Tìm hiểu về HTTPS, SSL, TLS và cách hoạt động

Tác giả: **tranducloi**

SSL và TLS là gì?

- SSL & TLS đều là **giao thức mã hóa** (*cryptographic protocols*) thiết kế để cung cấp giao tiếp bảo mật trong mạng máy tính. Có nhiều phiên bản của TLS được sử dụng rộng rãi: trình duyệt, email, tin nhắn và VoIP.
- SSL: Secure Socket Layer / TLS: Transport Layer Secure
- SSL được tạo ra bởi Netscape vào những năm 1990s để thêm giao thức HTTPS vào trình duyệt Netscape và giờ do IETF (*Internet Engineering Task Force*) quản lý.
- SSL hiện đã được coi là đã chết (*cùng với Netscape sau khi phát hành đến bản SSL 3.0 vào năm 1996*) và thay bằng TLS được phát hành lần đầu vào năm 1999.
- TLS được phát triển dựa trên người tiền nhiệm SSL. Phiên bản TLS gần nhất là TLS 1.3 định nghĩa trong RFC 8446 được phát hành vào tháng 8/2018.

SSL và TLS là gì?

- Các websites sử dụng TLS để bảo mật giao tiếp giữa server với trình duyệt.
- SSL/TLS nằm trong Application Layer trong mô hình 4 lớp gồm Link Layer, Internet Layer, Transport Layer và Application Layer cùng với SSH, Telnet, SMTP, HTTPS,…
- Giao thức TLS bao gồm 2 thành phần là: bản ghi TLS (*TLS Record*) và các giao thức bắt tay TLS (*TLS Handsake Protocols*)

Digital Certificate và CA là gì?

- 1 digital certificate (chứng thư số) là 1 bản chứng nhận sở hữu của 1 public key qua đó các bên khác có thể dựa vào chữ ký số được tạo ra bởi private key tương ứng với public key đã biết.
- Tên gọi khác: public key certificate
- Trong 1 certificate sẽ có: thông tin của public key, thông tin của người sở hữu key (the subject) và chữ ký số (digital signature) của đơn vị phát hành certificate (CA – Certificate Authority)

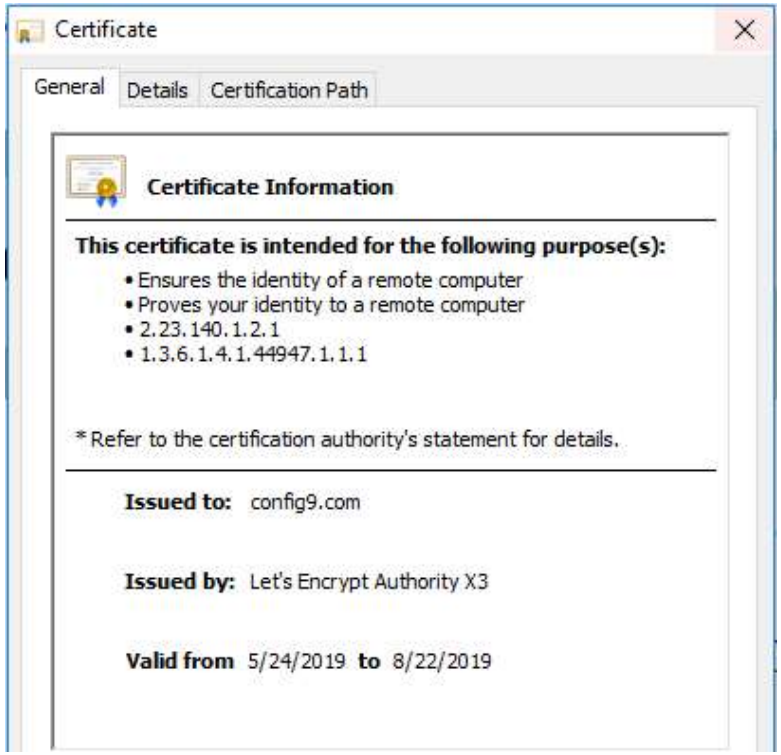
Digital Certificate và CA là gì?

- 1 digital certificate (chứng thư số) là 1 bản chứng nhận sở hữu của 1 public key qua đó các bên khác có thể dựa vào chữ ký số được tạo ra bởi private key tương ứng với public key đã biết.
- Tên gọi khác: public key certificate
- Trong 1 certificate sẽ có: thông tin của public key, thông tin của người sở hữu key (the subject) và chữ ký số (digital signature)(được ký bằng private key) của đơn vị phát hành certificate (CA – Certificate Authority)
- Chuẩn thông dụng nhất của chứng thư số là X.509

Digital Certificate và CA là gì?

- Một số CA nổi tiếng: Comodo, IdenTrust, DigiCert, Let's Encrypt, Trustwave, …
- Theo khảo sát năm 2018 bởi W3Techs, CA đang dẫn đầu thị trường là IdenTrust chiếm 39.7% sau đó là Comodo và DigiCert.
- CA phổ biến nhất là ký lên các chứng thư số sử dụng trong HTTPS sử dụng kỹ thuật Domain Validation – Xác thức domain.
- Một số CA còn cung cấp EV – Extended Validation: không chỉ xác thực domain mà còn xác thực them các thông tin khác như tên công ty, tổ chức sở hữu

Digital Certificate và CA là gì?



Làm thế nào để browsers xác thực HTTPS

- Đây là quá trình trao đổi 3 bên Browser – CA – Webserver (của website)