

Rozšířené ověření (extended validation)

Poslední aktualizace 21 srpna, 2024

Certifikáty s rozšířeným zabezpečením jsou uživatelsky jasně deklarovány jako důvěryhodné. V prohlížečích se projevují výrazným zeleným adresním řádkem a ikonkou zámečku. V ní se každý dozví o organizaci, která certifikát vlastní i certifikační autoritě, která ho vystavila.

Pro zajištění té nejvyšší bezpečnosti je postup ověření EV SSL důkladnější, veškeré informace jsou zjišťovány z více zdrojů, proto z tohoto důvodu trvá vystavení certifikátu déle než u běžných SSL s ověřením organizace. Proces má čtyři kroky, ověření majitele domény, ověření společnosti, ověření zaměstnaneckého poměru kontaktní osoby a telefonické ověření kontaktní osoby.

1. krok zaslání dokumentů

Comodo vyžaduje podepsání těchto dokumentů

[Certificate Request Form](#)

[EV SSL Subscriber Agreement](#)

[Certificate Request Form \(příklad\)](#)

[EV SSL Subscriber Agreement \(příklad\)](#)

Symantec/GeoTrust/Thawte do 3 dnů obdržíte emailem od certifikační autority formuláře k potvrzení

2. krok ověření společnosti: certifikační autorita si ověřuje informace o společnosti, která bude majitelem SSL certifikátu v obchodním rejstříku.

3. krok ověření domény: [ověření domény](#)

4. krok telefonické ověření společnosti a zaměstnance

Kontaktní údaje získává certifikační autorita z databází firem třetích stran jako například www.zlatestranky.cz. Následuje telefonické ověření autorizační osoby, která podepisovala dokumenty – viz bod 1.

Poznámka:

Pokud CA (certifikační autorita) není schopna některé informace dohledat, vyžádá si

dodatečné ověření. Vystavení certifikátu se pak v tomto případě může prodloužit.