SSL certifikáty

Postup nasazení certifikátu SSL

Pro možnost provozu webu přes HTTPS je nutné nasadit SSL certifikát.

Z bezpečnostních důvodů je nejlepším řešením vygenerovat certifikační žádost (CSR) a klíč přímo na serveru, na kterém bude certifikát nasazen. Klíč by neměl opustit server, rozhodně by neměl být posílán e-mailem, kdyby se dostal do nepovolaných rukou, je s jeho pomocí možné dekryptovat šifrovaný HTTPS provoz.

Pro vygenerování klíče a CSR potřebuje technická podpora znát následující informace (vyplněno vzorovými daty):

Country Name (2 letter code) [AU]:CZ
State or Province Name (full name) [Some-State]:Czech Republic
Locality Name (eg, city) []:Praha
Organization Name (eg, company) [Internet Widgits Pty Ltd]:Nejaka Firma s.r.o.
Organizational Unit Name (eg, section) []:Internet
Common Name (e.g. server FQDN or YOUR name) []:www.nejakadomena.cz
Email Address []:info@nejakadomena.cz

Nejdůležitější je položka Common Name, která udává doménové jméno, na které je certifikát vystavený.
Většina certifikačních autorit zahrne do Common Name doménu s www i bez www bezplatně automaticky.

Pokud budete žádat o vystavení wildcard certifikátu (pro všechny subdomény), vyplňte hvězdičku, tedy například *.nejakadomena.cz.

V případě, kdy máte k dispozici SSH přístup na server, může si sami vygenerovat klíč a certifikační žádost pomocí následujícího příkazu:

openssl req -out www.nejakadomena.cz.csr -new -newkey rsa:2048 -nodes -keyout www.nejakadomena.cz.key

V průběhu generování jsou vyžadovány výše uvedené údaje a výsledkem jsou dva soubory, certifikační žádost s příponou .csr a klíč .key.

Ohledně vystavení a podepsání certifikátu důvěryhodnou certifikační autoritou je zde možnost učinit tak prostřednictvím našeho obchodního oddělení.

Druhá možnost je svépomoci nechat vystavit certifikát u kterékoliv důvěryhodné certifikační autority (ComodoCA, RapidSSL, Symantec, GoDaddy..).

V obou případech bude vyžadována certifikační žádost CSR, na základě které bude certifikát vystaven.

Pro samotné nasazení vystaveného certifikátu na běžný managed server je nutné vznést požadavek na technickou podporu. Tato operace si vyžádá úpravu nastavení webserveru a jeho reload.

SSL certifikáty

Při obdržení požadavku na nasazení certifikátu musí technická podpora mít k dispozici samotný certifikát, privátní klíč a certifikát vystavující certifikační autority.

V PLESKu má zákazník možnost si certifikát nasadit sám.
U požadované domény, v sekci 'Websites & Domains', dále 'Secure your sites' => 'SSL Certificates' => 'Add SSL Certificate' je nutné nahrát klíč, certifikát a certifikáty certifikační autority, případně nakopírovat obsah těchto souborů jako prostý text do připravených formulářových polí.

Pokud je certifikát takto nahrán, ještě není pro konkrétní web nasazen. V sekci 'Websites & Domains' se nachází položka 'Hosting settings' a oddíl 'Security'. Zde je nutné zaškrtnout políčko 'SSL support' (pokud není) a certifikát z výsuvného menu vybrat, uložit a potvrdit.

Unikátní ID: #1009
Autor: Technicka podpora
Aktualizováno: 2016-04-30 00:38