SAUGUS DUOMENŲ PERDAVIMAS HTTPS PROTOKOLU

2009-12-23

ĮVADAS

Valstybinės duomenų apsaugos inspekcijos direktoriaus įsakymu „Dėl bendrųjų reikalavimų organizacinėms ir techninėms duomenų saugumo priemonėms“ patvirtinti bendrieji reikalavimai įpareigoja duomenų valdytojus užtikrinti internetu pateikiamų asmens duomenų saugumą naudojant saugius protokolus ir (arba) slaptažodžius.

Plačiausiai paplitęs būdas perduodamų duomenų saugumui užtikrinti yra https protokolo naudojimas. Naudojantis šiuo protokolu internetu perduodama užšifruota informacija, todėl užkertamas kelias perduodamos informacijos neteisėtam prieinamumui, užtikrinamas jos vientisumas ir konfidencialumas.

Duomenų valdytojai, kurie nenaudoja https ar kitų saugių protokolų, neužtikrina tinkamų duomenų saugumo priemonių, skirtų perduoti asmens duomenis išoriniais duomenų perdavimo tinklais. Tokiu atveju prisijungimo vardai, slaptažodžiai ir kita informacija, kurią jūs pateikiate interneto tinklalapyje, pavyzdžiui, asmens kodas, adresas, telefono numeris, darbovietės pavadinimas ir kt., internetu perduodami atviru pavidalu, t. y. neužšifruoti. Neužšifruota informacija perdavimo metu tampa prieinama ir kitiems interneto vartotojams, turintiems prieigą prie tos tinklo dalies, kuria keliauja jūsų pateikta informacija.

Šioje rekomendacijoje aptariamos tokios temos:

- https protokolo įdiegimas;
- https protokolo veikimo principai;
- SSL sertifikatų tipai.

HTTPS PROTOKOLO ĮDIEGIMAS

Norėdami savo tinklalapyje naudoti perduodamų duomenų saugumą užtikrinantį https protokolą, turite įsigyti SSL sertifikatą (angl. *secure sockets layer*). SSL sertifikatas yra kriptografinis protokolas, kuris užtikrina saugią komunikaciją kompiuteriniuose tinkluose, pavyzdžiui, internete.

SSL sertifikatą galite susikurti patys arba užsisakyti SSL sertifikatus išduodančioje įmonėje. Nepaisant to, ar jūs SSL sertifikatą susikursite patys, ar nusipirksite, jį turi patvirtinti trečioji šalis (CA) (angl. *certificate authority (CA)*). Tai yra mokama paslauga, kurią galima užsisakyti beveik visose prieglobos (angl. *hosting*) paslaugas teikiančiose įmonėse.

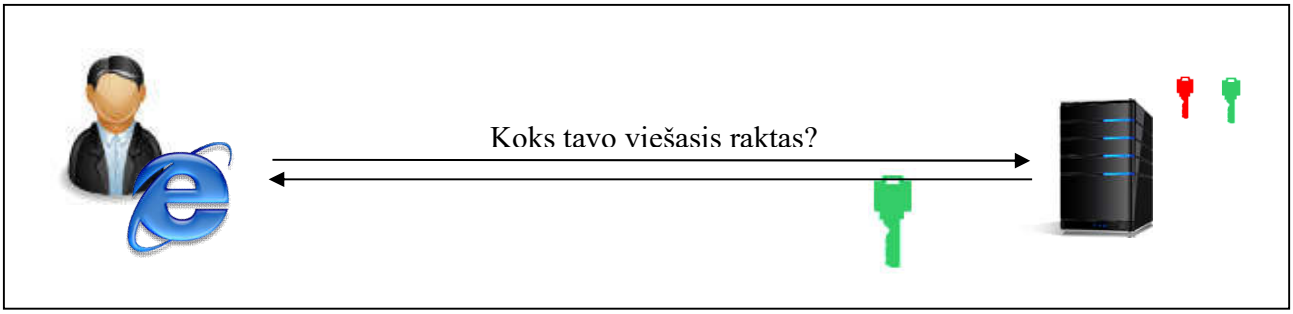
Įdiegus SSL sertifikatą ir sukonfigūravus tarnybinę stotį, kurioje yra tinklalapis, tinklalapį galima pasiekti jau saugiu https protokolu. Interneto naršyklėje rašome ne *http*://www.(tinklalapio pavadinimas).lt, o *https*://www.(tinklalapio pavadinimas).lt.

HTTPS PROTOKOLO VEIKIMO PRINCIPAS

Https protokolas duomenų perdavimo metu naudoja asimetrinį šifravimą. Tai reiškia, kad informacija yra užšifruojama vienu slaptažodžiu, o iššifruojama tiktai kitu slaptažodžiu. Štai kaip tai gali būti pritaikyta tinklalapyje:

1. Tarnybinėje stotyje, kurioje yra tinklalapis, yra įdiegiamas viešasis ir privatusis raktas. Viešasis raktas, skirtas informacijai užšifruoti, yra platinamas viešai, o privatusis, skirtas informacijai iššifruoti, saugomas paslaptyje.

2. Atvertus tinklalapį per https protokolą, jūsų interneto naršyklė užšifruoja informaciją, kuri bus perduodama internetu, pavyzdžiui, prisijungimo vardą ir slaptažodį, naudodama to tinklalapio viešąjį raktą.



1 pav. Viešojo rakto gavimo principas

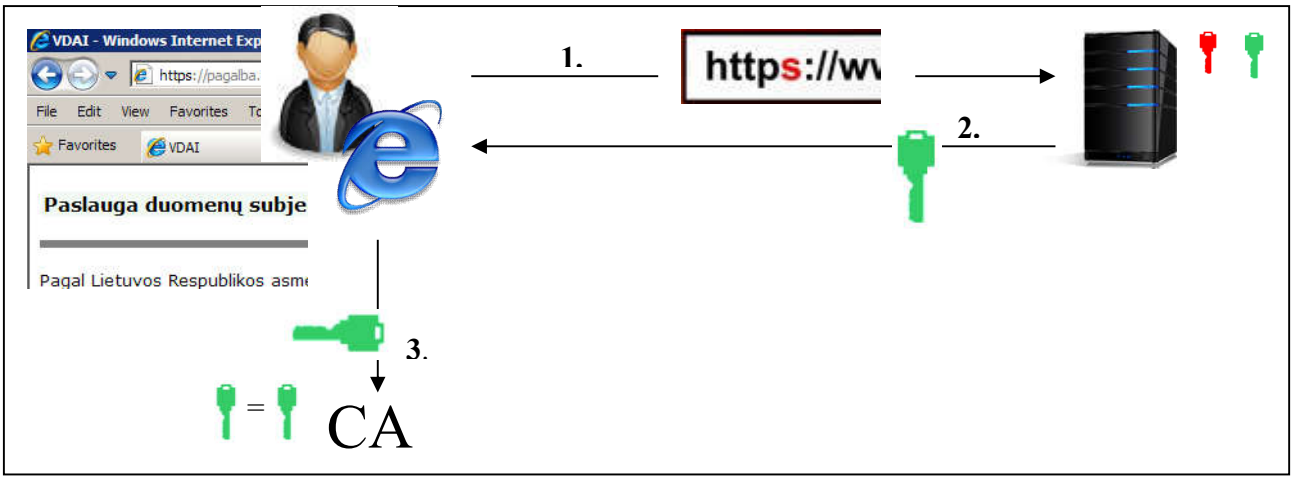
3. Jei viešąjį raktą užregistruoja trečioji šalis (CA), interneto naršyklė visuomet gauna patvirtinimą apie rakto galiojimą ir apie tai, kam jis priklauso. Jei raktas yra neregistruotas, tuomet interneto naršyklė pateikia pranešimą, rekomenduojantį nutraukti darbą šiame tinklalapyje.

Https protokolu perduodamų duomenų pavyzdys (žr. 2 pav.):

1. Interneto vartotojas įveda į naršyklę tinklalapio adresą https://www...

2. Tarnybinė stotis, kurioje yra tinklalapis, atsiunčia į naršyklę viešąjį raktą, skirtą informacijai užšifruoti.

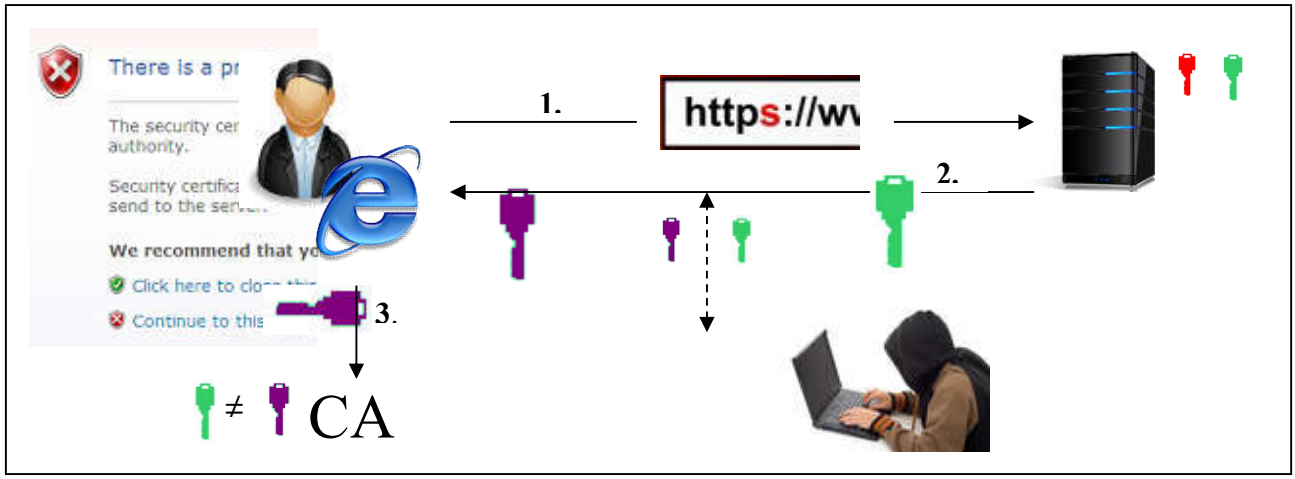
3. Interneto naršyklė susisiekia su trečiąja šalimi (CA) ir palygina viešąjį raktą, gautą iš tarnybinės stoties, su viešuoju raktu, kurį turi trečioji šalis (CA).



2 pav. Supaprastintas https protokolo veikimo principas

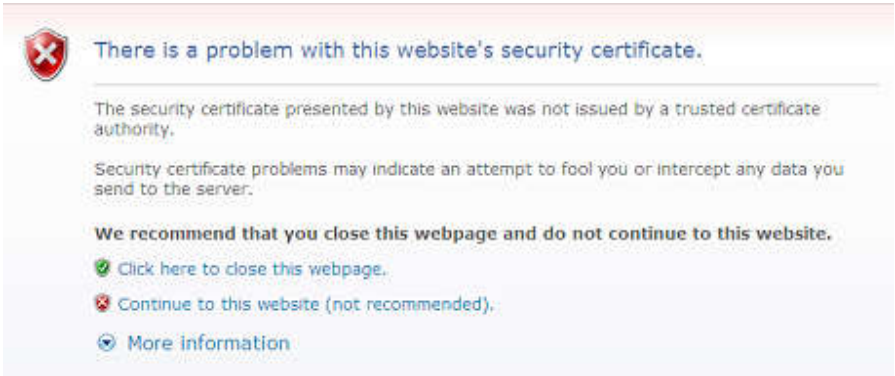
4. Jeigu raktai sutampa, visa internetu perduodama informacija yra užšifruojama šiuo raktu. Informaciją iššifruoja privatusis raktas, kuris yra tarnybinėje stotyje.

3 paveiksle pateikta pavyzdys, kaip piktavalis, turintis prieigą prie tos tinklo dalies, kuria keliauja jūsų pateikta informacija, perima viešąjį raktą ir jį pakeičia kitu. Tuomet jūsų naršyklė užšifruoja informaciją piktavalio viešuoju raktu ir ta informacija tampa jam prieinama. Tačiau interneto naršyklė tokį įsiskverbimą pastebi, nes piktavalio viešasis raktas nesutampa su tuo, kuris buvo užregistruotas trečiojoje šalyje (CA).



3 pav. Supaprastintas https protokolo veikimo principas, kai duomenis, perduodamus internetu, perima piktavalis

Apie tai, kad viešieji raktai nesutampa ir kad informacija bus perduodama nesaugiai, interneto naršyklė informuoja jus pranešimu (žr. 4 pav.).



4 pav. Interneto naršyklės perspėjimas

Matydami tokį perspėjimą, jūs turite dvi galimybes:

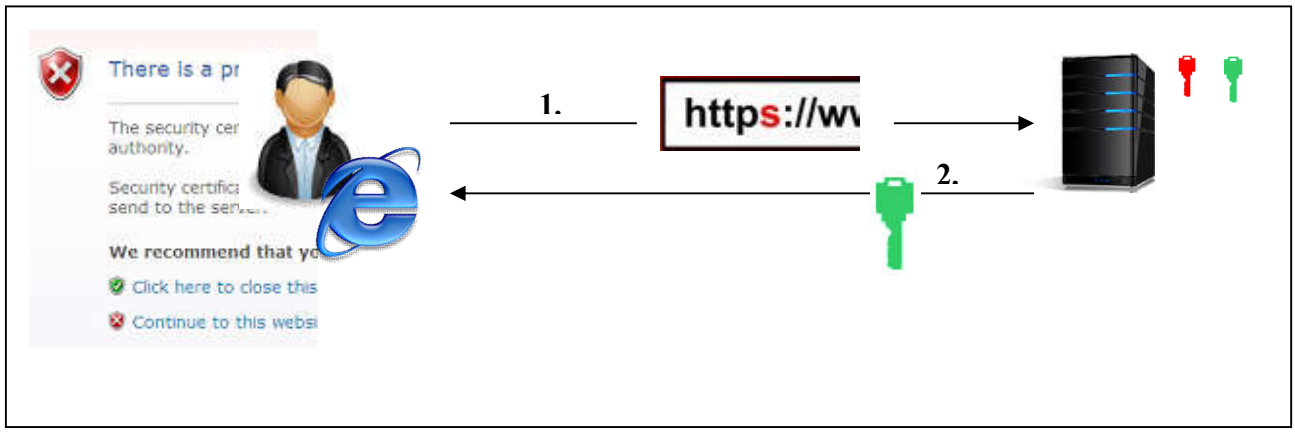
1. Atsisakyti tęsti prisijungimą prie svetainės pasirinkdami „Jei norite uždaryti šią svetainę, spauskite čia“ (angl. *„Click here to close this webpage“*). Pasirinkus šią galimybę interneto naršyklės langas bus tiesiog uždarytas.

2. Tęsti prisijungimą galite pasirinkdami „Atidaryti svetainę (nerekomenduojama)“ (angl. *„Continue to this website (not recommended)“*). Jei pasirinksite šią galimybę, žinokite, kad visa informacija, pavyzdžiui, prisijungimo vardas, slaptažodis, asmens kodas, adresas ir kt., kurią jūs įvesite į šį tinklalapį, bus perduodama nesaugiai.

Dažnai interneto naršytojai, neįsigilinę į pranešimo tekstą, ieško būdų, kaip tęsti darbą. Jie pamėgina pasirinkti pirmą variantą ir, naršyklei užsidarius, nusprendžia, kad pasirinkimas neteisingas. Tuomet pasirenka antrąjį variantą ir tinklalapis atsiveria. Atsivėrusiame tinklalapyje įveda informaciją, pavyzdžiui, prisijungimo vardą ir slaptažodį, kuri internetu bus perduodama nesaugiai. Tuo atveju, jei perspėjimas atsirado dėl piktavalio įsiterpimo, pateikta informacija pateks į jo rankas.

Kitas minėto perspėjimo (žr. 4 pav.) atsiradimo atvejis, kai tinklalapio administratorius, įdiegęs https protokolą savo tinklalapyje, neužtikrina, kad jį patvirtintų trečioji šalis (CA) (žr. 5 pav.). Taip yra daroma todėl, kad šiuo metu toks patvirtinimas yra mokamas ir kainuoja nuo kelių šimtų iki kelių tūkstančių litų per metus. Tokie atvejai ne tik klaidina interneto vartotojus, bet ir ugdo blogą įprotį pasirinkti atsiradusiame perspėjime antrąjį variantą, kuris leidžia tęsti prisijungimą prie tinklalapio. Toks duomenų šifravimas netenka prasmės, nes nelieka saugumo kontrolės (interneto vartotojas neturės galimybės atskirti, ar duomenis perima piktavalis, ar tiesiog sertifikatas nėra patvirtintas).

Interneto naršyklė leidžia peržiūrėti viešojo sertifikato informaciją, tačiau sužinoti, ar sertifikatas yra tikras, ar padirbtas, be trečiosios šalies (CA) patvirtinimo nėra galimybės. Pamačius tokį perspėjamąjį pranešimą, rekomenduojama pasiteirauti tinklalapio savininko apie tai, kokį viešąjį sertifikatą jis naudoja. Jei šis informuos, kad jo naudojamo sertifikato nepatvirtina trečioji šalis (CA), tuomet įsitikinti sertifikato tikrumu jūs galėsite tiktai pasiteiravę, koks yra sertifikato viešasis raktas ir palyginę jį su naršyklėje rodomu sertifikato viešuoju raktu. Jeigu tinklalapio savininkas pasakys, kad jo naudojamą sertifikatą patvirtina trečioji šalis (CA), vadinasi, jūsų duomenis šiuo metu kažkas perima. Jokiu būdu nepateikite savo duomenų ir apie tai praneškite už informacijos saugą atsakingam jūsų įmonės darbuotojui arba savo interneto paslaugų tiekėjams.



5 pav. Supaprastintas https protokolo veikimo principas, kai SSL sertifikatas nėra registruotas trečiojoje šalyje (CA)

SSL SERTIFIKATŲ TIPAI

SSL sertifikatai yra skirstomi pagal šiuos požymius:

- Šifravimo rakto ilgį.
- Draudimo išmokos dydį. *(Išmoka svyruoja nuo kelių tūkstančių iki kelių milijonų litų. Dažniausiai kuo brangesnis sertifikatas, tuo didesnė suma.)*
- Suderinamumą su naudojamomis naršyklėmis. *(Šiuo metu tinklalapiai yra prieinami naudojantis įvairiausiomis naršyklėmis (Internet Explorer, Mozilla Firefox, Opera ir kt.), todėl geriausiai būtų įsigyti tokį sertifikatą, kuris būtų suderinamas su visomis naršyklėmis ir visomis jų versijomis. Daugelis sertifikatų platintojų tvirtina, kad jų sertifikatai yra suderinami su 99 ir daugiau procentų naršyklių.)*
- Patvirtintos informacijos apie sertifikato turėtoją apimtį. *(Trečioji šalis (CA) gali patvirtinti ne tik tai, kad viešasis raktas priklauso būtent šiam tinklalapio adresui, bet ir įvardyti, kam priklauso šis tinklalapis. Tokiu atveju išauga pasitikėjimas tinklalapiu.)*