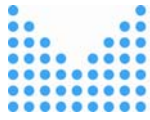


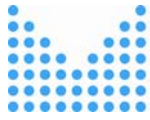


Informace k přechodu k bezpečnějším kryptografickým algoritmům v oblasti elektronického podpisu



Obsah

Úvod	3
1 Východisko	3
2 Zákon o elektronickém podpisu	3
3 Bezpečnost hashovacích funkcí.....	4
4 Subjekty, kterých se změna týká	5
5 Oblasti, kterých se změna týká.....	5
6 Národní bezpečnostní úřad a hashovací funkce.....	6
7 Situace v zahraničí.....	6
7.1 Německo	6
7.2 Slovensko	7
7.3 Spojené státy americké, NIST	7
8 Související problematika	7
8.1 Uznávání kvalifikovaných certifikátů v rámci EU	7
8.2 Produkty firmy Microsoft	7
8.3 Časová razítka.....	8
9 Opatření, která by měl přijmout každý orgán veřejné moci	8
10 Literatura.....	9
Příloha	10
Technické parametry související s implementací certifikátů SHA-2 v komerčně dostupných produktech společnosti Microsoft	10
11 Změny.....	11
11.1 Změny oproti předchozí verzi	11
11.2 Změnové řízení.....	11



Úvod

Kryptografické algoritmy, které mohou být používány v oblasti elektronického podpisu, musí respektovat neustálý rozvoj v oblasti kryptoanalýzy a výpočetních technologií. Z toho důvodu ustupuje Česká republika stejně jako ostatní členské státy EU od používání dosud využívaného algoritmu SHA-1. Tato změna se netýká pouze algoritmů používaných při vydávání kvalifikovaných certifikátů ale i algoritmů pro vytváření elektronického podpisu. Dotkne se tak nejen poskytovatelů certifikačních služeb vydávajících kvalifikované certifikáty, ale všech osob využívajících elektronický podpis. Tento dokument shrnuje problematiku a popisuje opatření, která by měl přijmout každý orgán veřejné moci, aby byl na tuto změnu připraven.

1 Východisko

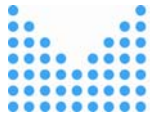
Ministerstvo vnitra vykonává gesci k problematice elektronického podpisu, a to na základě § 12 odst. 1 písm. n) zákona č. 2/1969 Sb., o zřízení ministerstev a jiných ústředních orgánů státní správy České republiky, ve znění pozdějších předpisů.

Ministerstvo vnitra (dále jen „ministerstvo“) odpovídá za celou řadu projektů elektronizace veřejné správy, které jsou průřezového charakteru a u nichž je nezbytné zajistit adekvátní úroveň bezpečnosti. Důvěra v elektronický podpis je závislá především na používání kryptografických algoritmů, které jsou v mezinárodním kontextu v dané době považovány za bezpečné pro daný účel, přičemž nehrozí bezprostřední nebezpečí jejich tzv. prolomení.

2 Zákon o elektronickém podpisu

Zákon č. 227/2000 Sb., o elektronickém podpisu o změně některých dalších zákonů, ve znění pozdějších právních předpisů (dále jen „zákon o elektronickém podpisu“) zmocňuje ministerstvo k vydání vyhlášky stanovující mimo jiné požadavky na bezpečné systémy a bezpečné nástroje používané poskytovateli certifikačních služeb. Na základě předmětné vyhlášky ministerstvo zveřejňuje na úřední desce kryptografické algoritmy a jejich parametry, které mohou použít poskyvatelé certifikačních služeb v rámci služby vydávání kvalifikovaných certifikátů nebo kvalifikovaných systémových certifikátů.

Zákon o elektronickém podpisu a ani jiný právní předpis nestanoví povinnost ministerstva definovat náležitosti používání kryptografických algoritmů a jejich parametrů jiným subjektům, než jakými jsou poskyvatelé kvalifikovaných certifikačních služeb ve smyslu zákona o elektronickém podpisu, nebo v jiných oblastech, než je oblast elektronického podpisu (například pro autentizaci či šifrování). Jednotná úprava by navíc nebyla vhodná, neboť nároky na kryptografické algoritmy nemusí být nutně stejné pro oblast elektronického podpisu a například pro autentizaci. Podle § 12 odst. 6 zákona č. 2/1969 Sb., o zřízení ministerstev a jiných ústředních orgánů státní správy České republiky, ve znění pozdějších předpisů, ministerstvo plní koordinační úlohu pro informační a komunikační technologie a v rámci naplňování stanovené role vydává tento dokument.



Zákonem o elektronickém podpisu je implementována směrnice Evropského parlamentu a Rady 1999/93/ES ze dne 13. prosince 1999 o zásadách Společenství pro elektronické podpisy (dále jen „Směrnice“). Pro praktickou část implementace Směrnice jsou orgánem k tomu Komisí určeným, tj. Evropským ústavem pro telekomunikační normy (European Telecommunications Standards Institute, ETSI) vydávány dokumenty typu „technical specification (TS)“. Jedním z nich je ETSI TS 102 176-1 V2.0.0 (dále jen „ALGO Paper“), který stanoví přípustné algoritmy a jejich parametry pro elektronické podpisy a kvalifikované certifikáty, které jsou vydávány v souladu se Směrnicí. Ministerstvo se při zveřejňování kryptografických algoritmů a jejich parametrů řídí tímto dokumentem. ALGO Paper stanoví pro jednotlivé algoritmy dobu, po kterou lze předpokládat, že budou považovány za bezpečné.

Tento text se primárně zabývá přechodem z hashovací funkce SHA-1 na SHA-2, protože v praxi bude tato změna působit nejméně obtížně. Součástí přechodu na silnější kryptografické funkce je ale i stanovení minimální přípustné délky klíče podpisového algoritmu RSA na 2048 bitů, které je nutné mít na paměti, přestože ve většině dnes využívaných aplikací nebude tato změna činit problémy a nebude vyžadovat žádný zásah uživatele.

3 Bezpečnost hashovacích funkcí

Kryptografické algoritmy jsou považovány za bezpečné pouze po dobu, po kterou lze jejich prostřednictvím zajistit požadovanou funkčnost. Hashovací funkce používaná při vytváření elektronického podpisu musí mít podle Algo Paperu následující tři vlastnosti:

- je-li znám hash zprávy, je obtížné z něj odvodit zprávu odpovídající tomuto hashi (pre-image resistance),
- je-li znám hash a zpráva, je obtížné najít jinou zprávu se stejným hashem (2nd pre-image resistance),
- je obtížné najít dvě zprávy, které mají stejný hash (collision resistance).

Nalezení teoretického postupu (metody) hledání kolizí nebo konkrétního příkladu kolizí degraduje bezpečnost použité hashovací funkce. Při existenci takového postupu by bylo možné, aby existoval stejný hash (a tedy stejný elektronický podpis) pro dvě zprávy s odlišným obsahem. Jakmile je tedy zveřejněn rychlý a efektivní postup hledání kolizí, má se za to, že hashovací funkce byla kryptograficky prolomena a není možné ji dále bezpečně používat.

S rozvojem kryptoanalytických metod a dostupností potřebné výpočetní techniky (síly) je nezbytné vzít na vědomí skutečnost, že u žádného algoritmu nelze předpokládat, jeho používání v horizontu desítek let. Například algoritmus MD5 (Message-Digest Algorithm) byl poprvé zpochybněn v roce 2004, prolomení algoritmu SHA-0 (Secure Hash Algorithm) bylo oznámeno v roce 2004, první indicie o prolomení algoritmu SHA-1 pocházejí z roku 2005. Nic nenasvědčuje tomu, že by se tento trend v blízké budoucnosti změnil a že nové a „silnější“ algoritmy by měly předpoklad výrazně delší doby životnosti. Předpokládá se, že hashovací funkce z rodiny SHA-2 budou bezpečné do roku 2015.

Přestože nebezpečí padělání podepsané zprávy jejím nahrazením jinou zprávou se stejným hashem je v běžné praxi ICT spíše teoretické, nelze jej vyloučit.



Je tedy nezbytné ukončit používání hashovací funkce třídy SHA-1 a nahradit ji hashovací funkcí třídy SHA-2. Poskytovatelé certifikačních služeb ukončili používání algoritmu SHA-1 při vydávání kvalifikovaných certifikátů k 31. 12. 2009. Pro vytváření elektronického podpisu je možné po přechodnou dobu nadále používat algoritmus SHA-1, nejdéle však do 31. 12. 2010.

4 Subjekty, kterých se změna týká

Hashovací funkce používané pro elektronický podpis se bezprostředně dotýkají zejména

- kvalifikovaných poskytovatelů certifikačních služeb při vydávání kvalifikovaných certifikátů a kvalifikovaných systémových certifikátů
- podepisujících osob při vytváření elektronického podpisu
- zaměstnavatelů, kteří dávají svým zaměstnancům k dispozici nástroje pro používání elektronického podpisu, resp. nakupují příslušné produkty
- tvůrců produktů (aplikací), ve kterých je elektronický podpis používán
- subjektů, které si tyto aplikace nechávají zhotovit
- poskytovatelů certifikačních služeb při vydávání kvalifikovaných časových razítek a „odběratelů“ kvalifikovaných časových razítek.

5 Oblasti, kterých se změna týká

Hashovací funkce jsou využívány rovněž při používání certifikátů, které nenesou označení „kvalifikované“ a zpravidla jsou označovány jako „komerční“ či „autentizační“. Na jejich vydávání se však zákon o elektronickém podpisu nevztahuje, resp. jejich vydávání neupravuje a ministerstvo tuto činnost žádným způsobem nereguluje. Je tedy na uvážení subjektů, které tyto certifikáty vydávají, zda příslušné změny realizují.

Jak je uvedeno výše v textu, používání hashovacích funkcí kvalifikovanými poskytovateli certifikačních služeb je regulováno ministerstvem. Kvalifikovaní poskytovatelé certifikačních služeb realizovali požadovanou změnu nejpozději k 1. lednu 2010. Zároveň ministerstvo vzalo na vědomí dohodu všech tří kvalifikovaných poskytovatelů certifikačních služeb, tj. České pošty s. p., První certifikační autorita a. s. a eIdentity a. s. spočívající v přednostním používání hashovací funkce SHA-256 v kombinaci s algoritmem RSA s délkou klíče 2048 bitů, přičemž každý z těchto tří poskytovatelů může na základě svého uvážení a na základě požadavků uživatelů přistoupit k vydávání certifikátů i s některou z dalších funkcí z „rodiny“ SHA-2, tj. SHA-224, SHA-384 nebo SHA-512.

Hashovací funkce však nejsou užívány pouze při vydávání certifikátu, ale rovněž při vytváření a ověřování elektronického podpisu. Zde je nutné zdůraznit, že ne všechny kombinace operačních systémů a podepisovacích aplikací jsou schopné v plné míře s novými hashovacími funkcemi pracovat. Dále v textu je popsána situace s produkty společnosti Microsoft, které jsou ve veřejné správě majoritně zastoupeny.



Je-li podepisující osoba zaměstnancem, je závislá na vybavení zajištěném zaměstnavatelem a je tedy na něm, aby vyhodnotil stávající softwarové vybavení každého pracoviště, kde bude třeba elektronické podpisy vytvářet nebo ověřovat, a případně zajistil přechod na adekvátní kombinaci operačního systému a podepisovací aplikace.

Podepisujícím osobám lze doporučit, aby využívaly komunikace prostřednictvím informačního systému datových schránek. Pokud se nejedná o úkon orgánu veřejné moci, pak datové zprávy zasílané prostřednictvím tohoto informačního systému nemusí být elektronicky podepsány. Je-li však činěn úkon orgánem veřejné moci a vyžaduje-li to zvláštní právní předpis (správní řád či jiný procesní předpis), musí být dokument elektronicky podepsán a je tedy na orgánu veřejné moci, aby zaměstnance, které k podpisu oprávnil, vybavil odpovídajícím aplikačním vybavením.

Tvůrci aplikací jsou zpravidla s trendy v oblasti kryptografie dobře obeznámeni. Pokud v případě vytváření nových aplikací nebo při úpravách již provozovaných aplikací sami na příslušné změny v kryptografických algoritmech neupozorní, je na objednateli, aby je v rámci zakázky požadoval.

6 Národní bezpečnostní úřad a hashovací funkce

Orgánem veřejné moci, který se zabývá kryptografickou bezpečností, je Národní bezpečnostní úřad. Přestože se působnost tohoto úřadu vztahuje na oblast utajovaných informací, v oblasti kryptografických algoritmů má jeho názor, publikovaný v roce 2006 na jeho webových stránkách, obecnou platnost:

„Vzhledem k tomu, že dochází k prudkému vývoji v oblasti kryptoanalýzy hashovacích funkcí (nalezení kolizí u některých hashovacích funkcí) a tyto funkce se používají v řadě bezpečnostních aplikací (např. elektronický podpis, atd.) a také v mnoha kryptografických prostředcích vydává NBÚ následující prohlášení:

1. Doporučuje se nadále nepoužívat hashovací funkce s výstupem menším než 160 bitů (např. hashovací funkce MD4, MD5, RIPEMD, HAVAL-128 atd.).
2. Doporučuje se neprodleně zahájit přípravu k přechodu od hashovací funkce SHA-1 na novou generaci hashovacích funkcí třídy SHA-2 (SHA-224, SHA-256, SHA-384 a SHA-512).
3. Doporučuje se prozkoumat všechny bezpečnostní aplikace i kryptografické prostředky, ve kterých se využívá hashovacích funkcí a odborně posoudit vliv nejnovějších kryptoanalytických útoků na jejich bezpečnost.“

7 Situace v zahraničí

7.1 Německo

Jak již bylo zmíněno, přechod od hashovací funkce SHA-1 k SHA-2 se netýká pouze České republiky. V celosvětovém měřítku však není dosaženo dohody na jednom termínu této změny, konec roku 2010 je však považován za maximální hranici použitelnosti SHA-1.



Německo, ve kterém jsou tradičně velmi vysoké nároky na bezpečnost, zahájilo přechod od SHA-1 k SHA-2 jako jeden z prvních evropských států: použití SHA-1 bylo v oblasti elektronického podpisu přípustné do 30. června 2008, s výjimkou použití algoritmů k vytváření kvalifikovaných certifikátů poskytovateli certifikačních služeb, které bylo povoleno do konce r. 2009, tj. u poskytovatelů bylo postupováno stejně jako v České republice.

7.2 Slovensko

Rovněž Slovensko přistoupilo k nezbytným změnám. Národní bezpečnostní úřad stanovil příslušnou vyhláškou, že certifikované produkty využívající hashovací funkci SHA-1 bylo možné používat nejdéle do konce roku 2009 a obecně odkazuje na mezinárodní standardizační dokument ALGO Paper.

7.3 Spojené státy americké, NIST

Situace ve Spojených státech amerických je pro Českou republiku zajímavá ze dvou aspektů – sídlí zde jednak Americký federální úřad pro standardy a technologie (NIST), který je nespornou autoritou v oblasti kryptografie, a své sídlo zde má rovněž firma Microsoft, která doporučení NIST akceptuje. NIST již v roce 2004 vydal prohlášení, ve kterém doporučil používat třídu funkcí SHA-2 a ukončit používání SHA-1 v roce 2010. V roce 2006 NIST publikoval následující, dosud platný pokyn:

„Federální úřady by měly přestat používat SHA-1 pro digitální podpisy, digitální časová razítka a jiné aplikace, které vyžadují kolizní odolnost, jakmile to bude možné, a po roce 2010 musí přejít na skupinu hashovacích funkcí SHA-2. Po roce 2010 mohou federální úřady používat SHA-1 pouze pro následující aplikace: kódy na autentizaci zpráv pomocí hashování (Hash-based Message Authentication Codes, HMAC), funkce na odvozování klíčů (key derivation functions, KDF) a generátory náhodných čísel (Random Number Generators, RNG). Bez ohledu na typ použití NIST doporučuje při vývoji nových aplikací a protokolů využívat hashovací funkce SHA-2.“

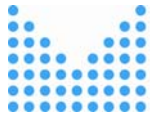
8 Související problematika

8.1 Uznávání kvalifikovaných certifikátů v rámci EU

Požadavek na přechod k algoritmu SHA-2 souvisí rovněž s povinností uznávat kvalifikované certifikáty v rámci EU bez ohledu na stát, ve kterém byly vydány. Pokud by byl elektronický podpis založený na kvalifikovaném certifikátu vytvořen pomocí hashovací funkce SHA-1, lze předpokládat, že by nemusel být akceptován. Pro přeshraniční komunikaci lze doporučit používat při vytváření elektronického podpisu hashovací funkci SHA-2.

8.2 Produkty firmy Microsoft

Ve veřejné správě jsou ve velké míře využívány produkty firmy Microsoft. Pro plné aktivní využívání SHA-2, tj. nejen pro ověřování ale rovněž pro vytváření elektronických podpisů je



nutné v případě podepisování v aplikaci, která využívá pro výpočet hashe zprávy služeb operačního systému, provozovat tyto aplikace na odpovídající verzi operačního systému. Technické parametry související s implementací SHA-2 v komerčně dostupných produktech společnosti Microsoft jsou uvedeny v příloze. Ministerstvo tuto informaci zveřejnilo 29. 6. 2009 na svých webových stránkách.

8.3 Časová razítka

Používání SHA-2 se doporučuje rovněž při vydávání kvalifikovaných časových razítek. Odběratelům časových razítek se doporučuje, aby se řídili pokyny poskytovatelů certifikačních služeb, kteří je vydávají. Rovněž pro elektronické značky, které jsou z technologického hlediska digitálním (elektronickým) podpisem, se doporučuje používání SHA-2.

9 Opatření, která by měl přijmout každý orgán veřejné moci

Pro přechod k silnějším algoritmům je žádoucí, aby každý orgán veřejné moci provedl u provozovaných informačních systémů a aplikací analýzu dopadu tohoto přechodu a zpracoval plán jeho realizace. Postup, kterým bude přechod k silnějším algoritmům realizován, je vhodné vydat jako interní akt řízení.

1. Specifikovat informační systémy a aplikace, které je třeba přizpůsobit k provozování s využitím doporučených silnějších algoritmů.
2. Určit, na kolika pracovních stanicích je nezbytné provést změnu programového vybavení pro používání nových aplikací a informačních systémů se silnějšími algoritmy a posoudit, v čem tato změna spočívá; k tomu je žádoucí
 - a) určit počet zaměstnanců, kteří pracují s aplikacemi, ve kterých je nutné činit úkony s elektronickým podepisováním; posoudit, zda podpis s využitím SHA-2 umožní používané aplikace, nebo zda je nutné provést změnu na pracovní stanici
 - b) určit počet zaměstnanců, kteří ověřují platnost elektronického podpisu, ale neprovádějí elektronické podepisování dat; posoudit, zda umožní ověření podpisu aplikace, nebo zda je nutné provést změnu na pracovní stanici
 - c) určit počet zaměstnanců, kteří zajišťují činnosti podle písmene a) ve styku s jinými členskými státy EU, případně se třetími státy.
3. Určit, zda je orgán veřejné moci správcem informačních systémů veřejné správy nebo provozních informačních systémů, ve kterých je používán zaručený elektronický podpis založený na kvalifikovaném certifikátu, a pokud ano, stanovit postup provedení příslušných změn, a to buď vlastními silami nebo dodavatelským způsobem. Ověřit, zda v aplikacích, jichž je orgán veřejné správy správcem, není zaručený elektronický podpis založený na kvalifikovaných certifikátech používán v rozporu s jeho určením. Pro autentizaci využívat výhradně komerční certifikáty, u nichž není přechod k silnějším algoritmům nezbytný.



4. Dotazem u dodavatele zjistit, zda elektronická spisová služba (příp. další informační systémy) používaná orgánem veřejné moci umožňuje přechod k silnějším algoritmům, vyžádat pokyny k nastavení, případně příslušné úpravy požadovat.
5. Dotazem u dodavatelů operačních systémů a základních kancelářských programů zjistit, zda používané operační systémy a základní kancelářské programy umožňují používání silnějších algoritmů. Pokud tomu tak není, je nutno na určený počet pracovních stanic opatřit potřebné licence. V případě, že nainstalovaný software byl zakoupen ad hoc, je nutno zakoupit nový software. V případě, že orgán veřejné moci využívá licenční programy typu Microsoft SELECT a Microsoft Enterprise Agreement, využije možností daných těmito programy pro upgrade licencí. Orgány veřejné moci, které přistoupily k centrálnímu zadávání nákupu licencí Microsoft, mohou využít služeb Clearingového centra.
6. Zajistit, aby specifikace pro nově vytvářené aplikace, ve kterých má být používán elektronický podpis, obsahovaly požadavek na použití silnějších algoritmů (např. při zadávání veřejných zakázek).

10 Literatura

1. Zákon č. 227/2000 Sb., o elektronickém podpisu a o změně některých dalších zákonů (zákon o elektronickém podpisu), ve znění pozdějších předpisů.
2. Vyhláška č. 378/2006 Sb., o postupech kvalifikovaných poskytovatelů certifikačních služeb, o požadavcích na nástroje elektronického podpisu a o požadavcích na ochranu dat pro vytváření elektronických značek (vyhláška o postupech kvalifikovaných poskytovatelů certifikačních služeb).
3. Směrnice Evropského parlamentu a Rady č. 1999/93/ES o zásadách Společenství pro elektronické podpisy.
4. ETSI TS 102 176-1 V2.0.0 (2007-11) Electronic Signatures and Infrastructures (ESI); Algorithms and Parameters for Secure Electronic Signatures; Part 1: Hash functions and asymmetric algorithms.

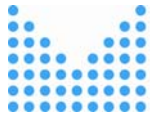
Dostupné z

http://webapp.etsi.org/action/PU/20071120/ts_10217601v020000p.pdf [cit. 2010-01-15]

5. Vyhláška č. 135/2009 Z. z. Národního bezpečnostního úřadu o formáte a způsobu vyhotovení zaručeného elektronického podpisu, způsobu zveřejnění veřejného klíče úřadu, podmínkách platnosti pre zaručený elektronický podpis, postupe při overování a podmínkách overování zaručeného elektronického podpisu, formáte časové pečiatky a způsobu jej vyhotovení, požiadavkách na zdroj časových údajov a požiadavkách na vedenie dokumentácie časových pečiatok (o vyhotovení a overování elektronického podpisu a časovej pečiatky).

Dostupné

z <http://www.zbierka.sk/Default.aspx?sid=15&PredpisID=208925&FileName=zz2009-00135-0208925&Rocnik=2009&AspxAutoDetectCookieSupport=1> [cit. 2010-01-15]



6. Secure Hashing. Approved Algorithms. Oficiální webové stránky NIST.
Dostupné z
http://csrc.nist.gov/groups/ST/toolkit/secure_hashing.html#Approved%20Algorithms
[cit. 2010-01-15]
7. Prohlášení Národního bezpečnostního úřadu k využívání hashovacích funkcí.
Dostupné z
<http://www.nbu.cz/cs/ochrana-utajovanych-informaci/kryptograficka-ochrana/informace/>
[cit. 2010-01-15]
8. Technické parametry související s implementací certifikátů SHA-2 v komerčně dostupných produktech společnosti Microsoft.
Dostupné z
<http://www.mvcr.cz/clanek/stanovisko-microsoft-ceska-republika-k-podpore-silnejsi-kryptografie.aspx>. [cit. 2010-01-15]
9. Nařízení vlády č. 495/2004 Sb., kterým se provádí zákon č. 227/2000 Sb., o elektronickém podpisu a o změně některých dalších zákonů (zákon o elektronickém podpisu), ve znění pozdějších předpisů.
10. KLÍMA, Vlastimil. Co se stalo s hašovacími funkcemi? Cryptoworld. Informační sešit GCUCMP. Ročník 7, číslo 4/2005.
Dostupné z
http://crypto-world.info/klima/2005/crypto_world_2005_03_08_10.pdf
[cit. 2010-01-15]
11. Notification in Accordance with the Electronic Signatures Act and the Electronic Signatures Ordinance (Overview of Suitable Algorithms).
Dostupné z
<http://www.bundesnetzagentur.de/media/archive/13617.pdf> [cit. 2010-01-15]

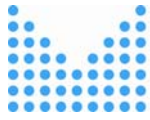
Příloha

Technické parametry související s implementací certifikátů SHA-2 v komerčně dostupných produktech společnosti Microsoft

Validace (ověření) certifikátů SHA-2 je podporováno v následujících produktech:

- Windows XP Service Pack 3
- Windows Vista
- Windows Server 2008 SP1
- Windows Server 2003 SP2 + speciální hotfix

Pod pojmem validace certifikátu rozumíme možnost ověřit podepsaný certifikát či řetězec certifikátů, které jsou například použity v rámci https relace.



Validace v žádném případě neznamená, že zcela všechny SHA-2 algoritmy jsou zároveň implementovány v rámci Secure-MIME (SMIME), nebo že mohou být využity aplikacemi, které používají Crypto-API (CAPI).

V rámci Windows XP SP3 je implementována podpora SHA-2 hashovacích algoritmů (SHA256, SHA384 a SHA512) pro validaci X.509 certifikátů. Implementace je provedena v rámci kryptografické knihovny rsaenh.dll.

Implementace SHA-2 algoritmů v rámci Windows XP SP3 slouží pouze k validaci certifikátu.

Považujeme za nutné zdůraznit fakt, že validace certifikátu není v žádném případě hashování, podepisování, kódování nebo dekódování binárních dat, v tomto případě za využití CAPI 2.0 (SHA-2 rodina, AES).

Komplexní implementace CAPI 2.0, umožňující plné použití algoritmů SHA-2, je součástí produktů:

- Windows Vista
- Windows Serveru 2008 SP1

Z tohoto důvodu je nutné pro plné aktivní používání (hashování, podepisování, kódování nebo dekódování binárních dat) SHA-2 pro SMIME provést upgrade operačního systému na prodávaný os Windows Vista nebo později na Windows 7.

Vytváření certifikátů s podporou těchto funkcí je podporováno na již volně dostupném serverovém operačním systému:

- Windows Server 2008 SP1 (Active Directory Certificate Services)

Stále velice často využívaný serverový operační systém Windows Server 2003 neobsahuje plnou implementaci CAPI2.0 a proto Certifikační autorita vybudována na této platformě algoritmy SHA-2 nepodporuje a podporovat nebude.

11 Změny

11.1 Změny oproti předchozí verzi

Verze 1.00 – První verze dokumentu.

11.2 Změnové řízení

Status	Datum	Popis	Garant	Schválil
Verze 1.00	27.1.2010	První verze	Odbor koncepce a koordinace ICT ve VS	Ředitelka odboru