matter

The Matter Standard: Implementing Improved Security and Connectivity for the Smart Home

Infineon

www.infineon.com/connectedhome

The smart home continues to evolve in available functions and complexity as several different connectivity protocols from numerous suppliers target a variety of products for use in smart homes. However, many consumers (71% according to incontrol) acknowledge fear of their personal information being stolen while using smart home products. At the same time, ease of use for user-installed products has often been elusive.

Working collectively, many leading suppliers and potential suppliers have taken the next step to provide improved interoperability to smart home products using the Internet Protocol (IP). Called Matter standard, the key to the success of these efforts is security. This white paper addresses the need for universal Smart Home standards with integral security, explains how Matter addresses both and identifies Infineon's role in making both connectivity and security for smart homes a reality.

True Connectivity and the Need for Security

While the idea of home automation using network technology has existed since the mid 1970's and perhaps earlier, the modern smart home with interconnected products to improve the home owner's quality of life required the internet and, specifically, the Internet of Things (IoT) to become a reality. However, today's smart home is usually still complicated, not appropriately secure and, in many cases, incompatible. The user buys something, brings it home and finds that each device works differently. Sometimes the setup is very complicated. Then, after it is setup, the new device does not work with already installed smart home products, such as a smart phone, thermostat, security system and others. Sometimes incompatibility is due to lack of standards. However, for the smart home, the cause can also be too many standards (Connectivity Standards Alliance, Z-Wave, Thread, Wi-Fi, Bluetooth and more), that all try to address smart home interconnectivity. Often, the standards do not enable devices on different networks to talk to each other.

The current issues and lack of plug and play capability have made smart home progress slower than it could have been. Early adopters expressing concerns and discussing compatibility issues they discovered tended to be heard and delayed others' adaption plans. In addition, all of the different branding initiatives make the current situation very confusing.

Lack of system security is also among the issues in existing smart home systems. Any data stored in or transported by the network including private information and even bank accounts could be accessible to an intruder. Distributed denial of service and other types of attacks, including web cameras spying on the homeowner, are also major concerns.

According to some projections, in spite of the issues and concerns, by the end of 2021, 25 billion IoT smart devices could be in use, including smart light bulbs, air quality monitors, doorbells, washing machines and refrigerators. This makes the need for network compatibility and addressing security issues more important than ever.

Matter – the interoperable, secure connectivity standard for the future of the smart home

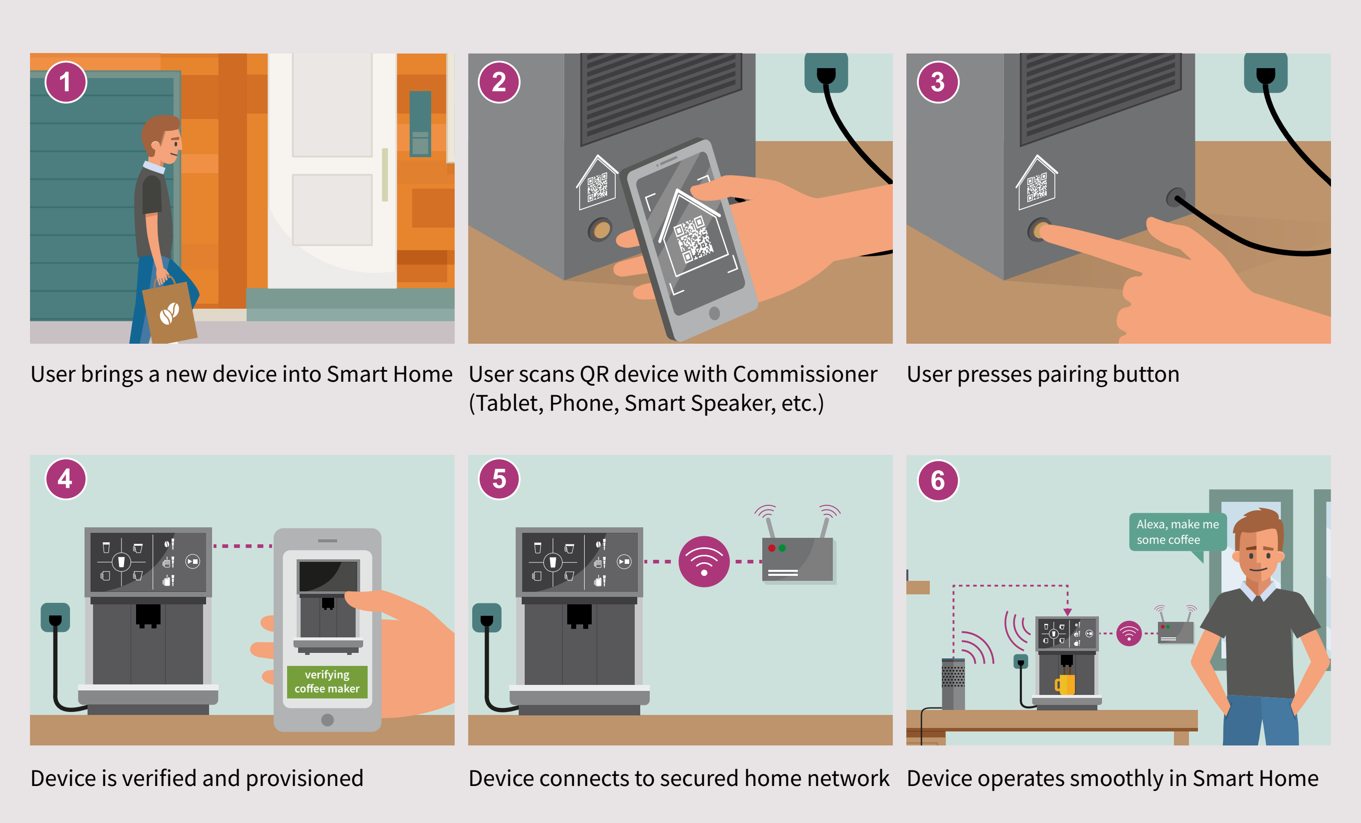
To bring the many diverse networking factions together and solve interconnectivity as well as security issues, the Connectivity Standards Alliance (formerly Zigbee Alliance) created the Matter Working Group. The Working Group consists of experts from more than 170 major players, including names like Apple, Amazon, Google, Infineon, Johnson Controls, Schneider Electric, LG Electronics and others. These companies include those who make the ecosystems, devices, and chips working together to create and open standards for smart homes. In addition to the usual list of definitions that occur in any standard, one of the first items that Matter addresses is the mapping of terminology so all developers use the same terms for critical network items.

The goal of Matter is that if a user buys two Matter-certified devices, they will actually work together. By meeting this goal, consumers will have confidence in their purchases and manufacturers will not have to integrate required capabilities separately for each of the major and even minor players. The process is intended to enable innovation by letting innovators add new aspects on top of the architecture as devices communicate in a standard manner. Since the need exists for security to be common to all of these devices, a common set of security mechanisms should be used everywhere. Matter strives to provide a great user experience while maintaining affordability and security. Here is an example.

Typical Matter User Experience

In a typical Matter scenario, a user can bring a new product home (refer to Figure 1) and use a smartphone to scan the Quick Response (QR) code attached to the back of the product. This QR code, which is unique to that device, establishes the identity of the device and enables secure communication. Pressing a pairing button on the device tells it to start installation. With this prompt, the smartphone establishes a secured connection to the device using the cryptographic information included in its scanned QR code, verifies the device to determine that it really is Matter certified, determines what kind of device it is (in this case a coffeemaker) and then sends all the necessary information (Wi-Fi passwords and more) needed for the coffeemaker to join the network. This includes providing a new set of credentials for the coffeemaker so it can communicate securely with anything else in the smart home. The coffeemaker can now securely communicate with a smart speaker so the smart speaker can initiate a specific brewing process and be an accepted and well-secured member of the smart home.

In summary, this is a simple 6-step process:



User brings a new device into Smart Home

User scans QR device with Commissioner (Tablet, Phone, Smart Speaker, etc.)

User presses pairing button

Device is verified and provisioned

Device connects to secured home network

Device operates smoothly in Smart Home

Figure 1: The desired connectivity process for smart home devices.

Matter Architecture: Based on IP

The Matter communication stack is based on the Internet Protocol (IP). Everything, except the pairing/commissioning process, runs over IP. Since IP works over many different types of networks, devices do not have to be concerned with how a message gets to a smart speaker or to anywhere else. The message is simply sent to an IP address and it reaches the intended destination. This enables interoperability even if, for example, a smart speaker does not understand Thread but a window sensor does and sends a message warning of a break-in. The message still gets through to all the intended recipients, even if it is a multicast message. A multicast message may go to other recipients in the home as well, which could take further action like sounding a siren alarm, turning on lights, or calling the police.

Another benefit of IP communication is the ubiquity of the IP protocol. As shown in Figure 2, lower-layer protocols that can be used with IP include: Digital Subscriber Line (DSL), Data Over Cable Service Interface Specification (DOCSIS), cellular, Ethernet, Wi-Fi, Thread, IEEE 802.15.4, IPv6 for Bluetooth Low Energy (BLE) and BLE. New ones are defined often, continuously expanding communications options.

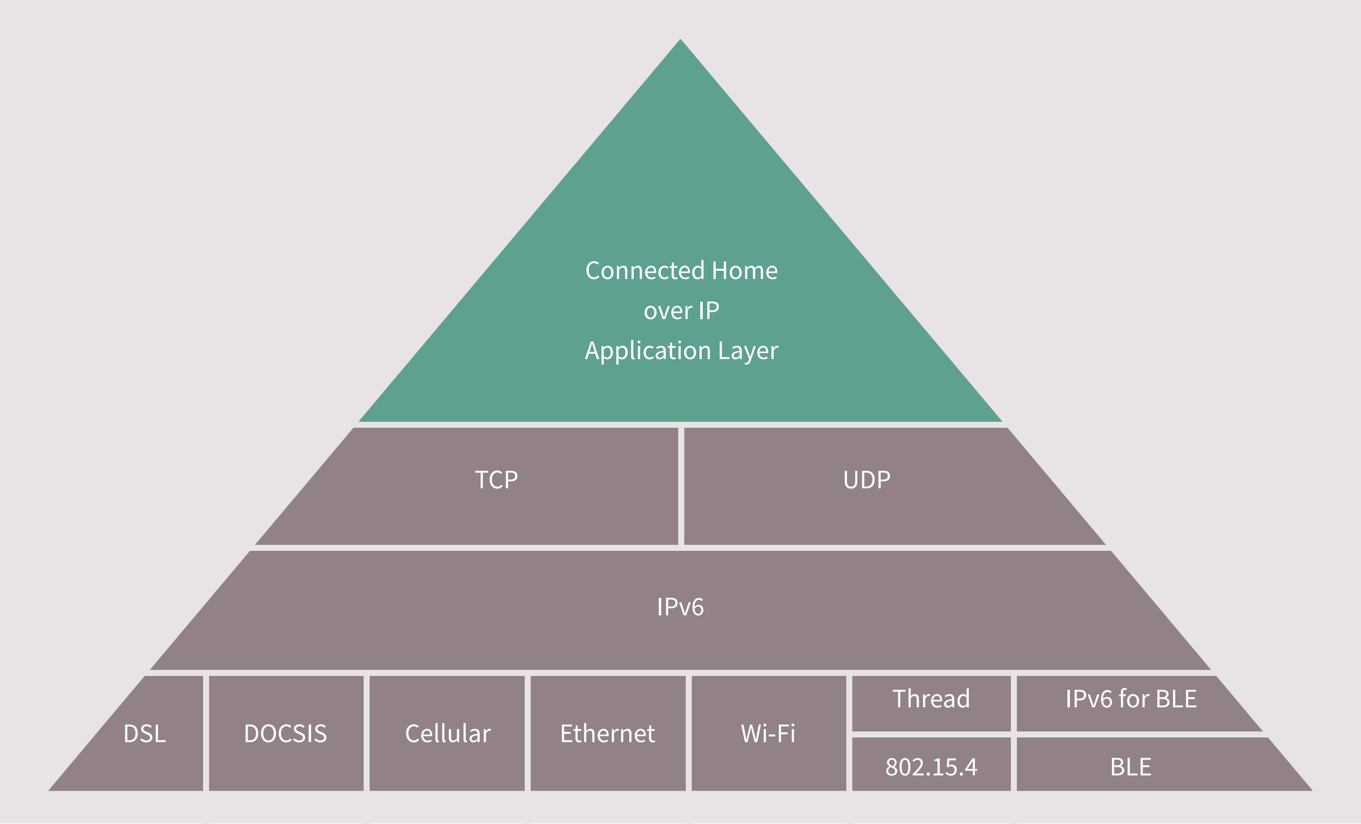


Figure 2: The application and network stack in the Matter specification and IPv6-based communication protocol.

Inside Matter

Figure 3 shows the layered nature of the Matter protocol stack.

The top (Application) layer of the protocol stack is where all the information about a particular type of device resides. If it is a temperature sensor, this is where the temperature reading would be defined. This Application layer contains different profiles for different types of devices, for example a window break sensor, thermostat, door lock, coffee maker and more. Commands such as turn on or turn off instructions occur in this layer.

Next comes the Data Model structure. This is how application data is structured. It is basically the nouns, their definition. Then the interaction model layer defines the verbs, the actions taken by the Data Model layer items, such as change the light dimming level or subscribe to light dimming level so if anything changes it will be updated. The Action Framing layer describes the bits and bytes of how those actions are put on the network. The Security level provides encryption, signing and authentication as well as confidentiality and protection for all the layers. Then the message gets framed and routed over the network across IP. Transport Management makes sure that the sent message gets delivered. If it did not get through, it is resent until it is acknowledged.

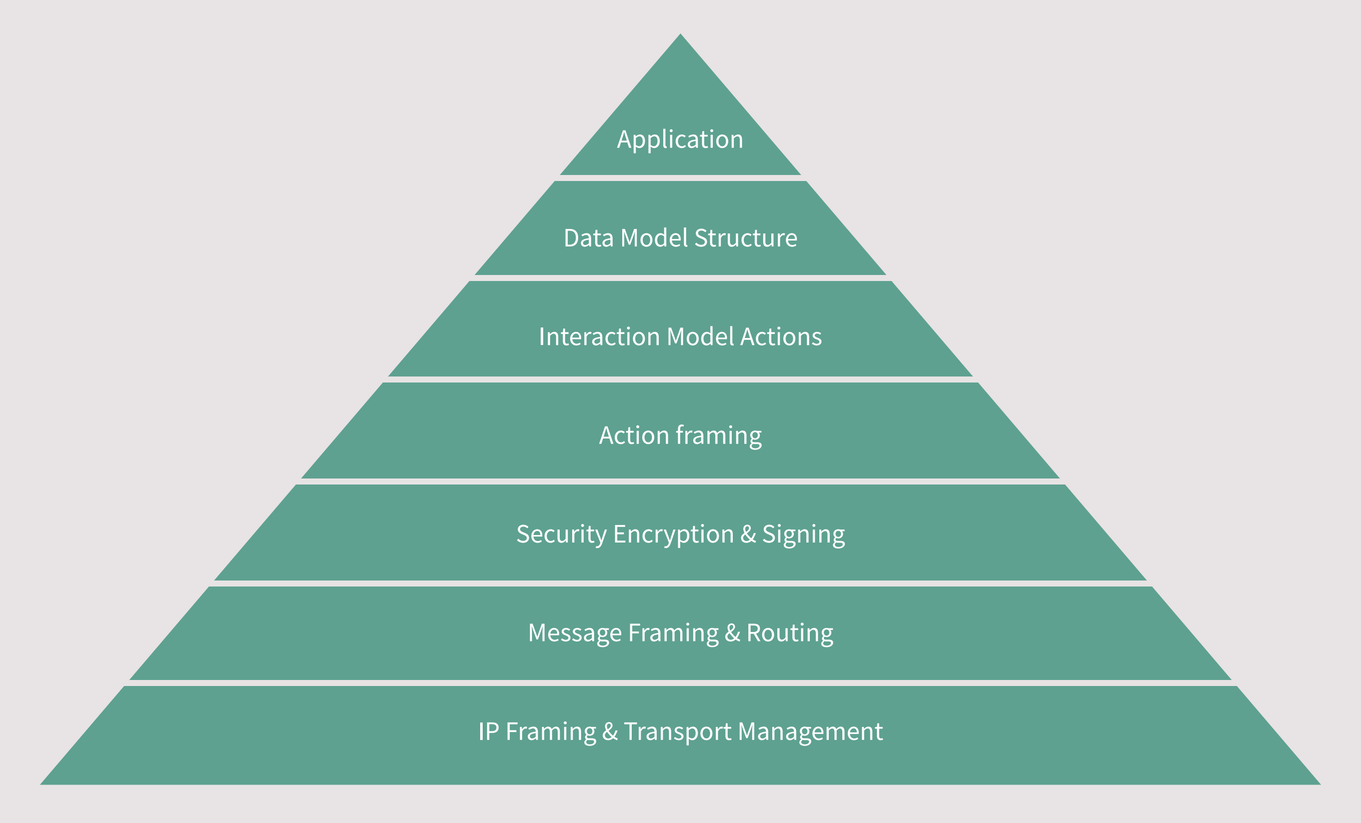

Application
Data Model Structure
Interaction Model Actions
Action framing
Security Encryption & Signing
Message Framing & Routing
IP Framing & Transport Management

Figure 3: The layered architecture in Matter specification separates and encapsulates different responsibilities.

Matter Implementation

The Matter protocol stack and its open source reference implementation are designed to work with any type of application in the smart home. Instead of being limited to just lights or a smart TV, Matter can work with any application and run on almost any hardware or operating system. The open source Matter software library is designed to be highly portable even working on the lowest level devices with minimal overhead. The stack and implementation are open to anyone royalty free and are based on the market tested technologies known to the contributors. Apple, Amazon, Google and many others have contributed their code and concepts and experience after more than 10 years in the smart home market to make this approach work well for device makers and consumers.

Certification

The process of bringing a device into a smart home depends on an open certification program. To reliably deliver on the promise of smart home interoperability, products will have to be certified through a testing regimen to use the Matter branding. Similar approaches have worked well in solving interoperability problems in other domains, such as HDTV. Creating reliable interoperability will enable smart homes to make the transition from early adopters who are willing and persistent in dealing with early issues, to middle and late adopters whose capabilities and persistence are much lower and who do not know the difference between a Connectivity Standards Alliance network and a Z-Wave network and do not want to find out. They just want to remove a product from a box, plug it in and have it work. But there are a few extra steps (behind the scenes) to really make this happen that will be discussed later in the how it works section.

Matter Security

In a smart home, security is essential to prevent hackers from initiating denial of service (DoS) attacks like Mirai and others. Consumers are aware of the potential for these unauthorized access attacks and realize that smart home devices have had security problems. These concerns are a significant impediment to widespread consumer adoption.

To address security concerns, Matter includes several protection features. The first step is knowing that a real device, from a qualified supplier and not a fake, is being connected to the network. Since consumers often use wireless networks in the smart home, protection from eavesdropping is required. Protection from manipulation of data over the air or on the device itself is another threat. Access control prevents unauthorized access to security cameras and other sensitive devices. Finally, firmware updates are essential to keep systems well-secured so these need to be securely installed while avoiding illegal updates with malware.

Security measures in Matter to protect against these threats include:

- Device attestation
- Mutual authentication of all parties
- Secured communication among devices using secured protocols
- Secured storage, especially of private keys
- Secured firmware updates
- Device integrity to prevent and detect compromise

Infineon Security and Connectivity for Matter

Infineon's leadership in Matter is based on our years of experience providing easy to implement and strong security measures for IoT security as a leading supplier of hardware needed to build secured IoT products.

Hardware-based security is especially valuable for Matter. Instead of using passwords, Matter uses cryptographic keys for authorization and device security. With this approach, a user does not have to remember and enter or periodically change a password. Instead, cryptographic keys stored in hardware security provide a more secure approach for keeping the key out of unauthorized hands. This is much better from a security standpoint. Since the key is a large random number, it is nearly impossible to determine what it is.

Hardware security products include cryptographic functions and unique identity credentials that are provisioned into a highly protected trust anchor, using a secured and Common Criteria certified manufacturing facility. These hardware security chips make Matter work. They include PSOC (Programmable System On Chip)and OPTIGA™ family products that enable smaller, more power efficient and less expensive designs for use in very small IoT applications, yet still provide secured identity credential and cryptographic functions required for IoT networks including random number generators, encryption/decryption, signing and verification. These chips are suitable for use in controller, network or nodes for IoT devices. Each unit can come preloaded with key pair and certificate and additional key pairs can be loaded when the device is commissioned into the Matter network.

Not only is Infineon a leader in every Matter security group, it is a thought leader across Matter initiating many innovative ideas and proposals to address security issues including contributed code to the open source implementation, text to the specifications and capabilities beyond security. These capabilities include communication ICs, IoT processors and memory products that add to the well-established security capability and provide complete system solutions.

Working with several software suppliers and partners, including open source and researchers, has added to the capabilities and ease of implementing numerous features Infineon offers. Working with Matter is one more example of these cooperative efforts, since Matter software runs on top of Infineon hardware.

How Matter Security Works in a Smart Home

In the manufacturing process, several items are added to the device that are special and unique to each one. For example, every device has its own public/private key and a device attestation certificate (DAC). This is installed into the device during manufacturing process as well as a certification declaration (CD) signed by Connectivity Standards Alliance certifying that devices of this model are certified with a specific firmware version and compliant with the Matter specification, a verifier, and a QR code unique to that device (either printed on the device or included with it). When the product arrives in the home (as stated before) the QR code is scanned to commission the device. A numeric version of the code is included with the QR code for those situations where the commissioner does not have a camera so the user can speak or type the QR code. Then the pairing button is pushed putting the device into the commissioning mode. With this process initiated by the user, several tasks are performed automatically.

When a device is brought into a network and commissioning is trifggered, the device starts beaconing, sending out messages over the Bluetooth network and potentially over Wi-Fi, as well acknowledging its presence, need to be added to the network and its ID information. The Commissioner listens on these networks and looks for the device that it scanned and establishes a secure connection with the device. A setup code or pass code, a unique long random number, assigned in the factory when the device was manufactured is included in the QR code that is only used when the product is commissioned. The verifier and setup code are used in a Password-Based Key Derivation Function (PBKDF).

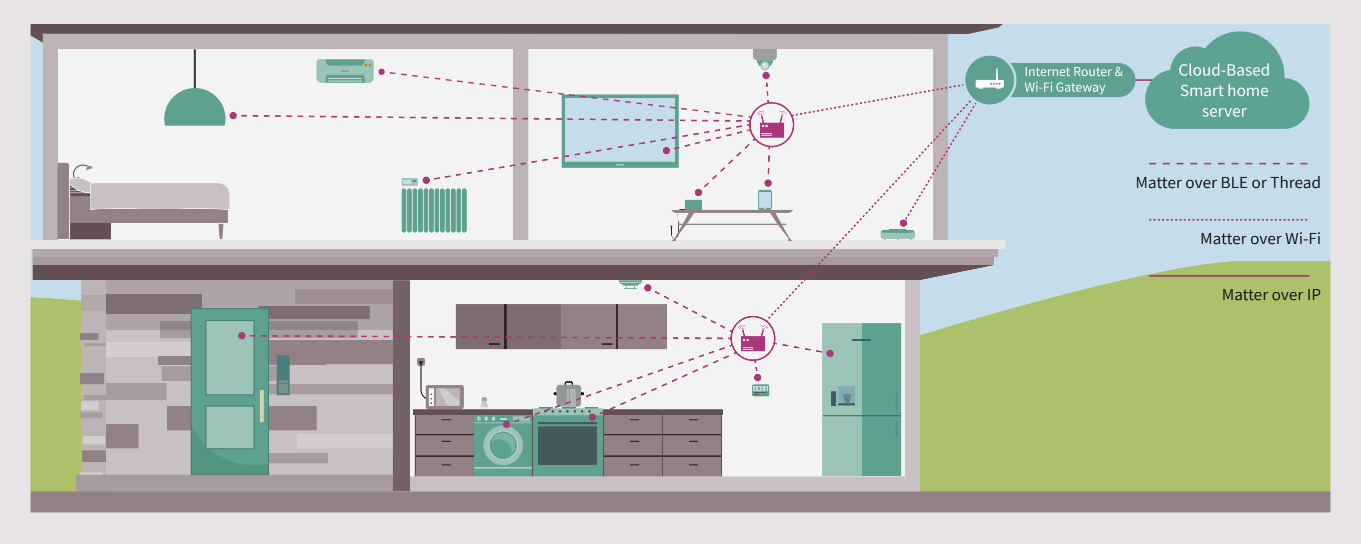


Figure 4: Commissioning a typical Matter network.

In this manner, Matter uses fairly short secrets (about 27 bits) to create a long 256-bit secret that will be used to secure the communications between the Commissioner and the device or Commissionee. Now, using the long random number, the two of them can have a secured communications channel and the Commissioner can authenticate the device to make sure it is authentic for commissioning and Matter certified. This is performed by a handshake with the device, obtaining the certification declaration (the digitally signed token from Connectivity Standards Alliance), verifying the signature, obtaining a copy of the device attestation certificate from the device and verifying its link to Connectivity Standards Alliance. This provides confirmation that not only is this type of product linked to Matter but that this specific device is authentic and not a fake. The unique key pair has the Connectivity Standards Alliance as the trusted root. Now that the device is authenticated, the Commissioner asks the device to make a new key pair and send a certification request from the new key pair. When this is done, the Commissioner creates or obtains a new certificate for the new device and sends it with a node identifier back to the device.

At this point, the device has an identity, its Operational Credential, that is used to authenticate with any other device on the home network. In fact, there are two public key infrastructure (PKI) identifiers, a device attestation PKI rooted in Connectivity Standards Alliance and then when the device comes into the home, a new operational certificate from a different PKI is now used on the network. Since the new name, certificate, and key pair comes from the operational PKI used in the home, everything else in the home will recognize this identity and trust it, too.

So far, all of this activity has occurred over a commissioning network that can be Wi-Fi, Bluetooth or others but is not the user's home network per se. Now it is time to bring the device into the smart home network. To connect to the smart home network, the necessary information must be sent to the device: the network name (Service Set Identifier, SSID) and password for a Wi-Fi network or similar values for Thread. Similar to all the other steps that happen automatically after the Commissioning button is pressed, this information is sent automatically from the Commissioner to the device without requiring the user to do anything more.

In addition to the activities already discussed, many more occur automatically behind the scene. For example, an access control list (ACL) is installed on the device, controlling which nodes are allowed to communicate with the device and the operations they are allowed to perform. For example, for a lightbulb, the ACL might say "if any of these specified light switches sends a command (on, off or dim), it should be obeyed. But only one or two Admin nodes can reconfigure the bulb.

The Commissioner could also tell the light switch that a new lightbulb has been added to the room and it should now send commands to it in addition to how it previously worked. All of the steps for properly configuring a new device in an existing network are performed automatically by the Commissioner. Once this is done, the light switch communicates with the lightbulb without further involvement from the Commissioner. Other devices' interaction with the new device are also defined and potentially linked together in groups, such as a security system, where a multicast message is sent to specific members of that group.

There are additional security steps that Matter performs as well. For example, if the user decides to sell a device, like a security camera, it can be factory reset (decommissioned) so no access information or credentials for the network goes with it. Also, secure firmware upgrades are an additional Matter feature.

Implementing Smart Home Security

Tool development for Matter has been ongoing since mid-2020 with test events occurring as well. The official launch of the 1.0 specification will occur and formal certification will occur in 2021. Even if some of these activities are delayed, as they often are with comprehensive standards, the time for developers to get involved is now.
For more Matter information, go to:

- https://buildwithmatter.com/
- Implementation Source Code for Matter: https://github.com/project-chip/connectedhomeip
- Infineon's Matter activities: www.infineon.com/connectedhome

Conclusion

With the development of the Matter specification by Connectivity Standards Alliance and 100s of key suppliers, the smart home is poised to provide unprecedented connectivity and security and overcome the concerns of yet-to-be-convinced buyers. With open source standards for connectivity and security and Infineon Technologies' products to implement them, smart home products and other smart (factory, city and more) concepts can be easily and securely added to users' networks to improve their lives.

www.infineon.com

Published by
Infineon Technologies AG
81726 Munich, Germany

Date: 05/2021

Please note!
This Document is for information purposes only and any information given herein shall in no event be regarded as a warranty, guarantee or description of any functionality, conditions and/or quality of our products or any suitability for a particular purpose. With regard to the technical specifications of our products, we kindly ask you to refer to the relevant product data sheets provided by us. Our customers and their technical departments are required to evaluate the suitability of our products for the intended application.

We reserve the right to change this document and/or the information given herein at any time.

Additional information
For further information on technologies, our products, the application of our products, delivery terms and conditions and/or prices, please contact your nearest Infineon Technologies office (www.infineon.com).

Warnings
Due to technical requirements, our products may contain dangerous substances. For information on the types in question, please contact your nearest Infineon Technologies office.

Except as otherwise explicitly approved by us in a written document signed by authorized representatives of Infineon Technologies, our products may not be used in any life-endangering applications, including but not limited to medical, nuclear, military, life-critical or any other applications where a failure of the product or any consequences of the use thereof can result in personal injury.