



## D. Trust Certifikačná Autorita, a.s.

### O SPOLOČNOSTI

Spoločnosť D. Trust Certifikačná Autorita, a.s., (ďalej DTCA) je poskytovateľom akreditovaných certifikačných služieb, t.j. vydávania a správy certifikátov a kvalifikovaných certifikátov verejných kľúčov v zmysle Zákona o elektronickom podpise č. 215/2002 Z.z.

DTCA bola založená spoločnosťami PVT, a.s., so sídlom v Prahe, DITEC, a.s., Bratislava a Tatra banka, a.s., Bratislava (člen finančnej skupiny Raiffeisen Banking Group). Hlavným dôvodom pre založenie DTCA bol záujem jej zakladateľov podporovať rozvoj a používanie elektronického podpisu na Slovensku. Pri poskytovaní certifikačných služieb DTCA veľmi úzko spolupracuje so spoločnosťou První certifikační autorita (I.CA), a.s., ktorá je dominantným poskytovateľom certifikačných služieb v rámci Českej republiky.

Najvyššiu kvalitu služieb poskytovaných D.Trust Certifikačnou Autoritou, a.s., potvrdil Národný bezpečnostný úrad SR udelením akreditácie v zmysle zákona č. 215/2002 Z.z. o elektronickom podpise. DTCA tak od 28.6.2004 získala oprávnenie poskytovať akreditované certifikačné služby a vydávať kvalifikované certifikáty a časové pečiatky.

Riešenia využívajúce technológiu elektronického podpisu majú svoju legislatívnu oporu v zákone č. 215/2002 Z.z. o elektronickom podpise, ktorý rieši zákonné otázky súvisiace s ich nasadením a používaním v systémoch Public Key Infrastructure (PKI).

### SLUŽBA VYDÁVANIA ČASOVÝCH PEČIATOK

Pri komunikácii a spracovaní papierových dokumentov v praxi sme zvyknutí bežne sa stretávať s vyznačovaním dátumu a času na týchto dokumentoch. Robíme to pri ich odoslaní a prijatí, pri vykonaní každej dôležitej činnosti vyžadujúcej zaprotokolovanie, pri určení počiatku platnosti zmluvy a podobne. Taktó vložené časové údaje sa následne stávajú efektívnym kľúčom napr. k zoradovaniu dokumentov pre ich archiváciu. Rovnaká potreba evidencie času prirodzene vzniká pri elektronickej komunikácii, tu je však situácia značne zložitejšia.

Po dosadnutí pečiatky overujúcej dátum podania dokumentu na papier máme vzhľadom na overené postupy správy dokumentov a na skutočnosť, že pečiatku nie je možné úplne bez stopy z papiera odstrániť, pomerne dobrú záruku, že nikto tento čas nezmení a ani nespochybní. Čo však v prípade podania elektronického dokumentu? Možnosť kedykoľvek jednoducho meniť obsah elektronického dokumentu je v tomto prípade kritickým problémom. Ako zabezpečíme, že čas, ktorý niekto jednoducho zapísal do dokumentu, napríklad v textovej forme, nebol následne zmenený? Takáto forma zápisu preto nemôže byť vo všeobecnosti pokladaná za dôveryhodnú.

Dôveryhodnosť vloženia časových údajov v papierovom dokumente rovnako pramení i zo skutočnosti, že pri tomto úkone sa spravidla nachádzajú zástupcovia všetkých zúčastnených strán. Títo zabezpečia, aby bol do dokumentu zanesený skutočne aktuálny čas, inak dokument neakceptujú. Aký postup však zvolíť v prípade elektronických dokumentov? Pri ich spracovaní sa obyčajne komunikujúce strany nestretnú. Dokument je dokonca obyčajne spracúvaný komunikujúcimi stranami v značnom časovom oneskorení, napr. pri posielaní elektronickej pošty. Jedna zo strán sa teda musí spoliehať na serióznosť druhej strany a na jej schopnosť získať presný čas. Splnenie ani jednej z týchto požiadaviek v praxi nie je jednoduché.

Tieto praktické problémy viedli k vytvoreniu novej služby - vydávaniu časových pečiatok. Časová pečiatka je v istom zmysle obdobou podacieho lístku s pečiatkou, ktorý získate na pošte pri podaní dokumentu, avšak v elektronickej forme. Časová pečiatka je elektronický dokument, ktorý dosvedčuje, že iný „opečiatkovaný“ elektronický dokument existoval v čase uvedenom v časovej pečiatke. Časová pečiatka však navyše umožňuje zistiť i to, že samotný opečiatkovaný dokument sa od jej vydania nezmenil. Časová pečiatka tak umožňuje chrániť ako čas, tak i obsah dokumentu.

Časové pečiatky smie v zmysle zákona o elektronickom podpise vydávať len akreditovaná certifikačná autorita - dôveryhodný poskytovateľ certifikačných služieb preverený Národným bezpečnostným úradom SR. Keďže služby akreditovanej certifikačnej autority sú overené a zdokumentované, možno ich považovať za všeobecne dôveryhodné. Týmto spôsobom je vyriešený problém spoľahlivého zdroja času. Nech časovú pečiatku získa ktorákoľvek z komunikujúcich strán, všetky strany môžu plne dôverovať časovým údajom v nej uvedeným, keďže ju vydala dôveryhodná tretia strana. Rovnako je možné spoliehať sa na presnosť času uvedeného v časovej pečiatke. DTCA prevádzkuje monitorovaný zdroj času a garantuje presnosť časových údajov uvedených v časovej pečiatke na úrovni niekoľkých desiatín sekundy - teda s presnosťou neporovnateľne vyššou ako sme zvyknutí z prostredia papierových dokumentov.

Problém zamedzenia dodatočnej zmeny dokumentu po vydaní časovej pečiatky sa rieši použitím elektronického podpisu. Pri vydaní časovej pečiatky, v ktorej je obsiahnutý jednoznačný odtlačok dokumentu, ju akreditovaná certifikačná autorita podpíše elektronickým podpisom. Týmto je zaručená autenticita a nemennosť údajov uvedených v časovej pečiatke. Každý má následne možnosť overiť podpis na časovej pečiatke a zistiť tak, či je skutočne platná.

### ZÍSKANIE ČASOVEJ PEČIATKY

Získanie časovej pečiatky z pohľadu žiadateľa o túto službu je mimoriadne jednoduché. Žiadateľ do DTCA zašle pomocou štandardizovaného protokolu digitálny odtlačok dokumentu, ktorý si praje opečiatkovať a autentifikuje sa pomocou certifikátu vydaného DTCA. DTCA následne vydáva časovú pečiatku a odošle ju žiadateľovi.

Pre účely individuálneho získavania časových pečiatok pre dokumenty poskytuje DTCA svojim klientom aplikáciu, ktorá umožňuje opečiatkovanie dokumentov prakticky automaticky. Užívateľ len vyberie súbor, ktorý chce opečiatkovať a certifikát, ktorým sa chce autentifikovať pre prístup k službe. Zvyšok procesu zabezpečí aplikácia samostatne. Užívateľ má následne možnosť pomocou tejto aplikácie overiť platnosť vydanéj časovej pečiatky.

Pre potreby vydávania časových pečiatok v automatizovaných procesoch (napr. pri vydávaní elektronických faktúr, vystavovaní potvrdení o prijatí dokumentu a pod.) môže DTCA poskytnúť pripravené moduly pre plne automatizované získavanie časových pečiatok, ktoré je možné jednoducho integrovať do existujúcich alebo vznikajúcich informačných systémov. Zákazníci tak majú možnosť pri minimálnych vstupných nákladoch značne zvýšiť úroveň bezpečnosti a dôveryhodnosti svojich systémov a služieb. V prípade špecifických požiadaviek je možné poskytnúť špecializované rozhrania a konzultácie pre integrovanie služby časových pečiatok do zákaznických systémov.

### MOŽNOSTI VYUŽITIA ČASOVÝCH PEČIATOK

Časové pečiatky sú silným nástrojom pre jednoznačné doloženie času existencie dokumentu a zabezpečenie jeho integrity. Ako také môžu byť použité v širokom spektre aplikácií vyžadujúcich tieto funkcie a to

často nečakaným spôsobom. V súčasnosti sú časové pečiatky najčastejšie využívané v nižšie uvedených oblastiach, vzhľadom na ich potenciál je však možné predpokladať ich rozšírenie i do mnohých ďalších oblastí:

- Vydávanie potvrdení o prijatí elektronických dokumentov v rámci elektronických podateľní
- Archivácia elektronických dokumentov
- Doloženie času vykonania senzitívnych transakcií
- Doloženie časovej súslednosti obchodných transakcií
- Uzatváranie zmlúv v elektronickej podobe
- Zaručenie integrity auditných záznamov
- Zaručenie integrity softvérových produktov
- Vytváranie elektronických podpisov s dlhodobou platnosťou

Vybraní zákazníci, využívajúci služby DTCA:

- Colné riaditeľstvo SR
- Daňové riaditeľstvo SR
- Kancelária Národnej rady Slovenskej republiky
- Centrálny depozitár cenných papierov SR, a.s.
- Tatra banka, a.s.
- ČSOB, a.s.
- Dexia banka Slovensko, a.s.
- Všeobecná sociálna poisťovňa TATRY, a.s.

### REGISTRÁCIA

Certifikačná autorita DTCA je registrovaná Národným bezpečnostným úradom. Certifikačné služby v zmysle zákona o elektronickom podpise poskytuje DTCA od 1.1.2003. Informačný systém DTCA je registrovaný Úradom na ochranu osobných údajov v zmysle zákona č. 428/2002 Z.z. o ochrane osobných údajov, pod registračným číslom 190829.

### AKREDITÁCIA

Certifikačná autorita DTCA je akreditovaná Národným bezpečnostným úradom. Akreditované certifikačné služby v zmysle zákona o elektronickom podpise je DTCA oprávnená poskytovať od 28.6.2004.



### KONTAKTNÉ INFORMÁCIE

D. Trust Certifikačná Autorita, a.s.  
Plynárska 7/C, 821 09 Bratislava 2  
zapísaná v bchodnom registri Okresného súdu  
Bratislava I, oddiel Sa, vložka číslo 2986/B  
tel.: (02) 58 222 153, fax: (02) 58 222 777  
e-mail: info@dtca.sk, web: <http://www.dtca.sk>

