ZABEZPEČENÍ STRÁNEK DCCSSRO.CZ BEZPEČNOSTNÍM CERTIFIKÁTEM

DCCS

https://www.dccssro.cz

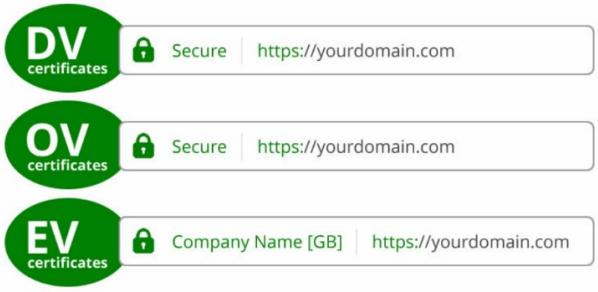
Při přístupu na stránky dccssro.cz probíhá celá komunikace mezi vámi a stránkami dccssro.cz prostřednictvím zabezpečeného hypertextového protokolu (zkr. HTTPS). Ten představuje zabezpečenou verzi HTTP, komunikačního protokolu World Wide Web (www). Protokol HTTPS byl vyvinut společností Netscape Communications Corporation pro poskytování ověření a šifrované komunikace.

Zabezpečený protokol HTTPS zajišťuje, že při vzájemné komunikaci, nebo výměně dat mezi dvěma komunikačními body není používána jednoduchá textová komunikace. Přenos dat je šifrován použitím protokolu SSL nebo TLS. V případě stránek dccssro.sk / dccssro.cz se jedná o protokol TLS, který je nástupcem protokolu SSL 3.0. Důvodem přechodu na protokol TLS byly chyby, které v sobě obsahoval protokol SSL 3.0 (a jeho předchůdci) a které znamenaly zásadní snížení bezpečnosti šifrované komunikace.

V ZKRATCE

Co je SSL certifikát?

SSL je zkratka pro označení protokolu Secure Sockets Layer. Během let používání se i pro digitální bezpečnostní certifikáty vžilo obdobné označení, které ale z pohledu správnosti není přesné. Webové stránky s platným SSL certifikátem jsou ve většině prohlížečů označené zelenou URL adresou a ikonou zámku.



To vypovídá o jejich bezpečnosti a budí v návštěvnících důvěru, že jejich připojení k tomuto webu bude bezpečné.

V ZKRATCE

Co musí obsahovat platný certifikát?

Platný SSL certifikát musí obsahovat několik informací:

- informace o vydavateli SSL certifikátu, který je označován za certifikační autoritu (CA). Jedná se o organizaci, jíž návštěvník (a v případě ověřené CA i IT svět) věří.
- své sériové číslo,
- datum použitelnosti (certifikáty obvykle platí 1–3 roky),
- kopii veřejného klíče majitele certifikátu,
- digitální podpis certifikační autority.

V ZKRATCE

Protokoly SSL a TLS, digitální certifikát SSL a jeho místo v zabezpečené komunikaci v online prostředí

Na to, aby byla komunikace opravdu zajištěna, jsou využívány digitální bezpečnostní certifikáty označované jako SSL certifikáty. Připojení zabezpečené SSL certifikátem chrání šifrováním všechna přenášená data – například přenášené údaje a data, platební údaje, nebo vaši online komunikaci. Přidanou hodnotou při koupi a implementaci SSL certifikátu je například zvýšená ochrana proti různým typům kybernetických útoků nebo budování důvěryhodnosti. Webové stránky s platným SSL certifikátem jsou ve většině prohlížečů označené zelenou URL adresou a ikonou zámku. To vypovídá o jejich bezpečnosti a budí v návštěvnících důvěru v to, že jejich připojení k tomuto webu bude bezpečné.

Protokol TLS umožňuje komunikovat přes síť mírně odlišným způsobem než v případě SSL, a to tak, aby zamezil možnostem odposlechu, manipulace, padělání zpráv. Protokol TLS poskytuje autentifikaci na koncových bodech (PC uživatele, web server stránek) a soukromí při komunikaci používáním kryptografie.

U TLS je typicky autorizovaný jen server (to znamená, že jeho identita je zaručena) zatímco klient zůstává neautorizovaný. To znamená, že koncový uživatel, ať už jednotlivec nebo aplikace, si může být jistý s kým komunikuje.

Další úroveň zabezpečení, ve které si obě strany „konverzace" mohou být jisté s kým komunikují, je známá jako oboustranná autorizace. Oboustranná autorizace vyžaduje infrastrukturu veřejného klíče (public key infrastructure – PKI).

Úroveň bezpečnosti certifikátu definuje několik parametrů:

- standard, jakým byl certifikát vytvořen
- úroveň šifrování, kterou používáme (např. 128- nebo 256-bitová šifra)
- kryptografický způsob vytváření klíčů (např. RSA SHA s 256bit hash)
- způsob šifrování (např. 2048-bitová šifra)

Základní typy SSL certifikátů podle úrovně zabezpečení:

Typ ověření	DV Domain Validation (ověření domény)	OV Organizational Validation (ověření organizace)	EV Extended Validation (rozšířené ověření)
Zabezpečení	nízké	střední	Vysoké
Co poskytuje příslušný typ ověření?	CA (Certifikační autorita) potvrzuje, že organizace má danou doménu pod svou kontrolou.	Vše, co DV + CA prostřednictvím kmenového zaměstnance prověřila, důvěryhodnost organizace, která danou doménu vlastní.	Vše, co OV + CA, dále ověřuje vlastnictví organizace, její fyzickou adresu, kontaktní údaje a legální formu organizace např. podle údajů v oficiálním a veřejném rejstříku společností.
Způsob ověření organizace – formální postup	U SSL certifikátu typu DV stačí vyplnit online formulář na stránkách CA nebo ověřit organizaci emailem. Certifikát je následně obratem vygenerován a stačí ho nahrát na web.	U SSL certifikátu typu OV kontroluje CA název a adresu majitele certifikátu.	U SSL certifikátu typu EV požaduje CA nad rámec předešlých kontrol i zaslání více fyzických dokumentů a mimo to vyhodnocuje také bezpečnostní možnosti a mechanismy organizace.
Čas pro vydání certifikátu	V rozmezí minut, maximálně hodin.	Několik dní.	Může přesáhnout i několik týdnů.
Jak vidíme SSL v prohlížeči?	HTTPS připojení, které indikuje zelená barva (v některých prohlížečích) a ikona zámku.	HTTPS připojení, které indikuje zelená barva (v některých prohlížečích) a ikona zámku. SSL certifikát obsahuje název majitele a detaily o něm.	HTTPS připojení, které indikuje zelená barva (v některých prohlížečích) a ikona zámku. Název společnosti se zobrazuje přímo v adresním řádku prohlížeče nebo po kliknutí na ikonu zámku.

Stránky dccssro.cz jsou zabezpečené tzv. EV (Extended Validation) SSL certifikátem. EV certifikáty nabízejí nejvyšší možné zabezpečení webových stránek. Díky zobrazení názvu společnosti prakticky hned vedle URL adresy uživatel snadno vidí, že je na správné a nepodvrhnuté stránce. Klasický SSL certifikát zobrazuje tuto informaci až v detailech certifikátu.

DCCS

Pokud máte jakékoli další otázky týkající se bezpečnosti komunikace se společnosti DCCS, s.r.o. na internetu, neváhejte a kontaktujte nás prostřednictvím emailu customer.service@dccssro.cz nebo na telefonním čísle Zákaznického centra v Praze +420 255 712 712.

Děkujeme,

Váš DCCS, s.r.o.