

Přechod na SHA-2

informace pro uživatele



Ministerstvo vnitra ČR

Odbor rozvoje projektů a služeb služeb eGovernment

7. 5. 2010

Přechod na SHA-2

Obsah dokumentu

1. Shrnutí	2
2. Všeobecná informace k SHA-2	3
3. Postup instalace kořenových certifikátů certifikační autority PostSignum	4
4. Aplikace, kterých se změna týká (z pohledu datových schránek)	5
5. Otázky a odpovědi	6

1. Shrnutí

Vážení uživatelé Informačního systému datových schránek,

přechod na šifrovací algoritmus SHA-2 je realitou, se kterou se musíme každý vypořádat. Pokusíme se vám vytvořit takové podmínky, aby pro vás tento nutný krok znamenal co nejméně komplikací.

Proto je důležité si hned v úvodu zopakovat důležitá fakta:

1. Přechod na SHA-2 je nutnou technologickou změnou v oblasti elektronických podpisů, kterou si nikdo nevymyslel jen tak pro nic za nic nebo aby vám komplikoval život.
2. Pokud můžete, používejte prosím moderní operační systémy a nainstalujte si nový kořenový certifikát, který vám zasíláme jako přílohu této systémové zprávy.
3. Nevíte-li si rady nebo jste identifikovali nějaký konkrétní problém, zavolejte prosím na infolinku datových schránek, tam vám poradí.
4. Od 23. 5. 2010 budou datové zprávy podepisovány novými SHA-2 certifikáty.
5. Od 23. 5. 2010 bude přihlášení do Informačního systému datových schránek zabezpečeno novým SHA-2 certifikátem.
6. Testovací prostředí, provozované na doméně czebox.cz, přešlo na SHA-2 certifikáty již k 18. 4., což uživatelům a dodavatelům aplikací poskytuje pět týdnů na otestování správné funkčnosti jejich systémů.

Děkujeme za pochopení.

Realizační tým ISDS

www.datoveschranky.info

informační web
nonstop

tel. 270 005 200

infolinka v pracovní dny
od 8:00 do 18:00

2. Všeobecná informace k SHA-2

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 a přechází na bezpečnější algoritmus SHA-2.

Tato změna se netýká pouze algoritmů používaných při vydávání kvalifikovaných certifikátů, ale i algoritmů pro vytváření elektronického podpisu a zajišťování šifrované komunikace. Dotkne se tak nejen poskytovatelů certifikačních služeb vydávajících kvalifikované certifikáty, ale všech osob využívajících elektronický podpis.

Je tedy nezbytné ukončit vytváření a ověřování digitálního otisku třídy SHA-1 a nahradit ji 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. Zároveň je od uvedeného data stanovena minimální přípustná délka kryptografického klíče pro algoritmus RSA na 2048 bitů.

Pro přehlednost uvádíme tabulku operačních systémů Windows s označením, zda je v nich možné certifikáty SHA-2 využívat.

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

Pokud využíváte podporovaný operační systém, jste připraveni na změnu ve vydávaných certifikátech. V opačném případě budete muset začít využívat jiný operační systém, který algoritmy SHA-2 podporuje.

V následující kapitole uvádíme postup instalace kořenového certifikátu v prostředí Windows.

Všechny další operační systémy (jmenovitě MacOS X a Linux) uvedené v seznamu konfigurací doporučených pro použití webového portálu datových schránek SHA-2 podporují. Instalaci v prostředí jiných operačních systémů provádějte tak, jak je v daných operačních systémech obvyklé. Výchozím úložištěm certifikátů pro OS Linux je úložiště, které využívá Mozilla Firefox. V případě jakýchkoli instalačních potíží, se kterými byste se na těchto platformách setkali, kontaktujte infolinku, kde Vám specialisté ochotně pomohou odbornou radou a přesným postupem.

Seznam konfigurací naleznete zde: <http://www.datoveschranky.info/priloha/82/>

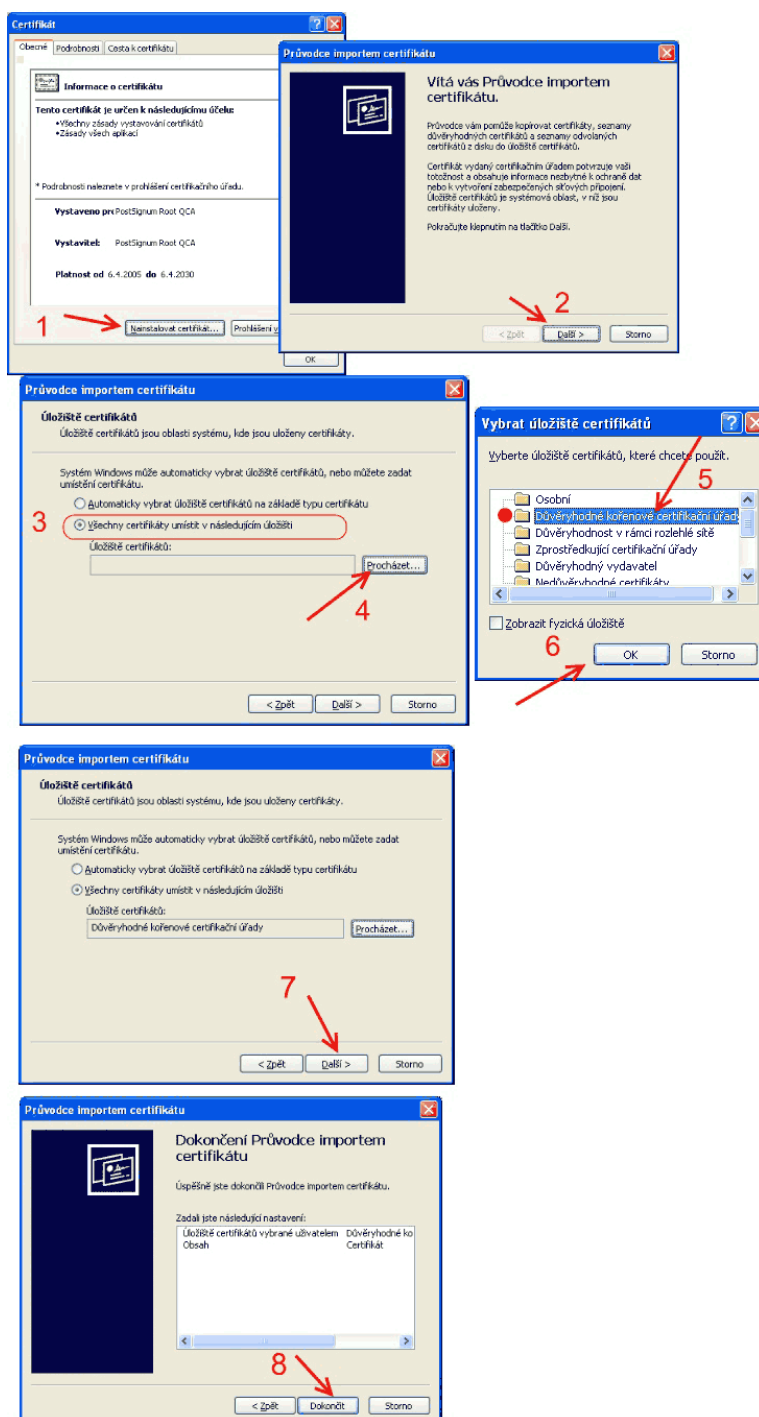
3. Postup instalace kořenových certifikátů certifikační autority PostSignum v prostředí Windows

Aby Váš počítač (operační systém i aplikace) dokázal správně vyhodnotit platnost elektronického podpisu, elektronické značky i časového razítka, je třeba do něj nainstalovat kořenový certifikát certifikační autority PostSignum, jejíž certifikáty jsou v rámci datových schránek primárně používány.

V průběhu května 2010 uvolní společnost Microsoft balíček Windows Update, který v sobě bude obsahovat SHA-2 kořenový certifikát certifikační autority PostSignum. Pokud tedy používáte operační systém Windows dle výše uvedené tabulky a máte zapnutý automatické aktualizace, následující postup provádět nemusíte.

Uložte si přílohu této datové zprávy, obsahující nový kořenový certifikát PostSignum (soubor **postsignum_qca2_root.cer**)

- Pокlepejte myší na soubor. Pokud se objeví dotaz, zvolte otevření souboru.
- Zobrazí se okno s informacemi o certifikátu.
- Stiskněte tlačítko Nainstalovat certifikát. Spustí se průvodce importem certifikátu. Stiskněte tlačítko Další.
- Na druhé obrazovce vyberte úložiště certifikátů „Důvěryhodné kořenové certifikační úřady“, resp. „Důvěryhodné kořenové certifikační autority“ (dle verze Window). Stiskněte tlačítko Další.
- Potvrďte poslední obrazovku stisknutím tlačítka Dokončit.
- Po dokončení importu se zobrazí okno s informací o úspěšném importu.



4. Aplikace, kterých se změna týká (z pohledu datových schránek)

4.1 Internetový prohlížeč

V rozsahu tohoto dokumentu nelze pojednat všechny kombinace internetových prohlížečů a operačních systémů. Nejpoužívanější prohlížeče využívají standardní systémová úložiště certifikátů, tudíž nevyžadují žádnou zvláštní péči. Mozilla Firefox má vlastní úložiště certifikátů. Doporučujeme postupovat dle bodu 3 návodu: <http://www.datoveschranky.info/clanek/302/>.

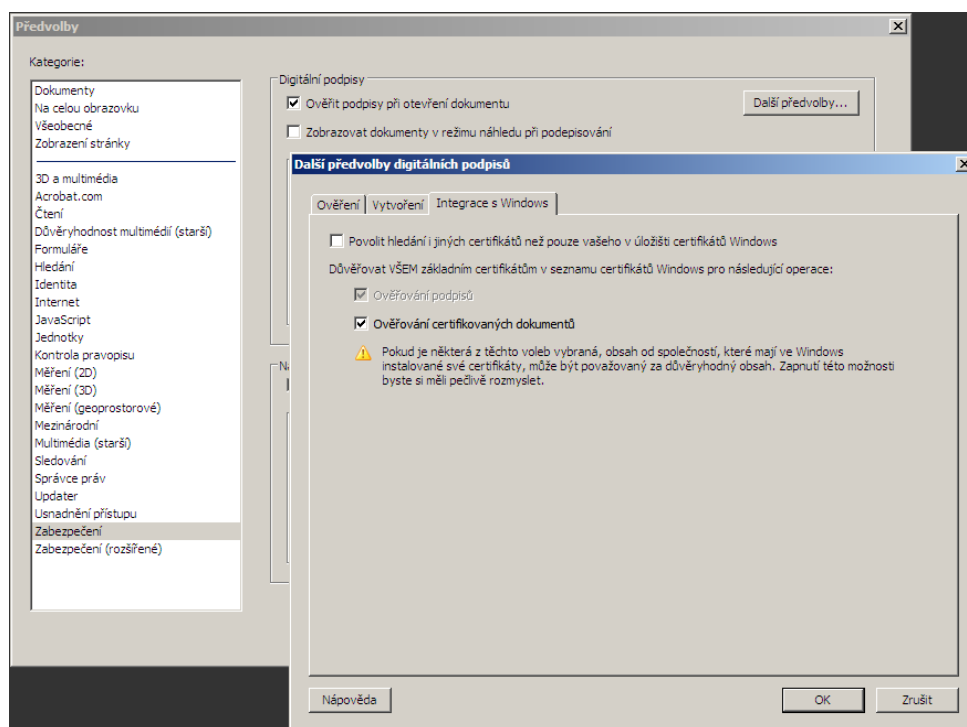
V každém případě doporučujeme aktualizovat prohlížeč na nejnovější dostupnou verzi.

4.2 Aplikace 602XML Filler

Aplikace 602XML Filler využívá systémové úložiště operačního systému Windows, případně standardní systémové úložiště certifikátů na ostatních podporovaných operačních systémech, nevyžaduje tedy speciální péči. Výchozím úložištěm certifikátů pro OS Linux je úložiště, které využívá Mozilla Firefox.

4.3 Prohlížeč PDF dokumentů Adobe Acrobat Reader

Aktuální verze aplikace Adobe Acrobat Reader je 9 — rozhodně doporučujeme používat nejnovější verzi. Acrobat Reader umožňuje využívat své vlastní úložiště certifikátů, nicméně pro uživatele Windows je mnohem jednodušší zvolit v Předvolbách volbu, která zajistí, že Acrobat Reader přebírá nastavení ze systému Windows, viz obrázek.



4.4 Vaše aplikace elektronické spisové služby

Podporu SHA-2 ze strany vámi používané aplikace musí zajistit výrobce aplikace. Pokud by tak neučinil, dopustil by nesoulad svého produktu s platnou legislativou České republiky i Evropské unie.

5. Otázky a odpovědi

- **Lze se přihlásit do datových schránek s nově vydaným (SHA-2) komerčním certifikátem?** Ano, lze — do testovacího i do ostrého prostředí.
- **Lze se přihlásit do datových schránek se starým (SHA-1) komerčním certifikátem?** Ano, přihlášení pomocí SHA-1 certifikátu je funkční do data ukončení platnosti vašeho certifikátu.
- **Platí stejná pravidla jako pro osobní certifikáty pro přihlašování komerčním serverovým (systémovým) certifikátem?** Ano.
- **Co mám dělat, když se mi objeví varování, že schránka je nedůvěryhodná?**
Varování neignorujte, nejdříve nainstalujte správný kořenový certifikát, přitom postupujte dle zde zveřejněného návodu na instalaci nových kořenových certifikátů.
- **Opatřování datových zpráv elektronickou značkou Ministerstva vnitra – musí uživatel do svého systému nainstalovat nové kořenové certifikáty, aby mu 602XML Filler neoznamoval, že zpráva není platně podepsaná?** Ano, musíte nainstalovat nové kořenové certifikáty. Aplikace 602XML Filler využívá systémové úložiště operačního systému Windows, případně standardní systémové úložiště certifikátů na ostatních podporovaných operačních systémech.
- **Co staré zprávy opatřené el. značkou Ministerstva vnitra založené na starém, expirovaném certifikátu — bude 602XML Filler oznamovat, že jsou podepsány podpisem založeným na neplatném certifikátu?** Ano bude, nicméně podle platné legislativy se považuje datová zpráva za pravou i v tomto případě, protože byla podepsána podpisem založeným na certifikátu, který byl platný v době podpisu. Zdali tomu tak skutečně je, si můžete ověřit z časového razítka.
- **Co časové razítko, kterým jsou opatřeny datové zprávy? Až vyprší platnost certifikátu časového razítka, bude 602XML Filler oznamovat, že razítko je založeno na neplatném certifikátu?** Ano, po vypršení certifikátu časového razítka bude prohlížeč zpráv hlásit neplatný certifikát, což ale automaticky neznamená, že datová zpráva není pravá. Platnost certifikátu časového razítka byla v červnu 2009 stanovena na tři roky. Od června 2010 bude nasazen nový certifikát s platností šest let, který bude každoročně obnovován, takže platnost časového razítka na datové zprávě bude vždy nejméně pět let od data vystavení.
- **Jak si tedy mohu ověřit pravost datové zprávy po vypršení platnosti el. značky a po vypršení certifikátu časového razítka?** Připravujeme novou službu Informačního systému datových schránek, která bude na základě systémových záznamů ověřovat, zda se předložená datová zpráva skutečně shoduje se zprávou, která systémem v minulosti prošla. Tato nová služba významně přispěje k vyřešení otázky dlouhodobé platnosti elektronických dokumentů.
- **Co písemnosti, které uživatel obdrží od úřadu podepsané podpisem založeným na novém SHA-2 certifikátu? Typicky to budou PDF přílohy — musí si uživatel instalovat kořenové certifikáty všech tří autorit, aby mu Acrobat neoznamoval, že jsou podpisy neplatné? Je na to někde návod?** Ano, vzhledem k tomu, že u nás působí tři certifikační autority, může se stát, že obdržíte písemnost vydanou úřadem, který používá kvalifikované certifikáty vydané jinou certifikační autoritou, než je PostSignum. Doporučujeme vám nainstalovat si i kořenové certifikáty dalších dvou certifikačních autorit, tedy První certifikační autority, a.s. (www.ica.cz) a elidentity a.s. (www.acaeid.cz).