Poster: An Analysis of Matter IoT Security Against International Standards and Regulatory Framework

Andrew Losty
University College London (UCL)
andrew.losty.23@ucl.ac.uk

Anna Maria Mandalari
University College London (UCL)
a.mandalari@ucl.ac.uk

I. Motivation

Our poster presents a work-in-progress comparative study examining the Matter security specification against national and international IoT security frameworks. The preliminary results evaluate Matter's compliance with 18 major IoT standards across six operational and security domains defined in our assessment framework. This ongoing research will be extended to cover the full set of sixteen domains, enabling a more comprehensive evaluation. Despite its preliminary nature, the analysis provides early insights relevant to manufacturers, developers, and regulators.

The Internet of Things (IoT) smart home ecosystem is undergoing a fundamental paradigm shift in its architectural design [1]. The Matter protocol introduces a novel operational framework and data model for smart home devices from a wide range of manufacturers [2]. Devices are uniquely authenticated using Device Attestation Certificates (DAC) [3], and all operational communications are encrypted using AES-128/256 [4], [5]. To ensure protocol conformance and interoperability, Matter devices are subject to mandatory third-party certification, with certification status recorded in a Distributed Compliance Ledger (DCL) [3] to ensure that only compliant devices join a Matter fabric. Architecturally, Matter supports local operation without cloud dependence, leverages IPv6 for end-to-end addressing, and operates over Ethernet, Wi-Fi, and Thread network transports.

Prior to the release of the Matter 1.0 standard in October 2022 [6] and its subsequent four updates [7], [8], [9], [10], smart home deployments were dominated by vendor-specific ecosystems developed by individual manufacturers. This led to highly fragmented environments, with major platforms such as Amazon Alexa, Apple HomeKit, Google Home, and Samsung SmartThings relying on proprietary communication protocols, device-specific control mechanisms, and distinct security models. Such heterogeneity limited cross-platform interoperability and increased the complexity of device integration and management.

The Matter standard is supported by 286 manufacturers [11], including major ecosystem providers such as Google, Amazon, Apple, and Samsung. The specification is maintained by the Connectivity Standards Alliance (CSA) [12]. Forecasts project 5.5 billion Matter-compliant smart home devices will be shipped worldwide between 2022 and 2030 [13].

II. Problem statement

The rapid adoption of the Matter standard, coupled with its endorsement by dominant smart home manufacturers, positions it to become a de facto architectural and security baseline for consumer IoT ecosystems. As such, misalignment between Matter's security specification and established international security frameworks could propagate systemic risks. This work investigates the extent to which the Matter specification conforms to widely adopted regulatory and best-practice security frameworks, including the Cyber Resilience Act (CRA) [14], National Institute of Standards and Technology (NIST) [15], and the European Telecommunications Standards Institute (ETSI) [16]. We identify areas of strong alignment, as well as systematic divergences that raise concerns regarding governance, accountability, and long-term security assurance.

III. Contributions

This work introduces a systematic security assessment of the Matter IoT specification using six operational and security domains. We compare Matter's specification-level security controls against 18 widely adopted IoT security standards and regulatory frameworks, including NIST SP 800-53, ETSI EN 303 645, the UK PSTI Act [17], [18], [19], and the EU Cyber Resilience Act (CRA), providing a structured view of how protocol-level security aligns with regulatory compliance requirements.

IV. Relation to prior/submitted work

Our work is based on preliminary results from an ongoing research effort submitted as the paper "An Analysis of Matter IoT Security Against International Standards and Regulatory Frameworks" to the SDIotSec workshop in December 2025. The poster presents a high-level summary of the work and does not constitute a duplicate publication.

V. Preliminary results

Our analysis indicates that Matter aligns with regulatory controls for attack-surface minimization. Matter devices typically expose a single primary application endpoint on UDP/TCP port 5540 for authenticated and encrypted traffic, with limited auxiliary use of DNS (port 53), NTP (port 123), and mDNS [20] for local service discovery. By consolidating

Fig. 1: Six Operational / Security Domains

functionality onto a small set of well-defined ports and leveraging encrypted application-layer protocols over IPv6, Matter reduces unnecessary network exposure.

Matter secure communications comply with international regulations. Security is provided through Password-Authenticated Session Establishment (PASE) during commissioning and Certificate-Authenticated Session Establishment (CASE) using X.509 certificates for post-commissioning operation. All communications employ authenticated encryption using AES-128/256-CCM [4], [5] and SHA-256 [21], ensuring confidentiality, integrity, and mutual authentication.

Matter's mandatory certification program aligns with Connectivity Standards Alliance (CSA) requirements; however, its implementation relies on a proprietary ecosystem, limiting transparency compared to open compliance frameworks.

Divergence from regulatory standards is observed in logging and telemetry, where visibility is platform-dependent, and in secure storage, which remains underspecified in the Matter specification.

Matter also does not mandate or publish software support periods, limiting alignment with UK Product Security and Telecommunications Infrastructure (PSTI) [22] and Information Commissioner's Office (ICO) [23] requirements. Future work will extend this evaluation across ten additional operational and security domains to provide a more comprehensive assessment of Matter's regulatory alignment and divergence.

References

[1] W. Zegeye, A. Jemal, and K. Kornegay, "Connected smart home over matter protocol," in *Proc. IEEE Int. Conf. on Consumer Electronics (ICCE)*, Las Vegas, NV, USA, Jan. 2023, pp. 1–7.

[2] W. Zegeye, R. Mangar, J. Qian, V. Morris, M. Khanafer, K. Kornegay, T. J. Pierson, and D. Kotz, "Comparing smart-home devices that use the matter protocol," in *2025 IEEE 22nd Consumer Communications Networking Conference (CCNC)*, 2025, pp. 1–6.

[3] K. Shashwat, F. Hahn, X. Ou, and A. Singhal, "Security analysis of trust on the controller in the matter protocol specification," in *2023 IEEE Conference on Communications and Network Security (CNS)*, 2023, pp. 1–6.

[4] National Institute of Standards and Technology, "Advanced encryption standard (aes)," U.S. Department of Commerce, National Institute of Standards and Technology, Gaithersburg, MD, USA, FIPS Publication FIPS 197-upd1, May 2023, Accessed: 2025-12-07.

[5] M. Dworkin, "Recommendation for block cipher modes of operation: The ccm mode for authentication and confidentiality," National Institute of Standards and Technology, Gaithersburg, MD, USA, NIST Special Publication SP 800-38C, 2007, updated July 20, 2007.

[6] C. S. A. (CSA), "Matter specification, version 1.0: Core specification," Sep. 2022, [Online]. Available: https://csa-iot.org/wp-content/uploads/2022/11/22-27349-001-Matter-1.0-Core-Specification.pdf (accessed Dec. 7, 2025).

[7] C. S. A. (CSA), "Matter specification, version 1.1: Core specification," May 2023, [Online]. Available: https://csa-iot.org/wp-content/uploads/2023/05/22-27349-002-matter-1-1-core-specification.pdf (accessed Dec. 7, 2025).

[8] C. S. A. (CSA), "Matter specification, version 1.2: Core specification," Oct. 2023, [Online]. Available: https://csa-iot.org/wp-content/uploads/2023/10/Matter-1.2-Core-Specification.pdf (accessed Dec. 7, 2025).

[9] C. S. A. (CSA), "Matter specification, version 1.3: Core specification," Apr. 2024, [Online]. Available: https://csa-iot.org/wp-content/uploads/2024/05/matter-1-3-core-specification.pdf (accessed Dec. 7, 2025).

[10] C. S. A. (CSA), "Matter specification, version 1.4: Core specification," Nov. 2024, [Online]. Available: https://csa-iot.org/wp-content/uploads/ (accessed Dec. 10, 2025).

[11] C. S. A. (CSA), "Matter — the power of membership," 2023, [Online]. Available: https://csa-iot.org/members/ (accessed Jan. 19, 2026).

[12] "Connectivity Standards Alliance (CSA-IoT)," Online, 2026, accessed: Jan. 21, 2026. [Online]. Available: https://csa-iot.org/

[13] A. Research, "More than 5.5 billion smart home matter-compliant devices will ship between 2022 and 2030," Dec. 2022, [Online]. Available: https://www.prnewswire.com/news-releases/more-than-5-5-billion-smart-home-matter-compliant-devices-will-ship-between-2022-and-2030–301477876.html (accessed Dec. 7, 2023).

[14] E. Parliament and C. of the European Union, "Regulation (eu) 2024/2847 on horizontal cybersecurity requirements for products with digital elements (cyber resilience act)," *Official Journal of the European Union*, L 2024/2847, Nov. 2024, [Online]. Available: https://eur-lex.europa.eu/eli/reg/2024/2847/oj/eng (accessed Dec. 7, 2025).

[15] N. I. of Standards and T. (NIST), "National institute of standards and technology," [Online]. Available: https://www.nist.gov/ (accessed Jan. 19, 2026).

[16] E. T. S. I. (ETSI), "European telecommunications standards institute," [Online]. Available: https://www.etsi.org/ (accessed Jan. 19, 2026).

[17] N. I. of Standards and T. (NIST), "Security and privacy controls for information systems and organizations, nist special publication 800-53 rev. 5," Sep. 2020, [Online]. Available: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf (accessed Jan. 19, 2026).

[18] E. T. S. I. (ETSI), "Cyber security for consumer internet of things: Baseline requirements, etsi en 303 645 v2.1.1," Jun. 2020, [Online]. Available: url = https://www.etsi.org/ deliver/etsien/303600303699/303645/02.01.0160/en303645v020101p.pdf, (accessed Jan. 19, 2026).

[19] U. Parliament, "Product security and telecommunications infrastructure act 2022, c. 46," 2022, [Online]. Available: https://www.legislation.gov.uk/ukpga/2022/46/part/1/enacted (accessed Jan. 19, 2026).

[20] S. Cheshire and M. Krochmal, "Multicast dns," RFC 6762, Feb. 2013, standards Track.

[21] National Institute of Standards and Technology, "Secure hash standard (shs)," Federal Information Processing Standards Publication 180-4, Aug. 2015. [Online]. Available: https://doi.org/10.6028/NIST.FIPS.180-4

[22] "Product security and telecommunications infrastructure act 2022 (c. 46)," https://www.legislation.gov.uk/ukpga/2022/46/contents, UK Government, 2022, Accessed: 2025-12-07.

[23] "Guidance for consumer internet of things products and services," https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/online-tracking/guidance-for-consumer-internet-of-things-products-and-services/, Information Commissioner's Office, 2025, Accessed: 2025-12-07.

Poster: An Analysis of Matter IoT Security Against International Standards and Regulatory Framework.

Andrew Losty, Anna Maria Mandalari
University College London

Abstract

Since its launch in October 2022, the Matter smart home protocol has emerged as a unifying standard for consumer IoT and is supported by leading technology companies.

Prior to Matter, IoT ecosystems were highly fragmented, relying on vendor-specific protocols, control mechanisms, and security models. This study examines how Matter aligns with 18 international standards such as CRA, NIST, and ETSI, initially focusing on six key security domains, with plans to expand the analysis to sixteen domains. We aim is to provide practical and actionable insights for manufacturers, developers, and regulators considering the adoption and implementation of the Matter protocol.

Research Questions.

RQ1: How do Matter security specifications (v1.0–1.4) align with requirements defined in major international IoT security frameworks and regulations?

RQ2: Across core security domains—device certification, attack-surface minimization, secure communications, software updates, logging/telemetry, and secure storage. Where does Matter provide strong guidance and where is it less well defined?

RQ3: What compliance gaps and divergences emerge when Matter's published security controls are mapped against frameworks such as the CRA, NIST, and ETSI?

RQ4: To what extent does Matter's standardized architecture support consistent and interoperable security practices across multi-vendor consumer IoT ecosystems?

Methodology

We analyze the Matter 1.0–1.4 specifications using a domain-based framework to compare them against 18 IoT security standards and four labeling schemes, highlighting alignments and gaps in the protocol's security and operational requirements.

Standard	Name / Description	Region	Year
PSTI	Product Security and Telecommunications Infrastructure	UK	2022
ICO	Information Commissioner's Office	UK	2025
CRA	Cyber Resilience Act	EU	2024
ETSI EN 303 645 (v3.1.3)	Cyber Security for Consumer Internet of Things: Baseline Requirements	EU	2024
ETSI TS 103 645 (v3.1.1)	Cyber Security for Consumer Internet of Things: Technical Specification	EU	2024
ETSI TR 103 621 (v2.1.1)	IoT Security Assurance Framework	EU	2025
ETSI TS 103 701 (v2.1.1)	Cybersecurity for Smart Home and Building IoT Systems	EU	2025
ETSI TS 103 815 (v1.1.1)	IoT Security Guidelines for Networked Devices	EU	2024
ISO/IEC 27400:2022	Cybersecurity - IoT security and privacy -Guidelines	International	2022
ISO/IEC 27402	Cybersecurity - IoT security and privacy - Device baseline requirements	International	2023
NIST SP 800-53 Rev.5	Security and Privacy Controls for Information Systems and Organizations	US	2020
NIST SP 800-53B	Control Baselines for Information Systems and Organizations	US	2020
NIST SP 800-53A Rev.5	Security and Privacy Controls in Information Systems and Organizations	US	2022
NIST IR 8259A	IoT Device Cybersecurity Capability Core Baseline	US	2020
NIST IR 8259 Rev.1	Foundational Cybersecurity Activities for IoT Product Manufacturers	US	2025
NIST IR 8259B	IoT Non-Technical Supporting Capability Core Baseline	US	2021
NIST CSF 2.0	Cybersecurity Framework Version 2.0	US	2025
NIST IR 8425A	Recommended Cybersecurity Requirements (Router Products)	US	2024

Table 1. Assessed IoT DNS Regulations and Standards

Standard	Name / Description	Region	Year
CLS	Consumer IoT Label Scheme (Cyber Label Singapore)	Singapore	2025
FCL	Finnish Cybersecurity Label for IoT Devices	Finland	2019
BSI	BSI IoT Security Label	Germany	2021
JC-STAR	Japan Cybersecurity for IoT Labelling Scheme	Japan	2025

Table 2. Assessed IoT Label Schemes

Framework	Device Certification	Attack Surface Reduction	Secure Comms	Defined SW Update period	Logging / Telemetry	Secure Storage
Matter	Mandatory: 3rd-party (Matter Logo)	✓	✓	✗	Manufacturer Decision	Manufacturer Decision
PSTI	✗	✗	✓	✓	✗	✓
ICO	✗	✗	✓	✓	✗	✓
CRA	Mandatory: 3rd-Party / Manufacturer (CE Mark)	✓	✓	✗	✓	✓
ETSI EN 303 645	Voluntary: (Label schemes) *	✓	✓	✓	✓	✓
ETSI TS 103 645	Voluntary: (Label schemes) *	✓	✓	✗	✓	✓
ETSI TR 103 621	✗	✓	✓	✗	Partial	✓
ETSI TS 103 701	Voluntary: 1st,2nd,3rd party	✓	✓	✗	✓	✓
ETSI TS 103 815	✗	✓	✓	✗	✓	✓
ISO/IEC 27400:2022	✗	✓	✓	✗	Partial	✓
ISO/IEC 27402	✗	✓	✓	✗	✓	✓
NIST-SP800-53 R5	✗	✓	✓	✗	✓	✓
NIST-SP800-53B	✗	✓	✓	✗	✓	✓
NIST-SP800-53A R5	✗	✓	✓	✗	✓	✓
IoT-NIST IR8259A	✗	Partial	✓	✗	Partial	✓
IoT-NIST IR8259	✗	✗	✓	✗	Partial	✓
IoT-NIST IR8259B	✗	✗	✓	✗	✓	✓
NIST CSF 2.0	✗	✗	✓	✗	✗	✓
NIST IR 8425A	✗	✗	Risk Mgmt	✗	✗	Risk Mgmt
CLS (Singapore) *	Voluntary: 3rd-Party / Manufacturer					
FCL (Finland) *	Voluntary: 3rd-party					
BSI (Germany) *	Voluntary: Manufacturer					
JC-STAR (Japan) *	Voluntary: 3rd-Party / Manufacturer					

Table 3. Mapping – Selected domains to IoT DNS Regulations and Standards

Initial Results (Six Domains)

Attack Surface, Secure Communications — Strong compliance
Logging/Telemetry, Secure Storage — Manufacturer Specific implementation
Software Update Period — Unspecified software update support period
Device Certification — Proprietary Certification

Future Work

This work is ongoing and currently evaluates six security and operational domains of Matter. Future work will extend the analysis to the remaining ten domains, providing a more comprehensive assessment of Matter's security and operational characteristics.

(Software Update Mechanism, Vulnerability Disclosure / Management, Identity / Authentication, Authorization / Access Control, Secure Boot / Integrity Verification, Data Protection and Minimization, Resilience / Fault Handling, Secure Default Configuration, Lifecycle Management / Decommissioning, Input Validation and Interface Hardening)

Conclusion

Matter aligns with established IoT security frameworks in attack-surface minimization and encrypted communications. However, it diverges from regulatory frameworks in areas such as; platform dependent logging and telemetry, unspecified software lifespan, manufacturer-dependent secure storage, and reliance on a proprietary certification regime rather than an open, international, multi-vendor standard.

These findings suggest Matter is technically robust but less prescriptive than compliance-driven standards such as ETSI, NIST, and CRA.

E: andrew.losty.23@ucl.ac.uk
E: a.mandalari@ucl.ac.uk
T: +44 (0)771404 5924
T: +44 (0) 20 7679 7303 (int. 37303)
University College London, Roberts Building - Department of Electronic & Electrical Engineering, 1108 Torrington Place, London, WC1E 7JE, United Kingdom