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

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

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

***Abstract*—As Matter adoption and device deployment grow, it is essential to assess alignment with international IoT security frameworks and standards. This interim study evaluates Matter specifications against 18 international frameworks to identify compliance and security gaps. An independent IoT security framework, the Cloud Security Alliance (CSA), was used to provide a taxonomy and grouping of security controls, from which six core security domains were initially selected: (i) device certification, (ii) attack-surface minimization, (iii) secure communications, (iv) software update mechanisms, (v) logging/telemetry, and (vi) secure storage. The analysis highlights areas where Matter provides strong guidance and where it is less prescriptive compared to regulations and frameworks such as the Cyber Resilience Act (CRA), NIST, and ETSI. Future work will extend the assessment with ten additional domains, extending the analytical mapping of Matter's compliance and non-compliance, and providing valuable insights for manufacturers, developers, and regulators.**

I. Introduction

The architecture of consumer Internet of Things (IoT) infrastructure may be undergoing a profound and fundamental transformation. Historically, consumer IoT developed in a fragmented manner, as manufacturers pursued differentiation through proprietary security, privacy, and operational features. This resulted in isolated consumer ecosystems, in which competing platforms such as Apple Home [1], Google Home [2], Samsung SmartThings [3], and Amazon Alexa [4] relied on device-specific implementations that severely limited interoperability.

To overcome interoperability and security inconsistencies in legacy IoT ecosystems, major industry stakeholders collaboratively developed the Matter standard, formally released in 2022 under the control of the Connectivity Standards Alliance (CSA) [5]. Matter defines a unified communication protocol and a common device-lifecycle architecture, spanning commissioning, operation, security, identity management, data handling, and upgrades, thereby enabling cross-vendor compatibility and enforcing consistent security practices. Matter is supported by over 288 manufacturers [6] and 3,856 certified models [7], including major providers from previously competing ecosystems such as Apple Home, Google Home, Samsung SmartThings, and Amazon Alexa. This momentum is reinforced by recent announcements from additional major vendors adopting the protocol, including Ikea [8], Philips Hue [9], and LG Electronics [10].Electronics [10].

Since its 2022 launch, Matter is forcast to grow rapidly at a CAGR of 23.8% from 2025 to 2033, reaching a market value of US$21.2 billion by 2033 [11].

Given the rapid expansion and projected growth of Matter-enabled devices, it is essential to critically evaluate the standard's architecture and operational behavior to assess its alignment with leading IoT security frameworks, identifying both areas of compliance and deviations from established security controls.

We evaluate Matter 1.0–1.4 security controls against 18 major IoT standards, identifying where it meets, exceeds, or diverges from security baselines. Six core domains from the CSA IoT Security Controls Framework v2 [12] are selected to be analyzed: device certification, attack-surface minimization, secure communications, software updates, logging/telemetry, and secure storage.

II. Standards, Guidelines & Regulations

We analyze the initial Matter specification 1.0 [13], along with the subsequent major updates 1.1–1.4 [14]–[17], and compare the published controls and operational security measures to 18 internationally recognized IoT security standards and regulatory frameworks, as defined in Table I.

The most significant frameworks for direct comparison with Matter are those that define specific controls using RFC 2119 [18] clauses (MUST, SHOULD, or OPTIONAL). In the UK, the PSTI Act [19] imposes legally binding operational obligations on IoT manufacturers, while the CRA [20] specifies mandatory and recommended measures and includes device certification requirements. ETSI EN 303 645 [21] defines security requirements for consumer IoT devices, and TS 103 701 [22] expands these with more detailed guidance. Internationally, ISO/IEC 27400:2022 [23] provides broader IoT security and privacy guidance. In the US, NIST SP 800-53 Rev.5 [24] provides comprehensive mandatory controls for federal systems. Together, these frameworks help organizations align device security across jurisdictions, prioritize critical controls, and identify gaps against established baselines, forming a strong foundation for compliance and risk management. Table I summarizes the standards and regulations evaluated.

Network and Distributed System Security (NDSS) Symposium 2026
23 - 27 February 2026 , San Diego, CA, USA
ISBN 979-8-9919276-8-0
ttps://dx.doi.org/10.14722/sdiotsec.2026.23066
www.ndss-symposium.org

Framework	Region	Year
PSTI [19]	UK	2022
ICO [25]	UK	2025
CRA [20]	EU	2024
ETSI EN 303 645 (v3.1.3) [21]	EU	2024
ETSI TS 103 645 (v3.1.1) [26]	EU	2024
ETSI TR 103 621 (v2.1.1) [27]	EU	2025
ETSI TS 103 701 (v2.1.1) [22]	EU	2025
ETSI TS 103 815 (v1.1.1) [28]	EU	2024
ISO/IEC 27400:2022 [23]	INT	2022
ISO/IEC 27402 [29]	INT	2023
NIST SP 800-53 Rev.5 [24]	US	2020
NIST SP 800-53B [30]	US	2020
NIST SP 800-53A Rev.5 [31]	US	2022
IoT NIST IR 8259A [32]	US	2020
IoT NIST IR 8259 Rev.1 [33]	US	2025
IoT NIST IR 8259B [34]	US	2021
NIST CSF 2.0 [35]	US	2025
NIST IR 8425A [36]	US	2024
IoT Label Framework	Region	Year
CLS [37]	Singapore	2025
FCL [38]	Finland	2019
BSI [39]	Germany	2021
JC-STAR [40]	Japan	2025

TABLE I
IOT SECURITY STANDARDS AND FRAMEWORKS BY REGION.

Note. CLS, FCL, BSI, and JC-STAR are excluded, as they are derived from the accessed frameworks. [41] [42] [43] [44].

Device	Vendor/Product	Ver	Spec	Certification ID
Orein	4456/1002	2.0	1.0	CSA22089MAT40089-24
Orein	4456/1002	3.0	1.4	CSA252B0MAT45570-24
Tapo	5010/264	1.0	1.0	CSA23545MAT41058-24
Tapo	5010/264	1.3	1.3	CSA2510FMAT45153-24

TABLE II
MATTER DEVICE RECERTIFICATION ON SOFTWARE UPDATE.

III. DEVICE CERTIFICATION

A. Matter Device Certification

Device certification is integral to the Matter architecture, ensuring compliance with CSA specifications, interoperability, and eligibility for Certified Product logos and listings [42]. Certification is limited to CSA members and is performed by one of 32 CSA-authorized test providers [43]. During commissioning, Matter controllers query the Distributed Compliance Ledger (DCL) to verify certification status. Offline commissioning is supported but triggers generic warnings in Apple Home, Google Home, and SmartThings, and a more specific warning in Alexa. Certification costs include CSA membership (US$7,000 at Adopter level) [44], testing fees (US$10,000–14,000) [45], and internal engineering effort. Certification remains valid for a product's lifetime; however, firmware updates targeting newer Matter specifications require re-certification, as shown in Table II.

B. Device Certification: Standards and Regulations

IoT standards and regulations define certification and conformity requirements. The Matter standard mandates certification for all commercial devices, while the European CRA applies a risk-based model, permitting manufacturer self-assessment for Default products, conditional self-assessment for Important Class I, and mandatory third-party assessment for Important Class II and Critical products. European frameworks such as ETSI EN 303 645 [21], ETSI TS 103 701 [22], and ETSI TS 103 645 [26] offer optional third-party conformity assessment via accredited laboratories (e.g., TÜV SÜD [45], DEKRA [46], RISE [47]). International, voluntary labeling schemes, including Singapore's Cybersecurity Labelling Scheme [37], the Finnish Cybersecurity Label [38], Germany's BSI IT Security Label [39], and Japan's JC-STAR [40], reinforce independent verification, generally aligning with EN 303 645 to provide a standardized security baseline and a visible trust mark for compliant devices. Table III summarizes these certification and assessment pathways for the frameworks that mandate certification, highlighting the differing levels of mandatory and voluntary verification across jurisdictions.

Framework	Certification	Assessment
Matter (International)	Mandatory	3rd-party
CRA (EU)		
Default	Mandatory	Manufacturer
Class I	Mandatory	3rd party/Manufacturer
Class II	Mandatory	3rd party
Critical	Mandatory	3rd party (Strict)
ETSI EN 303 645 (EU)	Voluntary	3rd-party
ETSI TS 103 701 (EU)	Voluntary	3rd-party
ETSI TS 103 645 (EU)	Voluntary	3rd-party
CLS (Singapore)	Voluntary	3rd-party/Manufacturer
FCL (Finland)	Voluntary	3rd-party
BSI (Germany)	Voluntary	Manufacturer
JC-STAR (Japan)	Voluntary	3rd-party/Manufacturer

TABLE III
DEVICE CERTIFICATION REQUIREMENTS.

IV. ATTACK SURFACE MINIMIZATION

A. Matter Surface Minimization

Matter devices have a highly constrained attack surface, with operational communications primarily limited to UDP/TCP port 5540 for commissioning and encrypted communications. Additional network use is minimal, restricted to DNS (UDP port 53) and NTP (UDP port 123). Service advertising is performed over UDP port 5353 for IPv4 (224.0.0.251) and IPv6 (FF02::FB) [48]. Open ports and available services on Matter devices are extremely limited; however, Matter controllers can obtain a rich set of data from a device over port 5540 using *General Diagnostics Cluster* commands. This allows controllers to retrieve detailed device information while the device itself exposes a minimal attack surface.

B. Surface Minimization: Standards and Regulations

Several standards explicitly require IoT devices to minimize their attack surface. The EU CRA (Annex 1, Part 1, 2(j)) mandates reducing exploitable interfaces and unnecessary services. ETSI specifications enforce similar controls, including disabling unused interfaces, restricting services, and applying secure defaults. ISO standards, such as ISO/IEC 27400:2022 (7.1.2.17) and ISO/IEC 27402 (5.2.6) [29], require interface

Framework	Provision	Compliance
Matter	Not in Standard	Yes
PSTI	Not in Standard	No
ICO	Not in Standard	No
CRA	Annex1 Part 1 2(j)	Yes
ETSI EN 303 645	Provision 5.6/4.6	Yes
ETSI TS 103 645	Ref to ETSI EN 303 645	Yes
ETSI TR 103 621	Provision 5.3-9	Yes
ETSI TS 103 701	Provision 5.6	Yes
ETSI TS 103 815	Provision 5.6	Yes
ISO/IEC 27400:2022	Clause 7.1.2.17	Yes
ISO/IEC 27402	Clause 5.2.6	Yes
NIST-SP800-53 R5	Control CM7	Yes
NIST-SP800-53B	Control L, M, H	Yes
NIST-SP800-53A R5	Control SA-15(05)	Yes
IoT-NIST IR8259A	Section Access Mgmt	Partial
IoT-NIST IR8259	Not in Standard	No
IoT-NIST IR8259B	Not in Standard	No
NIST CSF 2.0	Not in Standard	No
NIST IR 8425A	Not in Standard	No

TABLE IV
ATTACK SURFACE MINIMIZATION.

Framework	Provision	Period
Matter	Section 9.12.10	No
PSTI	Schedule 1 Para 3	Yes
ICO	Security Update Period	Yes
CRA	Annex1 Part 1 2(c)	No
ETSI EN 303 645	Provisions 5.3-1 to 5.3-10	Yes
ETSI TS 103 645	Ref to ETSI EN 303 645	No
ETSI TR 103 621	Provision 5.3.6	No
ETSI TS 103 701	Provision 5.3,5.7	No
ETSI TS 103 815	Provision 5.3,5.7	No
ISO/IEC 27400:2022	Clause 7.1.2.17	No
ISO/IEC 27402	Clause 5.2.7.1.1	No
NIST SP 800-53 Rev.5	Control MA-03(6)	No
NIST SP 800-53B	Control MA-03(6)	No
NIST SP 800-53A	Control MA-03(6)	No
IoT NIST IR 8259A	Secure Update Mech	No
IoT NIST IR 8259	Secure Update Mech	No
IoT NIST IR 8259B	Ref to 8259A	No
NIST CSF 2.0	ID.RA/PR.IP	No
NIST IR 8425A	Secure Update Integrity	No

TABLE V
SW UPDATE REQUIREMENTS AND SUPPORT PERIOD.

access control, least functionality, and disabling unnecessary capabilities. U.S. frameworks also address this: NIST SP 800-53 (CM-7) mandates least functionality, SP 800-53B [30] maps these requirements across baselines, and SP 800-53A [31] tests them via SA-15(05). In particular, several regulatory bodies, including PSTI, ICO [25], and the NIST CSF, do not explicitly require attack-surface minimization, addressing it only indirectly through broader security controls, as summarized in Table IV.

V. SECURE COMMUNICATION

A. Matter Secure Communication

Matter encrypts all operational data communications. During commissioning, PASE (Passcode Authenticated Session Establishment) provides a secure encrypted channel between the new device and its controller. This channel is established using either the unique 11-digit numeric code printed on the device or information encoded in a QR code or NFC tag.

Post-commissioning, CASE (Certificate Authenticated Session Establishment) secures communication using a unique X.509-v3 Node Operational Certificate (NOC) and its associated key pair [13]. The NOC is used to authenticate the device and to derive the session keys. Matter employs FIPS 197 [49] defined AES-128-CCM, or optionally AES-256-CCM, for encryption [50], while confidentiality, integrity, and replay protection are provided by SHA-256 [51].

B. Secure Communication: Standards and Regulations

Analysis of major IoT security frameworks shows that Matter, along with almost all leading standards, mandates secure communications. Three principal frameworks—NIST SP 800-53 Rev.5, ETSI EN 303 645, and the EU CRA—all explicitly require cryptographic protections for data in transit. Other frameworks, including ISO/IEC 27400/27402, NIST IR 8259A [32], and the ETSI 103-series, also mandate or strongly recommend secure communications, while purely architectural or profile-only documents (e.g., ISO/IEC 30141, NIST IR 8259B) do not. Overall, Matter's security model is consistent with the requirements of leading standards and regulatory frameworks.

VI. SOFTWARE UPDATE MECHANISM

A. Matter Update Mechanism

Matter provides a robust over-the-air (OTA) firmware update mechanism, ensuring devices run the latest applicable firmware. Update data and firmware locations are published via the Distributed Compliance Ledger (DCL), with access strictly restricted to certified Matter devices. Within the network, devices assume one of two roles: the OTA Requestor (0x0012), which polls for available firmware updates, and the OTA Provider (0x0014), which manages update discovery, download, and application to Requestors.

Matter enforces strict version control to provide anti-rollback protection. All firmware images are digitally signed and verified, ensuring authenticity, integrity, and resistance to tampering throughout the update lifecycle. However, the specification also permits manufacturers to implement custom update mechanisms if desired.

B. Update Mechanism: Standards and Regulation

Most major IoT security frameworks explicitly mandate or recommend the provision of secure software update mechanisms. These include the CRA, ETSI EN 303 645, ETSI TS 103 701, ETSI TS 103 815 [28], ISO/IEC 27402, NIST IR 8259 [33], IR 8259A, IR 8259B [34], NIST SP 800-53 (controls SI-2 and CM-14), NIST IR 8425A, and ETSI TR 103 621 [27]. Collectively, these frameworks address critical aspects of update security, including authenticity, integrity, anti-rollback protections, and secure delivery.

Few frameworks explicitly require manufacturers to define the duration of software updates. The UK PSTI Act and ETSI EN 303 645 (clause 5.3-13) mandate updates for a specified

support period, while UK ICO guidance advises disclosing this period to users. No other reviewed frameworks explicitly require update-lifespan disclosure (see Table V).

VII. Logging/Telemetry

A. Matter Logging/Telemetry

The Matter specification provides a standard mechanism for device telemetry via its Diagnostics Logs Cluster, enabling retrieval of unstructured data such as crash, fault, and network logs, and hardware and radio fault information. While Matter defines how diagnostics are requested and transmitted, it does not specify their volume, structure, or retention, leaving these choices to individual ecosystems. Consequently, diagnostic visibility varies across platforms; for example, Google Nest exposes minimal data, whereas Home Assistant provides extensive logs and execution traces.

B. Logging/Telemetry: Standards and Regulation

Compliance-oriented frameworks such as NIST SP 800-53 Rev.5, SP 800-53B, NIST IR 8259A, ETSI EN 303 645, and the EU CRA explicitly mandate event logging and monitoring. In contrast, architecture-focused standards, including ISO/IEC 30141 and NIST IR 8259B, emphasize design principles and governance rather than prescribing logging requirements.

VIII. Secure Storage

A. Matter Secure Storage

The Matter specification does not define a specific mechanism for secure key/certificate storage, allowing manufacturers to determine a suitable protection method. Common approaches include Silicon Labs' Secure Vault [52] and NXP's EdgeLock SE051H [53].

B. Secure Storage: Standards and Regulation

Many security frameworks explicitly require protection of cryptographic material. The CRA mandates encryption of relevant data at rest, while ETSI EN 303 645 provides more specific direction by requiring the use of Trusted Execution Environments (TEEs) and encrypted storage supported by hardware Secure Elements (SEs) or Dedicated Security Components (DSCs). In comparison, NIST SP 800-53 Rev. 5 (controls SC-12 and SC-13) mandates the use of FIPS-validated or NSA-approved key-management technologies and processes (See Table VI).

Framework	Provision
Matter	Manufacturer decision
PSTI	Not in Standard
ICO	Principle 5: Storage Limitation
CRA	Annex1 Part 1 2(e)
ETSI EN 303 645	Provision 5.6
ETSI TS 103 645	Provision 5.6
ETSI TR 103 621	Provision 5.4-1
ETSI TS 103 701	Provision 5.4
ETSI TS 103 815	Provision 5.4
ISO/IEC 27400:2022	Clause 7.1.2.7
ISO/IEC 27402	Clause 5.2.5
NIST SP 800-53 Rev.5	Control SC-12, SC-13
NIST SP 800-53B	Control L,M,H SC-12, SC-13
NIST SP 800-53A Rev.5	Control SC-28
IoT NIST IR 8259A	Section 4.1.2: Data at rest
IoT NIST IR 8259	Section 4.1.2: Data at rest
IoT NIST IR 8259B	Section 4.1.2: Data at rest
NIST CSF 2.0	PR.DS-01
NIST IR 8425A	Data Protection mechanisms

TABLE VI
IoT Device Secure Storage.

IX. Conclusion & Future Work

We observe that Matter exhibits security and operational characteristics beyond the scope of the 18 major security frameworks examined. Although commercial Matter devices must undergo independent certification, only the CRA mandates third-party certification, and then only for Critical or Important-Class II devices.

We find that Matter aligns with core security frameworks in its requirement to minimize its interface attack surface by enforcing least functionality, limited services, and access controls. Matter satisfies these controls by restricting secure communications to UDP/TCP port 5540. The principal standards mandating attack-surface controls include the CRA, ISO/IEC 27400:2022, ISO/IEC 27402, and NIST SP 800-53, all emphasizing secure design and minimal exposure.

Matter complies with key frameworks for secure communications by using AES-128-CCM encryption, PASE during commissioning, and CASE for ongoing operations. It addresses software updates via a robust OTA mechanism, ensuring firmware integrity, authenticity, and resilience. However, Matter does not mandate a minimum software-update support period, as required by the UK PSTI Act and ETSI EN 303 645, leaving this to manufacturers. Matter also aligns with IoT logging and telemetry requirements specified in NIST SP 800-53 Rev.5, SP 800-53B, NIST IR 8259A, ETSI EN 303 645, and the CRA.

It is observed that the accessibility and granularity of logs remain highly dependent on the ecosystem: for example, Google Nest provides only minimal telemetry data, whereas Home Assistant exposes significantly more detailed logging information.

While Matter is defined by its specifications, we find there are areas of limited alignment with established IoT security frameworks. Matter addresses key requirements such as attack-surface minimization, secure communications, and logging/telemetry. It fails to (i) define device certification methods, (ii) specify a period for software updates, or (iii) mandate secure IoT storage methods for keys and certificates while frameworks such as NIST and ETSI provide explicit guidance.

A subsequent, more comprehensive study will extend the analysis to address key categories, including vulnerability disclosure, data minimization, user authentication and roles, secure default operation, user-data protection, device resilience, input validation, and secure decommissioning.

REFERENCES

[1] A. Inc., "Homepod mini," https://www.apple.com/homepod-mini/, 2023, Accessed: 2025-12-10.

[2] Google, "Google nest and home device specifications," https://support.google.com/googlenest/answer/7072284, 2023, Accessed: 2025-12-10.

[3] SmartThings, "Works with smartthings," https://www.smartthings.com/works-with-smartthings, 2023, Accessed: 2025-12-10.

[4] Amazon, "Amazon echo & alexa devices," https://www.amazon.com/b?&node=9818047011, 2023, Accessed: 2025-12-10.

[5] Connectivity Standards Alliance, "Home — csa-iot," https://csa-iot.org/, 2025, Accessed: 2025-12-07.

[6] CSA, "Matter - the power of membership," https://csa-iot.org/members/, 2023, Accessed: 2025-12-10.

[7] Cloud Security Alliance (CSA), "Distributed compliance ledger (dcl) web portal," https://webui.dcl.csa-iot.org/, accessed: 2026-01-29.

[8] IKEA, "Ikea launches new smart home range with 21 matter-compatible products," https://www.ikea.com/global/en/newsroom/retail/the-new-smart-home-from-ikea-matter-compatible-251106/, 2025, Accessed: 2025-12-07.

[9] Philips Hue, "Philips hue and matter," https://www.philips-hue.com/en-gb/explore-hue/works-with/matter, 2025, Accessed: 2025-12-07.

[10] LG Electronics and Google Home Developers, "Lg: Unlocking the full potential of matter-enabled homes powered by google home," https://developers.home.google.com/case-studies/lg, 2025, last updated: 2025-01-07. Accessed: 2025-12-07.

[11] R. Sharma, "Matter iot market research report 2033," https://growthmarketreports.com/report/matter-iot-market, 2025, report ID: ICT-SE-126294, Growth Market Reports, Accessed: 2025-12-06.

[12] "CSA IoT Security Controls Framework v2," hspace0.5emAvailable online: https://cloudsecurityalliance.org/artifacts/csa-iot-security-controls-framework-v2, Cloud Security Alliance, 2021, accessed: Jan. 29, 2026; Release Date: Jan. 28, 2021.

[13] Connectivity Standards Alliance, "Matter Specification, Version 1.0 – Core Specification," 2022, [Online]. Available: https://csa-iot.org/wp-content/uploads/2022/11/22-27349-001_Matter-1.0-Core-Specification.pdf. Accepted by CSA Board of Directors Sept. 28, 2022. Accessed: Dec. 7, 2025.

[14] "Matter Specification, Version 1.1 – Core Specification," https://csa-iot.org/wp-content/uploads/2023/05/22-27349-002_matter-1-1-core-specification.pdf, Connectivity Standards Alliance, May 2023, accepted 17 May 2023. Accessed: 2025-12-07.

[15] "Matter specification, version 1.2 – core specification," https://csa-iot.org/wp-content/uploads/2023/10/Matter-1.2-Core-Specification.pdf, Connectivity Standards Alliance, October 2023, accepted 18 Oct 2023. Accessed: 2025-12-07.

[16] "Matter specification, version 1.3 – core specification," https://csa-iot.org/wp-content/uploads/2024/05/matter-1-3-core-specification.pdf, Connectivity Standards Alliance, April 2024, accepted 17 Apr 2024. Accessed: 2025-12-07.

[17] "Matter specification, version 1.4 – core specification," https://csa-iot.org/matter-1.4-core-spec, Connectivity Standards Alliance, November 2024.

[18] S. O. Bradner, "Key words for use in rfcs to indicate requirement levels," RFC 2119, Best Current Practice no. 14, March 1997, Accessed: 2025-12-10. [Online]. Available: https://www.rfc-editor.org/info/rfc2119

[19] "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.

[20] "Regulation (eu) 2024/2847 on horizontal cybersecurity requirements for products with digital elements (cyber resilience act)," https://eur-lex.europa.eu/eli/reg/2024/2847/oj/eng, European Parliament and Council of the European Union, 2024, official Journal L, 2024/2847, 20 November 2024. Accessed: 2025-12-07.

[21] "Etsi en 303 645 v3.1.3 (2024-09) — cyber security for consumer internet of things: Baseline requirements," https://www.etsi.org/deliver/etsi_en/303600_303699/303645/03.01.03_60/en_303645v030103p.pdf, ETSI — European Telecommunications Standards Institute, 2024, Accessed: 2025-12-07.

[22] "Etsi ts 103 701 v2.1.1 (2025-05): Cyber security for consumer internet of things — conformance assessment of baseline requirements," https://www.etsi.org/deliver/etsi_ts/103700_103799/103701/01.01.01_60/ts_103701v010101p.pdf, European Telecommunications Standards Institute, 2025, Accessed: 2025-12-07.

[23] *ISO/IEC 27400:2022 — Cybersecurity: IoT security and privacy — Guidelines*, https://www.iso.org/standard/44373.html, International Organization for Standardization and International Electrotechnical Commission Std. ISO/IEC 27 400:2022, 2022, Accessed: 2025-12-07.

[24] "Security and privacy controls for information systems and organizations," https://csrc.nist.gov/pubs/sp/800/53/r5/upd1/final, Tech. Rep. SP 800-53, Revision 5, 2020, final version including updates as of December 10, 2020. Accessed: 2025-12-07.

[25] Information Commissioner's Office, "Guidance for consumer Internet of Things products and services," 2025, [Online]. Available: https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/online-tracking/guidance-for-consumer-internet-of-things-products-and-services/. Accessed: Dec. 7, 2025.

[26] "Etsi ts 103 645 v3.1.1 (2024-01): Cyber security for consumer internet of things — baseline requirements," https://www.etsi.org/deliver/etsi_ts/103600_103699/103645/03.01.01_60/ts_103645v030101p.pdf, European Telecommunications Standards Institute, 2024, Accessed: 2025-12-07.

[27] "Etsi tr 103 621 v2.1.1 (2025-07): Guide to cyber security for consumer internet of things," https://www.etsi.org/deliver/etsi_tr/103600_103699/103621/02.01.01_60/tr_103621v020101p.pdf, European Telecommunications Standards Institute, 2025, Accessed: 2025-12-07.

[28] "Etsi ts 103 815 v1.1.1 (2024-01): Cyber security for consumer internet of things — requirements for residential smart door locking devices," https://www.etsi.org/deliver/etsi_ts/103800_103899/103815/01.01.01_60/ts_103815v010101p.pdf, European Telecommunications Standards Institute, 2024, Accessed: 2025-12-07.

[29] *ISO/IEC 27402:2023 — Cybersecurity: IoT security and privacy — Device baseline requirements*, https://www.iso.org/standard/80136.html, International Organization for Standardization and International Electrotechnical Commission Std. ISO/IEC 27 402:2023, 2023, Accessed: 2025-12-07.

[30] "Nist special publication 800-53b: Control baselines for information systems and organizations," https://csrc.nist.gov/pubs/sp/800/53/b/upd1/final, Tech. Rep. SP 800-53B, 2020, final version including updates as of December 10, 2020. Accessed: 2025-12-07.

[31] "Nist special publication 800-53a revision 5: Assessing security and privacy controls in information systems and organizations," https://csrc.nist.gov/pubs/sp/800/53/a/r5/final, Tech. Rep. SP 800-53A, 2022, final, January 2022. Accessed: 2025-12-07.

[32] M. Fagan, K. Megas, K. Scarfone, and M. Smith, "Nistir 8259a: Iot device cybersecurity capability core baseline," https://csrc.nist.gov/pubs/ir/8259/a/final, National Institute of Standards and Technology (NIST), Tech. Rep. IR 8259A, 2020, final, May 29, 2020. Accessed: 2025-12-07.

[33] "Foundational cybersecurity activities for iot product manufacturers – second public draft (nist ir 8259 r1 2pd)," https://csrc.nist.gov/pubs/ir/8259/r1/2pd, Tech. Rep. IR 8259r1, 2025, second Public Draft, published September 30, 2025. Accessed: 2025-12-07.

[34] M. Fagan, J. Marron, K. Brady, B. Cuthill, K. Megas, and R. Herold, "Nistir 8259b: Iot non-technical supporting capability core baseline," https://csrc.nist.gov/pubs/ir/8259/b/final, National Institute of Standards and Technology (NIST), Tech. Rep. IR 8259B, 2021, final, August 25, 2021. Accessed: 2025-12-07.

[35] "Nist cybersecurity framework (csf)," https://www.nist.gov/cyberframework, National Institute of Standards and Technology (NIST), 2025, Accessed: 2025-12-07.

[36] M. Fagan, K. Megas, P. Watrobski, J.Marron, B. Cuthill, D. Lemire, B. Hoehn, and C. Evans, "Nist ir 8425a: Recommended cybersecurity requirements for consumer-grade router products," https://csrc.nist.gov/news/2024/iot-program-published-nist-ir-8425a, National Institute of Standards and Technology (NIST), Tech. Rep. IR 8425A, 2024, published September 2024. Accessed: 2025-12-07.

[37] "Cybersecurity labelling scheme for iot (cls(iot)) — about," Web page, Cyber Security Agency of Singapore, Oct. 2025, Accessed: 2025-12-07. [Online]. Available: https://www.csa.gov.sg/our-programmes/certification-and-labelling-schemes/cybersecurity-labelling-scheme/about/

[38] "The finnish cybersecurity label — cybersecurity label for consumer iot devices," Web page, Traficom / NCSC-FI, 2025, Accessed: 2025-12-07. [Online]. Available: https://tietoturvamerkki.fi/en/cybersecurity-label

[39] "It-sicherheitskennzeichen für verbraucherinnen und verbraucher," Web page, Bundesamt für Sicherheit in der Informationstechnik, 2025, Accessed: 2025-12-07. [Online]. Available: https://www.bsi.bund.de/EN/Themen/Verbraucherinnen-und-Verbraucher/IT-SiK-fuer-Verbraucher/IT-SiK-fuer-Verbraucher_node.html

[40] "Japan cyber star (jc-star): Labeling scheme based on japan cyber-security technical assessment requirements," https://www.ipa.go.jp/en/security/jc-star/index.html, Information-technology Promotion Agency, Japan (IPA), 2025, Accessed: 2025-12-07.
[41] "Cybersecurity labelling scheme (cls) faqs," https://www.csa.gov.sg/faqs/cybersecurity-labelling-scheme/, Cyber Security Agency of Singapore (CSA), 2025, last updated 13 February 2025; Accessed 2025-12-16.
[42] "International development," https://www.tietoturvamerkki.fi/en/international-development, Finnish Transport and Communications Agency (Traficom) / Cybersecurity Label, 2025, accessed: 2025-12-16.
[43] "Consumer iot: Cybersecurity for consumer internet of things," https://www.bsi.bund.de/EN/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/Consumer-IoT/Consumer-IoT.html, Federal Office for Information Security (BSI), Germany, 2025, accessed: 2025-12-16.
[44] Information-Technology Promotion Agency, Japan (IPA), "Jc-star: Japan cybersecurity standardization technology assistance and research," https://www.ipa.go.jp/en/security/jc-star/index.html, 2025, accessed: 2025-12-16.
[45] TÜV Rheinland, "Testing and certification," 2025, [Online]. Available: https://www.tuv.com/landingpage/en/testing-and-certification/. Accessed: Aug. 18, 2025.
[46] "DTC – Testing Certification Services," https://www.dekra.com/en/dtc/, DEKRA, 2025, Accessed: 2025-12-09.
[47] "Certification – rise," https://www.ri.se/en/certification-rise, RISE Research Institutes of Sweden, 2025, Accessed: 2025-12-09.
[48] S. Cheshire and M. Krochmal, "Multicast dns," RFC 6762, Internet Engineering Task Force, Feb. 2013, Accessed: 2025-12-07.
[49] N. I. of Standards and Technology, "Advanced Encryption Standard (AES), FIPS Pub. 197," US Department of Commerce, National Institute of Standards and Technology, Gaithersburg, MD, USA, Federal Information Processing Standards Publication FIPS 197, 2001, Accessed: 2025-12-07. [Online]. Available: https://csrc.nist.gov/pubs/fips/197/final
[50] 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.
[51] "Secure hash standard (shs)," Gaithersburg, MD, USA, FIPS Publication FIPS 180-4, August 2015, Accessed: 2025-12-07. [Online]. Available: https://csrc.nist.gov/pubs/fips/180-4/upd1/final
[52] "Secure vault — iot security," https://www.silabs.com/security/secure-vault, Silicon Labs, 2025, Accessed: 2025-08-18.
[53] NXP Semiconductors, "SE051H—secure element," 2025, [Online]. Available: https://www.nxp.com/products/SE051H. Accessed: Aug. 18, 2025.