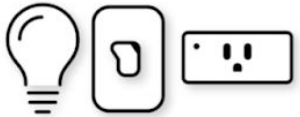
Matter and Open Screen Protocol

W3C Second Screen Working Group
Mark A. Foltz (mfoltz@google.com)
March 8, 2023

What is Matter?

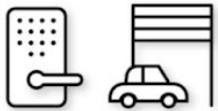
https://csa-iot.org/

Devices supported by Matter at launch:



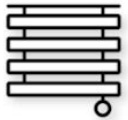
Lighting and Electrical

HVAC Controls



Access Control Products

Safety and Security Sensors



Window Coverings and Shades

TVs

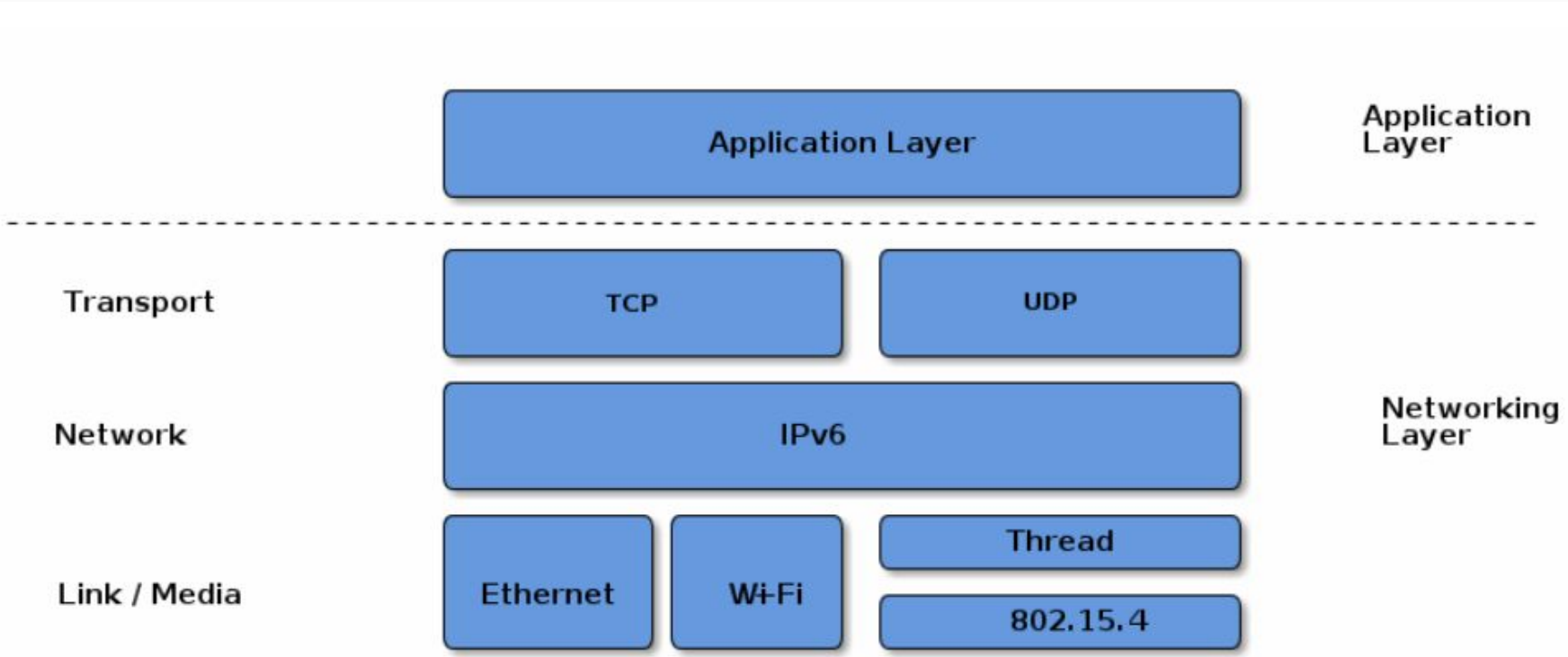
Access Points and Bridges

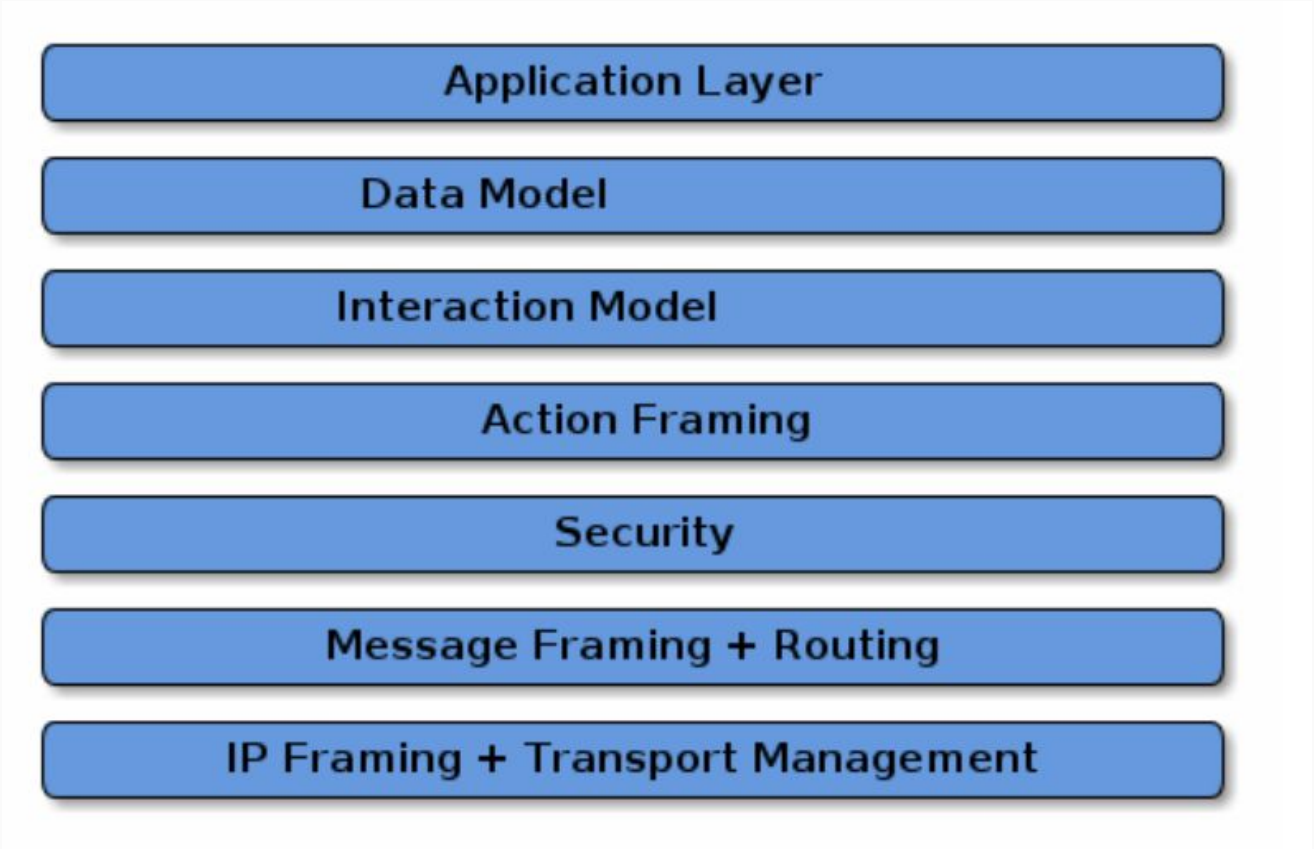
- 1.0 Specification released December 2022
- Open Source SDK - https://github.com/project-chip/connectedhomeip
- Certification and Testing Tools

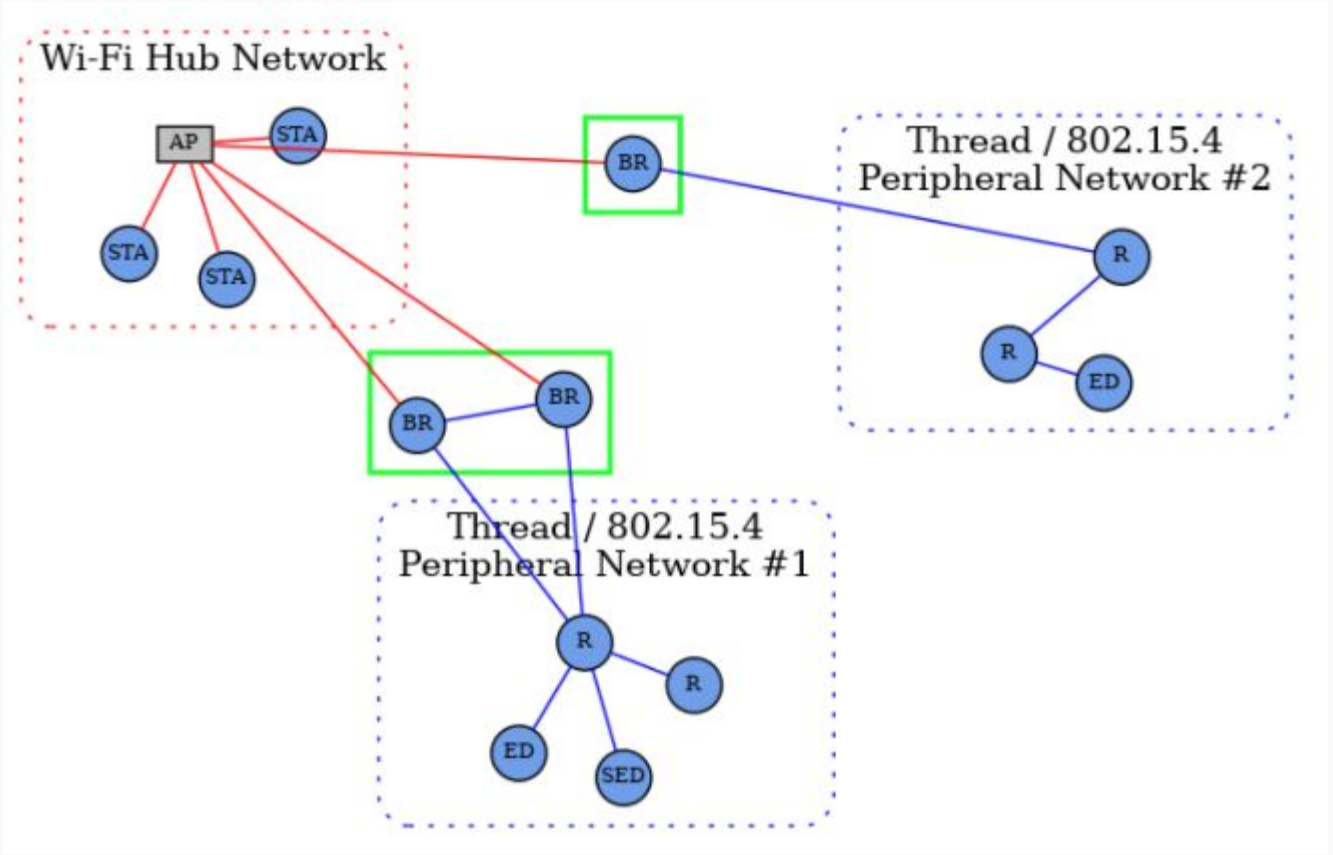
Matter Timeline (Updated)

- Spec 1.0 released in December 2022
- Over 600 products have been Matter certified
- Products are starting to become available
- Google, Apple, Amazon, and LG have OS support

Technical Architecture


Application Layer
Application Layer
Transport
TCP
UDP
Network
IPv6
Networking Layer
Link / Media
Ethernet
Wi-Fi
Thread
802.15.4


Application Layer
Data Model
Interaction Model
Action Framing
Security
Message Framing + Routing
IP Framing + Transport Management


Wi-Fi Hub Network
AP
STA
STA
STA
BR
Thread / 802.15.4
Peripheral Network #2
R
R
ED
BR
BR
Thread / 802.15.4
Peripheral Network #1
R
R
ED
SED

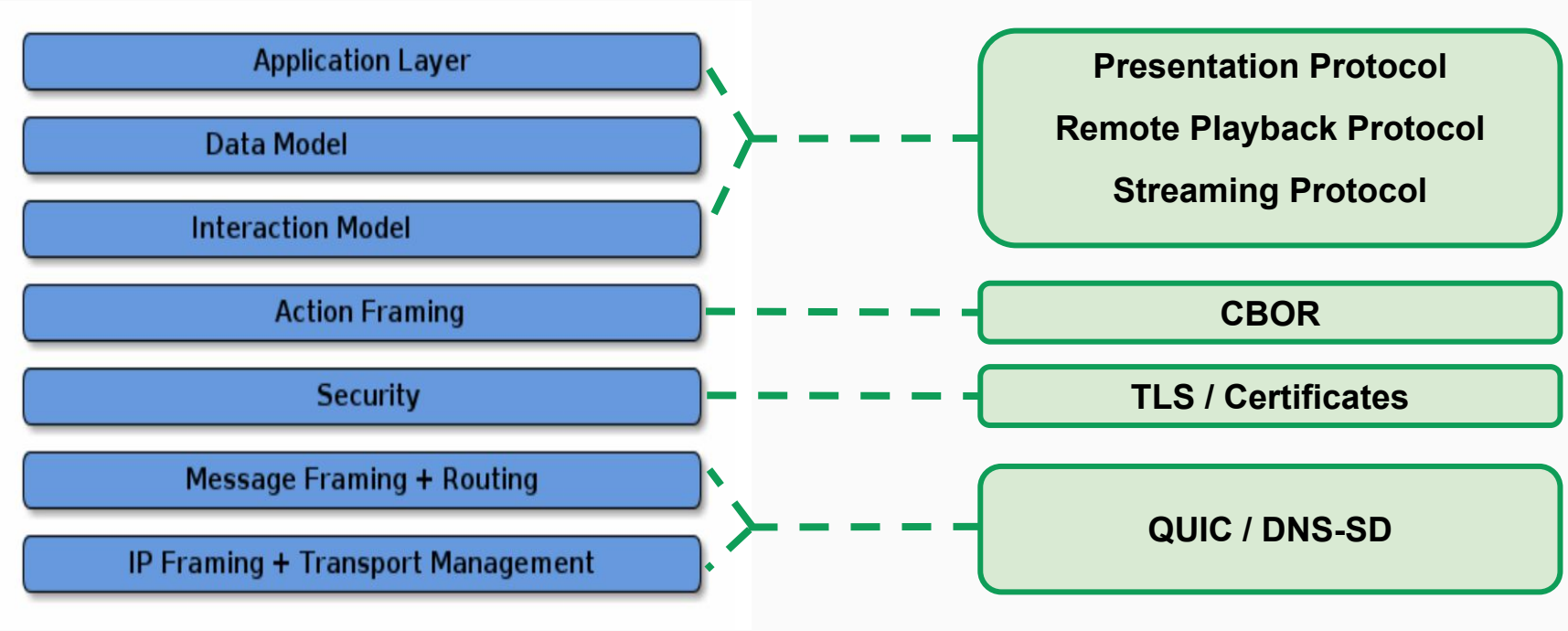
Commissioning and Trust

1. Discover device (BLE, DNS-SD) and obtain its passcode (QR Code, manually, NFC)
2. Establish a password-authenticated session via SPAKE2+
3. Establish verification of device (attestation) by challenge/response
4. Commissioner provides an Operational Certificate and Node ID to the device
5. Device can authenticate to other devices using its Operational Certificate

Matter + Open Screen Protocol

Matter

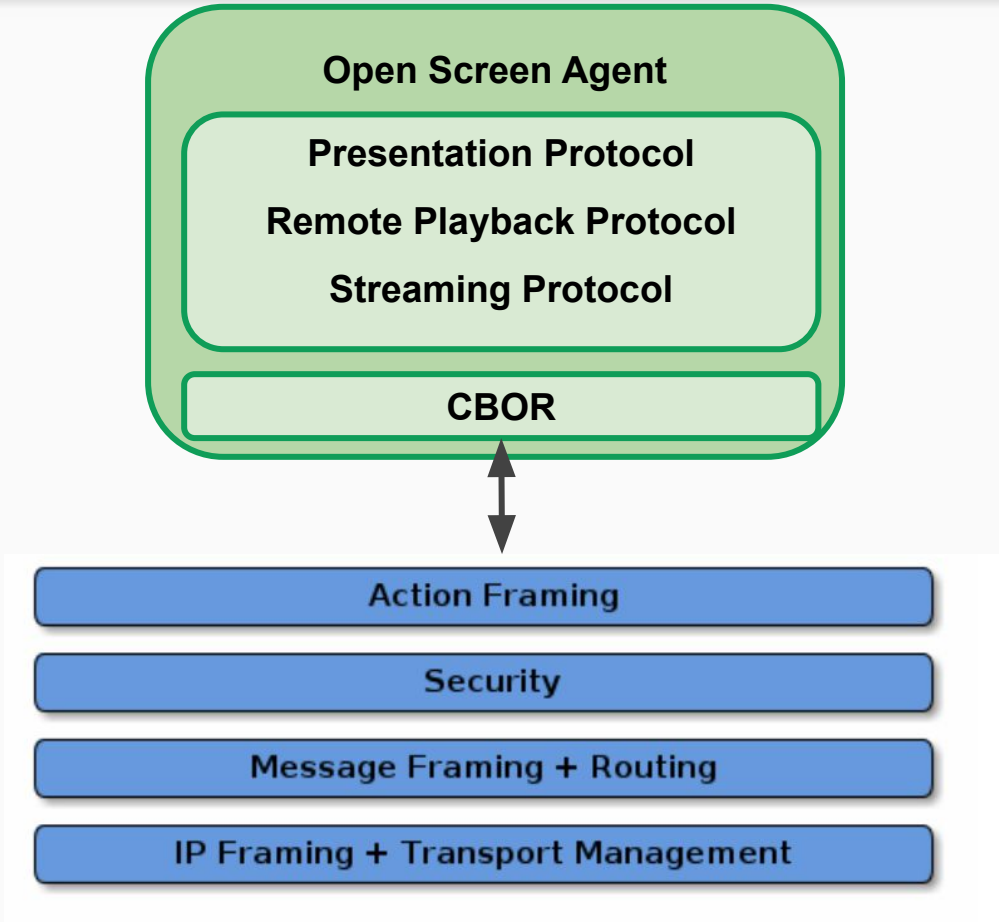
Open Screen Protocol



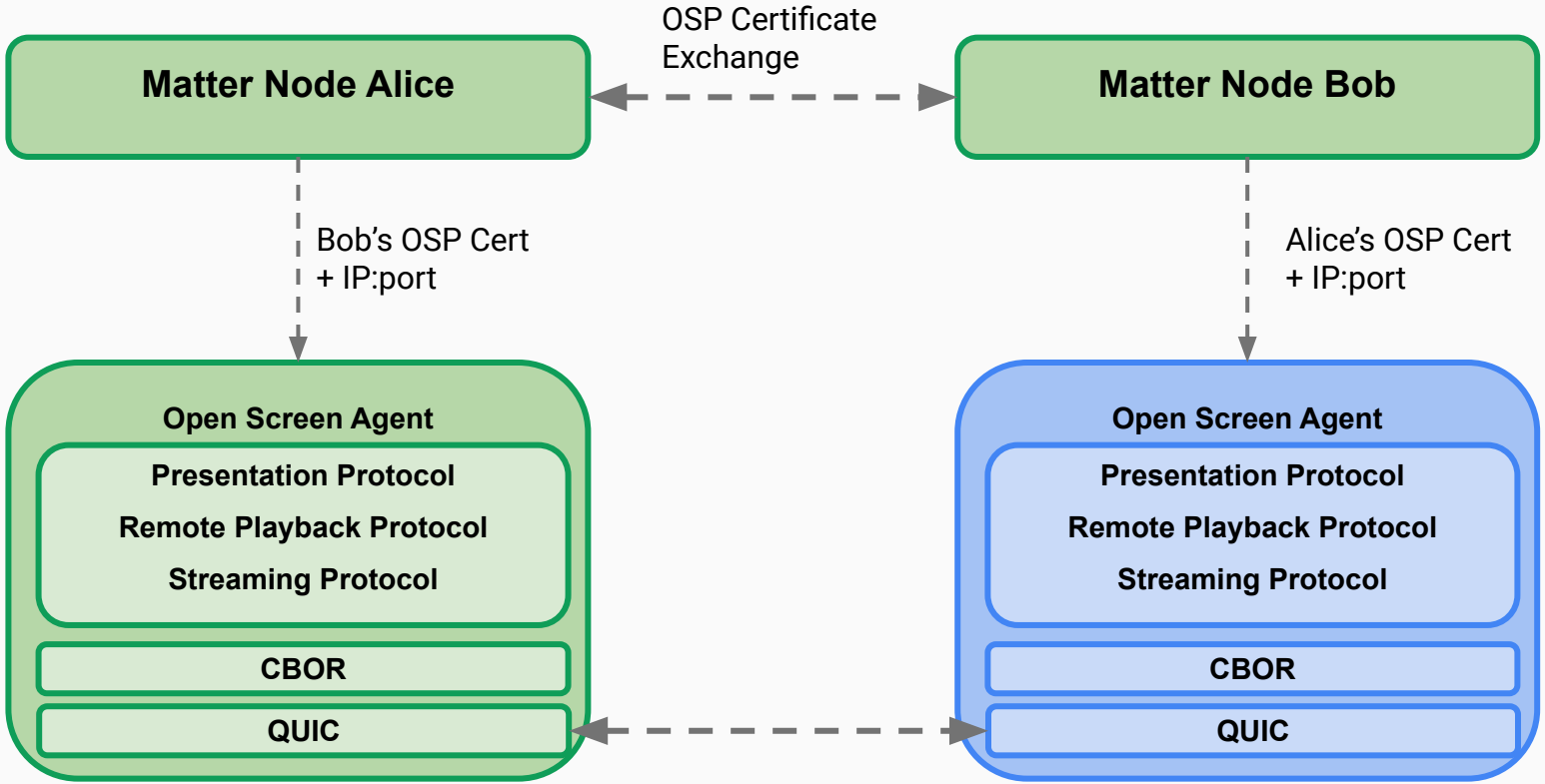
Assumptions

- World of devices that are Matter-only, devices that are OSP-only, and some that have Matter and want OSP
- OSP+Matter devices can find other OSP+Matter devices
- OSP+Matter devices can establish mutual trust and authentication
  - CASE, section 4.13.2
  - PASE, section 4.13.1

Hybrid approach #1, the “tunneling option”



Hybrid approach #2, the “bootstrap” option



Areas Of Investigation (Updated)

1. How to use Matter transport to convey CBOR messages (for “tunneling”)?
2. Suitability of the Matter transport for streaming use cases?
3. How to leverage Matter to create an authenticated QUIC connection?
4. Investigate the “Casting Video Client” device type (Device Library 10.6).

Open Screen Protocol 1.0 Spec status

Label/Category	**Number**	**With PR**
v1-spec	10	0
security-tracker	4	4
privacy-tracker	1	n/a?
meta	2	n/a
Total	**16**	**4**

Recommendations for SSWG (Updated)

1. **Land PRs for security-tracker issues in OSP.**
2. **Propose a white paper for the “tunneling” approach.**
3. **Draft a protocol extension for the “bootstrap” approach.**
4. **Attempt to implement OSP demo with either approach on top of Matter SDK.**

End


Matter Working Group
Zigbee Working Group
Data Model Working Group
Access Control Working Group
Member Group China
EU Interest Group
Industry Stakeholder Groups

Example Matter Device: Light Bulb from “Bulby Corp.”

Light Bulb

Initial Device Credentials

Product Attestation Authority Cert (PAA)
Issuer: Bulby
Subject: Bulby

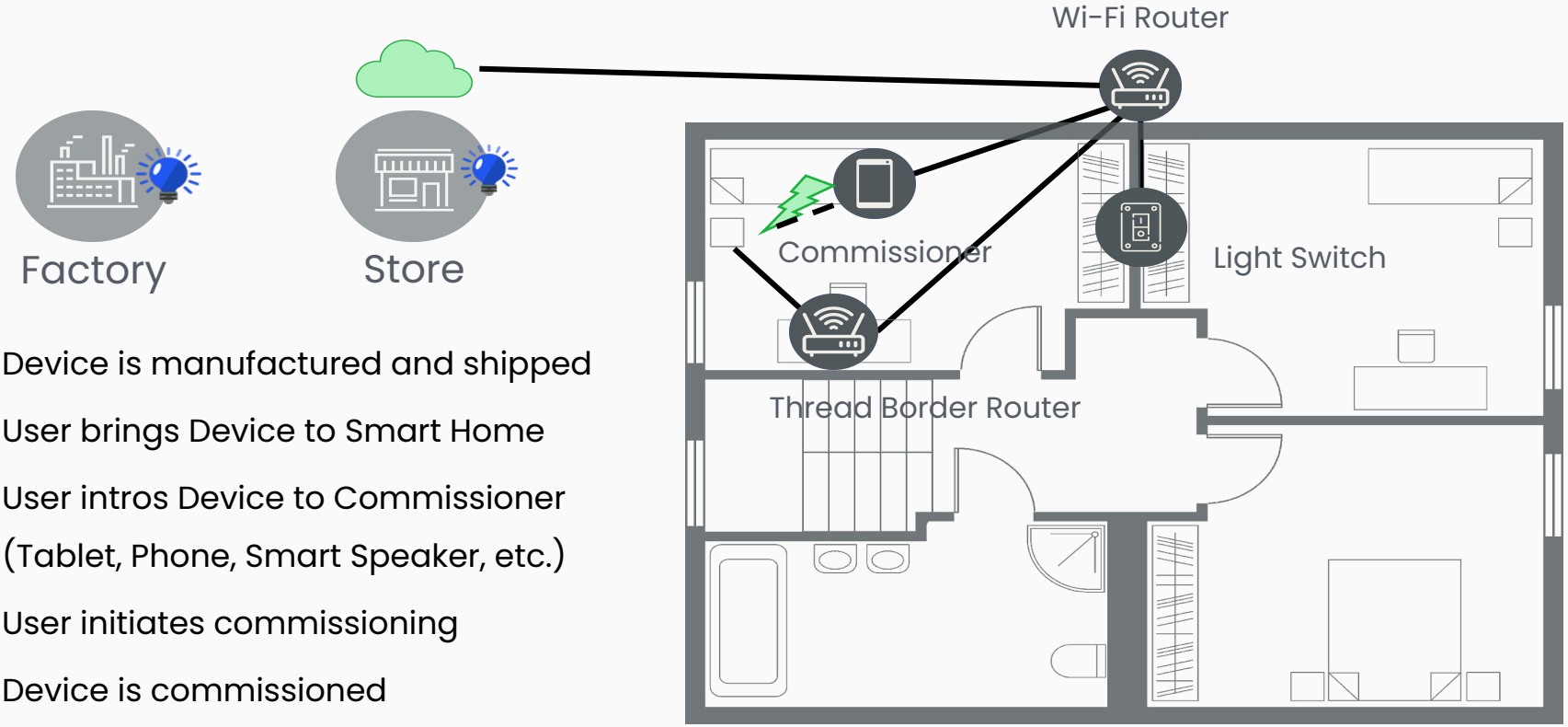
Implicit

Product Attestation Intermediate Cert (PAI)
Issuer: Bulby
Subject: Bulby PAI

Device Attestation Cert (DAC)
Issuer: Bulby PAI
Subject: Bulb 32487
Vendor ID (VID): 273
Product ID (ID): 298

Private Key for DAC
Certification Declaration (CD) Verifier

Matter Commissioning – User View



1. Device is manufactured and shipped
2. User brings Device to Smart Home
3. User intros Device to Commissioner (Tablet, Phone, Smart Speaker, etc.)
4. User initiates commissioning
5. Device is commissioned
6. Device operates smoothly in Smart Home

In the Commissioned Light Bulb

Light Bulb
Node N6 on Fabric AcmeRoot.F1

PAA Cert
Issuer: Bulby
Subject: Bulby

PAI Cert
Issuer: Bulby
Subject: Bulby PAI

Device Attn Cert (DAC)
Issuer: Bulby PAI
Subject: Bulb 32487
VID: 273
PID: 298

Private Key for DAC Certification Declaration (CD) Verifier

Root Cert
Issuer: Acme
Subject: Acme

Intermediate CA (ICA) Cert
Issuer: Acme
Subject: ICA 27

Operational Cert (OpCert)
Issuer: ICA 27
Subject:
FabricID: F1
NodeID: N6

Private Key for OpCert Access Control List (ACL) Operational Network

Security

	Open Screen Protocol	**Matter**
Pairing	SPAKE-2 Possibly C-PAKE: Issue #242	Commissioning ceremony
Trust Model	Self-signed certificates	Certificate chain for operational use
Auth stack	TLS 1.3 Ciphers: Issue #218 ECDSA certificates: Issue #280	• ECC P-256 certificates • Sigma protocol used for secure channel establishment • AES-128-CCM encryption with 128-bit AES-CBC
Attestation	None*	Manufacturer signed X.509 certificates

* - Future candidate for a protocol extension leveraging Matter PKI

Documents and Presentations

Matter One Pager

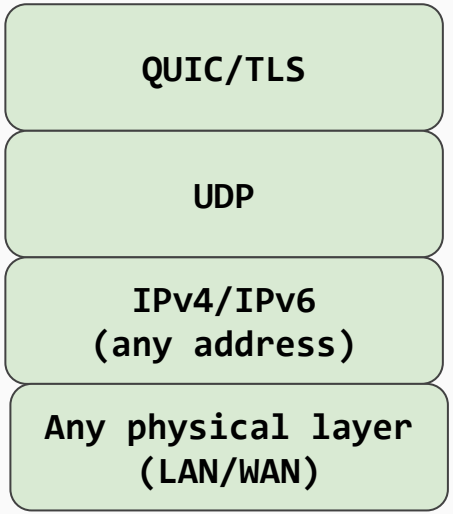
March 2022 Matter Introduction

Matter Security and Privacy Whitepaper

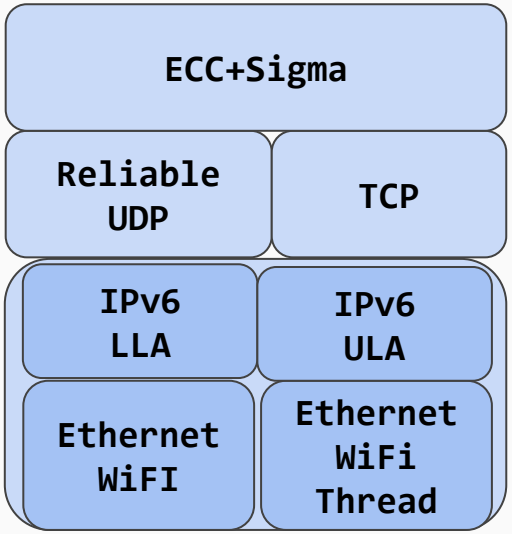
Matter Security and Privacy for the Experts

Transport / Networking

Open Screen Protocol



Matter



Network Provisioning via WiFi or BTLE