POLSKI KOMITET NORMALIZACYJNY

www.pkn.pl

eIDAS
standaryzacja usług zaufania

Andrzej Ruciński
Przewodniczący komitetu technicznego 172
ds. Identyfikacji Osób, Podpisu Elektronicznego,
Kart Elektronicznych oraz Powiązanych z nimi Systemów i Działań

CommonSign Warszawa 25-26 października 2017

Aktualny stan pracy Komitetu Technicznego nr 172

ds. Identyfikacji osób,
podpisu elektronicznego,
kart elektronicznych
oraz
powiązanych z nimi systemów i działań

Almanach **„Polskie Karty”** 2018

Tło „historyczne” - koordynacja prac standaryzacyjnych

EUROPEAN COMMISSION
ENTERPRISE AND INDUSTRY DIRECTORATE-GENERAL

Innovation policy
ICT for Competitiveness and Innovation

Brussels, 22nd December 2009
M/460 EN

STANDARDISATION MANDATE
TO THE EUROPEAN STANDARDISATION ORGANISATIONS CEN, CENELEC AND ETSI IN THE FIELD OF INFORMATION AND COMMUNICATION TECHNOLOGIES APPLIED TO ELECTRONIC SIGNATURES

EU eSignature Standardisation Work overview

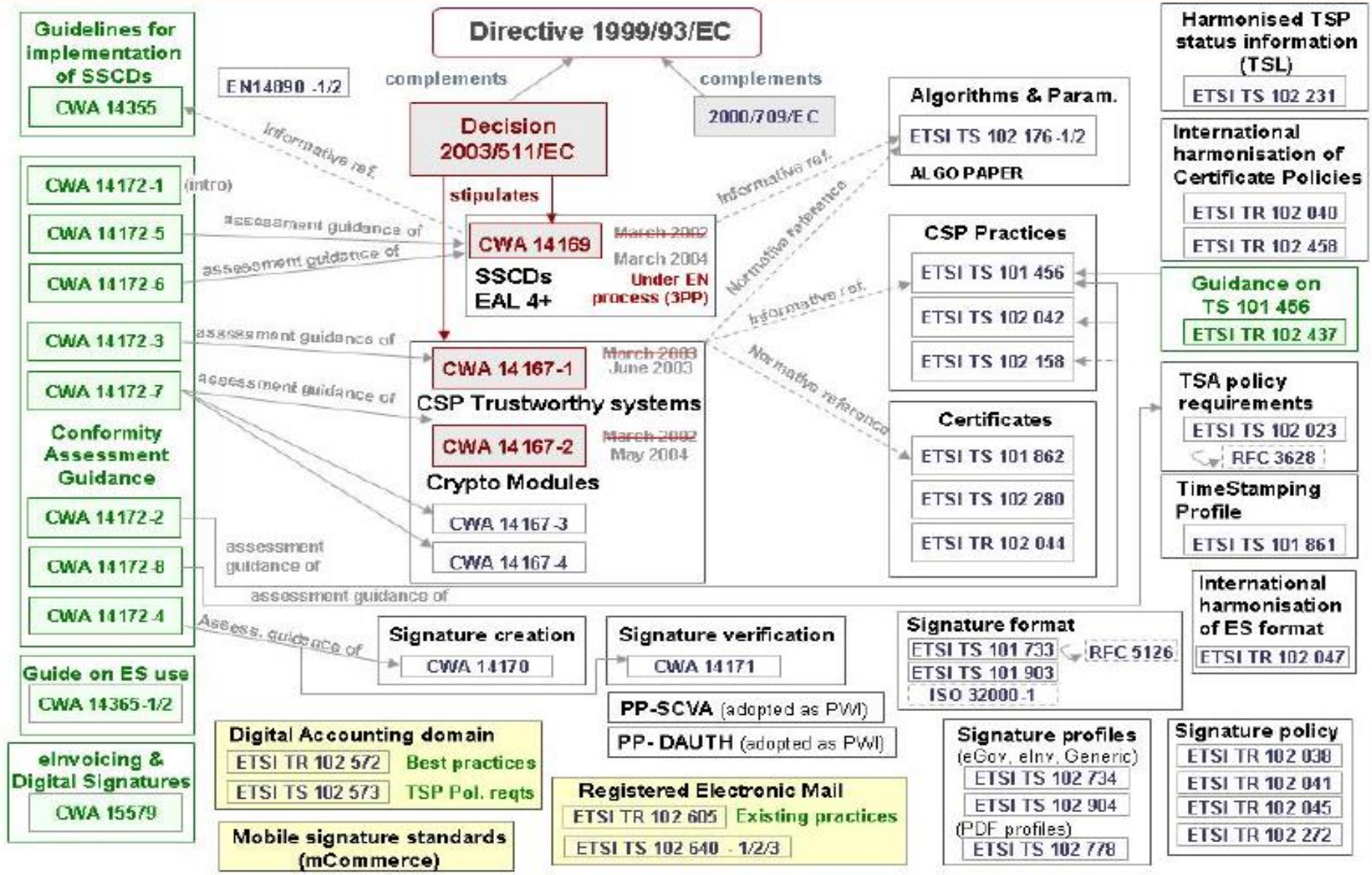

Figure 1 Current known status of the European eSignature standardisation deliverables

(source: Study on the standardisation aspects of e-signatures, SEALED, DLA Piper et al, 2007)

Jednolity rynek cyfrowy UE

KOMISJA
EUROPEJSKA

Bruksela, dnia 19.4.2016 r.
COM(2016) 176 final

KOMUNIKAT KOMISJI DO PARLAMENTU EUROPEJSKIEGO, RADY, EUROPEJSKIEGO KOMITETU EKONOMICZNO-SPOŁECZNEGO I KOMITETU REGIONÓW

Priorytety w normalizacji ICT na jednolitym rynku cyfrowym

eIDAS - usługi zaufania w systemie prawnym UE

28.8.2014 PL Dziennik Urzędowy Unii Europejskiej L 257/73

ROZPORZĄDZENIE PARLAMENTU EUROPEJSKIEGO I RADY (UE) NR 910/2014

z dnia 23 lipca 2014 r.

w sprawie identyfikacji elektronicznej i usług zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznym oraz uchylające dyrektywę 1999/93/WE

(2) Celem niniejszego rozporządzenia jest zwiększenie zaufania do transakcji elektronicznych na rynku wewnętrznym poprzez zapewnienie wspólnej podstawy bezpiecznej interakcji elektronicznej między obywatelami, przedsiębiorstwami i organami publicznymi, co pozwoli podnieść efektywność publicznych i prywatnych usług *online*, e-biznesu i e-handlu w Unii.

eIDAS – standaryzacja usług zaufania

(71) W celu zapewnienia jednolitych warunków wykonywania niniejszego rozporządzenia należy powierzyć Komisji uprawnienia wykonawcze, w szczególności w odniesieniu do określenia numerów referencyjnych norm, których stosowanie prowadzi do powstania domniemania spełnienia niektórych wymogów przewidzianych w niniejszym rozporządzeniu. Uprawnienia te powinny być wykonywane zgodnie z rozporządzeniem Parlamentu Europejskiego i Rady (UE) nr 182/2011 (1).

(72) Przy przyjmowaniu aktów delegowanych lub wykonawczych Komisja powinna w należyty sposób uwzględniać normy i specyfikacje techniczne opracowywane przez europejskie i międzynarodowe organizacje i organy normalizacyjne, w szczególności Europejski Komitet Normalizacyjny (CEN), Europejski Instytut Norm Telekomunikacyjnych (ETSI), Międzynarodową Organizację Normalizacyjną (ISO) lub Międzynarodowy Związek Telekomunikacyjny (ITU), tak aby zapewnić wysoki poziom bezpieczeństwa i interoperacyjności identyfikacji elektronicznej i usług zaufania.

Standaryzacja najważniejszych obszarów

- Ogólne ramy
- Status dostawców usług zaufania
- Kwalifikowane usługi zaufania
- Formaty podpisów
- Urządzenia do składania podpisu
- Funkcje kryptograficzne i generatory kluczy

Ogólne ramy

Grupa norm 119 0xx

- √ Zakres standaryzacji
- √ Wspólne definicje
- Wytyczne dla użytkowników

Status dostawców usług zaufania

Grupa norm 119 6xx

√ Listy kwalifikowanych dostawców usług zaufania i usługi nadzorowane przez państwa członkowskie

Usługi zaufania (1/2)

Grupa norm x19 4xx

- √ Wydawanie certyfikatów podpisu/pieczęci
- √ Znacznik czasu
- Usługa tworzenia podpisu/pieczęci
- Usługa walidacji

Usługi zaufania (2/2)

Grupa norm x19 5xx

- Usługa rejestrowanego doręczenia elektronicznego
- Długoterminowa konserwacja (podpisu/pieczęci/certyfikatów)

Formaty zaawansowanych podpisów elektronicznych

Grupa norm x19 1xx

- XAdES (XML)
- CAdES (CMS)
- PAdES (PDF)
- ASiC (containers)

Urządzenia do składania podpisu

Grupa norm 419 2xx

CC Protection Profiles:

√ **QSCD – karty elektroniczne**

HSM używane jako QSCD

HSM używane przez dostawcę usług

Zdalne (eemote) QSCD

Funkcje kryptograficzne i generatory kluczy

Grupa norm 119 3xx

√

Zestaw dla podpisu elektronicznego

- funkcja skrótu (hash)
- kryptografia asymetryczna (asymmetric cryptography)
- generowanie kluczy (key generation)
- okres stosowania (algorytmów, funkcji i kluczy - lifetime)

POLSKI KOMITET NORMALIZACYJNY

www.pkn.pl

DZIĘKUJĘ ZA UWAGĘ

andrzej.rucinski@assecods.pl