SCTE CABLE-TEC EXPO 22
SEPTEMBER 19-22 • PHILADELPHIA, PA

2022 Fall Technical Forum
SCTE • CABLELABS • NCTA

Matter

What It Is, How It Works and Why It Matters To The Cable Industry

Technical Paper prepared for SCTE by

Haefner, Kyle, Ph.D.
CableLabs
k.haefner@cablelabs.com

Haque, Asad
Comcast
asad_haque@comcast.com

Page, Jason
Charter Communications
jason.page@charter.com

Table of Contents

List of Figures

1. Introduction

1.1. General Overview of IoT

A new phenomenon is sweeping our lives, involving both small and large devices communicating with each other, and providing rich information that enhances how we live, work, and play. We can tell from miles away if our home is at the right temperature if the porch light is on or if the front door is locked. This is possible because thermostats, bulbs, and door locks can communicate their status, receive commands and act on them. These devices employ a range of network protocols to communicate over the Internet. By using the Internet as the medium, devices can be placed in geographically dispersed locations and still provide near real-time status or environmental reading.

However, this type of convenience comes with a price i.e., how can IoT devices be adequately secured given their constrained nature? How can they fend for themselves in a hostile network environment? These devices are often inexpensive, easy to use, and quick to set up. However, they lack the proper hardware and software security needed to ensure data privacy and integrity.

1.2. Lack of Interoperability - Lack of Open Standards

Lack of standards is manifested in consumer frustration, manufacturer headaches and service provider anxiety. OEM's need to support multiple "stacks" and service providers need to build complex integration models to support thermostats from five different manufacturers. The high-level diagram below (Figure 1.) shows current silos and industry fragmentation in IoT landscape.

The lack of widely adopted IoT application standards is a significant barrier to mass adoption of IoT devices, especially by consumers. The current wall garden approach not only stymies innovation by developers but also acceptance by consumers. The lack of standard results in increased investment by developers because they must develop for multiple application stacks. Similarly, consumers have to invest in new devices every time they switch to a new IoT ecosystem because their current investment in devices will be incompatible.

The disparate protocols create an IoT quilt consisting of a patchwork of communication standards and device models leaving devices unable to interact with each other based on which part of the quilt they belong.

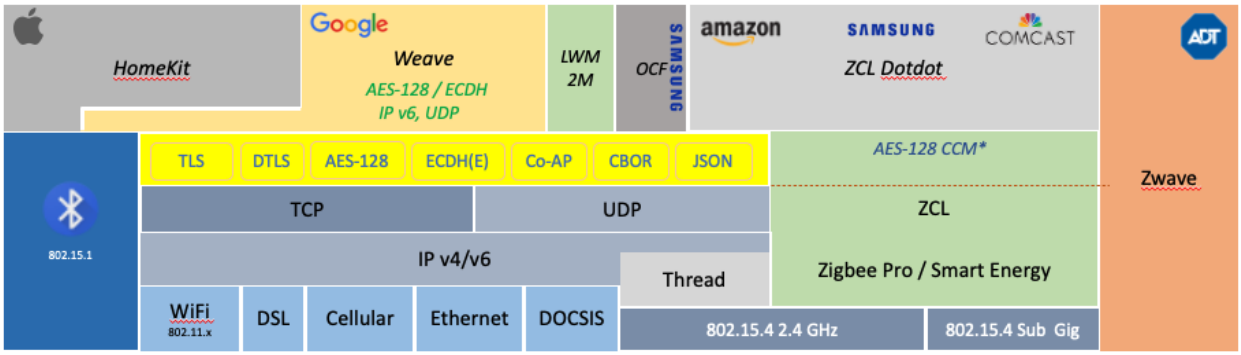

Figure 1: IoT Quilt

What industry needs is a cooperative effort that leads to a widely adopted standard with input from a wide swath of the IoT industry. This is exactly what Matter is. It grew from a need to create a new standard that

brings the best components from prevailing walled gardens in an open effort that guarantees participation from willing participants in drafting the new standard that will have wide acceptability from the launch.

1.3. Consumer Branding/Labeling/Proximal Interoperability

All the industry cooperation in the world will make little difference to the current smart home landscape if consumers do not literally buy in. The Connectivity Standards Alliance, CSA - the standards development organization (SDO) that maintains Matter - recognizes this and has developed marketing materials and a consumer-facing brand to help drive adoption. Starting this fall, consumers will be able to purchase products that contain the Matter logo on their packaging. This logo will signal to consumers that the device they purchase is guaranteed to work with their Matter applications. In the way that users currently associate the Wi-Fi logo with interoperable wireless connectivity, the Matter logo will be associated with guaranteed smart home interoperability.

Manufacturers can only display the Matter logo on their packaging if their devices have been certified. The certification process is run by CSA authorized test labs and is designed to guarantee conformance to the Matter specification. This process is analogous to devices being certified for Wi-Fi, Zigbee, Bluetooth, and many other protocols. With certification, a user can feel confident that the device they purchase will work seamlessly with their Matter application, access point, and other Matter devices. Certification is available to all CSA member companies.

1.4. Lack of Security/Uniform Standard for Security

IoT devices provide a fertile ground for hacking leading to either privacy violation, loss of service or dangerous situations. Two security researchers successfully commandeered a Jeep Cherokee using remote exploit (Greenberg, 2015). Incidents like these demonstrate that today's IoT needs to be empowered so that they can protect themselves in a hostile environment. In September 2016, the website of computer security consultant Brian Krebs was hit with 620 Gbps of traffic emanating from hijacked IoT devices, "many orders of magnitude more traffic than is typically needed to knock most sites offline" Kolias (2017, p.81). This attack exploited IoT devices such as cameras and DVRs that had default passwords to effectively turn thousands of these devices into a bot army. These devices were then used to launch a massive denial of service attack on DNS service provider Dyn, effectively causing an Internet blackout. This malware is dubbed "Mirai". One analysis of the attack showed that the Mirai malware had infected 49,657 unique devices, which included mostly IP based cameras, but also DVRs and routers (Herzberg, Bekerman, & Zeitman, 2016).

Such vulnerabilities are compounded by a lack of common IoT application standards that are created with security and privacy as one of the core principles. With disparate security implementations, IoT devices suffer from multiple possible attack vectors due to different security layers and their implementations.

1.5. Introduction to Matter

Matter is a next gen IoT application protocol designed from the ground up by IoT practitioners of the world. It is designed so that constrained IoT devices, controllers and Apps can interoperate, providing consumers with a rich experience that IoT devices offer. It also provides a standardized, compatible operating environment on which to build amazing experiences for developers. Similarly, retailers will benefit from simplified selling experience. Rather than invent underlying primitives, Matter uses proven technology and contributions from Amazon, Apple, Comcast, Google, Silicon Labs, Samsung, and others who have contributed resources in following key areas.

- Canonical Protocol Specifications
- Standardized SDK that implements the canonical Specification
- Test harness that checks SDK for compliance with the canonical Specification

Matter provides a unified out-of-box commissioning and pairing mechanism that ensures onboarding interoperability and compatibility between IoT devices made by a myriad of manufacturers. In addition to commissioning, included in the Matter stack are following features.

- Flexible device and service discovery
- A certificate-based device attestation process
- A secure end to end mutual authentication and encryption that provides security, privacy, and integrity of inter device communications.
- A unified and flexible interaction layer between data model and routing layer
- A unified data model with a wide range of device types defined

The following diagram depicts different layers of Matter protocol.

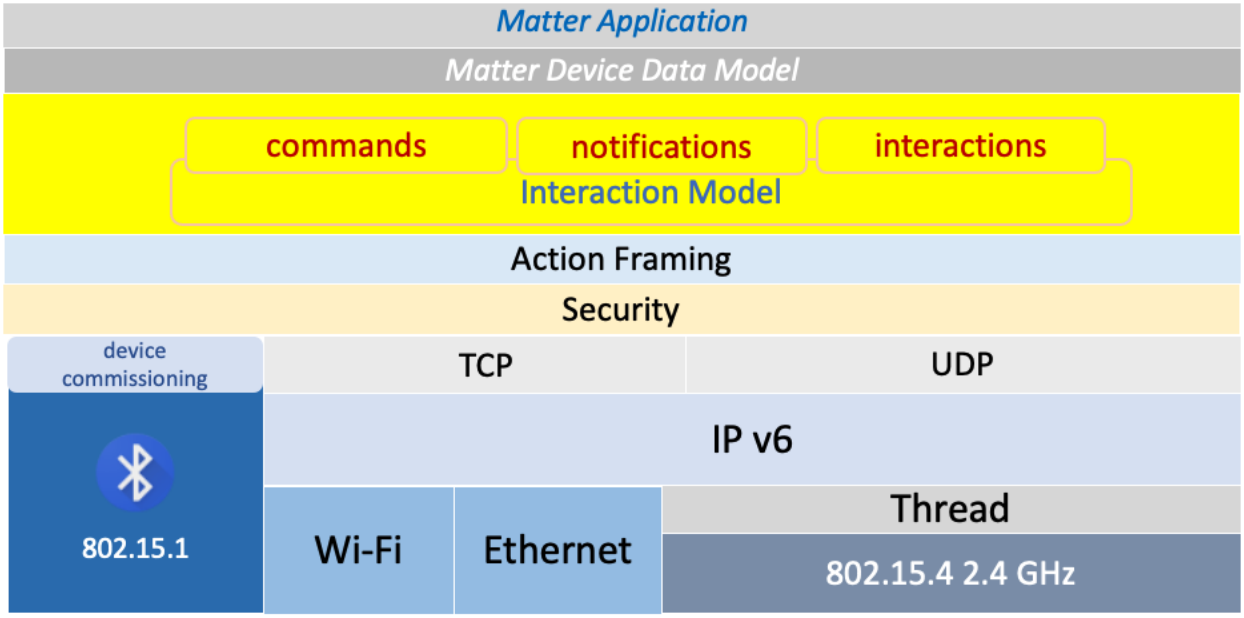

Figure 2: Matter Protocol Layers

1.6. Impact for Cable Operators.

Cable operators will be impacted by the emergence of Matter in several ways. Perhaps the most immediate impact is the introduction of a new wireless protocol, Thread, to the smart home. Over time, more and more low cost, low power, and low bandwidth devices will adopt this protocol and consumers will begin to expect support within their access point. Cable operators that fail to meet this expectation should expect increased call volume due to failed onboarding and lack of end device connectivity. Where Thread connectivity winds up being provided by some other device, such as a smart speaker, cable operators will lack any visibility into the state of the Thread network and have limited tools to support their customers. Matter will also increase the amount of broadcast and unicast traffic on a consumer's local area network. All this traffic will be encrypted leaving cable operators unable to effectively characterize it as malicious or safe. Participation in Matter will provide operators tools to better understand the devices on their customers networks and those devices' expected behavior. Matter also requires support for IPv6 and multicast DNS. Cable operators who do not currently support these technologies should expect increased call volume. Operators must support at least the basic requirements of Matter; Wi-Fi, Thread, IPv6, and mDNS. Failure to do so will risk their current managed access point offerings becoming obsolete, resulting in a lower take rate for this recurring source of revenue.

2. Matter Architecture

2.1. Transports and Network Stack (Wi-Fi, Thread, BLE, IPv6, DNS-SD)

At its core, Matter is a specification that defines a framework for interoperable, local network communication. The Matter specification allows for application layer messages to be transported over any IPv6 bearing network. Version 1.0 explicitly lists three compatible transports: Wi-Fi, Ethernet, and Thread. Wi-Fi and Ethernet are aimed at general purpose or high bandwidth applications and provide access to a local area network, LAN. Thread is aimed at low power and low bandwidth applications and

provides a mesh network topology known as a personal area network, PAN. A device known as a Thread Border Router allows for messages to be transported between the LAN and PAN. Cable companies that currently offer Wi-Fi routers should consider adding Thread support and enabling Border Router functionality. This will increase the range of devices they can currently support, provide access to useful information about the Thread PAN and network topology, and ensure their current connectivity solutions maintain pace with user expectations.

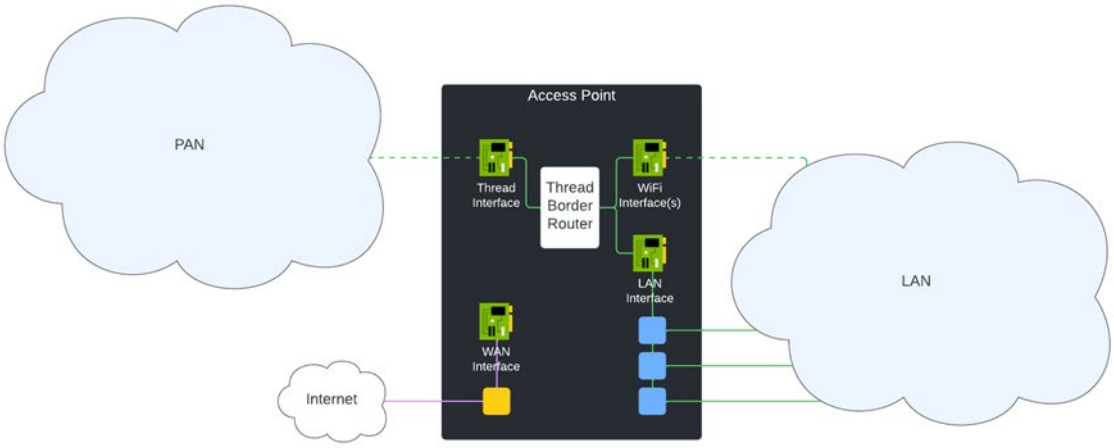

Figure 3: Router Architecture

In addition to IPv6 bearing transports, Matter also utilizes a few additional technologies to enable device discovery and network onboarding. One such technology is Bluetooth Low Energy, BLE. Matter utilizes BLE to enable discovery of commissionable devices and to facilitate a series of messages designed to verify the authenticity of a device, provision the device with Matter credentials, and to transmit credentials needed to connect to the user's Wi-Fi or Thread network. Devices that support BLE, this includes all Matter Thread devices, will initially advertise themselves over BLE when first powered on. Once they have been configured through the Matter commissioning process they will begin to operate over Wi-Fi or Thread.

Matter also makes extensive use of DNS service discovery, DNS-SD. This technology is utilized for device discovery and IP resolution. In the case of device discovery, devices that have already been onboarded to the user's LAN or PAN can publish themselves as commissionable for Matter commissioners to discover. In this situation the commissioning process would occur over IP on the respective transport and not utilize BLE. In the case of IP resolution, DNS-SD is utilized to resolve the IP address of commissioned devices, known in Matter as nodes, on the LAN or PAN. Utilizing DNS-SD to resolve a node's IP address allows for greater flexibility with IP assignment and does not require the node's IP to remain fixed over time. Nodes publish their presence with the **_matter._tcp** service and include an identifier consisting of their Fabric ID and Node ID. This allows the IP address of a Matter device to be resolved to its Fabric scoped Matter node identifier.

2.2. Fabrics

Matter groups collections of devices, Matter nodes, into what are known as Fabrics. Fabrics exist to provide: a common root of trust for this collection, enable encrypted communications between nodes, and

provide a set of scoped access controls. Fabrics exist only at the application layer and are completely decoupled from a user's LAN or PAN. In practice, most Matter users will operate multiple Fabrics, one per application they utilize to control their smart home.

Fabrics are created, or provisioned, by a Trusted Root Certificate Authority, TRCA. A Fabric ultimately consists of a unique 64-bit identifier and the public key certificate of the TRCA. A Matter device may belong to one or more Fabrics and would have a unique Node ID and Node Operational Certificate, NOC, for each Fabric it belongs to. This structure is what allows a Matter device to be controlled from multiple applications, provides users flexibility in granting applications access to Matter devices, and prevents ecosystem lock-in. Cable operators are well positioned to be TRCAs and provide supporting services to businesses that wish to participate in Matter but don't want to manage the required PKI.

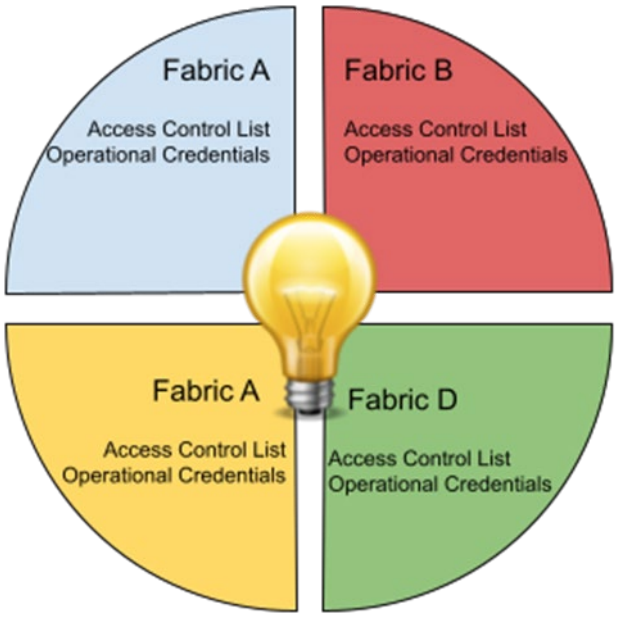

Figure 4: Matter Fabrics

Nodes within a Fabric are permitted to communicate with each other based on access controls scoped to that Fabric. Every Matter node must maintain a set of access controls for each Fabric it belongs to. These access controls dictate permissions other nodes on the Fabric have to interact with functionality, exposed through Clusters, that a given node hosts. Communications between nodes are encrypted using the NOC they were provisioned during commissioning into a Fabric. This functionality allows for a secure channel to be established between nodes and is analogous to how communications are secured between modern Internet websites and browsers using HTTPS and PKI.

2.3. Data Model

In Matter, physical devices such as light bulbs, door locks, TVs, and more expose their functionality through the Zigbee Cluster Library, ZCL, data model. This data model enables interoperability between clients that issue commands and servers that accept commands. The highest order element in the Matter data model is a Device Type. Device Types can be things like dimmable light bulbs, thermostats, video players, and Wi-Fi access points. There are two high level Device Type categories in Matter, Utility Device Types and Application Device Types.

These Device Types are exposed through Endpoints that in many ways are akin to IP ports. A single physical device may expose multiple endpoints and therefore functionality of multiple Device Types. However, in practice most physical Matter devices will host two endpoints. One, endpoint 0 in all cases, that is used for administration and one that is used for actual application functionality. More information about Matter device types can be found in Connected Home over IP Device Library.

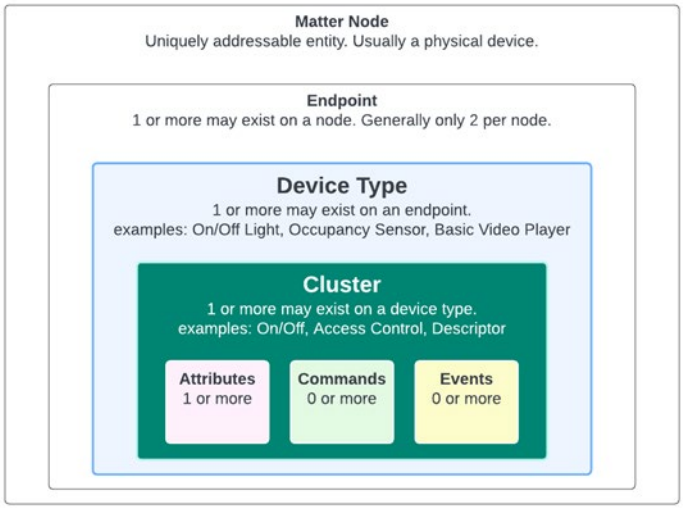

Figure 5: Device Types and Clusters

The functionality that a Matter Device Type exposes is done through implementing Clusters. Clusters are the foundational element of the ZCL data model and describe types of functionality such as the ability to turn something on or off, or adjust the level of something, like in a fan. Clusters are constructed from three lower-level elements: attributes, commands, and events. Attributes store state, such as the on or off state of a light bulb. Commands can be invoked to manipulate state, such as a toggle command to change the on or off state of a light bulb. Events can notify interested parties of updates to an attribute. An example of a complex interaction displaying all three Cluster conventions could involve an update to a thermostat that multiple occupants control from separate applications. In application 1, an occupant can invoke the 'SetpointRaiseLower' command hosted by the 'Thermostat Cluster' to adjust the 'OccupiedCoolingSetpoint' attribute. In a second application, another occupant that had subscribed to events on the 'Thermostat Cluster' could be notified through a Matter Cluster event of the update to the 'OccupiedCoolingSetpoint' attribute.

Clusters are defined as being either an application cluster or a utility cluster. Application clusters describe actual device functionality such as the ability to unlock a door lock. These clusters are generally hosted on endpoint 1 but may exist on multiple endpoints or have unconventional starting indices. Utility clusters are used to configure a Matter device or convey information about it. The functionality and information exposed on these clusters aids in commissioning, setting access controls, configuring bindings, reading logs, and more. In general, these clusters will be exposed through the Root Node device type that is always hosted on endpoint 0 for every Matter device. However, some utility Clusters, such as the Descriptor Cluster, exist on all endpoints that a device hosts. More information about application clusters can be found in Connected Home over IP Application Clusters. More information about utility clusters can be found in sections 9.5 – 9.14 and 11.1 – 11.19 of Connected Home over IP Specification.

2.4. Interaction Model

Matter defines four methods that a controller application can use to interact with the ZCL data model - read, write, invoke, and subscribe. These interactions ultimately allow an application to retrieve the current state of a device or to affect changes to its current state. Reads can be performed on cluster attributes to get their current state. An example would be reading the 'OnOff' attribute of a light bulb to determine if it was currently on or off. Writes can be performed on some cluster attributes to update their state. An example of this would be writing an entry to the 'NodeLabel' attribute to specify a user defined name for the Matter device. Invokes can be performed on cluster commands to affect the state of a cluster attribute. An example would be to invoke the 'Off' command to change the 'OnOff' attribute of a light bulb to off. Subscribes can be performed on many cluster attributes and events to receive notifications of changes to their state. An example would be to subscribe for updates to the 'CurrentLevel' attribute of a light bulb. With the subscription enabled, any time a user updates the level (brightness) of the bulb, all applications with active subscriptions would receive a message with the updated state.

2.5. Bridging - Current Networks and Legacy Devices

Bridges allow non-Matter IoT devices to participate in a Matter Fabric. This will allow consumers to continue to use some of their current (legacy) devices and will allow for a gradual transition to newer Matter-enabled devices. Bridges act as a translator between non-Matter protocols and Matter Fabrics. Similar to other Matter devices, a bridge can participate in many Matter Fabrics and must have at least one node on each Fabric. From that node the bridge will expose any number of endpoints through a specific device called an Aggregator. This device type has a cluster attribute that contains a list of all the bridged devices called a PartsList. Bridged endpoints are not full Matter nodes, they do not have their own Matter operational credential and all access control decisions for bridged devices will use the operational credential associated with the bridge. Access control entries can be specified using a set of targets that contain bridged device entries and bridged device types. For example, an ACL on a Matter lock could allow bridged device types of Window Sensor to read its state using the Node credential of the bridge.

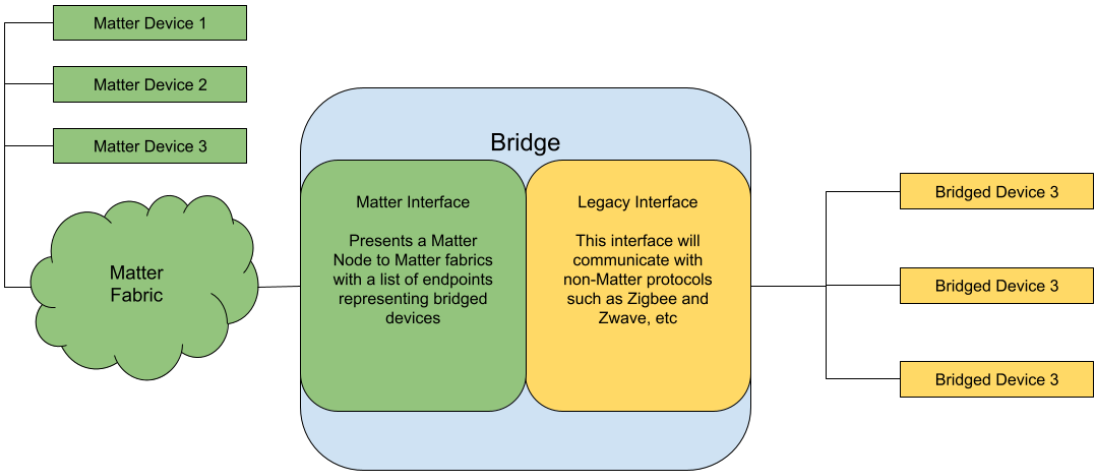

Figure 6: Bridging Architecture

3. Commissioning

The commissioning refers to a process of bootstrapping a network (aka a Fabric in Matter parlance) consisting of devices (including apps) that communicate with each other using Matter protocol. The commissioning process is designed to address following critical security principles.

a. User Intent - user is explicit in the intention to commission the device
b. Proof of Possession - the user is known to physically have and control the device
c. Initial Secure Channel - all communications to commission and configure are secure and encrypted
d. Device Authenticity - the user can be confident that the device is what it says it is

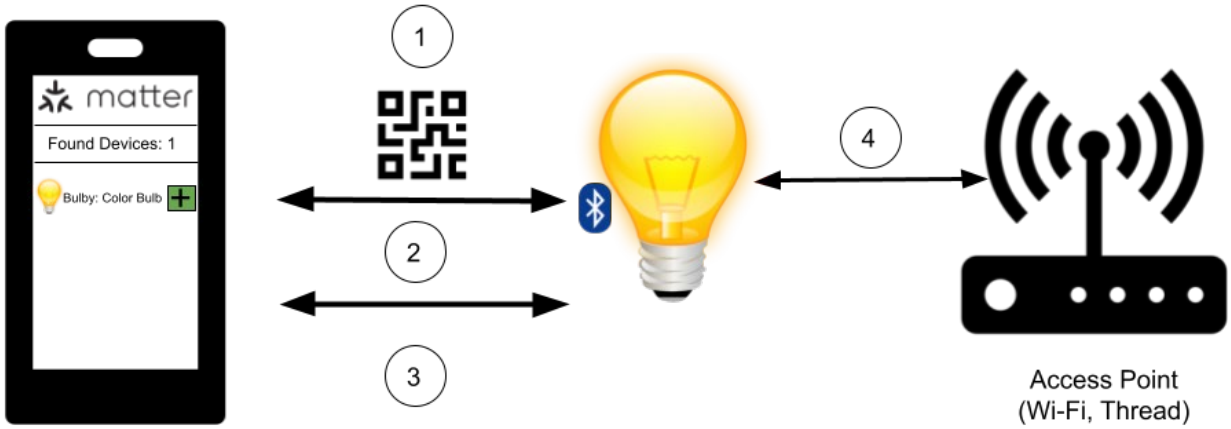

Figure 7: Matter Commissioning

In Figure X above the commissioning process ① is started by first scanning the QR code on the device or its packaging, this is usually done with an app on a smartphone referred to in Matter as a commissioner. The QR code contains among other things the product ID, the vendor ID and a passcode that is used to establish the initial secure connection with the device. This passcode can be manually entered by the user and even spoken into a smart speaker.

Next the commissioner will search for and connect to the device ②. This connection can be done over BLE, a temporary Wi-Fi connection to the device (SoftAP), or directly via IP. In this step the commissioner will check the device attestation certificate (DAC) and the certification declaration (CD) to establish that the device is authentic and has been tested and certified. The commissioner and the device will then establish a strong encrypted communication path with which to configure the device.

In ③ the commissioner configures the device with credentials for the Wi-Fi network as well as operational credentials that the device will use to connect to devices on the same fabric. Additionally, this step will often be used to set up access control lists so that the device will allow connections from other devices and applications.

Finally, in ④ the device will connect to the access point and begin normal operations.

The commissioning of a device can be done several times to add the device to new fabrics and to add administrators of the device.

4. Distributed Compliance Ledger

The Distributed Compliance Ledger (DCL) is a cryptographically secure, distributed network that allows device manufacturers (vendors), official test houses and Alliance certification centers to publish public information about a given device. Based on blockchain technology, it allows participants to update relevant device information that is cryptographically signed.

Connectivity Standards Alliance's (Alliance's) Distributed Compliance Ledger (DCL) is an industry-wide initiative to provide a cryptographically secure, distributed ledger of certified IoT devices and their roots of trust, without one company or an entity in charge of the ledger. By using an underlying permissioned blockchain framework, the DCL benefits from the following properties:

- Multi-node network that is run by the Alliance member companies
- Individually signed transactions using pre-approved keys
- Non-repudiation
- Distribution of data in different geographical locations
- Consensus protocol to ensure majority approval
- Public reads with available cryptographic proofs attached
- Transparency and auditability

4.1. Architecture

Conceptually, the DCL is a network of authorized "Validator Nodes" that comprise the consensus pool of the underlying blockchain framework. It works on the basis of a "Permissioned Ledger" where all write transactions are individually validated by the distributed validator nodes using the enrolled public keys. The CSA provides a public facing "Node" for full public access (Read Only). CSA members run their own nodes in their protected networks.

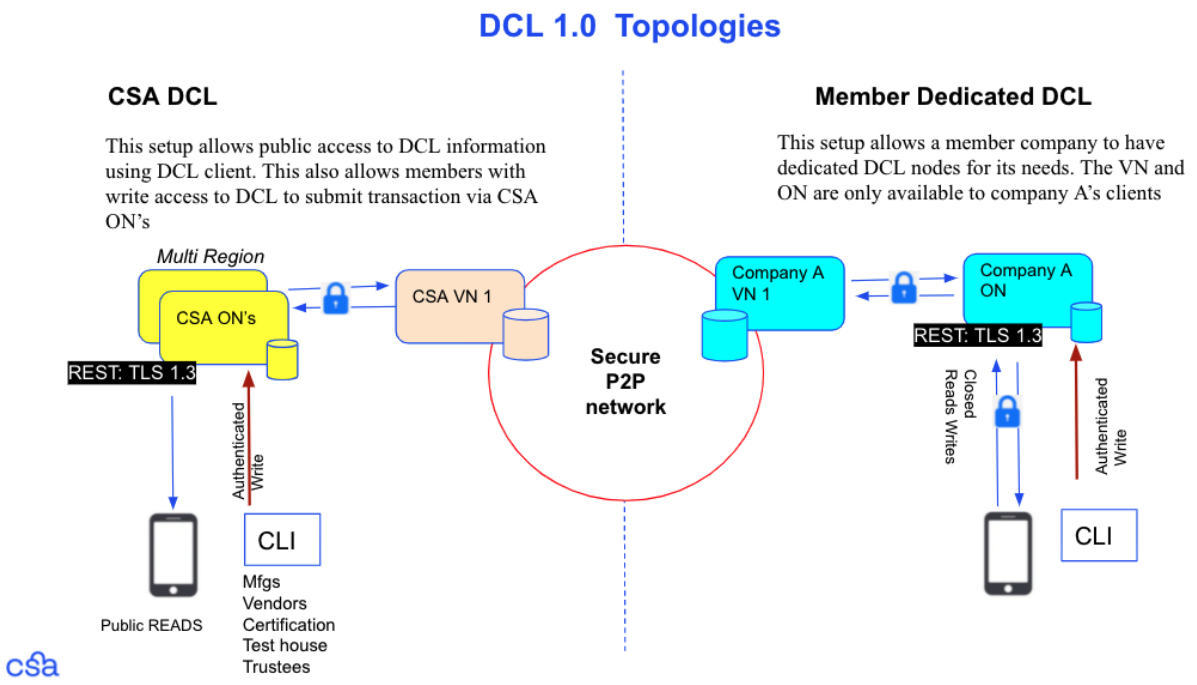

Figure 8: DCL Architecture

4.2. DCL Schema

DCL contains the following standard information, securely uploaded by individual members and validated using their public keys to provide nonrepudiation.

- **Vendor Info**, for example, company name, legal and preferred name, URL, etc.
- **Models and Model Software Versions:** models are identified by a unique combination of `VID` (vendor ID) and `PID` (product ID).
- **Model Certification:** DCL can be used as a source of information if certain Model Software versions are certified by a Certification Center. Certifications may be revoked.
- **PAA Certificates:** DCL can distribute authorized X509 Certificates (PAA and non-root).
- **Auxiliary Information:** DCL has an array of required auxiliary transactions:
  - **Validator Node** transactions define the current set of VNs participating in consensus.
  - **Account** transactions contain a role and a public key for every user wanting to write to the ledger and must be signed by the private key associated with the account.

- **Upgrade** transactions contain information about scheduled and completed updates of the DCL software.

4.3. DCL Nodes

The DCL network consists of a peer-to-peer network of Validator Nodes that communicate with each other using a secure and authenticated protocol.

- **Validator Node (VN)** is a full node that participates in the consensus protocol utilizing an authorized cryptographic key. A VN is responsible for validating new records. In order to run a VN, an organization must have an approved account with a Node Admin role - Access to VNs should be restricted by means of Sentry nodes and private networks. A better way to accept requests from the user is via Observer nodes.

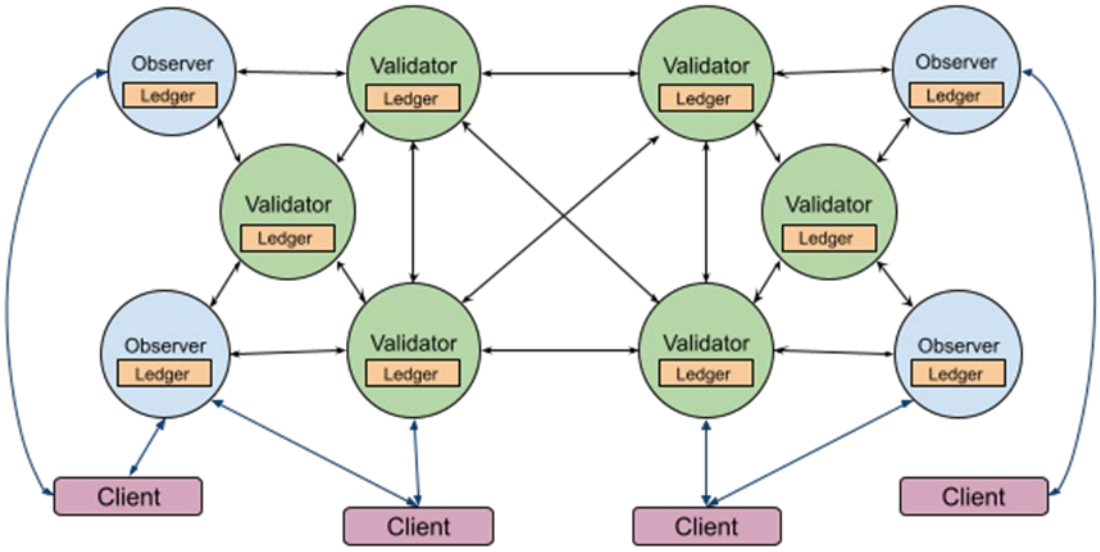

Figure 9: DCL Network

- **Observer Node (ON)** is a full node that does not participate in the consensus. ONs do not require an account with a Node Admin role to be created and member companies can govern their access to their ONs.

4.3.1.PKI Overview (PAA/PAI)

Matter specifies a three tier certificate chain for device attestation certificates to ensure device authenticity during commissioning. The top-level root is called “Product Attestation Authority” or PAA.

Each PAA can have one or more Intermediate known as ``Product Attestation Intermediate" or PAI. The PAI is responsible for issuing a unique device attestation certificate or DAC to each Matter device. The authorized pool of PAAs is entered in DCL so that they can be downloaded using the public DCL read interface to all Matter commissioners.

The Matter specification allows CSA members to operate their device PKI chain as long as the PAA and PAI adhere to the Matter Certificate Policy. Therefore, due care and best practice should be followed in setting up both a root and intermediate certificate authority and certain requirements must be met according to the Matter certificate policy for establishing and running a PAA/PAI. Several public PKI providers who are also CSA members can also provide PKI as a service by hosting PAA and PAI chains on behalf of Matter device manufacturers.

4.4. Running a DCL node

DCL consists of a pool of validator nodes that provide consensus based cryptographic integrity checks on the DCL entries. This provides blockchain level security and integrity for all the device data that is entered by authorized companies. Since DCL is a permissioned ledger, CSA and trustees of the DCL authorize each Validator node individually to become part of the DCL consensus pool.

CSA members can also run Observer Nodes which do not participate in the DCL consensus pool and therefore do not need to be authorized individually. CSA members can run Observer Nodes so that they have a full database of certified Matter devices in their network to enable individual company's use cases.

5. Security

Matter takes a comprehensive approach to security that involves securely onboarding the device to the Matter Fabric, encrypted mutually authenticated connections between devices, fine-grained access control between devices and users, and a software update mechanism for issuing patches and new firmware to devices.

5.1. Secure Communications

The set of protocols used in Matter assures that all unicast communications are secured (encrypted and integrity checks), authenticated and provide builtin replay protection.

There are two methods of establishing a secure session in Matter and their use depends on if the device is being commissioned or is in normal operation. Both methods set up a shared symmetric session key for fast data encryption.

Passcode-Authenticated Session Establishment (PASE) is used when a device is being commissioned. PASE uses a password or passcode communicated through an out-of-band channel such as Bluetooth Low Energy (BLE), scanning a QR code, or Near Field Communication (NFC). Once both the device and the commissioner have the passcode they use it to calculate a common symmetric key on both sides. This key is then used to establish AES-CCM session keys to provide confidentiality and integrity of communications between devices. PASE is used to set up connections that establish operational credentials between devices.

Certificate-Authenticated Session Establishment (CASE) is used once a device is configured. It uses operational credentials in the form of certificates that are established at the time the device is

commissioned. These operational credentials are used to authenticate both ends of the communication and set up shared session keys. These shared symmetric session keys are used by the devices to encrypt traffic using the AES-CCM cipher suite.

5.2. Replay Prevention

Matter nodes use sessions as a way to quickly setup previously authenticated channels between two nodes. Sessions provide a mechanism to pause and resume a connection between devices as long as the session keys remain valid. Sessions also provide the Matter protocol a way to keep track of messages as they traverse two nodes. A randomly initialized message counter is established with each session that serves a two-fold purpose. First, it acts as an encryption nonce to ensure that every message is encrypted in a unique manner. Second, it acts as a replay and duplicate message detection mechanism.

Message duplication can be caused by network latency and errors where the sender did not receive an acknowledgement. Unhandled duplicate messages present problems if control messages are sent multiple times and can change the state of the device in unpredictable ways. Threat actors, while they are incapable of decrypting the message, can intercept encrypted messages and re-send them or "re-play" them. This can cause an unintended state in a device. A common example of this is a legitimate unlock command that is captured by an attacker and resent to a door lock later allowing the attacker to gain physical access. Matter prevents these issues by maintaining a history window of message counts from a sender to determine if the message is a duplicate. Duplicate messages are dropped by devices before they reach the application layer.

5.3. Secure Group Communications

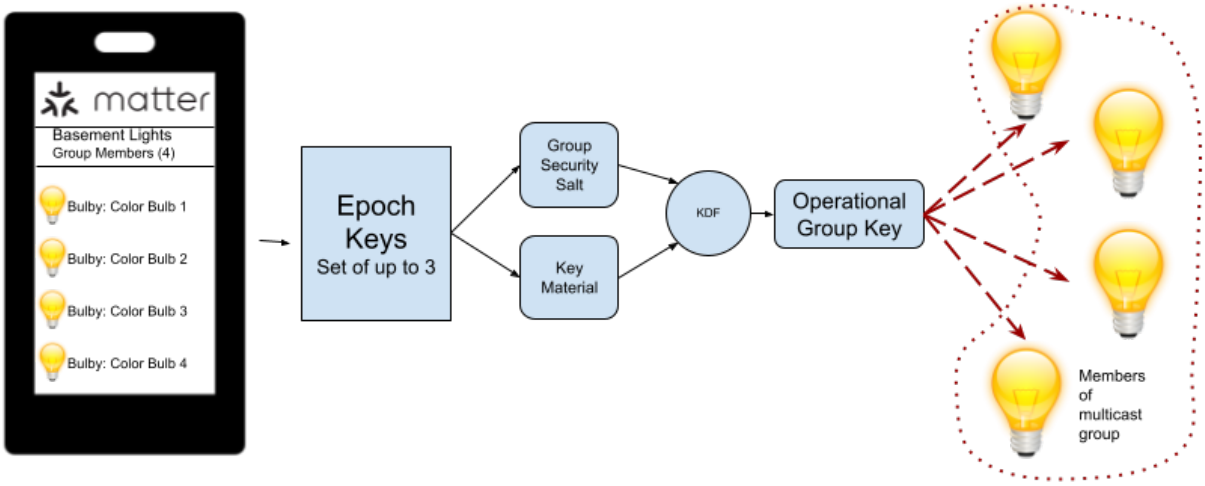

Figure 10: Secure Group Communications

Group communications in Matter take advantage of multicast networking. Multicast allows a single sender to send a message to a specific destination group and it is received by several devices simultaneously, relying on the network to replicate the message. An example use-case of this in the smart home is to send an "ON/OFF" command to a group of lights. Using multicast, a single command can be sent to a large group of devices instead of having to send individual unicast messages to each

device. This is both more efficient and faster than unicast as it requires fewer messages from the sender and can be done in parallel.

Because secure group communications is a one-to-many relationship i.e one sender and many recipients, securing this communication must be done in a way that provides three things:

1. All devices can prove that they are members of the associated group
2. All messages are encrypted and confidential.
3. Messages can only be decrypted by other members of the group

To accomplish the above goals Matter distributes through an Administrator Node a set of 1-3 keys to each device in the group called epoch keys. Devices use these epoch keys to derive an operational key that is used to encrypt and decrypt messages for the group.

5.4. Access Control

Access control provides fine grained access to devices. For example, your front door lock can be set up to allow one family member's phone (i.e., a parent) to manage who can change access settings on the lock (what other devices can view and perform actions on the lock), and another family member's phone (i.e., child) to operate (lock/unlock) the door.

Access control lists consist of the following attributes:

- Fabric Index: ID scoped to the associated Fabric
- Privilege Level: View, Proxy View, Operate, Manage, and Administer
- Targets: List of clusters (data model elements e.g DoorLock, temperature sensor)
- Subjects: List of sources of an action to which the ACL applies, often this will be the Node ID
- Authentication Mode: Type of secure channel (PASE, CASE)

An example of an ACL on a Matter device is shown below. The first entry gives "Administrator" privilege to a Matter node with ID "0xAABD65DF76230b54"over CASE authentication.

The second entry allows all devices on Fabric 1 to have "View" privilege on all target devices endpoint 1.

The last entry provides "Manage" privilege to subject 0x0000000000000001 on End Point 1 and Endpoint 3 of cluster ID 0x0000_0202.

ACL: [

{FABRIC: 1, PRIVILEGE: ADMIN, AUTHMODE: CASE, SUBJECTS: [0XAABD65DF76230B54], TARGETS: []},

{FABRIC: 1, PRIVILEGE: VIEW, AUTHMODE: CASE, SUBJECTS: [], TARGETS: [ENDPOINT: 1]},

{FABRIC: 1, PRIVILEGE: MANAGE, AUTHMODE: GROUP, SUBJECTS: [0X0000000000000001], TARGETS: [{ENDPOINT: 1}, {ENDPOINT: 3, CLUSTER: 0X0000_0202}]}

]

5.5. Software Update

All devices will need to be updated at some point in their life cycle either to provide new functionality or to patch a vulnerability. Matter mandates that all Matter certified devices support over-the-air (OTA) software update. Software images must be signed by the vendor using a private key dedicated to signing images. Firmware images are transferred over a Matter specific Bulk Data Exchange (BDX) protocol that treats images as a collection of bytes with metadata. BDX is modeled after TFTP and can use either TCP or UDP as an underlying transport.

The software update process in Matter involves two nodes:

- OTA Requestor is any node that requires updating of software.
- OTA Provider is a Node that fulfills software update requests. The OTA Provider downloads the image from the vendor and stores a copy or alternatively can act as a proxy through which the OTA Requestor can download the firmware image.

Software updates must be checked for authenticity and integrity by the device prior to being installed. Additionally, devices will not install version numbers that are lower than their current running firmware version to prevent downgrade attacks.

6. Administration

6.1. Operational PKI

Devices are permitted access to a Matter Fabric through the provisioning of a Node Operational Certificate, NOC. The NOC uniquely identifies a particular node within the scope of a particular Fabric. This certificate is also used to establish secure communication channels with other nodes belonging to the same Fabric. NOCs may be directly issued by a Trusted Root Certificate Authority or an Intermediate Certificate Authority and are provisioned during Matter commissioning. A Matter device will have exactly one NOC for every Fabric that it belongs to.

6.2. Configuring Access Control

Matter provides a flexible fine grained access control list for participating devices. The rule-based ACL defines no implicit access by default. Therefore, it works on the principle of implicit “deny” unless an explicit rule defined on a device grants access to a requesting device, further fine grained to a given endpoint (service) on the target device.

An access list is created on a device during its commissioning so that when it is put on the network, it has proper security in place. During the commissioning phase, the access control module on a device grants implicit “Administrative” access to a Commissioner over PASE session which entails creating a secure channel using SPAKE2+ protocol between the device and commissioner using a passcode for that device. Further updates to Access Control lists can be made over the network on a CASE session as long as the source device has “Administrator privilege” defined in the target device ACL.

6.3. Fabric Management

There are two roles that are necessary to fully manage a Fabric. The commissioner role is used to provision new nodes into the Fabric and provide them with operational credentials that chain up to an operational root of trust. The administrator role is used to change access control lists within their respective Fabrics. Additionally, administrators can remove a Fabric that is not directly under their control. This is an important feature of Matter as it allows a device owner to remove a Fabric from the device that they may no longer control or a Fabric they no longer wish to control the device.

6.4. Group Management

It is expected that groups of devices will change. For example, you may wish to add or remove a light from a group. Adding a device is as simple as commissioning a new device and adding it to the group along with the required group operational key so that it can decrypt signals sent to the multicast address of the group. Removing a device from the group requires a re-key of the remaining devices in the group with new operational keys.

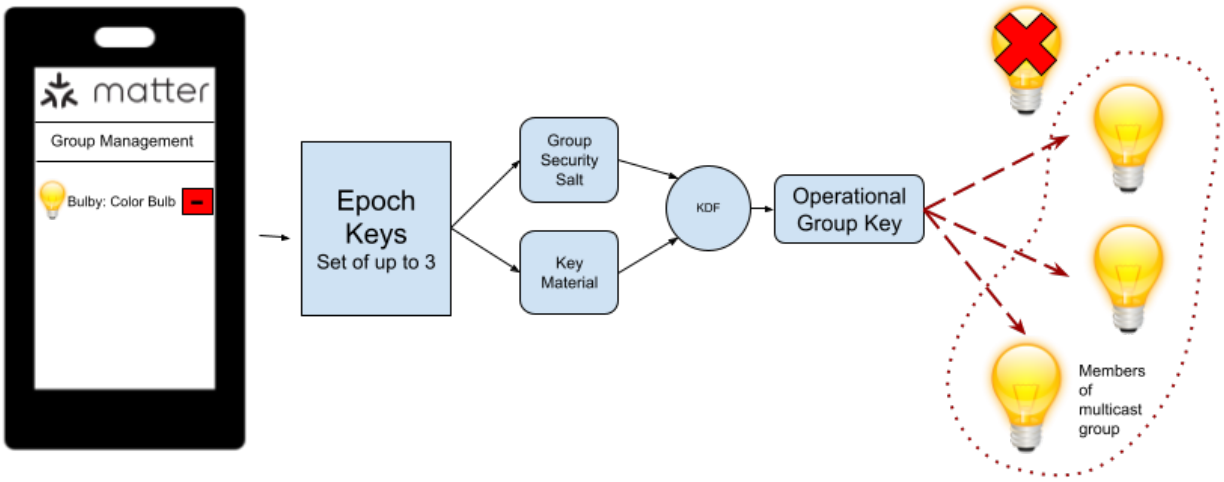

Figure 11: Group Management

6.5. Software Update

Software update announcements and notifications are automatic and happen in the background. To assure that the update does not disrupt the user, downloading and applying updates should be done after obtaining user consent. User consent can be stored for future use and is an optional process in Matter.

6.6. Multi-Admin

Matter has standardized simultaneous command and control of a device by multiple ecosystems. This key feature allows consumers to "commission" i.e. securely add control of their Matter devices by multiple ecosystems ensuring they are not locked into using a single vendor or ecosystem. For example, a door lock can be opened with multiple apps through multiple ecosystems if provided the initial owner intends to set it up in such a way.

The sequence diagram below depicts the steps initial Ecosystem (Eco A) takes to pair an already commissioned "bulb" to add it to the second ecosystem (Eco B). The process involves the user (Alice) instructing the device (Bulb) to go into commissioning mode using a new onboarding passcode and go into discovery mode. The commissioning window is open for a specified time in seconds. Alice conveys the new PIN to Bob who is connecting to the bulb using a different ecosystem. Bob discovers the bulb using "dns-sd" and completes commissioning using the new passcode.

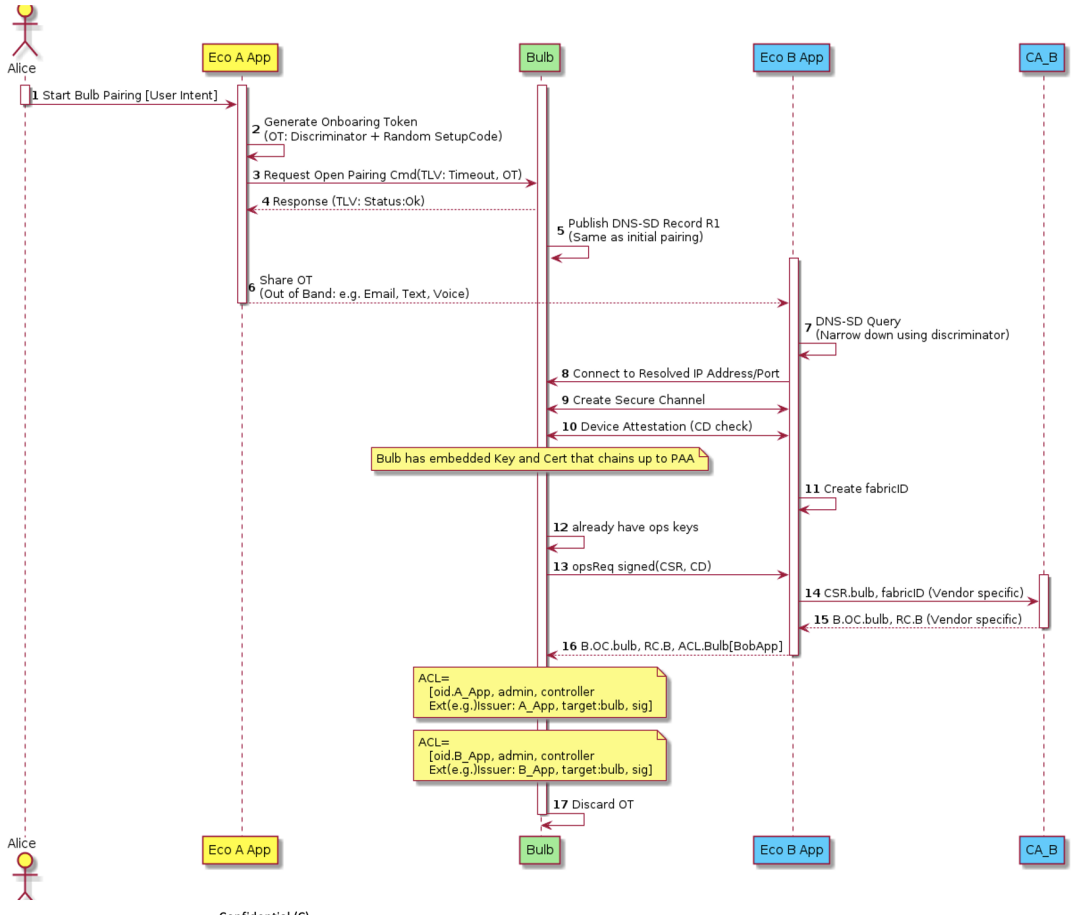

Figure 12: Multi-Admin Sequence

7. Matter and Operators

Matter represents a paradigm shift in traditional smart home management. This new specification simplifies the way applications and devices communicate by utilizing IP, the language of the Internet. It decouples the networking stack from the application stack, allowing for flexibility in use cases that require differing bandwidth and energy constraints. Matter is also open source and provides full access to specifications and reference SDKs. Given the unique relationship that Cable operators have as Internet and local connectivity providers to the smart home, they have a great opportunity to both add value to and derive value from Matter.

As wireless connectivity providers, Cable operators have a goal of ensuring their customer's devices seamlessly and consistently connect to their access points. Fundamentally, all that is needed to support the basic connectivity requirements of Matter is to provide Wi-Fi Access Points, Thread Border Routers, and IPv6 and multicast DNS support. Most operators already support many of these requirements and simply need to add Thread capable radios to their access points. Ensuring all Matter supported wireless transports, Wi-Fi and Thread, are present in customer's homes will reduce the potential for failed device connections and user confusion. This in turn will drive down customer service calls and improve user satisfaction. Cable operators should also consider certifying their access points as Matter certified Wi-Fi access points and Thread Border Routers. These additional device certifications are currently being defined and will be available in a future release of Matter.

As Internet Service Providers, Cable operators have a responsibility to help safeguard their customer's home networks and the broader Internet as a whole. The tools that allow this oversight often rely on the ability to uniquely identify network devices and to understand the applications they expose or interact with. In the evolving world of Internet security and privacy practices that encourage use of randomized MAC addresses and encrypted communication channels, the ability to acquire this information is becoming increasingly difficult. With Matter, Cable operators can directly query devices to uniquely identify them and understand what type of device they are. Additional helpful information such as a device's software version, hardware version, manufacturer, product ID, and serial number are also made available. Devices can be further vetted against the Matter Distributed Compliance Ledger to verify their authenticity and certification status. All of this represents a suite of tools that can be used to uniquely identify devices on a customer's network, understand the expected behavior of those devices, and provide a rich set of data to direct customers to appropriate support resources.

As customer premise equipment providers, Cable operators are well positioned to add value to Matter by proxying Matter communications from the Internet to a customer's local network. Matter is designed as a local network communication stack and does not define how the smart home may be interacted with when a user is not at home. Control of Matter devices while away from a user's local network will require routing messages through a locally connected device. Cable companies offer a range of devices including Wi-Fi routers, cable modems, and set-top-boxes that can act as proxies to relay these messages. Having a locally connected device that is always listening and addressable from the Internet provides Cable operators the ability to address this existing gap. Further value can be added by simplifying the device onboarding process. Cable's scale, access to the home, and ability to forge business to business relationships place it in a unique position to improve this area. Through arrangements with retailers, device onboarding information could be transferred to a customer's router at time of purchase so that the onboarding process automatically happens in the background when the device is first powered on. These are just a few of many potential value propositions the Cable industry can provide to Matter.

Matter is poised to transform the way that users, device manufacturers, and ecosystem providers approach the smart home market. Users will benefit from a recognizable brand that simplifies the purchasing process and ensures interoperability. Device manufacturers will be able to offer a reduced set of SKUs and take advantage of open-source SDKs. Ecosystem providers will be able to seamlessly connect to a range of devices with improved onboarding flows and enhanced security. With all these benefits in place, Cable operators must embrace Matter in order to meet their customer's evolving expectations and usher in the next generation of the smart home.

Abbreviations

AP	access point
BDX	Bulk Data Exchange
BLE	Bluetooth Low Energy
CASE	Certificate Authenticated Session Establishment
CPE	Customer Premise Equipment
CSA	Connectivity Standards Alliance
DAC	Device Attestation Certificate
DCL	Distributed Compliance Ledger
DNS	Domain Name System
DNS-SD	DNS - Service Discovery
IP	Internet Protocol
IPv6	Internet Protocol version 6
KDF	Key Derivation Function
LAN	local area network
NOC	Node Operational Certificate
PAN	personal area network
PASE	Passcode Authenticated Session Establishment
PID	Product Identifier
PKI	Public Key Infrastructure
ON	Observer Node
OTA	Over-the-Air
SDK	Software Development Kit
SKU	Stock Keeping Unit
TRCA	Trusted Root Certificate Authority
VID	Vendor Identifier
VN	Validation Node
ZCL	Zigbee Cluster Library

Bibliography & References

Greenberg, A. (2015, July 21). Hackers Remotely Kill a Jeep on the Highway—With Me in It. Wired. Retrieved from https://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/

Kolias, C., Kambourakis, G., Stavrou, A., & Voas, J. (2017). DDoS in the IoT: Mirai and Other Botnets. *Computer*, *50*(7), 80–84. https://doi.org/10.1109/MC.2017.201

Herzberg, B., Bekerman, D., & Zeitman, I. (2016, October 26). Breaking Down Mirai: An IoT DDOS Botnet Analysis. In *Incapsula.com*. Retrieved from https://www.incapsula.com/blog/malware-analysis-mirai-ddos-botnet.html

