

## 🔒 Podpora šifrovaného spojení – HTTPS 🔒

Pokud chcete zajistit šifrování přenosu dat po síti LAN mezi webovým prohlížečem klienta a docházkovým serverem, najdete níže potřebné kroky ke zprovoznění https protokolu.

Příručka obsahuje jen velmi jednoduchý postup s omezením na self-signed certifikát bez ověření serveru externí autoritou. Ten zajistí jen základní šifrovaný přenos dat. Pokud Vám tento jednoduchý postup nestačí, nebo chcete použít silnější šifrování, vyhledáte další postupy na webu.

U instalací v počítači RasPi je od verze programu 7.71 již vše přednastaveno a body 1 až 3 vynechte. (RasPi se starší verzí programu je třeba poslat k výrobci na aktualizaci – viz cení aktualizací na webu)

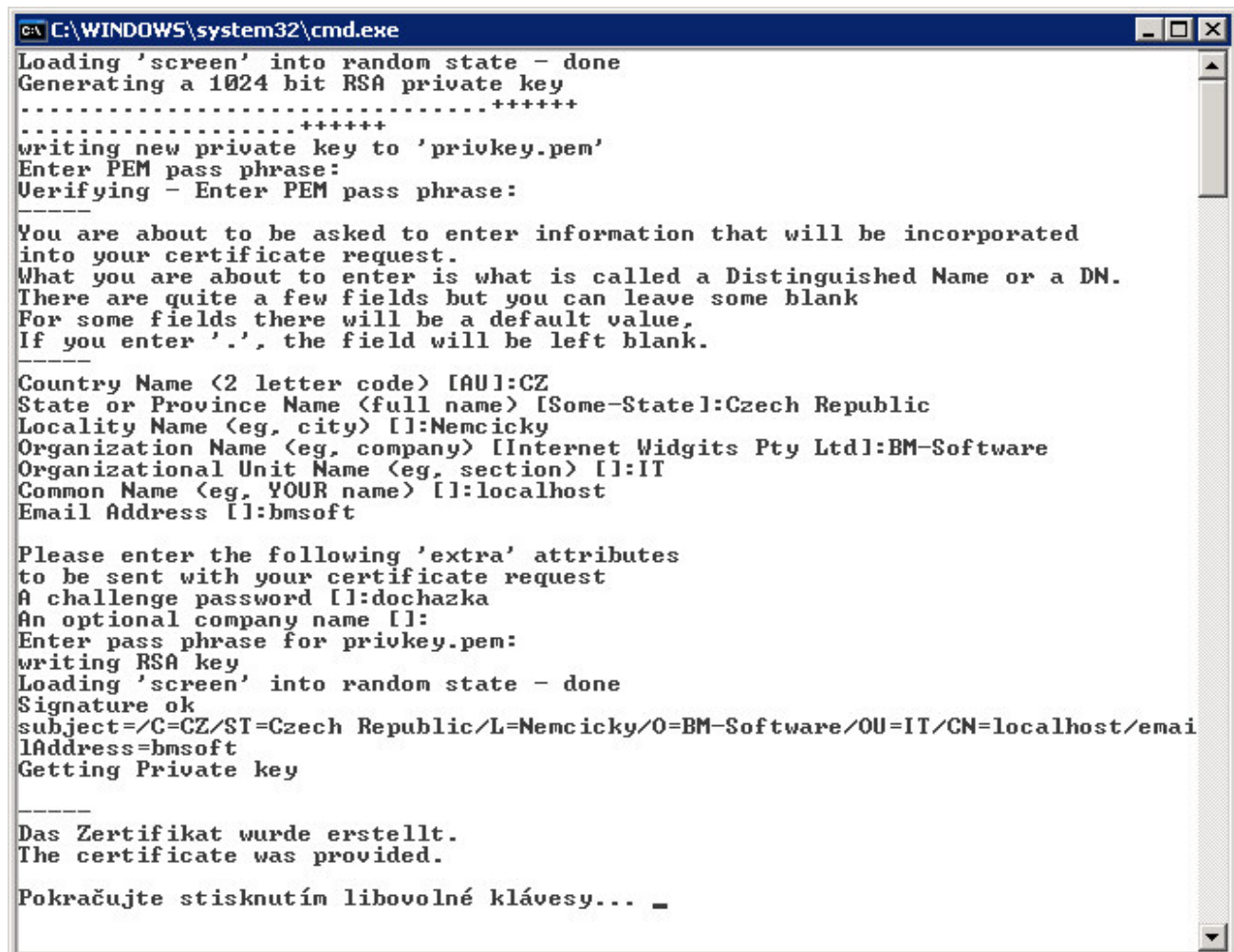
### Zprovoznění https:

Všechny níže uvedené kroky spouštějte na hlavním PC docházky - docházkovém serveru. Postup je určený pro standardní instalaci prostředí docházkového systému dodaného výrobcem po roce 2009. Nefunguje pro velmi staré instalace, nebo instalace s konfigurací prostředí (apache, php) upravovanou uživatelem či využívajícím jiný než dodaný webový server.

1. Generování certifikátu se provede jednoduše spuštěním souboru

```
C:\apache\apache\makecert.bat
```

Zvolíte si nějaké heslo k vašemu certifikátu, které zadáte na výzvu "PEM pass phrase" a poté ještě jednou na výzvu "Verify PEM ...". Na výzvu "Country name" zadáte CZ. Další 4 dotazy můžete buď vyplnit, nebo je stačí klávesou Enter potvrdit bez zadání údajů. Do „Common Name“ zadejte localhost (nebo lépe DNS název PC s docházkou) a další 3 položky opět můžete přeskočit. Jedná se o tvorbu lokálního self-signed certifikátu bez platnosti mimo vaši síť, takže zadání jmen, adres atd. není úplně nutné. Na dotaz "Enter pass phrase for privkey.pem" zadáte opět zvolené heslo. Certifikát se vygeneruje a poté program ukončíte klávesou Enter. Platnost certifikátu je 10 let.



```
C:\WINDOWS\system32\cmd.exe
Loading 'screen' into random state - done
Generating a 1024 bit RSA private key
.....+++++
.....+++++
writing new private key to 'privkey.pem'
Enter PEM pass phrase:
Verifying - Enter PEM pass phrase:
-----
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:CZ
State or Province Name (full name) [Some-State]:Czech Republic
Locality Name (eg, city) []:Nemcicky
Organization Name (eg, company) [Internet Widgits Pty Ltd]:BM-Software
Organizational Unit Name (eg, section) []:IT
Common Name (eg, YOUR name) []:localhost
Email Address []:bmssoft

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:dochazka
An optional company name []:
Enter pass phrase for privkey.pem:
writing RSA key
Loading 'screen' into random state - done
Signature ok
subject=/C=CZ/ST=Czech Republic/L=Nemcicky/O=BM-Software/OU=IT/CN=localhost/mai
lAddress=bmssoft
Getting Private key

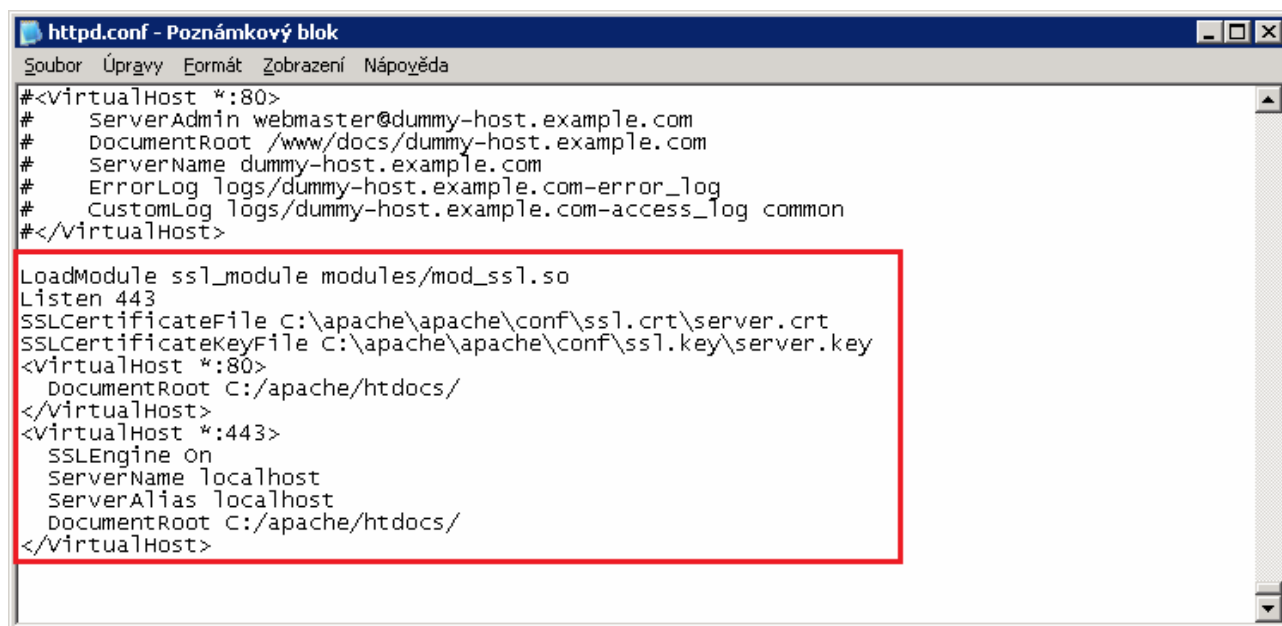
-----
Das Zertifikat wurde erstellt.
The certificate was provided.

Pokařujte stisknutím libovolné klávesy... _
```

2. Nyní je třeba upravit konfigurační soubor webového serveru Apache, aby začal používat šifrované spojení https protokolem. Spusťte si jednoduchý textový editor - ideálně program *Poznámkový blok*, který je součástí všech verzí windows a najdete jej v "Programy / Příslušenství" nebo na Windows 10 jednoduše zadáním názvu do vyhledávání (ikona lupy vlevo dole). V jeho menu zvolte *Soubor / Otevřít* a na disku vyhledejte soubor `C:\apache\apache\conf\httpd.conf`. Sjedťte úplně dolů a na samotný konec souboru nově doplňte tyto řádky:

```
LoadModule ssl_module modules/mod_ssl.so
Listen 443
SSLCertificateFile C:\apache\apache\conf\ssl.crt\server.crt
SSLCertificateKeyFile C:\apache\apache\conf\ssl.key\server.key
<VirtualHost *:80>
    DocumentRoot C:/apache/htdocs/
</VirtualHost>
<VirtualHost *:443>
    SSLEngine On
    ServerName localhost
    ServerAlias localhost
    DocumentRoot C:/apache/htdocs/
</VirtualHost>
```

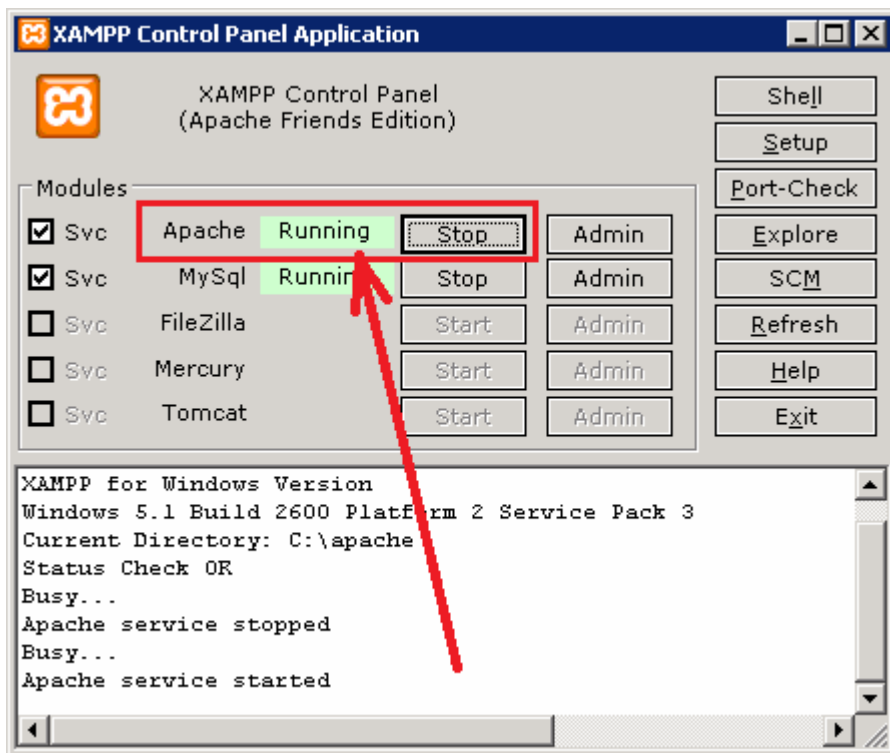
Pokud jste v bodě 1 zadali plný DNS název docházkového serveru , nahraďte jím řetězce *localhost* i zde. Poté soubor uložte pomocí *Soubor / Uložit*.



```
httpd.conf - Poznámkový blok
Soubor Úpravy Formát Zobrazení Nápověda
#<VirtualHost *:80>
#   ServerAdmin webmaster@dummy-host.example.com
#   DocumentRoot /www/docs/dummy-host.example.com
#   ServerName dummy-host.example.com
#   ErrorLog logs/dummy-host.example.com-error_log
#   CustomLog logs/dummy-host.example.com-access_log common
#</VirtualHost>

LoadModule ssl_module modules/mod_ssl.so
Listen 443
SSLCertificateFile C:\apache\apache\conf\ssl.crt\server.crt
SSLCertificateKeyFile C:\apache\apache\conf\ssl.key\server.key
<VirtualHost *:80>
    DocumentRoot C:/apache/htdocs/
</VirtualHost>
<VirtualHost *:443>
    SSLEngine On
    ServerName localhost
    ServerAlias localhost
    DocumentRoot C:/apache/htdocs/
</VirtualHost>
```

3. Dále se musí restartovat webový server Apache, aby se nová konfigurace načetla a začala fungovat. Stačí spustit program `C:\apache\xampp-control.exe` a v jeho menu v řádku se službou *Apache* kliknout na tlačítko *Stop*. Pokud se objeví výstražný dialog systému Windows, odsouhlaste provedení akce (může být nutné oprávnění administrátora). Během několika vteřin by měl v řádku *Apache* zmizet zelený nápis *Running*. Nakonec opět v řádku *Apache* klikněte na tlačítko *Start* a během několika vteřin se zelený nápis *Running* zase objeví. Pokud ne, udělali jste v některém z předchozích kroků chybu a je nutné ji opravit. Nyní klikněte na tlačítko *Exit* vpravo dole a program `xampp-control` se ukončí.



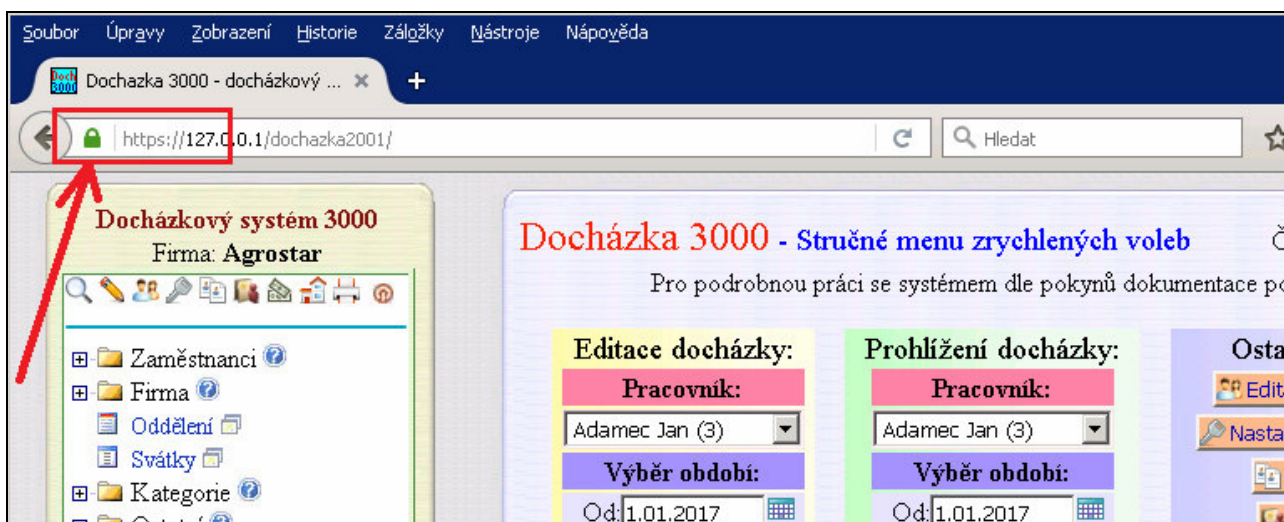
4. Připojení do docházky je nyní možné jak přes nešifrované http, tak nově i přes šifrovaný protokol https. Aby bylo spojení šifrované, je třeba opravit všechny odkazy klientských počítačů do docházky tak, aby již nepoužívaly původní protokol http, ale jen a pouze nový https. Např. na serveru se do docházky nyní dostanete tak, že spustíte webový prohlížeč a zadáte adresu <https://127.0.0.1/dochazka2001/>



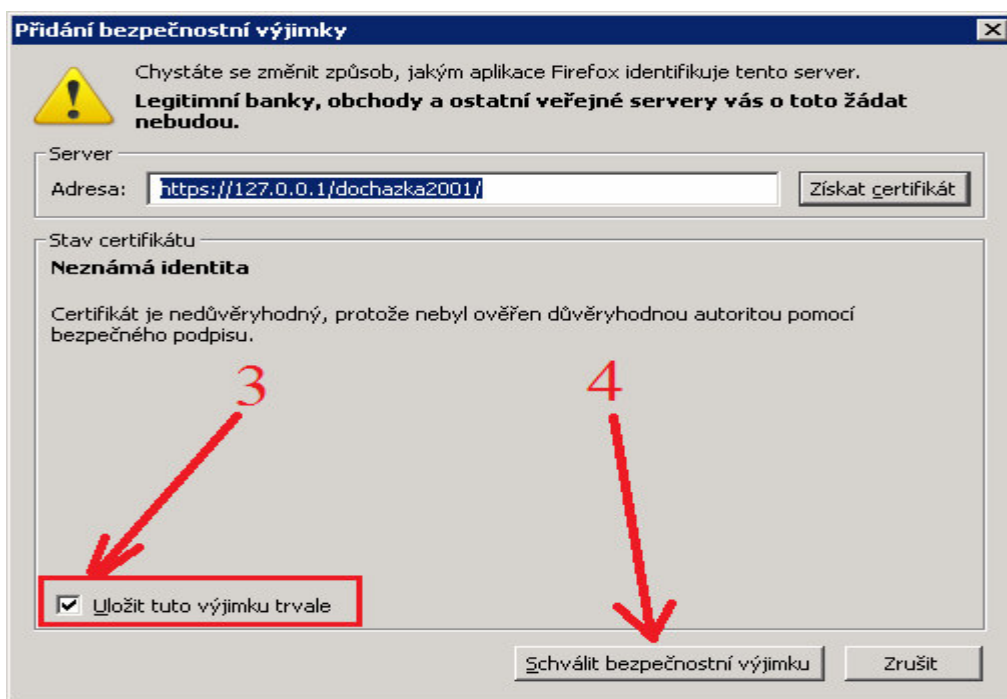
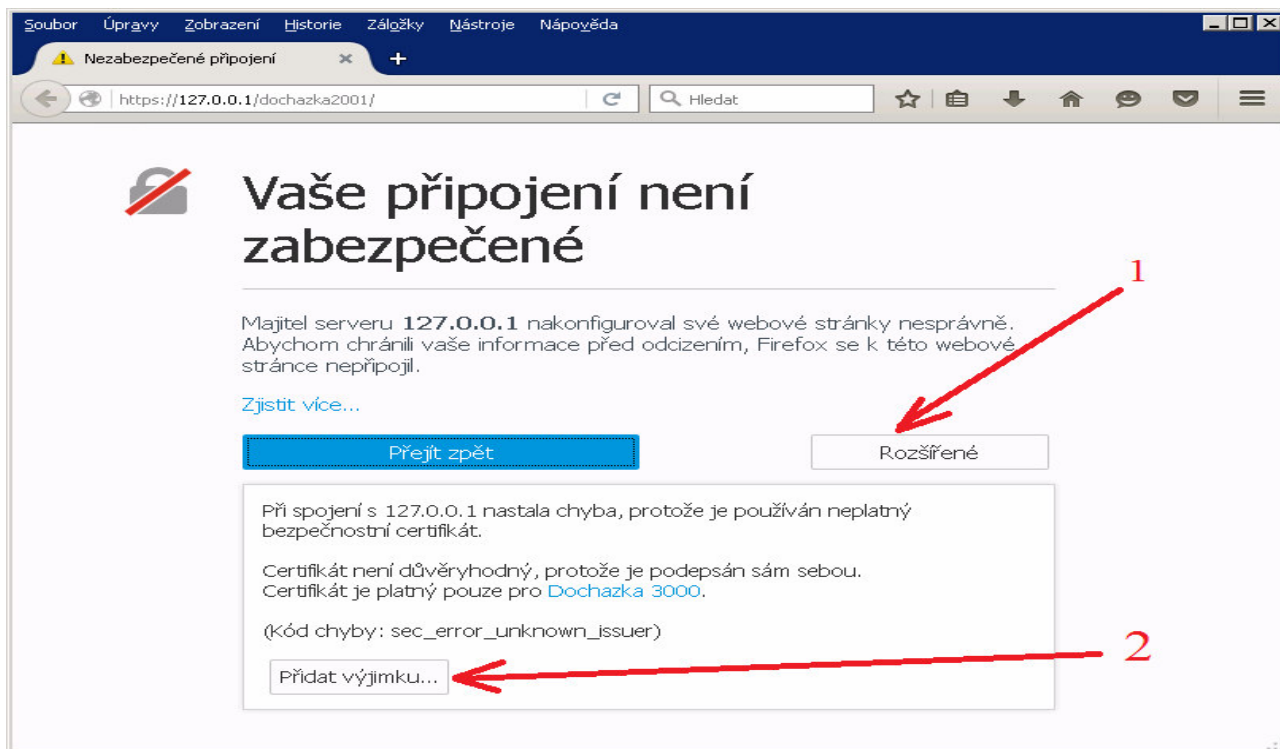
Pokud se zobrazí chybové hlášení o nutnosti použít TLS 1.2 a vyšší, najdete postup na dalších stranách tohoto návodu od strany 5 níže.

Nezapomeňte tedy uvést písmeno "s" v úvodu adresy. Pokud nebude https fungovat z počítačů klientů, musíte ve firewallu hlavního PC docházky odblokovat port 443. Dále je třeba v prohlížeči schválit použití tohoto self-signed certifikátu dle následujícího bodu 5.

Nešifrované spojení přes http protokol funguje i nadále, což je nutné kvůli přenosu dat z terminálů a některým sestavám (výsledovka, výkaz ...).



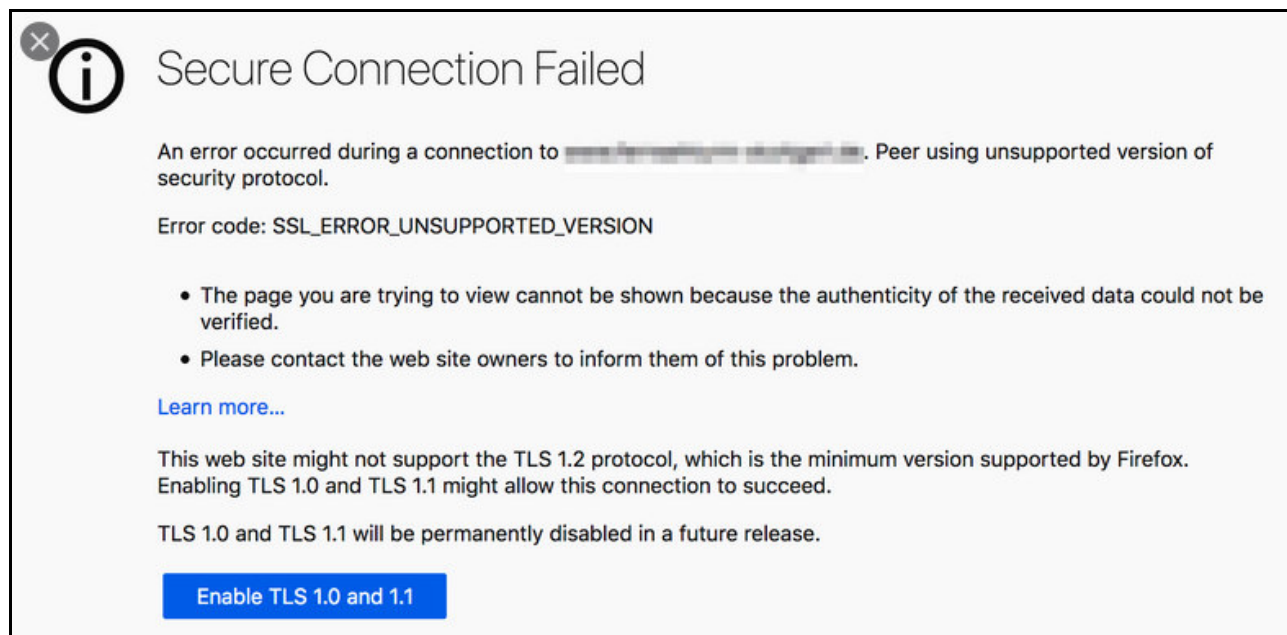
5. Prohlížeč po zadání nové adresy s https zobrazí varovné hlášení, že certifikát není ověřený nezávislou certifikační autoritou. Protože výše uvedeným postupem jste vytvořili tzv. self-signed certifikát. Prohlížeči je třeba potvrdit, že tento váš vlastní certifikát skutečně chcete použít a že mu důvěřujete. Například v Internet Exploreru je třeba na dotaz *Chcete pokračovat* kliknout na tlačítko *Ano*. V prohlížeči Firefox kliknout na "*Vím o co se jedná / Přidat výjimku / Uložit výjimku trvale / Schválit bezpečnostní výjimku*". Příště se již dotaz zobrazovat nebude. V prohlížeči Chrome je třeba kliknout na *Přesto pokračovat*, aby se stránka zobrazila. U Safari pak *Zobrazit certifikát*, zatrhnout „*Vždy důvěřovat ...*“, potvrdit tlačítkem *Pokračovat* a případně zadat heslo. Postupy se mohou v různých verzích prohlížečů lišit, princip je ale stejný - potvrdit, že stránku chcete otevřít, přestože certifikát není ověřen cizí (placenou) autoritou. Kdyby Vám tato skutečnost vadila, musíte si do Apache nahrát (místo bodu 1) komerční certifikát a případně použít i silnější šifrování.



## Přechod na TLS v1.2

níže uvedený postup vyžaduje Docházku 3000 verze 8.37 nebo vyšší

Od roku 2020 přestávají webové prohlížeče podporovat starší kryptografické protokoly. Tedy protokoly TLS verzí 1.0 a 1.1 s tím, že nadále budou podporovány jen TLS 1.2 a novější. Například Firefox verze 81 sice ještě umožní povolit TLS 1.0, ale zobrazuje následující varovné hlášení:

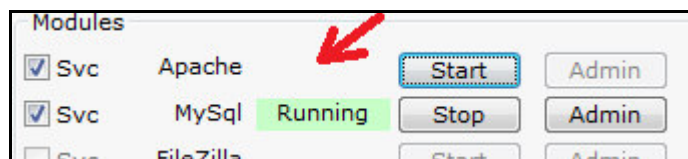


a aby se stránka načetla, musíte dolním tlačítkem TLS 1.0 povolit. Do budoucna však prohlížeče podporu těchto starších protokolů pravděpodobně úplně zruší, takže níže uvedený postup zajistí přechod Docházky na vyšší verzi TLS 1.2

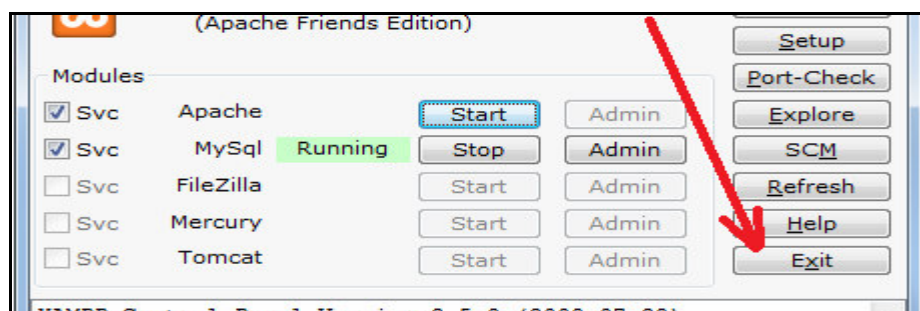
A) zastavte webový server Apache tak, že spustíte program `c:\apache\xampp-control.exe` a kliknete v něm na tlačítko *Stop* pro server Apache:



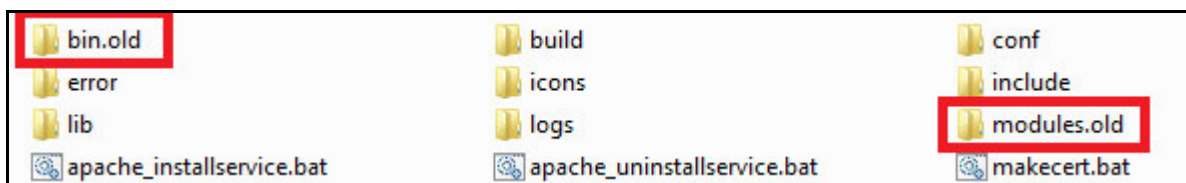
Vyčkáte, až se apache zastaví, což se pozná tak, že v jeho řádku zmizí zelený nápis *Running*



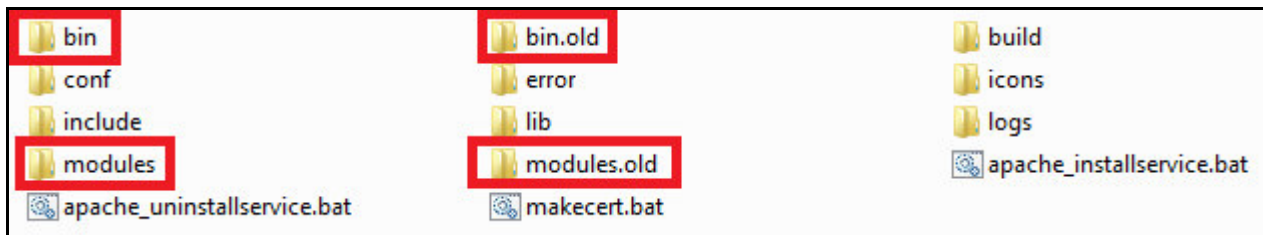
Nakonec program *Xampp-Control* ukončíte tlačítkem *Exit*



B) na disku C:\ ve složce c:\apache\apache\ přejmenujte složku bin na bin.old a dále složku modules přejmenujte na modules.old



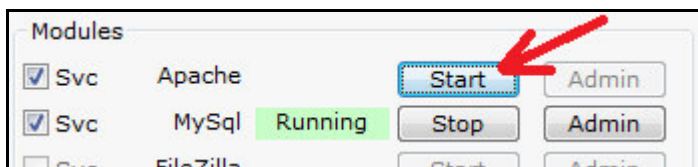
C) z instalačního nebo aktualizacího CD docházky verze 8.37 či vyšší ze složky \ostatni\tls1\_2\ rozzipujte soubor apache\_2\_2\_23.zip na disk C:\ do složky c:\apache\apache\ čímž zde vzniknou nové složky bin a modules, takže obsah c:\apache\apache\ pak bude tento:



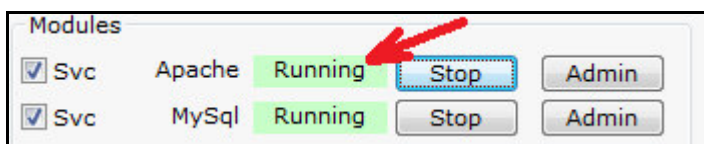
Pokud CD nemáte, lze zip soubor stáhnout zde:

[https://www.dochazka.eu/dochazka3000/download/apache\\_2\\_2\\_23.zip](https://www.dochazka.eu/dochazka3000/download/apache_2_2_23.zip)

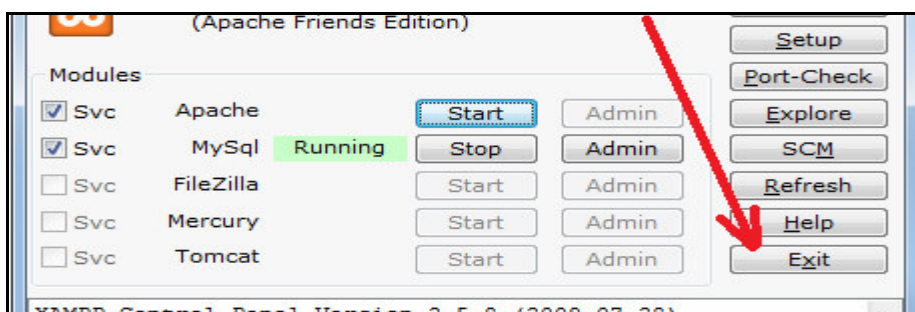
D) Opět nastartujete webový server Apache tak, že spustíte program c:\apache\xampp-control.exe a kliknete v něm na tlačítko Start pro server Apache:



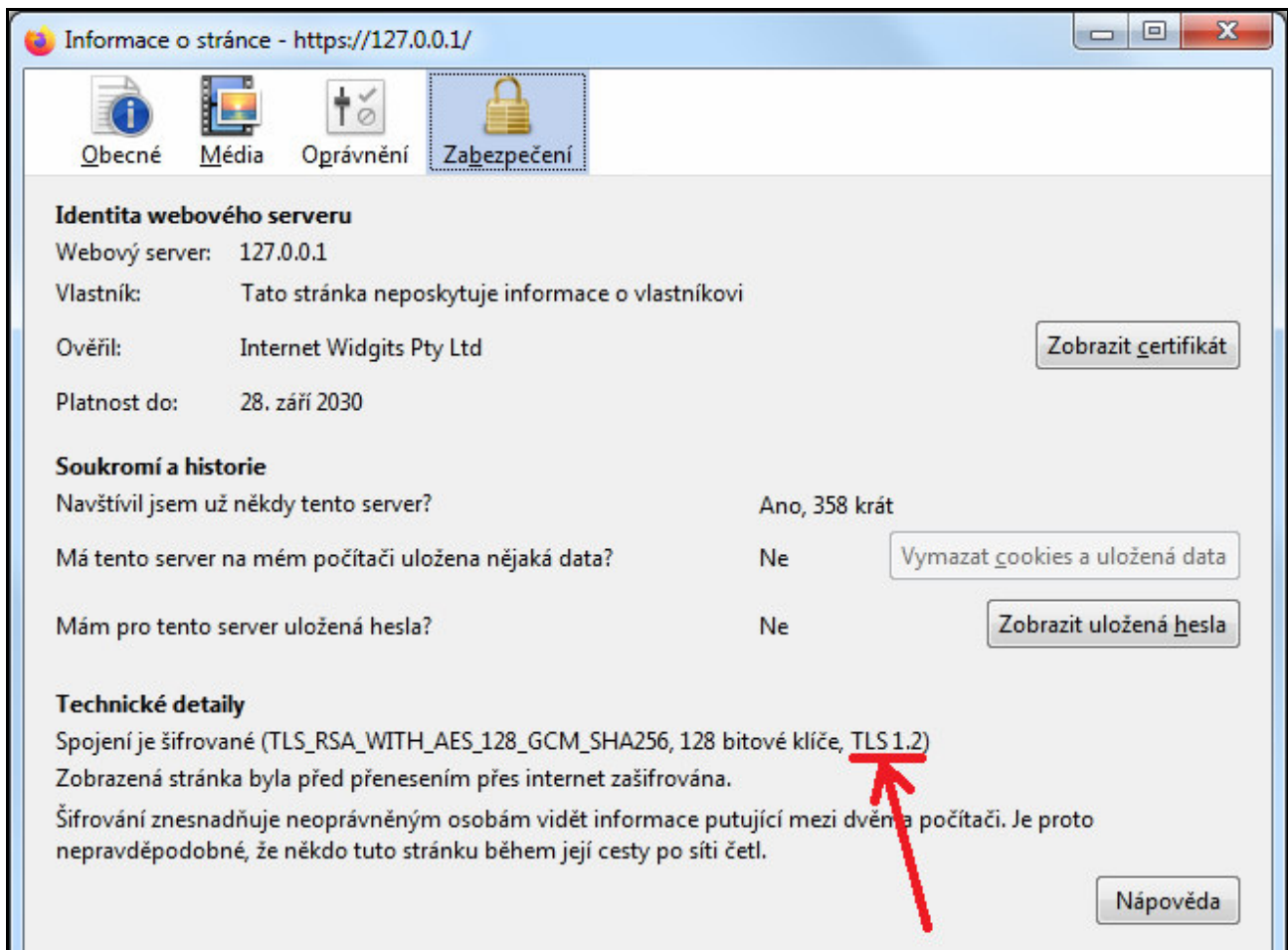
Vyčkáte, až se Apache spustí, což se pozná tak, že se v jeho řádku objeví zelený nápis Running



Nakonec program Xampp-Control opět ukončíte tlačítkem Exit



E) nyní by již měl prohlížeč podporovat spojení přes TLS verze 1.2 Viz obrázek na další straně. Samozřejmě jen v případě, že jste provedli i body 1 až 5 z úvodních stran návodu.



Volitelně lze zakázat starší verze TLS tak, že se do `c:\apache\apache\conf\httpd.conf` přidá dole pod řádek `SSL Engine On` nový řádek s tímto obsahem: `SSLProtocol -all +TLSv1.2` což zakáže všechny protokoly kromě TLS verze 1.2 (ovšem pak nebudou fungovat starší prohlížeče)

Výše uvedený postup přechodu na TLS v.1.2 ovšem vyžaduje docházkový systém ve verzi 8.37 nebo vyšší. Pokud máte nižší číslo verze, což zjistíte na úvodní obrazovce, kde je uvedeno zelenou barvou písma vedle barevného loga, nepokračujte a nejprve objednejte aktualizací CD.

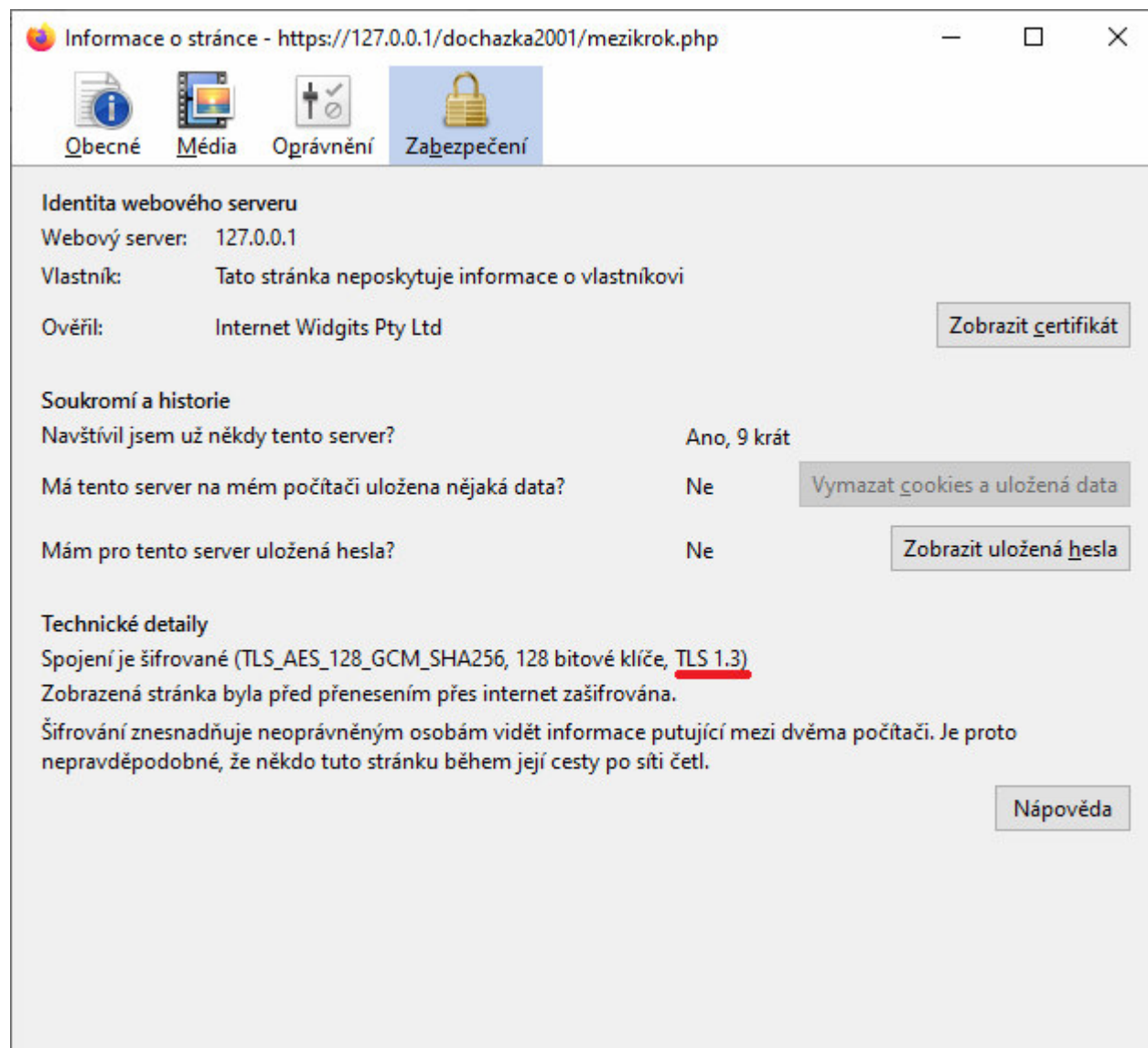


Aktualizaci Docházky 3000 na verzi 8.37 nebo vyšší, která TLS 1.2 podporuje, objednáte přímo v programu přes administrátorské menu *E-shop / Aktualizace SW Docházka 3000 / Koupit*



## **Přechod na TLS v1.3 a Apache 2.4.59** níže uvedený postup vyžaduje Docházku 3000 od verze 9.48

Pokud by byla požadovaná ještě vyšší úroveň zabezpečení, nebo by audit SW vyhodnotil původní verzi webserveru Apache dodávanou na instalačním disku jako nevyhovující, lze přejít na novou verzi Apache 2.4.59 dle postupu z příručky na instalačním či aktualizacím CD Docházky od verze programu 9.48 ve složce /Prirucky v souboru *Zmena\_webserveru.pdf* v části nazvané *Provoz docházky s novým Apache verze 2.4.59* a tato verze již obsahuje i zprovozněný šifrovaný přenos dat s protokolem https a zabezpečení odpovídající nejnovějším normám.



Informace o stránce - https://127.0.0.1/dochazka2001/mezikrok.php

Obecné Média Oprávnění **Zabezpečení**

**Identita webového serveru**  
Webový server: 127.0.0.1  
Vlastník: Tato stránka neposkytuje informace o vlastníkovi  
Ověřil: Internet Widgits Pty Ltd [Zobrazit certifikát](#)

**Soukromí a historie**  
Navštívil jsem už někdy tento server? Ano, 9 krát  
Má tento server na mém počítači uložena nějaká data? Ne [Vymazat cookies a uložená data](#)  
Mám pro tento server uložena hesla? Ne [Zobrazit uložena hesla](#)

**Technické detaily**  
Spojení je šifrované (TLS\_AES\_128\_GCM\_SHA256, 128 bitové klíče, TLS 1.3)  
Zobrazená stránka byla před přenesením přes internet zašifrována.  
Šifrování znesnadňuje neoprávněným osobám vidět informace putující mezi dvěma počítači. Je proto nepravděpodobné, že někdo tuto stránku během její cesty po síti četl. [Nápověda](#)

Pokud by bezpečnostní audit vyhodnotil jako nevyhovující i původní verzi databázového serveru MySQL, tak postup na novou verzi MariaDB 10.3 naleznete na instalačním či aktualizacím CD Docházky od verze programu 9.48 ve složce /Prirucky v souboru *Reseni\_problemu\_sw.pdf* v bodě 23.

## **Směrnice NIS2**

Od verze programu 9.50 jsou v programu k dispozici funkce a postupy pro splnění požadavků směrnice NIS2, které zahrnují změnu celhé prostředí tak, aby systém využíval nejnovější komponenty (Apache, MySQL) a poskytl informace pro podporu dodržení požadavků směrnice NIS2. Podrobný návod je od verze 9.50 v menu *Firma / Návod PDF / Směrnice NIS2*.





## Vynucení přihlašování do docházky přes šifrovaný protokol HTTPS

Od verze programu 9.48 lze vynutit přesměrování přihlašovacího dialogu na šifrovaný HTTPS protokol. Pokud administrátor nakonfiguruje webový server docházky dle výše uvedených postupů na podporu šifrovaného datového přenosu pomocí protokolu HTTPS, lze v programu od verze 9.48 vynutit přesměrování přihlašovacího dialogu z nešifrovaného protokolu http na šifrovaný https, takže pak se uživatelé budou vždy přihlašovat přes zabezpečené datové spojení. Slouží k tomu nová konfigurační volba "Přesměrovat úvodní dialog pro přihlašování do programu na šifrovaný protokol HTTPS" dostupná v administrátorském menu "Firma / Editace údajů".


Přesměrovat úvodní dialog pro přihlašování do programu na šifrovaný protokol HTTPS:

Tímto tedy lze zvýšit zabezpečení SW docházky tak, že po síti budou mezi počítačem uživatele a serverem docházky chodit data v šifrované podobě. Pokud tedy vstoupí na úvodní stránku docházky přes nešifrované http, program je během 3 vteřin přesměruje na šifrované https.

Volba pro přechod na https v nastavení firmy je dostupná jen pokud je administrátor přihlášený přes šifrovaný přenos s https. Není-li tato konfigurace webserveru provedena nebo když admin. přistupuje do konfigurace údajů firmy přes nešifrované http, nelze v nastavení firmy přesměrování z http na https zapnout a volba je vyšeděná:

Přesměrovat úvodní dialog pro přihlašování do programu na šifrovaný protokol HTTPS:

Nebo kdyby časem přestal https protokol fungovat (například po migraci serveru, vypršení platnosti certifikátu, chybě konfigurace ssl, a podobně), nezablokuje se přihlášení do docházky, ale zaměstnancům se zobrazí na 4 vteřiny tlačítko pro přihlášení přes nešifrované http, aby se jim přístup do programu chybou konfigurace nezablokoval úplně.

<p><b>Přesměrování na šifrovaný protokol HTTPS</b></p> <p>Administrátor docházky nastavil v konfiguraci programu přesměrování z nešifrovaného protokolu http na šifrovaný https. Proto vyčkejte 3 vteřiny a přihlašovací dialog se zobrazí přes šifrovaný datový přenos.</p> <p>Čekejte </p> <p><input type="button" value="Přejít na šifrované HTTPS"/></p>	<p>Pokud by se přechod na šifrovaný přenos přes https nepovedl a prohlížeč by vám zobrazil chybové hlášení, například protože vypršel certifikát nebo administrátor ve webovém serveru docházky nedokončil konfiguraci pro https a podobně, můžete přes tlačítko níže přejít na nešifrovanou verzi přihlašovacího dialogu s protokolem http.</p> <p><input type="button" value="Přejít na NEšifrované HTTP"/></p>
-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

Výše uvedenými postupy jste tedy dosáhli toho, že veškerý přenos dat posílaných po síti mezi prohlížečem na PC klienta a docházkovým serverem (včetně zadávaných hesel) je vždy šifrován, pokud v adrese uvedete https. Zároveň je povolen i nešifrovaný protokol http, který je nutný pro přenos dat z terminálů, fungování rozhraní webapi, výpočty sestav výsledovka, výkaz a další, které využívají vzájemná zpětná volání výpočetních skriptů (jejich data však neputují přes síť). To, zda se uživatelé připojují přes HTTPS dohledáte v menu „Firma / Historie logování“, sloupeček HTTPS.



Pokud byste chtěli šifrování přenosu vypnout a vrátit se k původnímu nastavení (jen protokolu http), stačí v souboru `C:\apache\apache\conf\httpd.conf` dole vymazat řádky přidané v bodě 2, restartovat Apache dle bodu 3 a odkazy na docházku opět upravit tak, aby neobsahovaly https, ale místo toho původní http (stačí tedy smazat písmeno s).

### **Řešení problémů:**

A) Pokud máte Apache web server přeměrovaný na jiný port než 80, je třeba v bodě 2 upravit položku `<VirtualHost *:80>` tak, že místo 80 uvedete Vámi používané číslo portu. Jinak nebude fungovat nešifrované spojení, které se používá pro přenos dat z terminálů a nemusí fungovat ani tvorba některých sestav (výsledovka, výkaz) či exporty do mezd a podobně.

B) Platnost certifikátu je 10 let. Po této době certifikát přestane platit a připojení https protokolem nebude dále možné. Aby šlo https protokol i poté používat, musíte vygenerovat certifikát nový. Případně revokovat stávající při změně certifikátu dříve.

C) Nezapomeňte odblokovat port 443 ve firewallu hlavního PC docházky. Viz PDF příručka „Přístup z jiných PC“. Jinak bude https fungovat pouze na serveru, ale z jiného počítače se nebude možné do docházky přes https připojit, takže by celý výše uvedený postup ztratil na významu.

D) Jestli Vám vadí varovná hlášení prohlížečů ohledně použití tohoto jednoduchého self-signed certifikátu, který není ověřený nezávislou autoritou, nebo chcete používat silnější šifrování, najdete na webu postupy pro použití placeného certifikátu. Ty mají sice kratší platnost, jejich tvorba je složitější a silnější šifrování více výpočetně zatěžuje docházkový server, ale vše pak bude odpovídat bezpečnostním standardům a prohlížeče nebudou zobrazovat varovná hlášení. U větších firem tento postup rozhodně doporučujeme.

E) Pokud šifrované HTTPS spojení používat nechcete, ale vadí vám varovná hlášení webových prohlížečů při zadávání hesla (např. Mozilla Firefox od verze 52), je možné tato hlášení v prohlížeči zakázat. U Firefoxu stačí zadat do řádku adresy text `about:config`, potvrdit varování, najít položku `“security.insecure_field_warning.contextual.enable“` a dvojklikem jí zakázat (nastavit na `false`).

F) S HTTPS nefunguje analytický modul OLAP v menu „Zaměstnanci / Prohlížení docházky / Analýza dat – OLAP / Přejít do modulu OLAP...“. Při používání tohoto modulu je třeba se do docházky přihlásit přes webovou adresu obsahující `http://` a tedy nikoli šifrované `https://`