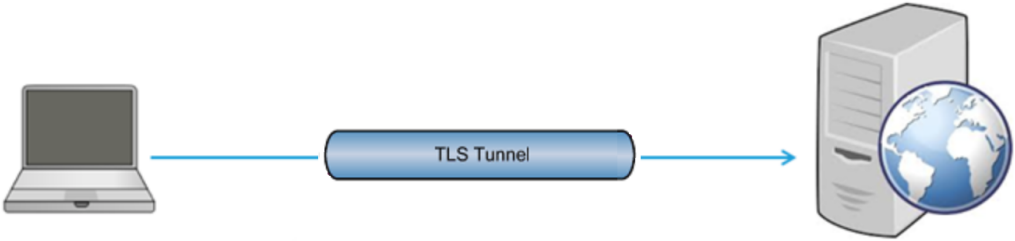
TLS biztonságos használata

Tihanyi Norbert

TLS vagy SSL?

Definíció

*A **Transport Layer Security (TLS)** és elődje a Secure Sockets Layer (SSL), titkosítási protokollok amely kliens/szerver alapú alkalmazások számára lehetővé teszi a biztonságos kommunikációt.*

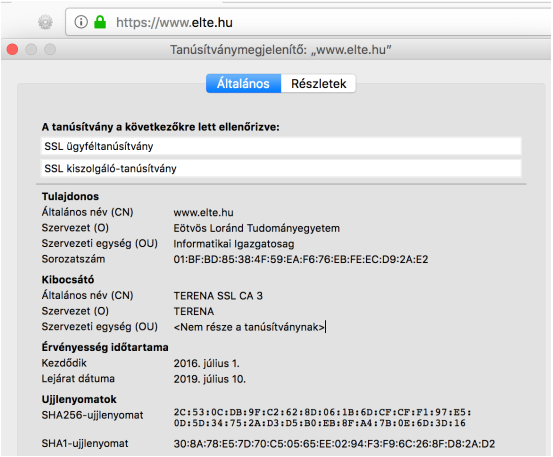


Felhasználási területek

A TLS felhasználási területe nagyon sokrétű. Néhány példa a teljesség igénye nélkül:

- Elektronikus levelezés
- Adatbázis kapcsoltok védelme
- Virtuális magánhálózat titkosítása
- VOIP
- **Web böngészés (HTTPS)**

A tanúsítványban szereplő adatok...



Tanúsítványok típusai

A Webes tanúsítványok 3 fő csoportját lehet megkülönböztetni:

- DV - Domain Validated tanúsítvány
- OV - Organization Validated tanúsítvány
- EV - Extended Validated tanúsítvány

Definíció (DV tanúsítvány)

A legelterjedtebb TLS tanúsítvány, amely során kizárólag a domain név kerül validálásra. ***A legtöbb esetben a tanúsítvány kibocsátó kizárólag azt ellenőrzi, hogy van-e hozzáférésünk az adott domainhez.***

Tanúsítványok típusai

Definíció (OV tanúsítvány)

Az OV tanúsítványok, már nem csak a Domain nevet ellenőrzik, hanem, hogy az igénylést végző cég valóban létezik-e. A tanúsítványban szerepel már az igénylést végző cég neve is. Ilyen módon sokkal több bizalmat nyújt egy OV tanúsítvány egy szimpla DV tanúsítvánnyal szemben.

Tanúsítványok típusai

Definíció (EV tanúsítvány)

Az EV tanúsítványok a nevükből adódóan adják a legnagyobb bizalmat a webes tanúsítványok körében. A cég név nem csak a tanúsítványban, hanem a böngészők címsorában is megjelenik, illetve a böngészők sávja zöldre vált, jelezve, hogy EV tanúsítvány gondoskodik a honlap védelméről. A tanúsítvány kiállításához sokkal több információt és további dokumentumokat kell szolgáltatni annak érdekében, hogy a cég hitelességét a kibocsátó ellenőrizni tudja.

Az a bizonyos zöld csík - EV tanúsítvány

Javasolt tanúsítványok használata

Nem minden szolgáltató ad ki DV SSL tanúsítványt. A phising támadások egyre gyakoribb elterjedése miatt több szolgáltató (Pl: DigiCert) nem ad ki egyszerű DV tanúsítványt.

Javasolt OV vagy a még szigorúbb ellenőrzési feltételeknek alávetett EV tanúsítványok használata.

Tökéletes SSL/TLS beállítás

- -SSLv2 -SSLv3 és -TLS 1.0 protokollok tiltása
- Javasolt a TLS 1.2 használata
- Ismert gyengeségeket tartalmazó algoritmusok tiltása. (Pl: RC4-SHA , RC4-MD5, stb.)
- Engedélyezni: HSTS, Forward Secrecy, Secure Renegotiation

TLS biztonságos használata

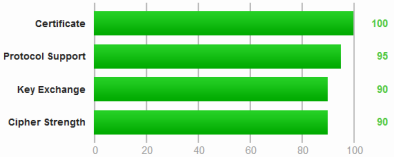
(Qualys teszt A+)

QUALYS® SSL LABS

Summary

Overall Rating

A+



Visit our documentation page for more information, configuration guides, and books. Known issues are documented here.

This server supports TLS_FALLBACK_SCSV to prevent protocol downgrade attacks.

This server supports HTTP Strict Transport Security with long duration. Grade set to A+. MORE INFO »

HTTPS = maximális biztonság?

A HTTP nem minden esetben jelenti azt, hogy az oldal biztonságos.

Az alábbi oldal a Microsofthoz tartozik

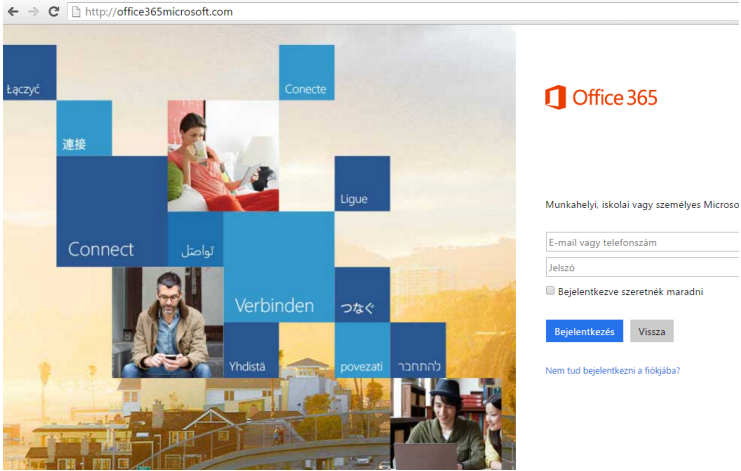
`https://login.microsoftonline.com/`

Az alábbi oldalt 8.99$ regisztráltuk:

`https://login.office365microsoft.com`

TLS biztonságos használata

Adathalászatra is használható `http://office365microsoft.com`



RSA - Figyelmeztetés! - please shut down![Microsoft Office E2127410] 198.199.76.26

”RSA, The Security Division of EMC (“RSA”), an information security company, has been appointed to assist Microsoft Office in preventing or terminating online activity that targets, or may target Microsoft Office’s clients as potential fraud victims.

RSA has been made aware that your company appears to be providing internet services to a website, which is making unauthorized use of Microsoft Office’s trademarks. This site http://office365microsoft.com not only violates Microsoft Office’s copyright, trademarks and other intellectual property rights, but may also become a host to a phishing attack, or other fraudulent scams directed against Microsoft Office and Microsoft Office’s clients. ”

A böngészők már figyelmeztetnek...

Let'sencrypt CA tanúsító

A Let's Encrypt egy ingyenesen használható CA tanúsító szervezet.

- Néhány másodperc alatt lehet DV tanúsítványt igényelni.
- A kiállítás is néhány másodpercen belül megtörténik.
- A biztonságos konfiguráció is néhány perc alatt elvégezhető

www.weakssl.com esettanulmány

Pollard $p-1$ algoritmusa

Algorithm 1 POLLARD $p-1$

```
select a smoothness bound B                          ▷ not necessary explicitly
while the time limit is not reached do
    L ← ∏_{primes q≤B} q^{⌊log_q B⌋}
    c ← a random integer comprime to N
    d ← gcd(c^L, N)                                  ▷ using modular arithmetic
    if 1 < d < N then return d
    end if
    if d = 1 then select a larger B
    else                                             ▷ d = N
        select a smaller B
    end if
end while
```

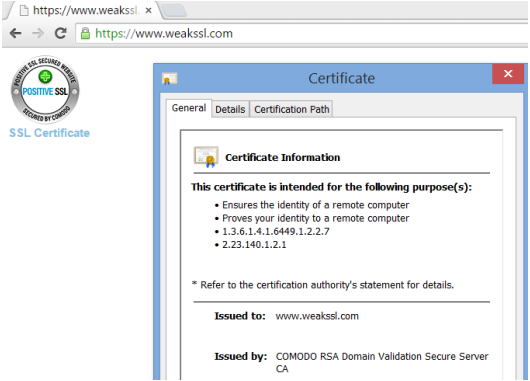
Nem biztonságos DV tanúsítvány?

A prímszámgeneráló metódus az alábbi módon történt:

```
while P ≠prime do
    P ← 2
    while BinaryLength(P < 1024) do
        P ← P · nextprime(random(100000))
    end while
    P ← P + 1
end while
```

Megfelelő tanúsítvány: www.weakssl.com

A Privát kulcs szándékosan ”rossz módon” került kiállításra. A tanúsítvány a COMODO CA által lett kiállítva a www.weakssl.com-ra.



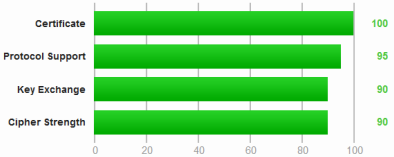
A lehető legjobb TLS beállítás a www.weakssl.com-on

QUALYS® SSL LABS

Summary

Overall Rating

A+



Visit our documentation page for more information, configuration guides, and books. Known issues are documented here.

This server supports TLS_FALLBACK_SCSV to prevent protocol downgrade attacks.

This server supports HTTP Strict Transport Security with long duration. Grade set to A+. MORE INFO »

2048 bites nyilvános kulcsból a privát kulcs visszaállítása

Kiadott parancs:

openssl s_client -connect www.weakssl.com:443 </dev/null | openssl x509 -noout -modulus

```
root@weakssl:~# openssl s_client  -connect www.weakssl.com:443 </dev/null  |  op
enssl x509 -noout -modulus
depth=3 C = SE, O = AddTrust AB, OU = AddTrust External TTP Network, CN = AddTru
st External CA Root
verify error:num=19:self signed certificate in certificate chain
verify return:0
Modulus=8E6994A179BF0D66327670641E08F57B14533BBD47D14C919C2BBA454E74E4C9647A966B
B01AA8DD5C287B50BF6DEA123E8B81C0B681CE69E0F7B7833232B852C9A2BDED515FFA150972A453
D1A59DEF05DF52EBFE80D810949792688C4163D80DA73D8CBEDBEA45134CD73E3ABD5FEA0362BF9E
C3F67A5EAAEED3560667AC018CE4A002B88803F9EC5A5193FB6DFF9FA53307E866E29E19FF4855B5
90EEE98089DC709A1CDBE55DEBE58E56B1773C2FC3BC8F712CEC7923FA02C8F8BA37A63444B7D9D3
11E8FA7AC0AE1EE35AA99871086653E7394170EB43112AE3ED1D80C76E48A1EEDFB97F1AE72B39F7
739203C67B20C39B6AD9D01546C1FA27D8F7510D
DONE
root@weakssl:~#
```

A faktorizáció kevesebb mint 2 percett vett igénybe

```
? \r PARI_source.txt
%2 = 1797790303401935406964498180248050792797869847223927013026898209960718636068
752177791898189796770606379490684129768533626164704560430224968673414035083488234
5170042540582931133624884735237597546391572852716769096627794708794127624765166
472662358993169988859217646097678425318193724107739605766420252499277695198925095
175994475739841682922637243505403562623971680638404095813809454376766531045786584
4276489890486268050750563221156854304974697788690592286508349460874653102748901
876169662086012364227278156326875888588698261901742792025702027430793394651931190
045693987696344630360681339962904598647711873462238030932 61
? Pollard
%3 = (n)->a=vector(10000003,i,i+1);k=2;while((gcd(n,a[k-1]-1)%n)==1,a[k]=Mod(a[k
-1],n)^k;k++;);print(lift(gcd(n,a[k-1]-1)))
? #
   timer = 1 (on)
? Pollard(N)
1055622402733389164788437146296377088525361874854296109586526021495709164316545188
1185617004249758205339643677465686952091522545020289237954998344446323993284150490
4924142811925441567952904913150856732738434780357666981857964002582637673402496296
77939712191826494239105251540255570038165263350367830028102507 9
time = 1min, 31,091 ms.
```

Köszönöm a figyelmet!