

Evaluating Thread, Zigbee and Z-Wave Against Common Criteria
Cryptographic Requirements

Evangelos Nannos^{1,*,}, Stylianos Katsoulis^{1,*,}, Fotios Zantalis^{1,*,}, Ioannis Chrysovalantis Panagou^{1,*,},
Konstantinos Boukouras^{1,2,*,}, Grigorios Koulouras^{1,*,}

¹ TelSiP Research Laboratory, Department of Electrical and Electronic Engineering, School of Engineering, University of West Attica, Ancient Olive Grove Campus, 250 Thivon Str., GR-12241 Athens, Greece
² Institute of Geodynamics, National Observatory of Athens, Thiseio, Athens, Greece
* Corresponding author

INTRODUCTION & AIM

The rapid expansion of the Internet of Things (IoT) into critical sectors necessitates a rigorous evaluation of the security mechanisms embedded in standard wireless protocols.

- ❖ **Context:** The rapid expansion of IoT in smart homes and industrial automation has introduced diverse devices operating in constrained environments.
- ❖ **Problem:** While widely used IoT protocols like Thread, Zigbee, and Z-Wave embed security mechanisms, their alignment with formal assurance frameworks is often unclear.
- ❖ **Aim:** This study evaluates the cryptographic posture of these three protocols against the Common Criteria (CC:2022) and the EU Cybersecurity Certification Scheme (EUCC).

METHODOLOGY

This study adopts a comparative analytical framework, mapping the technical specifications of each protocol against the strict functional requirements of Common Criteria (CC:2022).

- ❖ **Approach:** Systematic literature review and comparative analysis based on technical specifications and recent peer-reviewed studies.
- ❖ **Evaluation Framework:** The protocols were assessed against the CC Class FCS (Cryptographic Support) functional requirements:
 - **FCS_CKM.1:** Cryptographic Key Generation
 - **FCS_CKM.2:** Key Distribution
 - **FCS_CKM_EXT.7:** Key Agreement
 - **FCS_COP.1:** Cryptographic Operations
 - **FCS_RBG.1:** Random Bit Generation

RESULTS & DISCUSSION

Our analysis reveals distinct variations in cryptographic compliance, highlighting significant differences in how each protocol manages key lifecycles and Random Bit Generation (RBG).




Criterion	Thread 	Zigbee 	Z-Wave 
Key Generation	Decentralized, strong RNG, ECDH	Central Trust Center, variable RNG, AES-128	S2 Framework, ECDH, proprietary RNG
Key Distribution	DTLS/TLS, ECDH	Trust Center, pre-configured link keys	ECDH (Curve25519), segmented security classes
Key Agreement	ECDH, robust peer-to-peer	Trust Center, pre-shared keys	S2 Security ECDH
Crypto Operations	AES-CCM (auth.), fully compliant	AES-128/CCM, partial compliance	AES-128 CCM, S2 compliance in new devices
Random Bit Generation	Hardware TRNG/CSPRNG, compliant	PRNGs, variable implementation	S2: strong RBG, proprietary limitations

Table 1 – Thread, Zigbee and Z-Wave protocols are analyzed across five key cryptographic aspects defined in FCS CC:2022

A. Key Findings per Protocol

- ❖ **Thread:** Demonstrates the strongest alignment with CC requirements. It utilizes AES-CCM and ECDH-based key exchange within a robust, decentralized trust model, minimizing single points of failure.
- ❖ **Zigbee:** Offers comparable cryptographic strength (AES-128) but faces compliance challenges due to its reliance on a Centralized Trust Center for key distribution, which complicates the strict lifecycle management required by CC.
- ❖ **Z-Wave:** The S2 Security Framework significantly improves security via ECDH (Curve25519). However, proprietary constraints and limited transparency in its Random Number Generation (RNG) implementation hinder full compliance.

B. Compliance Overview

- ❖ **FCS_CKM (Key Management):** Thread excels in decentralized generation. Zigbee struggles with pre-configured link keys, while Z-Wave’s proprietary components limit transparency despite its strengthened S2 Security framework.
- ❖ **FCS_RBG (Random Bit Generation):** Thread leverages hardware TRNG/CSPRNG, fulfilling high-assurance requirements better than the variable implementations often found in Zigbee and Z-Wave modules.

CONCLUSION

While all three protocols provide a functional security baseline, their readiness for formal high-assurance certification under the EUCC scheme varies significantly.

- ❖ **Thread** is currently the only protocol among the three that shows comprehensive alignment with Common Criteria and EUCC standards without major modification.
- ❖ **Zigbee and Z-Wave** provide a solid security baseline but require protocol hardening, specifically in key lifecycle management and transparency, to achieve formal certification.
- ❖ Aligning these lightweight protocols with CC is critical for building trust in sensitive IoT domains like healthcare and critical infrastructure.

FUTURE WORK

- ❖ **Quantum-Safe Cryptography:** Researching the integration of lightweight Post-Quantum Cryptography (PQC) algorithms to future-proof next-generation IoT protocols against emerging threats.
- ❖ **Open Auditability:** Promoting the development of open, fully auditable IoT protocols for mitigating security risks associated with proprietary/closed-source implementations.
- ❖ **Unified Certification Frameworks:** Fostering harmonized global standards that facilitate industry adoption and ensure consistent security assurance across diverse IoT ecosystems.

REFERENCES

1. Yalli, J. S., Hasan, M. H., Jung, L. T., Yerima, A. I., Aliyu, D. A., Maiwada, U. D., Al-Selwi, S. M. & Shaikh, M. U. (2025). A Systematic Review For Evaluating IoT Security: A Focus On Authentication, Protocols and Enabling Technologies. IEEE Internet of Things Journal. DOI: [10.1109/JIOT.2025.3545737](https://doi.org/10.1109/JIOT.2025.3545737)

2. Kambourakis, G., Koliass, C., Geneiatakis, D., Karopoulos, G., Makrakis, G. M., & Kounelis, I. (2020). A state-of-the-art review on the security of mainstream IoT wireless PAN protocol stacks. Symmetry, 12(4), 579. DOI: [10.3390/sym12040579](https://doi.org/10.3390/sym12040579)

3. Holguin, I., & Errapotu, S. M. (2023, October). Smart home IoT communication protocols and advances in their security and interoperability. In 2023 7th Cyber Security in Networking Conference (CSNet) (pp. 208-211). IEEE. DOI: [10.1109/CSNet59123.2023.10339739](https://doi.org/10.1109/CSNet59123.2023.10339739)