



První certifikační autorita, a.s., (I. CA) was founded at the beginning of the year 2001. The use of digital certificates 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 of provided services.

The most important step forward was a 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 and in 2007 also in the Hungary.

Problematika dlouhodobého ověřování platnosti elektronických dokumentů

Our company is currently the biggest provider of electronic certification services in the Czech Republic. During the last years we have issued more than 40 million of certificates in all countries, mainly having electronic documents of 40000000. 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.

ITAPA 2016

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.

With the help of the information contained in the certificate.

This value is of paramount importance. Developments in performing power of computer technology 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 certificates is therefore a part of a full list of valid certificates with mention of invalidity of void



Představení společnosti



- První certifikační autorita, a.s. (I.CA) je poskytovatelem služeb vytvářejících důvěru dle **nařízení eIDAS**, nabízí služby vydávání certifikátů, služby časové autority a komplexní řešení PKI.
- Společnost v roce 2002 získala, jako první v ČR, akreditaci pro výkon činnosti akreditovaného poskytovatele certifikačních služeb. V roce 2006 tuto akreditaci získala i zde na Slovensku.

Elektronická časová razítka



- Mimo certifikačních služeb poskytuje také služby vydávání elektronických časových razítek.
- Elektronické časové razítko je datová zpráva, která spojuje elektronická data s konkrétním časem.
- V běžné „papírové agendě“ se považuje za jednotku času zpravidla den, v tom elektronickém je to sekunda. Jediným důvěryhodným a legislativně uznatelným nástrojem pro spojení dokumentu a události s časem je elektronické časové razítko, vydané poskytovatelem důvěryhodných služeb.



Ověřování platnosti elektronických dokumentů

- Elektronický dokument **musí obsahovat** (ve své vnitřní struktuře) veškeré informace pro jeho ověření, tzv. validační data:
 - Certifikační cestu k podpisovým certifikátům
 - Certifikační cestu k certifikátům časových autorit
 - CRL pro všechny vložené certifikáty
 - OCSP odpovědi pro vložené certifikáty



Ověřování platnosti elektronických dokumentů



- Ověření platnosti elektronického podpisu – rozhodný čas
 - dokument není opatřen časovým razítkem*, zadání času uživatelem, ověřuje se k tomuto zadanému času
 - dokument není opatřen časovým razítkem*, uživatel nezadá čas, ověřuje se k času přijetí požadavku na ověření
 - dokument je opatřen časovým razítkem, ověřuje se k času, který je uveden v tomto razítku

* *Povinnost připojení časového razítka, zákon č. 305/2013 (zákon e-Gov)*

Služby I.CA zahrnující časová razítka



- TSA (standardní časová razítka, v případě víceleté archivace je nutné zajištění přerazítkování uživatelem)
- ATSA (služba Archivní časová razítka, zajištění komplexní služby pro středně dobou archivaci v prostředí I.CA, bez nutnosti interakce uživatele)
- Archive Time TSA (komplexní služba TSA/ATSA s volitelnou dobou archivace)
- LTV eSign (komponenta pro řešení dlouhodobého uchovávání elektronických podpisů v elektronických dokumentech)
- I.CA Qverify (kvalifikovaná služba ověřování platnosti elektronických podpisů)

- Doporučujeme zvolit takovou službu časových razítek, která bude v souladu s požadavky na uchování dokumentů, a dále které vyplívají z povahy a typu dokumentů, z jejich následného používání, ze skartační lhůty dokumentů a ze způsobu ověřování.

Služba	Správa vydaných časových razítek	Volitelná délka archivace	Automatické přerazítkování
TSA	✗	✓	✗
ATSA	✓	✗	✓
ATTSA	✓	✓	✓

- Uchovávání elektronických dokumentů pro budoucí ověření není jednoduchá problematika. Není uživatelsky komfortní „ručně“ zajistit plnou ověřitelnost dokumentů po celou požadovanou dobu bez spolehlivé služby.



■ Iné možnosti riešenia dlhodobej archivácie elektronických dokumentov

- v prípade väčšieho počtu elektronických dokumentov potreba množstva časových pečiatok
 - Požiadavky na poskytovateľa služby (v prípade potreby „repečiatkovania“ pri ukočení platnosti vcertifikátu služby časovej pečiatky)
 - Cena v prípade veľkých množstiev
 - Duplicitné uchovávanie validačných údajov (v každej štruktúre elektronického podpisu)
- potreba hľadania efektívnejšieho riešenia



■ Modul dlhodobej archivácie (MDA)

- zabezpečenie dlhodobej archivácie a overiteľnosti dokumentov a k nim pripojených (zaručených) elektronických podpisov/pečatí
- základný princíp
 - preukázanie neporušenia integrity dokumentov, podpisov a k nim viazaných validačných dát
 - validačné dáta uchovávané samostatne, nie vo väzbe na konkrétny elektronický podpis/pečať
 - prepojenie na certifikačné authority (CRL a OCSP) a poskytovateľov TS
 - integrita a potvrdenie existencie v čase zabezpečované prostredníctvom TS pre skupiny údajov, nie k danému EP
 - efektívnosť tohto riešenia je založená na usporiadaných Merkleho hashovacích stromoch



- **z časového hľadiska zabezpečenie použitia nových kryptografických metód so zachovaním preukázateľnosti neporušenia integrity**
 - vytvorenie nového stromu s novou kryptografickou funkciou
- **riešenie je v súlade so špecifikáciami pracovnej skupiny IETF LTANS (Long-Term Archive and Notary Services)**
 - RFC4810
 - RFC4998
 - RFC6283



■ Základná funkcionality

- vytváranie dôkazových záznamov (Evidence Records) pre dlhodobu archivované dáta
 - dôkazový záznam je súbor informácií, ktoré môžu byť použité na demonštrovanie platnosti archivovaného dátového objektu
 - zabezpečuje ochranu integrity a neodmietnuteľnosť pre všetky objekty pokryté v rámci sekvencie archívnych časových pečiatok

■ praktické skúsenosti s implementáciou

- systém prevádzkovaný cca 4 roky
- nasadenie v rámci systémov Ministerstva vnútra a systému Centrálny elektronický priečinok

První certifikační autorita, a.s., (I. CA) was founded at the beginning of the year 2001.

of own expertise and experience gained in its development that has become the first one in a field of commercial practice in the area of issuing and administration of digital certificates. The determining factors for high quality of provided services are:

The most important step forwards was a successful completion of accreditation in the sense of Law 227/2000 about electronic signature and e-governing edicts.



Děkujeme za pozornost

Mgr. Kateřina Jarošová

První certifikační autorita, a.s.

jarosova@ica.cz

Pavol Frič

DITEC a.s.

pf@дитеc.sk