SSL sertifikatai

Kas yra SSL sertifikatas ir kam jis reikalingas

Nesvarbu, ar esate individualus asmuo arba įmonė, turėtumėte skirti tiek pat dėmesio saugumui internete, kaip ir įprastai fizinio turto apsaugai (namų užraktai, durys, apsaugos sistemos ir pan.).

Viena iš internetinio saugumo priemonių ir yra **SSL sertifikatas**. Jis ne tik apsaugo Jūsų duomenis internete, bet ir kitus žmones besilankančių Jūsų tinklapyje arba besinaudojančius Jūsų teikiamomis internetinėmis paslaugomis (elektroninis paštas, elektroninė parduotuvė ir pan.).

Pirmas žingsnis internetiniam saugumui yra suprasti ir įvertinti galimas rizikas ir grėsmes (asmeninių prisijungimo duomenų netekimas, nesankcionuota prieiga prie asmeninės paskyros ir pan.). Sparčiai besivystant internetinėms technologijoms ir skaitmeniniams sprendimas yra nelengva užduotis susiorientuoti specifinėje srityje, profesionaliai įvertinti minėtas grėsmes bei parinkti atitinkamas saugumo priemones. Tam, kad ši užduoti būtų lengviau įvykdoma yra teikiami paruošti naudojimui standartizuoti apsaugos internete sprendimai. Vienas iš jų kaip tik ir yra **SSL sertifikatas**.

Kas yra SSL serifikatas

SSL – ang.: Secure Sockets Layer. Apibrėžimas būtų: duomenų šifravimo protokolas skirtas apsaugoti siunčiamą informaciją kompiuteriniame tinkle. Realybėje SSL sertifikatas, tai skaitmeninis kompiuterinis failas arba kompiuterinio programinio kodo dalis skirta atlikti dvi funkcijas:

1. Autentifikuoti ir Patvirtinti. SSL sertifikate yra informacija apie internetinio tinklapio valdytoją arba savininką, kurią galite pamatyti spragtelėję pelyte ant atitinkamo spynelės ženklo internetinės naršyklės adreso laukelyje. Taip pat išskirtinis apsaugoto tinklapio SSl sertifikatu bruožas yra tinklapio adresas prasidedantis “https://” raidėmis. Būtent “s” raidė informuoja apie tai, kad ryšys su tinklapiu yra Saugus.

2. Šifruoti duomenis. SSL sertifikatas ne tik pateikia informaciją, kurios pagalba galima identifikuoti tikrąjį tinklapio savininką, bet ir šifruoja duomenis. Tai reiškia, kad privataus pobūdžio informacija siunčiama tarp naudotojo kompiuterio ir tinklapio negali būti perimta ir perskaityta.

Kaip veikia SSL apsauga

SSL duomenų šifravimą galima būtų palyginti su durų užraktu. Jei Jūs neturite tinkamo rakto, Jūs negalite atrakinti durų. Taip pat veikia ir SSL duomenų šifravimas ir dešifravimas. Jei neturi atitinkamo rakto – negalite “atrakinti” (dešifruoti) informacijos.

Kiekviena SSL sesija (prisijungimas prie SSL apsaugoto tinklapio) susdeda iš dviejų raktų:

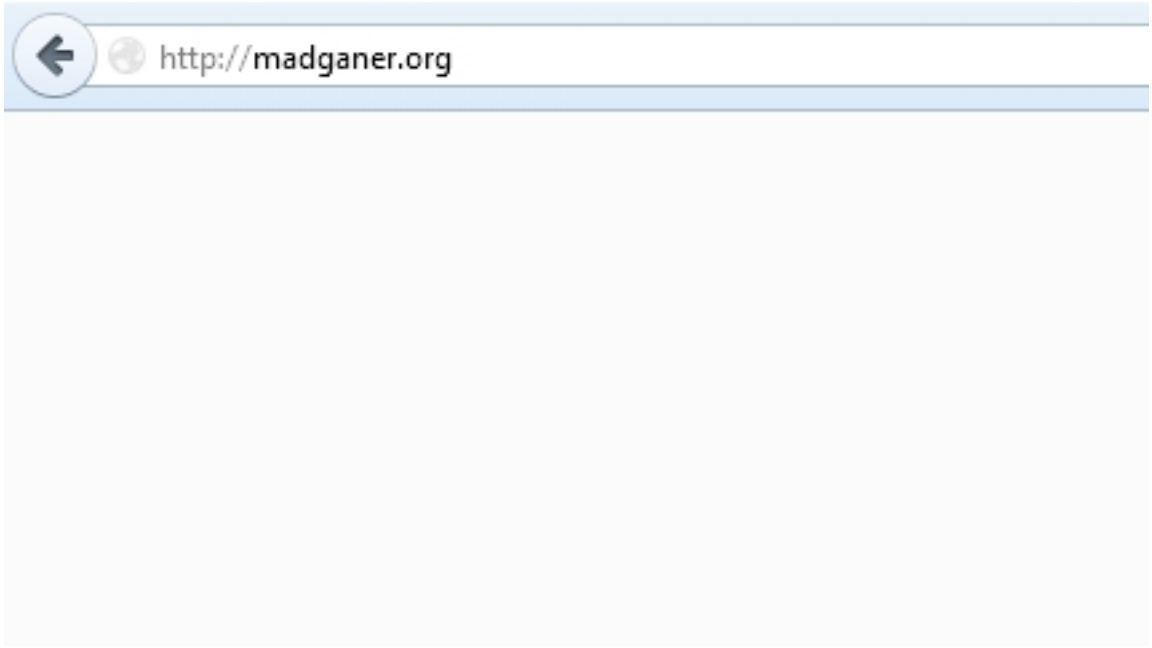
- Viešojo rakto informacijos užšifravimui.

- Privataus (Asmeninio) rakto informacijos dešifravimui.

SSL sertifikatas yra priskiriamas tam tikram internetiniam adresui. Kai Jūs užeinate į tinklapį apsaugotą SSL sertifikatu pradedama sesija tarp Jūsų interneto naršyklės ir serverio, kuriame talpinamas tinklapis. Apie tai indikuoja internetinio tinklapio adresas prasidedantis “https://” bei spynos ikona. Tai reiškia, kad saugus ryšys yra užmegztas šiai sesijai su unikaliu sesijos raktu ir informacija tarp Jūsų kompiuterio ir tinklapio yra apsaugota.

Kaip žinoti ar tinklapis turi galiojantį SSL sertifikatą

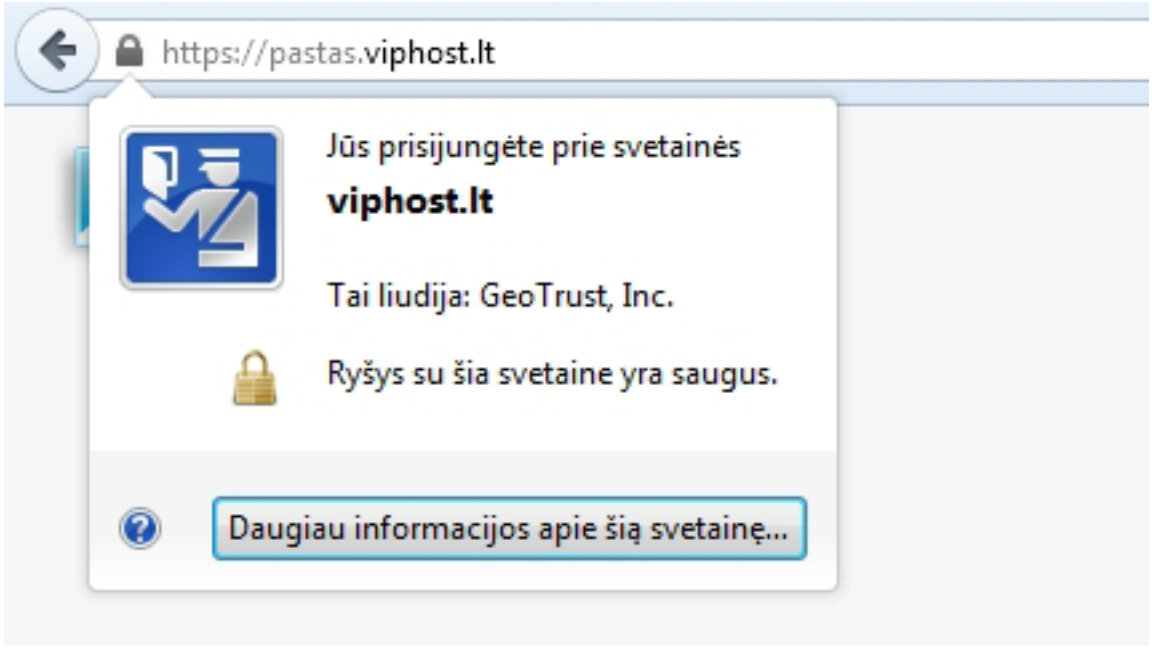
1. Neapsaugotų tinklapių adresai prasideda “http://”, kai apsaugotų tinklapių – “https://”.



2. Priklausomai nuo Jūsų naudojamos internetinės naršyklės, šalia internetinio adreso būna spynos ikona.

3. Paspaudus spynos ikoną, atsidariusiame informaciniame langelyje, galima susipažinti su tinklapį identifikuojančia informacija bei organizacija išdavusia sertifikatą ir SSL sertifikato technine informacija (galiojimo terminas, šifravimo lygis, ...).

SSL sertifikatai



Kur naudoti SSL sertifikatus

Trumpiausias atsakymas – visuose internetiniuose projektuose, kur pageidaujate, kad informacija tarp tinklapio ir kompiuterio būtų saugi.

Keletas pavyzdžių:

- apsaugoti siunčiamai ir gaunamai informacijai tarp Jūsų tinklapio ir kliento ar interesanto interneto naršyklės;

- apsaugoti vidinę informaciją intranet tinkle;

- apsaugoti elektroniniu paštu siunčiamą informaciją;

- apsaugoti informaciją tarp serverių;

- apsaugoti informaciją gaunamą ir siunčiamą mobiliais įrenginiais.

Unikalus sprendimo identifikatorius: #1011
Autorius: vip
Paskutinis atnaujinimas: 2015-06-09 10:08