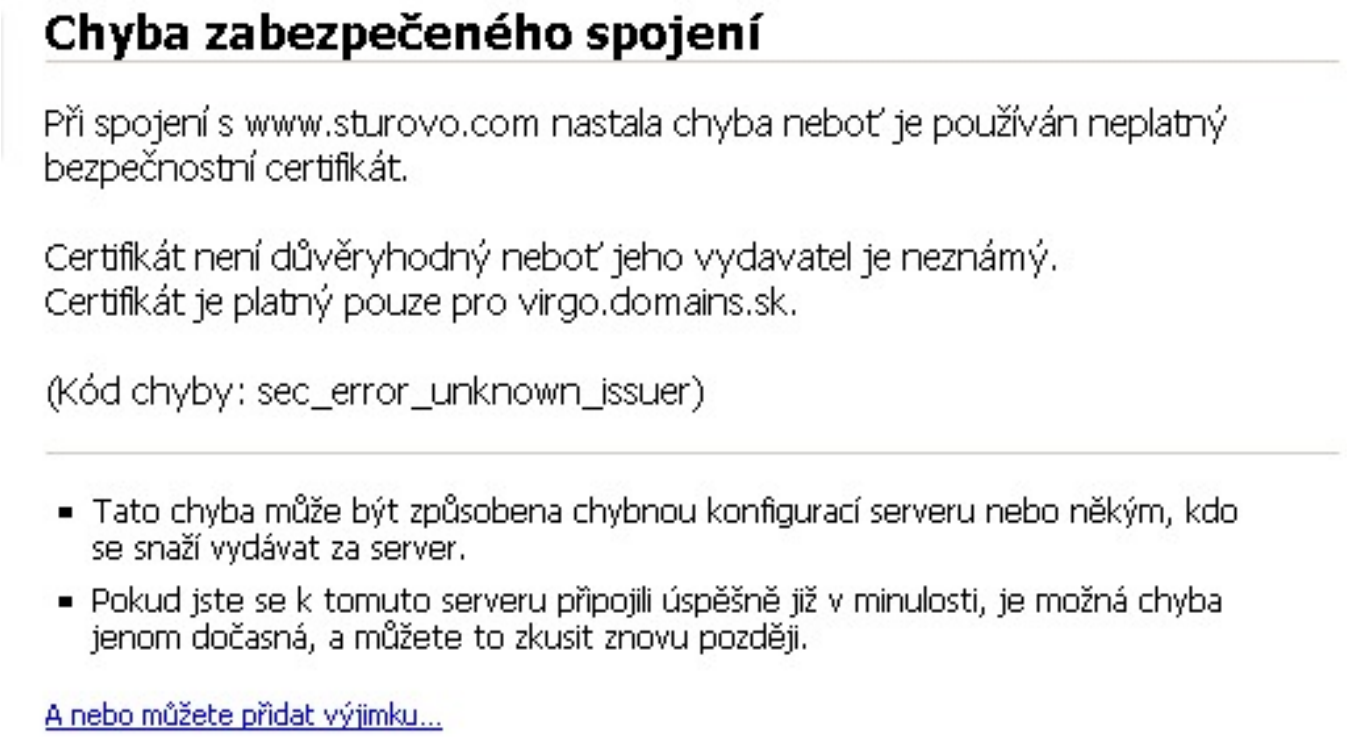
posted by Willant on 5. február 2009 - 14:45
14.02.2009 - posledná úprava článku.

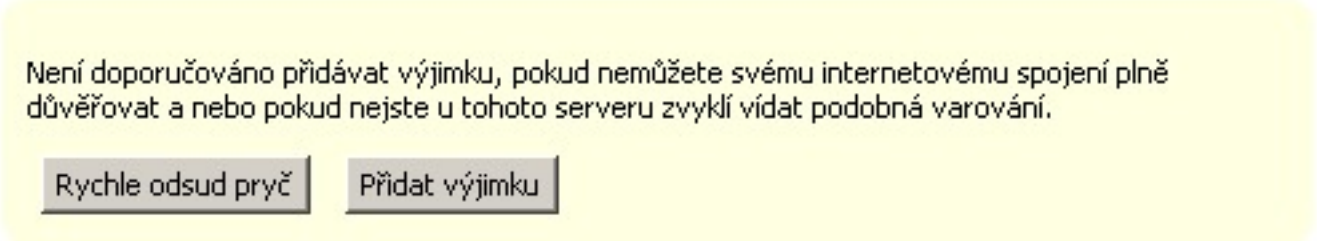
Ako si aktivovať natrvalo HTTPS prístup na našu stránku **[1]**

Výhoda SSL spojenia je hlavne to, že komunikácia je od vášho počítača až k serveru zašifrovaná protokolom SSL.

Po kliknutí na odkaz https:// by sa vám malo zobraziť toto okno.

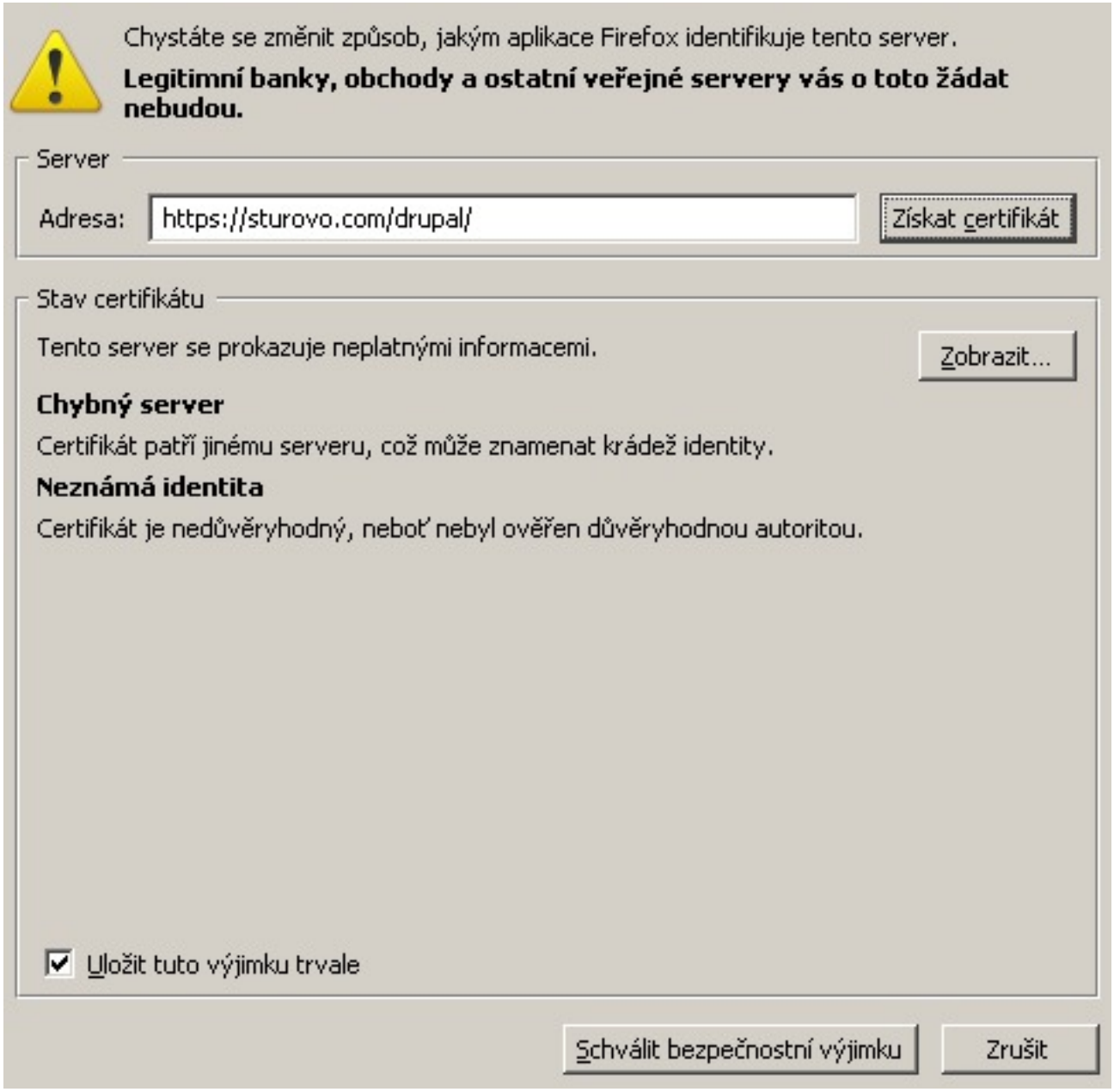


Je to preto, lebo je to len spoločný serverový certifikát a certifikát nie je vystavený na doménu www.sturovo.com [2] Prehliadač firefox sa vás snaží takto varovať. Tu si kliknite na "pridať výnimku". Ďalším krokom je potvrdenie pridania tejto výnimky. Je to tlačítko na ľavej strane PRIDAT VÝNIMKU.



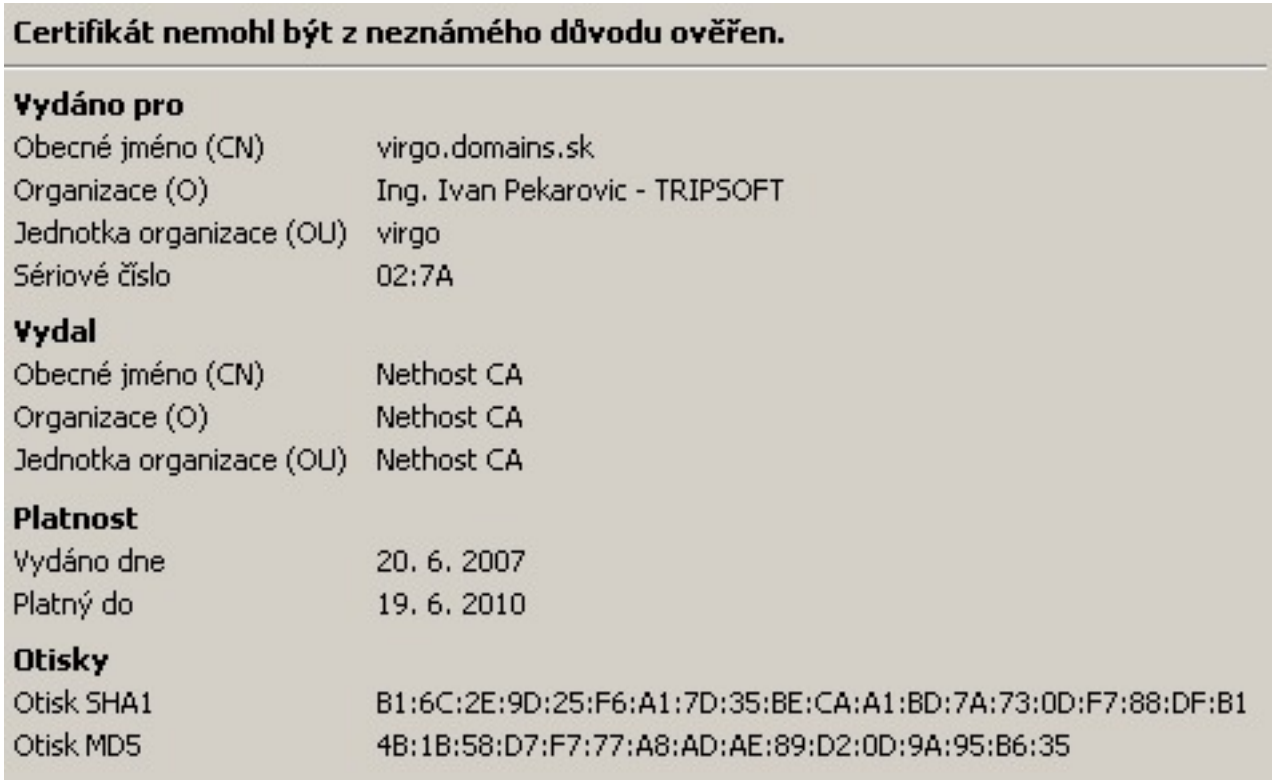
Zobrazí sa vám stránka s certifikátom, kde si musíte tlačítkom naľavo od adresy získať certifikát. Po vypísaní "chybní server a neznáma identita" treba schváliť bezpečnostnú výnimku. Chybný server a neznáma identita je len, preto lebo certifikát nie je vystavený na doménu, ale je to centrálny serverový certifikát, ktorý môžu vlastniť viaceré domény, takto je to lacnejšie.

Původně oznamovalo problém vyskakovací okno, nyní je přes celou plochu prohlížeče zobrazeno varování, které doporučuje nepoužívat problematickou internetovou stránku. Do tohoto varování jsou však zahrnuty i (nekomerční) certifikáty, které nejsou registrovány u certifikačních autorit, které Microsoftu platí za umístění jejich veřejného klíče v úložišti prohlížeče. Chování Internet Exploreru tak nutí správce serverů kupovat komerční certifikáty pro jejich webové servery za cenu 10 až 1200 USD za rok.



Samostatný certifikát by ma stál asi 120 € na dva roky. To je v rámci tohto neziskového projektu veľmi drahé.

Zdroj: wikipedia.org
Secure Sockets Layer, SSL (doslova vrstva bezpečných socketů) je protokol, resp. vrstva vložená mezi vrstvu transportní (např. TCP/IP) a aplikační (např. HTTP), která poskytuje zabezpečení komunikace šifrováním a autentizaci komunikujících stran.



Certifikát nemohl být z neznámého důvodu ověřen.

Vydáno pro	
Obecné jméno (CN)	virgo.domains.sk
Organizace (O)	Ing. Ivan Pekarovic - TRIPSOFT
Jednotka organizace (OU)	virgo
Sériové číslo	02:7A
Vydal	
Obecné jméno (CN)	Nethost CA
Organizace (O)	Nethost CA
Jednotka organizace (OU)	Nethost CA
Platnost	
Vydáno dne	20. 6. 2007
Platný do	19. 6. 2010
Otisky	
Otisk SHA1	B1:6C:2E:9D:25:F6:A1:7D:35:BE:CA:A1:BD:7A:73:0D:F7:88:DF:B1
Otisk MD5	4B:1B:58:D7:F7:77:A8:AD:AE:89:D2:0D:9A:95:B6:35

Protokol SSL se nejčastěji využívá pro bezpečnou komunikaci s internetovými servery pomocí HTTPS, což je zabezpečená verze protokolu HTTP. Po vytvoření SSL spojení (session) je komunikace mezi serverem a klientem šifrovaná a tedy zabezpečená.

Ustavení SSL spojení funguje na principu asymetrické šifry, kdy každá z komunikujících stran má dvojici šifrovacích klíčů - veřejný a soukromý. Veřejný klíč je možné zveřejnit a pokud tímto klíčem kdokoliv zašifruje nějakou zprávu, je zajištěno, že ji bude moci rozšifrovat jen majitel použitého veřejného klíče svým soukromým klíčem.

Ustavení SSL spojení (SSL handshake, tedy potřásání rukou) pak probíhá následovně:

Klient pošle serveru požadevek na SSL spojení, spolu s různými doplňujícími informacemi (verze SSL, nastavení šifrování atd.).
Server pošle klientovi odpověď na jeho požadavek, která obsahuje stejný typ informací a hlavně certifikát serveru.
Podle přijatého certifikátu si klient ověří autentičnost serveru. Certifikát také obsahuje veřejný klíč serveru.
Na základě dosud obdržených informací vygeneruje klient základ šifrovacího klíče, kterým se bude šifrovat následná komunikace. Ten zašifruje veřejným klíčem serveru a pošle mu ho.
Server použije svůj soukromý klíč k rozšifrování základu šifrovacího klíče. Z tohoto základu vygenerují jak server, tak klient hlavní šifrovací klíč.
Klient a server si navzájem potvrdí, že od teď bude jejich komunikace šifrovaná tímto klíčem. Fáze handshake tímto končí.
Je ustaveno zabezpečené spojení šifrované vygenerovaným šifrovacím klíčem.
Aplikace od teď dál komunikují přes šifrované spojení. Například POST požadavek na server se do této doby neodešle.

HTTPS
HTTPS (Hypertext Transfer Protocol Secure) je zabezpečená verzia HTTP, komunikačného protokolu World Wide Web. Bol vyvinutý firmou Netscape Communications Corporation pre poskytovanie overenia a šifrovanej komunikácie.

Namiesto používania jednoduchej textovej komunikácie, HTTPS šifruje prenos dát použitím SSL (Secure Socket Layer) protokolu alebo TLS (Transport Layer Security) protokolu a tým zaisťuje

primeranú ochranu pred odpočúvaním komunikácie a pred útokom „Man in the middle“. Pre HTTPS komunikáciu sa štandardne používa TCP/IP port 443.

Adresa zdroja (modified on 14.02.2009 - 21:25):http://www.sturovo.com/drupal/content/ako-si-aktivovat-natrvalo-https-pristup-na-nasu-stranku#comment-0

Odkazy
[1] http://www.sturovo.com/drupal/content/ako-si-aktivovat-natrvalo-https-pristup-na-nasu-stranku
[2] http://www.sturovo.com