Obsah

| Úvodem | 1 |
|--|---|
| Jak to vypadá, když certifikát není nainstalován | 2 |
| Instalace kořenového certifikátu ZŠ O. Březiny (pro Internet Explorer a Google Chrome) | 4 |
| Import certifikátu pro prohlížeč Mozilla Firefox | 9 |

Úvodem

Digitální certifikát je digitálně podepsaný veřejný šifrovací klíč, který vydává certifikační autorita (služba našeho serveru). Uchovává se ve speciálním formátu, který (kromě jiného) obsahuje informace o majiteli veřejného klíče a vydavateli certifikátu (tvůrci digitálního podpisu, tj. certifikační autoritě). Certifikáty jsou používány pro identifikaci protistrany při vytváření zabezpečeného spojení (HTTPS, VPN atp.).

Aby mohla být komunikace s našimi servery bezpečná a nesledovatelná (každý Váš běžný mail si může Váš poskytovatel internetu klidně přečíst, protože je přenášen v nešifrované podobě ze serveru až do Vašeho počítače), musí být přístup do školní sítě šifrován (poznáte to tak, že v adresovém řádku bude místo <u>http://www</u>. napsáno <u>https://www</u>.

Díky šifrování se tak žádný jiný člověk kromě Vás nedozví známky, obsah stránek atd., které se týkají Vašeho dítěte. Toto šifrování je zajištěno certifikátem. Protože máme potřebné technické znalosti a technické možnosti a abychom ušetřili finanční prostředky (podobně jako řada jiných organizací), vytvořili jsme si sami náš bezpečnostní certifikát.

Certifikát tedy pomáhá zajišťovat šifrování komunikace a potřebujete ho např. pro přihlášení do internetové klasifikace, ale i pro stažení některých souborů z našeho datového úložiště.

Prohlížeč může náš certifikát hlásit jako nedůvěryhodný, ale to jen proto, že Váš prohlížeč standardně nezná naši školu jako tvůrce certifikátu. Např. Internet Explorer říká, že se jedná o nedůvěryhodný web, M. Firefox hlásí "Toto připojení není důvěryhodné" atd.).

Tento návod Vám umožní jednoduše naimportovat si kořenový certifikát naší školy jako důvěryhodný a využít tak plnohodnotně zabezpečené připojení do našeho systému. Navíc se samozřejmě již přestanou objevovat varovná hlášení během připojování do naší školy.

Pokud jste připojeni ze školního počítače přímo v naší škole a použijete program Internet Explorer nebo Google Chrome, varovná hláška se nikdy nezobrazí (školní počítače mají tento certifikát automaticky uznán jako důvěryhodný).

Jak to vypadá, když certifikát není nainstalován.

Kořenový certifikát slouží k přístupu na zabezpečené stránky školy. Pokusí-li se uživatel přistoupit na zabezpečené stránky a nemá nainstalován příslušný certifikát, objeví se upozornění na potíže s certifikátem. Modelovým příkladem je:

- přihlášení se z domova do Internetové klasifikace na adrese: <u>https://bakalari.zsobreziny.cz/bakaweb</u>
- stažení nějakého velkého souboru z našeho vnitřního úložiště (např. balíčky fotografií za školní rok, videa atd.)

| 8 | Objevil se problém s certifikátem zabezpečení tohoto webu. |
|---|---|
| | Certifikát zabezpečení předložený tímto webem nebyl vydán důvěryhodným certifikačním úřadem. |
| | Problémy s certifikátem zabezpečení by mohly ukazovat na pokus podvést vás nebo zachytávat data, která odešlete na server. |
| | Doporučujeme, abyste zavřeli tuto webovou stránku a nepokračovali na tento web. |
| | 🖉 Tuto webovou stránku zavřete kliknutím sem. |
| | 😵 Pokračovat na tento web (nedoporučujeme) |
| | Další informace |

Pokud přesto pokračujete kliknutím na prostřední předvolbu s červeným štítem, do aplikace se dostanete, avšak stránky se nadále zobrazují s upozorněním na neznámý certifikát (růžově podložená pole v záhlaví).

| 🔁 🔄 nittps://bakalan.zsobreziny.cz/bakaweb/login.a 🗩 👻 Chyba certifikatu C 🖉 🖉 Bakalan – přihlášení 🗙 | ₼ ☆ 🕸 |
|--|---------------------|
| Soubor Úpravy Zobrazit Oblíbené položky Nástroje Nápověda | |
| 🖕 🄽 Navrhované weby 🔻 🙁 Google 🗃 Acer | |
| Základní škola Otokara Březiny, Jihlava, Demle BàKàl ÁŘI 1. pololetí šk. rok | ova 34 u 2014/15 |
| programy pro školní administrativu uživatel: jméno: nenřihlášen | odhlásit |
| | |
| Přihlášení | |
| Přihlašovací iméno: | |
| | |
| | |
| Přihlásit | |
| | |
| | |
| V případě problémů s přihlášením, příp. připomínky k internetové klasifikaci, pište na e-mail nekvinda.vladimir@zsobreziny.cz. | |
| | |
| | |
| | |
| | |
| | |
| | |
| 1 | |

Nainstalujete-li si správně vrcholový certifikát CA Root ZŠ Otokara Březiny, výstraha se neobjeví a při pokusu o přístup na zabezpečenou stránku se dostanete rovnou na požadovanou zabezpečenou stránku. V záhlaví místo varovného podbarvení najdete ikonu zámku.

Obrázek znázorňující situaci, kdy je již certifikát nainstalován.

| \sim | | |
|--|--|--|
| () () () () () () () () () () | 🔎 🖛 🖴 🖸 💢 ZŠ Otokara Březiny, Jihlava 🏉 Bakaláři - přihlášení | × ि ☆ 🔅 |
| Soubor Úpravy Zobrazit Oblíbené položky Nástroje N | Nápověda | |
| 🚖 🌄 Navrhované weby 🔻 <mark>8</mark> Google 👔 Acer | | |
| BAKALÁŘI programy pro školní administrativu | Základní škola Otokara Březiny, Jihlava, D 1. pololeti š uživatel: jméno: nepřihlášen | emiova 34 k. roku 2014/15 odhlásit |
| | Přihlášení | |
| | | |
| 1 | Přihlašovací jméno: | |
| | Přihlašovací jméno: Heslo: | |

Instalace kořenového certifikátu ZŠ O. Březiny (pro Internet Explorer a Google Chrome)

Instalace spočívá v importu certifikátu do systému Windows a je společná pro oba prohlížeče (otestováno na Windows XP, Windows 7 32/64bit, Internet Explorer verze 11.0.960017280, Google Chrome verze 37.0.2062.120).

Na stránkách školy si stáhněte certifikát (ca_root_zs_otokara_breziny.zip), soubor si uložte. Poté soubor rozbalte a spusťte.

| Knihovna Dokumenty CA Root ZS Otokara Breziny | | | |
|--|---------------|---------------------|----------|
| Název položky | Datum změny | Тур | Velikost |
| 🔄 CA Root ZS Otokara Breziny.cer | 6.9.2014 0:59 | Certifikát zabezpe… | 3 kB |
| | | | |

Objeví se okno s informacemi o certifikátu. Stiskněte tlačítko Nainstalovat certifikát.

| Certifikát 🗾 | 3 |
|--|---|
| Obecné Podrobnosti Cesta k certifikátu | |
| Informace o certifikátu | |
| Certifikát kořenové autority není důvěryhodný. Má-li být považován za důvěryhodný, nainstalujte tento certifikát do úložiště důvěryhodných kořenových certifikačních autorit. | |
| Vystaveno pro: CA Root ZS Otokara Breziny | |
| Platnost od 18. 11. 2007 do 18. 11. 2032 | |
| Nainstalovat certifikát Prohlášení vystavitele Další informace o <u>certifikátech</u> | |
| OK | |



V následujícím okně vyberte spodní volbu Všechny certifikáty umístit v následujícím úložišti, stiskněte Procházet.

| Průvodce importem certifikátu | x |
|---|---|
| Úložiště certifikátů Úložiště certifikátů jsou oblasti systému, kde jsou uloženy certifikáty. | |
| Systém Windows může automaticky vybrat úložiště certifikátů, nebo můžete zadat umístění certifikátu. | |
| 🔘 Automaticky vybrat úložiště certifikátů na základě typu certifikátu | |
| Všechny certifikáty umístit v následujícím úložišti | |
| Úložiště certifikátů: | |
| Procházet | |
| | |
| | |
| | |
| | |
| Další informace o <u>úložištích certifikátů</u> | |
| < Zpět Další > Storno | |

V malém okně *Vybrat úložiště certifikátů* vyberte položku **Důvěryhodné kořenové certifikační autority**, poté stiskněte **OK**, načež malé okno zmizí.

| Vybrat úložiště certifikátů Vyberte úložiště certifikátů, které chcete po | exe oužít. |
|--|-----------------------------------|
| Osobní Osobní Důvěryhodné kořenové certifikačn Důvěryhodnost v rámci rozlehlé si Osobní Zprostředkující certifikační autority Důvěryhodní vydavatelé Nedůvěryhodní certifikáty | n <mark>í autor</mark> tě ∕ |
| Zobrazit fyzická úložiště | Storno |

V předchozím okně, které je nyní aktivní a vidíte v něm vybranou možnost, vyberte **Další**.

| Průvodce importem certifikátu | × |
|---|----|
| Úložiště certifikátů Úložiště certifikátů jsou oblasti systému, kde jsou uloženy certifikáty. | |
| Systém Windows může automaticky vybrat úložiště certifikátů, nebo můžete zadat umístění certifikátu. | |
| 🔘 Automaticky vybrat úložiště certifikátů na základě typu certifikátu | |
| O Všechny certifikáty umístit v následujícím úložišti | |
| Úložiště certifikátů: | |
| Důvěryhodné kořenové certifikační autority Procházet | |
| Další informace o <u>úložištích certifikátů</u> | |
| < Zpět Další > Storn | 10 |

Objeví se následující okno s informací o vybrané volbě. Stiskněte tlačítko Dokončit.



V okně **Upozornění zabezpečení** potvrďte **Ano**.

| Upozorněn | í zabezpečení | × |
|-----------|--|---|
| <u>^</u> | Rozhodli jste se nainstalovat certifikát z certifikační autority (CA), která vyžaduje: CA Root ZS Otokara Breziny Systém Windows neověřil, zda je certifikát pochází skutečně z CA Root ZS Otokara Breziny. Měli byste jeho původ potvrdit dotazem na CA Root ZS Otokara Breziny. Následující číslo vám při procesu pomůže: Kryptografický otisk (sha1): 48BA6171 85588CF8 9A8EFD1E A43F412D | |
| | D8FF824C Upozornění: Jestliže nainstalujete tento kořenový certifikát, bude systém Windows automaticky důvěřovat všem certifikátům vydaným touto certifikační autoritou. Instalace certifikátu s nepotvrzeným kryptografickým otiskem představuje bezpečnostní riziko. Kliknutím na tlačítko Ano toto riziko uznáváte. Chcete tento certifikát nainstalovat? | |
| | Ano Ne | |

Potvrzení úspěšného importu certifikátu zavřete tlačítkem OK.



Zavřete také původní okno s informacemi o certifikátu kliknutím na tlačítko OK. Tím je certifikát naimportován.

| Certifikát |
|--|
| Obecné Podrobnosti Cesta k certifikátu |
| Informace o certifikátu |
| Certifikát kořenové autority není důvěryhodný. Má-li být považován za důvěryhodný, nainstalujte tento certifikát do úložiště důvěryhodných kořenových certifikačních autorit. |
| Vystaveno pro: CA Root ZS Otokara Breziny |
| Vystavitel: CA Root ZS Otokara Breziny |
| Platnost od 18. 11. 2007 do 18. 11. 2032 |
| Nainstalovat certifikát Prohlášení vystavitele Další informace o <u>certifikátech</u> |
| ОК |

Import certifikátu pro prohlížeč Mozilla Firefox.

Prohlížeč Mozilla Firefox (testováno na verzi 32.0.1) nepřijme automaticky informace o importovaných certifikátech a je nutné daný certifikát importovat přímo do tohoto prohlížeče. Pokud používáte např. Google Chrome a Mozilla Firefox na jednom počítači, musíte provést oba postupy (předchozí pro IE a G. Chrome i následující postup pro M. Firefox).

Níže uvedené okno zobrazuje obrazovku prohlížeče M. Firefox, který nemá importovaný náš certifikát.

| | Toto připojení není důvěryhodné |
|---|---|
| | Požádali jste Firefox o zabezpečené připojení k serveru bakalari.zsobreziny.cz , ale nelze ověřit, že tom tak skutečně je. |
| | Pokud je požadováno zabezpečené připojení, měl by server předložit důvěryhodnou identifikaci a tím prokázat, že se připojujete na správné místo. Nicméně, identita tohoto serveru nemohla být ověřena. |
| | Co mám teď dělat? |
| | Pokud se k tomuto serveru obvykle připojujete bez problému, může tato chyba znamenat, že se za tento server někdo snaží vydávat, a neměli byste pokračovat. |
| | Rychle odsud pryčl |
| • | Technické detaily |
| , | Vím, o co se jedná |

Na stránkách školy si stáhněte certifikát (ca_root_zs_otokara_breziny.zip), soubor si uložte. Poté zazipovaný soubor rozbalte, ale certifikát schovaný uvnitř nespouštějte.

| Knihovna Dokumenty CA Root ZS Otokara Breziny | | | |
|--|---------------|--------------------|----------|
| Název položky | Datum změny | Тур | Velikost |
| 🔄 CA Root ZS Otokara Breziny.cer | 6.9.2014 0:59 | Certifikát zabezpe | 3 kB |

V menu prohlížeče Mozilla Firefox vyberte Nástroje / Možnosti.

| <u>S</u> oubor Úpr <u>a</u> vy <u>Z</u> obrazení <u>H</u> istorie Zál <u>o</u> žky [| <u>N</u> ástroje Nápo <u>v</u> ěda |
|--|--------------------------------------|
| 👔 ZŠ Otokara Březiny, Jihlava 🗙 🗥 Ne | Správce s <u>t</u> ahování Ctrl + J |
| × == ===,,,,, == == = = | Správce <u>d</u> oplňků Ctrl+Shift+A |
| 📽 < 🕙 https://bakalari.zsobreziny.cz/bak | Nastavit Sync |
| 🙇 Překladač Google 🔅 Bakaláři - přihlášení 👿 | Vývoj <u>w</u> ebu 🕨 |
| | Informace o stránce |
| | <u>M</u> ožnosti |

Vyberte záložku Rozšířené / Certifikáty a potom klikněte na levé tlačítko Certifikáty.

| Možnosti | | | | | | | × |
|------------------|--------------------|-------------------|-----------------------|-----------------|-------------|------------|-----------|
| | | 页 | | 00 | | \bigcirc | iğ. |
| Obecné | Panely | Obsah | Aplikace | Soukromí | Zabezpečení | Sync | Rozšířené |
| Obecné N | ložnosti hlá | ášení Síť / | Aktualizace | Certifikáty | | | |
| Pokud s | erver vyžad | uje osobní | certifikát: | | | | |
| 💿 Zvol | it <u>a</u> utomat | icky 💿 👌 | √ž <u>d</u> y se dotá | izat | | | |
| | | | | | r | | |
| <u>C</u> ertifil | káty <u>(</u> | <u>)</u> věřování | <u>B</u> ezpečr | nostní zařízení | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | ОК | Zrušit | | ápo⊻ěda |

V novém okně vyberte záložku Autority a klikněte na tlačítko importovat.

| Správce certifikátů | | |
|---|---|----------|
| Osobní Lidé Servery Autority O | Istatní | |
| Tyto certifikáty jsou dostupné pr | o identifikaci certifikačních autorit: | |
| Jméno certifikátu | Bezpečnostní zařízení | ₽. |
| V tomto poli můžet importovaných cert | e mít buď prázdno, nebo naopak mnoho již tifikátů. | |
| 197 168 1 114 | Sotter hezn zařízení | . |
| Zo <u>b</u> razit Upr <u>a</u> vit důvěru | Importovat Exportovat S <u>m</u> azat nebo nedův | ěřovat |
| | | ОК |

Najděte místo, kam jste uložili z webu náš certifikát a vyberte ho.

V okně Stažení certifikátu vyberte všechna tři příslušná políčka.

| Stažení certifikátu 🗾 | × |
|--|---|
| Byli jste požádáni o uznání nové Certifikační Autority (CA). | |
| Chcete uznat "CA Root ZS Otokara Breziny" pro následující účely? | |
| 📃 Uznat tuto CA pro identifikaci serverů. | |
| 📃 Uznat tuto CA pro identifikaci uživatelů pošty. | |
| 📃 Uznat tuto CA pro identifikaci výrobců software. | |
| Před uznáním této CA, a to pro jakýkoliv účel, byste měli prozkoumat její certifikát, její pravidla a podmínky (pokud jsou dostupné). | |
| Zobrazit Zobrazit certifikát CA | |
| OK Zrušit |] |

Potom, co jste vybrali všechna tři políčka, klikněte na **OK**.

| Stažení certifikátu |
|--|
| Byli jste požádáni o uznání nové Certifikační Autority (CA). |
| Chcete uznat "CA Root ZS Otokara Breziny" pro následující účely? |
| 🔽 Uznat tuto CA pro identifikaci serverů. |
| 🔽 Uznat tuto CA pro identifikaci uživatelů pošty. |
| 📝 Uznat tuto CA pro identifikaci výrobců software. |
| Před uznáním této CA, a to pro jakýkoliv účel, byste měli prozkoumat její certifikát, její pravidla a podmínky (pokud jsou dostupné). |
| Zobrazit Zobrazit certifikát CA |
| OK Zrušit |

Zavřete klikáním na tlačítka **OK** všechna předchozí okna a restartujte prohlížeč Mozilla Firefox.

Tím je import certifikátu do prohlížeče Mozilla Firefox dokončen.

Přeji příjemné a bezpečné používání našich internetových služeb. Mgr. Robert Srbecký, správce sítě a koordinátor ICT ZŠ Otokara Březiny, Demlova 34, 586 01 Jihlava

Datum poslední aktualizace tohoto návodu: 21. 9. 2014