



# Elektronické časové razítko jako doplněk e-podpisu

Při psaní smluv nebo dopisů se k textu vždy připojuje vlastnoruční podpis, zároveň je uváděno i datum podpisu, sloužící k identifikaci platnosti smlouvy.

**P**rávní předpisy soukromého práva z neexistence data neodvozuji neplatnost smlouvy, ale pokud nebude datum uvedeno, může být platnost sporná (napadnutelná). Volitelnou, avšak velmi často požadovanou a neoddělitelnou součástí každého listinného dokumentu je tedy podpis a datum jeho vzniku či platnosti. Stejným způsobem datum slouží jako identifikátor např. i u účetních dokladů s ohledem na jejich datum vystavení nebo splatnost. Výhoda listinných dokumentů je v tom, že podpis i datum se dodatečně jen těžko mění, což je účel. U elektronických dokumentů je změna uvnitř dokumentu naopak dílem okamžiku, a tak je důležité mít tyto dokumenty podepsané a označené datem tak, aby dodatečná změna nebyla možná. Příkladem takových dokumentů mohou být smlouvy, účetní a daňové doklady, potvrzení apod. V řadě zemí byl zaveden takzvaný elektronický podpis a stanoveny procedury, jak elek-

tronický dokument podepsat a označit časovým údajem, aby jeho platnost byla právně stejná jako platnost podepsaného listinného dokumentu.

## Co je elektronický podpis?

Princip elektronického podpisu spočívá ve využití asymetrické kryptografie (dvojice klíčů). Data šifrovaná jedním z klíčů lze v rozumném čase dešifrovat pouze se znalostí druhého z dvojice klíčů a naopak. Jeden z nich, takzvaný privátní klíč, je s maximální bezpečností ukryván majitelem (čipové karty, disketa v trezoru...), zatímco druhý klíč je zveřejněn. Známe-li tedy vlastníka veřejného klíče, kterým jsme zprávu dešifrovali, známe odesílatele. K urychlení procesu se využívá vhodné hashovací funkce, kterou se pořídí tzv. otisk dokumentu, datový řetězec o pevné délce sloužící k jednoznačné charakteristice dokumentu a obsahující text nebo jinou informaci. Tento otisk se následně zašifruje

soukromým klíčem podepisujícího. Výsledkem je elektronický podpis, který spolu s původním textem znamená elektronicky podepsaný dokument. Správnost a platnost veřejného klíče podepisujícího potvrzuje certifikát vydaný a elektronicky podepsaný certifikační autoritou (poskytovatelem certifikačních služeb).

## Jak ověřit elektronický podpis

Dokumenty s dlouhou časovou platností někdy vyžadují ověření elektronického podpisu s časovým odstupem, tedy v době, kdy původní certifikáty obvykle ztratily svoji platnost. V okamžiku, kdy nemáme k dispozici údaj o datu vzniku dokumentu, nelze jednoduchým porovnáním s dobou platnosti certifikátu odvodit regulérnost podpisu dokumentu v době jeho platnosti. Východiskem je opětovné podepsání dokumentu a zároveň získání nového platného certifikátu. ■

**Jakub Humpolec,**  
technický ředitel IXTENT s.r.o.

Plné znění textu lze najít na  
[http://ihned.cz/c4-10036830-24518930-000000\\_d-elektronicke-casove-razitko-jako-doplnek-elektronickeho-podpisu](http://ihned.cz/c4-10036830-24518930-000000_d-elektronicke-casove-razitko-jako-doplnek-elektronickeho-podpisu)