




Vážení klienti,

dovolujeme si Vás upozornit, že dne 31.12.2009 bylo kvalifikovanými poskytovateli certifikačních služeb ukončeno vydávání kvalifikovaných certifikátů s algoritmem SHA-1. Více informací najdete zde: <http://www.mvcr.cz/clanek/zmena-v-kryptografickych-algoritmech-ktere-jsou-pouzivany-pro-vytvareni-elektronickeho-podpisu.aspx>.

Tato změna se dotkla i internetového serveru ČMZRB, a.s., přes který se zadávají platby internetového bankovníctví. Od 26.2.2010 je tento server zabezpečen certifikátem vydaným dle nové metodiky. Tento certifikát již podporuje vyšší algoritmus zabezpečení SHA-2. Komunikace mezi klientem a bankou tak splňuje nejnáročnější kritéria na bezpečnou komunikaci.




Nasazení nového certifikátu na server však mělo za následek, že některé prohlížeče mají problémy s přístupem na server. Označují jej jako nedůvěryhodný – viz. např. obr.

 **There is a problem with this website's security certificate.**

The security certificate presented by this website was not issued by a trusted certificate authority.
The security certificate presented by this website was issued for a different website's address.

Security certificate problems may indicate an attempt to fool you or intercept any data you send to the server.

We recommend that you close this webpage and do not continue to this website.

-  [Click here to close this webpage.](#)
-  [Continue to this website \(not recommended\).](#)
-  [More information](#)

Je to způsobeno tím, že stanice uživatele není vybavena patřičným certifikátem. Uživatel by si v tom případě měl na stanici nainstalovat správný certifikát certifikační autority, který podporuje již nové algoritmy. Certifikát je možné získat ze stránky certifikační autority. V našem případě je to certifikát od společnosti I.certifikační autorita, a.s.. Najdete jej na této stránce:

<http://www.ica.cz/cz/menu/112/prace-s-certifikaty/korenove-certifikaty-i-ca-sha-2/>

Uživatel si musí stáhnout a nainstalovat „Kořenový certifikát certifikační autority pro vydávané komerční certifikáty“ – viz. obr.

DALŠÍ INFORMACE

- Seznam veřejných certifikátů
- Žádost o zneplatnění certifikátu
- Seznam zneplatněných certifikátů
- Kořenové certifikáty I.CA SHA-1
- Kořenové certifikáty I.CA SHA-2**
- Potřebné dokumenty k žádosti

ČASTO Kladené otázky

Otázka: "Nelze generovat žádost SHA2, nutný upgrade OS" [▶ Odpověď](#)

Otázka: "Není nainstalována podpora pro podepisování (icapki.cab)" [▶ Odpověď](#)

Otázka: "Co je „Identifikátor MPSV“?" [▶ Odpověď](#)

[▶ Více otázek a odpovědí](#)

Navigace: [▶ Hlavní stránka](#) [▶ Práce s certifikáty](#) [▶ Kořenové certifikáty I.CA SHA-2](#)

Kořenové certifikáty I.CA SHA-2

Kořenový certifikát certifikační autority pro vydávané komerční certifikáty :

Parametry :

- kryptografický algoritmus **SHA-256**
- délka kryptografického klíče pro algoritmus RSA **2048 bitů**,
- doba platnosti : **od 1.9.2009 do 1.9.2019**

[▶ Instalovat certifikát](#)

▶ 1. Jméno certifikátu : **sica_root_key_20090901.der** Délka : 1070byte

Formát Typ otisku/Otisk
DER SHA-256/6468bf8cf3cf688ebb2a6841bd70e97b5229b49df8690d7b74193e9ce3886141
SHA-1/90dece77f8c825340e62ebd635e1be20cf7327dd
MD-5/86ef8e319d9f8569a2a41a127168ba1b

[▶ Formát DER](#)

▶ 2. Jméno certifikátu : **sica_root_key_20090901.pem** Délka : 1509byte

Formát Typ otisku/Otisk
PEM SHA-256/7449a917e246e5c336493d1eb877b95dee77c79666ff9ada1e3b5acea27a7bce
SHA-1/6472504137dd8cbb76a636382ac640225df1ff91
MD-5/c4bfa8052e15719e24e1b5cca623103d

[▶ Formát PEM](#)

▶ 3. Jméno certifikátu : **sica_root_key_20090901.txt** Délka : 3301byte

Formát Typ otisku/Otisk
TXT SHA-256/701a78e0667442ba6d0d19702a0981fcaaa272a4dc3722305daa0a8f286c1697
SHA-1/4e73ea0c1671fd1bfc25a5c380e5ec3fbb25b34a
MD-5/154fc80cb6ca05b0761d4e0a919658ad

[▶ Formát TXT](#)

▶ 4. Jméno certifikátu : **sica_root_key_20090901.cmf** Délka : 1336byte

Formát Typ otisku/Otisk
CMF SHA-256/0aa67e521ef20a4f2db1a496da46c8512dc0ca4350e19f8d00bc37830a45b396
SHA-1/2a942921ac605bfa58e3db62f9cd45e9708e3b56
MD-5/c0f2cc806c6b51b439402ebc02d49e3b

[▶ Formát CMF](#) - pro čipovou kartu Starcos 3.0

Pozn.
Uvedené otisky byly počítány z obsahu celého souboru.

Instalace se provádí dle standardních postupů daných operačním systémem či používaným prohlížečem.

Certifikát se musí nainstalovat do Trusted Root Certification Authorities (Důvěryhodných certifikačních autorit).

Po instalaci tohoto certifikátu by Váš prohlížeč již neměl mít problém s přihlášením na náš server.

Administrátor aplikace