



První certifikační autorita, a.s., (I. CA) was founded at the beginning of the year 2001. The use gained in implementation and operation of the project of commercial providing of sophisticated services in the Czech Republic is one of the determining factors for high quality services.

The most important step forward was successful completion of accreditation process in sense of Law 227/2000 about electronic signature and cohering edicts. The Office for Personal Data Protection confers on První certifikační autorita, a.s a certificate of accreditation provider of certification services in the Czech Republic with effectiveness since 1st of May 2002. In 2006 I.CA get certificate of accreditation provider of certification services in the Slovak Republic Law 215/2002 about electronic signature too.

In both countries I.CA provide time stamp services as accredited provider of certification services too.

První zkušenosti s implementací eIDAS

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 exceeded 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 risen six times during the last five years. These achievements enable the company to continuously develop its product portfolio as well as improve quality of services provided.

Ing. Petr Budiš, Ph.D., MBA
předseda představenstva a ředitel,

Certificates, Qualified certificates

A digital certificate is an electronic version of identity card, it even contains similar set of information. First of all, it explicitly connects physical and electronic identities.

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 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-



Témata



- (Ne)znalost obsahu eIDAS
- Opožděné přijetí adaptačního zákona v ČR i SR - údajně však problém téměř všech členských států
- Terminologie
- Nezájem o elektronické pečete, zatím setrvání u uznávaných elektronických značek
- Absence posuzovatelů shody
- Kvalifikovaný nebo „běžný“ elektronický podpis?
- Nové služby I.CA
- Další otevření obchodních příležitostí v zahraničí
- Náklady poskytovatelů

Typické dotazy



- Které ustanovení eIDAS stanoví, jak mají být elektronicky podepisovány smlouvy, nabídky faktury?
- Které ustanovení eIDAS stanoví, kdy je možné použít biometrický podpis?
- Které ustanovení eIDAS stanoví, kdo může používat elektronické pečete?
- Je možné místo elektronického podpisu použít pro podpis smlouvy elektronickou pečeť? Které ustanovení eIDAS tak stanoví?

Odpověď: Žádné, taková ustanovení eIDAS neobsahuje.

Znalost obsahu eIDAS



- I.CA od roku 2014 realizovala řadu akcí, na kterých své klienty a další zájemce seznamovala s obsahem eIDAS - odborné konference, semináře u klientů, publikování odborných článků, distribuce eIDAS jako publikace, konzultace a návrhy řešení.
- První zkušenosti ukazují, že
 - nedostatečná povědomost o eIDAS je u některých dodavatelů aplikací
 - ne každý, kdo o eIDAS mluví, ho skutečně četl
 - ne každý, kdo eIDAS četl, skutečně rozumí jeho obsahu.
- Z uvedených důvodů budeme pokračovat v realizaci odborných akcí a jistě tak bude činit i MV.

Terminologie - problémy



Dočasná ztráta označení „kvalifikovaný“ u některých služeb, problém zejména u elektronických časových razítek, tj. podle § 18 adaptačního zákona:

„(4) Po dobu 2 let ode dne nabytí účinnosti tohoto zákona lze namísto kvalifikovaného elektronického časového razítka podle § 11 použít elektronické časové razítko vydané kvalifikovaným poskytovatelem služeb vytvářejících důvěru.“.

Obdobně platí pro *(kvalifikované) systémové certifikáty*.

Příklad



- I.CA vydávala do 30. 6. 2016 kvalifikovaná časová razítka.
- Od 1. 7. 2016 I.CA vydává elektronická časová razítka vydaná kvalifikovaným poskytovatelem důvěryhodných služeb (protože vydává kvalifikované certifikáty, automaticky přechází pro tuto službu do režimu eIDAS)
- Po provedení posouzení shody a následném posouzení Ministerstvem vnitra - bude I.CA vydávat kvalifikovaná elektronická časová razítka.
- Naopak kvalifikované systémové certifikáty už budou pouze systémovými certifikáty, a to na dobu 2 let. Pak bude možnost jejich používání ukončena.

Uznávaný elektronický podpis



Uznávaný elektronický podpis - pojem pouze pro ČR.

- **Dosud** podle 227/2000 Sb. - zaručený elektronický podpis založený na kvalifikovaném certifikátu.
- **Nově** podle adaptačního zákona - buď původní uznávaný elektronický podpis nebo **kvalifikovaný elektronický podpis** (s QESCD, resp. QESigCD, s kvalifikovaným prostředkem pro vytváření elektronických podpisů).
- eIDAS pojem „uznávaný elektronický podpis“ neobsahuje.

QESigCD a kvalifikovaní poskytovatelé



Kvalifikovaní poskytovatelé budou pro generování soukromých klíčů akceptovat pouze ty QESigCD, které mají „pod svou kontrolou“.

Kvalifikovaní poskytovatelé nemohou přebírat odpovědnost za jiné QESigCD, a to i z toho důvodu, že podle eIDAS je důkazní břemeno v případě vzniku škody na kvalifikovaných poskytovatelích tj. tj. musí prokázat, že škoda nastala bez jejich úmyslu nebo nedbalosti.

Samostatnou kapitolou jsou bezpečné prostředky pro kvalifikované elektronické pečeti - čekáme na upřesnění z EK.

Elektronická značka versus elektronická pečeť



Po dobu 2 let lze namísto zaručené elektronické pečetě založené na kvalifikovaném certifikátu pro elektronickou pečeť

nebo namísto kvalifikované elektronické pečetě použít

- elektronickou značku podle zákona č. 227/2000 Sb., založenou na (*kvalifikovaném*) systémovém certifikátu vydaném akreditovaným poskytovatelem (I.CA)
- zaručenou elektronickou pečeť založenou na certifikátu pro elektronickou pečeť vydaném kvalifikovaným poskytovatelem služeb vytvářejících důvěru. (I.CA)

§ 18 odst. 2 adaptačního zákona

Značky a pečetě - rozdíl podle eIDAS



- Certifikát pro elektronickou pečeť může být vydán jen na **právníckou osobu**.
- Elektronickou značkou pečetí pouze **původce dokumentu** (nikoliv například příjemce).
- Platí pro kvalifikované i „nekvalifikované“ certifikáty pro elektronické pečetě a jejich použití.

V důsledku dvouletého odkladu prozatím uživatelé neprojevují zájem o používání elektronických pečetí. Očekáváme, že přechod budou řešit zejména v roce 2017.

Posuzovatelé shody



- Podle eIDAS jsou služby nejvyšší kvality označovány jako „kvalifikované“.
- Aby služba mohla nést označení „kvalifikovaná“, musí projít „posouzením shody“ s požadavky eIDAS.
- U kvalifikovaných certifikátů je tato povinnost o rok odložena.
- Posouzení shody mohou provádět jen k tomu určené subjekty - posuzovatelé shody. V ČR je určí ČIA.
- Tyto subjekty dosud neexistují. V krajní časové nouzi I.CA zvažuje, že se obrátí na zahraničního posuzovatele. To ovšem znamená další náklady, minimálně na překlady veškeré potřebné dokumentace do jazyka posuzovatele.

Nové služby, které vyžadují provedení auditu



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

Použit kvalifikovaný nebo „běžný“ e-podpis

Kvalifikovaný elektronický podpis

- pokud tak stanoví příslušný právní předpis, v ČR např. pro veřejnoprávní podepisující
- pokud se komunikující strany na této formě podpisu dohodnou
- při komunikaci do jiných členských států EU, pokud si komunikující nestanoví jinak.

V ostatních případech je žádoucí mít na zřeteli ustanovení čl. 25 odst. 2) eIDAS:

Pouze „kvalifikovaný elektronický podpis“ má právní účinek rovnocenný vlastnoručnímu podpisu.

Odpovědnost za škodu



Při rozhodování o typu podpisu je důležité ustanovení eIDAS o odpovědnosti za škodu (čl. 13):

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

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

Nové služby I.CA



- I.CA bude na základě dosavadních zkušeností s požadavky a potřebami zákazníků rozvíjet prioritně následující služby:
- ověřování elektronických podpisů
 - čipové karty - kvalifikované prostředky pro vytváření elektronických podpisů (též prostředky pro kvalif. pečeti)
 - podpis v mobilu (MobileSign)
 - vytváření elektronického podpisu na dálku
 - vydávání certifikátů pro elektronické pečeti.

Zachovány zůstanou „tradiční“ služby - vydávání různých typů certifikátů, časových razítek, tvorba aplikací podle požadavků zákazníků aj.

Obchodní příležitosti v zahraničí



- eIDAS je pro I.CA vstupenkou na zahraniční trhy, především v EU.
- I.CA je zcela konkurenceschopná kvalitou služeb a cenami svých produktů.
- V zahraničí má I.CA již řadu klientů, narážela však na absenci nebo nesoulad právních úprav, a to zejména u časových razítek (úprava na úrovni EU před eIDAS neexistovala).
- Naopak vydávání kvalifikovaných certifikátů probíhalo zcela bez problémů.
- Na Slovensku je situace jiná, zde I.CA řádně působí již více než 10 let jako akreditovaný/kvalifikovaný poskytovatel.

Náklady poskytovatelů



- S přechodem na režim eIDAS vznikly poskytovatelům nemalé náklady - osvěta, úpravy interních systémů a aplikací, účast pracovníků I.CA na odborných akcích EU aj.
- Možnost zvýšení příjmů poskytovatelů v souvislosti s eIDAS se díky dvouletému odkladu některých povinností výrazně snížila.
- Přesto je snaha zachovat stávající ceny a výše uvedené náklady do nich nepromítat.
- Identifikujeme zájem o komplexní návrhy řešení přechodu na režim eIDAS.

Upozornění z praxe



- Podle § 11 adaptačního zákona platí povinnost opatřování dokumentu obsahujícího úkon veřejnoprávního podepisujícího nebo úkon jiné osoby při plnění jejích veřejnoprávních úkolů elektronickým časovým razítkem.
- eIDAS klade důraz na **řádné ověřování elektronického podpisu/pečetě**, ověřování definuje i jako samostatnou kvalifikovanou službu. Jako službu, do provedení posouzení shody bez označení „kvalifikovaná“, ji I.CA již nyní nabízí.

Závěr



Poděkování našim klientům, kteří s námi přechod na režim eIDAS absolvovali, za maximální vstřícnost a součinnost.

Děkuji za pozornost.

budis@ica.cz