SSL

1 Zer da SSL?

SSL (Secure Sockets Layer) bezero eta zerbitzari batean informazioaren transmisioa era seguruan egin dezaten sortutako protokolo estandar bat da. Normalean web zerbitzari baten eta nabigatzaile baten artean, edo posta zerbitzari eta bezero baten artean egiten den komunikazioa segurua izateko erabiltzen da.

SSLren bidez kreditu txartel zenbakia, gizarte segurantzako zenbakia, saioa hasteko kredentzialak eta antzeko isilpeko informazioa era seguruan bidali ahalko ditugu. Normalean zerbitzariaren eta bezeroaren artean transmititzen diren datuak testu laua bezala bidaltzen dira, entzun nahi dutenek eskuratzeko aukera emanez. Erasotzaile batek web zerbitzari eta nabigatzailearen artean bidaltzen den informazioa atzematen badu zailtasunik gabe irakurtzeko eta erabiltzeko aukera izango du.

SSL, zehazki, segurtasun protokolo bat da. Protokoloek algoritmoak nola erabili beharko liratekeen deskribatzen dute. Kasu honetan, SSL protokoloak datuak lotu eta bidali behar ditugunean nola enkriptatu zehazten dute.

Nabigatzaile guztiek dute web zerbitzari seguruekin elkarreragiteko aukera SSL protokoloa erabiliz. Hala ere, bai nabigatzaileak bai zerbitzariak SSL Certificate ziurtagiria beharko dute konexio segurua finkatu ahal izateko.

SSLk egunero milioika Interneteko erabiltzaileren datuak aseguratzen ditu, batez ere online transakzioetan eta informazio konfidentziala transmititzean.

2 Nola funtzionatzen du?

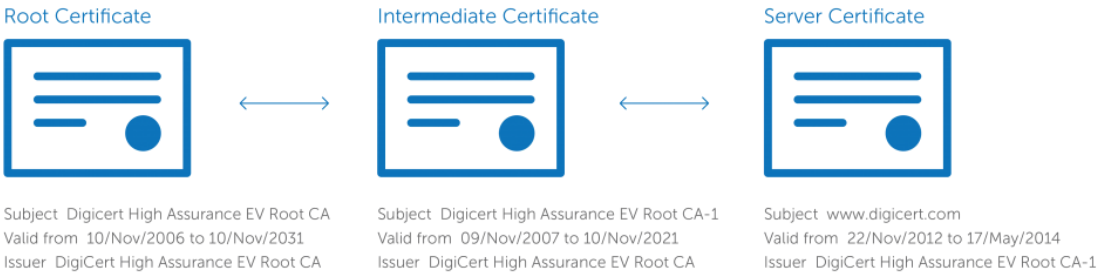
Online enpresen ezinbesteko osagai bat bezero potentzialak seguru sentituko diren ingurune bat sortzea da. SSL ziurtagiriek konfiantza erlazio bat ematen dute konexio segurua bermatuz. Bisitariei konexioa segurua dela bermatzeko, nabigatzaileek keinu bisual batzuk egiten dituzte sarraila baten ikonoa edo barra berde bat erakutsiz.

SSL ziurtagiriek giltza pare bat dute: giltza publikoa eta pribatua. Giltza hauek batera lan egiten dute konexio enkriptatu bat sortzeko. Ziurtagiriek “gaia” delakoa ere badute, hau ziurtagiri/webgunearen jabearen identitatea da.

Ziurtagiri bat sortzeko CSR (Certificate Signing Request) bat sortu beharko da zerbitzarian. Prozesu honek giltza pribatu bat sortzen du. CSR datu fitxategiak zure ziurtagiri publikoa du eta hau SSL ziurtagiri bidaltzaileari (Certificate Authority edo CA) bidaltzen zaio. CAk CSR hori darabil zure gako pribatuarekin datorren egitura bat sortzeko, baina gakoa bera konprometitu gabe. CAk ez du inoiz gako pribatua ikusten.

Behin SSL ziurtagiria jasotzen denean zure zerbitzarian instalatuko duzu. Baita zure sinesgarritasuna bermatuko duen tarteko ziurtagiria ere. Hau CAren oinarrizko ziurtagirira lotuta egongo da. Zure ziurtagiria instalatu eta probatzeko pausoak ezberdinak izango dira zure zerbitzariaren arabera.

Ondorengo irudian ziurtagiri katea delakoaren adibide bat ikus daiteke, zure zerbitzariaren ziurtagiriaren CAren ziurtagirira lotzen duena tarteko ziurtagiri baten bidez.



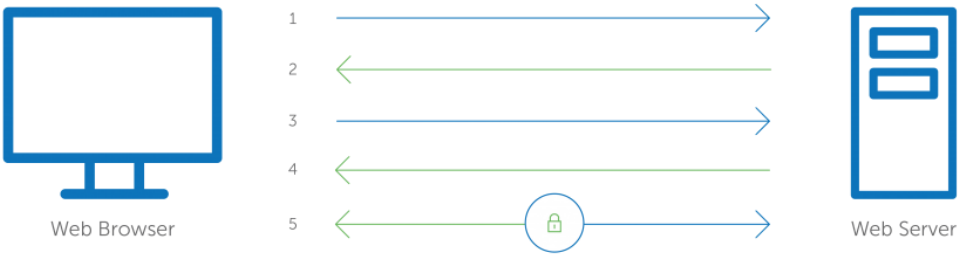
SSL ziurtagiri baten atal garrantzitsuena konfiantzako CA ezagun baten ziurtatua egotea da. Edonork sortu dezake ziurtagiri bat baina zerbitzariek beraien konfiantzazko organizazioek emandako ziurtagirietan bakarrik sinesten dute. Nabigatzaileak aurre-instalatutako konfiantzazko CA zerrenda batekin datoz.

3 Nola sortzen du SSL ziurtagiri batek konexio segurua?

Nabigatzaile batek SSL bidez ziurtatuta dagoen webgune batera sartzean, nabigatzaileak eta web zerbitzariak SSL konexio bat ezartzen dute “SSL Handshake” izeneko prozesu baten bidez. Aipatu behar da prozesu hau bat-batekoa dela eta erabiltzaileak ez duela sumatzen.

Oinarrian, hiru gako erabiltzen dira SSL konexio bat sortzeko: publikoa, pribatua eta tartekoa. Gako publikoarekin enkriptatutako edozer gako pribatuarekin bakarrik desenkriptatu daiteke, eta alderantziz.

Enkriptatze eta dekriptatze prozesuek prozesamendu indar asko hartzen dutenez, SSL Handshake prozesuaren bitartean bakarrik egiten da sesio simetrikoko gako bat sortzeko. Konexio segurua egin ondoren sesio gakoa erabiltzen da transmititutako datu guztiak enkriptatzeko.



1. Nabigatzailea web zerbitzari (webgune) batera konektatzen da SSL seguru baten bidez (https). Nabigatzaile eskari hauek zerbitzariak berak identifikatzen ditu.
2. Zerbitzariak bere SSL ziurtagiriaren kopia bat bidaltzen du, bere gako publikoa barne.
3. Nabigatzaileak ziurtagiriaren oinarria bere konfiantzazko zerrendarekin alderatzen du ziurtagiria indarrean dagoela, eta izena konektatzen ari garen zerbitzariarekin bat datorrela ikusteko. Nabigatzaileak ziurtagiria ontzat ematen badu, sesio simetrikoko gakoa sortu, enkriptatu eta bidaliko dio zerbitzariari bere gako publikoa erabiliz.
4. Zerbitzariak sesio simetrikozko gakoa dekriptatuko du gako pribatua erabiliz eta onarpen mezu bat bidaliko dio nabigatzaileari enkriptatutako sesioa hasteko.

5. Zerbitzariak eta bezeroak transmititutako informazio guztia sesioko gakoa erabiliz enkriptatuko dute hemendik aurrera.

4 Nire ziurtagiria SSL edo TLS da?

SSL izan da informazioa era seguruan transmititzeko beti erabili den protokoloa. Bertsio berri bat publikatzen zen bakoitzean bertsio zenbakia bakarrik aldatzen zen. Baina SSL3v3.0tik SSLv4.0ra aldatzeko momentua iritsi zenean izena aldatu zitzaion TLSv1.0ra. Gaur egun TLSv1.2 bertsioan gaude.

5 Nola instalatu SSL Apache Zerbitzarian

Ondorengo adibideak Ubuntu 12.04 LTS Server batean SSL ziurtagiria nola instalatu daitekeen azaltzen du. Prozedura hau desberdina izan daiteke beste distribuzio batzuentzat.

Lehenik eta behin Apache martxan izan behar dugu gure Ubuntu zerbitzarian.

SSL ziurtagiriak non izango ditugun erabakiko dugu (adibidez /etc/apache2/ssl):

```
sudo mkdir /etc/apache2/ssl
```

Orain 3 urterako (1095 egun) balioko diguten ziurtagiriak sortuko ditugu ondorengo agindua erabiliz:

```
sudo openssl req -x509 -nodes -days 1095 -newkey rsa:2048 -out
/etc/apache2/ssl/server.crt -keyout /etc/apache2/ssl/server.key
```

Honekin ondorengoa agertuko zaigu eta galdera batzuk egingo dizkigu.

```
Generating a 2048 bit RSA private key
.....................................+++
.....................+++
writing new private key to '/etc/apache2/ssl/server.key'
-----
You are about to be asked to enter information that will be
incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or
a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:FR
State or Province Name (full name) [Some-State]:Poitou
Locality Name (eg, city) []:Montamise
Organization Name (eg, company) [Internet Widgits Pty Ltd]:Internet
Self CA
Organizational Unit Name (eg, section) []:IT
Common Name (e.g. server FQDN or YOUR name) []:demo.hallard.me
Email Address []:mydummy@email.com
```

Garrantzitsuena Common Name edo izen arrunta da, FQDN interneteko izenarekin bat etorri beharko litzateke (kasu honetan demo.hallard.me).

Orain Apacheren SSL modulua instalatuko dugu. Agindu honek /etc/apache2/ports.conf fitxategia aurrekonfiguratzen du lerro batzuek gehituz. Hauen artean 443 portua entzuteko esaten duena.

```
sudo a2enmod ssl
```

Aurrezarritako SSL (default-ssl) eskuragarri jarriko dugu lotura sinboliko bat eginez:

```
sudo ln -s /etc/apache2/sites-available/default-ssl.conf
/etc/apache2/sites-enabled/000-default-ssl.conf
```

Orain eskuragarri jarri berri dugun default-ssl.conf aldatuko dugu.

```
sudo nano /etc/apache2/sites-enabled/000-default-ssl.conf
```

Eta SSL ziurtagiriari dagozkion bi lerroak aldatuko ditugu ondoren azaltzen den bezala:

```
SSLCertificateFile    /etc/apache2/ssl/server.crt
SSLCertificateKeyFile /etc/apache2/ssl/server.key
```

Berrabiarazi ezazu Apache zerbitzaria eta konektatu zaitez zure webgunera. Nabigatzaileak abisu bat erakutsiko dizu, erabiltzen ari zaren ziurtagiria zuk sortutakoa delako eta ez konfiantzazko CA batena. Onartu ezazu salbuespena eta zure webgunea ikusi ahal izango duzu.

Salbuespena gehiago agertzerik nahi ez baduzu ziurtagiria zure konfiantzazko CA zerrendara gehitu dezakezu bezeroan. Prozedura hau sistema eragilearen eta nabigatzailearen araberakoa da.

Doako CA ziurtagiri bat lortu nahi izanez gero hemen duzu doako aukera bat (StartSSL erabiliz).

Montajetxoa

Entregatu beharrekoa: Worden dokumentatu pausoz-pauso.

Egin beharrekoa:

Hiru makina birtual

- Wbuntu (web zerbitzaria izango dena, Apacherekin)
- Windows Server (DNS zerbitzaria izango dena)
- Bezeroa, nahi den sistema eragilearekin

Hiru makinak sare lokal berdinean egon beharko dira, Host Only modua erabiliko dugu VMWaren, IP ta maskara zuek aukeratu.

Ubuntu bat muntatuko dugu Apache web zerbitzariarekin eta bertan bi webgune jarriko ditugu eskuragarri, Virtual Hostak erabiliz. Virtual Hostak aukera ematen digu, web zerbitzari bakarrean hain bat webgune eskaitzeko, adibide ohikoena hosting-a eskaintzen duen enpresa bat izango litzake, web zerbitzari oso potentea izan eta hain bat webgune ahokatuko dituelarik. Baina oraingoan https bidez konektatzeko aukera emango dugu, SSL erabiliz. Webgunea modu seguruan bidaliko delarik. Horretarako OpenSSL erabiliz ziurtagiria eta giltza sortu beharko ditugu, webgune bakoitzarentzat bana sortu daiteke edo biak berdinarekin, nahi den bezala (hemen tutorial bat).

Windows Serverra, DNS zerbitzaria izango da, gure domeinuak gehitu beharko dizkiogu, nire kasuan, adibidez amaia.eus eta luis.eus

Bezerotik Ubuntuan alojatuta dagoen webguneak ikusi beharko ditugu https://amaia.eus eta https://luis.eus helbidea sartuta, ziurtagiria atera beharko da, baimena eman eta erakutsiko digu, horretarako erabiliko duen DNS-a Windows Serverrean muntatua duguna dela esan beharko diogu.