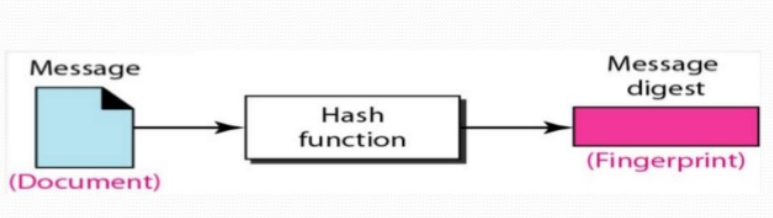
1/ Các khái niệm:

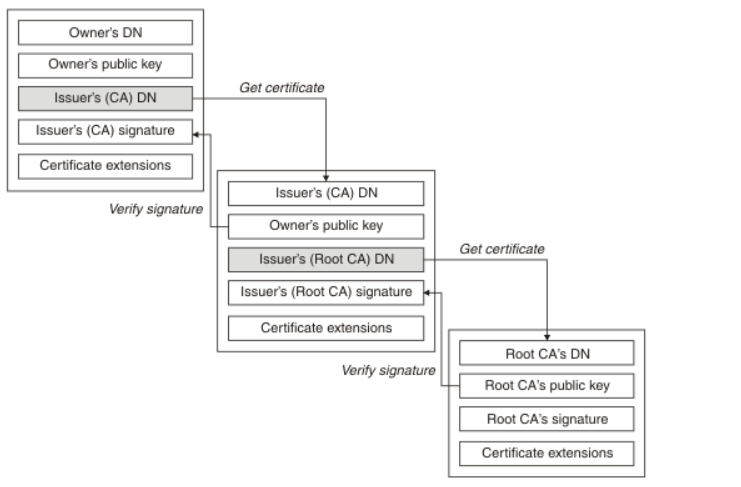
* Cryptography: Quá trình chuyển đổi từ văn bản gốc (Plaintext) thành văn bản đã được mã hóa (Ciphertext)
* Encryption: Quá trình người gửi chuyển đổi Plaintext -> Ciphertext
* Decryption: Quá trình người nhận chuyển đổi Ciphertext -> Plaintext
* Digital signatures: Chữ ký số, đảm bảo tính bảo mật và toàn vẹn của dữ liệu
* Message digest: Đặc trưng cho dữ liệu, có thể xem như vân tay của người. Message digest có thể encrypted để trở thành digital signature. Thông thường message digest sẽ đi cùng với message của người gửi, người nhận có thể tạo digest cho tin nhắn để kiểm tra với digest của người gửi thông qua hash function, đảm bảo được tính ko mất mát dữ liệu khi truyền.



Any message -> same message digest

ONE WAY

* Digital certificates: Chứng chỉ số, dùng để bảo vệ khi có kẻ mạo danh chiếm đoạt. Xác định public key thuộc về một thực thể cụ thể. Được cấp bởi Certificate Authority (CA). Digital Certificate không lưu trữ PRIVATE KEY.
* Khi nhận được certificate từ một thực thể nào đó (Website, Google,...) thì bạn cần phải thiết lập một chuỗi xác thực certificate trung gian cho đến khi nhận được rootCA



2/ TLS-SSL

* Là 1 giao thức giúp bảo mật dữ liệu liên lạc giữa A với B (Cụ thể là Client và server)
* Tóm tắt quá trình handshake client với server

+ Lựa chọn version TLS.

+ Lựa chọn thuật toán mã hóa.

+ Xác thực lẫn nhau bằng cách trao đổi và xác nhận Digital Certificate (Xác thực cả Server và Client).

+ Ban đầu sử dụng thuật toán mã hóa bất đối xứng để tạo ra shared secret key. Sau đó sử dụng thuật toán mã hóa đối xứng dựa trên shared secret key để trao đổi messages.

Open hab không hỗ trợ cho những Broker yêu cầu certificate từ client bởi vì chứng chỉ của OpenHab (SSL Certificate) chỉ là self-signed. Nếu muốn OpenHab hỗ trợ thì chỉ còn cách tìm hiểu cách add Certificate của OpenHab vào Broker