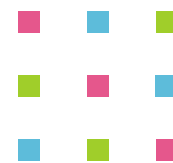
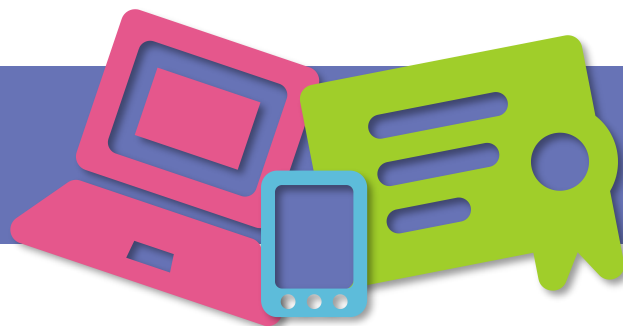


SECURITY 2015



23. ročník konference o bezpečnosti v ICT



Archivace elektronických dokumentů po eIDAS

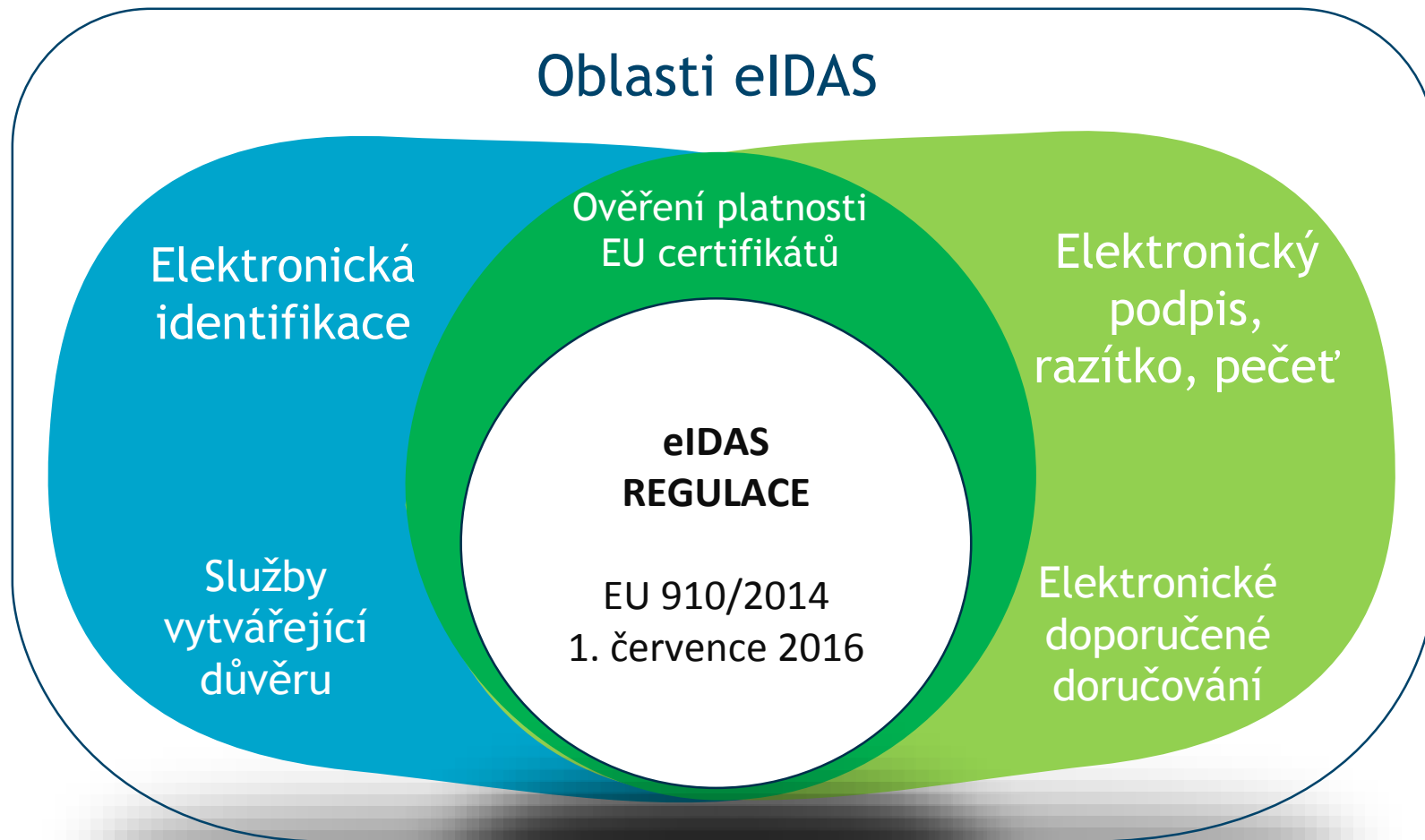
Martin Vondrouš

Software602 a.s.



Co je to eIDAS?

**NAŘÍZENÍ EVROPSKÉHO PARLAMENTU A RADY
(EU) č. 910/2014
ze dne 23. července 2014
o elektronické identifikaci a službách
vytvářejících důvěru pro elektronické transakce
na vnitřním trhu a o zrušení směrnice
1999/93/ES**





Historicky

- Služby vytvářející důvěru na úrovni EU?
 - Směrnice o el. podpisu 1999/93/EC
 - Směrnice o službách 2006/123/EC
 - Formáty podpisů – Rozhodnutí komise 2011/130EU a 2014/148/EU
 - Trust List – Rozhodnutí komise 2009/767/EC a 2013/662/EU
- Elektronická identifikace?
 - Technické projekty, např. STORK
 - Ale bez právního rámce



Všimněte si!

■ Trust services

- Služby vytvářející důvěru
- Poskytovatel služby vytvářející důvěru
- Kvalifikovaný poskytovatel služby poskytující důvěru
- *Trusted document – důvěryhodný dokument*



Co to implikuje a co existuje?

- Základní koncepty e-podpisu, kvalifikovaného podpisu, autorit
- Volný trh, akreditace
- Částečně ekvivalence právní hodnoty elektronického a papírového dokumentu
- Technické a kvalitativní požadavky
- To vše je roztržštěně implementováno lokálně v rámci legislativ členských států



Co chybí?

- Elektronické podpisy – ok
 - Jaký je správný formát, kdy je validní?
- Razítka? Archivace? Elektronické doručování? eID?
- Ověřování

- Technologie se vyvíjí
 - Překonané, nekompletní standardy
 - Mobilní technologie
 - Serverové podepisování



Jak z toho ven?

■ EU nařízení eIDAS

Nařízení Evropského parlamentu a Rady (EU) č. 910/2014 ze dne 23. července 2014 o elektronické identifikaci a službách vytvářejících důvěru pro elektronické transakce na vnitřním trhu a o zrušení směrnice 1999/93/ES

- Platí přímo, netransponuje se do národních legislativ

■ eIDAS má dvě hlavní oblasti

- eID
- Služby vytvářející důvěru



eIDAS Regulation

eID

Trust services

Mutual
recognition

eSignatures

eSeals

Time stamp

Electronic
delivery

Website
authen-
tication

For the
public
sector only

Hand
written
only!

Legal
persons –
origin and
integrity

Evidence of
existence

Sender,
recipient,
time of
receipt

Website
control



Trust Services

- Služby vytvářející důvěru (budoucí řada EN 319 4xx)
 - Elektronický podpis – FO, ekvivalent ručního podpisu
 - Elektronická značka (Seal) – PO, původnost a integrita
 - Časové razítko – evidence času a existence
 - Kvalifikované ověřování
 - Elektronické doručení – evidence odesílatele, příjemce a času (isds)
 - Autentizace webových stránek – původnost webových stránek, https



Dopad na e-dokumenty

■ Podpis

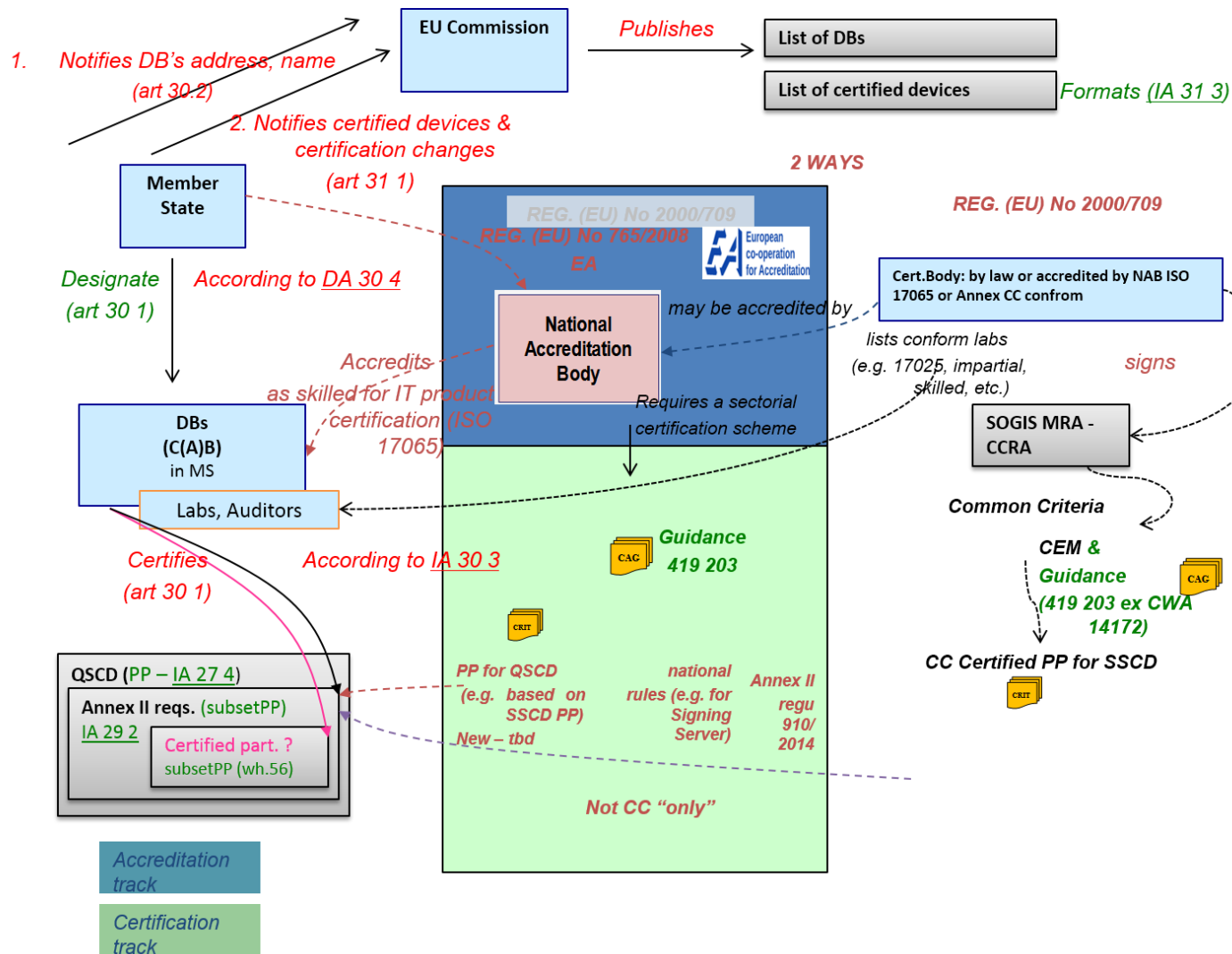
- ETSI specifikace – PAdES, XAdES, CAdES
- Kvalifikované časové razítko
- Prostředky na ověření
- eIDAS definuje
 - Electronic Signature
 - Advanced Electronic Signature
 - Qualified Electronic Signature



SCDev – Signature Creating Device

- Prostředek pro vytváření podpisu
 - Serverový
 - HSM
 - Běžné úložiště
- Kvalifikovaný prostředek
 - SSCDev – může být jak hardware, tak software, musí splňovat předpoklad pro výlučnou kontrolu
 - Kvalifikovaný token, aplikace

Kvalifikované prostředky





Archivace dokumentů, dat

- V každém případě vznikne elektronicky podepsaný dokument, jehož pravost a autenticitu je možné ověřit díky atributům
 - Podpis
 - Razítko
 - Kvalifikovanost prostředku
 - Dle ETSI
- Tyto atributy je třeba udržovat ověřitelné v čase, v souladu s definicí ETSI – pravidelným připojováním časových razítek a ověřovacích metadat – Archivní časové razítko



Ověřitelnost

- Může být jednou ze služeb kvalifikovaného poskytovatele služeb vytvářejících důvěru
- Jistota, že elektronické podpisy na dokumentu (resp. certifikáty, na základě kterých vznikl podpis) budou ověřeny vždy dle aktuálních informací a stejných metodik. Na libovolném zařízení.
 - V ČR CzechPoint, řešení Software602



Archivace teď a potom ...

Pořád stejná

ALE

- Už teď se vyplatí vytvářet dokumenty tak, aby bylo možné je zařadit k archivaci, až se bude blížit vypršení jejich ověřitelnosti.



Archivace teď a potom ...

Jak?

- vytvářet dokumenty tak, aby bylo možné je zařadit k archivaci, až se bude blížit vypršení jejich ověřitelnosti.
 - Kvalifikovaný certifikát a správně podepsaný dokument dle AdES s časovým razítkem
 - Aplikace, služba



Archivace teď a potom ...

Pořád stejná

ALE

- Elektronické dokumenty, kterým vyprší jejich ověřitelnost, již nyní ošetřit v souladu aktuální specifikací.



Archivace teď a potom ...

Jak?

- Ošetřit dokumenty v souladu aktuální specifikací
 - Ověřit platnost podpisů
 - Připojit ověřovací metadata a kvalifikované časové razítko
 - Zajistit jejich následnou archivaci



Archivace teď a potom ...

Pořád stejná

ALE

- Je třeba sledovat nárůst kvality a bezpečnosti poskytovatelů cloudových úložišť a sledovat tento trend.



Dělejte co nemusíte

- Nečekejte na legislativu, až Vám něco přikáže
 - Ověřitelnost dokumentů, dat a podpisů vyžaduje péči.

- Autorizace a uchování dokumentů dle aktuální legislativy
 - 499/2004 Sb. – Archivnictví a spisová služba
 - 300/2008 Sb. – Datové schránky a autorizovaná konverze
 - 227/2000 Sb. – O elektronickém podpisu
 - 235/2004 Sb. – O dani z přidané hodnoty
 - 365/2000 Sb. – O IS veřejné správy
 - 2014/148/EU – přeshraniční zpracování dokumentů (původní 2011/130/EU)
 - 1999/93/ES – Zásady společenství pro elektronické podpisy
 - 910/2014 – O elektronické identifikaci a službách vytvářejících důvěru

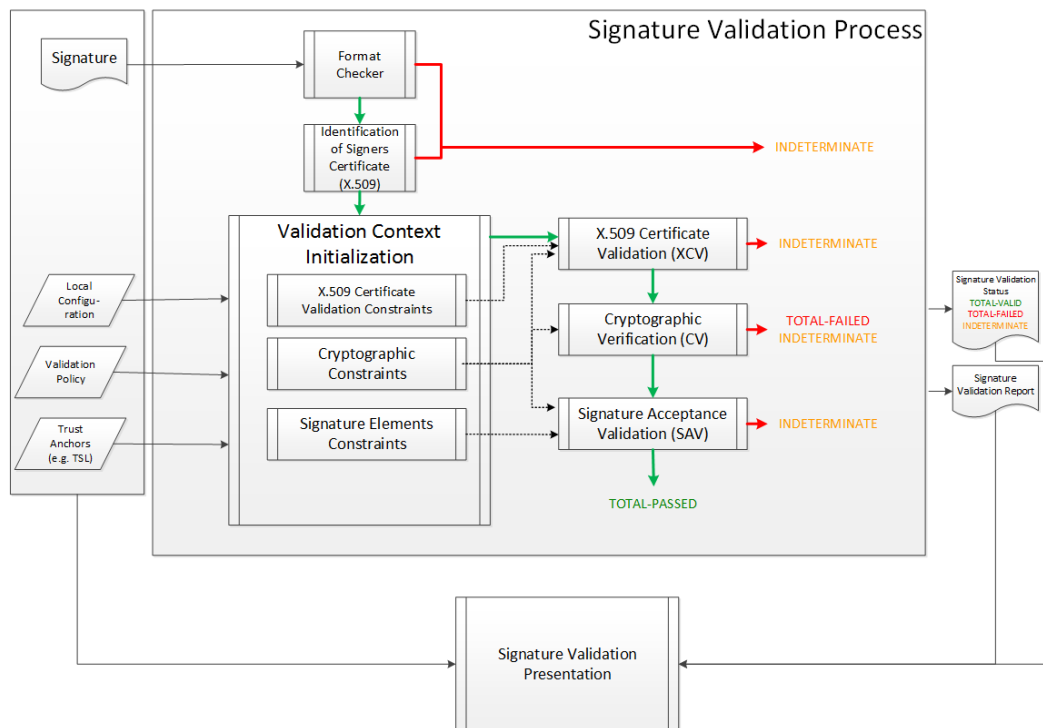


Dělejte co nemusíte

- Vytvářejte elektronické dokumenty jednoduše a správně
 - PDF/A jen pro dlouhodobé dokumenty. Word dokument s platností na 5-6 let podepište tak, jak je – ale správně a s razítkem
 - Ověřujte elektronické dokumenty na jejichž základě konáte

Dělejte co nemusíte

- Archivujte, starejte se o platnosti vašich dokumentů a dat
 - Zpětně se to opravdu udělat nedá





Nebojte se zeptat



SECURITY 2015



23. ročník konference o bezpečnosti v ICT

Děkuji za pozornost.

Martin Vondrouš
Software602 a.s.
vondrous@602.cz



SECURITY 2015



23. ročník konference o bezpečnosti v ICT

Panelová diskuse

Dokumentace, digitalizace a bezpečnost

