Security of eSIM Technology: Latest Trends and Innovations in 2025

Zulkharnain Muhammad [1], Ali Ahmed Alqudaihi [2]

1,2 Electrical Engineering Technology Department, College of Applied Industrial Technology (CAIT), Jazan University, 45142, Saudi Arabia

zbadruzzama@jazanu.edu.sa, aalqudaihi@jazanu.edu.sa

Corresponding Author:
Zulkharnain Muhammad
Phone# +966-556610624
zbadruzzama@jazanu.edu.sa

Abstract

The brisk advancement and broad acceptance of embedded SIM (eSIM) technology are markedly transforming the landscape of global connectivity, especially in connection with various consumer devices, the Internet of Things (IoT), and succeeding generations of telecommunications networks.

By 2025, the deployment of eSIM technology reached levels that were previously deemed extraordinary, thereby bringing to the forefront a plethora of security concerns that warrant meticulous consideration and analysis. This comprehensive research scrutinizes the continuously evolving threat landscape associated with eSIM technology, while simultaneously exploring the forefront of innovative defense mechanisms designed to bolster eSIM security, which encompasses recent discoveries of vulnerabilities inherent in eUICC technology, advancements in authentication protocols, the establishment and adherence to industry standards, as well as the promising field of quantum-safe cryptography. This study places significant emphasis on the transformative innovations that are characteristic of 2025 and how these advancements are pivotal in shaping the future of secure digital identities and seamless connectivity in an increasingly interconnected world.

.

KEYWORDS: eSIM, eUICC, cryptography, PKI, TLS eSIM, eUICC, cryptography, PKI, TLS

1. Introduction

The embedded SIM (eSIM) revolution is fundamentally altering the telecommunications ecosystem. Unlike traditional SIMs, eSIMs are digitally embedded within devices, allowing remote provisioning and profile management. By 2025, eSIM adoption spans smartphones, wearables, tablets, laptops, industrial IoT devices, and connected automobiles, driving a global market boom projected to exceed USD 6 billion by 2032.[1][2][3]

Amid this growth, security emerges as a primary concern. The remote, programmable, and software-centric nature of eSIMs introduces a set of unique risks as well as opportunities for stronger, more resilient security paradigms.

2. The Current eSIM Security Landscape

2.1 Authentication Methods

eSIM authentication relies on a blend of traditional and next-generation security mechanisms:

Method	Description	Reference
Profile-based Authentication	Each eSIM holds a unique digital profile verified by the network	[4]
Public Key Infrastructure (PKI)	Utilizes public-private key pairs for device authentication	[4]
Two-Factor Authentication (2FA)	Adds biometric or knowledge-based factors	[5][6]
Mutual Authentication	Both device and network verify each other's identity	[4]
Biometric Authentication	Devices leverage facial/fingerprint/iris verification for identity checks	[4][6][7]

2.2 Encryption Standards

State-of-the-art encryption shields eSIM assets:

- **Elliptic Curve Cryptography (ECC)**: Provides robust, lightweight encryption, crucial for IoT[8]
- **TLS Protocols (Transport Layer Security)**: Encrypts communications and provisioning sessions[9][10]
- **Post-Quantum Cryptography**: Emerging schemes ensure future-proofing against quantum attacks[11][12][13]
- **GSMA Security Specifications**: Rigorous frameworks governing profile and network access[10][14]

3. Security Vulnerabilities and Threats in 2025

3.1 Major Discoveries

Groundbreaking research in 2025 unearthed critical vulnerabilities in eSIM technology:

- **Kigen eUICC Java Card Vulnerability**: Exposed by Security Explorations, this flaw enabled attackers (with brief physical access and knowledge of test keys) to install malicious Java Card applets, clone eSIMs, extract credentials, intercept network traffic, and even brick eSIM chips.[15][16][17][18][19][20][21][22]

- **Profile Cloning Attacks**: Successful profile cloning was demonstrated, allowing interception of calls/SMS (including 2FA codes), identity theft, and undetectable backdoors.[17][21][22][23]
- **Test Profile Exploits (GSMA TS.48)**: Deploying outdated or mismanaged test profiles with known keys facilitated attacks. GSMA responded with rapid standards revisions (TS.48 v7.0, SGP.32, enhanced RAM key protection).[3][19][24]

3.2 Attack Vectors

Vector	Description	Impact
Profile Swapping	Attacker initiates a swap, hijacking identity and connectivity	Device disconnect, data theft
Memory Exhaustion	Overloading eSIM memory can cause denial-of-service, killing connectivity	DoS, profile/data loss
Locking Profile Attacks	Locks eSIM to specific MNO, preventing network switching	Consumer choice, flexibility loss
Malicious Applet Install	Deployment of unauthorized code, including persistent “backdoors”	Total compromise, surveillance

4. 2025 Innovations: Raising the Bar for eSIM Security

4.1 Post-Quantum Security

Quantum-safe eSIMs are no longer conceptual:

- Operators and vendors have piloted eSIMs with quantum-resistant algorithms (e.g., for IoT utilities and smart meters), ensuring secure provisioning and encrypted communications even in a post-quantum world.[12][13][25][8]
- Crypto agility—ability to rapidly update cryptographic schemes within eSIM infrastructure—has become a design principle.

4.2 Standards and Protocol Enhancements

- **SGP.32 (2025)**: New eSIM standards enhance secure provisioning and management, crucial for 5G/IoT devices.[26]
- **GSMA TS.48 v7.0**: Fixes the test profile exploit, requiring RAM keys randomization and blocking of unverified Java Card installations.[19][24]
- **eUICC Protection Profile**: Heightened EAL4+/AVA_VAN.5 resistance for software/hardware implementations.[10]

5. Next-Gen Security Technologies

- **AI-Powered Fraud Detection**: Telecoms are embedding AI to identify anomalies in eSIM provisioning and usage.[1]
- **Biometric Verification**: Rapid expansion of biometric authentication for eSIM activation and management.[5][6][7][1]

- **5G & Network Slicing**: eSIM standards now support highly granular, secure access to 5G network slices, improving subscriber privacy and isolation.[26]
- **IoT SAFE Standard**: Secures low-power and constrained IoT environments with tamper-proof embedded secure elements.[27]

6. Security Measures and Industry Response

6.1 Frameworks, Certification, and Best Practices

Approach	Measures Adopted
GSMA Compliance & Certification	SAS-UP and SAS-SM for eUICC/software/server compliance[14][28]
Security Assurance Schemes	eUICC Security Assurance (eSA) for hardware and software verification[14]
Remote Provisioning Security	Mandated TLS for all remote provisioning, regular credential renewal[9][10][29]
Multi-Layer Authentication	Combining biometric, knowledge, and device-based verification[5][4][6]
Secure Element Protections	Hardware Root of Trust (HRoT), physical tamper resistance[27]

6.2 Incident Response: Vendors reacted to newly disclosed flaws with software patches, deprecated vulnerable test profiles, closed legacy RAM keys, and updated certification processes.[16][24][15][19]

7. Discussion: Open Challenges and Future Directions

Despite huge advances, challenges persist:

- **Legacy Device Vulnerabilities**: Billions of devices globally remain at risk until patched or replaced.[20][21][15][16][17]
- **Vendor Ecosystem Weaknesses**: Not all vendors promptly address or acknowledge Java Card flaws, risking the broader ecosystem.[18][21][22]
- **Usability vs. Security Trade-offs**: Tighter controls can impede user experience—solving this balance remains an open area for design innovation.[5]
- **Quantum Security Standardization**: Post-quantum cryptography is still evolving—widespread, interoperable deployment requires continued standardization efforts.[13][25][8][11][12]

8. Conclusion

eSIM technology is at the forefront of digital identity and global connectivity, but its security posture is constantly challenged by both sophisticated attackers and the expanding threat surface of IoT, mobile, and 5G. The past year saw alarming vulnerabilities—most notably around Kigen eUICC Java Card implementations—spur rapid industry responses, leading to stronger standards, advanced authentication, quantum-safe crypto, and enhanced compliance protocols. The drive toward higher assurance, coupled with innovations in AI and biometric security, sets a strong trajectory for trust and resilience in the eSIM ecosystem through 2025 and beyond.

References:

1. https://www.airalo.com/blog/future-of-esim-2025-and-beyond
2. https://thehackernews.com/2025/07/esim-vulnerability-in-kigens-euicc.html
3. https://motive.com/news-and-resources/sim-connectivity
4. https://terminalesim.com/top-esim-trends-you-need-to-know-in-2025/
5. https://www.thaicert.or.th/en/2025/07/16/critical-esim-vulnerability-in-kigens-euicc-cards-puts-billions-of-iot-devices-at-risk/
6. https://www.neuralt.com/news-insights/how-esim-is-revolutionizing-iot-and-enterprise-connectivity-in-2025
7. https://www.gojimobile.com/blog/esim-trends-in-2025
8. https://zendata.security/2025/07/14/esim-cloning-via-java-card-flaws-a-hidden-threat-returns/
9. https://www.telna.com/blog/android-esim-adoption
10. https://yohomobile.com/future-esim-technology-trends-2025
11. https://www.enisa.europa.eu/sites/default/files/publications/Embedded Sim Ecosystem Security Risks and Measures.pdf
12. https://security-explorations.com/esim-security.html
13. https://www.scworld.com/brief/esim-cloning-flaw-exposes-mobile-id-vulnerabilities
14. https://alertify.eu/esim-trends-for-2025/
15. https://www.verifiedmarketreports.com/blog/top-7-trends-in-esim/
16. https://www.infosecurity-magazine.com/news/iot-risk-esim-flaw-kigens-euicc/
17. https://arxiv.org/abs/2211.15323
18. https://www.gsma.com/solutions-and-impact/technologies/esim/security-analysis-of-the-consumer-remote-sim-provisioning-protocol/
19. https://www.gsma.com/solutions-and-impact/technologies/esim/wp-content/uploads/2025/07/AN-2025-07-v1.0-Preventing-misuse-of-an-eUICC-Profile-and-installation-of-malicious-Java-Card-Application.docx
20. https://www.1nce.com/en-eu/euicc-sim-card-for-iot-esim/remote-sim-provisioning-in-iot-definition-tech-aspects-and-key-players
21. https://securityaffairs.com/179894/security/experts-uncover-critical-flaws-in-kigen-esim-technology-affecting-billions.html
22. https://motive.com/remote-sim-provisioning
23. https://www.gsma.com/solutions-and-impact/technologies/esim/compliance/
24. https://www.1global.com/blog/mobile-operators/what-is-remote-sim-provisioning
25. https://www.linkedin.com/pulse/securing-esims-age-quantum-computing-case-ankit-jogi

26. https://www.globalyo.com/blog/exploring-different-esim-authentication-methods-a-comprehensive-guide/
27. https://www.idemia.com/news/idemia-and-telefonica-showcase-post-quantum-esim-technology-2025-07-18
28. https://www.globalyo.com/blog/exploring-advanced-encryption-techniques-for-esim-security/
29. https://voyeglobal.com/is-esim-safe-for-banking/
30. https://www.gsma.com/solutions-and-impact/technologies/esim/expanding-the-esim-ecosystem/
31. https://www.telefonica.com/en/transformation-handbooks/innovation-handbook/quantum-safe/quantum-safe-esim-for-utilities/
32. https://www.biometricupdate.com/202502/saudi-arabia-partners-with-valid-while-biometric-sim-card-registration-picks-up-pace
33. https://trustedconnectivityalliance.org/trusted-connectivity-alliance-updates-esim-specification-to-enhance-secure-remote-sim-provisioning-for-5g-and-constrained-iot-devices/
34. https://www.telefonica.com/en/transformation-handbooks/innovation-handbook/quantum-safe/
35. https://iot-analytics.com/role-of-esim-for-iot-better-security-simplified-roaming-easier-provisioning/
36. https://www.securityweek.com/esim-hack-allows-for-cloning-spying/
37. https://www.iotforall.com/esim-iot-challenges-opportunities
38. https://www.emnify.com/blog/iot-security
39. https://zendit.io/esim-security/
40. https://www.linkedin.com/pulse/does-hackable-esim-pose-security-risk-how-someone-can-steal-na61c
41. https://ppl-ai-code-interpreter-files.s3.amazonaws.com/web/direct-files/e2267e28761eef8cd234f840b060b803/23f13de9-2672-4c37-98e6-38c4177415ac/22052fb2.json