



www.thales-esecurity.com

Protection Profiles for Signing Devices



Report on CEN Standardisation Activities
on Security of Electronic Signatures

THALES

- ◆ **EU Legislation driving standardisation for Electronic Signature**
- ◆ **Past standardisation**
- ◆ **CEN TC 224 Working Group WG17 on
Protection Profiles for Signature Creation Devices**
- ◆ **Standardisation activities of TC 224 WG17**

Directive 1999/93

on a Community framework for electronic signatures

- ◆ Provides common basis for EU national legislation on Electronic Signatures

- ◆ Identifies “qualified” form of electronic signature meeting specific requirements defined in the Directive:
 - Advanced electronic signature (c.f. X.509 based digital signature)
 - Based on “qualified certificate”:
requirements defined in Annex I & II
 - Created by a “secure signature creation device” (SSCD)
requirements defined in Annex III

legally equivalent to “hand-written” signature

ANNEX III - Requirements for secure signature-creation devices

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

Specifications for SSCD & related Protection Profiles published in as “CEN Workshop Agreements” (CWA) issued 2001-2005

- ◆ **CWA 14167 - Security Requirements for Trustworthy Systems Managing Certificates for Electronic Signatures**
 - Part 1: System security requirements
 - Parts 2-4: protection profiles for cryptographic module used for signing
- ◆ **CWA 14169 – Protection Profile for secure signature-creation devices**

Note: CWAs do not have the legal recognition as “standards” and are only considered as documents with limited lifetime.

For full recognition need to be updated and issued as “European Norms”

TC 224 - Personal identification, electronic signature and cards and their related systems and operation

WG17 – Protection Profiles in the context of SSCD

- ◆ **Fully constituted body with voting to accept proposed standard by European National Standards Bodies**
- ◆ **Proposed European Norms drafted by WG17 consisting technical experts**
- ◆ **WG17 member companies include:
TÜViT, Gemalto, Thales, SRC, Oppida, Giesecke & Devrient, ANSSI, ANTS, T-Systems, Bull**

- ◆ **EN 14169 – SSCD protection profiles**
- ◆ **EN 16248 – Authentication device protection profiles**
- ◆ **EN 14167 – Cryptographic modules for Certification Service Providers protection profiles**
- ◆ **EN tbd - Security requirements for trustworthy systems managing certificates for electronic signature**
- ◆ **EN tbd - Security requirements for server signing**
- ◆ **EN tbd - Protection profiles for signature creation and verification application**

EN 14169 (replaces CWA 14169)

“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*

Status:

Being prepared for final national ballots

Specifications shortly to be formally evaluated

EN 16248

Security requirements for device for authentication

- *Part 1* Protection profile for core functionality
- *Part 2*: Protection profile for extension for trusted channel to certificate generation application
- *Part 3*: Additional functionality for security targets

For applications only requiring authentication (not e-signatures)

Status:

Proposed draft Under national review (CEN Enquiry)

EN 14167 (replaces CWA 14167 parts 2-4) Title & EN reference to be confirmed

Parts to include:

- Cryptographic module for CSP signing operations= with back-up
- Cryptographic module for CSP key generation services
- Cryptographic module for CSP signing operations

CSP = Certification Service provider

e.g Certification Authority, Time-stamping authority, Certificate Status (OCSP)

Status:

Work started on initial drafts

First round of national review (“CEN Enquiry”) expected early 2012

EN tbd (replaces CWA 14167 part 1)

Security requirements for trustworthy systems managing certificates for electronic signature

- ◆ **Semi formal definition of security requirements not a fully evaluated protection profile**

Status:

Work started on initial drafts

First round of national review (“CEN Enquiry”) expected early 2012

EN tbd

Security requirements Secure requirements for server signing

- ◆ **Networked server holding signing keys and signing documents on behalf of remote users (e.g. Mobile phone)**
- ◆ **Semi formal definition of security requirements not a fully evaluated protection profile**

Status:

Work started on initial drafts

First round of national review (“CEN Enquiry”) expected early 2012

EN tbd

Protection profiles for signature creation and verification application

- Part 1 - Introduction
- Part 2 - Signature creation application: Core
- Part 3 - Signature creation application
Possible extensions (e.g. Content checker, certificate management, secure SSCD channel)
- Part 4 - Signature verification application: Core
- Part 5 - Signature verification application
Possible extensions (e.g. Content checker, time-stamp attribute, complete validation data attribute, explicit policy)

Status:

Working drafts under expert review in WG 17

Proposed drafts expected ready for national review end 2011.

CEN TC 224 WG17 is producing standards:

- ◆ **Covering range of e-signatures security requirements**
- ◆ **Fully standardised as European Norms**

Thank you for your attention.

Any questions ?



marcus.streets@thales-esecurity.com