ZABEZPEČENIE STRÁNOK DCCSSRO.SK BEZPEČNOSTNÝM CERTIFIKÁTOM

https://www.dccssro.sk

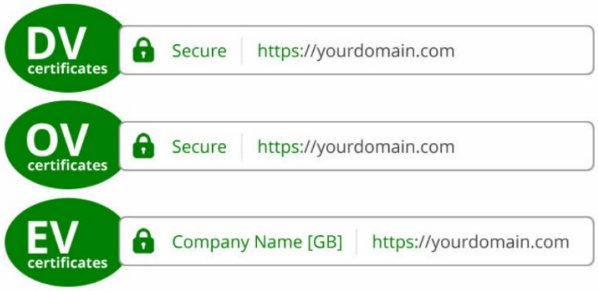
Pri prístupe na stránky dccssro.sk prebieha celá komunikácia medzi Vami a stránkami dccssro.sk prostredníctvom zabezpečeného hypertextového protokolu skr. HTTPS. Tento predstavuje zabezpečenú verziu HTTP, komunikačného protokolu World Wide Web (www). Protokol HTTPS bol vyvinutý spoločnosťou Netscape Communications Corporation pre poskytovanie overenia a šifrovanej komunikácie.

Zabezpečený protokol HTTPS zabezpečuje, že pri vzájomnej komunikácii, alebo výmene dát medzi dvoma komunikačnými bodmi nie je používaná jednoduchá textová komunikácia, ale prenos dát je šifrovaný použitím protokolu SSL alebo TLS. V prípade stránok dccssro.sk a dccssro.cz sa jedná o protokol TLS, ktorý je nástupcom protokolu SSL 3.0. Prechod k protokolu TLS bol spôsobený chybami, ktoré v sebe niesol protokol SSL 3.0 (a jeho predchodcovia) a ktoré znamenali zásadné zníženie bezpečnosti šifrovanej komunikácie.

V SKRATKE

Čo je SSL certifikát?

SSL je skratka pre označenie protokolu Secure Sockets Layer. Počas rokov používania sa aj pre digitálne bezpečnostné certifikáty zaužívalo obdobné označenie, ktoré ale z pohľadu správnosti nie je je presné. Webstránky s platným SSL certifikátom sú vo väčšine prehliadačov označené zelenou URL adresou a ikonou zámku.



Tie hovoria o ich bezpečnosti a vzbudzujú v návštevníkoch dôveru v to, že ich pripojenie k tomuto webu bude bezpečné.

V SKRATKE

Čo musí obsahovať platný certifikát?

Platný SSL certifikát musí obsahovať niekoľko informácií:

- informáciu o vydavateľovi SSL certifikátu, ktorý je označovaný za certifikačnú autoritu (CA). Jedná sa o organizáciu, ktorej návštevník (a v prípade overenej CA aj IT svet) verí,
- svoje sériové číslo,
- dátum expirácie (certifikáty zvyčajne platia 1 až 3 roky),
- kópiu verejného kľúča majiteľa certifikátu,
- digitálny podpis certifikačnej autority.

V SKRATKE

Protokoly SSL a TLS, digitálny certifikát SSL a jeho miesto v zabezpečenej komunikácii v online prostredí

Na to aby bola komunikácia naozaj zabezpečená, sú využívané digitálne bezpečnostné certifikáty označované ako SSL certifikáty. Pripojenie zabezpečené SSL certifikátom chráni šifrovaním všetky prenášané dáta – napríklad prenášané údaje a dáta, platobné údaje, či vašu online komunikáciu. Pridanou hodnotou pri kúpe a implementácii SSL certifikátu je napríklad zvýšená ochrana proti rôznym typom kybernetických útokov. Alebo budovanie dôveryhodnosti. Webstránky s platným SSL certifikátom sú vo väčšine prehliadačov označené zelenou URL adresou a ikonou zámku. Tie hovoria o ich bezpečnosti a vzbudzujú v návštevníkoch dôveru v to, že ich pripojenie k tomuto webu bude bezpečné.

Protokol TLS umožňuje komunikovať cez sieť mierne odlišným spôsobom ako v prípade SSL, a to to tak, aby zamedzoval možnostiam odpočúvania, manipulácie, falšovaniu správ. Protokol TLS poskytuje autentifikáciu na koncových bodoch (PC užívateľa, web server stránok) a súkromie v komunikácii používaním kryptografie.

Pri TLS je typicky autorizovaný len server (to znamená, že jeho identita je zaručená) zatiaľ čo klient ostáva neautorizovaný. To znamená, že koncový užívateľ, či už jednotlivec alebo aplikácia, si môže byť istý s kým komunikuje.

Ďalšia úroveň zabezpečenia, v ktorej si obe strany „konverzácie" môžu byť isté s kým komunikujú, je známa ako obojstranná autorizácia. Obojstranná autorizácia vyžaduje infraštruktúru verejného kľúča (public key infrastructure – PKI).

Úroveň bezpečnosti certifikátu definujú viaceré parametre:

- štandard akým bol certifikát vytvorený (napr. X.509),
- úroveň šifrovania, ktorú používa (napr. 128- alebo 256-bitová šifra),
- kryptografický spôsob vytvárania kľúčov (napr. RSA SHA s 256bit hash),
- spôsob šifrovania (napr. 2048-bitová šifra).

Základné typy SSL certifikátov podľa úrovne zabezpečenia:

Typ overenia	DV Domain Validation (overenie domény)	OV Organizational Validation (overenie organizácie)	EV Extended Validation (rozšírené overenie)
Zabezpečenie	nízke	stredné	vysoké
Čo znamená príslušný typ overenia?	CA (Certifikačná Autorita) potvrdzuje, že organizácia má danú doménu pod svojou kontrolou.	Všetko čo DV + CA (Certifikačná Autorita) prostredníctvom kmeňového zamestnanca, preverila dôveryhodnosť organizácie, ktorá danú doménu vlastní.	Všetko čo OV + CA (Certifikačná Autorita) overuje vlastníctvo organizácie, jej fyzickú adresu, kontaktné údaje a legálnu formu organizácie napr. podľa údajov v oficiálnom a verejnom registri spoločností.
Spôsob overenia organizácie – formálny postup	Pri SSL certifikáte typu DV postačuje vyplniť online formulár na stránkach CA, alebo overiť organizáciu emailom. Certifikát je následne obratom vygenerovaný a stačí ho nahrať na web.	Pri SSL certifikácie typu OV, CA kontroluje názov a adresu majiteľa certifikátu.	Pri SSL certifikáte typu EV, CA požaduje nad rámec predošlých kontrol aj zaslanie viacerých fyzických dokumentov a okrem iného vyhodnocuje aj bezpečnostné možnosti a mechanizmy organizácie.
Čas na vydanie certifikátu	V rozmedzí minút, maximálne hodín.	Niekoľko dní.	Môže presiahnuť aj niekoľko týždňov.
Ako vidíme SSL v prehliadači?	HTTPS pripojenie, ktoré indikuje zelená farba (pri niektorých prehliadačoch) a ikona zámky.	HTTPS pripojenie, ktoré indikuje zelená farba (pri niektorých prehliadačoch) a ikona zámky. SSL certifikát obsahuje aj názov majiteľa a detaily o ňom.	HTTPS pripojenie, ktoré indikuje zelená farba (pri niektorých prehliadačoch) a ikona zámky. Názov spoločnosti sa zobrazuje alebo priamo v adresnom riadku prehliadača, alebo po kliknutí na ikonu zámky.

Stránky dccssro.sk sú zabezpečené tzv. EV (Extended Validation) SSL certifikátom. EV certifikáty ponúkajú najvyššie možné zabezpečenia webových stránok. Vďaka zobrazeniu názvu spoločnosti, prakticky hneď vedľa URL adresy užívateľ ľahko uvidí, že je na správnej a nepodvrhnutej stránke. Klasický SSL certifikát zobrazuje túto informáciu až v detailoch certifikátu.

DCCS

Ak máte akékoľvek ďalšie otázky týkajúce sa bezpečnosti komunikácie so spoločnosťou DCCS, s.r.o. na internete, neváhajte a kontaktujte nás prostredníctvom emailu customer.service@dccssro.sk alebo na telefónnom čísle Zákazníckeho centra v Bratislave +421 2 5778 9440.

Ďakujeme,

Váš DCCS, s.r.o.