Rubrica legale - ICT Security Maggio 2004
Autore: Daniela Rocca (SG&A)
Gianluca Ramunno (Politecnico di Torino)

The standardisation effort in CEN/SSS E-Sign workshop

In 1999 the European Commission launched the EESSI (Euroepan Electronic Signature Standardisation Initiative) to support the European Directive 1999/93/EC on the electronic signatures.

The activities were divided into two working groups: the ETSI TC-SEC ESI (now TC-ESI) and the CEN/ISSS E-Sign.

These working groups, during these years, have worked actively in order to standardize the technical aspects left by the European Directive to the standardisation bodies. So, a certain number of deliverables has been approved. Some of them have been referenced on the Official Journal of the European Community. Some of them are still *in itinere*. Some of them are in the phase of maintenance.

While the activities of ETSI TC-ESI will continue, these of CEN/ISSS E-Sign have been closed on February 2004 with the achievement of the goals.

The CEN BT/WG 159 is an *ad hoc* working group created by CEN to deal with the maintenance of the documents delivered by the CEN/ISSS E-Sign workshop. The kick-off meeting was held on 4th March with the following provisional conclusions.

The CWAs will be grouped in three categories:

- the first attempt will be made to transpose as many CWAs as possible (make them ENs or ISes);
- for some CWAs transferring their ownership to some *de jure* organization is an option;
- the usage of the remaining ones will be monitored; the ones with market relevance will be transferred or transposed, the others will be allowed to lapse.

The purpose of this document is to syntetize the state of art in the field of the documents delivered by CEN/SSS E-Sign workshop.

For each CWA the following details are reported:

- CEN ID
- CWA title
- Publication date
- Relation (if any) with specifications by ETSI and/or other bodies
- Notes (if any)

References to relevant web pages for WS/E-Sign CWAs

WS/E-Sign published CWAs:
http://www.cenorm.be/cenorm/businessdomains/businessdomains/informationsocietystandardizationsystem/published+cwas/cwa+download+area.asp#ES
WS/E-Sign CWAs: http://www.uninfo.polito.it/ws_esign/docs.htm
SERMA Technologies: http://www.serma.com/
DCSSI: http://www.ssi.gouv.fr/en/dcssi/index.html
BSI: http://www.bsi.bund.de/
BSI list of SSCD certified PPs: http://www.bsi.bund.de/cc/pplist/pplist.htm#signatur
TÜV: http://www.tuev-sued.de/international.asp

Autore: Daniela Rocca (SG&A)
Gianluca Ramunno (Politecnico di Torino)

CEN/ISSS WS/E-Sign CWAs published, approved and being published:

CEN Identifier	CWA Title	Publication date	Related specifications	Notes
CWA 14167-1:2003	Security Requirements for Trustworthy Systems Managing Certificates for Electronic Signatures - Part 1: System Security Requirements	June 2003	CWA 14169:2004, CWA 14172-3:2004, ETSI TS 101 456, ETSI TS 101 862	1) Supersedes CWA 14167-1:2001 2) Referenced in Official Journal with wrong publication month: the reference must be corrected
CWA 14167-2:2004	Security Requirements for Trustworthy Systems Managing Certificates for Electronic Signatures - Part 2: Cryptographic Module for CSP Signing Operations with Backup - Protection Profile (CMCSOB-PP)	Waiting for publication (expected not before April 2004)	CWA 14172-7:2004	1) Will supersede CWA 14167-2:2002 2) PP (v. 0.28) successfully evaluated by SERMA and certified by DCSSI (waiting for publication) 3) Companion specification of CWA 14167-4:2004 (spin-off from the previous version: CWA14167-2:2002) 4) Previous revision (2002) referenced in Official Journal: the reference must be updated after the CEN publication 5) There is the need to deal with some comments received during the voting and not yet taken into account; these comments are listed in WSES N 0414, an internal WS/E-Sign document
CWA 14167-3:2004	Security Requirements for Trustworthy Systems Managing Certificates for Electronic Signatures - Part 3: Cryptographic Module for CSP Key Generation Services - Protection Profile (CMCKG-PP)	Waiting for publication (expected not before April 2004)	CWA 14172-7:2004	1) Will supersede CWA 14167-3:2003 2) PP (v. 0.12) not evaluated because of lack of sponsors, but updated according to the certified CWA 14167-2 and CWA 14167-4 after their certifications; *if a sponsor were found, it can be submitted for evaluation* 3) There is the need to deal with some comments received during the voting and not yet taken into account; these comments are listed in WSES N 0414, an internal WS/E-Sign document

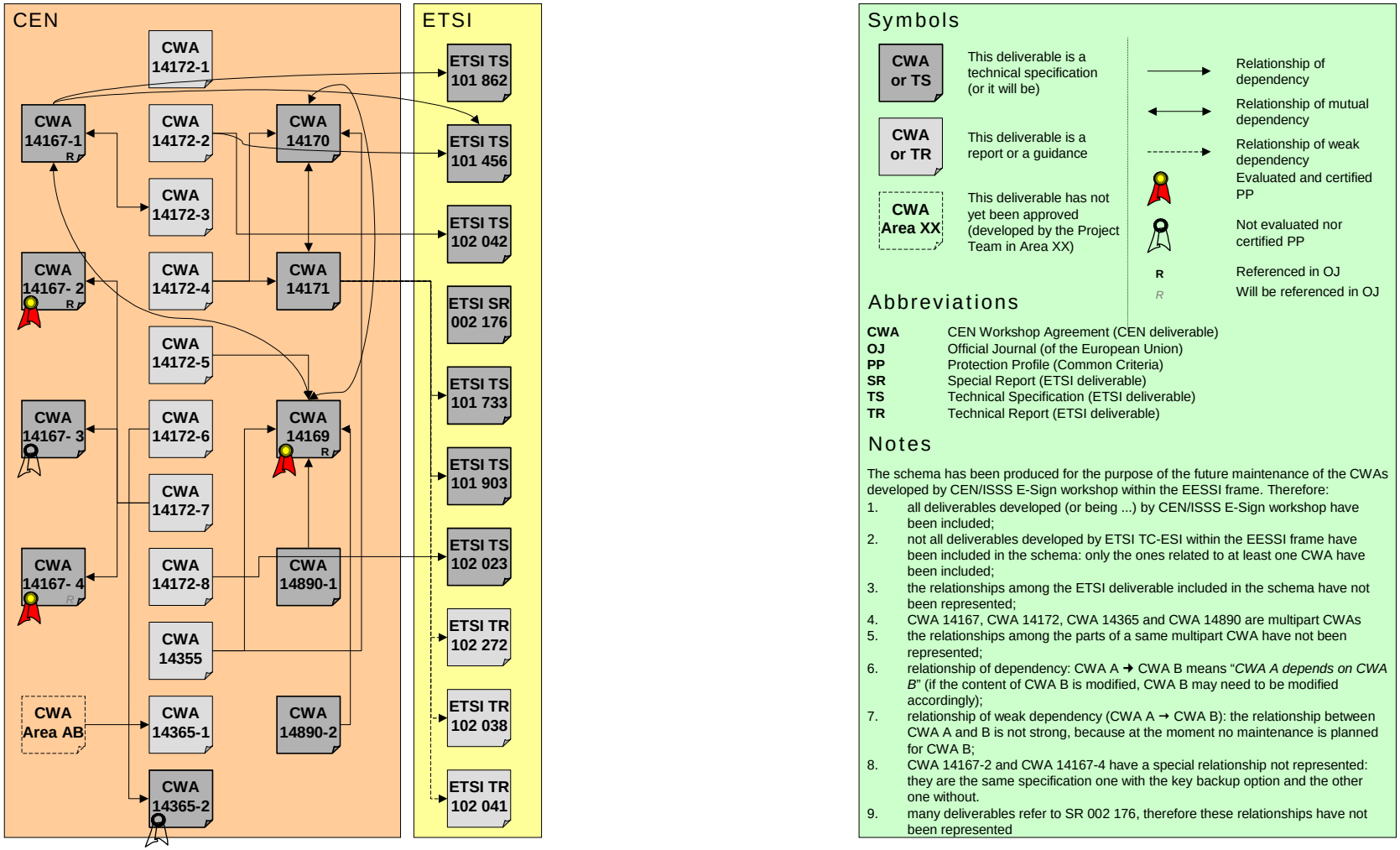
CEN Identifier	CWA Title	Publication date	Related specifications	Notes
CWA 14167-4:2004	Security Requirements for Trustworthy Systems Managing Certificates for Electronic Signatures - Part 4: Cryptographic Module for CSP Signing Operations - Protection Profile (CMCSO-PP)	Waiting for publication (expected not before April 2004)	CWA 14172-7:2004	1) PP (v. 0.28) successfully evaluated by SERMA and certified by DCSSI (waiting for publication) 2) Companion specification of CWA 14167-2:2004 (spin-off from the previous version: CWA14167-2:2002): same specification as CWA 14167-2:2004 without the backup function 3) Previous revision (CWA14167-2:2002, whose this document is a spin-off) referenced in Official Journal: the reference to this new part must be added after the CEN publication 4) There is the need to deal with some comments received during the voting and not yet taken into account; these comments are listed in WSES N 0414, an internal WS/E-Sign document
CWA 14169:2004	Secure Signature-Creation Devices, version 'EAL 4+'	Waiting for publication (expected not before April 2004)	CWA 14890-1:2004, CWA 14890-2:2004, CWA 14172-5:2004, CWA 14355:2004	1) Will supersede CWA 14169:2002 2) Three PPs successfully evaluated by TÜV and certified by BSI (Type 1, v. 1.05 – Type 2, v. 1.04 – Type 3, v. 1.05) 3) Some small errors were found after the certification; the version 2004 of this specification include the list of the corrections that the implementors should apply. The MS Word sources of the three PPs properly amended (v. 1.06) are already available: *if a new sponsor were found, they could be submitted for a new evaluation* 4) Previous revision (2002) referenced in Official Journal: the reference must be updated after the CEN publication
CWA 14170:2004	Security Requirements for Signature Creation Applications	Waiting for publication (expected not before April 2004)	CWA 14172-4:2004, CWA 14355:2004, CWA 14171:2004	1) Will supersede CWA 14170:2001
CWA 14171:2004	General Guidelines for Electronic Signature Verification	Waiting for publication (expected not before April 2004)	ETSI TS 101 733, ETSI TS 101 903, ETSI TR 102 272, ETSI TR 102 038 ETSI TR 102 041, CWA 14172-4:2004, CWA 14170:2004	1) Will supersede CWA 14171:2001

CEN Identifier	CWA Title	Publication date	Related specifications	Notes
CWA 14172-1:2004	EESSI Conformity Assessment Guidance - Part 1: General introduction	Waiting for publication (expected not before April 2004)		1) Will supersede CWA 14172-1:2001
CWA 14172-2:2004	EESSI Conformity Assessment Guidance - Part 2: Certification Authority services and processes	Waiting for publication (expected not before April 2004)	ETSI TS 101 456, ETSI TS 102 042	1) Will supersede CWA 14172-2:2001
CWA 14172-3:2004	EESSI Conformity Assessment Guidance - Part 3: Trustworthy systems managing certificates for electronic signatures	Waiting for publication (expected not before April 2004)	CWA 14167-1:2003	1) Will supersede CWA 14172-3:2001
CWA 14172-4:2004	EESSI Conformity Assessment Guidance - Part 4: Signature-creation applications and general guidelines for electronic signature verification	Waiting for publication (expected not before April 2004)	CWA 14170:2004, CWA 14171:2004	1) Will supersede CWA 14172-4:2001
CWA 14172-5:2004	EESSI Conformity Assessment Guidance - Part 5: Secure signature creation devices	Waiting for publication (expected not before April 2004)	CWA 14169:2004	1) Will supersede CWA 14172-5:2001
CWA 14172-6:2004	EESSI Conformity Assessment Guidance - Part 6: Signature-creation devices supporting signatures other than qualified	Waiting for publication (expected not before April 2004)	CWA 14365-2:2004	
CWA 14172-7:2004	EESSI Conformity Assessment Guidance - Part 7: Cryptographic modules used by Certification Service Providers for signing operations and key generation services	Waiting for publication (expected not before April 2004)	CWA 14167-2:2004, CWA 14167-3:2004, (CWA 14167-4:2004)	
CWA 14172-8:2004	EESSI Conformity Assessment Guidance - Part 8: Time-stamping Authority services and processes	Waiting for publication (expected not before April 2004)	ETSI TS 102 023	
CWA 14355:2004	Guidelines for the implementation of Secure Signature-Creation Devices	Waiting for publication (expected not before April 2004)	CWA 14169:2004, CWA 14170:2004	1) Will supersede CWA 14355:2002

CEN Identifier	CWA Title	Publication date	Related specifications	Notes
CWA 14365-1:2004	Guide on the use of Electronic Signatures - Part 1: Legal and Technical Aspects	Waiting for publication (expected not before April 2004)	CWA ?????:2004 (Area AB)	1) Will supersede CWA 14365:2003
CWA 14365-2:2004	Guide on the use of Electronic Signatures - Part 2: Protection Profile for Software Signature Creation Devices	Waiting for publication (expected not before April 2004)	CWA 14172-6:2004	1) Will supersede CWA 14365:2003
CWA 14890-1:2004	Application Interface for smart cards used as Secure Signature Creation Devices - Part 1 - Basic requirements; version 1.09 rev2	Waiting for publication (expected not before April 2004)	CWA 14169:2004	1) CEN WS/E-Sign expressed the preference that this CWA will be maintained by CEN TC-224
CWA 14890-2:2004	Application Interface for smart cards used as Secure Signature Creation Devices - Part 2 - Additional services; version 1.03 rev1	Waiting for publication (expected not before April 2004)	CWA 14169:2004	1) CEN WS/E-Sign expressed the preference that this CWA will be maintained by CEN TC-224
CWA ?????:2004 (Area AB)	Evidential Value of Electronic Signatures	On going	CWA 14365-1:2004	

Autore: Daniela Rocca (SG&A)
Gianluca Ramunno (Politecnico di Torino)

The following schema explains the relationship between Cen/Isss and Etsi deliverables:



Symbols

CWA or TS — This deliverable is a technical specification (or it will be)

CWA or TR — This deliverable is a report or a guidance

CWA Area XX — This deliverable has not yet been approved (developed by the Project Team in Area XX)

Relationship of dependency

Relationship of mutual dependency

Relationship of weak dependency

Evaluated and certified PP

Not evaluated nor certified PP

R — Referenced in OJ

R — Will be referenced in OJ

Abbreviations

CWA	CEN Workshop Agreement (CEN deliverable)
OJ	Official Journal (of the European Union)
PP	Protection Profile (Common Criteria)
SR	Special Report (ETSI deliverable)
TS	Technical Specification (ETSI deliverable)
TR	Technical Report (ETSI deliverable)

Notes

The schema has been produced for the purpose of the future maintenance of the CWAs developed by CEN/ISSS E-Sign workshop within the EESSI frame. Therefore:

1. all deliverables developed (or being ...) by CEN/ISSS E-Sign workshop have been included;
2. not all deliverables developed by ETSI TC-ESI within the EESSI frame have been included in the schema: only the ones related to at least one CWA have been included;
3. the relationships among the ETSI deliverable included in the schema have not been represented;
4. CWA 14167, CWA 14172, CWA 14365 and CWA 14890 are multipart CWAs
5. the relationships among the parts of a same multipart CWA have not been represented;
6. relationship of dependency: CWA A ➔ CWA B means "*CWA A depends on CWA B*" (if the content of CWA B is modified, CWA B may need to be modified accordingly);
7. relationship of weak dependency (CWA A ➞ CWA B): the relationship between CWA A and B is not strong, because at the moment no maintenance is planned for CWA B;
8. CWA 14167-2 and CWA 14167-4 have a special relationship not represented: they are the same specification one with the key backup option and the other one without.
9. many deliverables refer to SR 002 176, therefore these relationships have not been represented

Gianluca Ramunno, Politecnico di Torino

Daniela Rocca, Studio Genghini & Associati