

## Certifikáty

Od 13. 6. 2014 se servery prostředí registrů resortu zdravotnictví prokazují servery certifikátem CA Thawte. Kořenový certifikát této autority je již součástí běžných prohlížečů.

Viz další informace na <http://www.thawte.com/>

**Následující informace je určena pouze pro uživatele starších verzí operačních systémů Windows, verze XP a starší:**

### Přechod na vyšší kryptografické algoritmy SHA-2 v oblasti vydávání certifikátů

V souladu se [stanovením Ministerstva vnitra České republiky](#) musí být kvalifikované certifikáty a kvalifikované systémové certifikáty od 1. 1. 2010 vydávány s podporou algoritmu SHA-2 a minimální délky kryptografického klíče algoritmu RSA 2048 bitů.

Stanovisko společnosti Microsoft Česká republika k podpoře silné kryptografie v operačních systémech Windows naleznete [zde](#).

Pro vstup na zabezpečené stránky je zapotřebí operační systém, který je schopen ověřit platnost certifikátu s využitím algoritmu SHA-2 (sha256).

Operační systém	Podpora ověření certifikátu s SHA-2
Windows 2000	Ne
Windows XP před SP3	Ne
Windows XP <a href="#">SP3</a>	Ano
Windows Server 2003	Ano, musí být nainstalován hotfix KB938397
Windows Vista	Ano
Windows Server 2008	Ano
Windows 7	Ano


**Dřívější verze Windows včetně Windows XP SP2 neumí pracovat s těmito certifikáty, proto se ujistěte, že máte nainstalovaný systém s aktualizací Service Pack 3!**

### K čemu slouží certifikát?

Prostřednictvím certifikátu se vytváří zabezpečené šifrované spojení protokolem SSL/HTTPS mezi Vaším počítačem a servery KSRZIS.

Připojení na takto zabezpečené stránky poznáte podle adresy (obsahuje navíc písmeno s) <http://snzr.ksrzis.cz>.

### Jak zjistím, zda mám nainstalovaný Service Pack 3?

Informaci o systému je možné zobrazit buď klávesovou zkratkou Win + Pause nebo kliknutím na ikonu Tento Počítač -> pravým tlačítkem myši vybrat v roletce Vlastnosti .

Na kartě Obecné jsou informace o verzi systému Windows. Pokud používáte starší verzi než Windows XP SP3, obraťte se na Správce počítače s žádostí o update.

### Jak nainstaluji chybějící Service Pack 3 do svého počítače?

Pro instalaci potřebujete administrátorská práva k systému. Informace k instalaci naleznete [zde](#), samotný servisní balíček je možné stáhnout [zde](#).

## Certifikáty vydané certifikační autoritou MZČR

- <http://crl.mzcr.cz/mzcrca.crt> (nainstalovat do Důvěryhodné kořenové certifikační autority)
- [http://crl.mzcr.cz/mzcrca\(1\).crt](http://crl.mzcr.cz/mzcrca(1).crt) (nainstalovat do Důvěryhodné kořenové certifikační autority - **nový od 20. 2. 2017** (předchozí certifikát zůstává v platnosti a instalují se tak oba dva tyto certifikáty))
- <http://crl.mzcr.cz/mznetinterca.crt> (default - tj. ponechat volbu automaticky vybrat úložiště)
- <http://crl.mzcr.cz/eregca.crt> (default)

## Instalace ovládacího SW – aplikace SafeSign (token)

Stáhněte aplikaci SafeSign (3.0.112) podle verze operačního systému:

- Aplikace SafeSign pro 32bitový operační systém: [safesign\\_x86.zip](#)
- Aplikace SafeSign pro 64bitový operační systém: [safesign\\_x64.zip](#)