Problematika přechodu na SHA-2 algoritmy v elektronickém podpisu

Ministerstvo vnitra svým sdělením ze dne 17.10.2008 (http://www.mvcr.cz/clanek/zmena-v-kryptografickych-algoritmech-ktere-jsou-pouzivany-pro-vytvareni-elektronickeho-podpisu.aspx) stanoví akreditovaným certifikačním autoritám k 1.1.2010 vydávat kvalifikované certifikáty „podporující některý z algoritmů SHA-2“ a s minimální délkou RSA klíče 2048 bitů.

V praxi toto rozhodnutí znamená, že kvalifikované certifikáty vydané v ČR po uvedeném datu budou mít elektronický podpis vydávající certifikační autority učiněný s využitím HASH algoritmu (digitálního otisku) z rodiny SHA-2. Aby mohl být takový certifikát použit k vytvoření či ověření elektronického podpisu, musí aplikace respektive operační systém uživatele tyto nové algoritmy v rámci zpracování elektronického podpisu podporovat.

Dále je z důvodu roční platnosti kvalifikovaných certifikátů v ČR stanoveno roční přechodné období (do konce roku 2010), po které musí aplikace podporovat oba typy certifikátů – staré s SHA-1 i nové s SHA-2:

- aplikace, ve kterých je elektronický podpis používán, musí podporovat nejpozději od 1. 1. 2010 všechny algoritmy třídy SHA-2,
- podpora algoritmu SHA-1 musí být v aplikacích zachována minimálně do 31.12.2010.

Ministerstvo vnitra je tuto změnu oprávněno vyhlásit na základě vyhlášky č. 378/2006 Sb. pouze v oblasti elektronického podpisu jen vůči akreditovaným poskytovatelům certifikačních služeb. Zároveň však důrazně doporučuje zvážit rizika dalšího používání SHA-1 dalším odpovědným osobám – uživatelům zaručeného elektronického podpisu.

Dále je třeba zdůraznit, že technické parametry elektronického podpisu certifikační autority na daném certifikátu nemají přímou souvislost s technickými parametry elektronických podpisů, které jsou s využitím odpovídajícího privátního klíče učiněny respektive s využitím veřejného klíče z certifikátu ověřovány. Tedy – s „novým certifikátem“ založeným na SHA-2 lze činit/ověřovat elektronické podpisy (elektronických dokumentů) využívajících stále SHA-1 a naopak.

Celní správa v souladu s uvedeným sdělením bude postupovat následujícím způsobem:

- Na všech svých technických prostředcích a ve všech aplikacích, které pracují s elektronickým podpisem, zajistí k 1.1.2010 podporu zpracování kvalifikovaných certifikátů vydaných po tomto datu a využívajících HASH z rodiny SHA-2. Zároveň po dobu stanoveného ročního přechodného období bude zpracovávat i platné kvalifikované certifikáty vydané před 1.1.2010 využívající algoritmus SHA-1.

Celní správa dále, jako správce a provozovatel tzv. externí domény Elektronického celního řízení, využije rok 2010 jako přechodné období pro změny v elektronických podpisech dokumentů v externí doméně:

- Bude označovat odchozí zprávy svojí zaručenou elektronickou značkou s využitím původního certifikátu s SHA-1 do června 2010. 22.6.2010 končí platnost stávajícího certifikátu a tak v průběhu měsíce června dojde k přechodu na certifikát nový, který již bude obsahovat SHA-2.
- Pro ECRObálku verze 1.x (využívající formát S/MIME) neplánuje k 1.1.2010 žádné změny, tedy zachová elektronický podpis využívající HASH SHA-1. V průběhu roku 2010 dojde k posouzení možnosti přechodu na HASH SHA-2 podle stavu podpory SHA-2/RSA a S/MIME v prostředí OS

Microsoft starších verzí (Windows XP a Windows 2003 Server) či k migraci komunikačních domén z ECRObalky 1.x na 2.0.

- Pro ECRObalku verze 2.0 využívající XML-Signature bude krátce po 1.1.2010 nasazena nová verze vstupní brány, která bude na příjmu akceptovat elektronické podpisy zpráv s využitím SHA-1 i SHA-2. Odchozí zprávy (směrem k deklarantům) budou stále používat SHA-1. Přechod na SHA-2 u odchozích zpráv nenastane dříve než v červnu 2010 v souvislosti s novým serverovým certifikátem pro zaručenou elektronickou značku a přechodem na RSA klíč dlouhý 2048 bitů.
- Výrobci deklarantského SW mohou testovat nový formát podpisu využívající SHA-2 vůči testovacímu prostředí ECR brány.

Všechny změny v externí doméně vzhledem k SHA-2 budou jako obvykle konzultovány s dostatečným předstihem na smíšených pracovních skupinách s deklaranty a výrobci deklarantského SW a budou zveřejněny na internetu celní správy.

Celní správa jako správce a provozovatel elektronické komunikace v režimu přepravy zboží podmínečně osvobozeného od platby SPD (systém EMCS):

- začne používat zaručený elektronický podpis v deklarantském modulu EMCS k 1.4.2010. Tento deklarantský modul je provozován jako webová SilverLight aplikace pro všechny deklaranty s výjimkou jednoho případu. Od 1.4.2010 bude rovnou využívat podpisy s SHA-2.

Celní správa jako správce a provozovatel elektronické komunikace pro podání daňových přiznání k SPD:

- Provozuje pro daňové subjekty webovou aplikaci umožňující vyplnění a podání eDAP.
- Podepisovací modul této aplikace bude během roku 2010 nahrazen novou verzí, která v podpisech přejde na SHA-2. O změně bude celní správa v předstihu informovat.

Závěrem bychom rádi upozornili všechny uživatele aplikací využívajících (zaručený) elektronický podpis na platformě Windows na zásadní článek o podpoře SHA-2 na této platformě od Roberta Hernadyho z českého zastoupení Microsoftu, který vyšel na serveru LUPA.CZ (http://www.lupa.cz/clanky/zavedeni-hash-algoritmu-sha-2-v-prostredi-ms-win/).

V Praze dne 22.12.2009 Jan Forejt, odd. 122 GŘC