

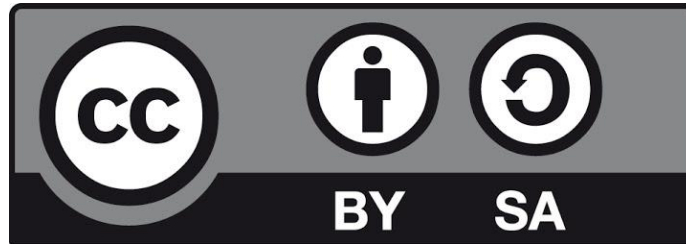
Το πρωτόκολλο TLS και εφαρμογές

Εισηγητής: Χρήστος Δαλαμάγκας

cdalamagkas@gmail.com

Άδεια χρήσης

Το παρόν εκπαιδευτικό υλικό υπόκειται στη διεθνή άδεια χρήσης Creative Commons Attribution-ShareAlike 4.0 (<https://creativecommons.org/licenses/by-sa/4.0/>).



Ατζέντα

- Εισαγωγή στο TLS
- Η χειραψία TLS
- Εφαρμογές του TLS
 - HTTPS
 - DNS over TLS
 - SSH

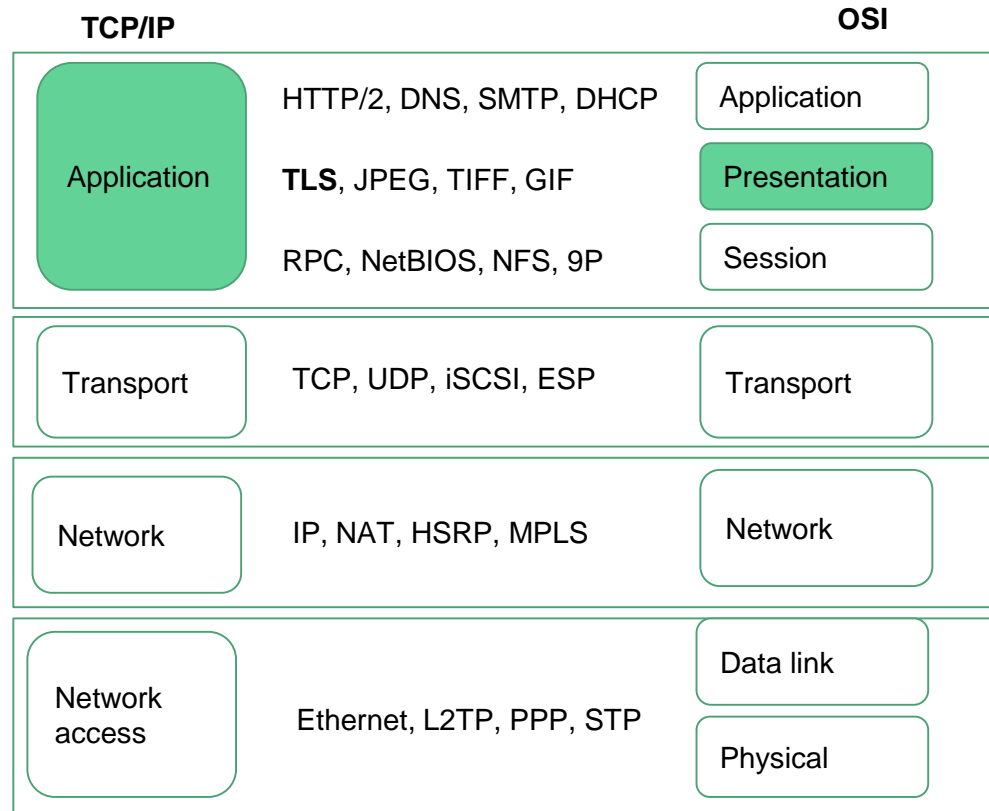
Εισαγωγή στο TLS

Transport Layer Security (TLS)

- Ορισμός: Είναι το πρωτόκολλο που διαπραγματεύεται παραμέτρους ασφάλειας σε μια σύνδεση στο Διαδίκτυο. Συγκεκριμένα, διασφαλίζει:
 - Κρυπτογράφηση δεδομένων (data encryption)
 - Πιστοποίηση εξυπηρετητή (server authentication)
 - Ακεραιότητα μηνυμάτων (data integrity)
 - Προαιρετικά, πιστοποίηση πελάτη (client authentication)
- Το TLS αποτελεί διάδοχος του πρωτοκόλλου SSL (Secure Socket Layer)
- Τρέχουσα έκδοση: TLS v1.3 και TLS v1.2

Το TLS στα εννοιολογικά μοντέλα

- Το TLS ανήκει στο επίπεδο παρουσίασης του OSI
- Παρέχει υπηρεσίες ασφάλειας στις τελικές εφαρμογές



Χειραψία Transport Layer Security (TLS)

- Το TLS ορίζει μια διαδικασία ανταλλαγής μηνυμάτων ώστε να επιλεγούν τα κατάλληλα πρωτόκολλα κρυπτογράφησης για την εγκαθίδρυση της ασφαλούς συνεδρίας
- Η διαδικασία της διαπραγμάτευσης ονομάζεται χειραψία TLS
- Σημαντικό: Η κρυπτογράφηση του περιεχομένου μιας συνεδρίας TLS γίνεται με τη χρήση ενός συμμετρικού κλειδιού που δημιουργείται και ανταλλάσσεται κατά τη διάρκεια της χειραψίας
- Το πιστοποιητικό στο TLS χρησιμοποιείται μόνο για την ταυτοποίηση εξυπηρετή ή για την κρυπτογράφηση (με το δημόσιο κλειδί) μόνο κάποιων αρχικών πληροφοριών

Παράδειγμα χειραψίας TLS

- Ο πελάτης στέλνει ένα μήνυμα **ClientHello** στον εξυπηρετητή με τα εξής:
 - Αίτηση για την εγκαθίδρυση ασφαλούς σύνδεσης, μαζί με την υποστηριζόμενη έκδοση TLS
 - Λίστα με τα υποστηριζόμενα σετ πρωτοκόλλων κρυπτογραφίας (cipher suites)
 - Έναν τυχαίο αριθμό
- Ο εξυπηρετητής επιλέγει ένα από τα cipher suites και την κατάλληλη έκδοση TLS και αποστέλλει το μήνυμα **ServerHello**, μαζί με έναν δικό του τυχαίο αριθμό
- Αμέσως μετά, ο εξυπηρετητής στέλνει το πιστοποιητικό του με το μήνυμα **Certificate**
- Αν χρησιμοποιείται Diffie-Helman για την ανταλλαγή κλειδιών, τότε στέλνεται και ένα μήνυμα **ServerKeyExchange**

Παράδειγμα χειραψίας TLS

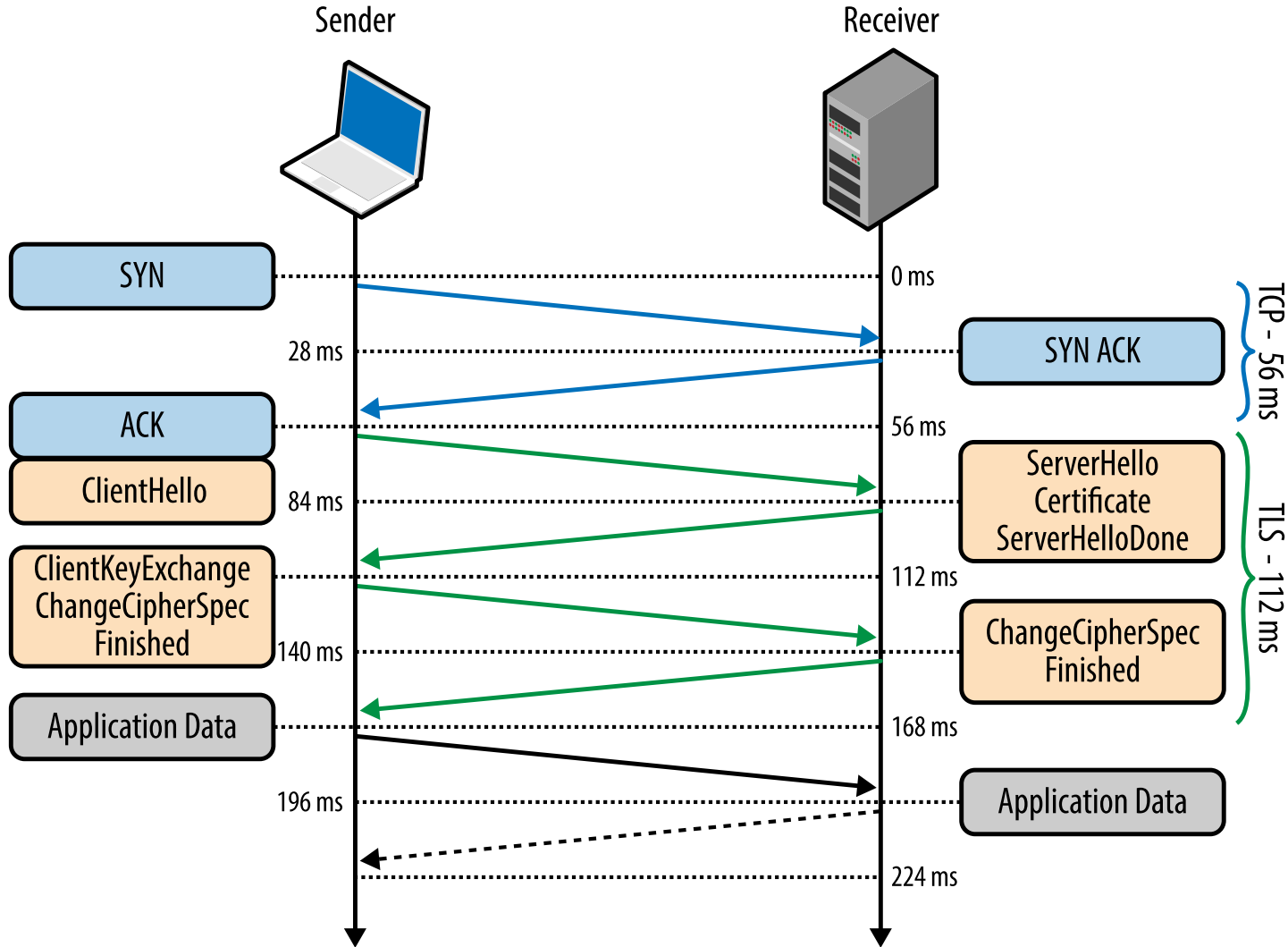
- Ο εξυπηρετητής ολοκληρώνει την αποστολή μηνυμάτων με το **ServerHelloDone**
- Αφού έχει επιβεβαιωθεί η ταυτότητα του εξυπηρετητή, ο πελάτης απαντά με το μήνυμα **ClientKeyExchange**, στο οποίο ενσωματώνει ένα προσωρινό μυστικό κλειδί (PreMasterSecret) που κρυπτογραφείται με το δημόσιο κλειδί του εξυπηρετητή
- Το κάθε άκρο επικοινωνίας παράγει ανεξάρτητα ένα κοινό μυστικό κλειδί (**MasterSecret** ή κλειδί συνόδου – session key) χρησιμοποιώντας τα εξής:
 - Τους τυχαίους αριθμούς που έλαβε ο καθένας στα πρώτα βήματα
 - Το PreMasterSecret

Παράδειγμα χειραψίας TLS

- Η ασφαλής συνομιλία συνεχίζεται με συμμετρική κρυπτογράφηση

Παρατηρήσεις:

- Οι αλγόριθμοι RSA και Diffie-Helman καταναλώνουν τους περισσότερους επεξεργαστικούς πόρους
- Ο αλγόριθμος RSA χρησιμοποιείται ΜΟΝΟ κατά τη χειραψία TLS (αυθεντικοποίηση και μοιρασμός του PreMasterSecret)
- Η ασφάλεια της συνομιλίας εξαρτάται από τον συμμετρικό αλγόριθμο κρυπτογράφησης που θα επιλεγεί κατά τη χειραψία



Εναλλακτική αναπαράσταση της χειραψίας TLS

- **Πελάτης:** Γειά! Θέλω να εγκαθιδρύσουμε ασφαλή σύνδεση μεταξύ μας. Να, πάρε τα cipher suit που υποστηρίζω, έναν τυχαίο αριθμό και την έκδοση TLS που υποστηρίζω
- **Εξυπηρετητής:** Γειά σου πελάτη. Έλεγξα τα cipher suit και την έκδοση TLS, είμαστε OK για να προχωρήσουμε. Πάρε το πιστοποιητικό μου και τσέκαρέ το. Α, πάρε και έναν δικό μου τυχαίο αριθμό.
- **Πελάτης:** Επίτρεψέ μου να επιβεβαιώσω το πιστοποιητικό [...] Φαίνεται OK το πιστοποιητικό αλλά πρέπει να επιβεβαιώσω το ιδιωτικό σου κλειδί. Για να το κάνω αυτό, θα δημιουργήσω και θα κρυπτογραφήσω ένα pre-master key με το δικό σου δημόσιο κλειδί. Αποκρυπτογράφησε το με το ιδιωτικό σου κλειδί και μαζί με τον τυχαίο αριθμό που σου έδωσα, φτιάξε το συμμετρικό κλειδί

Client Server

3. The Client verifies
the SSL certificate
information



SSL Server

5. The server
verifies client
certificate (if
required)



1. Client Sends Hello, Cipher Suite, & Client Random

2. Server respond back by sending the server random & SSL
certificate (Private Key)

4. Pre-master key generated using the Public Key

6. Pre-master key decrypted using the Private key

7. A Master Key or Master-secret is in place now

8. This master key is used for encryption & decryption



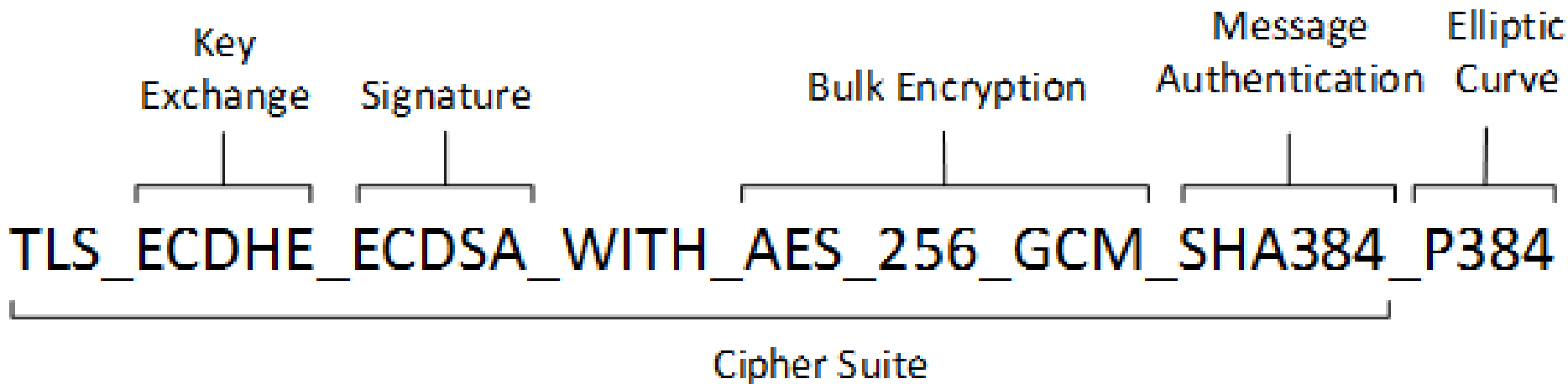
SSL Handshake Process

Cipher suites

- Ορισμός: Είναι σετ αλγορίθμων που βοηθούν την εγκαθίδρυση και διατήρηση μιας ασφαλούς σύνδεσης TLS
- Ένα cipher suite αποτελείται από τα εξής:
 - Αλγόριθμος ανταλλαγής κλειδιών (πχ Diffie-Helman)
 - Αλγόριθμος συμμετρικής κρυπτογράφησης - bulk encryption algorithm (πχ AES, 3DES)
 - Τον αλγόριθμο HMAC (πχ SHA1, SHA256)
- Στη διαπραγμάτευση TLS, ένας συνδυασμός από τους παραπάνω χρησιμοποιείται για τη συνέχιση της ασφαλούς σύνδεσης
- Ένα cipher suite προσδιορίζεται από ένα αλφαριθμητικό - string

Ενδεικτικά cipher suite

- TLS_DHE_RSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256



Το εργαλείο openssl

Openssl

- Σε λειτουργικά συστήματα Linux υπάρχει διαθέσιμη η βιβλιοθήκη / σουίτα εργαλείων openssl
- Το openssl παρέχει μια πλήρως λειτουργική υλοποίηση των πρωτοκόλλων και αλγορίθμων TLS
- Είναι γραμμένο σε C, Perl και assembly
- Τρέχουσα έκδοση η 1.1.1
 - TLS 1.3
 - SHA-3
- Πολλές εφαρμογές που χρησιμοποιούν TLS χρησιμοποιούν τις υλοποιήσεις που παρέχει το openssl

Παράδειγμα - Δημιουργία πιστοποιητικού self-signed

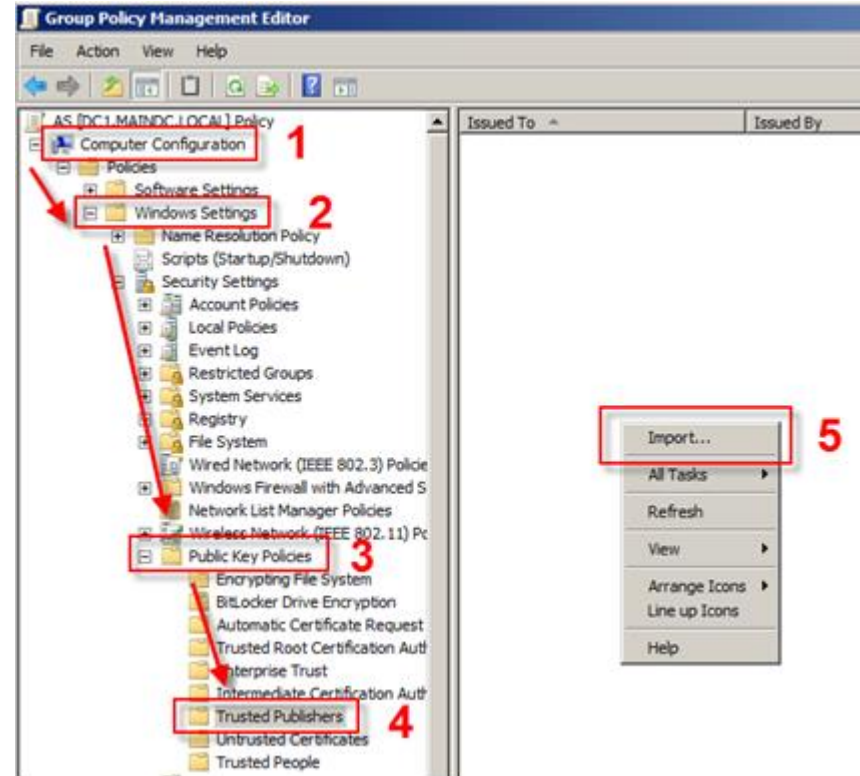
Αν δεν έχουμε πρόσβαση σε Αρχή Πιστοποίησης, μπορούμε να φτιάξουμε ένα αυτοϋπογραφόμενο πιστοποιητικό (self-signed)

- `openssl genrsa -out example.key 4096`
- `openssl req -new -key example.key -out example.csr -sha384`
- `openssl x509 -req -in example.csr -signkey example.key -out example.crt -days 365`

Περισσότερες εντολές: <https://medium.freecodecamp.org/openssl-command-cheatsheet-b441be1e8c4a>

Παράδειγμα – Δημιουργία CA και υπογραφή πιστοποιητικού

- Αρχή Πιστοποίησης (CA) είναι οποιαδήποτε οντότητα που της ανήκει ιδιωτικό/δημόσιο κλειδί και πιστοποιητικό
- Η διαφορά με τα υποκείμενα είναι ότι οι CA θεωρείται **έμπιστη**
- Μπορούμε και μεις να φτιάξουμε μια CA, ως self-signed certificate, αρκεί να το μοιράσουμε στους υπολογιστές που θέλουμε να το εμπιστεύονται
- Το Active Directory δίνει τη δυνατότητα μοιρασμού ενός πιστοποιητικού μέσω Group Policy



Παράδειγμα – Δημιουργία Αρχής Πιστοποίησης και υπογραφή πιστοποιητικού

Για την δημιουργία ενός πιστοποιητικού για έναν πελάτη/υποκείμενο και υπογραφή του από την CA:

- `openssl genrsa -out client.key 4096`
- `openssl req -new -key client.key -out client.csr -sha384`
- `openssl x509 -req -in client.csr -signkey myca.key -out client.crt -days 365`

Εφαρμογές του TLS

Εφαρμογές του TLS

- **HTTPS:** Ασφαλείς συνδέσεις σε ιστότοπους
- **DNS over TLS:** Ασφαλής ανταλλαγή μηνυμάτων DNS
- **SSH:** Ασφαλής σύνδεση στο κέλυφος (shell) ενός απομακρυσμένου υπολογιστή
- **SMTP, POP3, IMAP over TLS:** Ασφαλής ανταλλαγή email με το TLS
- **OpenVPN:** Εγκαθίδρυση ασφαλών τούνελ VPN με το TLS

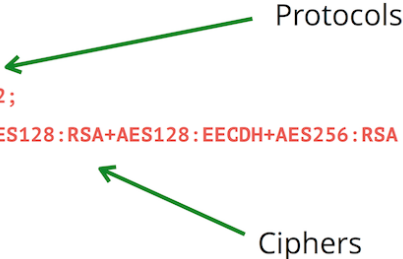
Ένα VPN διασυνδέει με ασφάλεια απομακρυσμένα τοπικά δίκτυα ή έναν χρήστη με ένα απομακρυσμένο τοπικό δίκτυο.

Ρύθμιση HTTPS στον nginx

Ρύθμιση HTTPS σε nginx

- Για ενεργοποίηση του HTTPS στο nginx μπορεί κάποιος να τροποποιήσει το αρχείο ρυθμίσεων (/etc/nginx/sites-available/default) ως εξής:
- Πολλά είναι τα διαθέσιμα ciphers που μπορούν να χρησιμοποιηθούν
- Η επιλογή των κατάλληλων cipher είναι σημαντική για την ασφάλεια του web server
 - <https://cipherli.st/>
Για μια προτεινόμενη λίστα με τα πιο ασφαλή cipher

```
server {  
    listen 443 ssl;  
  
    ssl_certificate /path/to/signed_cert_plus_intermediates;  
    ssl_certificate_key /path/to/private_key;  
    ssl_session_timeout 1d;  
    ssl_session_cache shared:SSL:50m;  
  
    ssl_protocols TLSv1 TLSv1.1 TLSv1.2;  
    ssl_ciphers EECDH+CHACHA20:EECDH+AES128:RSA+AES128:EECDH+AES256:RSA  
+AES256:EECDH+3DES:RSA+3DES:!MD5;  
    ssl_prefer_server_ciphers on;  
}
```





You are here: [Home](#) > [Projects](#) > [SSL Server Test](#) > [www.domsys.eu](#) > 81.0.237.109

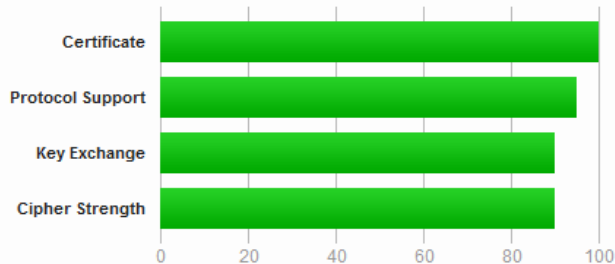
SSL Report: [www.domsys.eu](#) (81.0.237.109)

Assessed on: Fri, 07 Dec 2018 20:37:19 UTC | [Clear cache](#)

[Scan Another »](#)

Summary

Overall Rating



Visit our [documentation page](#) for more information, configuration guides, and books. Known issues are documented [here](#).

HTTP Strict Transport Security (HSTS) with long duration deployed on this server. [MORE INFO »](#)

Χαρακτηριστικά ενός ασφαλούς website

- Μήκος κλειδιού RSA ≥ 2048 bit
- Απενεργοποιημένα πρωτόκολλα παλαιότερα του TLS v1.2
- Forward Secrecy: Η εμπιστευτικότητα του κλειδιού συνόδου δεν παραβιάζεται ακόμη και αν παραβιαστεί το ιδιωτικό κλειδί
- Strict Transport Security (HSTS): Ο webserver υποχρεώνει τον browser να χρησιμοποιήσει HTTPS
- Αυτόματη ανακατεύθυνση από HTTP σε HTTPS (HTTP 301 redirect)
- ...

Γενικά βήματα ρύθμισης HTTPS στον nginx

- Απόκτηση ζεύγους ιδιωτικού/δημόσιου κλειδιού και πιστοποιητικού από μια Αρχή Πιστοποίησης
 - Δωρεάν από τη Let's Encrypt: <https://www.digitalocean.com/community/tutorials/how-to-secure-nginx-with-let-s-encrypt-on-ubuntu-18-04>
- Εναλλακτικά, μπορεί να εκδοθεί και πιστοποιητικό που οι ίδιοι υπογράφετε:
- Δημιουργία ισχυρών παραμέτρων Diffie-Helman (4096 bit)

```
openssl dhparam -out dhparam.pem 4096
```
- Ενεργοποίηση της αυτόματης ανακατεύθυνσης από θύρα 80 σε 443 (ανακατεύθυνση HTTP 301)
- Προσδιορισμός του πιστοποιητικού, του ιδιωτικού κλειδιού, των παραμέτρων DH, των cipher suite και άλλων επιλογών ασφαλείας (πχ HSTS) στο αρχείο ρυθμίσεων του nginx (/etc/nginx/sites-available/default)
 - Παραδείγματα στο <https://cipherli.st/>
- Ενεργοποίηση nginx

```
sudo service nginx start
```

DNS over TLS

DNS over TLS

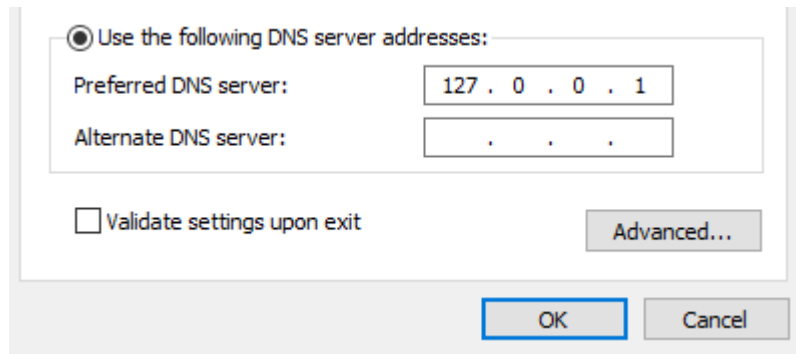
- Το DNS over TLS (DoT) χρησιμοποιεί κρυπτογράφηση για τη μετάδοση των μηνυμάτων DNS στη θύρα 853
- Προτυποποιήθηκε αρχές του 2018
 - Τα σύγχρονα λειτουργικά συστήματα δεν υποστηρίζουν εγγενώς το DoT
 - Το Android Pie (Android 9.0) πρόκειται να υποστηρίξει το DoT
- Για τα ΛΣ που δεν υποστηρίζουν DoT, μπορεί να εγκατασταθεί μια Τρίτη εφαρμογή που λειτουργεί ως dns server/resolver
 - Unbound Server

Ρύθμιση DoT με το Unbound

- Λήψη του Unbound από το επίσημο website
- Προσθήκη των ακόλουθων γραμμών στο αρχείο ρυθμίσεων του unbound

```
forward-zone:  
name: "."  
forward-ssl-upstream: yes  
forward-addr: 1.1.1.1@853
```

- Ενεργοποίηση της υπηρεσίας Unbound από το μενού Services των Windows
- Από το μενού ανάθεσης στατικών ρυθμίσεων IP, ορισμός της διεύθυνσης DNS ως τη διεύθυνση localhost
- Στη localhost ακούει ο unbound για plaintext ερωτήματα, τα οποία προωθεί κρυπτογραφημένα



Secure SHell

Secure SHell

- Πρωτόκολλο που επιτρέπει ασφαλή εγκαθίδρυση συνεδριών στο τερματικό απομακρυσμένων υπολογιστών (κύρια χρήση)
- Λειτουργεί με το μοντέλο client – server
- Για τη ρύθμιση απαιτείται ο server να δημιουργήσει ένα ζεύγος δημοσίου και ιδιωτικού κλειδιού – δε χρειάζεται πιστοποιητικό
- Ο πελάτης μπορεί να ταυτοποιηθεί με εισαγωγή ενός κωδικού πρόσβασης
- Εναλλακτικά, ο πελάτης μπορεί να κάνει login με το δημόσιο κλειδί του
 - Ο server διατηρεί όλα τα δημόσια κλειδιά, που δικαιούνται πρόσβαση στον server, στο αρχείο `authorized_keys`