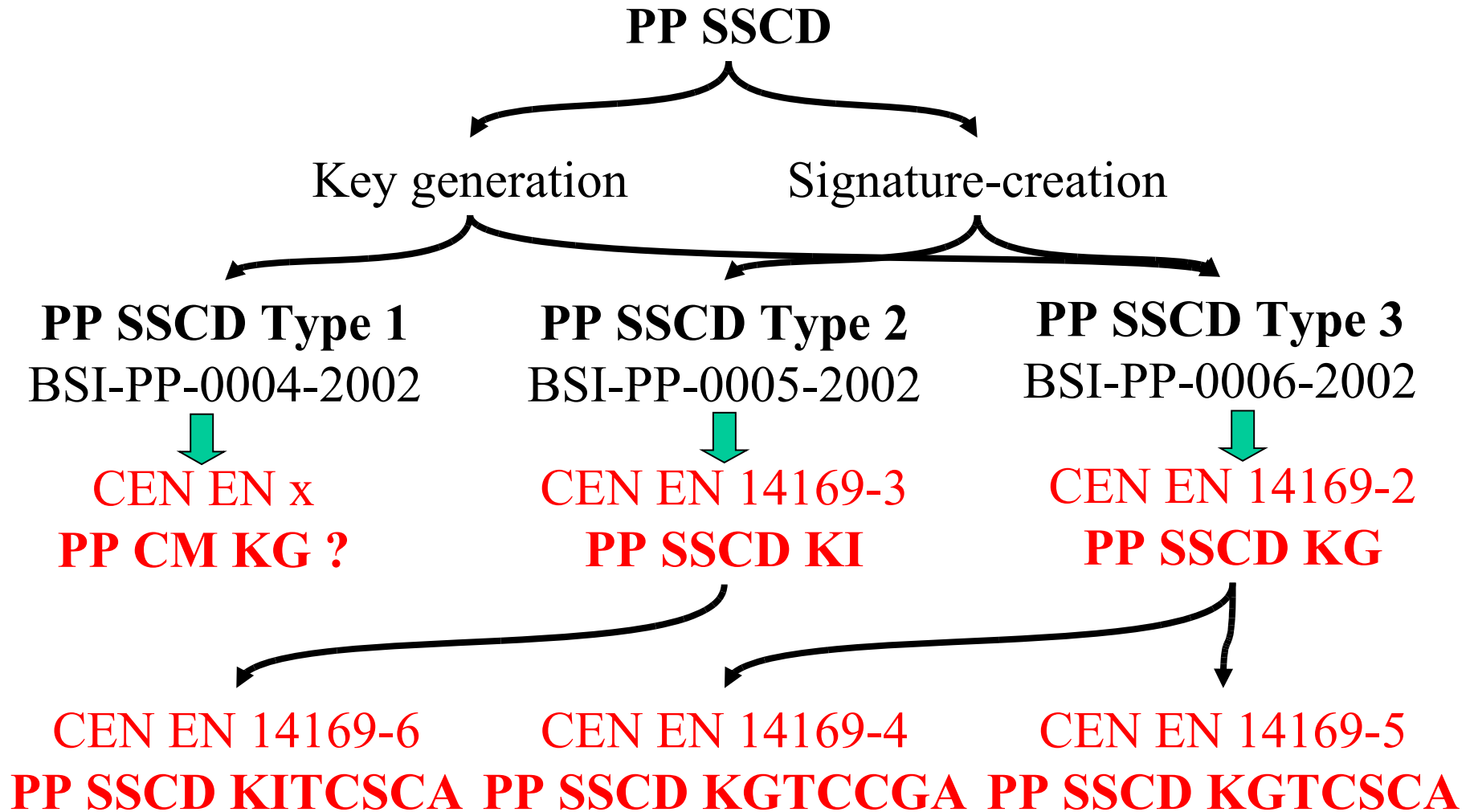
Structure of SSCD Standard (I)

Protection Profiles for Secure Signature Creation Device —

- ❑ Part 1: Overview
- ❑ Part 2: Device with key generation
- ❑ Part 3: Device with key import
- ❑ Part 4: Extension for device with key generation and trusted channel to certificate-generation application
- ❑ Part 5: Extension for device with key generation and trusted channel to signature-creation application
- ❑ Part 6: Extension for device with key import and trusted channel to signature-creation application



Structure of SSCD Standard (II)



Structure of SSCD Standard (III)

Part 1- Part 6: each PP requires strict conformance

Part 4, 5: conformance claim to Part 2

Part 6: conformance claim to Part 3

Goal: SSCD PPs combinable !

→ necessary from CC point of view:

appropriate extension of 'strict conformance'



Contents of CEN EN 14169-1

1 Scope

2 Normative references

3 Terminology (Legislative references, Technical terms)

4 Abbreviated terms

5 Protection Profile Overview

6 Target of Evaluation:

General, Functions of an SSCD (core, additional, others),
TOE life cycle, Operations of the TOE

7 TOE definitions:

TOE with key generation,

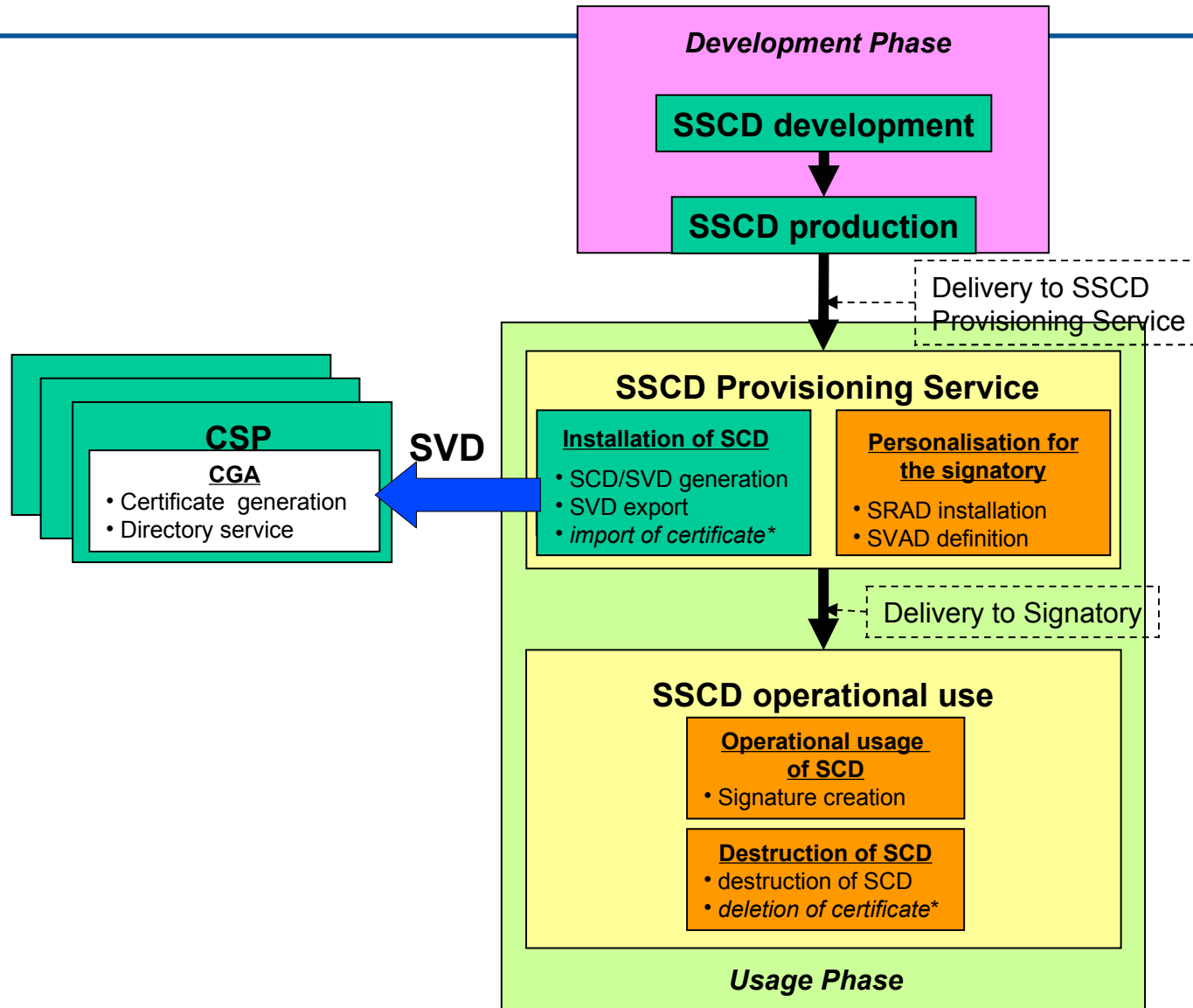
TOE with key import,

TOE with key generation and trusted channel to CGA,

TOE with trusted channel to SCA

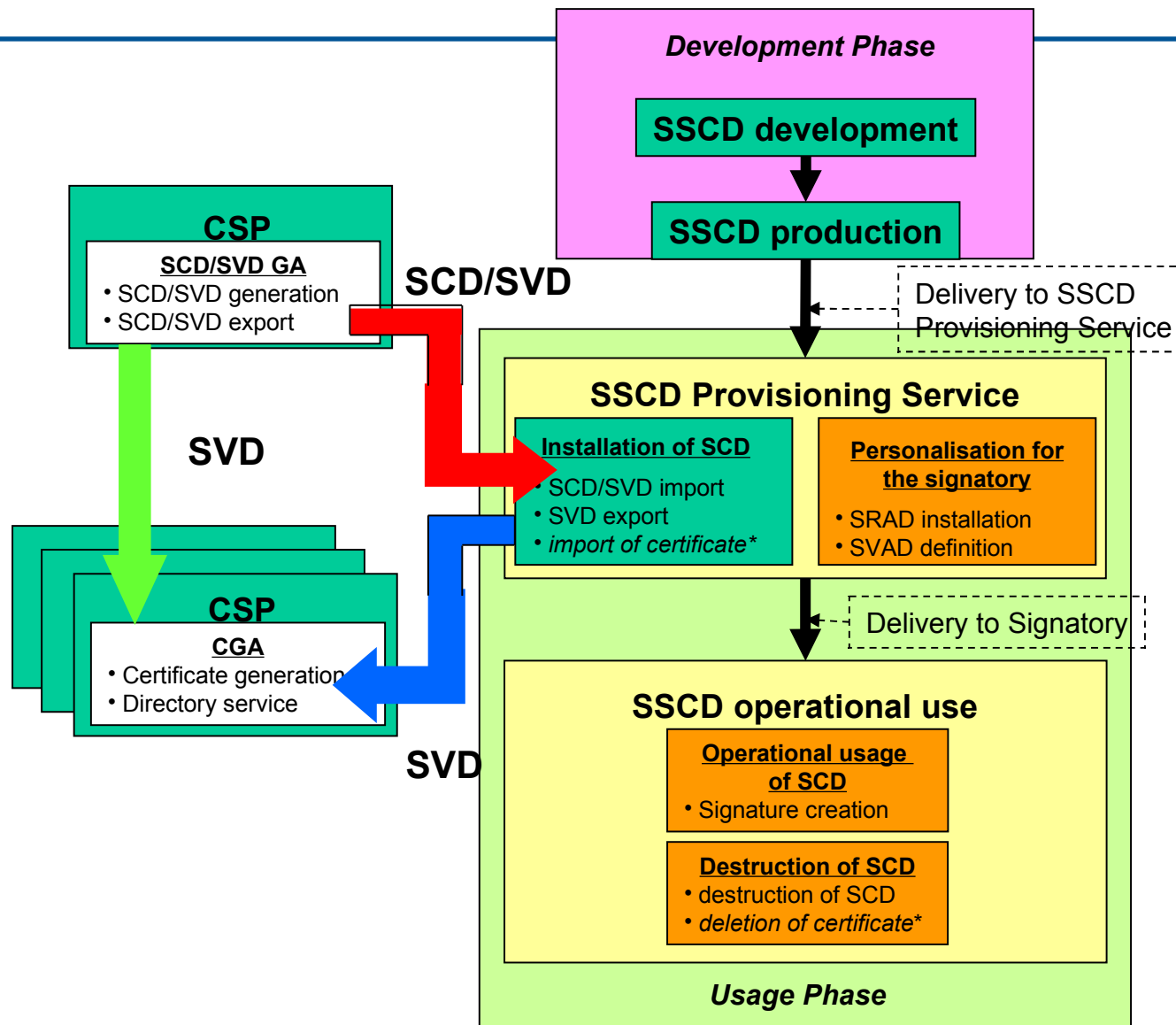
Annex A Comparison with CWA 14168:2002 Annex C (informative)

Life Cycle Model (On-board KG)





Life Cycle Model (KI)





Contents of CEN EN 14169-2

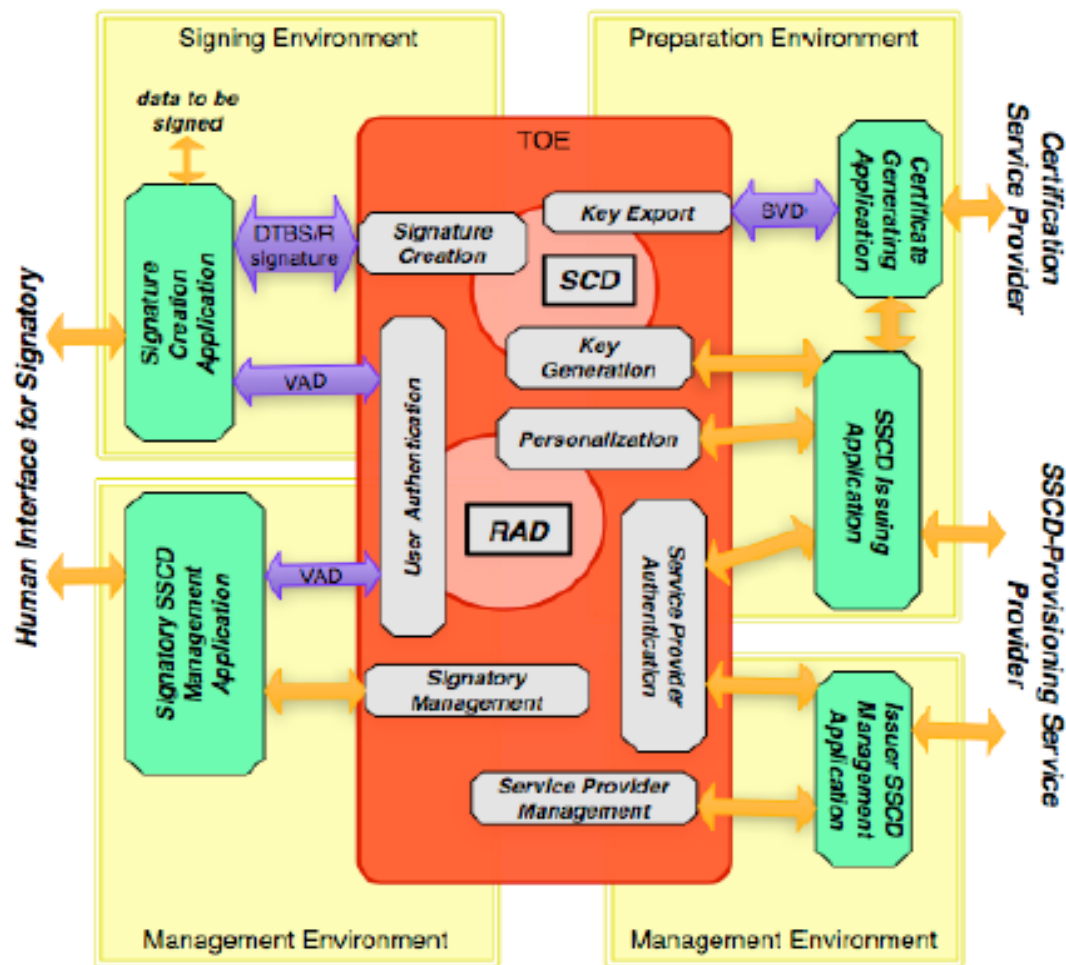
TOE: SSCD with core operations including key generation:

- ❑ generation of the signature-creation data (SCD) and the correspondent signature-verification data (SVD)
- ❑ export of the SVD for certification, optionally receipt and storage of certificate info
- ❑ initialisation of the user authentication data (RAD)
- ❑ switch the SSCD from a non-operational state to an operational state
- ❑ user authentication
- ❑ creation of digital signatures

constraint: secured operational environment for the SVD export and the signature-creation application !



Contents of CEN EN 14169-2



Refer to:
CEN EN 14169-1,
figure 2

TOE and operational environments with key generation



Contents of CEN EN 14169-3

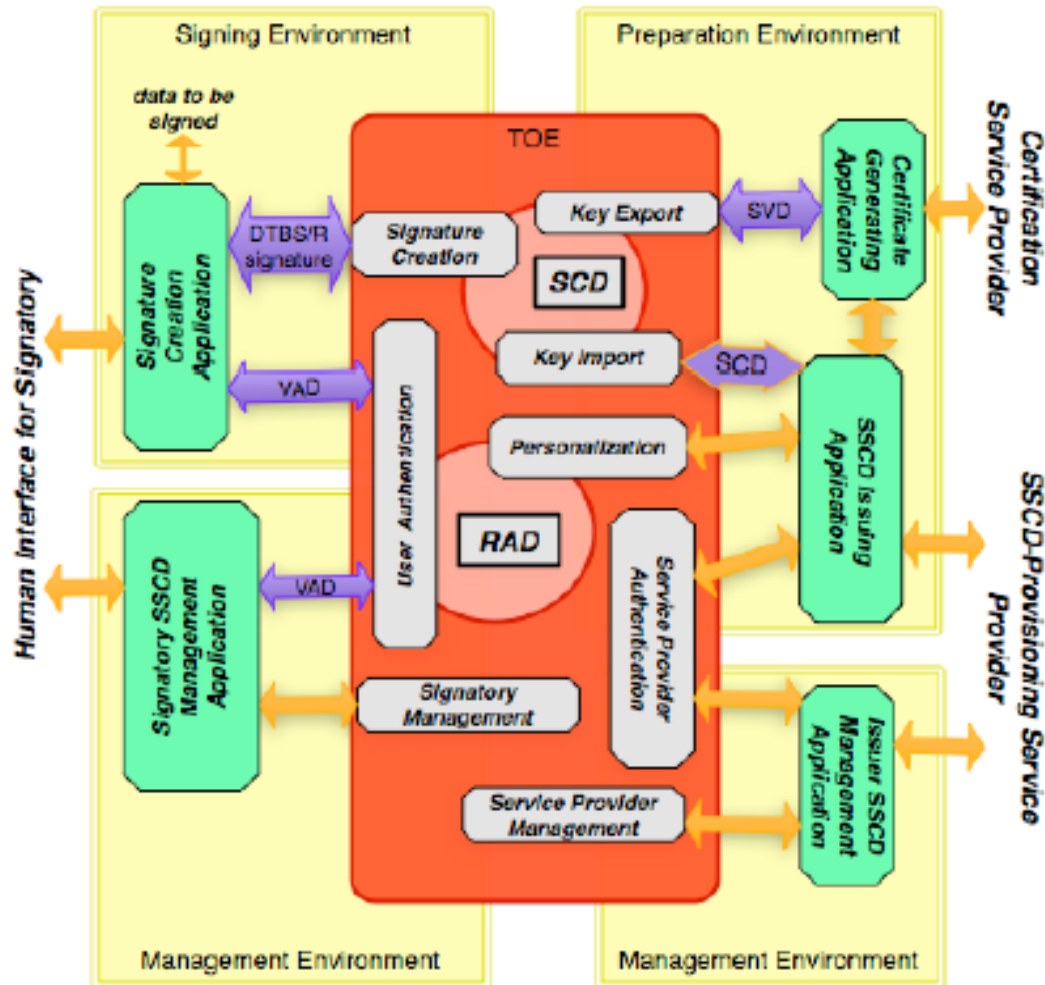
TOE:

SSCD that performs its core operations including the import of the signature key generated in a trusted manner outside the device

constraints:

- ❑ secured operational environment for the key generation and the key transfer to the SSCD !
- ❑ secured operational environment for the signature-generation application !

Contents of CEN EN 14169-3



Refer to:
 CEN EN 14169-1,
 figure 3

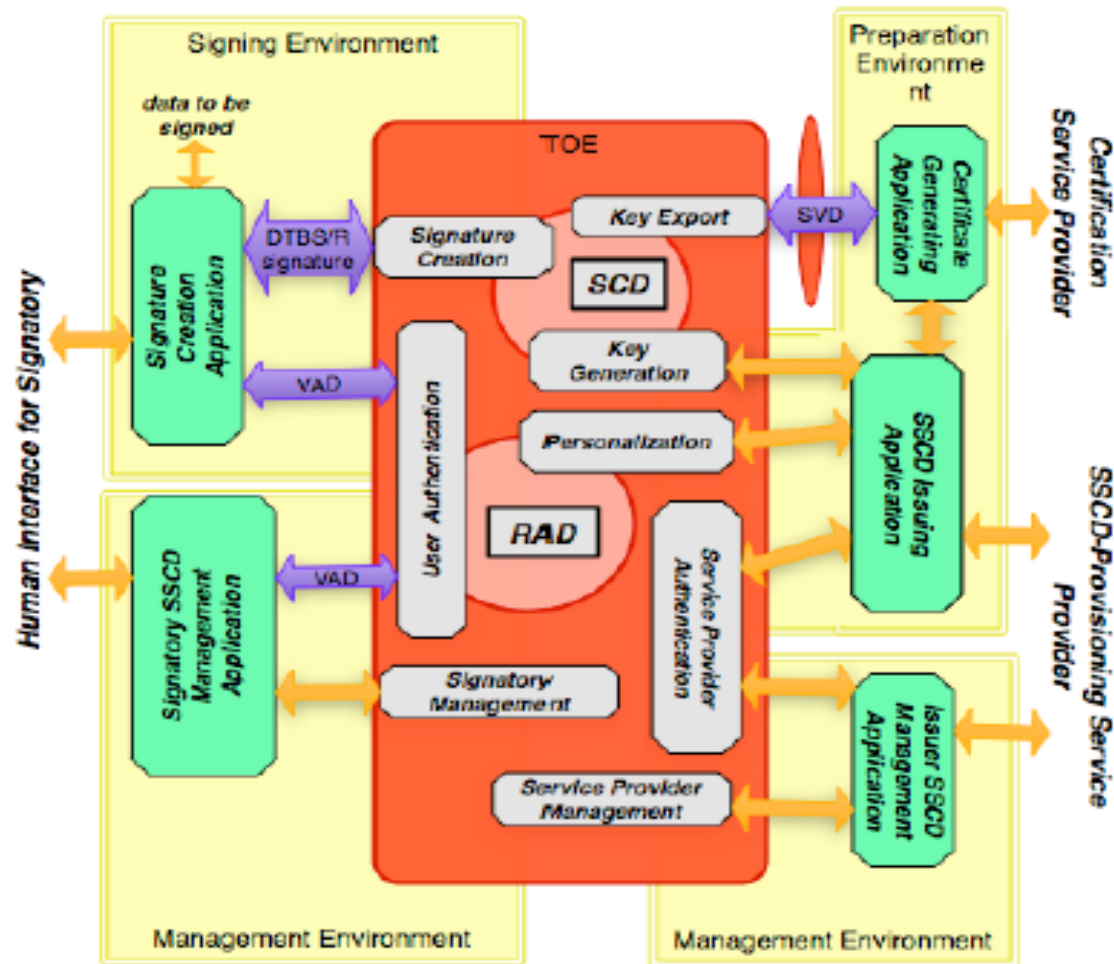
TOE and operational environments with key import



Contents of CEN EN 14169-4

Specification of an extension of the PP for an SSCD with key generation (CEN EN 14169-2) that additionally supports the establishment of a **trusted channel between the SSCD and a certificate-generating application (CGA)**

Contents of CEN EN 14169-4



Refer to:
 CEN EN 14169-1,
 figure 4

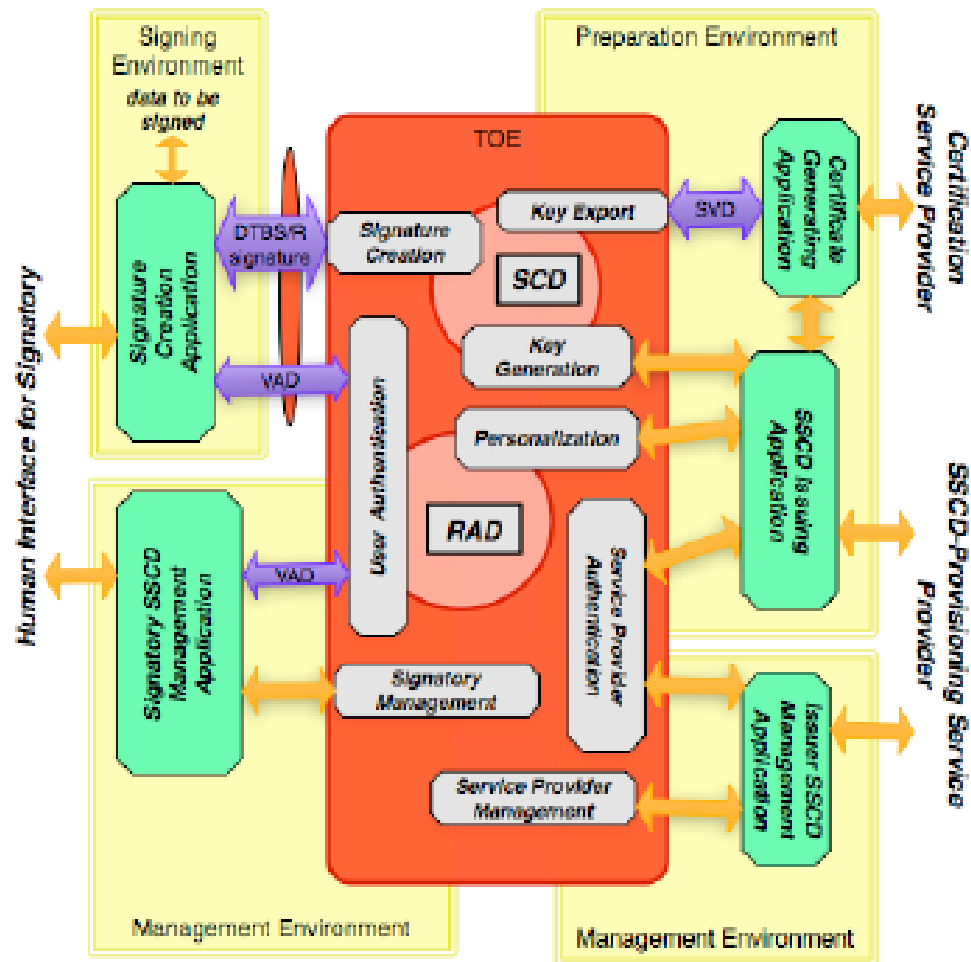
TOE and operational environments with trusted channel to CGA



Contents of CEN EN 14169-5

Specification of an extension of the PP for an SSCD with key generation (CEN EN 14169-2) that additionally supports the establishment of a **trusted channel between the SSCD and a signature-creation application (SCA)**

Contents of CEN EN 14169-5



Refer to:
CEN EN 14169-1,
figure 5

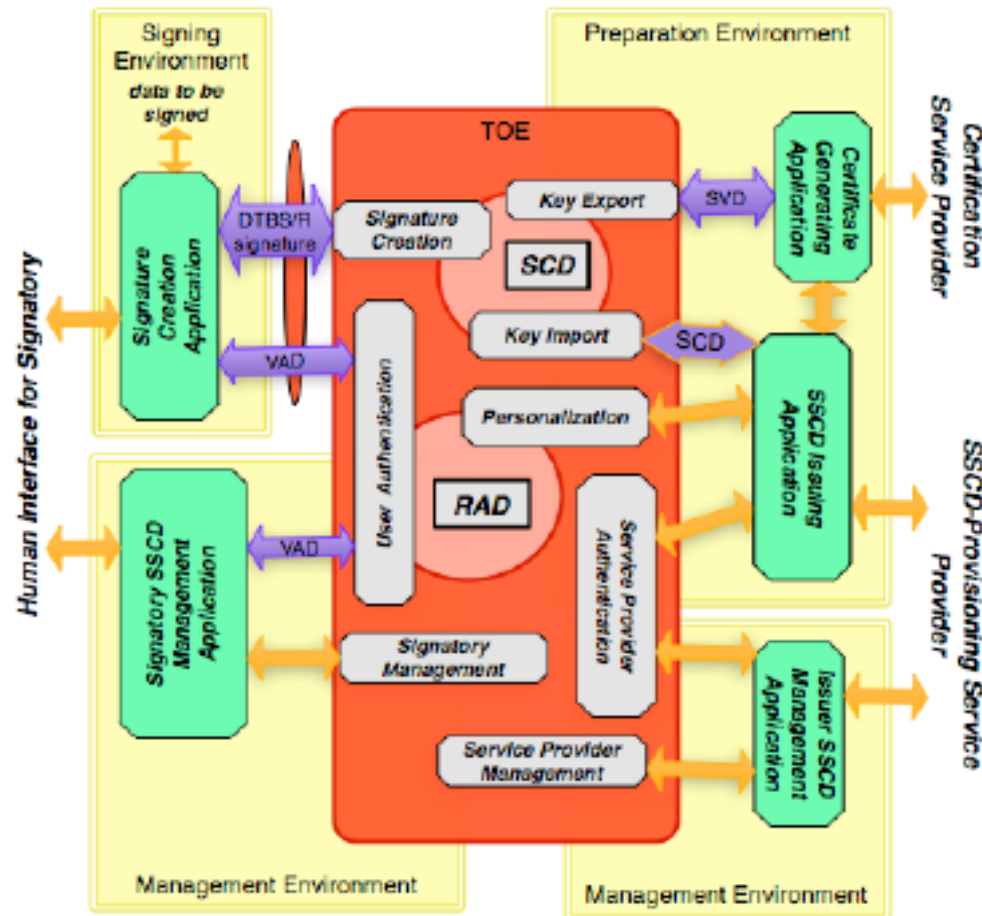
TOE and operational environments with key generation and trusted channel to SCA



Contents of CEN EN 14169-6

Specification of an extension of the PP for an SSCD with key import (CEN EN 14169-3) that additionally supports the establishment of a **trusted channel between the SSCD and a signature-creation application (SCA)**

Contents of CEN EN 14169-6



Refer to:
 CEN EN 14169-1,
 figure 6

TOE and operational environments with key import and trusted channel to SCA



Comparison with CWA 14168 (I)

CEN EN 14169-1, Annex A:

Comparison with CWA 14168:2002 Annex C (informative)

A.1 General

- ❑ CWA 14168 established a number of PPs for an SS CD, each PP addressing different functional configuration of the device (so-called “Type 1”, “Type 2” and “Type 3”)
- ❑ in CEN EN 14169: different functional configurations for an SS CD explicitly mentioned in the titles of its various parts
- ❑ “Type 2” in CWA 14168 → see CEN EN 14169-3
- ❑ “Type 3” in CWA 14168 → see CEN EN 14169-2
- ❑ “Type 1” in CWA 14168 → not supported by CEN EN 14169



Comparison with CWA 14168 (II)

A.2 Technical Differences

CEN EN 14169 supports new product features:

- ❑ **Multiple signing keys:** one device can store certificate info, which can be presented to the user to select/confirm a particular key to be used in a signature creation process
- ❑ **Off-line use:** SSCD can be used in environments deemed “trusted” by the user to create advanced/qualified electronic signatures without a cryptographically protected communication channel to the SCA
- ❑ **User-initiated device preparation:** issuer of SSCD may offer the user the option to initiate key generation or import after receiving the device → delivery of the product to the user without signing keys; additional signing keys may be created during the operational life of the device



Status / Time Schedule

CEN EN 14169 status for parts 1 to 6:

- ❑ in general: enquiry (public commenting period) over 5 months → followed by an approval by weighted vote by CEN members
- ❑ Part 2: CEN enquiry in October 2009
- ❑ Part 1, 3: first working draft for TC224 January 2010 changed to March 1st, draft for CEN enquiry in July 2010
- ❑ Part 4: first working draft for TC224 March 2010, draft for CEN enquiry in September 2010
- ❑ Parts 5, 6: first working draft for TC224 July 2010, draft for CEN enquiry in January 2011



Status / Time Schedule

Certification:

- ❑ Part 2 already CC certified by BSI in December 2009 (BSI-CC-PP-0059-2009) → maintenance planned due to some editorial changes and overall re-structuring of the existing standard's parts
- ❑ Parts 4, 5: CC evaluation started, first comments by evaluator received
- ❑ as all parts were already sent to CEN enquiry, no change of these documents is possible at present, but:
- ❑ changes resulting from evaluation comments will be incorporated together with the comments from CEN enquiry



Questions





Contact

Federal Office for Information Security (BSI)

Dr. Susanne Pingel

Godesberger Allee 185-189, D-53175 Bonn

Phone: +49 (0) 22899-9582-5023

Email: susanne.pingel@bsi.bund.de

Internet: www.bsi.bund.de



T-Systems GEI GmbH

Wolfgang Killmann

Vorgebirgsstr. 49, D-53119 Bonn

Phone: +49 (0) 228-9841-1150

Email: Wolfgang.Killmann@t-systems.com

Internet: www.t-systems.com