unizeto TECHNOLOGIES

Электронная подпись: от стандартов до интероперабельности

Andrzej Bendig-Wielowiejski
Ałła Stoliarowa-Myć

PKI -FORUM

St. Petersburg 18-20 сентября 2012

Содержание

1. Стандарты по электронной подписи в ЕС
2. Интероперабельность: декларации и реальность
3. Выводы

Юридические акты обязывающие в ЕС

касающиеся электронной подписи и связанных с ней услуг

- Регуляции на уровне ЕС
  - Директива 1999/93/WE о внутренних рамках по электронных подписях
- Регуляции внутригосударственные стран членов ЕС
  - Законы об электронных подписях
- Стандарты
  - De facto i de iure (не все и не всегда обязательны).

Виды электронной подписи в ЕС:

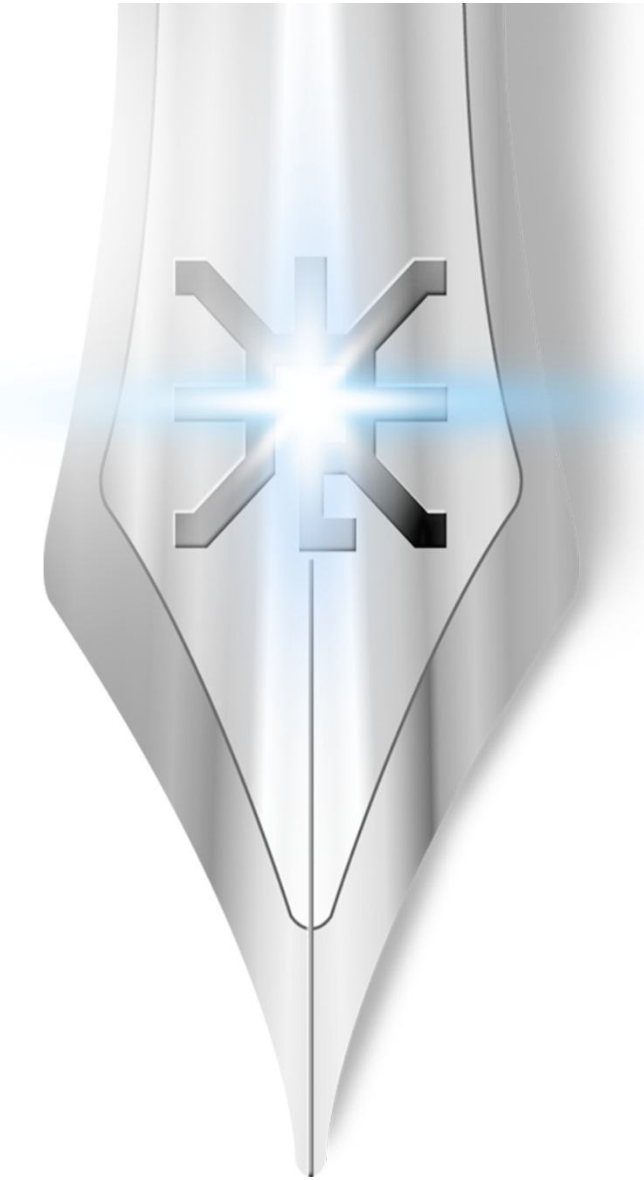
•Электронная подпись „простая ”

•Усиленная электронная подпись:
- Без SSCD
- с SSCD

•Квалифицированная электронная подпись
(без необходимости использования SSCD)

•Безопасная электронная подпись (PL)
= Квалифицированная электронная подпись с SSCD

где SSCD: Secure Signature Creation Device

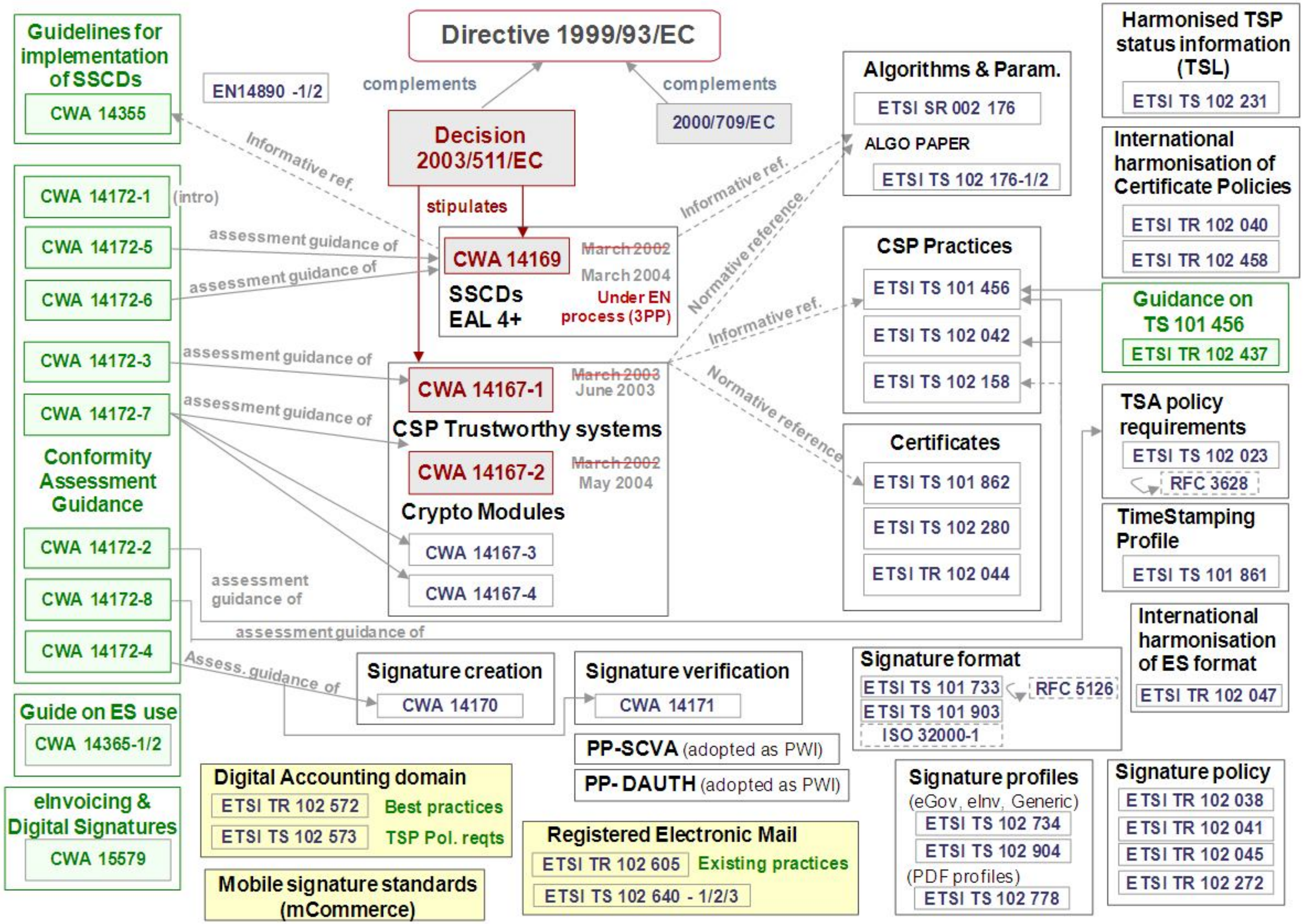


Форматы электронной подписи

Согласно стандартам :

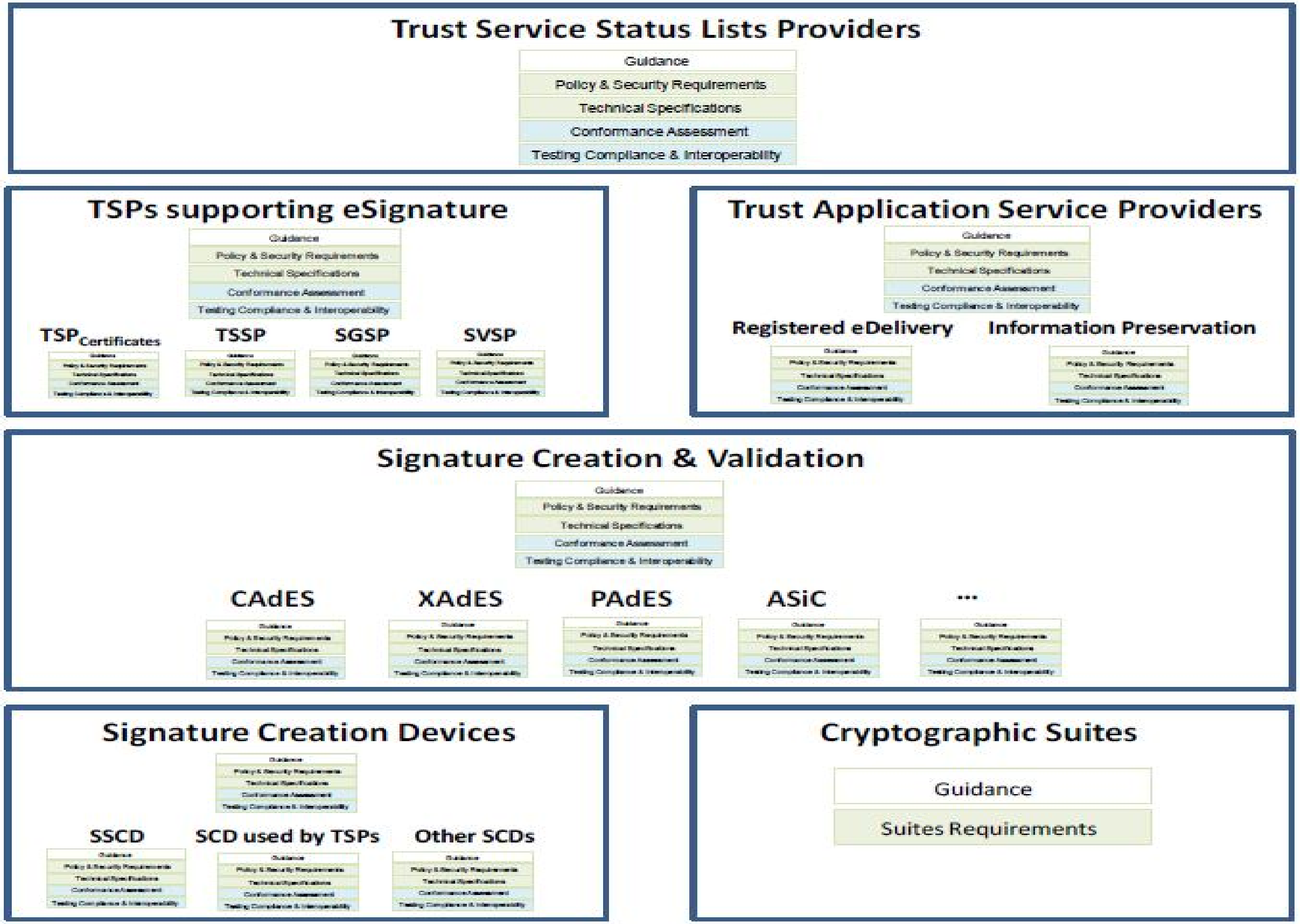
- *CAdES:*
  - *CAdES,*
  - *CAdES-T (timestamp),*
  - *CAdES-C (complete),*
  - *CAdES-X (extended),*
  - *CAdES-X-L (extended long-term),*
  - *CAdES-A (archival),*
- *XAdES:*
  - *XAdES*
  - *XAdES-T (timestamp)*
  - *XAdES-C (complete)*
  - *XAdES-X (extended)*
  - *XAdES-X-L (extended long-term)*
  - *XAdES-A (archival)*
- *PAdES:*
  - *PAdES Basic (ISO 32000-1)*
  - *PAdES Enhanced*
  - *PAdES-Long Term Validation*
  - *PAdES for XML Content*

Нормы и стандарты на сегодняшний день



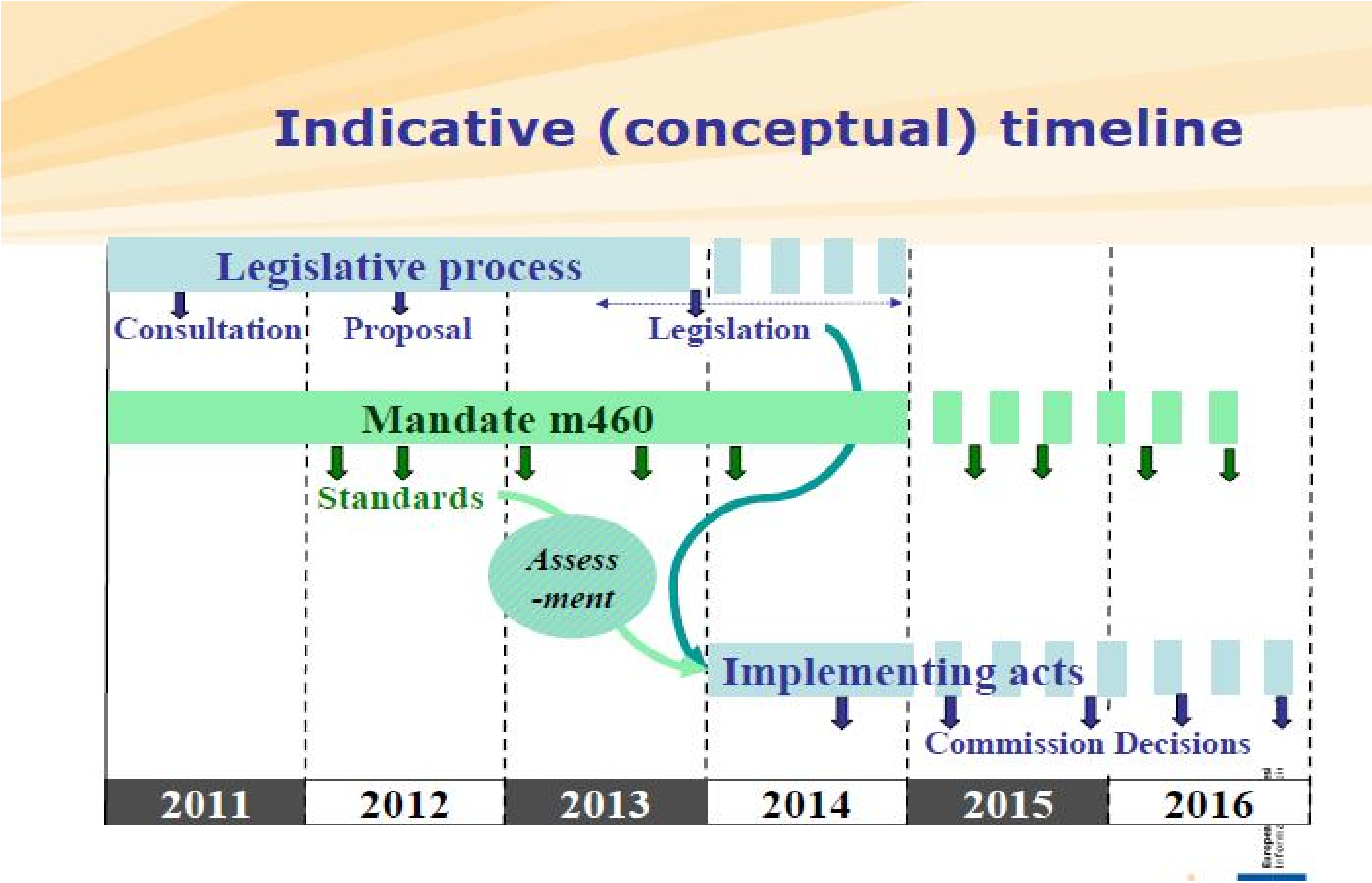
Olivier Delos - Standardisation mandate m460, Boosting trust in the digital single market: the role of e-signature

Нормы и стандарты - будущее



Olivier Delos - Standardisation mandate m460, Boosting trust in the digital single market: the role of e-signature

Развитие законодательства и стандартов – горизонт времени



Gérard Galler European Commission, DG Information Society & Media, Paris 21.11.2011, CEN-ETSI e-Signature workshop – mandate m460

Стандарты ЕС

Работы касающиеся электронной подписи и связанных с ней услуг:

European Commission Mandate 460 on Electronic Signatures Standardization

для **ETSI /CEN, где**

ETSI:European Telecommunications Standards Institute ,

CEN: European Committee for standardization

ETSI создало несколько проектов Specialist Task Forces projects (STF):

- **STF 425** Inventory of eSignature Standards (worldwide), Rationalised Framework Definition
- **STF 427** CSP Conformity Assessment, QC profile, Sig. Validation Procedures, Sig. algorithms maintenance
- **STF 426** X/C/PAdES & ASiC baseline profiles
- **STF 428** XAdES conformance testing, PAdES & ASiC interoperability tests

CEN Update CWA 14169 & CWA 14167 towards EN's

Стандарты ЕС

работы касающиеся электронной подписи и связанных с ней услуг

STF428 занимается деятельностью связанной с быстрым и простым введением функциональности существующих стандартов в области электронной подписи

STF428 разработал соответсвующие тестовые случаи и технические средства для организации и проведения тестов на соответствие форматам подписи

Стандарты ЕС –

тесты интероперабельности в 2011 и 2012 годах

- 2011 PAdES Remote Plugtests™ Event (Nov-Dec 2011) - 38 разных организаций
- 2012 XAdES Remote Plugtests™ Event (March-April 2012) - 27 разных организаций

финальные протоколы можно найти на сайте http://www.etsi.org

- Polish Interoperability Test for Electronic Signature Warsaw, 26-27 October 2011 – 10 программных продуктов (2 продукта касались только проверки подписи) - производители из Польши, Венгрии, Германии, Италии, Японии

Замечание:

- заинтересование тестированием поставщиков ПО для электронной подписи не большое (при около 100 квалифицированных доверенных поставщиков сертификационных услуг в ЕС, декларативном использовании в многих прикладных системах госадминистации стран членов ЕС и Бизнес-системах)

- количество участников является достаточным чтобы сделать обобщенные выводы

Стандарты ЕС –

тесты интероперабельности в 2011 и 2012 годах

- Создание подписей - около 70 первичных тестов при XAdES Remote Plugtests™
- Проверка подписей – каждый участник проверяет подписи созданные ПО всех остальных участников
- Проверка случаев с отрицательным эффектом – подготовленных организаторами
- Тесты „Upgrade and arbitration”

Примеры тестовых случаев:

X-BES-5.xml содержит следующие элементы:

SigningCertificate
SigningTime
SignatureProductionPlace
SignerRole

This test case tests an external SigningCertificate and has the SigningTime and SignatureProductionPlace property.Now also the SignerRole with a CertifiedRole is added.

X-BES-11.xml содержит следующие элементы:

SigningCertificate
SigningTime
SignatureProductionPlace
CounterSignature

This is to test the CounterSignature, for simplicity it is signed by the same party.

Из документа External Report of the 2012 XAdES Remote Plugtests™ Event
(March-April 2012) © European Telecommunications Standards Institute

Стандарты ЕС – тесты интероперабельности в 2011 и 2012 годах

6.1 Summaries for Positive Test Cases

XAdES-BES

Signature	Generated Signatures	Number of Verifiers	Total Verifications	Success		Failure		Not Applicable		Incomplete		Non Conformant	
					%		%		%		%		%
X-BES-1	21	23	399	347	86,97	48	12,03	0	0,00	4	1,00	0	0,00
X-BES-2	22	23	351	323	92,02	24	6,84	0	0,00	4	1,14	0	0,00
X-BES-3	20	22	363	332	91,46	28	7,71	0	0,00	3	0,83	1	1,09
X-BES-4	15	18	198	181	91,41	13	6,57	0	0,00	4	2,02	0	0,00
X-BES-5	10	18	116	106	91,38	7	6,03	1	0,86	2	1,72	0	0,00
X-BES-6	16	20	251	236	94,02	13	5,18	0	0,00	2	0,80	0	0,00
X-BES-7	14	19	191	181	94,76	8	4,19	0	0,00	2	1,05	0	0,00
X-BES-8	12	18	184	177	96,20	6	3,26	0	0,00	1	0,54	0	0,00
X-BES-9	10	14	119	119	100,00	0	0,00	0	0,00	0	0,00	0	0,00
X-BES-10	9	13	114	114	100,00	0	0,00	0	0,00	0	0,00	0	0,00
X-BES-11	11	15	135	109	80,74	16	11,85	0	0,00	10	7,41	0	0,00
X-BES-15	7	12	66	55	83,33	10	15,15	0	0,00	1	1,52	0	0,00
Total /Average	167	215	2487	2280	91,86	173	6,57	1	0,07	33	1,50	1	0,09

Из документа External Report of the 2012 XAdES Remote Plugtests™ Event (March-April 2012) © European Telecommunications Standards Institute

Выводы

Програмное обеспечение связанное с созданием и проверкой электронной подписи часто реализует конкретную ограниченную часть стандарта, необходимую в данном юридическом и бизнес оточении на данный момент времени:

Это вызвано, например:

•Ограничением издержек на разработку, тестирование и сопровождение ПО

•Отсутствием соответствующих специалистов при разработке ПО в данной организации

•Отсутствием определения базовых профилей форматов подписи на основании соотв. стандартов –для конктретных систем

•... ?

Хорошие практики:

Решение Еврокомиссии от 25-02-2011 года об определении минимальных требований при трансграничной обработке документов подписанных в электронном виде соответствующими органами согласно директиве 2006/123/WE Европарламента и Совета касающейся услуг на внутреннем рынке (2011/130/UE), как приложение указан документ:

Спецификация усиленной электронной подписи для документов в виде XML, CMS и PDF, которые должны технически обслуживаться страной членом ЕС получающей документ.

26.2.2011 PL Dziennik Urzędowy Unii Europejskiej L 53/6

Tabela 1

XAdES–BES (EPES)		Wspólne minimalne wymagania
(Zastosowanie ma specyfikacja ETSI TS 103 903 z następującymi, profilowanymi elementami)		
O = obowiązkowy; F = fakultatywny; Z = zalecany; N = niewykorzystany		
ds: Signature ID	O	
ds: SignedInfo	O	
ds: CanonicalizationMethod	O	*Na potrzeby weryfikacji podpisu MUSZĄ być obsługiwane wszystkie wymienione poniżej algorytmy, natomiast tworzenie podpisu POWINNO BYĆ ograniczone do jednego z nich:*

Спасибо за внимание!

Digitally signed by Ałła Stoliarowa-Myć; Unizeto Technologies S.A.
Date: 2012.10.03 12:05:53 CEST
Reason: The final version

astoliarowa@unizeto.pl

www.unizeto.pl
www.certum.pl
www.webnotarius.pl
www.efpe.pl