Přechod na nové hash algoritmy rodiny SHA-2

Robert Hernady, Regional Solution Architect, Microsoft

Microsoft | Services

Agenda prezentace

- Seznámení s problematikou
  - Principy elektronického podpisu
  - Certifikáty
  - Co je třeba změnit pro využití algoritmů SHA-2
  - Shrnutí nutných podmínek pro podporu algoritmů SHA-2

- Zodpovězení základních otázek
  - Je nutný upgrade z Windows XP na novější verzi operačního systému?
  - Je nutný upgrade z Windows Serveru 2003 na novější verzi operačního systému?
  - Bude problém zavedení algoritmů SHA-2 vyřešen v případě upgrade na novější operační systém?
  - Jaké jsou dopady na provozované aplikace z rodiny produktů Office společnosti Microsoft?
  - Jaké jsou dopady na provozované aplikace dodávané třetími stranami (např. spisová služba)?

Proč přechod na SHA-2?

U algoritmu SHA-1 byly nalezeny bezpečnostní slabiny, které umožňují vyhledávání kolizí jinak než hrubou silou.

Vzhledem k výpočetní náročnosti není v současné době tento útok plně realizovatelný, algoritmus již však není považován za bezpečný.

Z tohoto důvodu je třeba přejít na algoritmy, u kterých dosud nebyly nalezeny bezpečnostní slabiny.

Ministerstvo vnitra ČR „vyhláškou"/oznámením předepsalo používání algoritmu SHA-2 v oblasti elektronického podpisu od 1. 1. 2010.

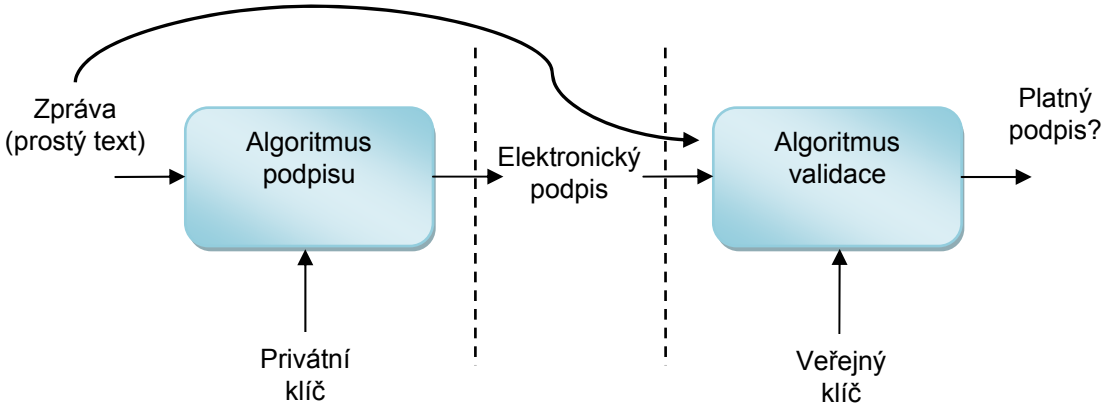
Zároveň je od uvedeného data stanovena minimální přípustná délka kryptografického klíče pro algoritmus RSA na 2048 bitů.

http://www.mvcr.cz/clanek/zmena-v-kryptografickych-algoritmech-ktere-jsou-pouzivany-pro-vytvareni-elektronickeho-podpisu.aspx

Principy elektronického podpisu

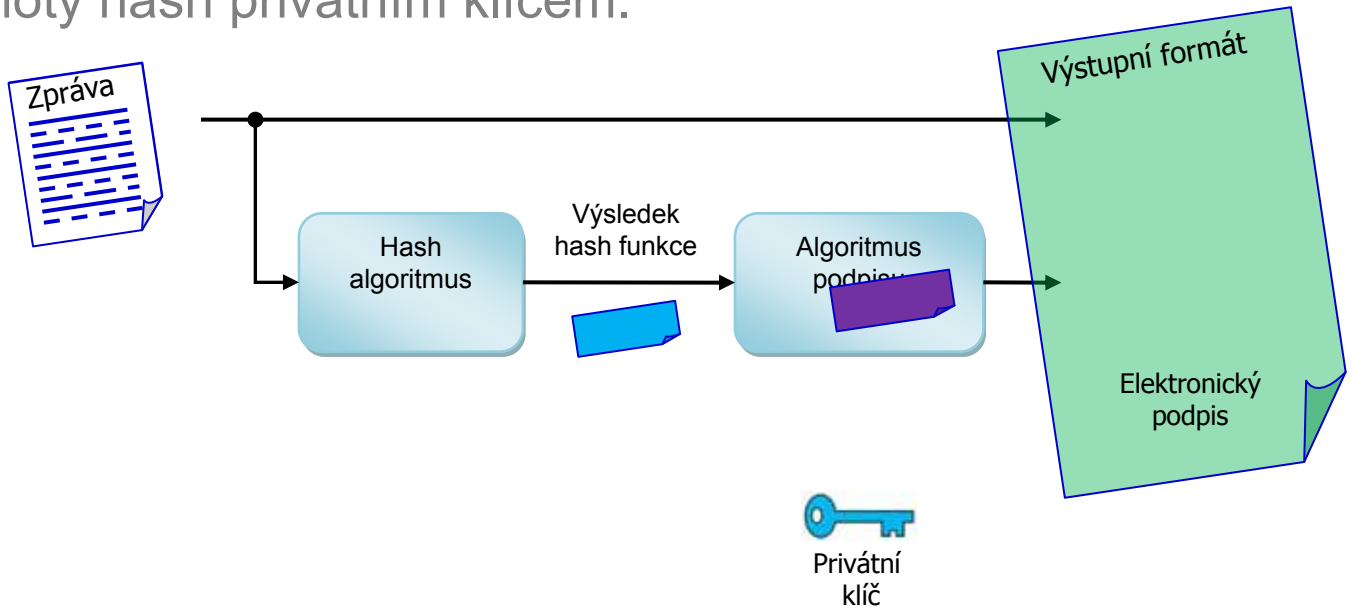
Elektronický podpis reprezentuje malý objem dat, která jsou zašifrována privátním klíčem odesílatele.

Při rozšifrovaní dat se použije veřejný klíč odesílatele, který zaručí, že data byla zašifrována odesílatelem popř. někým, kdo má přístup k privátnímu klíči odesílatele.



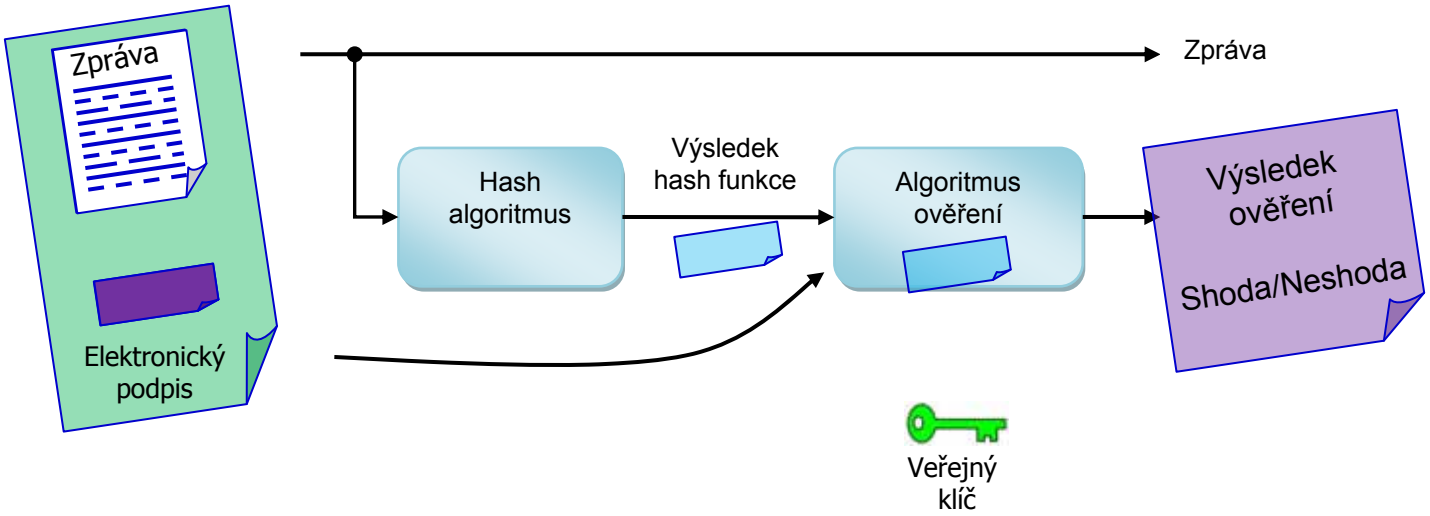
Vytváření elektronického podpisu

V průběhu vytváření elektronického podpisu vstupují do hry dva základní kroky. V prvním kroku je z vlastní zprávy vytvářena hodnota funkce hash (známá také jako *message digest*). Tato výsledná hodnota je následně v dalším kroku podepsána s využitím privátního klíče odesílatele. Proces podepsání ve skutečnosti znamená zašifrování hodnoty hash privátním klíčem.



Kontrola elektronického podpisu

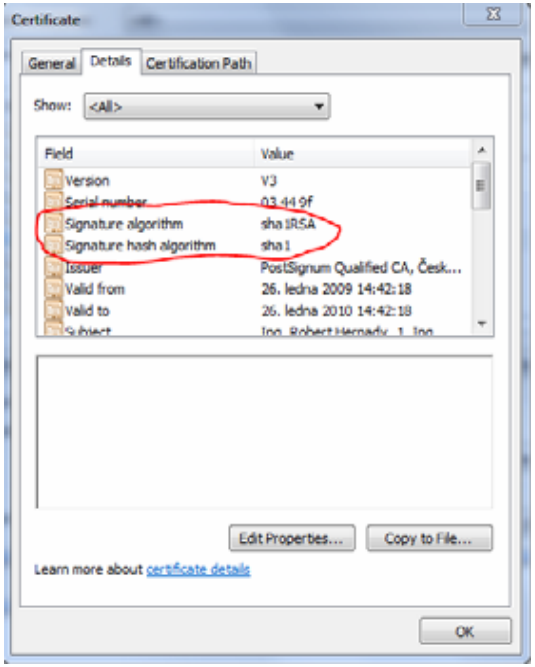
Pro vlastní kontrolu podpisu je nezbytné mít k dispozici vlastní zprávu a elektronický podpis. Za prvé se ze zprávy vytvoří hodnota funkce hash stejným postupem jaký byl použit při vytváření elektronického podpisu. Veřejným klíčem odesílatele se rozšifruje hodnota funkce hash v elektronickém podpisu (ta byla vytvořena při podepisování).
V případě, že se první hodnota funkce hash shoduje s rozšifrovanou hodnotou je **prokázáno**, že zpráva je ta, kterou odesílatel podepsal a že nebyla změněna.



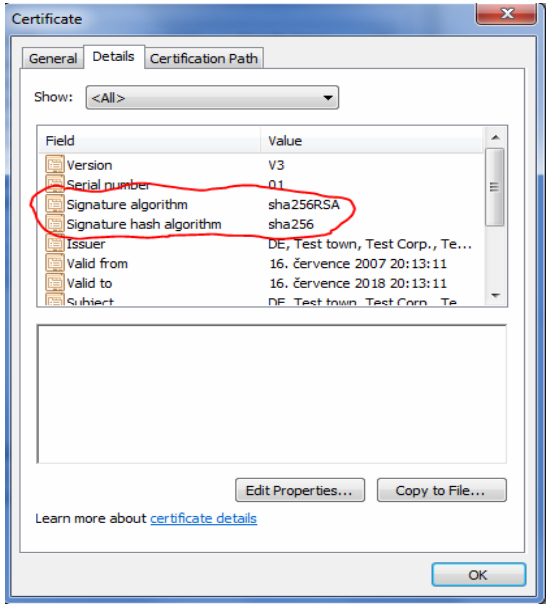
Certifikáty

Jednou základních funkcí certifikátu je mimo jiné zajistit distribuci veřejného klíče odesílatele a ověření platnosti tohoto veřejného klíče. Certifikát je vlastně zpráva, která je podepsána certifikační autoritou.

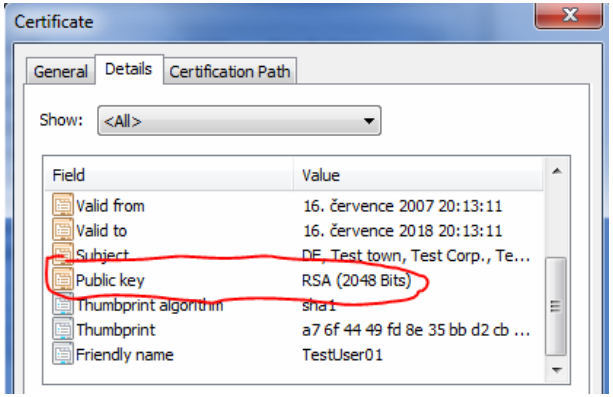
Certifikát, který je podepsán za pomocí algoritmu SHA-1



Vyhláška MV zavádí vydávání certifikátů, které budou podepsány s využitím hash algoritmu z rodiny SHA-2.



Vyhláška dále předepisuje minimální přípustnou délku klíče nastavenou na hodnotu 2048 bitů



Základní přehled podmínek pro práci s SHA-2

- Operační systém musí být schopen ověřit platnost certifikátu podepsaného s využitím algoritmu SHA-2
- *Cryptographic Service Provider* musí podporovat podepisování výsledné hodnoty hash z rodiny SHA-2
- Privátní klíč uživatele, který podepisuje data, musí být spojen s CSP, který podporuje podepisování výsledné hodnoty hash z rodiny SHA-2
- Aplikace, která podepisuje data, musí podporovat využití hash algoritmů SHA-2.
- Aplikace nebo operační systém musí podporovat požadované výstupní formáty podepsaných zpráv

Shrnutí nutných podmínek pro podporu SHA-2

Operační systém musí být schopen ověřit platnost certifikátu (platnost podpisu), který je podepsán s využitím algoritmu rodiny SHA-2.

Podepsání certifikátu realizuje certifikační autorita.

Následující tabulka shrnuje podporu ověření planosti certifikátu

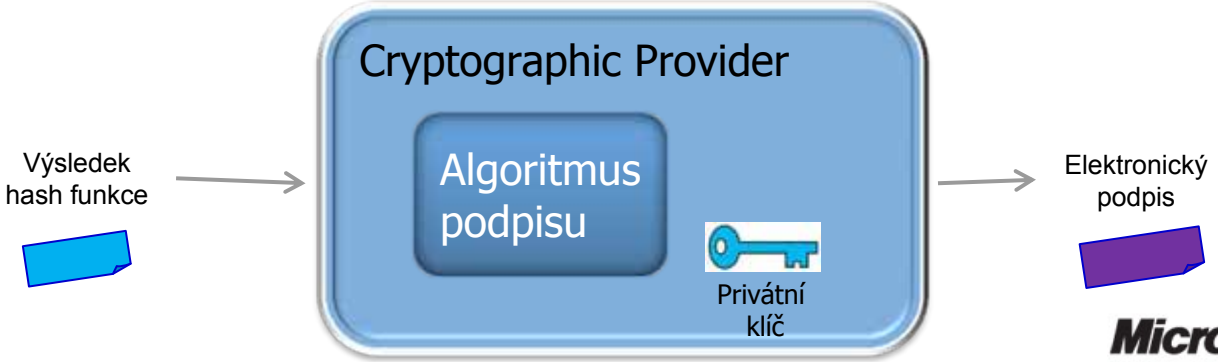
Operační systém	Podpora ověření certifikátu s SHA-2
Windows 2000	Ne
Windows XP před SP3	Ne
Windows XP SP3	Ano
Windows Server 2003	Ano, musí být nainstalován hotfix KB 938397
Windows Vista	Ano
Windows Server 2008	Ano
Windows 7	Ano

Shrnutí nutných podmínek pro podporu SHA-2

Cryptographic Provider musí podporovat podepisování výsledné hodnoty hash z rodiny SHA-2

Upozornění: Privátní klíč podepisujícího subjektu musí být spojen s tímto CSP.

CSP	Podpora SHA-2
Microsoft Enhanced Cryptographic Provider v1.0 (*ME_CP 1.0*)	Ne
Microsoft Enhanced RSA and AES Cryptographic Provider (Prototype) (*ME_RSA_AES_CP_Prototype*)	Ano
Microsoft Enhanced RSA and AES Cryptographic Provider (*ME_RSA_AES_CP*)	Ano
Microsoft Base Smart Card Crypto Provider (*MBSC_CP*)	Ano, v závislosti na vlastnostech čipové karty



Microsoft Services

Shrnutí nutných podmínek pro podporu SHA-2

CSP	Windows					
	XP	XP SP3	Vista	7	2003	2008
(ME_CP 1.0)	Ano	Ano	Ano	Ano	Ano	Ano
(ME_RSA_AES_CP_Prototype)	Ne	Ano	Ne	Ne	Ne	Ne
(ME_RSA_AES_CP)	Ne	Ne	Ano	Ano	Ano	Ano
(MBSC_CP)	Ano	Ano	Ano	Ano	Ano	Ano

Poznámka: Výše uvedené tabulky shrnují možnosti využívání podpisového schématu RSA/SHA. Pro jiné varianty např. s využitím „*Elliptic Curve Digital Signature Algorithm (ECDSA)*“ by matice podpory v operačních systémech byla jiná.

Shrnutí nutných podmínek pro podporu SHA-2

Aplikace, která podepisuje data, musí podporovat využití hash algoritmů SHA-2

Funkce musí být přímo zabudována v aplikaci (tj. **aplikace musí být upravena**) a uživatel musí mít možnost toto nastavení ovlivnit buď výběrem z dialogových oken, nebo pomocí konfigurace aplikace

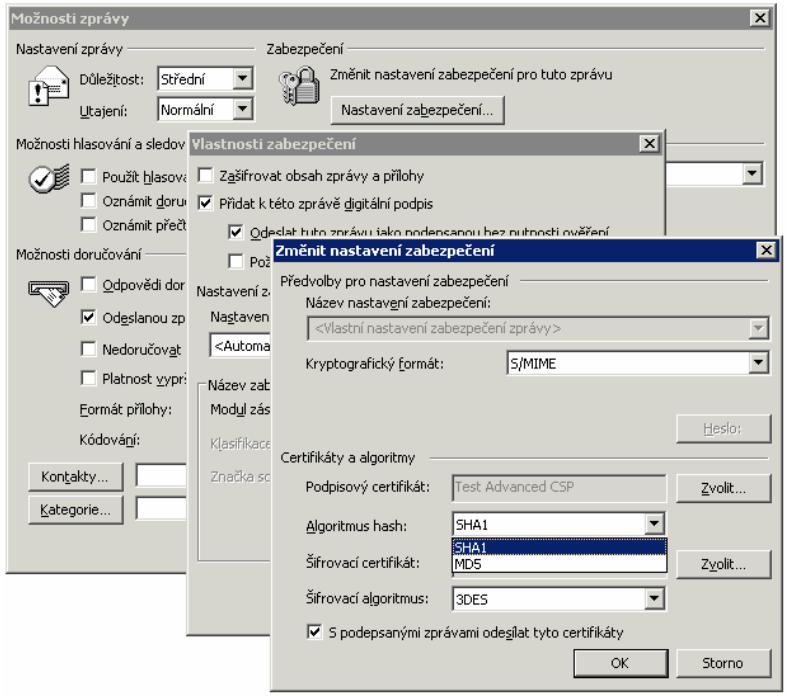
Upozornění 1: Nezaměňovat z podpisem vlastního certifikátu, který provádí certifikační autorita (první podmínka)

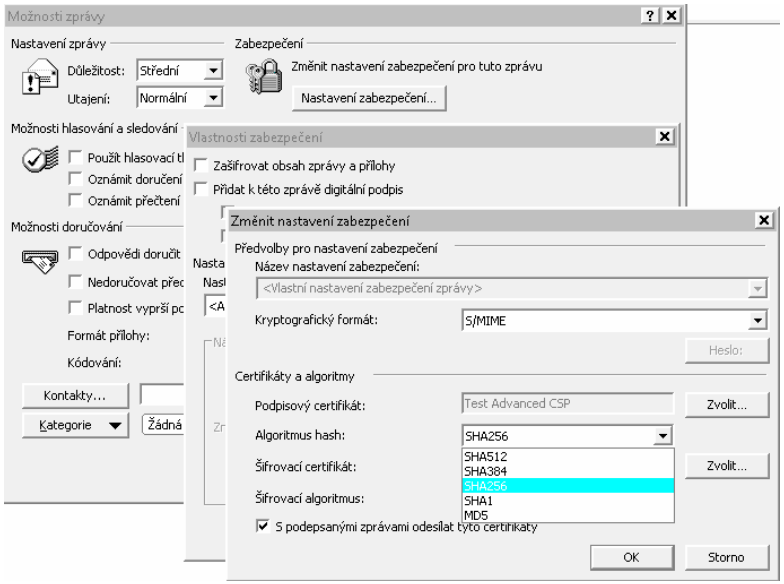
Upozornění 2: I s certifikátem, který je od certifikační autority podepsán s využitím algoritmu SHA-1 je možné podepisovat data s využitím algoritmů rodiny SHA-2

Upozornění 3: S certifikátem, který je od certifikační autority podepsán s využitím algoritmu SHA-2 je možné podepisovat data s využitím algoritmu SHA-1

Shrnutí nutných podmínek pro podporu SHA-2

Příklady nastavování hash algoritmů v aplikacích Microsoft Outlook 2003 a Microsoft Outlook 2007

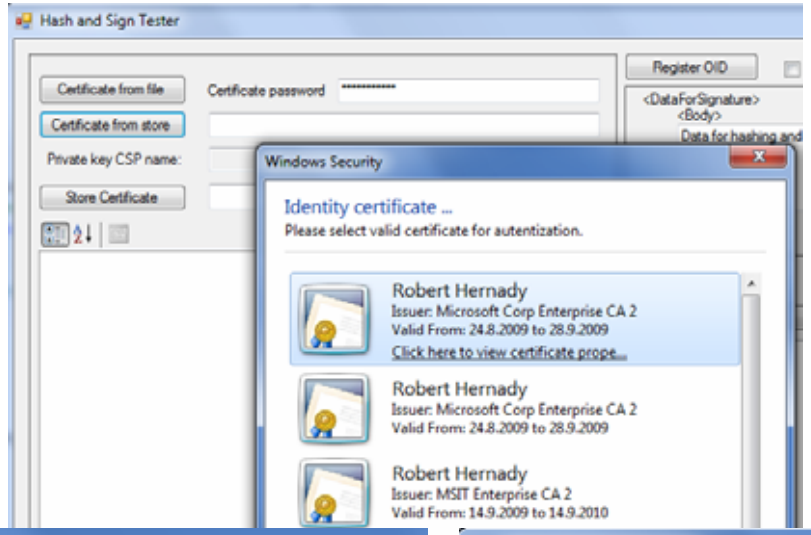


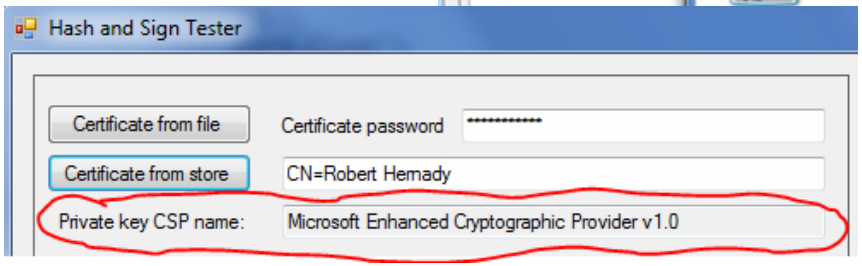


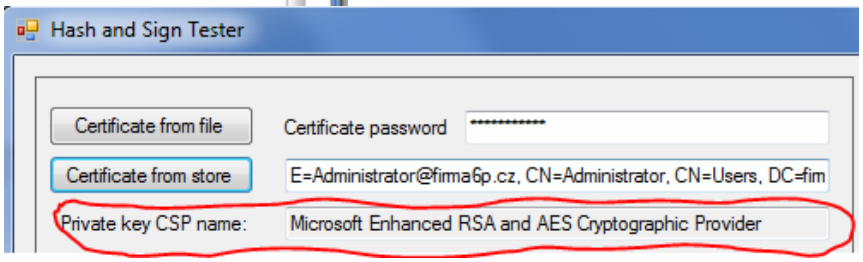
Microsoft | Services

Shrnutí nutných podmínek pro podporu SHA-2

Privátní klíč uživatele, který podepisuje data, musí být spojen s CSP, který podporuje podepisování výsledné hodnoty hash z rodiny SHA-2







Shrnutí nutných podmínek pro podporu SHA-2

Přestože podmínka pro spojení privátního klíče se správným CSP podle popisu vypadá velmi problematicky má několik řešení i pro případy, kdy je privátní klíč spojen s CSP bez podpory algoritmů SHA-2.

- Jednak je možné vytvořit nástroj, který „přehodí“ privátní klíč ke správnému CSP
- nebo je možné tuto situaci ošetřit přímo v kódu aplikace, která si za běhu spojí privátní klíč uživatele se správným CSP.
- Pro jistotu je potřeba znovu zdůraznit, že tyto „opravné“ mechanismy je možné provádět pouze s certifikáty uloženými v souboru nebo v úložišti Windows a nelze je použít pro certifikáty na čipových kartách.

Podpora výstupních formátů v OS Windows

Výstupní formát	Windows					
	XP	XP SP3	Vista	7	2003	2008
PKCS#1 – SHA 2 [1)]	Ne	Ano	Ano	Ano	Ano	Ano
PKCS#7 – SHA 2	Ne	Ne/Ano*	Ano	Ano	Ne	Ano
XML DSIG – SHA 2 .NET Framerwork 3.5 SP1 [2)]	Ne	Ano	Ano	Ano	Ano	Ano

1) PKCS#1 je doporučení pro implementaci kryptografie pracující s veřejným klíčem založené na algoritmech RSA. Zavoláním CSP je vytvořen elektronický podpis na základě doporučení PKCS#1. Jedná se o výstup definované délky. Volání CSP je možné realizovat v prostředí .NET nebo přímým voláním Win32 API

2) - XML DSIG je možné realizovat i s podporou dalších platforem např. JAVA

Upozornění: Předchozí tabulky shrnují technologie přímo dodávané společností Microsoft. Třetí strany mohou realizovat CSP, výstupní formáty, podepisování vlastními prostředky.

* - musí být naistalován hot fix KB968730

Microsoft | Services

Využívají Windows XP SP3 algoritmy SHA-2?

Využívají aplikace nad Windows XP SP3 SHA-2?

Stačí upgrade na Windows Vista/7?

Budou aplikace po upgrade na Windows Vista automaticky podporovat hash funkce rodiny SHA-2?

Modelová situace

Uživatel, který posílá maily, elektronicky zasílá data celní správě a prostřednictvím transakční části PVS zasílá elektronicky Evidenční listy důchodového pojištění ČSSZ.

Vybavení

- Windows XP SP2, Microsoft Office 2003
- Dekarantský sw vytvořený Firmou X, data se zasílají prostřednictvím VAN operátora
- Personální systém vytvořený Firmou Y, data se zasílají prostřednictvím transakční části PVS

V polovině ledna 2010 získá od akreditované certifikační autority nový certifikát, který bude podepsán s využitím algoritmu rodiny SHA-2.

Co nastane?

Modelová situace – činnosti uživatele

Uživatel provede import certifikátu vč. kořenových certifikátů certifikační autority (předpokládáme, že budou nové)

Uživatel si musí naistalovat SP3 pro Windows XP

- Operační systém bude schopen ověřit platnost elektronického podpisu certifkátu, který provedla CA s využitím algoritmu SHA-2

Od tohoto okamžiku může uživatel bez prolému certifikát používat a elektronicky komunikovat s tím, že:

- Outlook 2003 bude elektronicky podepisovat maily s využitím algoritmu SHA-1
- Komunikace s celní správou bude probíhat beze změny. Tj. podpsaná data budou přenášena ve formátu S/MIME (PKCS#7). Podpis bude realizován s využitím algoritmu SHA-1
- Komunikace s ČSSZ bude probíhat dle definovaného formátu datové zprávy a data budou podepisována s využitím algoritmu SHA-1

V této fázi uživatel nemusí provádět upgrade OS. Pouze musí nainstalovat SP3.

Modelová situace – změny na straně GŘC a ČSSZ

Nyní předpokládejme, že na straně GŘC a ČSSZ dojde ke změně datového formátu a nově bude k dispozici i možnost zasílat data, která budou podepsána s využitím algoritmu SHA-2

- Oznámení na stránkách MV přesto stále počítá se zachováním podpory algoritmu SHA-1. Lze předpokládát, že tuto komunikaci resorty dostatečně dlouho zachovají

Po zveřejnění nových principů elektronického podepisování dat musí firmy X a Y do svých programů provést příslušné změny

- Předpokládá se, že nově bude využíván formát XML DSIG

Po dokončení nových verzí příslušných programů si uživatel udělá upgrade těchto aplikací

Příslušné aplikace, pokud budou „řádně“ napsány, budou funkční i na Windows XP

Koncový uživatel nebude muset provádět upgrade Windows XP SP3 na novější verze OS

Modelová situace – odesílání mailů

Uživatel se rozhodne, že bude chtít odesílat maily, které budou elektronicky podepsány a uživatel bude chtít použít hash algoritmus z rodiny SHA-2

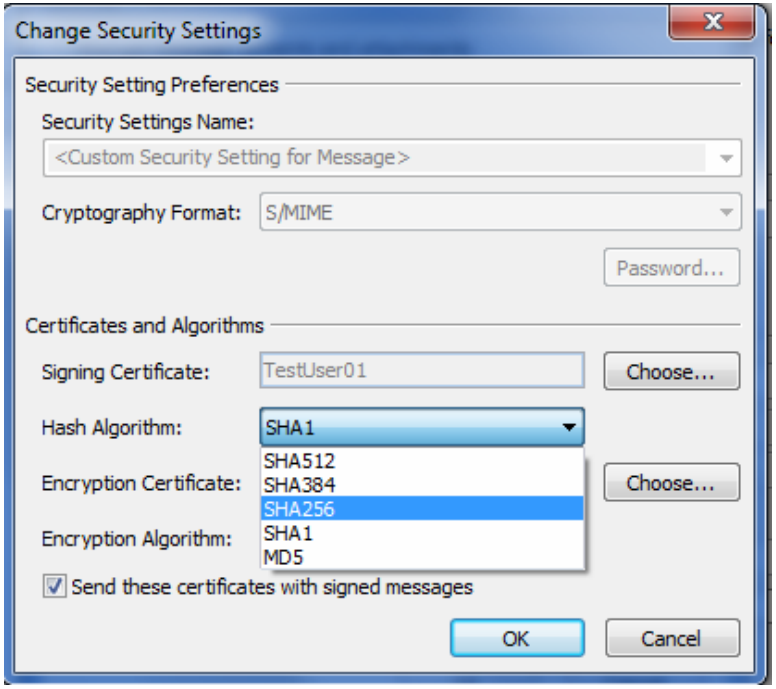
Toto je okamžik, kdy uživatel bude muset přistoupit k povýšení svého prostředí.

Bude nezbytné provést upgrade OS na Windows Vista nebo Windows 7

- Obsahují Cryptography API: Next Generation (CNG)

Bude nezbytné provést upgrade Office 2003 na Office 2007

- Office 2007 má zabudovanou podporu pro algoritmy z rodiny SHA-2 ve spolupráci s CNG



Poznámka: V současné situaci je to dobrovolné rozhodnutí uživatele, protože oznámení MV nemůže uživatele k tomuto kroku nutit

Podpora SHA-2 – mailová komunikace

	Outlook 2003			Outlook 2007			OWA Exchange 2007			OWA Exchange 2010		
	vytvořit	zobrazit	ověřit	vytvořit	zobrazit	ověřit	vytvořit	zobrazit	ověřit	vytvořit	zobrazit	ověřit
XP SP3	NE	ANO*	NE**	NE	ANO*	NE**	NE	ANO	NE	NE	ANO	NE
Vista/7	N/A	N/A	N/A	ANO	ANO	ANO	NE	ANO	ANO	ANO***	ANO	ANO
2003	NE	ANO*	NE**	N/A	N/A	N/A	NE	ANO	NE	NE	ANO	NE
2008	N/A	N/A	N/A	ANO	ANO	ANO	NE	ANO	ANO	ANO***	ANO	ANO

* - musí být naistalován hot fix KB968730
** - pouze částečné ověření platnosti podpisu
*** - nutné nastavení na Exchange 2010 Client Access serveru v registry
Vytvořit – možnost podepsání mailu s využitím algoritmu SHA-2
Zobrazit – možnost zobrazit mail, který je podepsán s využitím SHA-2
Ověřit – možnost ověření podpisu
N/A – Netestováno, lze očekávat, že chování bude obdobné jako na příbuzné platformě

OWA – podepisování je realizováno na straně klienta za pomoci ActiveX komponenty S/MIME

Office 2010 – podpora SHA-2 a XAdES

XML Advanced Electronic Signatures

EU kritéria pro „Advanced Electronic Signature“ podle direktivy 1999/93/EC

Tabulka ukazuje podporované varianty v Microsoft Office 2010

Signature Level	Description
XML-DSig	A simple digital signature that should not be trusted after its signing certificate expires.
XAdES-BES/EPES (Base)	Adds information about the signing certificate to the XML-DSig signature. A malicious user cannot switch the signing certificate for another certificate with the same public/private key. This is the default format for Office 2010 signatures.
XAdES-T (Timestamp)	Timestamps the XML-DSig and XAdES-BES/EPES portions of the signature. The signature is protected against expiration.
XAdES-C (Complete)	Includes all of the above plus references to revocation and certificate chain information.
XAdES-X (Extended)	Timestamps the XML-DSig SignatureValue node, the -T, and –C portions of the signature. The additional timestamp protects the additional data from repudiation.
XAdES-X-L (Extended Long-Term)	Includes all of the above and in addition stores the actual certificates and certificate revocation information with the signature. The additional information allows certificate validation even if the certificate servers are no longer available.

demo

Podepsání dokumentu ve Wordu

Microsoft | Services

Závěr

Zavedení hash algoritmů z rodiny SHA-2 je komplexní proces

Do hry vstupují vlastnosti operačního systému, certifikátů, kryptografických providerů a vlastních aplikací

Aplikace, které podepisují data budou muset být zrevidovány a s velkou pravděpodobností upraveny pro podporu algoritmů SHA-2

Bude nutné mít proces pro správu certifikátů tak, aby privátní klíče uživatelů byly spojeny se správným kryptografickým providerem

Jaroslav Tománek

Odbor koncepce a koordinace ICT ve VS
Ministerstvo vnitra ČR

Informace publikovaná MV ČR

- Informace k přechodu k bezpečnějším kryptografickým algoritmům v oblasti elektronického podpisu
- http://www.mvcr.cz/soubor/informace-k-prechodu-k-bezpecnejsim-kryptografickym-algoritmum-v-oblasti-elektronickeho-podpisu.aspx
- shrnutí problematiky a návod pro OVM

Děkujeme za pozornost