



eIDAS v praxi

Aktuální témata

Position on the Market

Our company is currently the biggest provider of electronic certification services in the Czech and Slovak Republic. Demands of clients are met through an infrastructure of so-called registration authorities, recently having expanded the number of 400 in count. Their spread over the whole territory of the country is a notable competitive advantage. These contacting offices thus provide optimum accessibility of our products and services.

The quantity of certificates issued in the Czech Republic is also unmatched. Their number has reached six-digit numbers. These competitive advantages enable the company to continuously develop its product portfolio as well as improve quality of services provided.

První certifikační autorita, a. s.

Ing. Petr B u d i š, Ph.D., MBA

5. 4. 2018

Validity of certificates is limited and is among the information contained in the certificate. This value is of paramount importance. Developments in performing power of computer technology has chances, however remote, of breaking of protocols and algorithms could in long-term void the reliability of digital certificates. Regularly issued certificates bear six-month validity. Validity of a certificate can be nullified even during the period if required e.g. by disclosure of private key of the certificate.

Nullified certificate is registered in the list of nullified certificates (CRL). The list of void certifi-



Právní základ



eIDAS

Nařízení je platné od 17.9.2014 a účinné od 1. července 2016 s tím, že jednotlivá ustanovení budou nabývat účinnosti postupně v období let 2016 - 2018. Všechna ustanovení související s elektronickými podpisy, pečetěmi a razítky jsou již účinná od roku 2016.

Zákon o službách vytvářejících důvěru

- účinnost celého zákona nastala 19. 9. 2016
- platnost přechodných ustanovení končí 19. 9. 2018 (včetně)

Oba právní předpisy tedy v roce 2018 budou plně účinné.

Zákon o službách vytvářejících důvěru



Přechodná ustanovení platná do 19. 9. 2018 reagovala především na skutečnost, že veřejnoprávní podepisující mají povinnost - pokud právně jednají - používat **kvalifikovaný elektronický podpis nebo kvalifikovanou elektronickou pečeť**.

Kvalifikovaný elektronický podpis je vytvářen pomocí kvalifikovaného prostředku pro vytváření elektronických podpisů (QSigCD - příslušně hodnocené čipové karty).

K 19. 9. 2016 nebyly povinné subjekty dostatečně vybaveny QSigCD - v současné době zaznamenáváme výrazné zlepšení, úřady a ostatní subjekty intenzivně řeší.

Pozor: Ne každá ČK je QSigCD a ne vše, co je nabízeno jako QSigCD, jím skutečně je! Je nutné kontrolovat na webu MV, resp. EK!!!

Kvalifikovaná elektronická časová razítka



Všichni veřejnoprávní podepisující mají od 19. 9. 2016 povinnost opatřovat kvalifikovaným elektronickým časovým razítkem elektronicky podepsané dokumenty, kterými právně jednají (§ 11 zákona č. 297/2016 Sb.).

Podle vyjádření zástupců MV může být nedodržení této povinnosti shledáno jako „nesprávný úřední postup“ se všemi důsledky z toho vyplývajícími.

Nesprávným úředním postupem se rozumí porušení pravidel předepsaných právními normami pro počínání státního orgánu při jeho činnosti. Je možné žádat náhradu vzniklé škody.

Zákon o službách vytvářejících důvěru

CERTIFICATION
AUTHORITY

Kvalifikovaná elektronická pečeť je vytvářena pomocí kvalifikovaného prostředku pro vytváření elektronických pečetí (QSealCD - příslušně hodnocený hardwarový modul).

QSealCD

- stále nejsou na trhu běžně k dispozici (3 čipové karty, 4 HSM moduly, avšak pro režim vzdáleného pečetění)
- cena HSM je vysoká a úřady a další povinné subjekty by příslušný výdaj výrazně zatížil (menší úřady až likvidačně)
- implementace a údržba QSealCD je technicky velmi náročná (a tedy i finančně).

Řešení? Použití služby vzdáleného vytváření kvalifikovaných elektronických pečetí jménem pečetící osoby (tj. vzdálené pečetění).
QSealCD nemá uživatel, ale kvalifikovaný poskytovatel (např. I.CA).

Pečetění na dálku



I.CA službu intenzivně připravuje, tj.

- má QSealCD
- připravuje testování služby a následné uvedení do provozního režimu
- následovat bude žádost o udělení statutu kvalifikované služby, který uděluje MV.

MV je o přípravě služby informováno a přislíbilo posouzení žádosti tak, aby - pokud budou ze strany I.CA splněny všechny zákonné požadavky - služba mohla být na trhu během léta 2018.

Podrobněji následující příspěvky.

QWAC a jejich uplatnění



Novinka dle eIDAS - kvalifikované certifikáty pro autentizaci internetových stránek (qualified certificates for website authentication - QWAC) - de facto SSL certifikáty.

QWAC podle eIDAS - umožňuje autentizovat internetové stránky a spojuje je s fyzickou nebo právnickou osobou, jíž je certifikát vydán.

Právními předpisy není stanovena povinnost QWAC používat - mohlo by v budoucnu být například povinné pro webové stránky orgánů státu.

Aktuální uplatnění - pro splnění požadavků směrnice EU o platebních službách na vnitřním trhu (PSD2), zejména pro účely přístupu nových poskytovatelů/zprostředkovatelů platebních služeb na finančním trhu k finančním institucím a jejich platebním systémům.



Potenciál eIDAS



Potenciál eIDAS zdaleka nebyl plně využit.

Jsou a budou připravovány další nové služby:

- Vytváření elektronického podpisu na dálku
- Služba elektronické doporučené zásilky
- Využití elektronické identifikace i soukromým sektorem.

Potenciál eIDAS



Potenciál eIDAS zdaleka nebyl plně využit.

Co je stále podceňováno:

Ověřování platnosti kvalifikovaných elektronických podpisů/pečetí.

Službu nabízíme, zájem však není velký, byť se jedná o splnění zákonné povinnosti. Řádné ověřování platnosti elektronického podpisu je stále podceňováno, přičemž následky mohou být velmi nepříjemné.

Závěr



Děkuji za pozornost.
budis@ica.cz