

Aplikace pro tvorbu Elektronického podpisu Čipové karty



I.CA Secom je klientská aplikace, která umožňuje vytváření a ověřování elektronického podpisu vybraných souborů. Elektronický podpis lze vytvářet samostatně nebo s kvalifikovaným časovým razítkem. V aplikaci je možné zvolit mezi **interním** a **externím podpisem** (ve formátech p7s nebo p7m), které jsou v souladu s vyhláškou č. 194/2009 Sb.,

o stanovení podrobností užívání a provozování informačního systému datových schránek. Další možností aplikace je využití podpory pro formát dokumentů **PDF** (PADES), kde je možné zvolit také vložení viditelného podpisu. I zde lze využít vložení časového razítka. Kromě výše uvedených funkcí je možné vytvářet dlouhodobý elektronický podpis dle stan-

dardu RFC 5126 ve formátu Cades-T při podepisování podpisem CMS a vícenásobný podpis k jednomu souboru. Aplikace I.CA Secom je k dispozici také ve verzi **I.CA Secom ZEP**, která podporuje formát, požadovaný pro komunikaci s orgány veřejné moci Slovenské republiky.

Pro implementaci elektronického podpisu do informačních systémů I.CA poskytuje specializované komponenty.

ICASigner umožňuje vytvoření a ověření elektronického podpisu ve formátu PKCS#7. Komponenta podporuje interní

i externí elektronický podpis a také práci s časovými razítky. ICASigner je k dispozici ve formátu ActiveX komponenty, dle knihovny nebo ve formátu Java appletu.

AdvICASigner slouží k realizaci interního a externího elektro-

nického podpisu obecných souborů dle podpisového profilu CAdES (BES, T, A) a k realizaci interního podpisu PDF souboru dle podpisového profilu PADES-BES.

I tato komponenta poskytuje podporu pro časová razítka.



Čipové karty jsou jedním z nástrojů pro zabezpečení dat pro tvorbu elektronického podpisu (úložiště privátních klíčů).

I.CA nabízí komplexní řešení **SecureStore I.CA**, spojující čipovou kartu řady Starcos, renomovaného výrobce Giesecke & Devrient, se sadou uživatelských aplikací, které umožňují uživateli komfortní práci s čipovou kartou. Toto řešení je certifikováno jako bezpečný prostředek pro vytváření elektronického podpisu (SSCD) v souladu s platnou legislativou Čes-

ké republiky a Slovenské republiky.

Čipová karta má dostatečný prostor pro uložení až osmi privátních klíčů klienta, dále je na ní možné uložit současně několik kvalifikovaných i komerčních certifikátů. Karta je využívána i pro bezpečné uložení kořenového certifikátu vybrané Certifikační autority.

Čipová karta má životnost několik let, během života karty si může majitel na kartu nechat vydat několik certifikátů.

Bezpečnostně citlivé operace je

na kartě možné vždy realizovat pouze po zadání PIN, jehož délka je volitelná na 4 – 8 numerických znaků.

V případě blokace karty chybným zadáním PIN, jí lze odblokovat s využitím PUK.

Čipové karty jsou k dispozici v podobě běžných kontaktních karet nebo ve formátu Plug-in (výřez ve velikosti SIM karty), určené pro umístění do USB tokenů, které je možné připojit přímo do USB rozhraní.

O společnosti

První certifikační autorita, a.s. (I.CA), je v současnosti největším poskytovatelem komplexních služeb vydávání a správy certifikátů v České republice a na Slovensku.

Vznikla na pevných základech špičkového světového i tuzemského know-how a týmů kvalifikovaných odborníků v oblasti bezpečnostních technologií a certifikačních autorit.

Jako samostatná společnost

nabízí I.CA svoje služby klientům od roku 2001.

S účinností od 18.3.2002 I.CA získala jako první v České republice osvědčení pro výkon činnosti akreditovaného poskytovatele certifikačních služeb ve smyslu zákona č. 227/2000 Sb., o elektronickém podpisu.

Následně v roce 2006 získala akreditaci pro vydávání kvalifikovaných systémových certifikátů a kvalifikovaných časových razítek.

vých razítek.

Rovněž v roce 2006 získala společnost akreditaci pro vydávání kvalifikovaných certifikátů a pro poskytování služby časové autority na Slovensku.

Počty vydaných certifikátů jsou dnes evidovány ve statistických ročnících.

Komplexností a rozsahem svých služeb je I.CA jednou z nejvýznamnějších evropských společností v této oblasti.

