



Realizace eIDAS u poskytovatele důvěryhodných služeb

ICTU Workshop -
Správa a ukládání důvěryhodných dokumentů

Dagmar Bosáková

16. 2. 2016



Evropská směrnice a český zákon



Dosud do 30. 6. 2016:

Směrnice Evropského parlamentu a Rady **1999/93/ES ze dne 13. prosince 1999 o zásadách Společenství pro elektronické podpisy.**

Implementace: zákon č. 227/2000 Sb., o elektronickém podpisu

Obecně evropská **směrnice** (directive) - povinnost transpozice, tj. promítnutí do vnitrostátního právního předpisu.

Obecně evropské **nařízení** (regulation) platí v každém členském státu přímo, bez prováděcího vnitrostátního aktu.

Evropské nařízení a český zákon



Nově od 1. 7. 2016:

Nařízení Evropského parlamentu a Rady 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 (zkráceně: eIDAS)

Doplní český adaptační zákon: **zákon o službách vytvářejících důvěru pro elektronické transakce** (návrh – před vládou), zruší zákon o elektronickém podpisu. Novely dalších zákonů, ve kterých se stanoví možnost/povinnost e-podpisu, e-značky.

Poznámka: Je-li v prezentaci barva písma červená, jedná se o **návrh zákona.**

Prováděcí rozhodnutí a nařízení EU



1. procesní opatření pro spolupráci mezi členskými státy v oblasti elektronické identifikace
2. **podoba značky důvěry EU pro QSVD**
3. interoperabilita systémů elektronické identifikace
4. úrovně záruky prostředků pro elektronickou identifikaci
5. důvěryhodné seznamy QPSVD a QSVD
6. **formáty zaručených elektronických podpisů a zaručených pečetí uznávaných subjekty veřejného sektoru**
7. oznamování systémů elektronické identifikace

Dosud nejsou vydány všechny technické normy.

eIDAS – tři oblasti úpravy



1. Elektronická identifikace
2. Služby vytvářející důvěru/kvalifikované služby vytvářející důvěru
3. Elektronický dokument

Služby vytvářející důvěru - oblasti



- **Elektronický podpis**
- **Elektronická pečeť**
- **Elektronické časové razítko**
- **Služba elektronického doporučeného doručování**
- **Kvalifikované certifikáty pro autentizaci internetových stránek (de facto SSL certifikáty)**

Elektronický podpis



- Zaručený elektronický podpis
- Zaručený elektronický podpis založený na QC
- **Pouze „kvalifikovaný elektronický podpis“ má právní účinek rovnocenný vlastnoručnímu podpisu, tj.**
 - ZEP,
 - kvalifikovaný certifikát pro elektronické popisy,
 - kvalifikovaný prostředek pro vytváření elektronických podpisů (Starcos)
- Qualified Electronic Signature Creation Device (QESCD nahradí dnešní SSCD – Secure Signature Creation Device)

QEP v rámci EU



- SSCD (Secure Signature Creation Device) se stanou automaticky kvalifikovanými prostředky pro vytváření podpisů podle eIDAS. **V ČR pouze I.CA pro Starcos 3.0 a 3.2.**
- Komise povede bude zveřejňovat **seznam certifikovaných kvalifikovaných prostředků pro vytváření elektronických podpisů**, a to na základě hlášení členských států.
- **Kvalifikovaný elektronický podpis** založený na kvalifikovaném certifikátu vydaném v jednom členském státě **se uznává jako kvalifikovaný elektronický podpis ve všech ostatních členských státech.**

QC kolem 1. 7. 2016



Kvalifikované certifikáty vydané fyzickým osobám podle směrnice 1999/93/ES se považují za kvalifikované certifikáty pro elektronické podpisy podle eIDAS až do doby skončení jejich platnosti.

Tj. QC vydané do 30. 6. 2016. Nehrozí zneplatňování.

Od 1. 7. 2016 bude I.CA vydávat **kvalifikované certifikáty pro elektronické podpisy** v roli QPSVD. Následně povinnost projít auditem provedeným k tomu určeným subjektem a předložit do 1. 7. 2017 MV zprávu o posouzení shody. MV má nejméně 3 měsíce na posouzení a zařazení do jím vedeného seznamu.

Ostatní služby po 1. 7. 2016



- Poskytování ostatních kvalifikovaných služeb - podmínkou je **provedení auditu podle eIDAS**, který logicky může být proveden až eIDAS nabude účinnosti a budou k tomu vytvořeny příslušné nástroje (například určení subjektů, které budou audit provádět).
- **Přechod od režimu zákona o elektronickém podpisu k režimu eIDAS**, a to zejména u elektronických značek a časových razítek, stanoví připravovaný adaptační zákon o službách vytvářejících důvěru pro elektronické transakce, v gesci Ministerstva vnitra.

Příklad



- I.CA vydává do 30. 6. 2016 **kvalifikovaná časová razítka.**
- Od 1. 7. 2016 může I.CA vydávat **elektronická časová razítka vydaná kvalifikovaným poskytovatelem důvěryhodných služeb** (protože vydává kvalifikované certifikáty, automaticky přechází do režimu eIDAS)
- Po provedení auditu a posouzení Ministerstvem vnitra – bude vydávat **kvalifikovaná elektronická časová razítka.**

Český zákon a typy podpisů - návrh



- Dokument, kterým se činí **úkon vůči orgánu veřejné správy/moci** – uznávaný elektronický podpis
(nejméně ZEP + QC).
- Dokument, kterým činí **úkon orgán veřejné moci** – kvalifikovaný elektronický podpis.
(ZEP + QC + QESCD) – 2 roky odklad, stačí ZEP+QC
- **Povinnost OVS opatřit dokument kvalifikovaným elektronickým časovým razítkem, resp. e-časové razítko vydané QPSVD.**

Nové služby, které vyžadují provedení auditu



- Kvalifikovaná služba **ověřování platnosti kvalifikovaných elektronických podpisů / uchování**
- Vydávání **kvalifikovaných certifikátů pro elektronické pečete**
- Kvalifikovaná služba **ověřování platnosti kvalifikovaných elektronických pečetí / uchování**
- Kvalifikovaná služba **vydávání kvalifikovaných elektronických časových razítek**
- Kvalifikovaná služba **vydávání kvalifikovaných certifikátů pro autentizaci internetových stránek**

Další nové služby



eIDAS je ve vlastním textu výslovně neupravuje, ale v preambuli je uvádí jako perspektivní a ekonomicky výhodné:

- **podepisování prostřednictvím mobilního telefonu a podepisování v cloudech, nutnost kvalifikovaných prostředků pro vytváření elektronických podpisů**
- **vytváření elektronického podpisu na dálku.**

eIDAS vytváří právní prostředí pro tyto služby.

Elektronické pečetě - charakteristika



- Podobnost s uznávanou e-značkou (pouze v ČR)
- Zaručené elektronické pečetě
- Zaručené elektronické pečetě + QC pro e-pečetě
- **Kvalifikované elektronické pečetě:**
 - jsou zásadně **spojeny s původcem dat**
 - jsou založeny na **kvalifikovaných certifikátech pro elektronické pečetě** (obdoba kvalifikovaných systémových certifikátů)
 - musí být vytvořeny pomocí **kvalifikovaných prostředků pro vytváření elektronických pečetí** (qualified electronic seal creation device - QESCD)

Co bude s uznávanými e-značkami



- Český adaptační zákon umožní, aby byly používány ještě dva roky po 1. 7. 2016, resp. 2 roky od nabytí účinnosti českého adaptačního zákona. Po příslušnou dobu budou vydávány i QSC.
- Neplatí pro komunikaci v rámci EU, resp. žádná česká výjimka není použitelná v EU.

Elektronická časová razítka



- Elektronická časová razítka
- **Kvalifikovaná elektronická časová razítka**
- **Beze změny oproti současnému stavu.**

Český adaptační zákon:

Po dobu 2 let od nabytí účinnosti tohoto zákona lze namísto kvalifikovaného elektronického časového razítka použít **elektronické časové razítko vydané kvalifikovaným poskytovatelem služeb vytvářejících důvěru.**

Kvalifikovaný poskytovatel, kvalifikovaná služba



Pokud služby vytvářející důvěru mají označení **kvalifikované**, mohou je poskytovat pouze kvalifikovaní poskytovatelé služeb vytvářejících důvěru.

Pokud poskytovatel, služba nebo produkt má označení **kvalifikovaný**, má klient záruku, že poskytovatel/ služba/produkt splňuje povinné požadavky Nařízení a je zárukou nejvyšší úrovně kvality a bezpečnosti.

Kvalifikovaný poskytovatel služeb vytvářejících důvěru – alespoň jednu kvalifikovanou službu a event. další nekvalifikované služby.

Odpovědnost za škodu



Poskytovatelé služeb vytvářejících důvěru odpovídají za úmyslně nebo z nedbalosti způsobenou škodu nesplněním Nařízení, přičemž:

- „nekvalifikovaný“ poskytovatel - důkazní břemeno je na osobě uplatňující nárok na náhradu,
- kvalifikovaný poskytovatel – důkazní břemeno je na něm, tj. musí prokázat, že škoda nastala bez jeho úmyslu nebo nedbalosti.

Výhodné pro klienty!

„Nekvalifikovaný“ poskytovatel



Nekvalifikovaný poskytovatel

- poskytuje nejméně jednu službu vytvářející důvěru která je poskytována veřejnosti a která má vliv na třetí osoby
- musí splňovat především bezpečnostní požadavky uvedené v Nařízení.

Povinnost hlásit incidenty s významným dopadem do 24 hodin příslušnému orgánu (MV, NBÚ, ÚOOÚ), povinnost informovat dotčené právnické a fyzické osoby.

Povinnost orgánu dohledu - zasáhnout v případě oznámení (kohokoliv), že „nekvalifikovaný“ poskytovatel nesplňuje požadavky Nařízení. Orgán dohledu má právo požadovat nápravu.

Závěr



Děkuji za pozornost.

<http://www.ica.cz>