Proces generování SSL certifikátu

SSLS

1 Vygenerujete pár privátního a veřejného klíče (tzv. CSR).

Privátní klíč je tajný, nikomu ho nedávejte! Uložte si ho, budete ho potřebovat k instalaci SSL certifikátu na server. Bez privátního klíče je SSL certifikát nepoužitelný.

Privátní klíč

+

CSR

CSR žádost obsahuje mj. **veřejný klíč** a **doménu**, pro kterou chcete SSL certifikát vystavit.

Doména je uvedena v poli CN (Common Name).

2 CSR žádost poskytněte při aktivaci na **www.ssls.cz**

V této fázi může certifikační autorita požadovat ověření vaší kontroly nad doménou.

U DV certifikátů stačí provést autorizaci kliknutím na odkaz v e-mailu, který vám zašle certifikační autorita.

U certifikátů s ověřením organizace (OV) nebo rozšířeným ověřením (EV) můžete být vyzváni k doložení některých dokumentů.

CSR

Certifikační autorita

Certifikační autorita žádost prověří a je-li vše v pořádku, pak ji tzv. **podepíše** svým důveryhodným klíčem, čímž fakticky vystaví SSL certifikát.

Certifikační autorita **vystaví SSL certifikát**.

3

Instalace na server

Privátní klíč, SSL certifikát a CA certifikát nainstalujete na server.

Privátní klíč

+

SSL certifikát

+

CA certifikát

CA certifikát (**intermediate certifikát**) získáte společně s SSL certifikátem.

Jak rozlišit jednotlivé soubory?

Privátní klíč

Začíná řádkem:
`-----BEGIN RSA PRIVATE KEY-----`

CSR

Začíná řádkem:
`-----BEGIN CERTIFICATE REQUEST-----`

SSL certifikát

CA certifikát

Začínají řádkem:
`-----BEGIN CERTIFICATE-----`

www.ssls.cz