csa connectivity standards alliance

matter

Security & Privacy

for Security & Privacy Experts

Agenda

#	Topic
1	Introduction to Matter
2	Security & Privacy Principles
3	Threat Model
4	Security & Privacy Architecture

Introduction to Matter

matter

- The foundation for connected things
- A seal of approval that devices will work seamlessly together today & tomorrow
- Simplifying development for manufacturers and increasing compatibility for consumers.

Simplicity – Interoperability – Reliability - Security

How We Stack Up

Common application layer + data model
Interoperability, simplified setup & control

IP-based
Convergence layer across all compatible networks

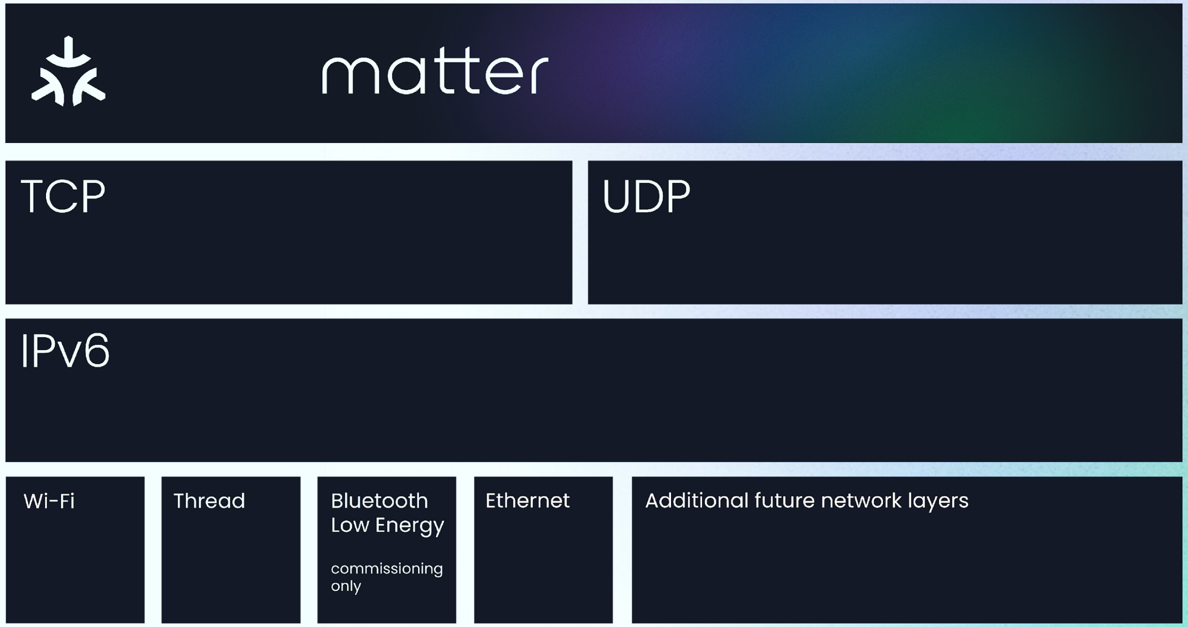
Secure
AES-128-CCM encryption with 128-bit AES-CBC

Open-source development approach
Based on market-proven technologies

Common protocol across device and mobile
Extensible to cloud

Common data model
Core operational functions, multiple device types

Low overhead
MCU-class compute, <128KB RAM, <1MB Flash



Creating Experiences that Matter

Consumers

- More consistent set up experience
- Multi –Admin works across & with multiple ecosystems

Developers

- Develop once / deploy everywhere
- Secure-by-design approach
- Community of support

Retailers

- Simplified purchasing experience
- Minimized returns

Commercial / Builders

- Future proofed ecosystem compatibility
- Flexibility for users

Target Device Types

Lighting, Electrical

Blinds/Shades

HVAC Controls

TVs

Access Control

Safety & Security

Access Points, Bridges

Matter controllers can be implemented in a variety of devices and interfaces

Scoping exercises for additional device types and use cases underway and continual.

Open Source

Matter open source project:
github.com/project-chip/connectedhomeip

Collaborative, open-source development

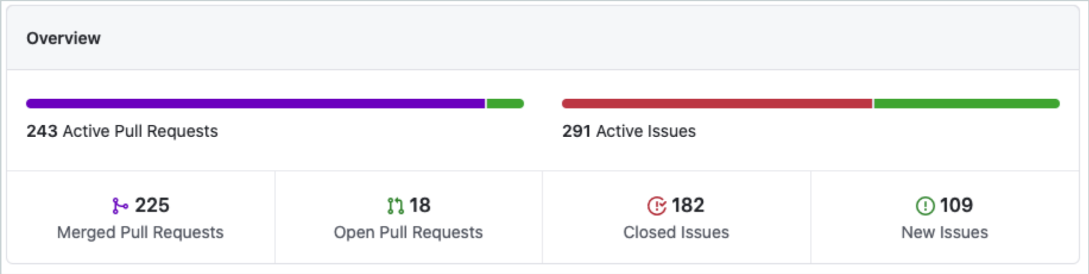
Accessible, transparent, robust, and secure. Code examples showing interactions on multiple transports.

Built on market-proven technologies

Companies from across the industry are contributing market-proven technologies and best practices.

Implementation-first approach

Growing to implement the overall architecture. Not just a technical spec, but deployable code.



Overview

243 Active Pull Requests

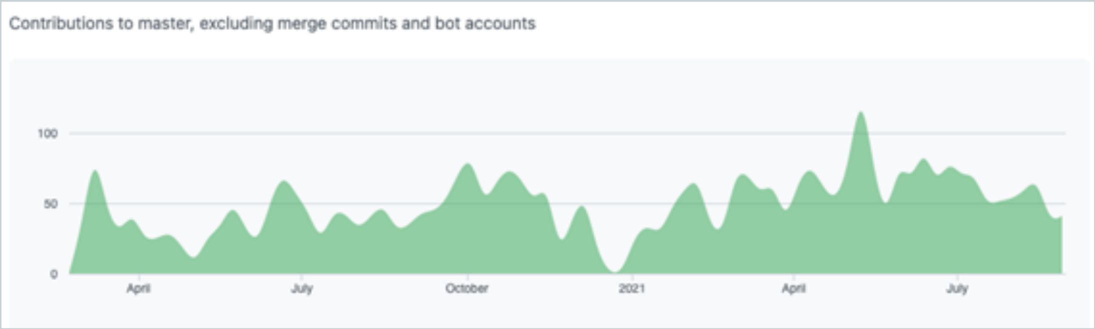
291 Active Issues

225 Merged Pull Requests

18 Open Pull Requests

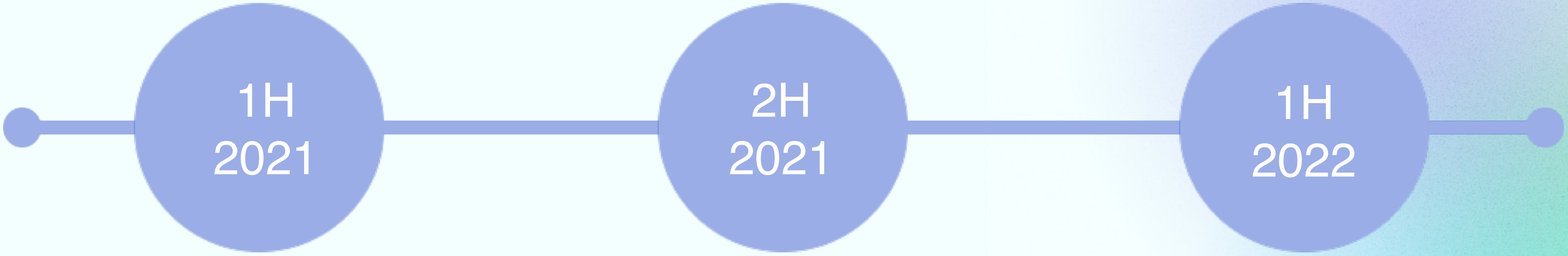
182 Closed Issues

109 New Issues



Contributions to master, excluding merge commits and bot accounts

Looking Ahead



1H 2021

Initial technical specifications available to Members
Initial SDK and Test Event Efforts

2H 2021

Pre-balloting technical specifications available to members
Ongoing SDK & Cert Program Dev
Test Events Continue

1H 2022

SDK Released
1st Products Certified
Certification Program Released
Members action GTM plans

Note: Timeline, subject to change

Security & Privacy Principles

Matter Security & Privacy Principles

Security and privacy are foundational tenets

Designed to keep devices and information secure and private, while still being easy to use

Comprehensive

Layered approach

Strong

Well-tested standard cryptographic algorithms

Easy

Improve ease of use

Resilient

Protect, Detect and Recover

Agile

With crypto-flexibility in mind to address new developments and threats

Threat Model

Attackers

Motivations – Political, personal, financial, indirect, …

Capabilities

- Resources – Time, money, tools, …
- Expertise – Skills, knowledge, …
- Access – Physical, proximity, remote, …

Role – User, former user, guest, supplier, trusted party, intruder, …

Lifecycle – Former owner or new owner, scavenger, …

Targets

Devices – Sensors, alarms, appliances, controllers, …

Network – Mesh, local area, wide area, wired & wireless, …

Gateways – Bridges, router, legacy devices & protocols, …

Services – Cloud, update servers, security services, …

Data – Stored, in processing, in transit, …

Humans – Users, former users, guests, trusted parties, …

Protocols – Matter, Thread, Wi-Fi, IP, …

Algorithms – Design flaws, breaks, quantum, …

Attack Methods

Network – Eavesdrop, modify, jam, …

Device – Exploit vulnerabilities, …

Gateway – Infect gateway, attack traffic or nodes behind it

Services – Compromise CA or other critical service

Physical – Physically attack device or other component

Humans – Trick or influence trusted humans to attack

Protocols – Find and exploit vulnerabilities in protocols

Algorithms – Find and exploit vulnerabilities in algorithm

Threat Analysis

Severity – Based on Likelihood & Impact

Likelihood – Probability, based on

- **Access** – Physical, Proximity, or Remote
- **Difficulty** – Difficult, Moderate, or Easy

Impact – Effect of successful attack, based on

- **Scope** – Single Device, Home Network, or Fleet
- **Data & Control** – Low Sensitivity, Limited Sensitivity, or Complete Compromise

Countermeasures

- Identified many possible Countermeasures
- Tied to Threats they address
- Included Countermeasures in spec for as many threats as possible

Example

Threat Description							
Applicable TT	ID	Description	Threat Agent	Impact/Consequence	Severity	Impact	Likelihood
TM	T59	Maliciously crafted message exploits Device vulnerability, causing Device compromise	Attacker using a Device on the network	Trusted Device could be hijacked	High	High	High

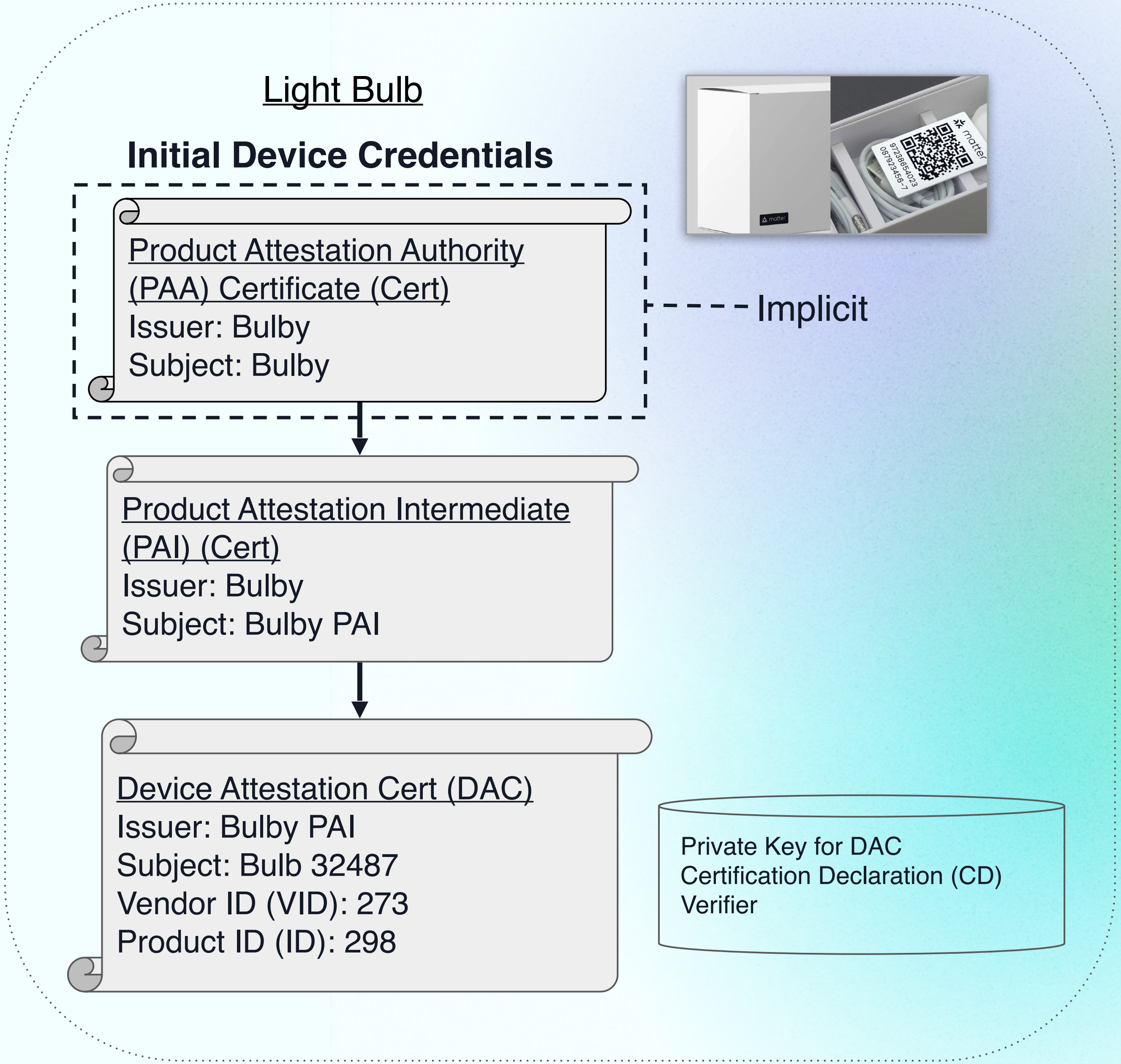
Countermeasure in Matter Specification

13.5. Firmware

a. Nodes SHALL support OTA firmware updates, either using Matter-provided means (see Section 11.20, “Over-the-Air (OTA) Software Update”) or proprietary means. [CM58 for T59]

Security & Privacy Architecture

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



Light Bulb

Initial Device Credentials

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

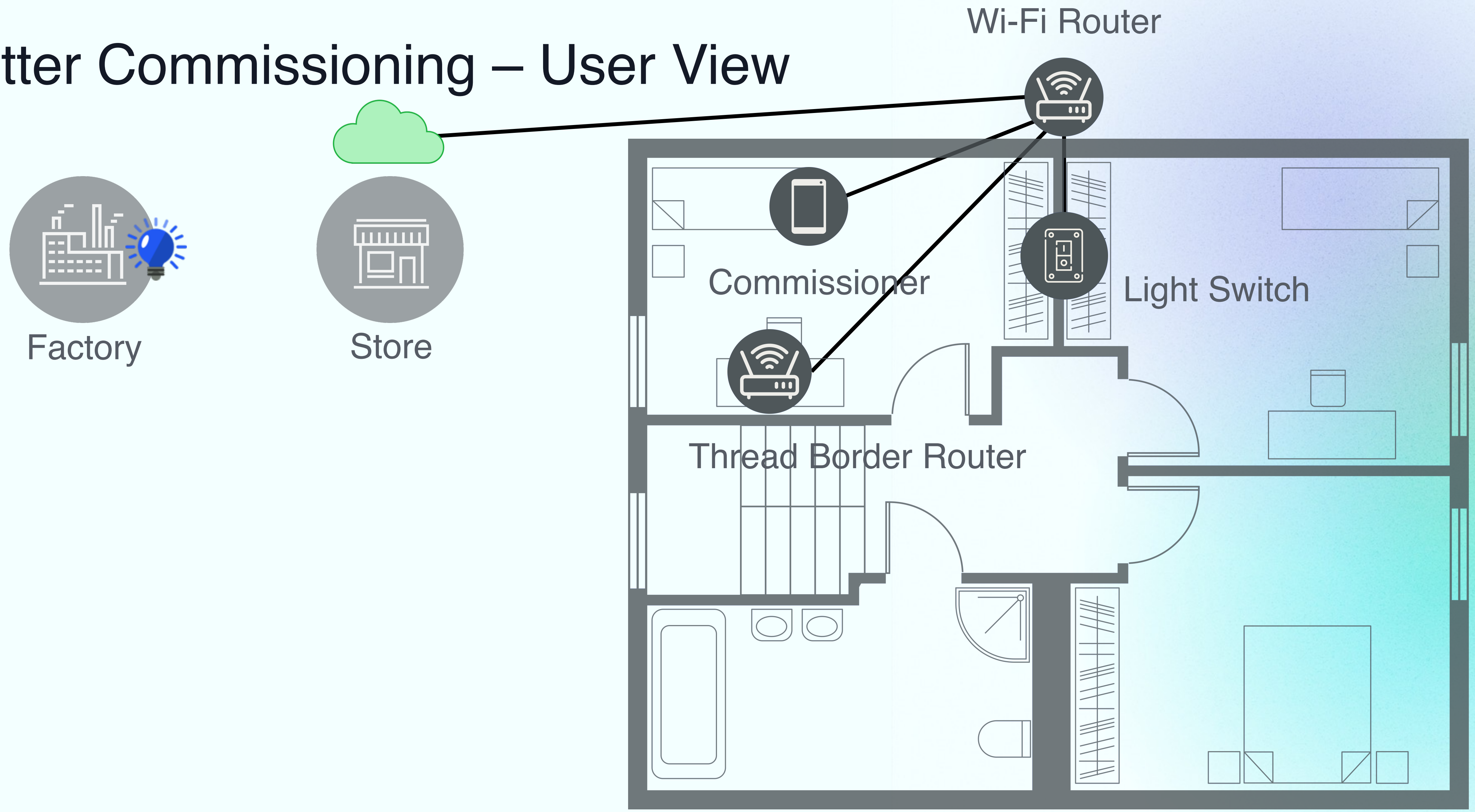
Implicit

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

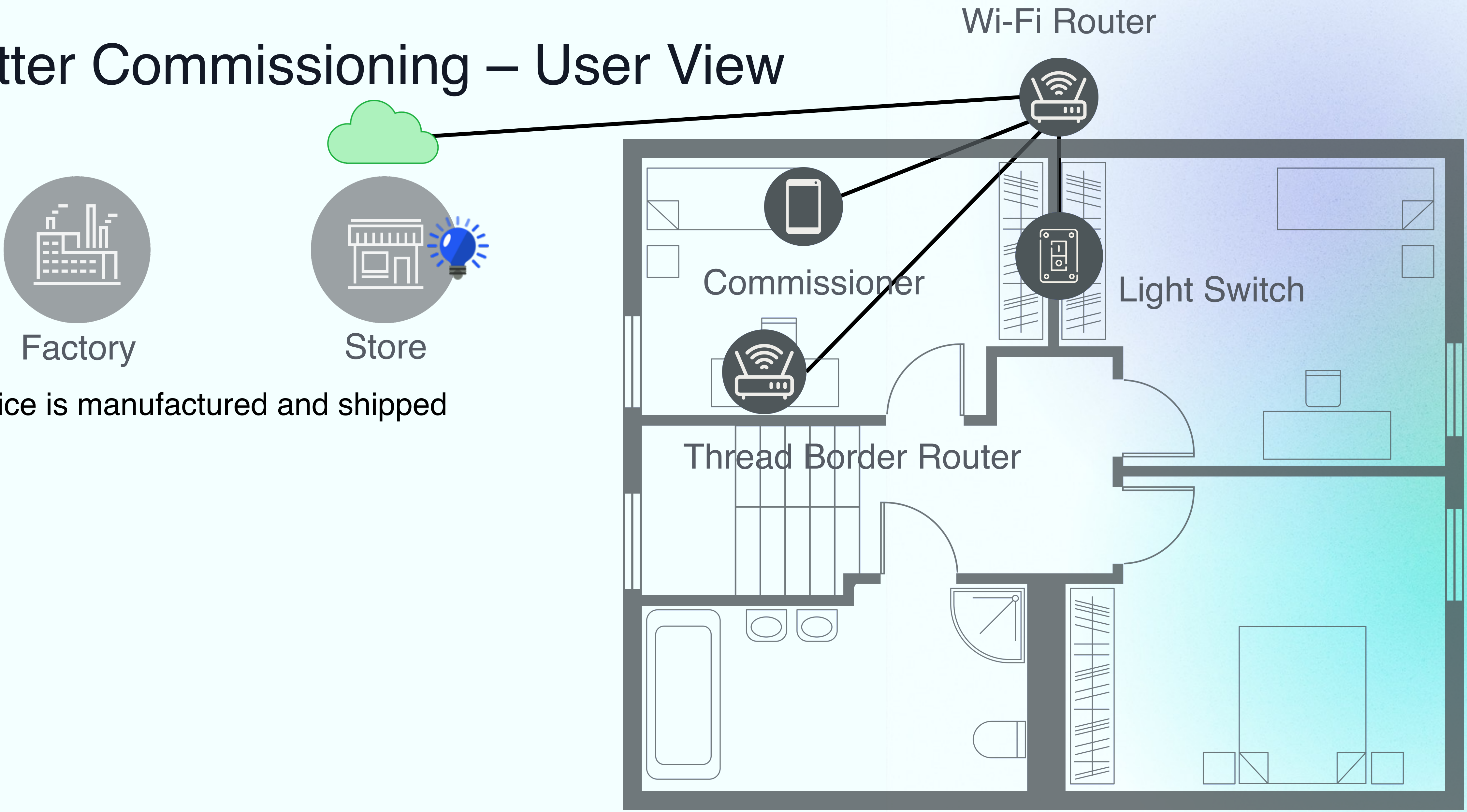
Device Attestation Cert (DAC)
Issuer: Bulby PAI
Subject: Bulb 32487
Vendor ID (VID): 273
Product ID (ID): 298

Private Key for DAC
Certification Declaration (CD)
Verifier

Matter Commissioning – User View

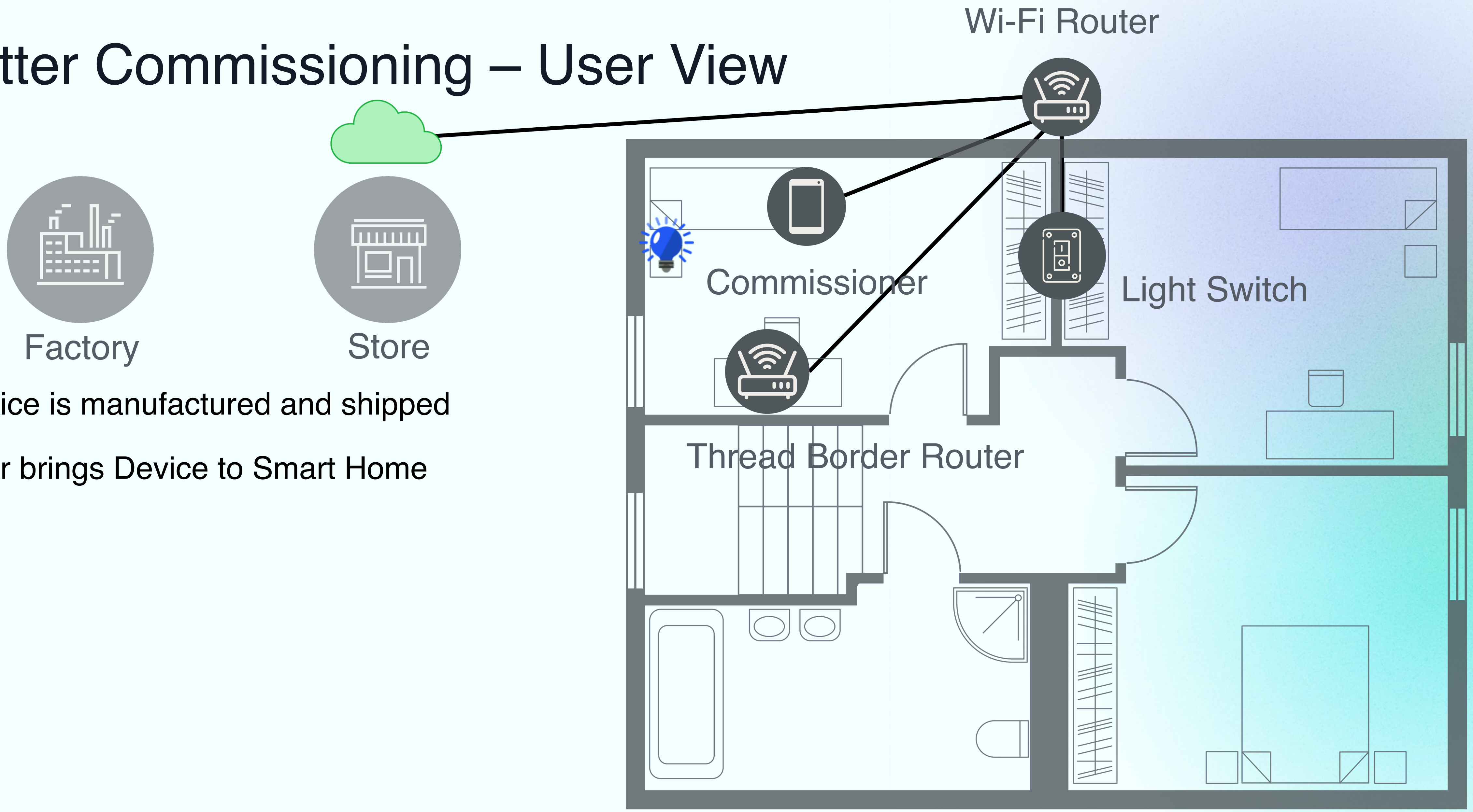


Matter Commissioning – User View



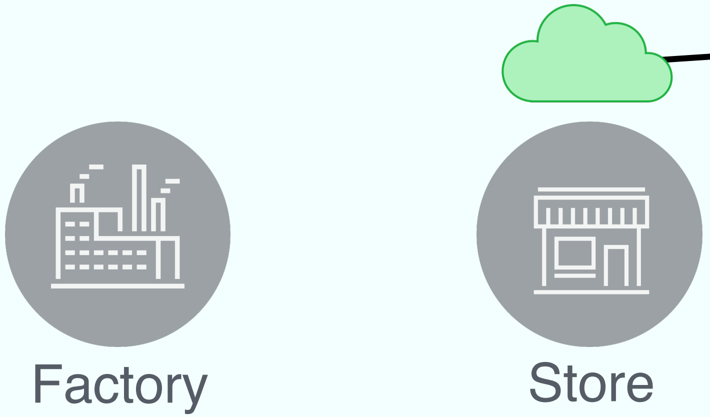
1. Device is manufactured and shipped

Matter Commissioning – User View

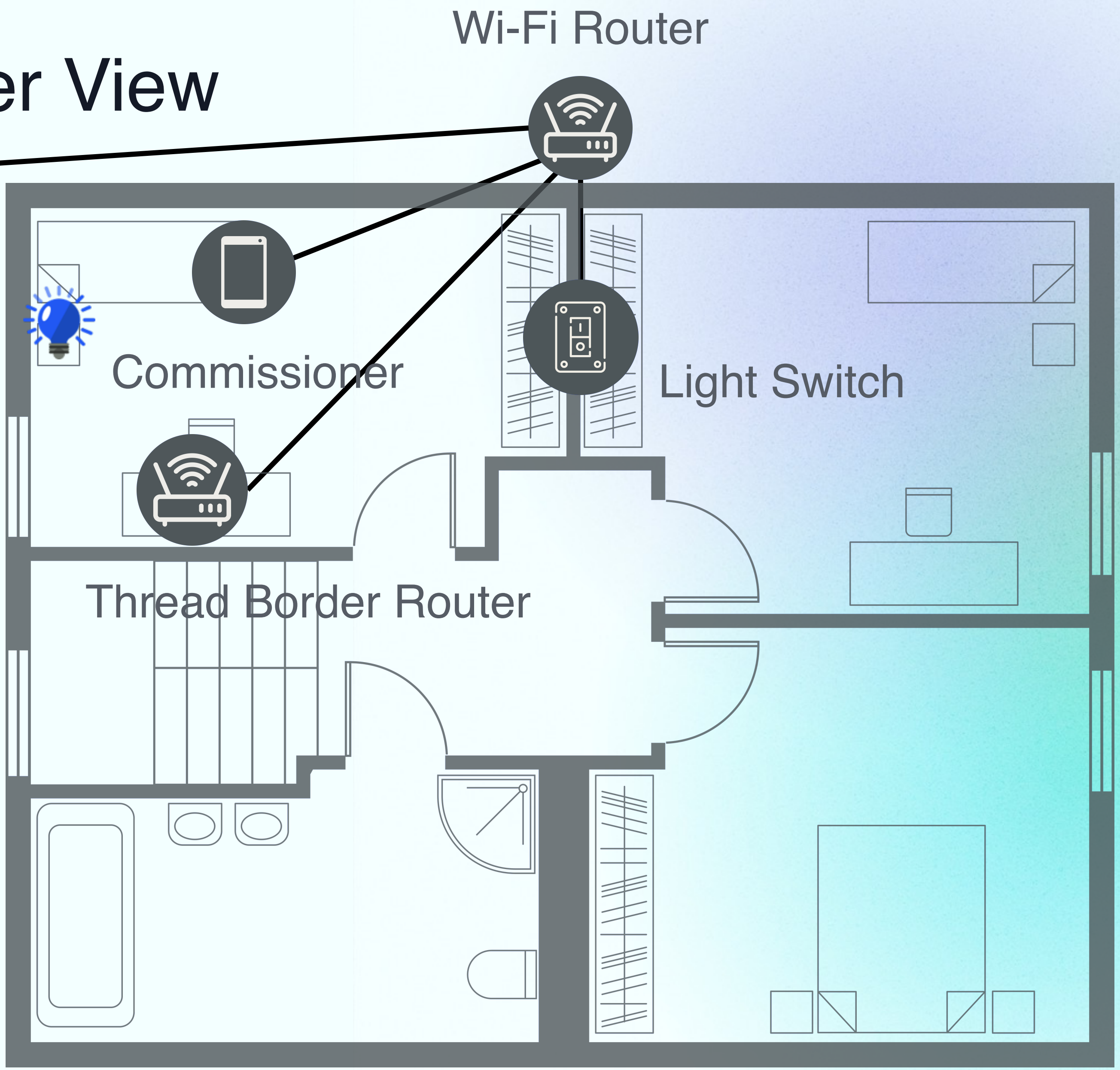


1. Device is manufactured and shipped
2. User brings Device to Smart Home

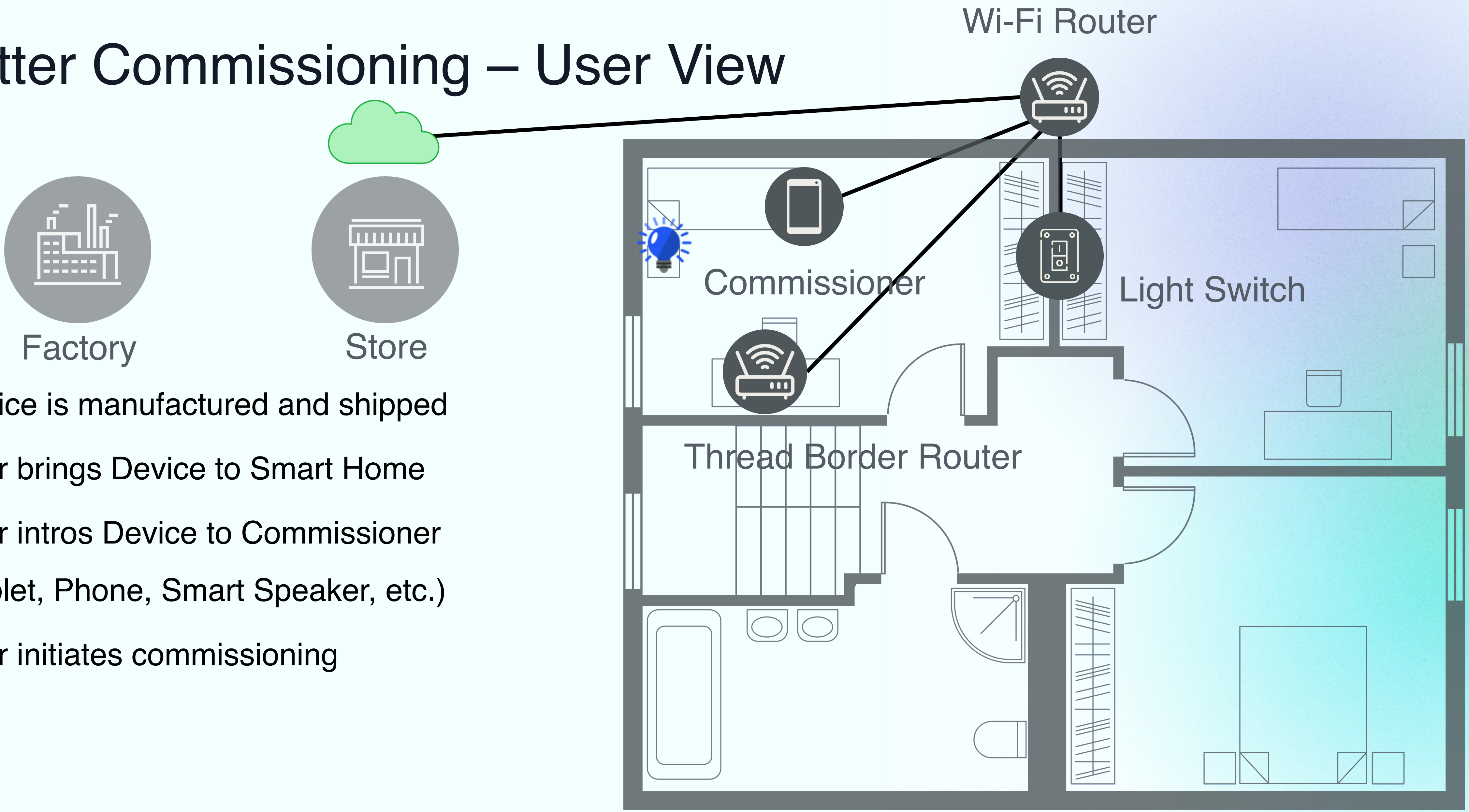
Matter Commissioning – User View



1. Device is manufactured and shipped
2. User brings Device to Smart Home
3. User intros Device to Commissioner (Tablet, Phone, Smart Speaker, etc.)

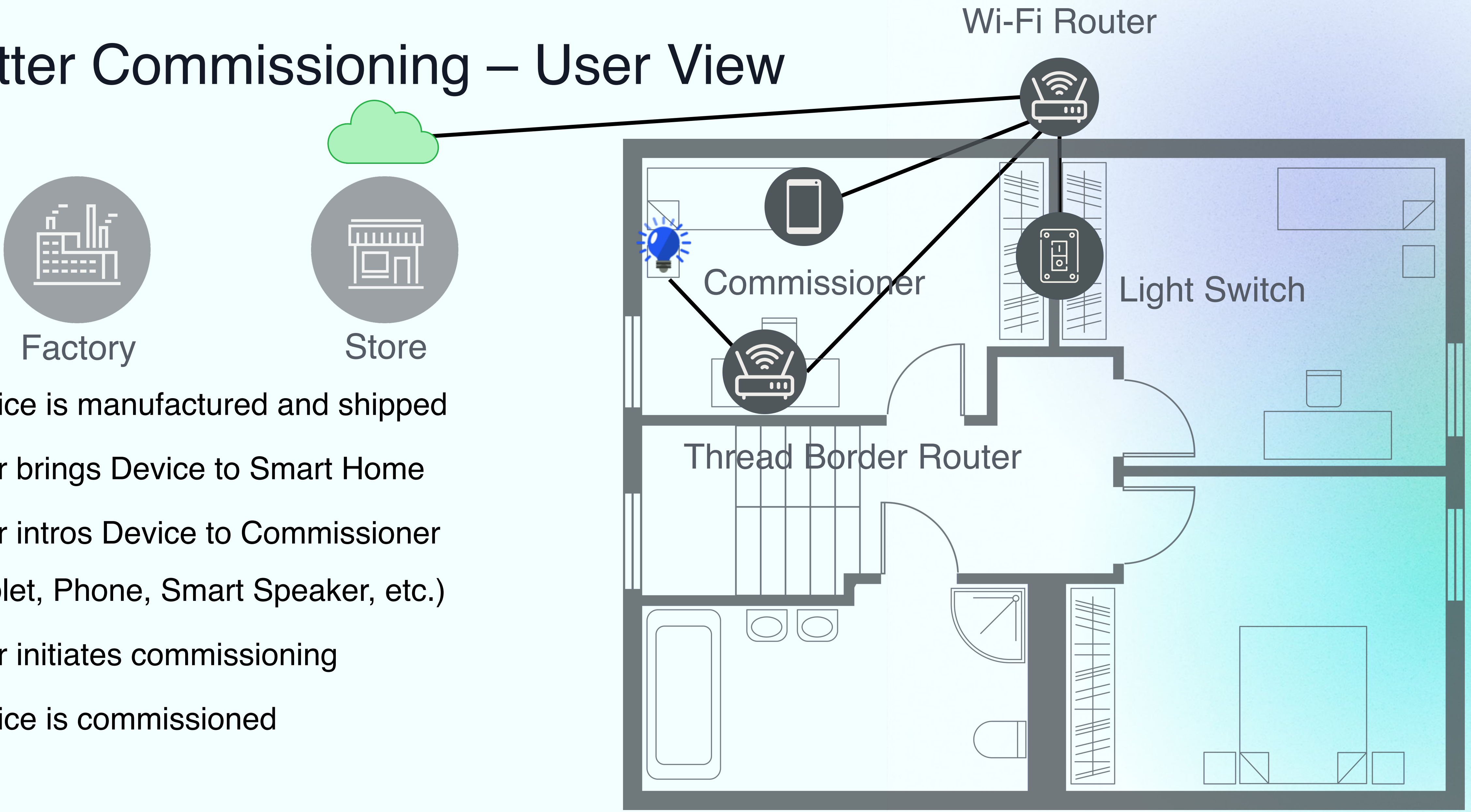


Matter Commissioning – User View



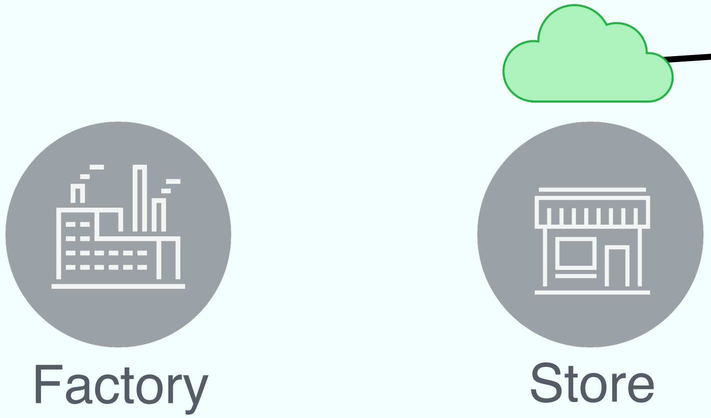
1. Device is manufactured and shipped
2. User brings Device to Smart Home
3. User intros Device to Commissioner (Tablet, Phone, Smart Speaker, etc.)
4. User initiates commissioning

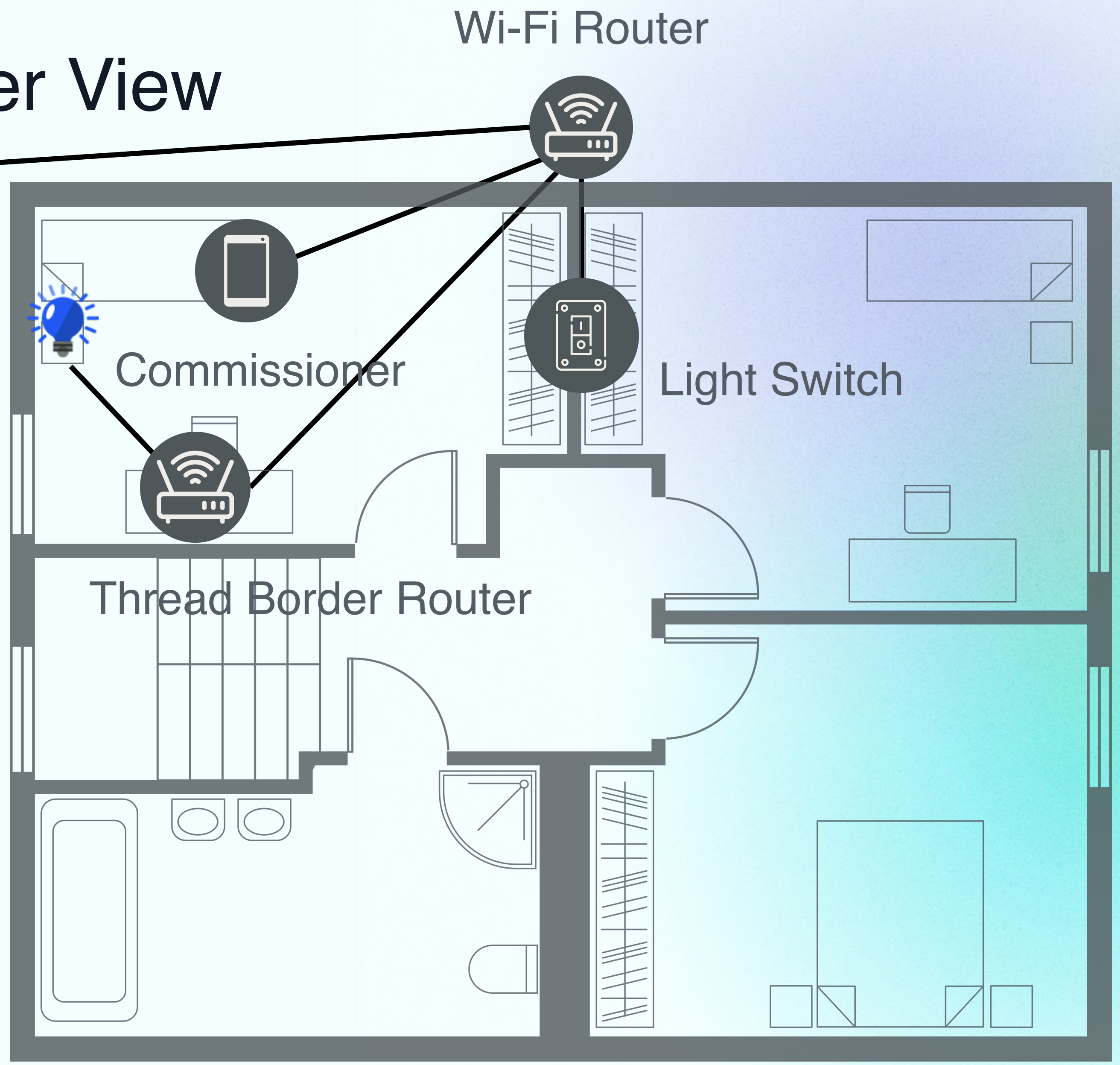
Matter Commissioning – User View



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

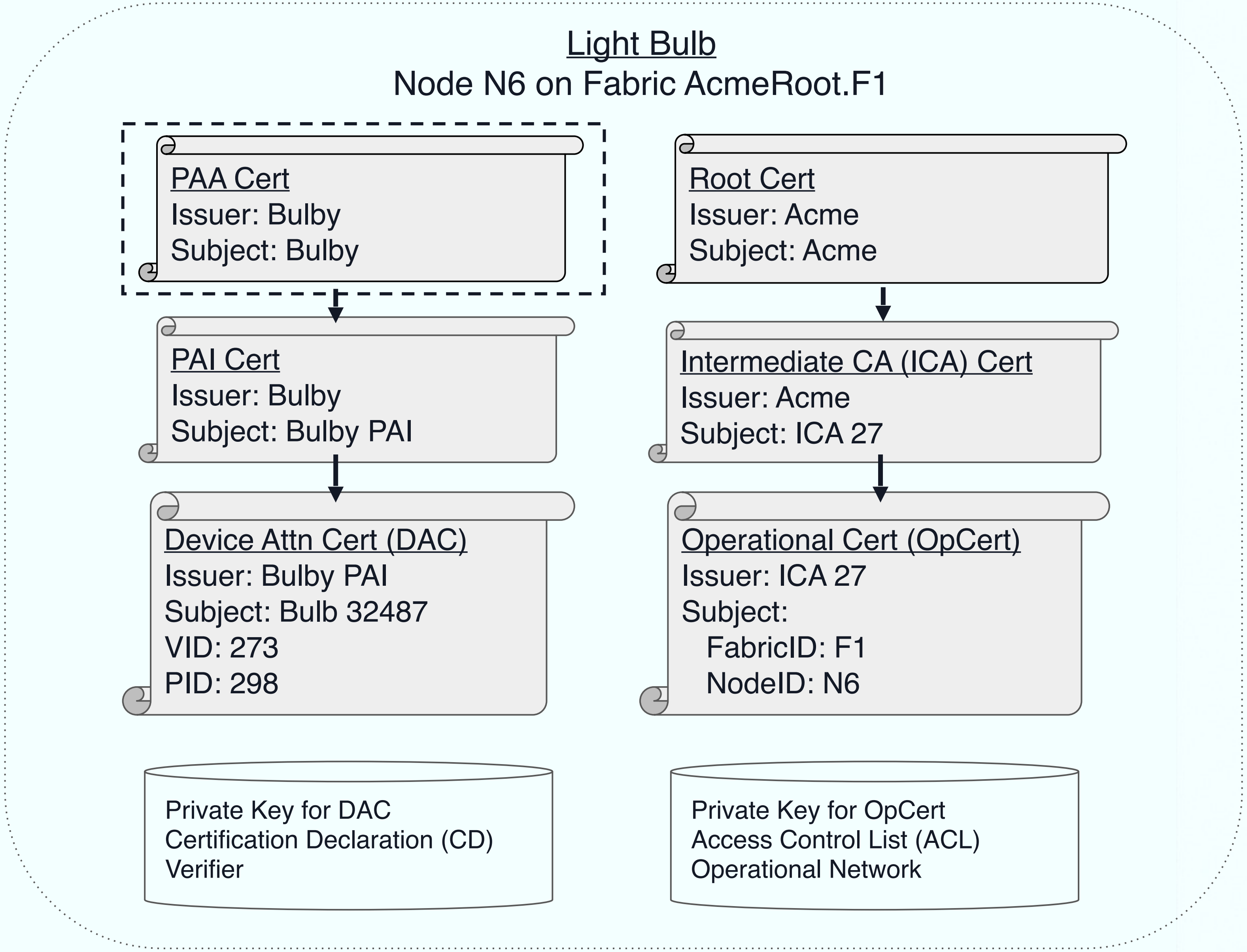
Matter Commissioning – User View





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

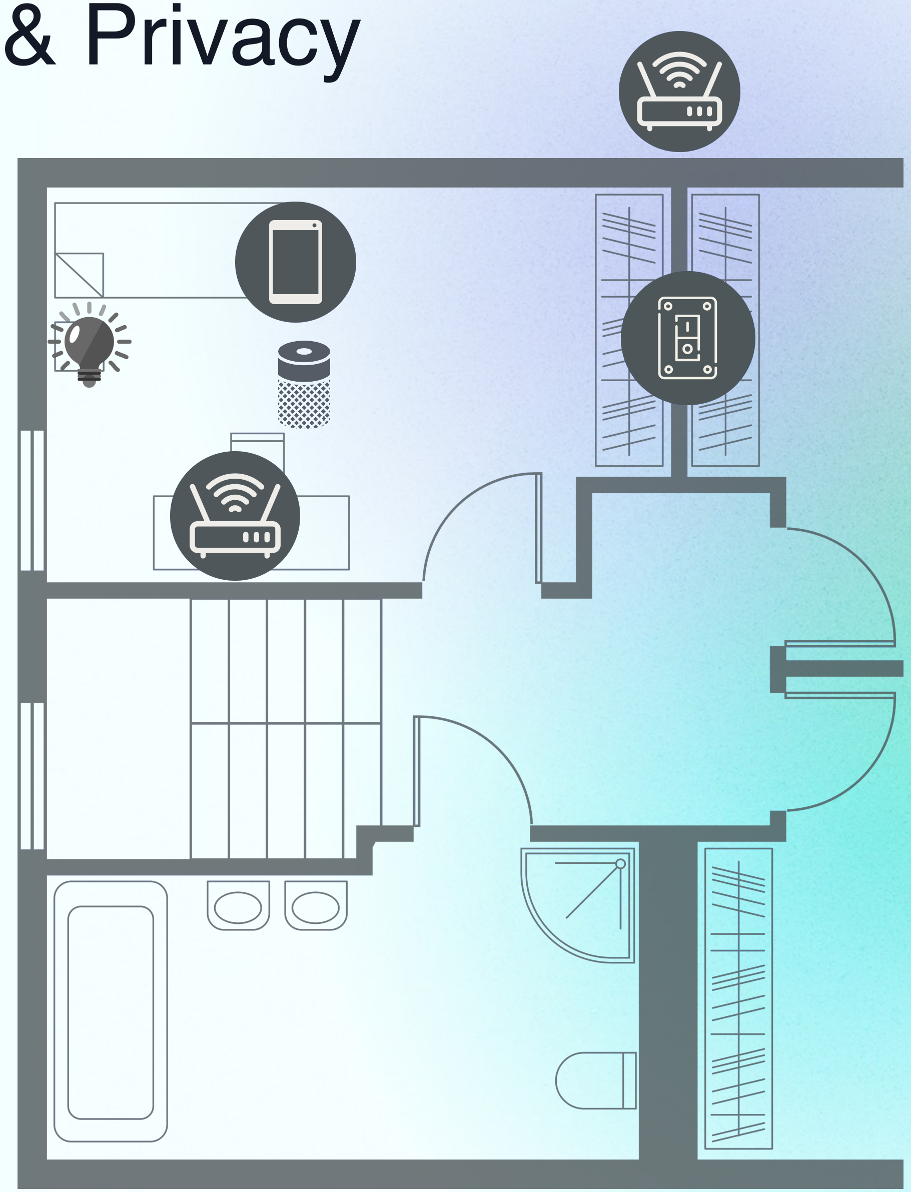
Root Cert
Issuer: Acme
Subject: Acme

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

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

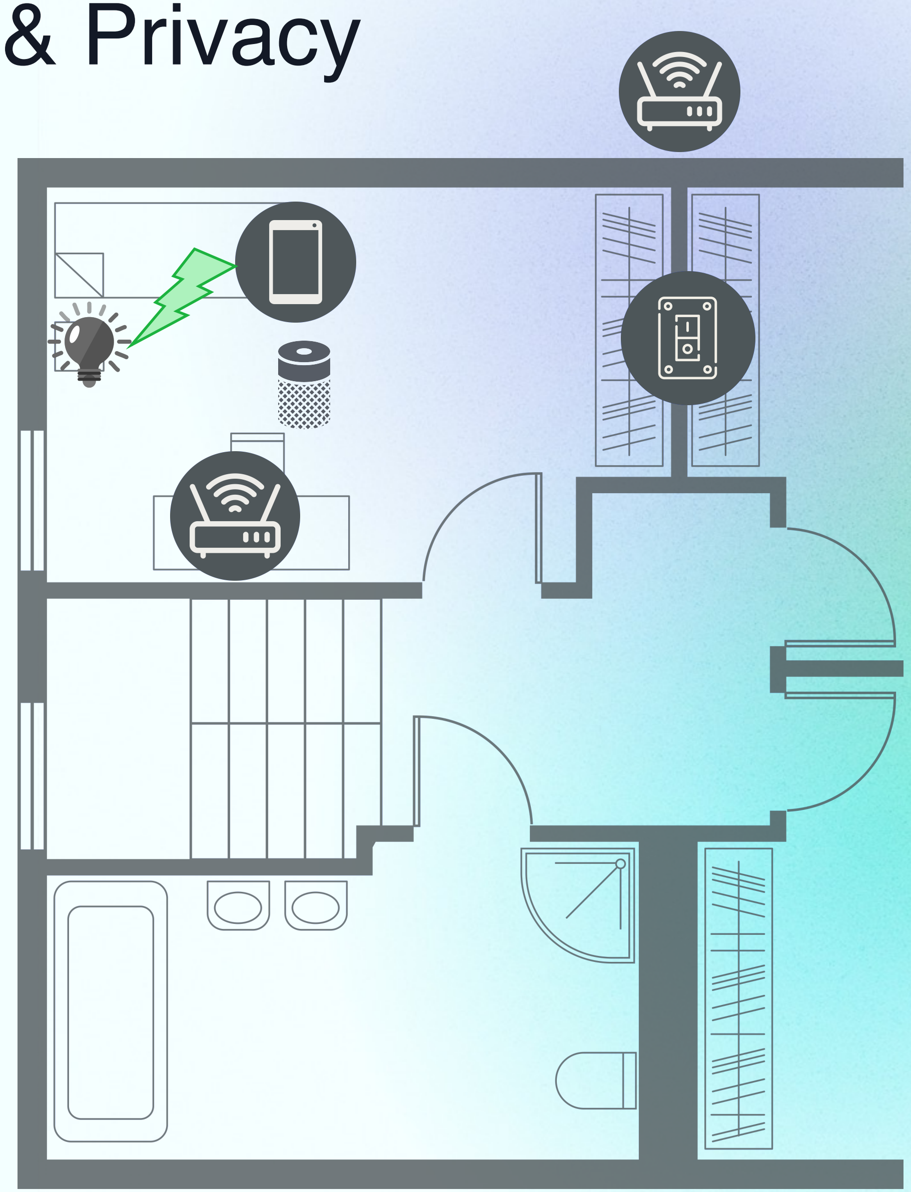
Private Key for OpCert
Access Control List (ACL)
Operational Network

Matter Raises the Bar for IoT Security & Privacy



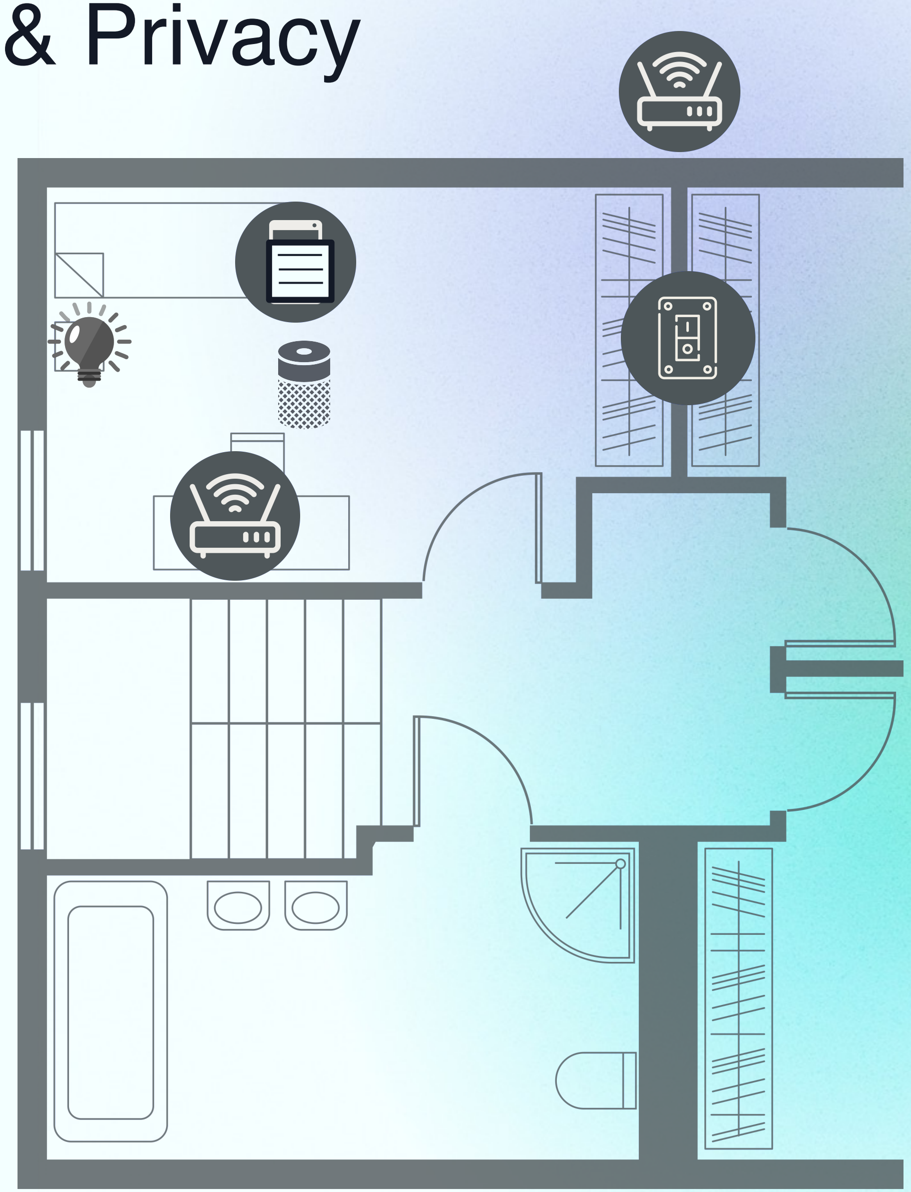
Matter Raises the Bar for IoT Security & Privacy

1. Easy, secure, and flexible device commissioning



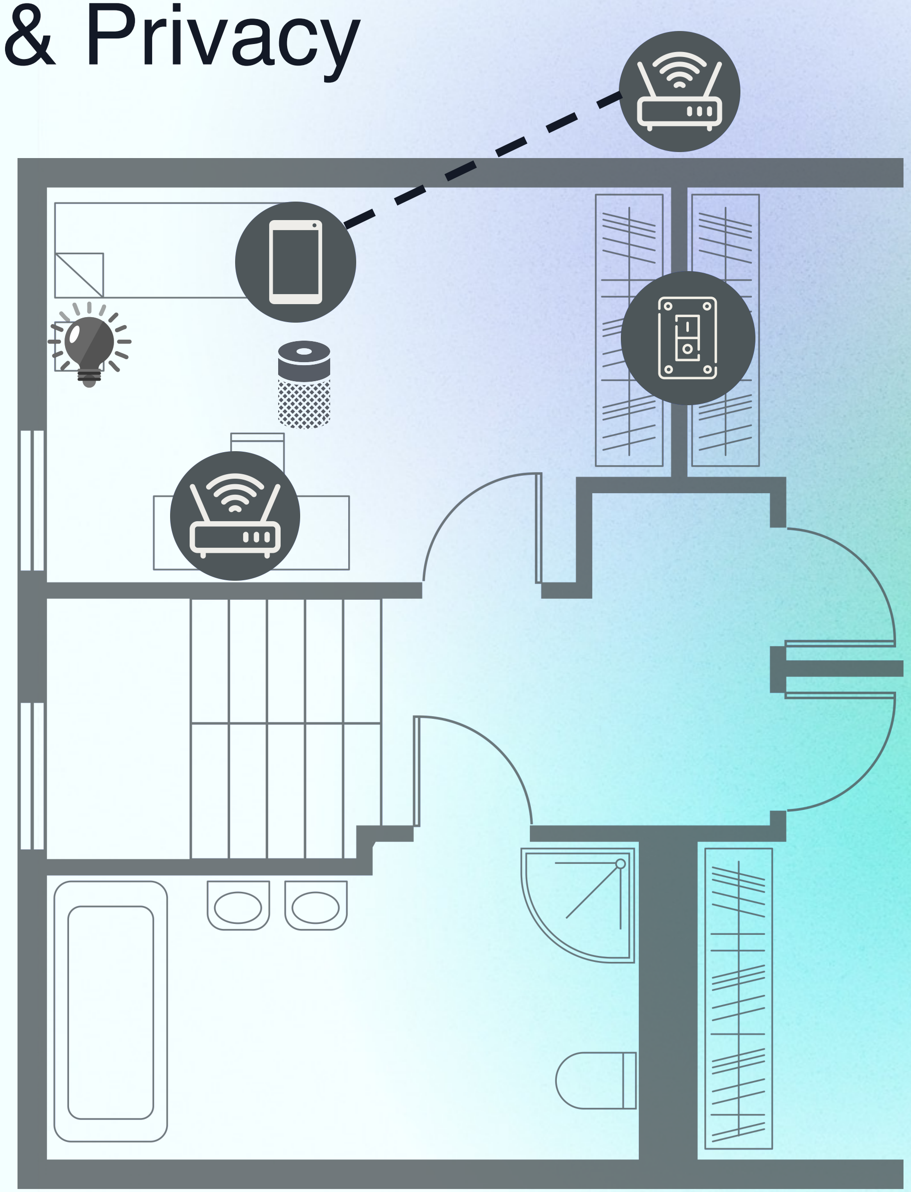
Matter Raises the Bar for IoT Security & Privacy

1. Easy, secure, and flexible device commissioning
2. Validation that each device is authentic and certified



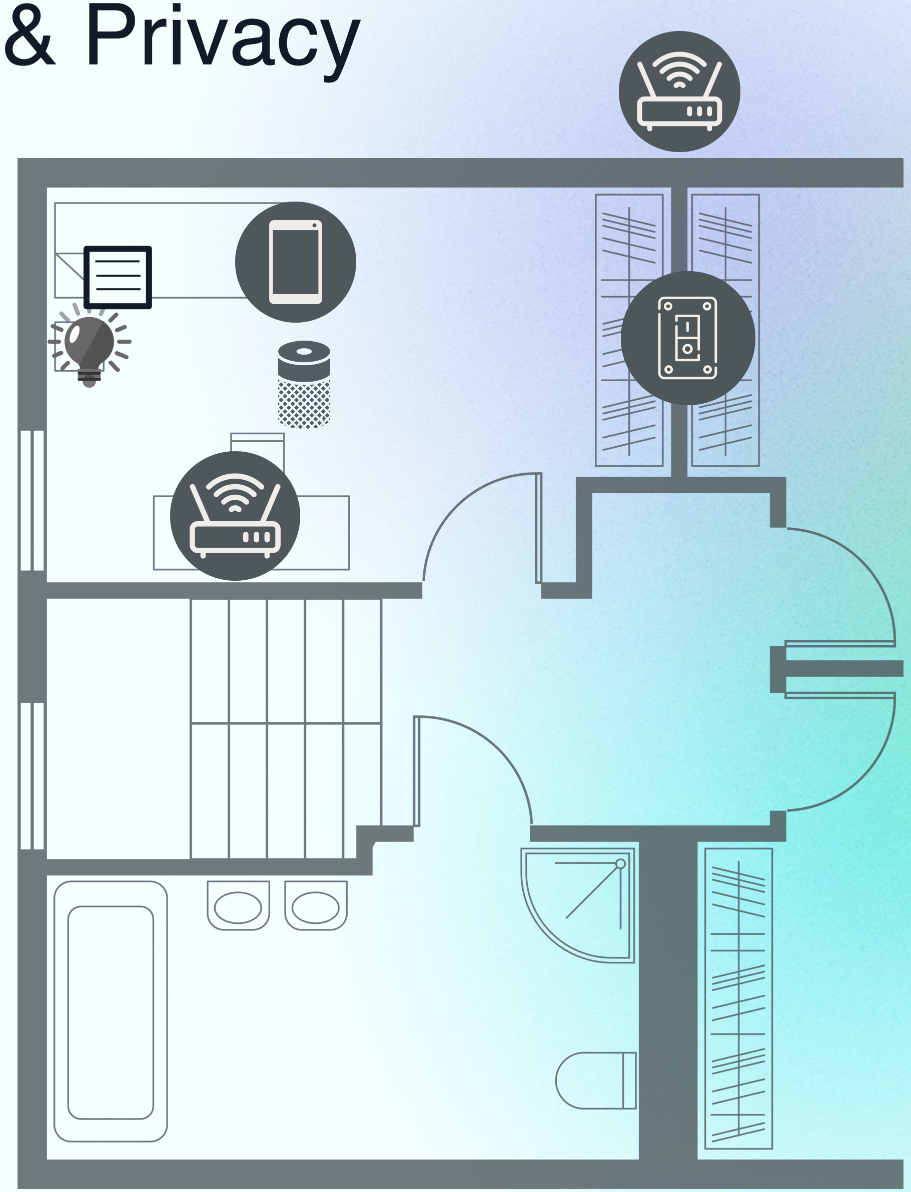
Matter Raises the Bar for IoT Security & Privacy

1. Easy, secure, and flexible device commissioning
2. Validation that each device is authentic and certified
3. Up-to-date info via Distributed Compliance Ledger



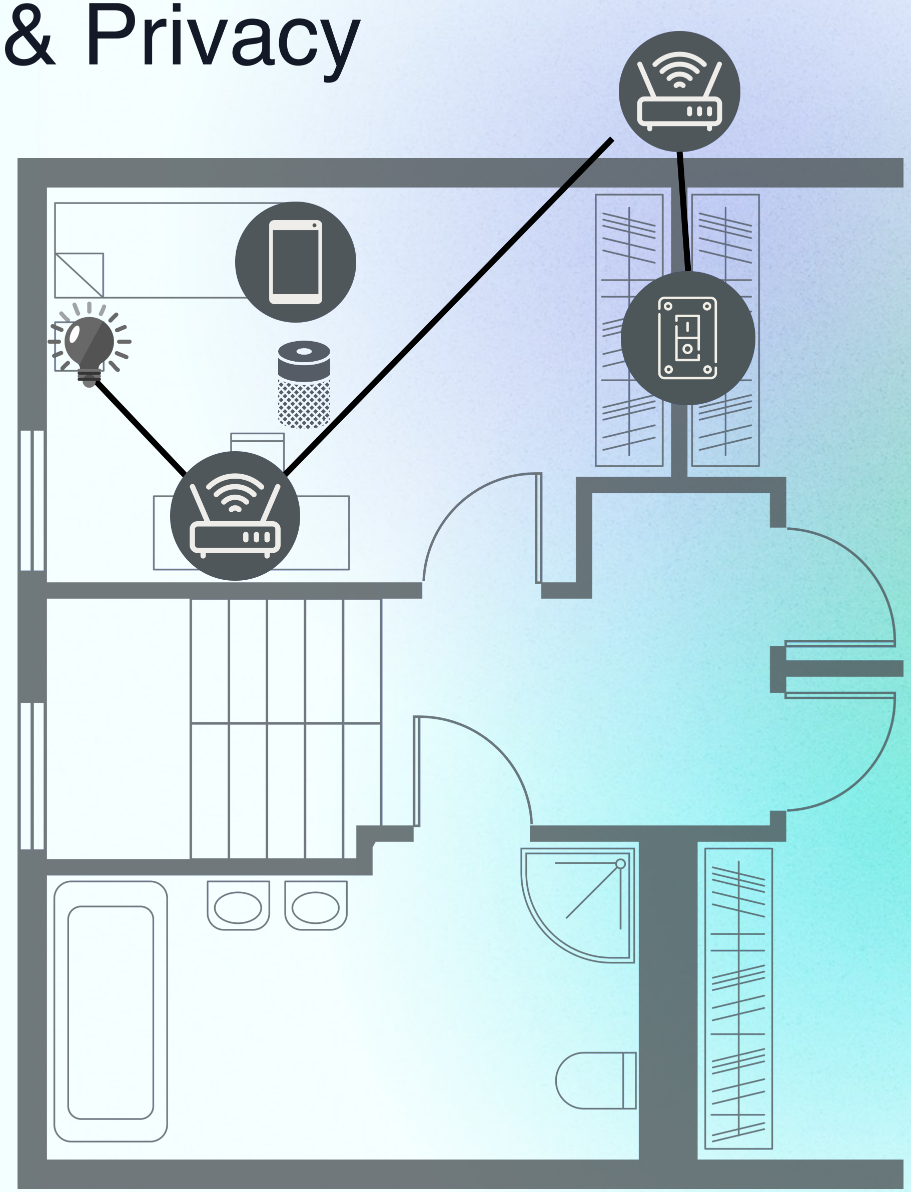
Matter Raises the Bar for IoT Security & Privacy

1. Easy, secure, and flexible device commissioning
2. Validation that each device is authentic and certified
3. Up-to-date info via Distributed Compliance Ledger
4. Strong device identity so only your devices can join your smart home



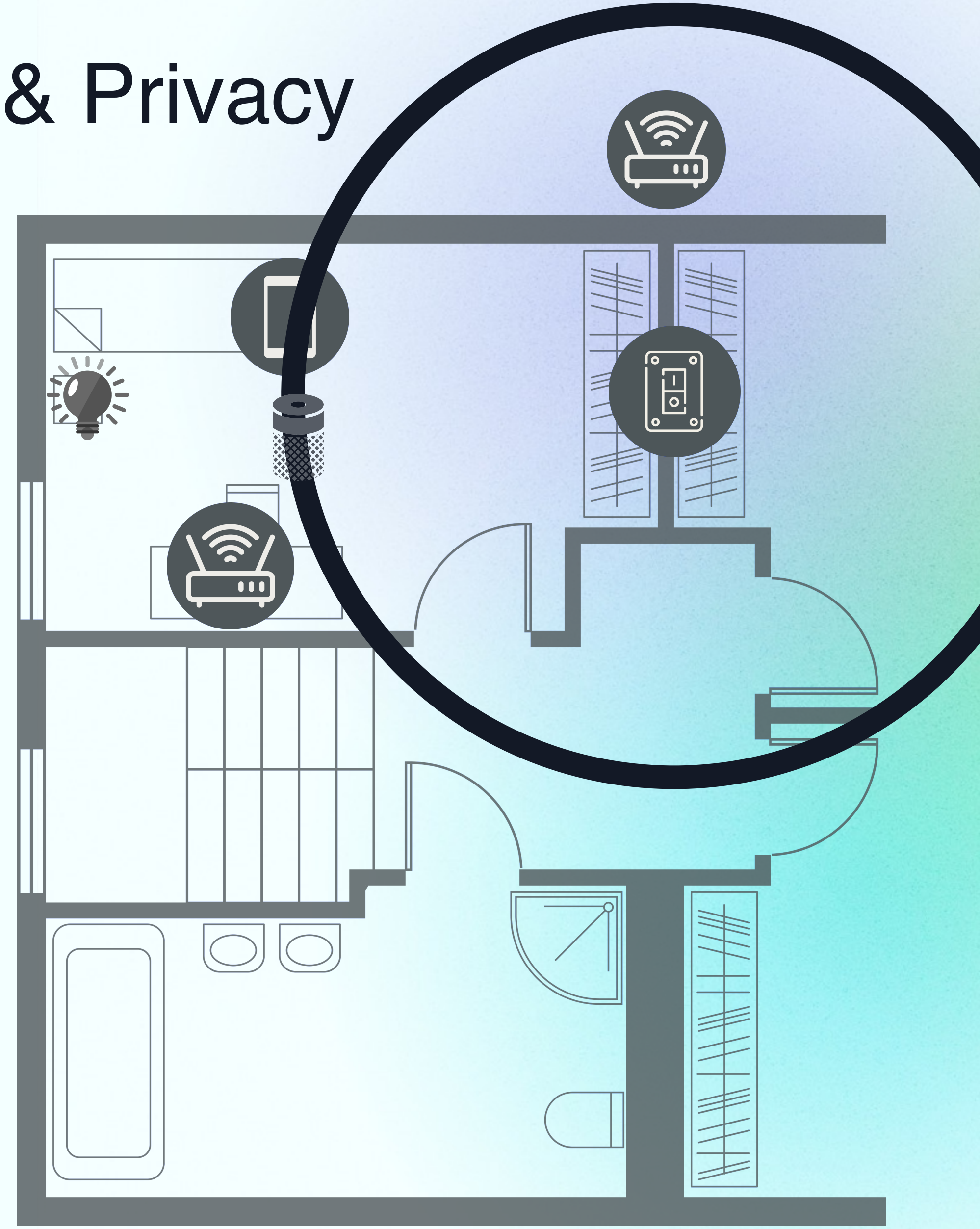
Matter Raises the Bar for IoT Security & Privacy

1. Easy, secure, and flexible device commissioning
2. Validation that each device is authentic and certified
3. Up-to-date info via Distributed Compliance Ledger
4. Strong device identity so only your devices can join your smart home
5. Secured unicast communications



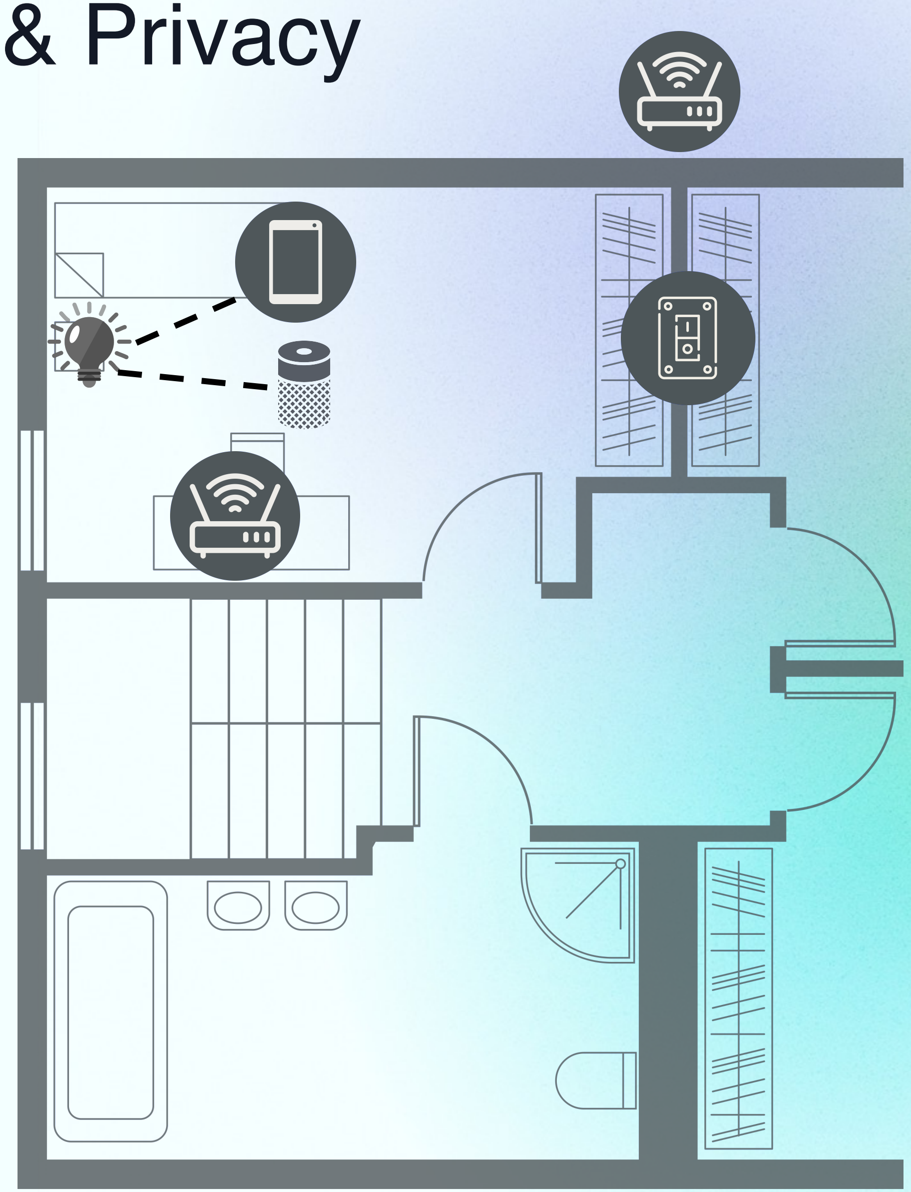
Matter Raises the Bar for IoT Security & Privacy

1. Easy, secure, and flexible device commissioning
2. Validation that each device is authentic and certified
3. Up-to-date info via Distributed Compliance Ledger
4. Strong device identity so only your devices can join your smart home
5. Secured unicast communications
6. Secured group communications



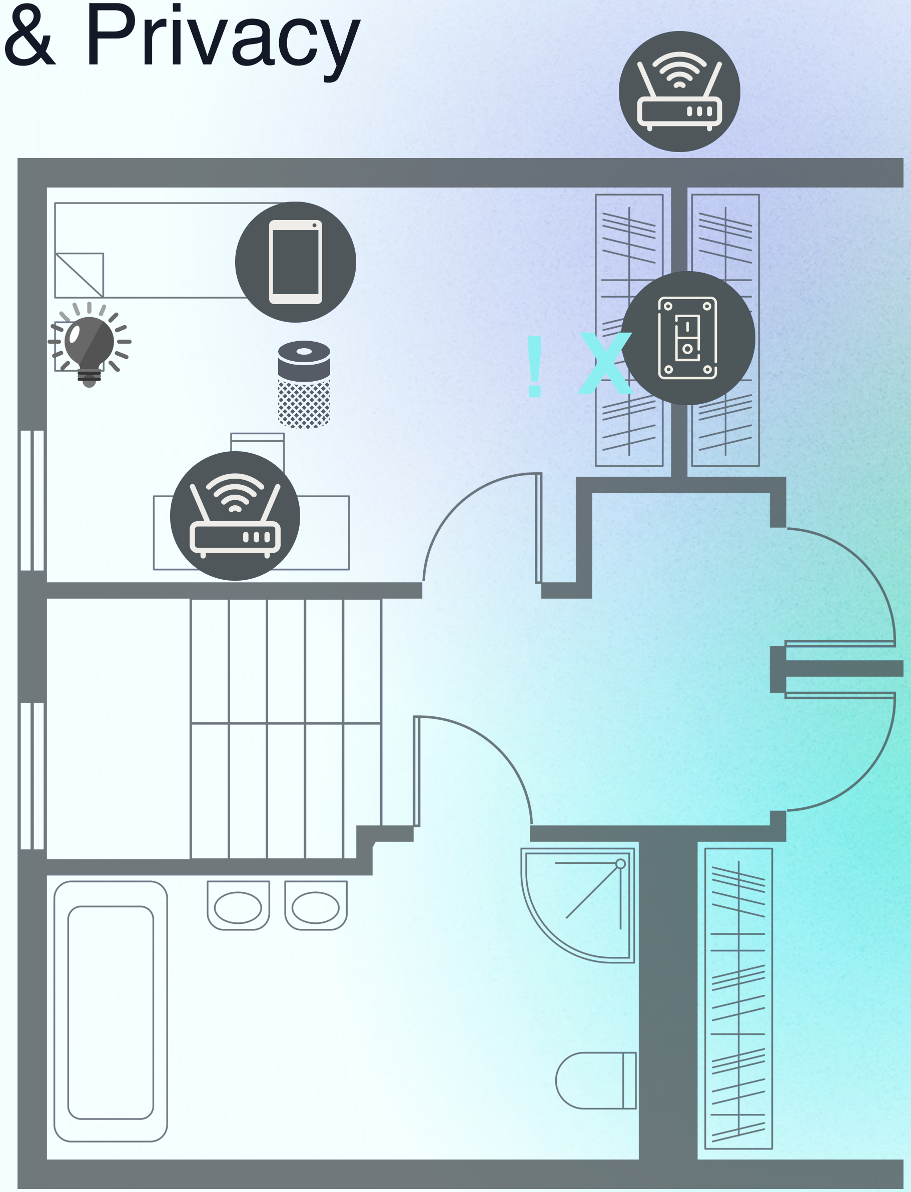
Matter Raises the Bar for IoT Security & Privacy

1. Easy, secure, and flexible device commissioning
2. Validation that each device is authentic and certified
3. Up-to-date info via Distributed Compliance Ledger
4. Strong device identity so only your devices can join your smart home
5. Secured unicast communications
6. Secured group communications
7. Multiple administrators and controllers, maximizing choice



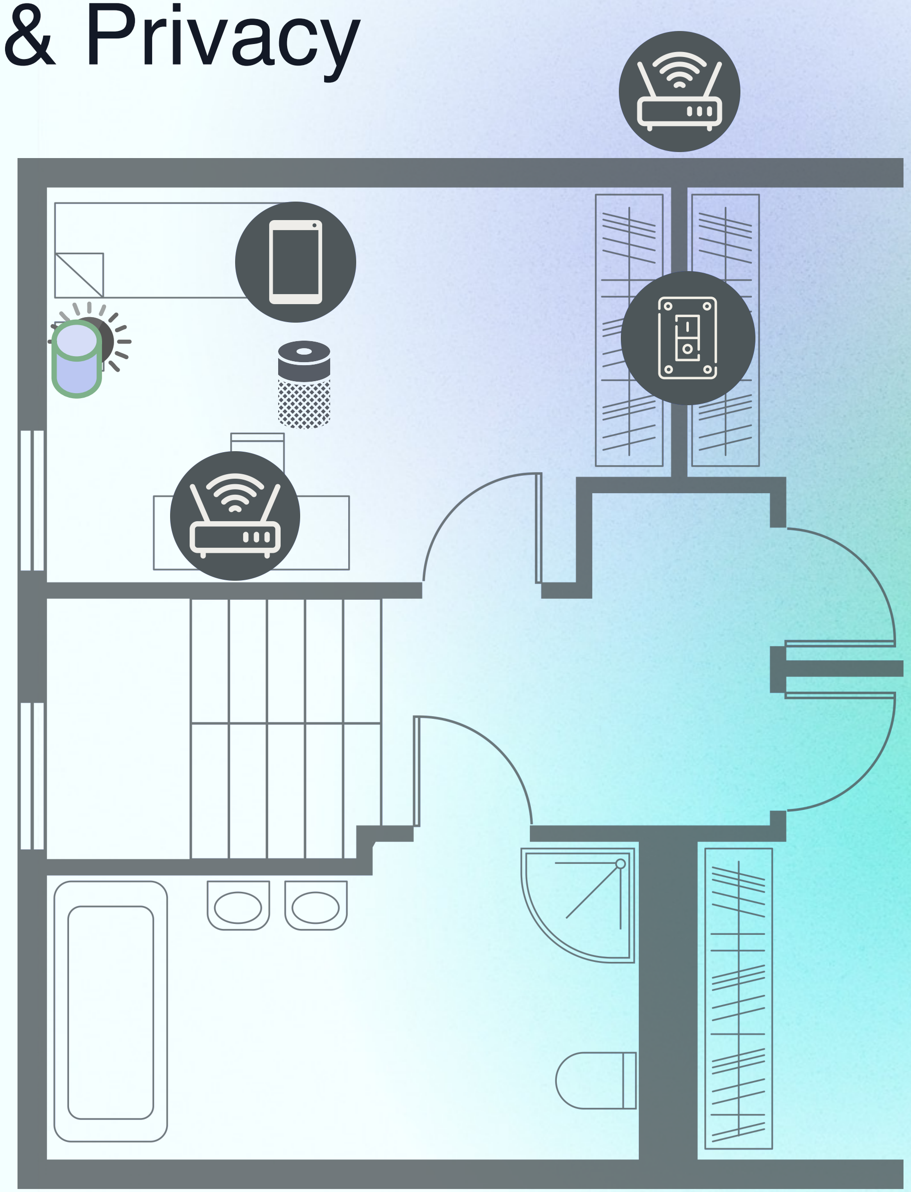
Matter Raises the Bar for IoT Security & Privacy

1. Easy, secure, and flexible device commissioning
2. Validation that each device is authentic and certified
3. Up-to-date info via Distributed Compliance Ledger
4. Strong device identity so only your devices can join your smart home
5. Secured unicast communications
6. Secured group communications
7. Multiple administrators and controllers, maximizing choice
8. Verified access controls to prevent unauthorized actions



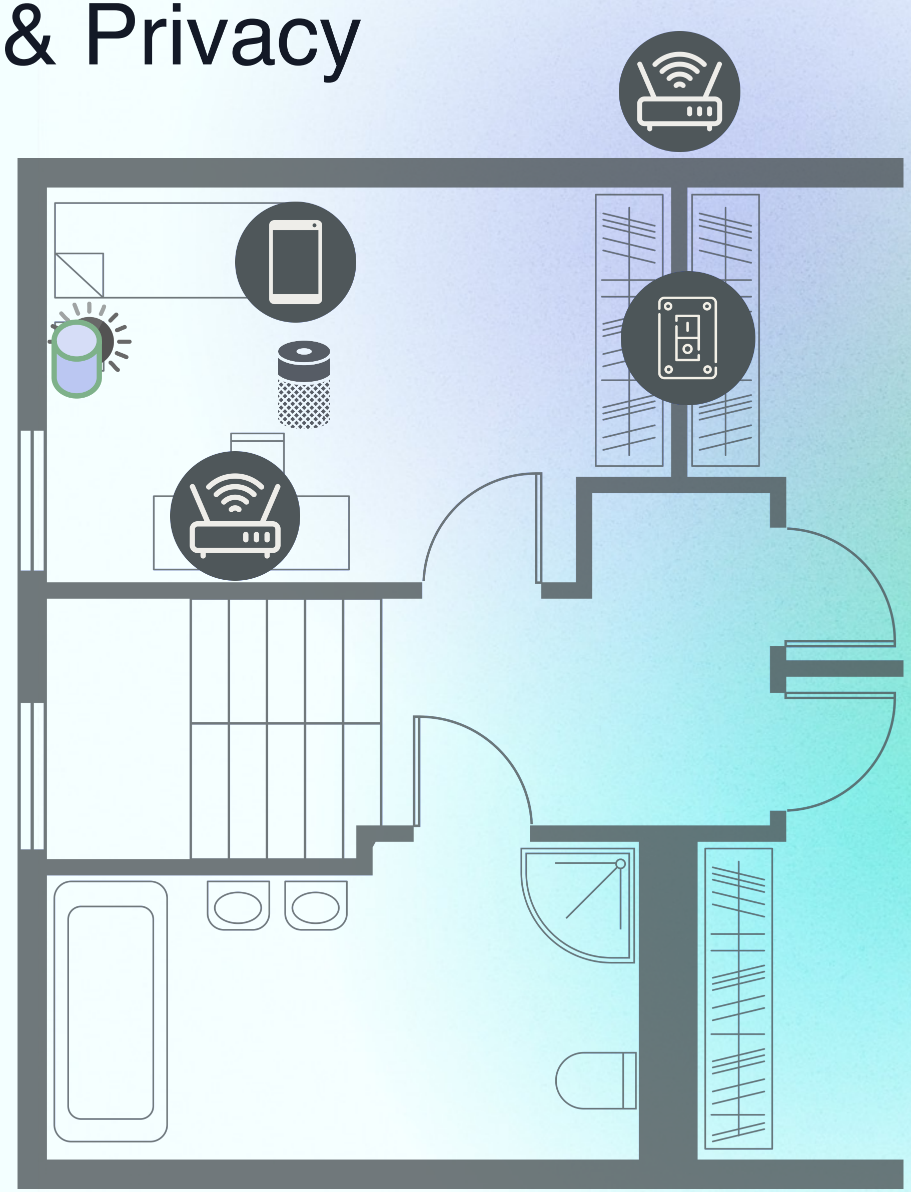
Matter Raises the Bar for IoT Security & Privacy

1. Easy, secure, and flexible device commissioning
2. Validation that each device is authentic and certified
3. Up-to-date info via Distributed Compliance Ledger
4. Strong device identity so only your devices can join your smart home
5. Secured unicast communications
6. Secured group communications
7. Multiple administrators and controllers, maximizing choice
8. Verified access controls to prevent unauthorized actions
9. Secured, standard software updates



Matter Raises the Bar for IoT Security & Privacy

1. Easy, secure, and flexible device commissioning
2. Validation that each device is authentic and certified
3. Up-to-date info via Distributed Compliance Ledger
4. Strong device identity so only your devices can join your smart home
5. Secured unicast communications
6. Secured group communications
7. Multiple administrators and controllers, maximizing choice
8. Verified access controls to prevent unauthorized actions
9. Secured, standard software updates
10. Verification of software integrity



Continuing to Raise the Bar

Matter will continue to raise the bar for security and privacy

Ongoing Initiatives

- Positive engagement with security researchers
- Open source and specs to encourage analysis and improvement
- Rapid vulnerability response process
- Continuous enhancements to Matter design and implementation

To learn more, visit: www.buildwithmatter.com csa connectivity standards alliance

The Connectivity Standards Alliance is the foundation and future of the Internet of Things. With its Members' diverse expertise, robust certification programs, and a full suite of open IoT solutions, the Alliance is leading the movement toward transforming the way we live, work and play.

Visit us at:
csa-iot.org and @csaiot