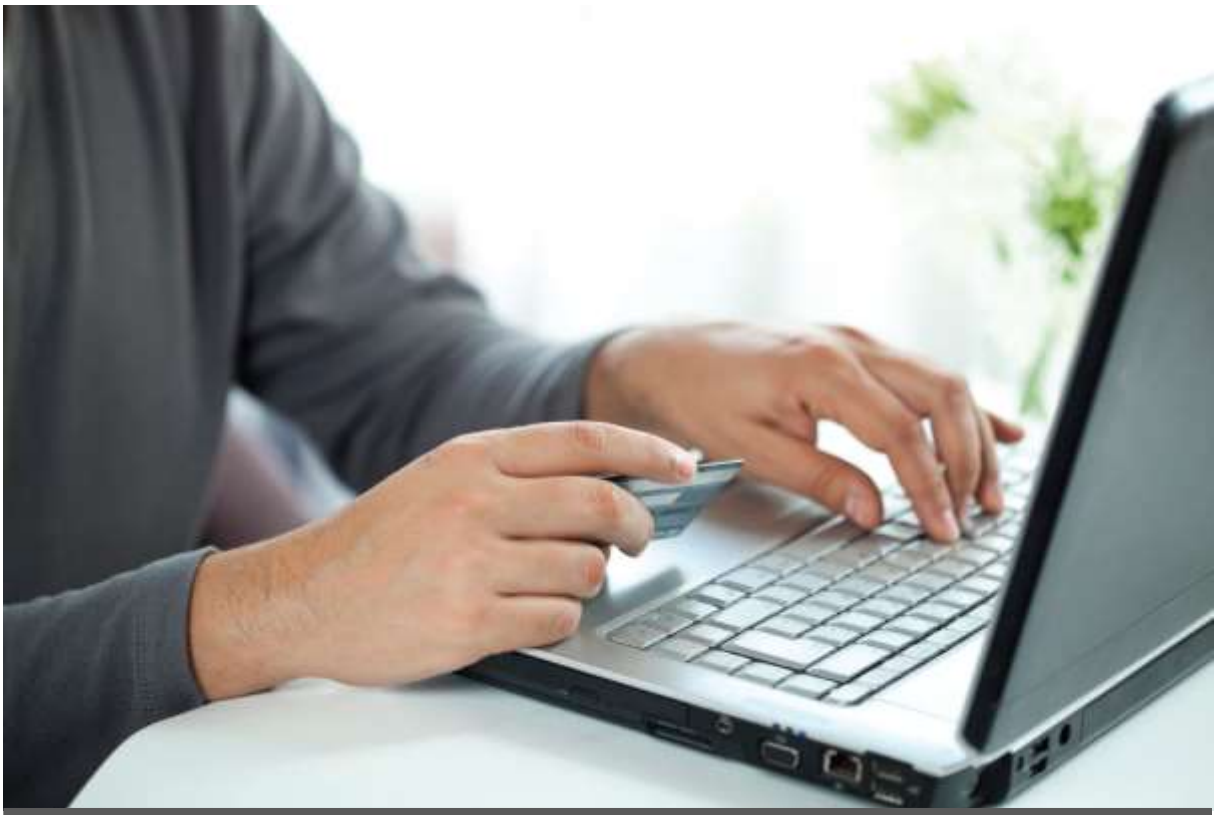


Vodič kroz proizvode Symantec Website Security

Net++ TECHNOLOGY

Sadržaj

SSL sertifikati 2

Kako SSL sertifikati rade? 2

Kome treba SSL? 3

Vrste SSL sertifikata 4

SAN sertifikati 7

Symantec Website Security Solutions 8

Premium Brend Symantec SSL Solutions 9

Norton™ Secured Seal 10

Procena ranjivosti 10

Website Malware Scanning 11

Symantec Seal-in-Search™ 11

High Value Brand Thawte SSL sertifikati 12

High Value Brand GeoTrust SSL sertifikati 13

Poređenje Website Security brendova 14

Net++ technology 15

SSL sertifikati

Secure Socket Layer (SSL) je bezbednosni protokol koji koriste Web čitači (Web browsers) i Web serveri za zaštitu podataka prilikom transfera. SSL sertifikati si mali data fajlovi koji digitalno povezuju kriptografski ključ sa podacima organizacije. U slučaju Web čitača, SSL aktivira katanac i https i omogućava bezbednu vezu od Web servera do čitača.

SSL je bezbednosni protokol koji:

- Štiti podatke korisnika prilikom transfera.
- Digitalno povezuje kriptografski ključ sa podacima organizacije.
- Štiti transakcije putem kreditnih kartica, prenos podataka, ovlašćenja za pristup sajtovima i više.
- Pruža autentifikaciju preduzeća i/ili domena.

Kako SSL sertifikati rade?

Kada Web čitač naiđe na sajt sa SSL-om:

1. **Čitač** pokušava da se poveže sa sajtom koji je obezbeđen SSL-om.
2. **Čitač** zahteva od web servera da se identifikuje.
3. **Server** šalje čitaču kopiju svog SSL sertifikata.
4. **Čitač** proverava da li je SSL sertifikat od poverenja. Ako jeste šalje poruku serveru.
5. **Server** šalje natrag digitalnu potvrdu za otpočinjanje kriptovane SSL sesije.
6. **Razmenjuju se kriptovani podaci između čitača i servera.**

Enkripcija štiti podatke u toku prenosa

Web serveri i web čitači oslanjaju se na SSL protokol za kreiranje jedinstvenog kriptovanog kanala za privatnu komunikaciju preko javnog Interneta. Svaki SSL sertifikat sastoji se od para ključeva kao i od verifikovanih informacija za identifikaciju. Javni ključ se koristi za kriptovanje podataka, a privatni ključ za njihovo dešifrovanje. Kada Web čitač krene na bezbedan domen, nivo enkripcije se uspostavlja na osnovu tipa SSL seritifikata kao i na osnovu Web čitača klijenta, operativnog sistema i kapaciteta host servera. To je razlog zašto postoje SSL sertifikati sa različitim rasponom enkripcije koja može biti do 256 bita.

Jaka enkripcija, od 128 bita, može da računa 2^{88} puta više kombinacija od 40-bitne enripcije. **To je bilion puta jače**. Pri sadašnjoj brzini interneta i alatima koji danas postoje, hakeru bi trebalo bilion godina da upadne u sesiju zaštićenu SGC sertifikatom. Da biste omogućili jaku enkripciju za većinu posetilaca sajta, izaberite SSL sertifikate koji omogućavaju najmanje 128-bitnu enkripciju za 99.9 procenata posetilaca.

Akreditivi utvrđuju identitet online

Akreditivi ili dokumenta za utvrđivanje identiteta su uobičajena pojava: vozačka dozvola, pasoš, oznaka kompanije. SSL sertifikati su akreditivi za online svet, jedinstvene potvrde koje se izdaju za određen domen i web server i izdaje ih provajder SSL sertifikata. Kada se Web čitač poveže sa serverom, server šalje informacije o identifikaciji čitaču.

Da biste videli akreditive web sajta:

- Kliknite na zatvoren katanac u prozoru Web čitača.
- Kliknite tzv. trust mark to jest žig (kao što je Norton Secured Seal).
- Pogledajte zelenu adresnu liniju koju pokreće SSL sa proširenom validacijom (Extended Validation – EV).

Autentifikacija stvara poverenje u akreditive

Poverenje u akreditive zavisi od pozdanosti onih koji su te akreditive izdali, jer izdavač garantuje autentičnost tih akreditiva. Sertifikaciona tela (Certificate Authorities) koriste različite autentifikacione metode za verifikovanje informacija koje im pružaju organizacije. Symantec, vodeće sertifikaciono telo (CA), dobro je poznat proizvođačima Web čitača zbog svojih rigoroznih metoda za autentifikaciju i veoma pouzdane infrastrukture. Poverenje koje imaju u Symantec, čitači prenose na SSL sertifikate koje izdaje Symantec.

Kome treba SSL?

Svako kome je potreban bezbedan prenos informacija preko interneta trebalo bi da koristi SSL sertifikate. SSL ne služi samo bezbedne transakcije sa kreditnih kartica i tebalo bi da se koristi za zaštitu osetljivih informacija koje se prenose preko mreže na svim nivoima. Koristite SSL da:

- Zaštitite online transakcije kreditnim karticama.
- Zaštitite web forme i login podatke korisnika.
- Zaštitite email i webmail aplikacije uključujući Microsoft Outlook Web Access, Exchange i Office Communications Server.
- Zaštitite korporativne komunikacije na inranetu, ekstranetu, internim mrežama, file sharing i Microsoft SharePoint.
- Zaštitite komunikacije na cloud platformama i virtualizovanim aplikacijama.
- Zaštitite file transfer preko https i ftp.
- Zaštitite hosting control panels logins uključujući Parallels i cPanel.
- Zaštitite informacije poslate i primljene putem mobilnih uređaja.

Vrste SSL sertifikata

Zbog rasprostranjenosti lažnih odnosno faslifikovanih sajtova na internetu, jedna od ključnih namena SSL sertifikata je da uveri korisnike da su zaista na sajtu koji su želeli da posete. SSL sertifikat koji izdaje treća strana potvrđuje identitet sajta kroz proces validacije koji vrši sertifikaciono telo (CA). Ipak, postoji nekoliko različitih nivoa validacije koji prethode izdavanju SSL sertifikata i oni zavise od sertifikata i od sertifikacionog tela.

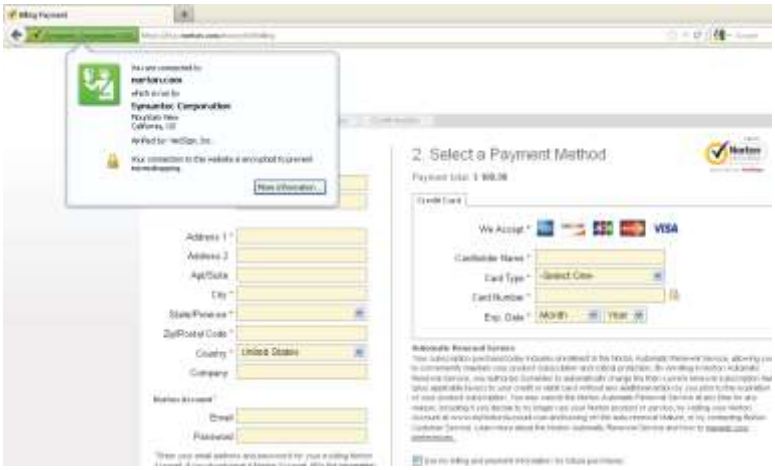
Nivo potvrde identiteta koji garantuje sertifikaciono telo je značajan faktor razlikovanja SSL seritfikata. Eksplozivni rast „pecanja“ i drugih lažnih sajtova dizajniranih da kradu podatke korisnika stavio je pod lupu snagu autentifikacije različitih SSL sertifikata i autentifikacionih procesa koje sprovode različita sertifikaciona tela. Tri najpoznatije kategorije SSL autentifikacije koje nude Symantec-ovi brendovi su proširena validacija – Extended Validation (EV), validacija organizacije – Organization Validation (OV) i validacija domena – Domain Validation (DV).

Proširena validacija (EV)

Proširena validacija predstavlja najbolji SSL sertifikat i to je preporučen tip SSL sertifikata. Kao najviši nivo autentifikacije koristi validacione kriterijume koje je definisao forum sertifikacionih tela i Web čitača, čiju reviziju jednom godišnje se vrši KPMG, EV aktivira zelenu boju adresne linije u Web čitaču i prikazuje ime organizacije kao i ime sertifikacionog tela koje je izdalo sertifikat. Takođe potvrđuje vlasništvo domena i informacije o organizaciji, zajedno sa pravnim postojanjem organizacije i prikazuje potvrdu zahteva za sertifikacijom. Ono što dobijete ako se opredelite za EV sertifikate više vrednosti je više bezbednosti i više poverenja, što vodi do više obavljenih online transakcija.

- Garantuje ispravnost informacija o upravljanju registrovanim domenom.
- Prikazuje sliku katanca u Web čitaču.
- Potvrđuje legitimnost organizacije i da postoji kao pravno lice.
- Traži dokaz da podnosilac ima pravo da zahteva sertifikat.

- Potvrđuje da je podnosilac zaposlen u organizaciji, odnosno da je ovlašćen od organizacije da za nju zahteva sertifikat.
- Prikazuje detalje o organizaciji u informacijama o sertifikatu.
- Prikazuje zelenu adresnu liniju u Web čitaču.



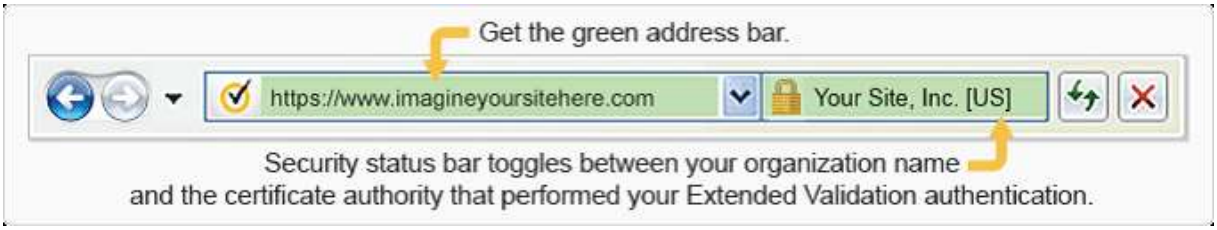
Kome je potrebna proširena validacija?

Za preduzeća koja imaju prepoznatljiv brend, korišćenje EV SSL sertifikata pokazalo se kao efikasna odbrana od „phishing“ prevara. Za svaki online biznis, korišćenje SSL sa EV može imati značajan uticaj na zaradu. Online kupci će radije uneti podatke o kreditnoj kartici ili bilo koji poverljivi finansijski podatak na sajtu sa SSL EV zelenom linijom. Sajtovi koji imaju najviše koristi od EV su:

- E-prodavnice koje prikupljaju informacije o kreditnim karticama.
- Sajtovi koji imaju jaku konkurenciju i kojima je lojalnost kupaca i zaštita brenda od ključne važnosti.
- Sajtovi koji prikupljaju lične podatke.
- Sajtovi sa login formama za kupce i zaposlene.
- Sajtovi koji omogućavaju posredno plaćanje (npr. putem PayPal).

Zašto izabrati Symantec za proširenu validaciju?

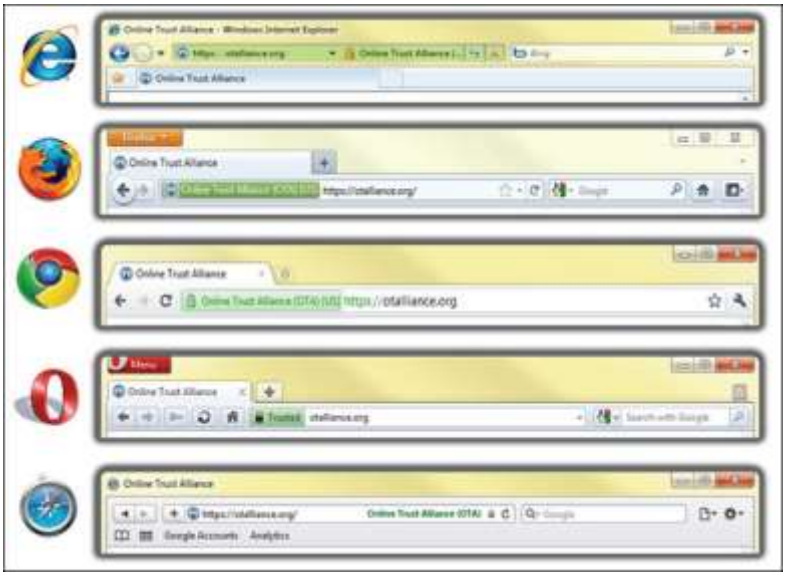
Symantec je pomogao razvoju proširene validacije i od januara 2012. izdao više EV SSL sertifikata od ijednog drugog sertifikacionog tela. Symantec-ova rigorozna praksa autentifikacije postavila je standard za garanciju online bezbednosti i revidira je KPMG. Kontinuirano investiranje u istraživanje i infrastrukturu pomaže Symatec-u da održi najviši standard u industriji i da ostane daleko ispred bezbednosnih rizika koji evoluiraju.



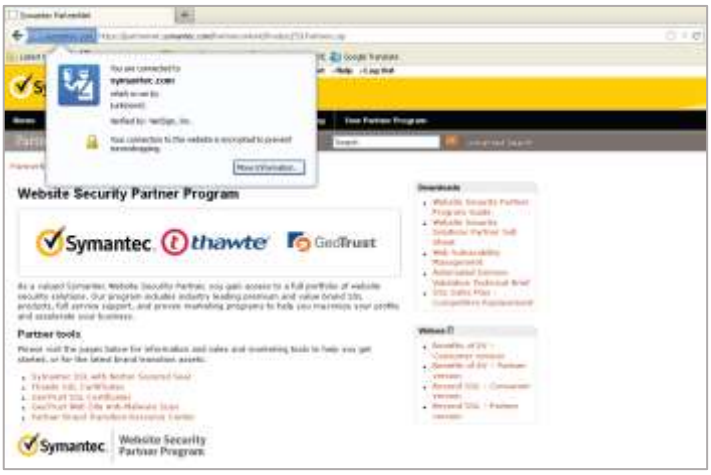
Zelena boja je važna

EV SSL sertifikat uliva korisnicima više poverenja da komuniciraju sa sajtom kome mogu verovati i da su njihovi podaci bezbedni. EV SSL sertifikat aktivira kod Web čitača visoke bezbednosti prikazivanje imena organizacije u zelenoj adresnoj liniji i pokazuje ime sertifikacionog tela koje je izdalo sertifikat. Sertifikaciono telo koristi rigorozan metod autentifikacije i čitač kontroliše prikaz, otežavajući ljudima koji se bave phishing prevarama i falsifikovanjem sajtova da preotmu vaš brend i korisnike.

Izgled proširene validacije u Web browser-ima



Validacija organizacije (OV)



Validacija organizacije važi za napredniji i bolji SSL sertifikat jer postavlja više validacionih zahteva. OV potvrđuje vlasništvo domena plus informacije o organizaciji koje su uključene u sertifikat (ime, grad, država i zemlja). OV aktivira plavu adresnu liniju u Firefox Web čitačima.

- Garantuje ispravnost informacija o upravljanju registrovanim domenom.
- Prikazuje sliku katanca u Web čitaču.
- Potvrđuje legitimnost organizacije i da postoji kao pravno lice.
- Traži dokaz da podnosilac ima pravo da zahteva sertifikat.
- Prikazuje detalje o organizaciji u informacijama o sertifikatu
- Prikazuje plavu adresnu liniju u Web čitaču (važi samo za Firefox browser-e).

Validacija domena (DV)

Validacija domena predstavlja najjednostavniji „dobar“ SSL sertifikat. DV potvrđuje da je domen registrovan i neko sa administrativnim pravima je upoznat i odobrava zahtev za sertifikacijom.

- Garantuje ispravnost informacija o upravljanju registrovanim domenom.
- Prikazuje sliku katanca u Web browser-u.

SAN sertifikati

Sertifikati koji koriste Subject Alternative Names (SAN) su moćni alati koji mogu da zaštite više domenskih imena jeftino i efikasno. SAN je još poznat i kao Unified Comunications (UC) sertifikat i najčešće se koristi za Microsoft Exchange Server 2007, Microsoft Exchange Server 2010 i Microsoft Communications Server.

Kod SAN sertifikata postoji polje za alternativno ime subjekta što omogućava da se dodatna imena domena zaštite jednim sertifikatom. Umesto da kupujete posebne sertifikate za svako domensko ime, možete dodati imena domena u SAN polja, tako da dele isti sertifikat. Na primer jedan sertifikat koji podržava SAN može da obezbedi:

- www.abccompany.com
- Abccompany.com
- www.abccompany.net
- www.abccompany.org
- Mail.abccompany.com

SAN funkcija je dostupna za Symantec, Thawte i GeoTrust.

Ključne prednost SAN-a

- **Niži administrativni i troškovi implementacije** tako što štitite više različitih domenskih host imena jednim sertifikatom.
- **Lakša instalacija sertifikata i upravljanje** putem jedinstvene podrške bilo koje kombinacije domenskih imena (čak i na različitim poddomenskim nivoima), localhost imena i internih IP adresa.
- **Maksimizuje fleksibilnost** tako što obezbeđuje web, SMTP, POP/IMAP i druge UC servere uključujući i Microsoft Exchange Server 2007, Microsoft Exchange Server 2010 i Microsoft Office Communications Server 2007.
- **Zadovoljava administratorske potrebe** za okruženjem sa širokom paletom funkcija koje zahteva bezbednu klijent-server i server-server komunikaciju.
- **Smanjuje rizik** tako što zahteva specifična host imena i otklanja mogućnosti neovlašćenog zahteva.

Symantec Website Security Solutions

Symantec Website Security rešenja obuhvataju prepoznatljive, pouzdane i raznovrsne SSL sertifikate i rešenja za bezbednost Web sajtova. Porodicu Symantec rešenja za website bezbednost čine tri brenda: Symantec, Thawte i GeoTrust. Svaki brend ima svoje specifičnosti što znači da zadovoljava razlitite potrebe koje se tiču bezbednosti Web sajtova.

Portfolio Symantec SSL proizvoda

Po čemu se brendovi međusobno razlikuju?

- Prepoznatljivost imena
- Reputacija sertifikacionog tela
- Nivo sigurnosti
- Karakteristike proizvoda
- Kompletno rešenje

Zašto je brend važan? Sve je u poverenju.

- Symantec štiti više od milion Web servera štirom sveta, što je više od bilo kog drugog sertifikacionog tela.
- Symantec je vodeći SSL provajder SSL sertifikata koji omogućavaju 128 ili 256-bitnu enkripciju.
- Symantec ima moćnu infrastrukturu koja obuhvata data centre koji se mogu porediti sa vojnim data centrima i disaster recovery sajtove za nenadmašnu zaštitu i dostupnost korisničkih podataka.
- Symantec-ova rigorozna pravila za autentifikaciju najstroža su u branši, što garantuje kredibilitet vašem sajtu.
- Symantec kontinuirano ulaže u istraživanje i infrastrukturu kako bi održao svoj standard i lidersku poziciju u branši, kao i da bi nastavio da bude korak ispred bezbednosnih rizika.

Premium Brend
Symantec SSL Solutions

Symantec nudi rešenja za bezbednost sajtova koja omogućavaju kompanijama i kupcima da se upuste u online komunikaciju i poslovanje bezbrižno. U avgustu 2010. Symantec je kupio VeriSign Authentication Services Business od VeriSign, Inc., prvog sertifikacionog tela koje izdaje SSL sertifikate od 1995. Symantec je nastavio dobru praksu VeriSign-a, ali i podigao SSL bezbednost na viši nivo zahvaljujući novim karakteristikama koje omogućavaju skeniranje malware-a i ocenu ranjivosti sajta.

Symantec pruža više bezbednosti i poverenja u jednom rešenju

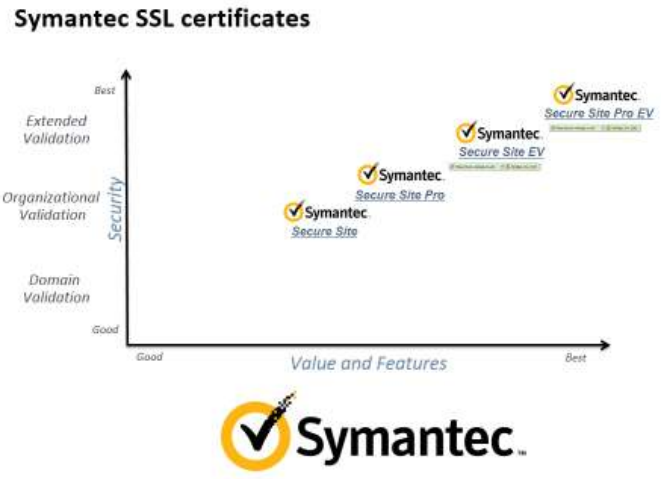
Svi Symantec SSL sertifikati uključuju Norton™ Secured Seal, znak od najvećeg poverenja na internetu, Symantec Seal-in-Search™ i dnevno skeniranje malware-a na sajtu, što vašim korisnicima uliva poverenje i omogućava bezbrižno online iskustvo. Svaki sertifikat sa proširenom validacijom ili Pro SSL sertifikat uključuju procenu ranjivosti i pomažu vlasnicima sajta da brzo otkriju slabe tačke sajta i preduzmu neophodne mere za bezbednost sajta.

Symantec SSL rešenja odlikuju se autentifikacijom i SSL enkripcijom koje su vodeće u industriji i u njih su uključeni:

- Norton Secured Seal
- Procena ranjivosti
- Skeniranje malvera na sajtu
- Symantec Seal-in-Search

Symantec SSL sertifikati

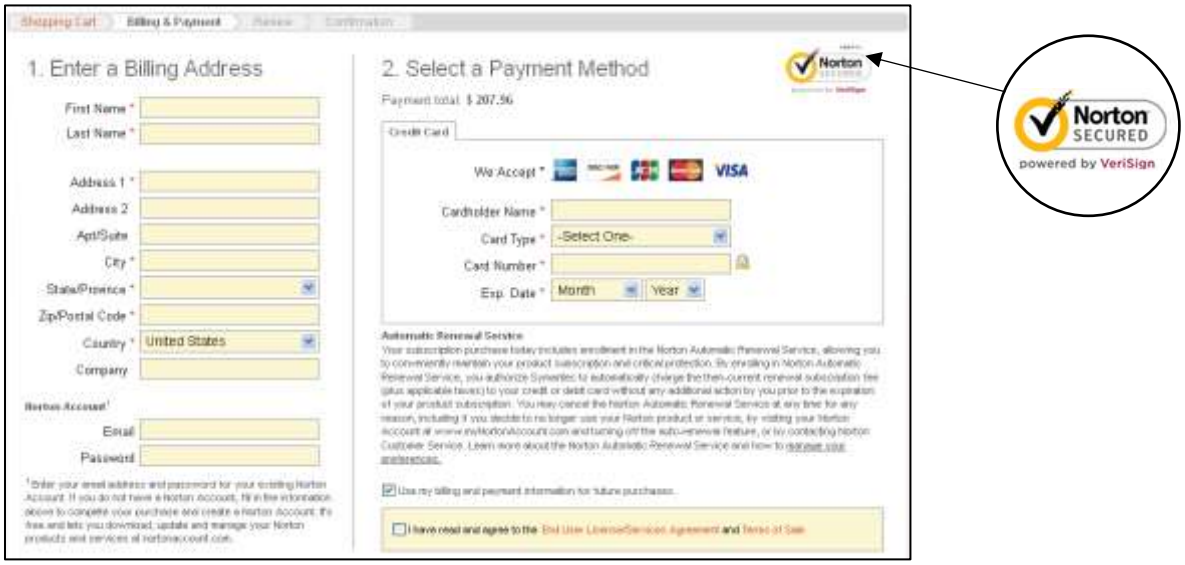
- **Symantec Secure Site Pro with EV** – sertifikat sa proširenom validacijom je najsigurniji izbor kada je bezbednost Web sajta u pitanju, privlači više kupaca na sajt i uverava ih u bezbednost transakcije, dok omogućava najjaču SSL enkripciju dostupnu najvećem broju posetilaca sajta.
- **Symantec Secure Site with EV** – sertifikat sa proširenom validacijom koji privlači više kupaca i uliva im poverenje u vaš sajt što rezultira većim brojem završenih online transakcija.
- **Symantec Secure Site Pro** – sertifikat za validaciju organizacije koji omogućava svakom posetiocu sajta iskustvo najjače SSL enkripcije uključujući i SGC (Server Gated Cryptography).
- **Symantec Secure Site** – sertifikat za validaciju organizacije koji štiti transfer osetljivih podataka na sajtovima, intranetu i ekstranetu.



Norton™ Secured Seal

Norton Secured Seal (pečat) je dinamička, animirana grafika koja se prikazuje na Web stranama koje su zaštićene Symantec SSL sertifikatom i na sajtovima koje je Symantec autentifikovao. Kada korisnik klikne na Norton pečat otvori se verifikaciona strana koja sadrži informacije o organizaciji, status skeniranja malvera i detalje o SSL sertifikatu. Sva tri Symantec-ova brenda imaju svoju varijaciju pečata poverenja, ali Norton Secured pečat je najprepoznatljiviji globalno.

- Norton Secured pečat se prikaže više od pola milijarde puta dnevno na sajtovima u 170 zemalja i u rezultatima pretrage na omogućenim Web čitačima kao i na partnerskim online prodavnicama i stranama koje sadrže opise proizvoda.
- U aprilu 2012. svi VeriSign pečati ažurirani su u Norton Secured pečat, koji je kombinacija snage VeriSign-ovog znaka za štikliranje i moći Nortonovog imena.
- Kada je rađeno testiranje Norton Secured pečata, 77 % korisnika prepoznalo je pečat, više nego znak konkurenata.



Procena ranjivosti

Ranjivost je potencijalna tačka upada kroz koju funkcionalnost sajta ili podaci mogu biti oštećeni, preuzeti ili manipulisani. Tipični Web sajt (čak i najobičniji blog) može imati hiljade potencijalnih tačaka ranjivosti.

Procena ranjivosti ide besplatno uz kupovinu proširene validacije ili Pro SSL sertifikata Symantec brenda. Procena ranjivosti pomaže vam da brzo otkrijete i preduzmete mere potrebne za zaštitu najslabijih tačaka vašeg sajta. Procena ranjivosti omogućava automatsko nedeljno skeniranje slabosti na javnim Web stranama. Takođe uključuje izveštaj u kom su identifikovane najslabije tačke koje treba odmah istražiti i slabosti koje nose manji rizik za bezbednost sajta.

Website Malware Scanning

Malver je skraćenica za maliciozni softver, poznat još i kao maliciozni kod. Hakeri koriste slabosti u bezbednosti vašeg servera kako bi dobili pristup vašem sajtu i instalirali maliciozni kod. Oni koriste vaš sajt za širenje virusa, preuzimanje kompjutera i za krađu osetljivih podataka kao što su brojevi kreditnih kartica ili drugi lični podaci. Malver kod nije lako otkriti i može da zarazi kompjutere vaših korisnika kada posete vaš sajt.

Skeniranje malvera na vašem sajtu je uključeno u svaki Symantec SSL sertifikat, a dostupno je i kao dodatna opcija za GeoTrust SSL sertifikate. Servis skeniranja malvera skenira kod Web sajta koji je lociran u host imenu koje se koristi za SSL sertifikat, uključujući javascript i iframes. Servis radi kompletnu statičku analizu koda sajta kao i bihejvioralnu kroz browser simulaciju kako bi našao kod koji se može aktivirati prikazivanjem stranice. Servis ne skenira svaku Web stranu na vašem sajtu, već pregleda optimalan broj strana kako bi otkrio malicioznu aktivnost i odmah vas obavestio o otkrivanju malicioznog koda, što vam omogućava da ga brzo otklonite.

Symantec Seal-in-Search™

Kada kupci pretražuju online, često nalaze dugačku listu sajtova koji su konkurencija vašem sajtu. Symantec Seal-in-Search, ekskluzivna karakteristika Symantec SSL sertifikata, stavlja Norton pečat uz link za vaš sajt i time pokazuje da je vaš sajt od poverenja, tj. da Symantec garantuje da je vaš sajt bezbedan. Korisnici mogu da veruju vašem sajtu i pre klika na link. Symantec Seal-in-Search mogu da vide korisnici koji koriste Web čitač koji podržava besplatan plug-in, kao i na partnerskim online prodavnicama i stranama koje sadrže opise proizvoda.

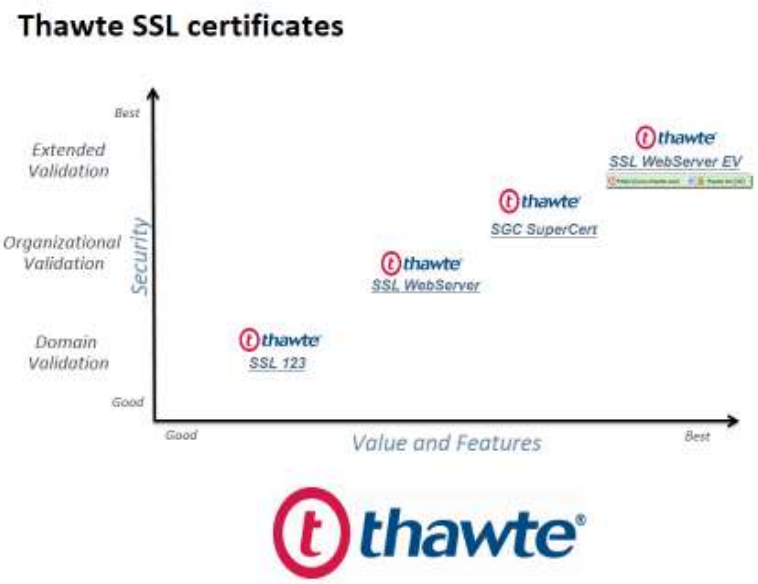
High Value Brand

Thawte SSL sertifikati

Thawte je prvo sertifikaciono telo koje je izdalo SSL sertifikate za javne subjekte izvan SAD i izdalo je više od 945,000 SSL i code signing sertifikata od 1995. Thawte sertifikati koriste prednosti Symantec infrastrukture za autentifikaciju.

Thawte je ključni član Symantec SSL porodice koji nudi sertifikate visoke vrednosti za proširenu validaciju, validaciju organizacije i validaciju domena.

- **Thawte® SSL Web Server Certificates with EV –** proširena validacija obezbeđuje najvidljiviji indikator bezbednosti: zelenu adresnu liniju u Web čitačima.
- **Thawte® SGC SuperCerts –** sertifikat za validaciju organizacije pomaže da online transakcije ostanu bezbedne tako što omogućava da svaki posetilac sajta iskusi najjaču SSL enkripciju.
- **Thawte® SSL Web Server Certificates** – sertifikat za validaciju organizacije obezbeđuje poverljivost informacija koje se razmenjuju online i potvrđuju identitet vašeg sajta.
- **Thawte® SSL123 Certificates** – sertifikat za validaciju domena ima najkraće vreme izdavanja što vam omogućava da brzo uspostavite kriptovanu konekciju sa vašim web serverom.

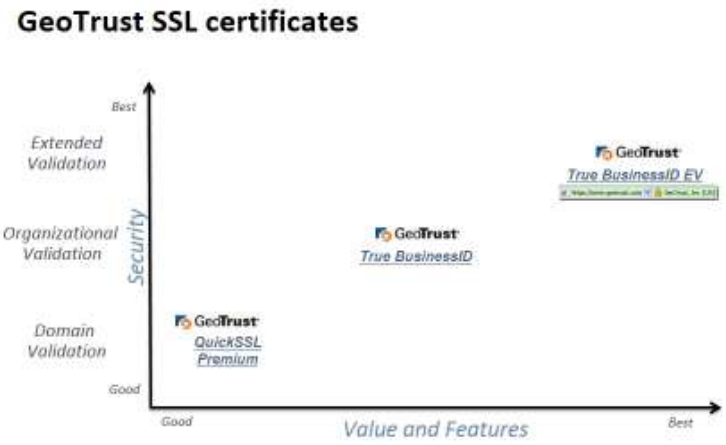


High Value Brand

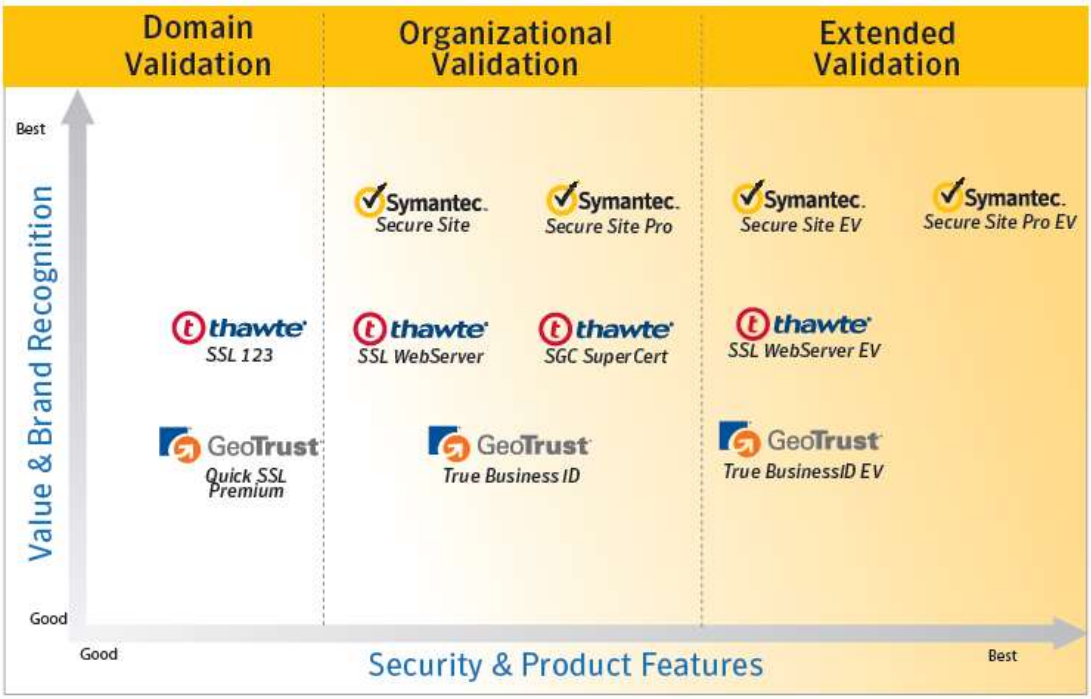
GeoTrust SSL sertifikati

GeoTrust je drugi najveći svetski provajder digitalnih seritfikata, odmah iza Symantec-a. Više od 100,000 korisnika u preko 170 zemalja poverilo je GeoTrust-u posao obezbeđenja online transakcija i obavljanja poslova putem interneta. Više od 500,000 aktivnih sertifikata instaliranih širom sveta u više od 300,000 organizacija svih veličina dokaz su kvaliteta ovih sertifikata i poverenja korisnika u GeoTrust brend. GeoTrust je ključni član Symantec Website Security porodice i nudi sertifikate visoke vrednosti za proširenu validaciju, validaciju organizacije i validaciju domena.

- **GeoTrust True BusinessID with EV** – sertifikat sa proširenom validacijom za maksimalan kredibilitet i bezbednost.
- **GeoTrust True BusinessID** – sertifikat za validaciju organizacije za snažan business-level SSL.
- **GeoTrust Quick SSL Premium** – sertifikat za validaciju domena za osnovnu pristupačnu enkripciju.



Poređenje Website Security brendova



Poređenje SSL proizvoda

	Symantec Secure Site Pro with EV	Symantec Secure Site with EV	Symantec Secure Site Pro	Symantec Secure Site	Thawte SSL Web Server with EV	Thawte SGC SuperCerts	Thawte SSL Web Server	Thawte SSL123	GeoTrust True BusinessID with EV	GeoTrust True BusinessID	GeoTrust Quick SSL Premium
Encryption strength	128-bit to 256-bit	40-bit to 256-bit	128-bit to 256-bit	40-bit to 256-bit	128-bit to 256-bit in	128-bit to 256-bit	128-bit to 256-bit	128-bit to 256-bit	40-bit to 256-bit	40-bit to 256-bit	40-bit to 256-bit
Extended Validation	✔	✔			✔				✔		
Full organization authentication	✔	✔	✔	✔	✔	✔	✔		✔	✔	
Vulnerability assessment	✔	✔	✔								
Daily website malware scanning	✔	✔	✔	✔					Add-on Option	Add-on Option	Add-on Option
Symantec Seal-in-Search	✔	✔	✔	✔							
Trust Seal											
NetSure extended warranty	$1,500,000	$1,500,000	$1,250,000	$1,000,000	$750,000	$500,000	$250,000	$100,000	$500,000	$250,000	$100,000
Customer support	24/7 - Phone/Email Chat/Web	24/7 - Phone/Email Chat/Web	24/7 - Phone/Email Chat/Web	24/7 - Phone/Email Chat/Web	Chat/ Email/Web	Chat/ Email/Web	Chat/ Email/Web	Chat/ Email/Web	Chat/ Email/Web	Chat/ Email/Web	Chat/ Email/Web
Universal browser compatibility	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔
Support for SAN (UC)	Up to 24	Up to 24	Up to 24	Up to 24	Up to 5	Up to 5	Up to 5	Up to 5	Up to 25	Up to 25	Up to 5
Support for IDN	✔	✔	✔	✔	✔	✔	✔	✔			
Server licenses per certificate	Single	Single	Single	Single	Single	Single	Single	Single	Unlimited	Unlimited	Unlimited

Net++ technology

Net++ technology je preduzeće specijalizovano za ITC bezbednost, koje nudi kompletno rešenje za vaše IT potrebe - od projektovanja i planiranja uvođenja proizvoda, preko instalacije i implementacije, do obuke administratora za korišćenje proizvoda, tehničke podrške i provere stanja.

Dugi niz godina smo vodeći Symantec Gold Partner u Srbiji sa navećim brojem uspešno implementiranih Symantec rešenja, počev od antivirusa i backup rešenja, preko rešenja za visoku raspoloživost sistema (high availability), arhiviranje elektronske pošte i dokumenata, rešenja za enkripciju – šifrovanje i rešenja za sprečavanje curenja podataka (data loss prevention).

Prvi smo Symantec Authorized Technical Support Partner u Srbiji. Autorizacija za tehničku podršku pored garancije visokog kvaliteta usluge omogućava nam i direktni pristup višem nivou Symantec tehničke podrške što za naše korisnike znači brzo i kvalitetno rešenje svakog problema.

2011. postali smo i prvi Symantec Specialist Partner u Srbiji, za dve oblasti Arhivirnje i eDiscovery i Enterprise Security.