



DITEC je vedúcim integrátorom informačných technológií. Svojim zákazníkom poskytujeme komplexné služby v oblasti nasadzovania a prevádzky informačných systémov.



DITEC je firma s tradíciou. Počas svojej existencie sme sa vypracovali na stabilný subjekt, ktorý je dôveryhodným a dlhodobým partnerom významných organizácií.

Platí eIDAS – a čo teraz ?

zamyslenie sa dopadmi pre eGovernment

Pavol Frič

Obsah

- O čom je eIDAS
- eIDAS a eGovernment v SR
- Otvorené otázky

1. O čom je eIDAS

■ Celý názov

- Nariadenie Európskeho parlamentu a Rady (EÚ) č. 910/2014 o elektronickej identifikácii a dôveryhodných službách pre elektronické transakcie na vnútornom trhu

■ Základný cieľ

- jednotný digitálny trh EÚ - bezpečná elektronická interakciu subjektov na vnútornom trhu:
 - » elektronická identifikácia
 - » poskytovanie a využívanie dôveryhodných služieb
- dopady nielen pre procesy eGovernmentu, ale taktiež pre komerčnú sféru

■ Stav

- **nariadenie účinné od 1.7.2016**
- **vydané Vykonávacie rozhodnutia pre vybrané oblasti**
 - » **presnejšie určenie spôsobu riešenia vybraných aspektov**
 - » **referencia na štandardy**
- **stále však mnohé praktické problémy neriešené**
 - » **zatiaľ neexistujú štandardy (napr. pre službu overovania podpisov, „vzdialeného vytvárania podpisov“ ...**
 - » **skôr orientácia na „formálnu“ stránku služieb, mnohé praktické problémy neriešené**

2. eIDAS a eGovernment v SR

- **eIDAS má dopad na legislatívny systém v SR**
 - **zrušenie Zákona č. 215/2012 o elektronickom podpise, nahradenie Zákonom o dôveryhodných službách**
 - **určuje viaceré procesy, ktoré podrobnejšie rieši aj Zákon č. 305/2013 o eGovernmente**
- **nakoľko je eIDAS účinný, je potrebné určiť dopad na existujúce eGov procesy**

■ Základné súčasti eIDAS

- elektronická identita
- elektronický podpis/elektronická pečať
- dôveryhodné služby



■ Elektronická identita

- pravidlá pre rozpoznanie a akceptovanie elektronických identifikačných prostriedkov pre fyzické a právnické osoby
 - » dobrovoľná notifikácia identifikačných schém
 - » povinná akceptácia identifikačných prostriedkov v rámci notifikovaných identifikačných schém
- stav v SR
 - » identifikátor pre PO a FO definovaný v Zákone o eGovernmente
 - je možné predpokladať náhradu existujúceho identifikátora FO (pravdepodobne BIFO)

» **autentifikácia – autentifikátor**

- pre autentifikáciu používané eID
- zatiaľ neexistuje alternatívny autentifikátor
- je však možné používať autentifikačný certifikát (podrobnosti vydá MV SR vo vyhláške)

» **SR a eIDAS**

- pravdepodobne bude notifikované eID ako prostriedok pre preukazovanie identity
- bude potrebné riešiť akceptáciu iných identifikačných prostriedkov (pravdepodobne centralizované riešenie)
- služby pre elektronickú identifikáciu budú musieť byť dostupné nielen pre eGovernment, ale aj pre komerčné subjekty (aj pre budovanie komerčných služieb) !!

■ Elektronický podpis/pečať

– zabezpečenie skutočnej interoperability

» definovanie štandardov a záväzných profilov

- možnosť používania iných štandardov a profilov IBA ak existuje voľne dostupná služba pre overenie platnosti

» povinnosť uznávania podpisov/pečatí a certifikátov v rámci všetkých členských štátov

» prechodné obdobie pre SSCD = QSCD

– legislatívne ukotvenie

» národná legislatíva môže rozšíriť právnu použiteľnosť mimo preukázania pôvodu a integrity (napr. autorizácia úkonu)

» ak sa vyžaduje použitie kvalifikovanej elektronickej pečate PO, kvalifikovaný elektronický podpis FO oprávnenej konať za danú PO má rovnakú právnu váhu

■ Elektronický podpis/pečať

– stav v SR

» legislatívne „rozšírenia“

- elektronická pečať ako prostriedok autorizácie úkonu (Zákon o eGovernmente)
- možnosť zadefinovania oprávnenia/postavenia držiteľa certifikátu – mandátny certifikát (Zákon o dôveryhodných službách)
- možnosť on-line overovania platnosti elektronického podpisu/pečate pri vzájomnej komunikácii OVM – zoznam platných certifikátov pre elektronickú pečať (Zákon o eGovernmente)

■ Elektronický podpis/pečať

- » technická pripravenosť na eIDAS
- » na technickej úrovni všetko pripravené (certifikované prostriedky, podateľňa UPVS)
 - certifikované prostriedky pre vytváranie a overovanie elektronického podpisu a elektronickej pečate, posúdenie zhody systému elektronickej podateľne
 - súlad s požiadavkami eIDAS a Výnosu o štandardoch
 - požiadavka používať certifikované prostriedky pre OVM (Výnos o štandardoch ISVS)
 - riešenia nenasadzované v plnom rozsahu vzhľadom na potrebu zabezpečenia interoperability s ostatnými systémami (napr. používanie ASiC)

■ Dôveryhodné služby

- **povinnosti uznávať dôveryhodnú službu**
 - » **nezakladá povinnosť orgánu verejnej moci získať technické prostriedky pre zabezpečenie možnosti využitia všetkých dôveryhodných služieb**
- **nie je ustanovená povinnosť používať dôveryhodné služby**
- **možnosť využitia dôveryhodných služieb ako dôkazu v prípade sporov**
- **členské štáty môžu definovať aj ďalšie dôveryhodné služby nad rámec Nariadenia pre využitie na národnej úrovni**
 - » **možnosť pre komerčné subjekty poskytovať služby s pridanou hodnotou**

■ Kvalifikované dôveryhodné služby

– definovanie spôsobu získania štatútu kvalifikovanej služby

- » orgán dohľadu NBÚ

- » EU má publikovať pravidlá, na základe ktorých sa posudzovanie zhody bude vykonávať

- otázka, akým spôsobom je možné TERAZ získať štatút kvalifikovaného poskytovateľa dôveryhodnej služby

- » posudzovanie zhody - vzhľadom k štandardom

- pre mnohé zatiaľ neexistujú – napr. služba overovania podpisu, služba vzdialeného vytvárania podpisu/pečate

– definovanie spôsobu zverejňovania poskytovateľov

- » „trusted list“ – na úrovni EU aj členských štátov

- » značka dôvery

■ Kvalifikované dôveryhodné služby

- služba vydávania a správy certifikátov
 - » prechodné obdobie pre súčasné ACA – 1 rok
 - » povinnosť poskytovať OCSP
- služba vydávania časovej pečiatky
 - » prechodné obdobie pre súčasné ACA – 1 rok
- služba vytvárania podpisu/pečate
 - » mobile signing, cloud signing
 - » použitie QSCD pre správu kľúčov a vytváranie podpisov, vytváranie QES a QESe
 - » pripravujú sa štandardy

■ Kvalifikované dôveryhodné služby

– služba overovania podpisov/pečatí

- » zatiaľ nie sú štandardy, výstup má byť autorizovaný AdES
- » využiteľná pre mnohé procesy (napr. zaručená konverzia, resp. spracovanie správ v elektronickej schránke)

– služba uchovávaní podpisov/pečatí

- » aj existujúca legislatíva SR túto možnosť dávala, ale nebola poskytovaná na komerčnej báze

– služba doručovania pre registrované zásielky

- » iba všeobecná definícia a určenie právnych účinkov doručenia
- » absentujú štandardy (bude treba pravdepodobne zosúladiť Zákon o eGovernmente)

3. Otvorené otázky

- eIDAS primárne rieši dôveryhodné služby a ich interoperabilitu, jednotlivé procesné detaily bude pravdepodobne potrebné doriešiť
- existuje viacero otázok aplikácie pre eGovernment, ktoré bude potrebné doriešiť

■ Použitie elektronických dokumentov

- eIDAS síce vyžaduje akceptáciu elektronických dokumentov, ale:
 - » musím akceptovať elektronický dokument v akomkoľvek formáte ?
 - » ako sa vysporiadať s formátmi, kde informačný obsah nie je jednoznačne daný vizualizáciou (napr. XML ?)
- stav v SR
 - » výnos o štandardoch - minimálny rozsah formátov, ktoré musí orgán akceptovať, iné dobrovoľne
 - » pre XML dáta definované formuláre – vždy spojené s definíciou dátovej štruktúry a vizualizáciou, ktoré umožňujú údajom jednoznačne priradiť informačný obsah
 - » ako bude zabezpečená interoperabilita v EU ?

■ Autorizácia úkonov

- QES je na úrovni vlastnoručného podpisu
 - » nie je riešená potreba jednoznačnej identifikácie osoby, ani jej statutu (podpis síce platný, ale nemožnosť vyhodnotenia platnosti úkonu)
 - » aj keď viem identitu (identifikátor) otázne sprístupnenie údajov o osobe
- stav v SR
 - » QES s časovou pečiatkou zrovnoprávňuje s úradne osvedčeným podpisom
 - » zavedenie MOŽNOSTI uvedenia RČ v certifikáte
 - ako bude OVM reagovať ak tam identifikátor nebude ?
 - » prepojenie na referenčné registre
 - » definovanie „mandátnych certifikátov“ a ich používania

■ Elektronická komunikácia/doručovanie

– v eIDAS všeobecné definovanie princípov, zatiaľ bez štandardov

» nie je jasný obsah komunikácie – správy, možnosť aj neštruktúrovaného textu

■ možný problém s automatizovaným spracovaním QES je na úrovni vlastnoručného podpisu

» nakoľko použitie služby je dobrovoľné, otázka zistenia či je subjektu možné doručovať elektronicky

» nakoľko môžu poskytovať viaceré subjekty aj cezhranične, problém s registrom adries (obdobne ako pri mobilných operátoroch)

– stav v SR

» Zákon o eGov jednoznačne definuje

- formát správ pre elektronickú komunikáciu
- miesto doručovania – elektronická schránka
- povinnosť elektronicky komunikovať
- zatiaľ jeden poskytovateľ – NASES

» elektronickú komunikáciu nielen v eGov procesoch bude potrebné upraviť, rovnako ako aktualizovať v tomto kontexte Zákon o eGovernmente



**Ďakujem za
pozornosť**