Matter Security and Privacy Fundamentals

March 2022

Notice and Disclaimer

Revision History

Revision	Date	Comments
1.0	3/18/2022	Release version

Table of Contents

Document Authors

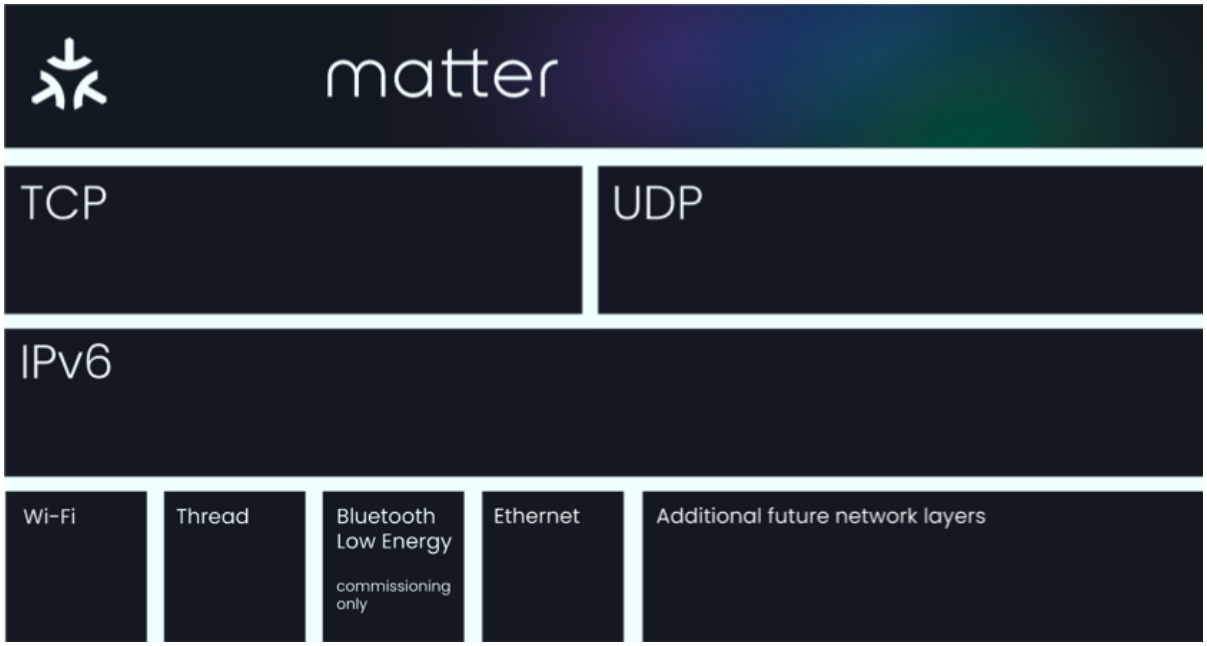
Naama Bak, NXP
Thomas Ben, NXP
Steve Hanna, Infineon
Sujata Neidig, NXP
Raj Rajagopalan, Resideo
Oscar Sanchez, Infineon
Marc Vauclair, NXP

Introduction to Matter

Matter[1] is the foundation for connected things, an industry-unifying standard to deliver reliable, seamless and secure connectivity. Built on IP (Internet Protocol), Matter enables communication across smart home devices and ecosystems over a specific set of IP-based networking technologies, starting with Thread, Wi-Fi and Ethernet. Built on market-proven technologies contributed by companies across the industry and developed in a collaborative and open source methodology with an implementation-first approach, Matter is simplifying development for manufacturers and increasing compatibility and ease-of-use for consumers.

As the IoT connects more and more devices and systems, risks of cyber attacks increase; driving concern and hesitation by users and limiting adoption. To address this obstacle, Matter was created with security and privacy as key design tenets.

[1] www.buildwithmatter.com



Security concepts for the Smart Home

The concept of “Smart Home” is no longer something that we treat as science fiction but is now a reality of our everyday lives. From smart lights and ovens to washing machines and smart locks, today there are more than 13 billion interconnected digital and electronic devices[2] in operation globally. These network-connected devices, which are known as “Smart Devices”, are typically interconnected to a smartphone or tablet via technologies like Wi-Fi, Thread or Bluetooth to control, automate and optimize functions like temperature, lighting, security, safety or entertainment within the smart home.

As these smart home solutions continue to evolve, so are cyberattacks on smart home systems and devices. And, the risks are significant:

- Product malfunction through remote control
- DDoS (Distributed Denial of Service) attacks
- Data and privacy breaches
- Theft of intellectual property
- Potential for harm to humans

The good news is that best practices have been developed for mobile, PC and cloud that can be leveraged for IoT with:

- Proven Device Identity / Device Authenticity
- Secure Communication
- Access Control

[2] Juniper Research Report on IoT

One of the challenges in smart homes is deployment of security best practices at scale, such as how to provision an identity securely into a smart home device, how to securely control a device remotely, and how to securely do a software update and device reset, etc. Key aspects to address while deploying security in smart homes include:

1. Manufacturing: While in the factory or in the supply chain, devices may be subject to a variety of attacks such as malicious code injection.
2. Operations: Once in the field, devices are susceptible to a wide range of remote attacks and, in some cases, physical attacks.
3. Maintenance: There is limited security without a mechanism for maintenance over time, the software update process for devices should be secure to prevent loading of unauthorized software.

To mitigate these challenges, the following cybersecurity practices are often used:

- Secure Manufacturing: This encompasses provisioning of device identity and firmware securely at trusted facilities.
- Secure Communications and Operations: Communications need to be encrypted and authenticated to protect against remote and local attacks once installed. Secured communications can be unicast, from one device to another, or multicast, from one device to many. Protecting against attacks means ensuring the data arrives at its intended destination in a confidential, authenticated and unaltered form.
- Over-the-air Updates: Secure updates to installed devices in operation should be supported, including firmware and credentials updates to add protections against newer attack threats or to push new features. A secure upgrade process helps prevent loading of malware or unauthorized firmware.
- Security Regulations: IoT regulatory initiatives for security and privacy differ from country to country and continue to evolve. Smart Devices should be designed with future-proofing capabilities to be able to support these changes.

Matter Security Principles

Matter addresses security as a foundational tenet. Matter functional security has been defined to embody the five following properties:

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.

Comprehensive - Providing comprehensive security means implementing it with a layered approach with authentication and attestation for commissioning, protecting every message and securing over-the-air firmware updates.

Matter functional security is self-contained; it does not rely on the security of the communication technologies on top of which Matter runs. For example, Matter security does not rely on the integrity and confidentiality of wireless protocols like Wi-Fi. Matter features (application clusters and device libraries) defined on top of the Matter core specification use the functional security defined by the Matter core specification. Matter comes with reference implementations with all functional security available in a self-contained package: there is no need to add functional security features on top. Matter is defined in an open-source framework easing the adherence to the specification and the interoperability across different manufacturers and different device types.

Strong - Matter employs a variety of state-of-the-art security techniques.

Matter relies on one strong cryptographic suite based on well-tested, standard and recognized cryptographic primitives. AES in CCM mode is used for confidentiality and integrity with 128 bit keys. AES in CTR mode is used for protecting identifiers to preserve privacy. SHA-256 is used for integrity and ECC with the “secp256r1” curve for digital signatures and key exchanges, standard key derivation schemes and truly random number generators.

On top of this cryptosuite, Matter relies on standard passcode based session and certificate based establishment protocols to establish secure sessions for onboarding, attestation, and operation.

In addition, Matter adopts the very strong concept of device attestation that implements the core concept that a Matter device cannot join a Matter fabric unless proven genuine.

To guarantee a uniform and compliant ecosystem, Matter also extends the CSA Distributed Compliance Ledger technology[3] to Matter devices to provide a world-wide interoperable platform that allows Matter commissioner devices to check on whether the other Matter devices have been Matter certified[4].

Easy to use - Matter security is designed to make smart devices easier for device makers to implement and for consumers to use.

The Matter core specification comes with examples and test vectors for each functional security aspect. Matter reference implementations available to all manufacturers in open source on a GitHub repository come with a modularly defined software implementation of Matter functional security. This implementation offers examples of alternative integrations of hardware security modules (HSM). The Matter security assets are well defined (keys, secrets…). Customers buying Matter devices will not have to think about security: it is just there.

Resilient - Matter security is resilient - it's designed to protect, detect and recover.

Matter provides more than one way to perform certain operations. For example, a secure session establishment attempts a shorter secure resumption protocol first for efficiency, but if the resumption cannot be performed, or fails, the full protocol is utilized.

Matter does not rely on the underlying security of the communications medium used between Matter devices. Several mechanisms have been built in the Matter definition to prevent the most common denial of service attacks. The Matter protocols themselves have been defined to be resilient even when sleeping devices are involved or when using group communications; for example, Matter introduces a sophisticated message counter mechanism to offer this resilience. Further, Matter recommends firmware integrity attestation which provides a measured boot and attested firmware measurements.

Agile - With crypto-flexibility in mind, Matter can address new developments and threats.

Matter core specification abstracts all cryptographic primitives to give room for future Matter specification versions that would adopt new cryptographic primitives without having to change the whole specification. The modular design of the protocols also gives room to replace some of them by new protocols should future security risk and threats analysis show that Matter should be upgraded to utilize new protocols.

[3] https://spectrum.ieee.org/forget-cryptocurrencies-and-nftssecuring-devices-is-the-future-of-blockchain-technology

[4] https://staceyoniot.com/project-chip-embraces-a-timeline-and-the-blockchain

Matter Privacy Principles

Data Privacy is an important requirement of all systems that handle personal information and Matter is no exception. Data Privacy is embedded in Matter and is a core concept for all protocols and interaction methods.

Since the advent of General Data Protection Regulation (GDPR[5]) and subsequent privacy regulations in other parts of the world, the following principles are generally recognized as the common subset of principles underlying all data privacy requirements.

- Lawfulness, fairness, and transparency
- Purpose limitation
- Data minimization
- Accuracy
- Storage limitation
- Cybersecurity (integrity and confidentiality)
- Accountability

Complete adherence to these principles requires not only the support of the Matter standard protocols but also all the supporting environment and infrastructure in which Matter devices live and operate. This is because data privacy requirements are aimed at protecting the privacy of individuals whose data is being consumed and transacted by the system of interest, and Matter protocols by design do not directly handle human-relevant information but only information about and from interacting devices and software agents. However, for all data that may be indirectly related to personal information through correlation or inference, Matter protocols uphold all the above principles within the boundary of Matter-related device interactions. Specifically:

- All data communications between Matter devices have the highest level of confidentiality and integrity supported by current civilian standards of network communications. This ensures that unauthorized entities cannot easily eavesdrop upon or tamper with data communicated between Matter devices.
- All Matter devices are required to provide proof of identity via attestation keypair and x.509 certification signed by a Trusted CA so that the data is shared only between known Matter entities.
- Matter is an open standard enabling peer review and validation of protocol and security controls it includes, including interaction between legitimate Matter devices.
- All data that is shared within Matter interactions is the minimum required for proper and robust operations of the Matter protocols. Great care has been taken in the design of Matter to minimize the amount of information that needs to be

[5] Complete guide to GDPR compliance https://gdpr.eu/

shared between nodes, thereby minimizing the potential for inadvertent leakage of information.

- All data shared between Matter nodes, as defined in the standard, is strictly for a defined purpose such as establishing identity of interacting parties, creating secure mutual contexts or associations for continuous operation, mutually agreed upon interaction modalities, etc. All data related to the specific operations of devices above the Matter protocol layer may affect data privacy but are not within the Matter scope.
- Matter addresses privacy by incorporating many privacy preserving mechanisms in the core specification such as unique random node identifiers, session establishment with configurable privacy, non-trackable IP addresses and sessions with private message headers. Specifically, when entities within the same fabric communicate over the network, their node identifiers in the message (that would normally be in the clear) are optionally encrypted using a separate encryption key that is negotiated for the session. This ensures that anyone eavesdropping on the network, in addition to not being able to read the messages due to message encryption, cannot see the identities of the communicating parties as well.

Platform Security

Depending on the targeted application, each Matter device implements an application layer on top of a Matter enabled software stack, and this combination runs on a hardware platform. The hardware platform is typically an MCU, secure MCU, or SoC with an optional companion secure element, and provides core security services (APIs) available for the other software layers. Security services such as cryptographic primitives, random number generation, secured cryptographic key storage, or even tamper resistance are then provided by the platform with a variable level of (proven) robustness against attacks depending on the platform.

Matter leaves room to the device manufacturer to select the appropriate platform security related to the risk and threat analysis of the use cases associated with their devices, as long as it does not endanger the ease of use and functionality of Matter devices. The device manufacturer can then select the platform that best matches their needs in terms of cost, security services, and robustness against attacks, in order to concentrate on the development of their dedicated application layer while the root security services are supported by the selected platform. To illustrate this, a door lock in a public area should resist remote network attacks but may also require a tamper resistant platform due to the threats inherent to the product use case, while tamper resistance for a light bulb inside a home area may not be necessary.

Device manufacturers can benefit from an easier integration with shorter development time, and trusted security services on which to rely with strong technical support from the platform vendor. This modular approach enhances maintainability since any evolution of the cryptographic suite or robustness requirements that may be introduced in future Matter revisions can be partly or entirely managed by the platform vendor (e.g.

through field update), with little impact for the device manufacturer and seamlessly from the user point of view.

The choice is left to the device manufacturer to use a Matter ready hardware platform (*i.e.*, with security services matching Matter needs) or to implement the needed low-level security features themselves on a more generic platform.

Conclusion

Matter is a unifying, IP-based connectivity protocol built on proven technologies and the collective expertise of the industry. By working together, we are creating more reliable and secure smart homes and IoT ecosystems. Matter's unified approach simplifies connected experiences while providing greater compatibility and security.

Security and privacy are key concerns that users of IoT devices have and IoT device manufacturers are looking to address. Matter provides a baseline for building secure IoT devices through a comprehensive, strong, easy and resilient architecture - the foundation for connected things.

Acknowledgements

The authors of this white paper acknowledge contributions to the Matter Security standard from numerous security subject matter experts in the Matter Working Group who were foundational to the authoring of this paper.