3. The Matter communication standard

The communication standard Matter, originally developed under the name Project Connected Home over IP (CHIP), was designed by CSA (2021) in cooperation with leading IoT manufacturers for use in the smart home environment. The project was announced in 2019 and development started in 2020. The implementation-first approach was followed during the development process, so that the reference implementation was provided before the technical specifications were published (Heater, 2019). The final version of the reference implementation became available as open source and the certification process started in October 2022 (CSA N.D.a).

The primary focus in the development of the Matter standard was to solve the interoperability problems in the field of IoT smart home networks. Furthermore, security has been pursued by Matter as a fundamental principle (CSA, 2022a). It is also intended to simplify the usability of the devices and to support the development process of new devices.

3.1 Structure of Matter

The structure of Matter is shown in Figure 4.

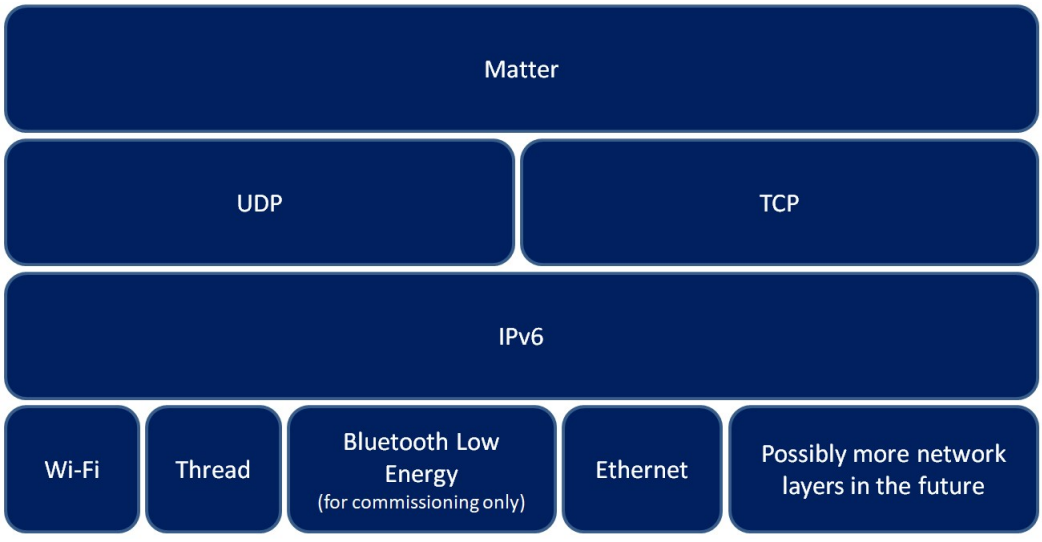

Figure 4: Structure of Matter (revised according CSA, 2022a)

At the lowest level, the Matter communication standard is based on data transmission via Wi-Fi, Thread, BLE and Ethernet. It should be noted that BLE is only used to authorise new devices as it allows for a simple pairing process (CSA, 2022b). While the transmission of data

is realised via Ethernet for wired connections, there is a choice between Wi-Fi and Thread for wireless connections.

All participating standards on the network layer support IPv6, which ensures the basis of Matter interoperability. The network communication protocols TCP and UDP, which are typical for IP-based stacks, are used on the transport layer (Kumar & Rai, 2012). In this way, connection-oriented as well as connectionless applications can be realised. Figure 5 shows the splitting of the architecture into seven components.

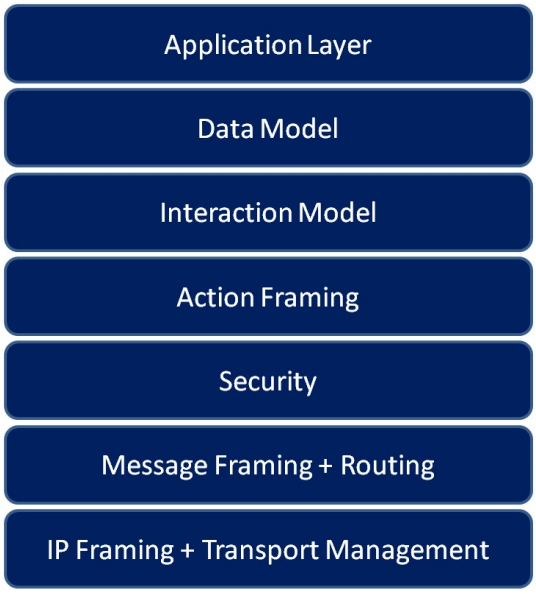

Figure 5: Architecture of the Matter framework (revised according CSA, 2023)

The application layer represents the highest level of logic within the framework. Simple functions such as commands to switch on or off and colour characteristics of a light bulb are implemented on this level. The data model describes the structure through which the data of an application can be accessed. The interaction model determines which commands can be used to interact with the device based on the defined elements of the data model. This includes, for example, how data can be read or changed on the device. The action framing layer transforms the incoming interaction commands into a binary format for transmission. Security mechanisms are used on the security layer to encrypt and authenticate the data for the sender and recipient. The data is then organised into packets and provided with routing information and headers. Finally, the packets are forwarded to the transport management layer, where the IP management of the data takes place.

3.2 Network topology by Matter

A central goal of Matter is to improve interoperability in the smart home area. Due to the compatibility of several communication standards, a Matter network can take on different topologies, with the primary topology being a mesh network. Figure 6 shows various possible applications of a Matter network.

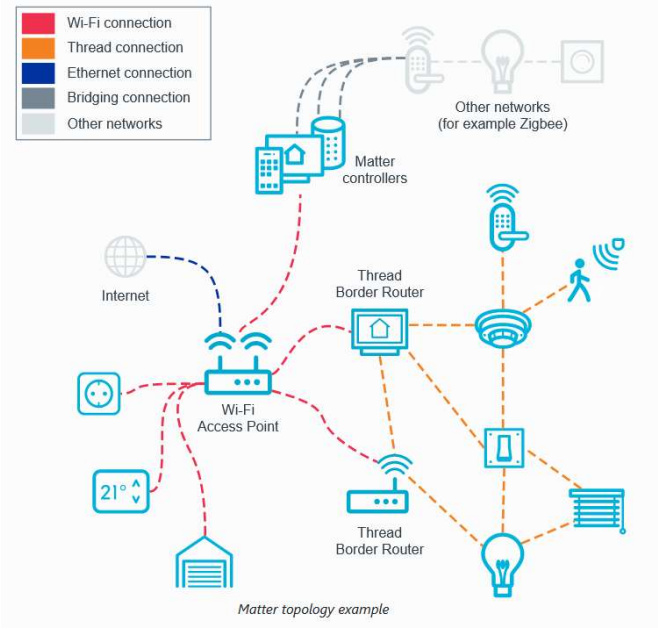

Figure 6: Matter network topology (Nordic, 2023)

The centre of the network is the connection between the Wi-Fi router and control devices (CSA, 2021). Smartphones, tablets or smart speakers are suitable as control devices, which enable the user to interact with the network and the devices connected to it. BLE is used to integrate new devices into the network, as this allows for a simple initial connection (Asadullah & Ullah, 2017). If the Bluetooth connection is successful, the device is implemented in the Wi-Fi network through secure transmission of the access information. Finally, the Bluetooth connection will be disconnected and is no longer used for further communication between the devices (CSA, 2022c).

The implementation of Thread devices in the Matter network is made possible by border routers, which connect the subnets and realise the translation between Wi-Fi and Thread. In addition, Matter Bridge Devices enable the embedding of other communication standards such as Z-Wave or Zigbee (CSA, 2023). The Matter Bridge functions in the same way as a border router does when embedding threads in a Matter network.

3.3 Security principles and considerations by Matter

The goal when developing Matter was to implement the security of the standard using five principles (CSA, 2022a). A representation of these principles can be found in Table 1.

Table 1: Matter security principles (CSA, 2022 a)

Principle	Explanation
Comprehensive	Layered approach
Strong	Well-tested standard cryptographic algorithms such as ECC NIST P256 & AES-CCM-128
Easy	Improve ease of use not decrease it
Resilient	Protect, Detect and Recover
Agile	With crypto-flexibility in mind to address new developments and threats.

The first principle builds on the comprehensive, layered structure of Matter. The security mechanisms are not dependent on the protocols on which Matter is based. All functions relevant to the security of communication are provided in the open source framework (CSA, 2022c). This should enable device manufacturers to build on the reference implementations without having to consider additional security mechanisms. However, it should be questioned to what extent the implementation of communication standards for which vulnerabilities are known can be securely transferred to Matter without posing a security risk.

The second principle relates to the use of proven and strong cryptographic algorithms and encryption techniques. As with BLE and Thread, AES is also used in CCM mode to maintain secrecy, with Matter using 128-bit keys. Furthermore, the hash method SHA-256 is used to support integrity, which is currently classified as secure (NIST, 2022). The setup of a session is based on the use of x.509 certificates, which are used to authorise a device to participate in the network (CSA, 2022a). Device certificates can be checked using the Distributed Compliance Ledger (DCL) technology (CSA, 2022c). DCL provides a blockchain-based platform on which manufacturers can upload product information for their products without the risk of the data being manipulated (Higginbotham, 2021). This data includes the device ID, the manufacturer ID and meta data, such as references to a device's update sources. This is to ensure that anyone can verify the integrity and certification of a device.

Another principle of Matter is that it is easy to use for both manufacturers and users. Through freely accessible reference implementations, manufacturers can adopt the security measures

designed and specified by Matter (CSA, 2022b). According to Matter, when it comes to security, users do not have to consider the security aspect at all when implementing and using their devices due to the security functions implemented in the standard (CSA, 2022a).

The resilience of Matter represents the fourth principle. In order to realise this, there are often several ways to carry out an action. An example of this can be found in establishing a session. If a session already exists but is unexpectedly interrupted, Matter first attempts to re-establish the connection using an abbreviated recovery protocol to minimise disruption to communication (CSA, 2022a). However, if this attempt fails, the session is re-established using the full protocol. Precautions against the most common DoS attacks and checking firmware integrity are mentioned as further resilience measures (CSA, 2022b).

Finally, the fifth principle deals with the agility of the standard. Due to the modular structure of Matter, it should be possible in the future to exchange the cryptographic methods and protocols used without having to completely revise the present specification. This should allow Matter to be flexibly adapted to future developments in the field of cryptography and quickly close new security threats (CSA, 2022a).

3.4 Identity attribution of Matter devices

Device identity supports security in already existing mechanisms, since before a device is added to a new network, its origin and firmware can be checked (CSA, 2022c). Each device's identity is assured by a chain of certificates, which is shown in Figure 7.

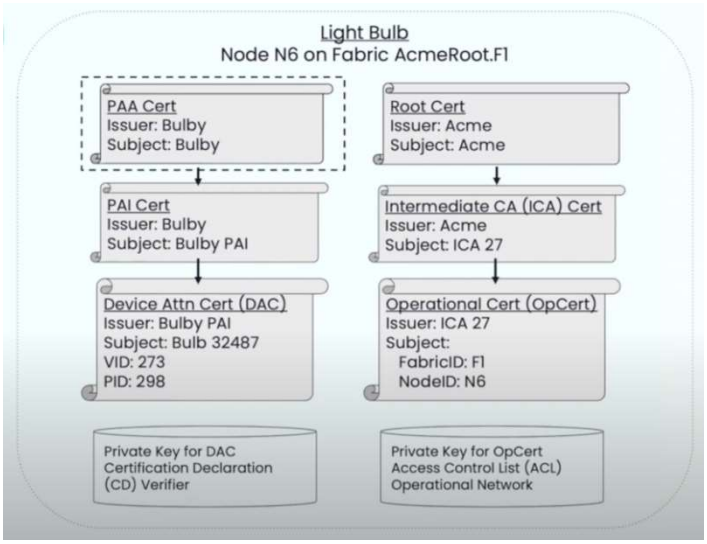

Figure 7: Certificate chain example (CSA, 2022b)

Each device has a Device Attestation Certificate (DAC) that contains information such as device ID, vendor ID, device name, public key, and a reference to a parent certificate to verify the authenticity of the DAC. This chain goes all the way to the root certificate, also known as the Product Attestation Authority (PAA) certificate, which is held by the manufacturer and serves as a source of trust. This infrastructure is similar to the public key infrastructure used in the web environment by Internet browsers and by Matter to authenticate devices and ensures that only certified devices can access the network (Clutterbuck, 2010).

In the factory state, the private key for checking the certificate, a declaration of the certificate and a verification of the declaration are also stored on the device. This declaration confirms that the device has been tested and certified with the specified vendor ID and device ID. If the device is successfully integrated into the network, an additional certificate is created that describes the identity in the network. This operational certificate contains a unique designation of the device in the network, the network designation, the public key of the device and a reference to the parent certificate. Similarly, the chain of certificates goes back to the root certificate, which is trusted by all devices in the network. The original DAC is preserved so that the device can be added to another network in the future (CSA, 2022b).

References

Asadullah, M. & Ullah, K. (2017) 'Smart home automation system using Bluetooth technology', *International Conference on Innovations in Electrical Engineering and Computational Technologies.* Karachi, Pakistan, 05-07 April. IEEE. 1-6. Available from: https://ieeexplore.ieee.org/abstract/document/7916544 [Accessed 26 April 2023].

Clutterbuck, P. (2010) 'Spyware Security Management via a Public Key Infrastructure for Client-Side Web Communicating Applications', *10th IEEE International Conference on Computer and Information Technology.* Bradford, United Kingdom, 29 June - 01 July. IEEE. 859-864. Available from: https://ieeexplore.ieee.org/abstract/document/5578087 [Accessed 04 May 2023].

CSA (2021) The Future of IoT is Now: Project Connected Home over IP. Available from: https://www.youtube.com/watch?v=Dqy6ASRgWmI [Accessed 05 April 2023].

CSA (2022a) Matter Security and Privacy Fundamentals. Available from: CSA_Matter_Security_WP.docx (csa-iot.org) [Accessed 06 April 2023].

CSA (2022b) Matter Security and Privacy: A Deep Dive with the Experts – Connectivity Standards Alliance. Available from: https://www.youtube.com/watch?v=Q4jhK-IBKuI [Accessed 04 April 2023].

CSA (2022c) Matter Specification Version 1.0. Available from: https://csa-iot.org/wp-content/uploads/2022/11/22-27349-001_Matter-1.0-Core-Specification.pdf [Accessed 25 April 2023].

CSA (2023) Matter. Available from: https://github.com/project-chip/connectedhomeip#readme [Accessed 06 April 2023].

CSA (N.D.a) The Foundation for Connected Thing. Available from: https://csa-iot.org/all-solutions/matter/ [Accessed 16 March 2023].

Heater, B. (2019) Amazon, Apple, Google and Zigbee join forces for an open smart home standard. *Techcrunch*. Available from: https://techcrunch.com/2019/12/18/amazon-apple-google-and-zigbee-join-forces-for-an-open-smart-home-standard/?guccounter=1&guce_referrer=aHR0cHM6Ly9kZS53aWtpcGVkaWEub3JnLw&guce_referrer_sig=AQAAAMNaRe4lUPYn2zI24yRH3mZgqsLrkCDg6qKJHDeXfK0yKf3RuTrFkyFU3ceAwSgk_npWNH9bUd7FRVZr9xhDRYA3sIX5pFTUo81KeLx1t8faL1Za2sLRx7N6toYV0WKGrvZGvR-WvyAy6J9U7PNikJH1kgJt3ehPIxVXAGV9YRrx [Accessed 06 April 2023].

Higginbotham, S. (2021) Forget Cryptocurrencies and NFTs—Securing Devices Is the Future of Blockchain Technology. *IEEEE Spectrum*. Available from: https://spectrum.ieee.org/forget-cryptocurrencies-and-nftssecuring-devices-is-the-future-of-blockchain-technology [Accessed 04 May 2023].

Kumar, S. & Rai, S. (2012) Survey on transport layer protocols: TCP & UDP. *International Journal of Computer Applications 46*(7): 20-25. Available from: https://citeseerx.ist.psu.edu/document?repid=rep1&type=pdf&doi=ac50f6aeb6a5372f85cf05dab2a229b97a084555 [Accessed 25 April 2023].

NIST (2022) NIST Transitioning Away from SHA-1 for All Applications. Available from: https://csrc.nist.gov/news/2022/nist-transitioning-away-from-sha-1-for-all-apps [Accessed 03 May 2023].

Nordic (2023) Matter network overview. Available from: https://developer.nordicsemi.com/nRF_Connect_SDK/doc/2.1.2/nrf/ug_matter_overview_network_topologies.html [Accessed 31 July 2023].