Změna v kryptografických algoritmech, které jsou používány pro vytváření elektronického podpisu

Na základě aktuálních poznatků v oblasti kryptografie a dokumentu ETSI TS 102 176-1 V2.0.0 (ALGO Paper) Ministerstvo vnitra stanoví:

Kvalifikovaní poskytovatelé certifikačních služeb ukončí vydávání kvalifikovaných certifikátů s algoritmem SHA-1 do 31. 12. 2009. Od 1. 1. 2010 budou tito poskytovatelé vydávat kvalifikované certifikáty podporující některý z algoritmů SHA-2.

Zároveň je od uvedeného data stanovena minimální přípustná délka kryptografického klíče pro algoritmus RSA na 2048 bitů.

Komentář ke změně v kryptografických algoritmech, které jsou používány pro vytváření elektronického podpisu

Ministerstvo vnitra podle vyhlášky č. 378/2006 Sb., o postupech kvalifikovaných poskytovatelů certifikačních služeb, zveřejňuje kryptografické algoritmy a jejich parametry, které mohou být použity pro elektronický podpis ve smyslu zákona č. 227/2000 Sb., o elektronickém podpisu. Ministerstvo vnitra při stanovení zveřejňovaných algoritmů a jejich parametrů vychází jednak z dokumentů vydaných z iniciativy Evropské komise organizacemi, které k tomu EK určila (tzv. ALGO paper zveřejňovaný ETSI), a dále z aktuálního vývoje v oblasti bezpečnosti kryptografických algoritmů. V úvahu bere zároveň stanoviska významných mimoevropských institucí (např. NIST v USA) a českého Národního bezpečnostního úřadu (viz sdělení tohoto úřadu publikované na jeho webových stránkách).

V návaznosti na směrnici ES č. 1999/93/EC o zásadách Společenství pro elektronické podpisy a v ní obsažený princip vzájemného uznávání kvalifikovaných certifikátů vydaných v kterémkoliv členském státu EU je nezbytné vycházet z dokumentu ALGO paper, který stanoví, že od 1. 1. 2010 je algoritmus SHA-1 „unusable“ a je tedy nezbytné ukončit jeho používání pro oblast elektronického podpisu a zahájit přechod na bezpečnější algoritmy třídy SHA-2. Česká republika patří k těm členským státům, ve kterých je tento přechod rozložen do delšího časového období. Je však nezbytné jej realizovat, a tak zachovat důvěru uživatelů v bezpečnost elektronického podpisu.

V případě SHA-2 se jedná o tzv. rodinu čtyř hashovacích funkcí (SHA-224, SHA-256, SHA-384 a SHA-512), které jsou součástí standardu FIPS PUB 180-2 a u kterých dosud nebyly nalezeny bezpečnostní slabiny.

Je nesporné, že tento přechod bude náročný nejen pro poskytovatele certifikačních služeb, kteří vydávají kvalifikované certifikáty, ale i pro tvůrce a provozovatele aplikací, ve kterých je elektronický podpis využíván. V praxi tato změna znamená, že

- poskytovatelé certifikačních služeb přestanou vydávat kvalifikované certifikáty s algoritmem SHA-1 nejpozději do 31. 12. 2009,
- poskytovatelé certifikačních služeb zahájí vydávání kvalifikovaných certifikátů s hashovací funkcí třídy SHA-2 nejpozději 1. 1. 2010 (mohou tak však učinit kdykoliv dříve); tato změna se samozřejmě týká i vydávání kořenových certifikátů, kterými poskytovatel certifikačních služeb označuje jím vydané certifikáty,
- 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.

Obecně lze konstatovat, že se nejedná o nepředvídatelnou změnu. Naopak tato problematika je již několik let diskutována a byla publikována řada odborných článků a studií. Kryptografické algoritmy stejně jako jiné prvky související s informační bezpečností nejsou schopné v delším časovém horizontu odolat nejrůznějším útokům a nelze na ně plně spoléhat. Pokud jde konkrétně o algoritmy, prolomen byl dříve oblíbený algoritmus MD5 (již od roku 2004 je veřejně znám postup pro nalezení kolizního páru zpráv – tj. dvou různých zpráv se stejným hashem). Necelý rok poté byl pro SHA-1 zveřejněn objev algoritmu, který umožňuje nalézt kolizi podstatně rychleji než hrubou silou. Výpočetní náročnost s ohledem na současnou techniku je sice předmětem diskusí mezi odborníky, použití tohoto algoritmu pro elektronický podpis však nelze považovat za bezproblémové (nelze například vyloučit, že i pro tento algoritmus bude nalezen způsob generování kolizních zpráv).

Ministerstvo vnitra konzultuje uvedené změny s poskytovateli certifikačních služeb, kteří vydávají kvalifikované certifikáty (tj. Česká pošta s.p., eIdentity a.s., První certifikační autorita a.s.). Ti ve svých plánech rozvoje s přechodem na nové algoritmy počítají. Tvůrcům aplikací lze doporučit, aby případně úpravy s poskytovateli podle potřeby konzultovali.

Ministerstvo vnitra je oprávněno tuto změnu vyhlásit pouze pro oblast elektronického podpisu, avšak i pro jiné oblasti využití důrazně doporučuje, aby odpovědné osoby zvážily rizika spojená s dalším používáním hashovací funkce SHA-1.

Publikováno dne 17. 10. 2008

Aktualizováno dne 23. 6. 2009
Zdroj: http://www.mvcr.cz/clanek/zmena-v-kryptografickych-algoritmech-ktere-jsou-pouzivany-pro-vytvareni-elektronickeho-podpisu.aspx