CERTIFIKÁTEM TO NEKONČÍ

Bezpečná archivace elektronických dokumentů

Motto: jak zajistit důvěryhodné uložení elektronických dokumentů bez narušení vlastností integrity, časového určení a neodmítnutelnosti odpovědnosti? Produkty pro krátkodobou, střednědobou i dlouhodobou archivaci nabízí společnost První certifikační autorita, a. s. (I.CA).

Východiskem je právní rámec

Pro problematiku archivace elektronických dokumentů platí vyvratitelná právní domněnka uvedená v §69a odst. 8 zákona č.499/2004 Sb., o archivnictví a spisové službě, ve znění pozdějších předpisů: „Neprokáže-li se opak, dokument v digitální podobě se považuje za pravý, byl-li podepsán platným uznávaným elektronickým podpisem nebo označen platnou elektronickou značkou osoby, která k tomu byla v okamžiku podepsání nebo označení oprávněna... a opatřen kvalifikovaným časovým razítkem". Prokázání pravosti může být problematické, je tedy vhodné použít takové nástroje, které prokazatelnosti napomohou.

Platnost certifikátu, na kterém je založen uznávaný elektronický podpis, je 1 rok. Po uplynutí této doby, tj. po exspiraci certifikátu, není možné technicky stav podpisu ověřit. Jak tedy uložit elektronické dokumenty, aby bylo důvěryhodně prokazatelné, že dokument se nezměnil (je stále originálem), existoval v daném časovém okamžiku (je zafixován v čase) a byl podepsán podepisující osobou (a podepisující osoba nemůže tvrdit, že dokument nepodepsala)?

Řešením jsou produkty společnosti I.CA pokrývající krátkodobou (do 3 let), střednědobou (do 10 let) i dlouhodobou archivaci (nad 10 let).

Krátkodobá archivace

Při opatření elektronického dokumentu kvalifikovaným časovým razítkem, vydaným akreditovaným poskytovatelem certifikačních služeb, je dokument označen v čase. Každé časové razítko je vydavatelem podepsáno certifikátem serveru časové autority a protože platnost certifikátu je obvykle 3–5 let a po dvou letech dochází k obnově, je minimální doba, po kterou je časové razítko plně technicky ověřitelné, tři roky. Lze tedy konstatovat, že použití kvalifikovaného časového razítka prodlouží ověřitelnost archivovaného elektronického dokumentu o dva roky nad dobu platnosti certifikátu, tedy na období 3 let.

Střednědobá archivace

Jestliže vyjdeme z premisy, že platnost elektronického podpisu je neomezená, avšak platnost certifikátu, na kterém je podpis založen, činí 1 rok, a tuto dobu pro plnou technickou ověřitelnost lze prodloužit na 3 roky, lze řetězením časových razítek (RFC 4998) prodloužit dobu ověřitelnosti na 6, 9 i více let. Delší časové období však není možné ze strany akreditovaného poskytovatele certifikačních služeb garantovat, protože dochází ke slábnutí kryptografických algoritmů.

Průměrná doba elektronické archivace řetězení časových razítek dle doporučení I.CA činí 10 let. Protože obsah dokumentu, ke kterému je připojeno časové razítko, je věcí jeho původce, pracují produkty I.CA při řetězení razítek tak, že prvním razítkem se označuje hash dokumentu a druhým razítkem v řadě hash prvního razítka atd. I.CA nabízí řetězení razítek buď ve svých systémech bez jakýchkoli nároků na straně klienta (klient razítkuje a na vyžádání mu I.CA poskytne přerazítkované razítko, protokol o řetězení razítek, pseudo on-line službu na vyhledání přerazítkovaného razítka či kompletní strukturu pro soudního znalce) nebo jako klientskou aplikaci či knihovnu pro implementaci do prostředí klienta.

Dlouhodobá archivace

V oblasti archivace delší než 10 let spolupracuje I.CA se společností Telefónica O2 Czech Republic, a.s., a v rámci svého uceleného portfolia archivačních produktů nabízí O2 Důvěryhodný archiv, který poskytuje možnost dlouhodobého uchovávání dokumentů se zachováním validity.

Řešení je nezávislé na prostředí klienta, představuje samostatný modul, který komunikuje s ostatními systémy pomocí webových služeb. Z pohledu těchto systémů představuje zvláštní typ úložiště s funkčnostmi vkládání, čtení (získání), vyhledávání dokumentů a získání důkazu validity uloženého dokumentu.

Samo úložiště pak interními procesy zajišťuje periodické prodloužení validity na základě zvolené archivační politiky s využitím certifikátů a časových razítek I.CA. K dispozici jsou předdefinované šablony této politiky, pokrývající plně potřeby všech typů organizací.

Nejdůležitějším aspektem vývoje produktu bylo zabezpečení. Data v samotném úložišti jsou ukládána zabezpečeně, veškeré záznamy (logy) jsou elektronicky podepisovány a archivovány obdobným způsobem jako vlastní dokumenty. Originálním způsobem je řešeno řízení přístupu, které vylučuje jakoukoli neoprávněnou manipulaci s daty, každý požadavek či činnost jsou navíc zaznamenány a archivovány. Uložené dokumenty nelze přepisovat ani mazat, lze pouze uložit další verze. ■

Ing. Roman Kučera
obchodní ředitel segmentu veřejná správa
První certifikační autorita, a. s.

První certifikační autorita, a. s., vznikla v roce 2001. Hlavní náplní společnosti po celou dobu existence je zajišťování činností, bezprostředně souvisejících s poskytováním služeb certifikační autority. V březnu 2002 získala akreditaci v České republice a v únoru 2006 ve Slovenské republice. V současné době vydává cca 180.000 ks kvalifikovaných a komerčních certifikátů ročně a cca 3,3 mil. ks kvalifikovaných časových razítek měsíčně.