**Matter Security**

**Nguyên tắc**

* Không cho phép xâm nhập lạ (No anonymous joining) : Luôn yêu cầu “bằng chứng về quyền sở hữu” (nghĩa là mật mã dành riêng cho thiết bị).
* Chứng thực thiết bị: Mỗi thiết bị đều có danh tính duy nhất được nhà sản xuất xác thực và xác minh thông qua CSA như một thiết bị được chứng nhận.
* Thông tin xác thực hoạt động: Khi được đưa vào mạng Matter, mọi thiết bị đều được cấp thông tin xác thực hoạt động duy nhất sau khi xác minh thông tin xác thực của nhà sản xuất.
* Thông tin xác thực mạng: Khóa mạng Wi-Fi hoặc khóa Thread Master không được cung cấp cho đến khi chứng chỉ của thiết bị được xác minh và xác thực chính xác.
* Tiêu chuẩn mở: Phần mềm nguồn mở được mở cho các bên thứ ba xem xét các khiếu nại bằng cách kiểm tra tiêu chuẩn và kiểm tra mã nguồn.

**Tổng quan về chứng chỉ và quy trình**

* Mỗi thiết bị Matter nhận được hai chứng chỉ.  Đầu tiên, chứng chỉ thiết bị, được nhà sản xuất lập trình trước khi thiết bị được xuất xưởng. Điều này sẽ được sử dụng sau này để chứng thực thiết bị khi cố gắng tham gia mạng.
* Chứng chỉ còn lại là chứng chỉ vận hành do ủy viên cấp trong giai đoạn vận hành thử. Chứng chỉ vốn sử dụng định dạng CHIP TLV nhưng có thể chuyển đổi sang/từ định dạng X.509. Tất cả các thiết bị đều được cấp chứng chỉ hoạt động để chứng minh quyền của chúng trên mạng Matter (kết cấu) và nhận dạng chúng một cách an toàn.
* Giao tiếp giữa các thiết bị Matter được bảo vệ bằng các khóa khác nhau ở các giai đoạn khác nhau.
* Ở giai đoạn chạy thử, khóa là kết quả của quá trình Thiết lập phiên xác thực bằng mật khẩu (PASE) trên kênh chạy thử bằng cách sử dụng mật mã từ mã QR của thiết bị làm đầu vào. Trong quá trình thiết lập ban đầu này, việc xác minh quyền sở hữu mật mã của cả người ủy quyền và thiết bị tham gia sẽ được xác nhận.
* Ở giai đoạn vận hành, khóa là kết quả của quy trình Thiết lập phiên xác thực chứng chỉ (CASE) qua kênh vận hành sử dụng chứng chỉ vận hành làm đầu vào. Các phiên này được sử dụng trong quá trình hoạt động bình thường giữa bộ điều khiển và thiết bị để xác thực rằng cả hai đều là một phần của mạng Matter.

**Message Protection**: Các thuật toán mã hóa khác nhau được sử dụng để đảm bảo tính bảo mật và toàn vẹn của thông tin liên lạc

* Hashing Algorithm: SHA-256
* Message Authentication: HMAC-SHA-256
* Public Key: ECC Curve NIST P-256
* Message Encryption: AES-CCM (128 bit keys)

A diagram of a computer program

Description automatically generated

Figure 1: Confidentiality: Message payload is encrypted by the encryption key (AES)

A diagram of a computer

Description automatically generated

Figure 2 :Privacy: Addresses are encrypted by the privacy key

**Commissioning Steps** : Có bốn bước liên quan đến việc vận hành thử các thiết bị để bắt đầu tham gia trên mạng Matter:

**1. Khám phá Thiết bị (Device Discovery)**: Trong giai đoạn này, thiết bị thông báo về sự sẵn có của nó để được kết nối. Ủy viên (Commissioner) sau đó tìm ra thiết bị thông qua các thông tin như Discriminator, Vendor ID, Product ID. Sau khi xác định được thiết bị, ủy viên kết nối với thiết bị để tiếp tục quá trình onboarding.

2 .**Kênh An Toàn (Secure Channel):** Giai đoạn này tập trung vào việc thiết lập một kênh an toàn giữa ủy viên và thiết bị. Giao thức PASE (Password Authenticated Session Establishment) được sử dụng, dựa trên giao thức SPAKE2+. Điều này bao gồm việc sử dụng mật khẩu và verifiers để thiết lập một kết nối an toàn.

3 . **Device Attestation (xác nhận)**: mỗi thiết bị được trang bị một chứng chỉ duy nhất do nhà sản xuất ký. Không có một Root Certificate Authority (CA) duy nhất áp dụng cho tất cả các thiết bị. Trong quá trình commissioning (thuê giao), thiết bị được thách thức để chứng minh sở hữu khóa riêng tư tương ứng. Chứng chỉ này có thể được xác thực thông qua Distributed Compliance Ledger (DCL) để xác minh trạng thái chứng nhận của thiết bị.

+ Cấu trúc của hệ thống cho phép tồn tại 3 cấp độ:

* Cấp độ đầu tiên là Product Attestation Authority (PAA).
* PAA sẽ được sử dụng để ký Product Attestation Intermediate (PAI).
* PAI sẽ được sử dụng để ký Device Attestation Certificate (DAC). DAC sẽ được chuyển đến ủy viên và được xác minh so với DCL.

A diagram of a product

Description automatically generated

+ Quá trình xác thực chứng chỉ tập trung vào việc xác minh tính xác thực của Thiết bị. Các bước cao cấp bao gồm:

* Ủy viên xác minh các thông tin của Thiết bị như: Vendor ID (VID), Product ID (PID), trạng thái chứng nhận.
* Để thực hiện điều này, Ủy viên sử dụng:

+ Các thông tin chứng nhận Thiết bị

+ Distributed Compliance Ledger (DCL) hoặc

+ Certification Declaration (CD)

A cell phone with a blue and green rectangle

Description automatically generated

+ Để trở thành một thiết bị hợp lệ, DAC được truy xuất và xác minh trước khi thiết bị tham gia mạng. Ủy viên đưa ra một thách thức cho thiết bị để chứng minh rằng nó sở hữu khóa riêng tư tương ứng.

+ Trước tiên, Ủy viên yêu cầu Thiết bị cung cấp CD, PAI Certificate, và DAC. Sau đó, Ủy viên trích xuất Certificate ID, PAA Certificate, và Device VID/PID từ DCL để thực hiện xác minh. Sau khi kiểm tra chuỗi chứng chỉ từ DAC đến PAI, nếu mọi thứ đều kết nối chính xác, Ủy viên so sánh certification ID từ DCL với CD ID từ chính thiết bị để đảm bảo thiết bị là một thiết bị được chứng nhận của CSA thật sự.

+ Bước cuối cùng là xác minh rằng khóa công khai trong DAC tương ứng với khóa riêng tư được chèn vào thiết bị trong quá trình sản xuất. Điều này được thực hiện bằng cách gửi một tin nhắn đến thiết bị trong bước cuối cùng của quá trình Attestation, và có tin nhắn được ký bởi thiết bị, sau đó chữ ký được xác minh bằng khóa công khai từ DAC.

+ **Node Operational Credentials** cho phép một Node xác định chính nó trong một Fabric. Một Node nhận bộ thông tin xác thực ban đầu của Node khi nó được thuê giao cho một Fabric bởi một Ủy viên.

+ Các thông tin xác thực của Node bao gồm :

* Node Operational Key Pair
* Node Operational Certificate (NOC)
* Intermediate Certificate Authority (ICA) Certificate (optional)
* Trusted Root Certificate Authority (CA) Certificate(s)

+ **Commissioning Process** sử dụng DAC để xác định rằng Ủy viên đang nói chuyện với một Thiết bị Matter được chứng nhận và sau đó tải các định danh hoạt động cho mỗi hệ sinh thái mà nó tham gia.

A diagram of a light bulb

Description automatically generated

**4 . Còniguration**

Quá trình cấu hình bao gồm :

1. Tải Node Operational Credentials cho mỗi hệ sinh thái:

- ID của Fabric

- ID của Node

- Chứng chỉ Root đáng tin cậy

- Chứng chỉ ICA

- Chứng chỉ hoạt động

- Cặp khóa hoạt động của Node

- Danh sách kiểm soát truy cập (ACL)

- Mạng hoạt động

- Thời gian (tùy chọn)

2. Thiết lập kết nối với các Node khác bằng cách sử dụng CASE (Cryptography for Authenticated Session Establishment).

Những bước này hoàn tất quá trình thuê giao và hiện đã sẵn sàng hoạt động trên Mạng Matter.

**Matter Security Requirements**

Yêu cầu bảo mật của Matter được quy định bởi CSA và các yêu cầu bảo mật khác như sau:

1. Sản xuất: Các thiết bị Matter phải được tiêm chứng chỉ/private key DAC duy nhất, Onboarding Payload (QR code), Certification Declaration (CD), và các dữ liệu tĩnh/dynamic khác trong quá trình sản xuất. (YÊU CẦU)
2. Thuê giao: DAC với VID/PID phải được kiểm tra trên DCL và CD phải được xác minh để đảm bảo chỉ có các thiết bị Matter chính thức và được chứng nhận được thuê giao. (YÊU CẦU)
3. Giao tiếp của Thiết bị: Giao tiếp giữa các thiết bị Matter phải được bảo mật và mã hóa bằng các khóa mật mã và PBKDF. (YÊU CẦU)
4. Cập nhật Phần mềm: Thiết bị phải hỗ trợ cập nhật phần mềm qua không dây (OTA) để cho phép vá các lỗ hổng. (YÊU CẦU)

**Các yêu cầu bảo mật khác bao gồm:**

* Các khóa xác thực và mã hóa phải được tạo ra bởi một "Trình tạo số ngẫu nhiên quy định" được khởi tạo bởi NIST 800-90B TRNG. (YÊU CẦU)
* Giao diện gỡ lỗi và truy cập vào các thức ăn mật mã khởi đầu an toàn nên bị vô hiệu hóa chỉ cho phép truy cập được ủy quyền (fusing). (NÊN)
* Bảo mật bí mật của DAC và khóa riêng tư hoạt động nên được bảo vệ khỏi các cuộc tấn công từ xa. (NÊN)
* Các nhà cung cấp nên có chính sách công khai và cơ chế để xác định và khắc phục các lỗ hổng bảo mật kịp thời. (NÊN)
* Phần mềm nên được mã hóa khi nằm yên để ngăn chặn truy cập trái phép vào IP cốt lõi. (CÓ THỂ)
* Một số thiết bị nên được bảo vệ chống lại các cuộc tấn công vật lý để ngăn chặn can thiệp, tấn công kênh bên hoặc glitching gỡ lỗi. (CÓ THỂ)

**Giải pháp bảo mật tuân thủ Matter bao gồm:**

* Secure Vault Mid hoặc High hỗ trợ tất cả các chức năng bảo mật của Matter hiện tại và tương lai.
* Các khóa không thể bẻ được được tạo ra bởi Bộ Tạo Số Ngẫu Nhiên Thực (TRNG) cho DAC, khởi đầu an toàn, gỡ lỗi an toàn, OTA, hình ảnh phần mềm và mã hóa giao tiếp.
* Crypto Engine hỗ trợ các thuật toán đặc biệt như SPAKE2+ và CASE với bảo vệ chống lại các cuộc tấn công kênh bên.
* Lưu trữ khóa an toàn ở cấp độ PSA/SESIP Level 2 (Mid) và Level 3 (High); Các khóa riêng tư được lưu trữ bằng TEE/TZ (SV Mid) hoặc PUF Wrapped (SV High).
* Định danh Matter an toàn (DAC) được lập trình an toàn tại nhà máy của chúng tôi.
* Khởi đầu an toàn với RTSL đảm bảo mã chạy trên thiết bị được tin tưởng.
* Cập nhật phần mềm OTA an toàn phối hợp với Secure Boot ngăn chặn việc cài đặt phần mềm độc hại và cho phép vá lỗ hổng.
* Khóa/Gỡ lỗi an toàn chống lại lỗi Glitch chỉ cho phép truy cập được ủy quyền với các token bảo mật có thể bị thu hồi.
* Chống lại Can