eSIM: SIMplifying Connectivity, Expanding the Attack Surface

Group Members

HUSSAINI Mohmmad Qasim

VOLONTERIO Luca

ADJEI Ernest

FABIAN Dandy

ELECH-423 - Mobile and Wireless Networks

Professor DRICOT Jean-Michel

Université Libre de Bruxelles

Academic Year 2025–2026

Contents

Terminology

For the purpose of this document, the following abbreviations and definitions are used.

Table 1: Key terminology used in this document

Term	Description
SIM	Subscriber Identity Module
eSIM	Embedded Subscriber Identity Module
UICC	Universal Integrated Circuit Card
eUICC	Embedded Universal Integrated Circuit Card
IMSI	International Mobile Subscriber Identity
ICCID	Integrated Circuit Card Identifier
EID	eUICC Identifier
RSP	Remote SIM Provisioning
LPA	Local Profile Assistant
SM-DP+	Subscription Manager–Data Preparation
SM-DS	Subscription Manager–Discovery Service
MNO	Mobile Network Operator
MVNO	Mobile Virtual Network Operator
PKI	Public Key Infrastructure
LTE	Long Term Evolution
NB-IoT	Narrowband Internet of Things
AUSF	Authentication Server Function
UDM	Unified Data Management
3GPP	3rd Generation Partnership Project
GSMA	GSM Association
GDPR	General Data Protection Regulation
EDPB	The European Data Protection Board
DPIA	Data Protection Impact Assessment
FCC	Federal Communications Commission
CPNI	Customer Proprietary Network Information
OEM	Original Equipment Manufacturers
LNP	Local Number Portability
AKA	Authentication and Key Agreement
MVNO	Mobile Virtual Network Operators
FISA	Foreign Intelligence Surveillance Act
ITU-T	International Telecommunications Union
SUCI	Subscription Concealed Identifier
SUPI	Subscription Permanent Identifier

1 The Evolution in Mobile Identity

1.1 Background and Motivation

Mobile connectivity is evolving beyond traditional handset-centric models as cellular networks transition from GSM and LTE toward 5G, private networks, and large-scale IoT deployments. Central to this evolution is the mobile identity layer, which enables authentication, provisioning, roaming, and service access across heterogeneous devices and networks [4]. As connectivity expands to wearables, vehicles, enterprise endpoints, and unattended IoT devices, the mechanisms used to bind identity to devices have become a critical architectural and operational concern.

The transition from physical SIM cards to eSIMs represents a fundamental shift in how mobile identity is provisioned, managed, and governed. By enabling RSP, eSIM supports software-defined identity management, dynamic operator selection, and scalable global onboarding. While these capabilities simplify connectivity and reshape deployment models, they also redistribute trust across ecosystem actors, introduce new governance challenges, and expand the attack surface of mobile networks [10]. Motivated by these developments, we study eSIM from an end-to-end perspective, examining architectural evolution alongside security, regulatory, and deployment implications in modern mobile communications.

1.2 Architectural View of SIM and eSIM

From an architectural standpoint, the defining difference between SIM and eSIM lies in how subscriber identity is bound to hardware and how subscription lifecycles are managed.

As shown in Figure 1, SIM-based systems store identifiers such as the IMSI and ICCID in a single profile bound to the removable UICC. eSIM systems, by contrast, manage multiple operator profiles within the eUICC, each uniquely associated with an EID and independently enabled or disabled. This structural decoupling of identity from physical card replacement enables dynamic, software-controlled subscription lifecycle management without modifying core network authentication mechanisms.

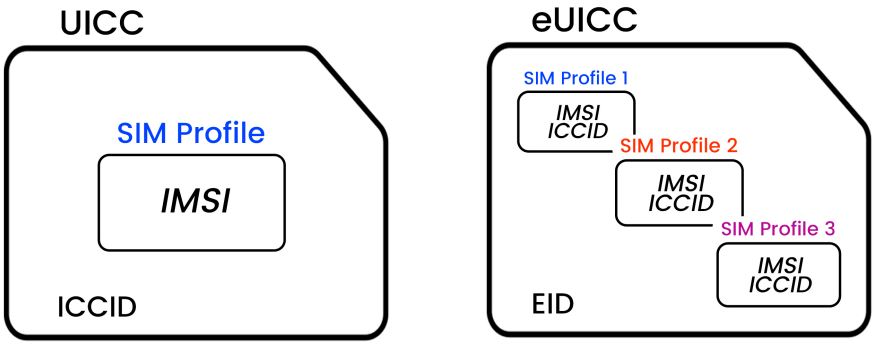

Figure 1: Comparison between the UICC architecture of SIM cards and the eUICC architecture of eSIMs, adapted from [19].

1.3 Redistribution of Trust

Although SIM and eSIM share the same underlying authentication and key agreement mechanisms defined by 3GPP [4], the introduction of eSIM fundamentally alters how trust is distributed across the mobile ecosystem. In SIM-based systems, long-term subscriber credentials are generated under MNO authority and injected into the UICC by a certified SIM vendor during manufacturing, tightly coupling trust, credential ownership, and lifecycle control to the physical supply chain.

In eSIM systems, subscription credentials are packaged as profiles by the SM-DP+ and delivered to devices using standardized RSP interfaces. Figure 2 presents the GSMA-defined consumer eSIM provisioning architecture, highlighting the roles of the eUICC, the LPA, and the subscription management infrastructure (SM-DP+ and SM-DS). This architecture introduces a network-mediated control plane for identity lifecycle management, replacing manufacturing-time personalization with runtime provisioning.

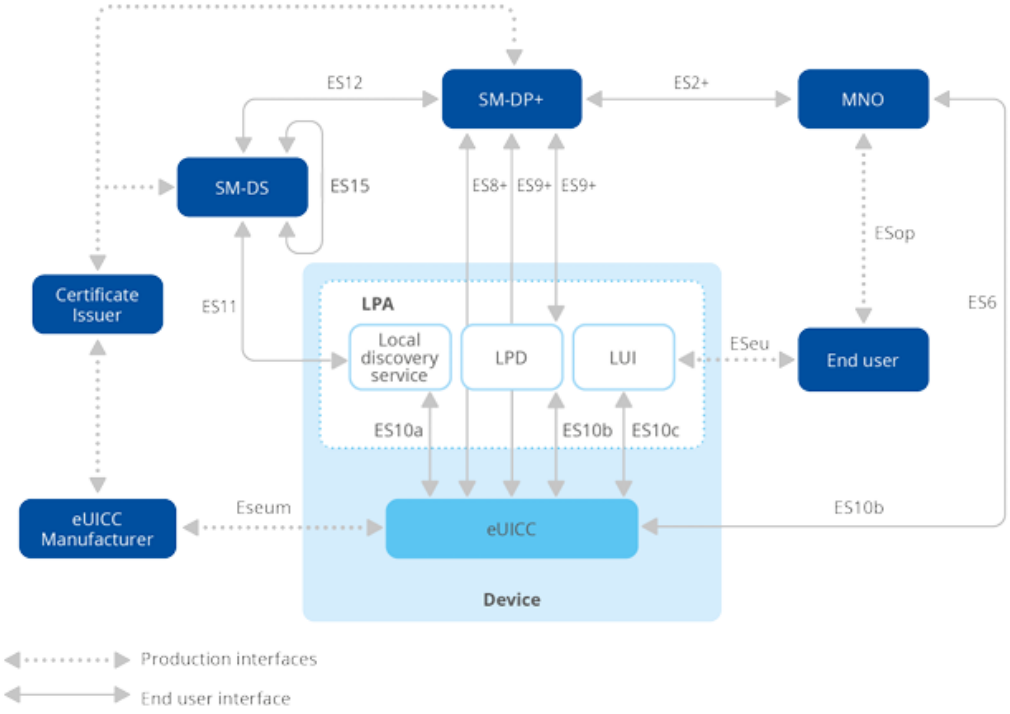

Figure 2: GSMA-defined consumer eUICC remote provisioning architecture, illustrating interactions between the device, subscription management infrastructure, certificate authorities, and mobile network operators.[2, 10].

RSP relies on multiple cryptographic protections, including profile encryption, digital signatures, and mutual authentication between the device and provisioning infrastructure. While MNOs retain authority over subscription credentials and network access, eSIM platform providers and device manufacturers play a central role in profile preparation, delivery, and lifecycle management. Recent academic analyses show that although the cryptographic primitives remain strong, the expanded provisioning workflow increases exposure to misconfiguration, implementation flaws, and abuse [19].

Consequently, the primary security impact of eSIM is not weaker cryptography, but a redistribution of trust. Control over identity lifecycle management extends beyond the MNO to include MVNOs, device OEMs, and eSIM platform providers, increasing architectural flexibility while simultaneously expanding the attack surface and complicating governance and accountability.

1.4 Integration with Modern Mobile Networks

From a network architecture perspective, eSIM primarily affects provisioning and onboarding rather than authentication procedures. Core LTE and 5G network functions, including the AUSF and UDM, consume subscriber identity in the same manner regardless of whether credentials originate from a SIM or an eSIM. As a result, the introduction of eSIM does not alter standardized authentication, mobility management, or session establishment processes in the radio access or core network.

Figure 3 provides a conceptual illustration of this architectural invariance from the network viewpoint. The figure abstracts radio access and core network components to emphasize that an eSIM-based device presents subscriber identity to the network using the same interfaces and procedures as a SIM-based device.

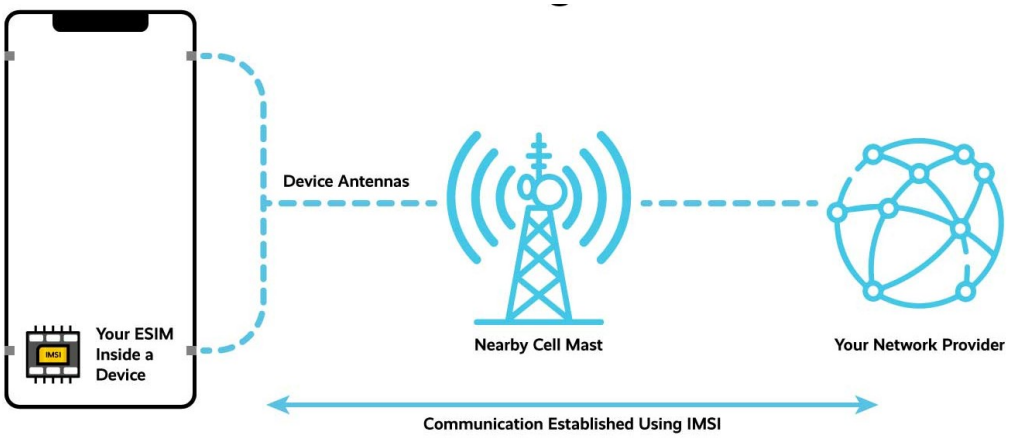

Figure 3: Conceptual illustration of eSIM-based device integration with the cellular network. From the network perspective, subscriber identity is handled identically to SIM-based devices [3].

This architectural consistency enables eSIM-based identities to integrate seamlessly with public 5G networks, private LTE/5G deployments, and IoT-oriented access technologies such as NB-IoT and LTE-M. The principal benefit of eSIM lies in enabling scalable, remote onboarding and dynamic subscription management without modifying core network security mechanisms. At the same time, increased reliance on remote provisioning infrastructure elevates the importance of securing signaling paths, provisioning channels, and inter-actor trust relationships, particularly in large-scale and unattended deployments.

2 eSIM Adoption and Ecosystem Dynamics in Global Mobile Markets

This chapter looks at how the eSIM architecture from Chapter 1 is actually showing up in the real world, not just in standards and slides. The focus is on how fast eSIM is being adopted, where it is growing, and how much this depends on the surrounding ecosystem of devices, operators, and regulation rather than on the technology alone. By looking at global and regional adoption rates and the concrete decisions made by Apple, major MNOs, and policymakers, this chapter builds the context for why the regulatory and security questions.

2.1 eSIM Adoption Rate in Consumer and IoT

Before diving into the adoption rate of eSIM, it is useful to look at the ecosystem that supports eSIM adoption. eSIM, just like SIM, heavily relies on MNOs and devices for general customers to adopt it. By 2024, the eSIM ecosystem has been quick to adapt, with around 400 operators supporting eSIM. On the device side, eSIM-enabled devices are predicted to reach around 9 billion units shipped by the end of 2030 [7].

eSIM has been in development for more than 10 years; however, market intelligence firms that focus on eSIM, such as GSMA and Counterpoint, still report a low adoption rate for the technology. By the end of 2025, eSIM adoption is only 5% globally, while the initial prediction made six years ago estimated adoption at 22% [12][17].

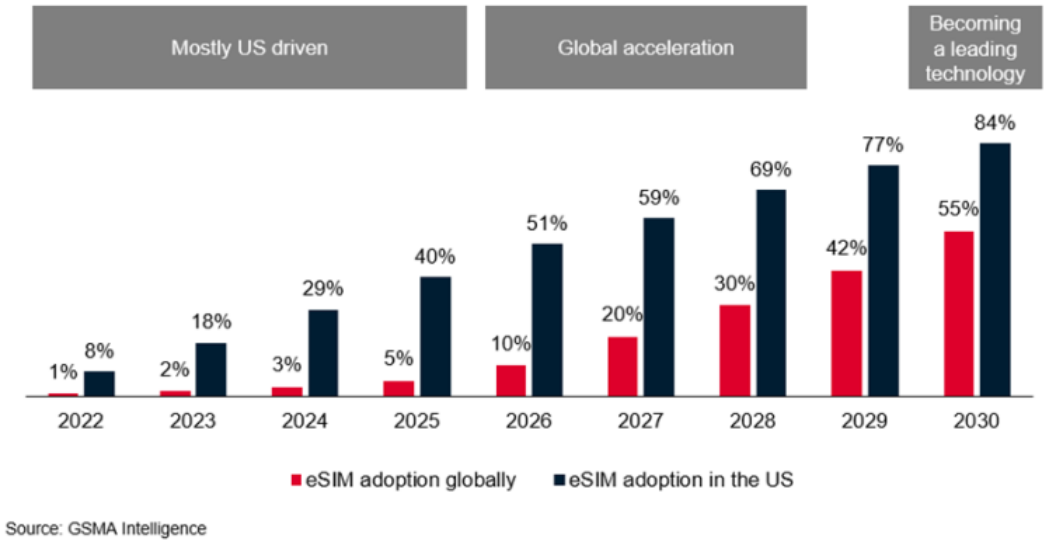

Figure 4: eSIM adoption rate Globaly and in North America [12]

eSIM not only affects the consumer SIM card market, but it also impacts the IoT market where SIM cards are widely used, accounting for over 21% of the 16.6 billion IoT devices across the world. However, the slow adoption rate is also visible in the IoT domain, where only 600 million IoT devices use eSIM, corresponding to roughly a 19% adoption rate [16].

2.2 Regional Adoption and Drivers

According to Figure 4, the adoption rate in the US is much more significant compared to the rest of the world reaching up to 40% in 2025. To understand this further, we will take a look the market between North America and Europe as both country are the leaders for eSIM. This significant difference in adoption can be pinpointed to the following five reasons:

- Device push from Apple: eSIM-only iPhone 14/15 were launched first in the US (2022), forcing all major US carriers to fully support and promote eSIM, which rapidly drove usage there.
- Simpler market structure: A few dominant US carriers can make fast, aligned decisions on eSIM rollout and UX, while Europe's highly fragmented, multi-country market slows consistent implementation and marketing.
- More flexible regulation: The US regulatory environment is described as more flexible, letting carriers move faster on digital-only activation and remote provisioning, whereas European rules emphasize consumer protection and create more complexity.
- Stronger carrier-led digital onboarding: US carriers invested early in digital-first activation flows (eSIM Carrier Activation, Quick Transfer, app-based onboarding), making eSIM setup relatively easy and pushing up adoption.
- Higher awareness triggered by eSIM-only devices: In the US, eSIM-only flagships forced both carriers and media to educate users, while in Europe overall awareness of eSIM remains low and many consumers still prioritize traditional factors (coverage, price) over eSIM flexibility, slowing uptake. [23]

These reasons significantly show that in eSIM adoption rate, the ecosystem really control how the market adoption rate is with market such as US having such great ecosystem adoption that it spillover to the consumer adoption.

The analysis above shows that eSIM adoption is not driven by technology alone but by the surrounding ecosystem of device vendors, operators, regulators, and platform providers that decide how quickly and smoothly users can move to digital identities. In many markets, a small number of powerful actors now sit in the critical path of eSIM provisioning and lifecycle management, from OEM-controlled onboarding flows to globally hosted SM-DP+/SM-DS platforms. While this concentration brings efficiency and a more consistent user experience, it also raises difficult questions about who ultimately controls mobile identity, where sensitive data is processed, and how failures or abuses in these platforms would propagate. The next sections therefore examine how this evolving governance structure intersects with regulation, data sovereignty, and privacy (Further explain in Chapter 3), before turning to the concrete security threats and attack models emerging around eSIM, iSIM, and modern mobile networks (Further explain in Chapter 4)

3 Regulation, Governance & Privacy in Next-Generation Mobile Identity

3.1 Connection to Mobile and Wireless Networks

Mobile identity is the technical key that allows a device to access the network and authenticates the user. Because this identity is part of the network access layer, the regulations discussed here directly affect how wireless networks operate and how eSIM devices connect to LTE and 5G networks. This section analyzes how laws and governance affect this technical process.

3.2 Comparison of Regulatory Frameworks (EU vs. US)

When we look at how mobile identity is regulated, we see a big difference between the European Union and the United States. This difference is very important for eSIM technology because eSIM profiles can be downloaded from anywhere in the world.

In the European Union, the main focus is on protecting the fundamental rights of the user. The General Data Protection Regulation (GDPR) [1] is the key law here. According to Article 4 of the GDPR, personal data includes any information that can identify a person, such as location data or an online identifier. This means that the IMSI (International Mobile Subscriber Identity) or the profile data inside an eSIM is considered personal data. Therefore, mobile network operators (MNOs) must follow strict rules when they process this data. For example, Article 44 says that if data is transferred to a country outside the EU to the third country, the protection level must not be undermined. The European Data Protection Board (EDPB) [20] reinforces this. EDPB states that transferring data to third countries cannot be a way to undermine the protection provided in the EU.

Because eSIM uses new technology that involves cross-border data flows, it can be considered high-risk processing. Article 35 of the GDPR [1] states that when a type of processing uses new technologies and is likely to result in a high risk to the rights of people, the controller must do an assessment first. This is called a Data Protection Impact Assessment (DPIA). For mobile operators deploying eSIM, this means they cannot just install the server and forget it. They must analyze the risks of the provisioning logs, the profile metadata, and the device identifiers leaving the EU before they start the service.

In the United States, the approach is different. The focus is more on consumer protection against fraud rather than a broad fundamental right to privacy. The Federal Communications Commission (FCC) [11] uses rules related to Customer Proprietary Network Information (CPNI). Under Section 222 of the Communications Act, carriers must protect the confidentiality of customer information. Recently, the FCC updated these rules to fight against specific frauds like SIM swap and Port-out fraud. A SIM swap happens when a bad actor convinces a provider to transfer a victim's service to a SIM the attacker controls. Port-out fraud occurs when the bad actor moves the victim's phone number to a different wireless provider. The new FCC

rules require wireless providers to use secure methods to verify a customer's identity before transferring a number to a new device or provider.
The US system is also more fragmented compared to the EU. While the EU has one big law (GDPR) for everyone, the US has different rules for different sectors. For mobile networks, the primary authority is the FCC. The FCC Fact Sheet [11] explains that they set baseline requirements for the mobile industry to stop fraud, but they give providers flexibility on how to do it. This contrasts with the EU approach, where the rules on data transfer are very strict and apply to everyone equally.

3.3 Data Sovereignty and Remote Provisioning

The eSIM changes how we think about Data Sovereignty. In the past, a physical SIM card was bought in a specific country. Now, an eSIM profile can be downloaded over the air (OTA) from a server located in another country. This creates a legal challenge regarding where the data actually lives.
To understand the privacy risk, we must look at how the eSIM works technically. The ENISA report [10] explains the architecture of the consumer solution. It relies on two main servers: the SM-DP+ (Subscription Manager - Data Preparation) and the SM-DS (Subscription Manager - Discovery Server). How does the process work? The SM-DP+ securely creates and stores the MNO profiles. The SM-DS acts like a notification center that helps the device find the SM-DP+. When a user scans a QR code, the device (using a tool called LPA) connects to these servers to download the profile package. This process generates metadata like timestamps, device IDs, and profile types. If these servers are located outside the user's country, this sensitive data leaves the country's jurisdiction.
The EDPB recommendations [20] explain that when personal data is transferred to a third country, we must check if the laws of that country allow government surveillance that goes beyond what is necessary. For example, if a European user downloads an eSIM profile from a server in the US, US laws like Section 702 FISA might allow US authorities to access that data. It is important to note that FISA 702 [20] applies specifically to data held by US electronic communication service providers, which allows the government to access communications of non-US persons located outside the US. The EDPB [20] warns that if the third country's laws do not respect the essence of the fundamental rights, the transfer might need to be stopped or extra measures must be used.
ENISA warns about a specific risk here; security of third-party dependencies. Many mobile operators (MNOs) cannot afford to build their own eSIM platforms. Instead, they use third-party providers who are often large global vendors. This means the governance of the eSIM ecosystem shifts away from the national operator to global tech companies. ENISA [10] states that MNOs should include specific security clauses in contracts, but the risk remains that the keys and logs are managed by actors in different jurisdictions.
To handle these risks, the EDPB [20] gives a detailed roadmap for companies that send

personal data outside the EU. We think these steps are very useful for understanding eSIM compliance because using a foreign SM-DP+ is essentially a data transfer. Based on the EDPB recommendations, the steps are:

1. **Know your transfers:** Operators must map exactly where their data goes. They must know if the SM-DP+ is hosted in the EU or elsewhere.

2. **Identify the transfer tools:** They must verify the legal basis, for example, if they are using Standard Contractual Clauses (SCCs).

3. **Assess effectiveness:** They must assess if the law of the third country (like US surveillance laws) impinges on the protection of the data.

4. **Adopt supplementary measures:** If the foreign law is risky, operators must add extra protections. The EDPB suggests technical measures like strong encryption or split processing so that no single server can see the full data.

5. **Procedural steps:** Take necessary formal steps depending on the tool used.

6. **Re-evaluate:** Because hosting locations and laws change, this must be checked continuously.

3.4 Identity Ownership and Portability

With eSIM, the question of (who owns the identity?) becomes complicated. Is it the user, the Mobile Network Operator (MNO), or the device manufacturer (OEM)?
According to the ITU-T Recommendation E.164, [15] the international telephone number is a public resource used to identify networks and subscribers. It is not the private property of the operator. The numbering plan allows users to be identified globally. However, in the eSIM model, the profile is software. The ENISA report [10] explains that MNOs use a locking profile policy (like the *CannotBeDisabled* rule) to lock a device to their network. This restricts the user's ownership. If a MNO uses a modified policy, they can prevent the user from switching to another provider, effectively claiming ownership of the profile.
There is also a shift in power toward the Original Equipment Manufacturers (OEMs), like phone makers. In the eSIM ecosystem, the device manufacturer is responsible for implementing the Local Profile Assistant (LPA) on the device. This means the user relies on the phone maker's software to download and manage the operator's profile. This creates a new governance dynamic where the OEM controls the door to the network, potentially reducing the direct relationship between the user and the operator.
On the other hand, regulators try to give ownership back to the user. The FCC report [11] emphasizes Local Number Portability (LNP). FCC states that consumers must be able to keep their phone numbers when switching providers. To balance security and portability, the FCC now requires providers to let customers lock their accounts to prevent fraudulent transfers, but they also

require providers to unlock them promptly when the customer asks. This confirms that the regulator views the number as belonging to the user, even if the MNO tries to control the technical profile.

3.5 Regulatory Gaps

This section does not analyze the attacks technically, because that is covered in another part of the project. Here we only show the regulatory and privacy implications. We identified several gaps where current regulations struggle to keep up with eSIM technology.

1. **Technical Gaps (Signaling Attacks):** While laws like GDPR demand a high level of security and privacy, they do not specify how signaling protocols should be fixed or updated. Regulations require operators to protect user privacy, but they often do not translate into concrete obligations to address specific weaknesses at the protocol or implementation level. As a result, there is a gap between legal expectations and what is actually enforced in mobile networks. Regulators frequently lack the technical mechanisms or enforcement tools to require immediate corrections when privacy risks are discovered.

2. **Resellers and MVNOs:** The FCC report [11] explicitly extends its new anti-fraud rules to resellers of commercial mobile radio service. This is crucial because the mobile ecosystem includes many Mobile Virtual Network Operators (MVNOs) who resell services without owning the underlying infrastructure. These actors often depend on upstream MNOs or third-party vendors for eSIM provisioning. Without explicit regulatory coverage, they could become a weak link in the privacy and security chain, as they may lack the resources or authority to effectively audit third-party providers.

3. **Legacy Protocols:** The transition to next-generation mobile networks is slow, and older network technologies remain widely deployed. Regulatory frameworks often focus on new standards and future deployments, while the continued use of legacy protocols receives less attention. This creates a regulatory gap where outdated technologies with known privacy weaknesses remain operational, even though regulations emphasize strong privacy protection and security requirements.

3.6 Privacy Risks: Metadata and Location

eSIM technology introduces specific privacy risks related to how mobile networks handle metadata. In the EU legal framework, metadata is considered highly sensitive because it can reveal behavioral patterns and location information about individuals.
One major risk concerns location-related metadata. Even when user identities are protected at a high level, metadata can still allow third parties to infer sensitive information about a user's presence or movement. From a regulatory perspective, this raises concerns about compliance with data minimization and purpose limitation principles under EU data protection law [20].

Another privacy risk relates to network signaling practices that generate observable metadata during normal operation. These processes occur without user awareness, which challenges the principles of transparency and informed consent required by privacy regulations. Such forms of metadata exposure can undermine location privacy even when the content of communications remains protected [1].

Finally, there is the risk of Profile Lifecycle Visibility. The ENISA report [10] highlights risks related to how eSIM profiles are created, managed, and stored. Limited transparency and control over profile lifecycle events can allow misuse of provisioning mechanisms in ways that harm users, including denial of service. From a regulatory perspective, this shows that governance of eSIM profile management is a critical privacy surface that requires stronger oversight and accountability mechanisms.

4 Evolving Attack Models in Mobile Communications

The transition from physical SIM cards to remotely provisioned eSIM and integrated iSIM reshapes where and how mobile identity can be attacked. Rather than weakening the underlying AKA protocols, these technologies redistribute trust from manufacturing-time personalization toward runtime provisioning platforms, device software, and cloud-based management infrastructure [10, 19]. At the same time, legacy SIM processes, emerging IoT provisioning standards, and 4G/5G signalling-plane weaknesses remain part of the effective threat surface, so modern attack models must consider both the identity module and the surrounding protocol and software ecosystem [14].

4.1 Legacy SIM Threats

Before the introduction of eSIM, attackers primarily targeted legacy SIM cards through social engineering, over-the-air (OTA) management channels, and smart-card implementation weaknesses [10]. These threats remain relevant because physical SIMs still coexist with eSIM and iSIM across many 4G and 5G deployments, and because many operational processes (e.g., number portability, customer support) were designed around the legacy model [10].

A first category consists of SIM swap fraud and related social-engineering attacks, where adversaries trick or bribe operator staff into reassigning a victim's number to an attacker-controlled SIM, enabling interception of one-time passwords and takeover of SMS-based multi-factor authentication [11]. A second category exploits SIM Toolkit and OTA update mechanisms, where special SMS messages are used to install or update applets on the SIM; if these channels are insufficiently authenticated or validated, malicious or vulnerable applets can be deployed to execute privileged operations such as sending SMS, initiating calls, or modifying security parameters [10]. Finally, physical and side-channel attacks target the UICC itself as a secure element: under laboratory conditions, power and timing analysis can be used to extract or weaken cryptographic keys, demonstrating that the hardware root of trust is robust but not infallible [10].

4.2 eSIM-Specific Threats and Supply-Chain Risks

With eSIM, the most significant shift in the attack surface comes from Remote SIM Provisioning (RSP) and the introduction of subscription management entities such as SM-DP+ and SM-DS [19, 10]. In contrast to SIM cards that are personalized in a factory, eSIM profiles are generated, encrypted, and delivered at runtime by these platforms, which now hold profile packages, keys, logs, and device metadata for large user populations [19, 10]. This turns the provisioning infrastructure and its cloud supply chain into high-value targets whose compromise directly impacts the integrity, availability, and privacy of mobile identities [10].

A first class of eSIM-specific threats involves rogue resellers and opaque intermediaries, such as travel eSIM providers or small MVNOs, that mediate access to foreign networks [19]. These entities may rely on third-party data centers and cloud services in jurisdictions with weaker privacy protections, creating situations where user traffic or metadata is routed through infrastructure outside the control of the home operator [19]. Even when radio and core signalling are correctly secured, this effectively introduces a "man-in-the-middle" at the service layer, where traffic analysis, profiling, and data monetization become possible without violating the letter of 3GPP security specifications [19, 10].

More interestingly from an architectural perspective, eSIM enables new denial-of-service and integrity attacks that exploit the multi-profile lifecycle itself. The ENISA report discusses "Inflated profile" scenarios, in which a malicious or careless operator requests the creation of a very large profile that fills up the eUICC's non-volatile memory, preventing users from adding new profiles or performing normal lifecycle operations [10]. The underlying architectural fault is that the eSIM model delegates profile packaging to SM-DP+ and operators, but does not enforce strong device-side quotas or per-tenant memory isolation; if the device and home MNO do not validate profile size or enforce strict limits, a single oversized profile can effectively lock the user into a specific provider and create a persistent identity-layer denial of service [10, 19].

A related class of attacks targets profile lifecycle visibility and residual data. Empirical analyses show that some commercial platforms mishandle the deletion phase, leaving residual keys, identifiers, or detailed provisioning logs even after a profile is flagged as removed [19, 10]. Architecturally, the eSIM ecosystem separates backend state (SM-DP+/SM-DS databases) from on-device state (eUICC storage), but does not prescribe uniform, provably secure erasure semantics across all actors [10]. An insider or an attacker who compromises the provisioning backend can therefore correlate historical profile installations, infer which devices moved between operators, or attempt unauthorized re-provisioning based on stale identifiers, turning lifecycle metadata into a long-term privacy and integrity vulnerability rather than a purely operational log [19]. These examples illustrate how eSIM redistributes trust from tamper-resistant cards toward distributed provisioning backends and device software, and how faults in that architecture can be exploited even when classical SIM authentication remains cryptographically sound [10, 19].

4.3 iSIM: Hardware Integration and Side-Channel Risks

The transition to Integrated SIM (iSIM) further evolves the threat model by moving SIM functionality from a discrete secure element (the eUICC) into a Tamper-Resistant Element integrated on the main System-on-Chip (SoC) [6]. This integration reduces bill-of-materials cost, board space, and power consumption, and aligns with industry trends toward hardware enclaves and trusted execution environments, but it also tightens the coupling between the identity module and the rest of the device hardware [6].

Unlike a discrete eSIM, an iSIM often shares power rails, clocks, and potentially cache and interconnect resources with the application processor or baseband subsystems, which increases the risk that malware running on the application processor could mount side-channel attacks against the iSIM, attempting to infer cryptographic keys from power consumption, timing, or electromagnetic emissions [21]. In addition, the logical isolation of the iSIM typically relies on hardware firewalls or secure enclave mechanisms; if these isolation boundaries are misconfigured or contain implementation flaws, "noisy neighbor" effects on the SoC can be exploited to inject faults into security-critical operations, such as key generation or authentication checks, thereby weakening the effective security guarantees of the integrated identity module [6]. In this work, however, iSIM is treated mainly as a forward-looking variant, and detailed side-channel analysis remains out of scope compared to eSIM.

4.4 IoT Provisioning Shift and Authentication Gaps

The IoT ecosystem is in the middle of a transition from the legacy M2M eSIM standard (SGP.02) toward the newer EIoT standard (SGP.32), and this shift has direct implications for attack models [10]. SGP.02 heavily relied on SMS-based triggers and proprietary integration between operators and connectivity management platforms, which exposed clear-text signalling and made it difficult to deploy fine-grained security controls at scale [10]. SGP.32 replaces this with an IP-centric model centered on the eSIM IoT Remote Manager (eIM), which orchestrates profile downloads and updates over secure data channels [5].

While the new model improves scalability and flexibility, it also concentrates control in the eIM. If an attacker compromises an enterprise eIM instance or its credentials, they can silently push profile changes, disable connectivity for large device fleets, or redirect devices to unauthorized networks without direct operator involvement [5]. Moreover, IoT application authentication typically relies on frameworks such as AKMA (Authentication and Key Management for Applications) on top of the network-layer identity, and recent analyses suggest that naive AKMA deployments can suffer from linkability and metadata exposure, allowing adversaries to correlate service usage across sessions or devices [24]. These issues show that even when eSIM-based identity is robust, higher-layer authentication and key management must provide comparable privacy guarantees to avoid reintroducing linkability and large-scale abuse [24].

4.5 Advanced 5G Signalling and Availability Attacks

Even when SIM, eSIM, or iSIM credentials are stored securely, the 4G/5G control plane remains a rich attack surface, especially in the pre-authentication and radio resource control phases [14]. Recent work has demonstrated that carefully crafted signalling messages can be used to degrade availability, force downgrades, or reintroduce legacy vulnerabilities [18, 9].

For example, the SNI5GECT framework shows that an adversary operating a rogue or misconfigured base station can inject malicious control messages into the early 5G NR connection establishment to trigger denial-of-service conditions or force devices to fall back from 5G to 4G, after which known 4G privacy weaknesses, such as those exploited by paging-based attacks, become applicable again [18, 14]. Beyond simple wideband jamming, location-aware denial-of-service techniques such as GLaDOS selectively disrupt connectivity only when a target device enters a specific geographic region, creating "black holes" for communication that are difficult to detect because service appears normal elsewhere [9]. In this sense, signalling-plane attacks are orthogonal to eSIM but interact with it: secure identity provisioning does not prevent an attacker from abusing radio procedures to undermine availability and privacy [14].

4.6 Implementation Flaws in Baseband and Core Networks

Modern attack models must also account for implementation flaws in both device-side baseband stacks and the virtualized 5G core. Protocol specifications may offer strong theoretical security, but real-world code often contains memory-safety bugs, state-machine inconsistencies, and error-handling issues that can be exploited over the air [13, 8].

On the device side, large-scale fuzzing of LTE and 5G baseband implementations has revealed memory corruption and logic errors in PHY/MAC and RRC processing, allowing attackers to trigger device crashes or potentially execute code by sending malformed radio frames from a nearby transmitter [13]. On the network side, the move to a Service-Based Architecture (SBA) in the 5G Core means that functions such as the AMF and SMF are implemented as microservices communicating over HTTP/2 and JSON. The CORECRISIS study highlights that inconsistent state handling and insufficient input validation in these services can be abused to bypass parts of the authentication flow, hijack sessions, or cause network-wide denial of service through crafted sequences of API calls [8]. These results emphasize that secure mobile identity requires not only robust SIM, eSIM, and iSIM designs, but also careful hardening of the entire protocol and implementation stack [8, 13].

4.7 Comparing Threat Surfaces Across Deployment Contexts

The evolution from SIM to eSIM and iSIM affects consumer, enterprise, and IoT deployments in different ways, leading to distinct, context-dependent threat surfaces [10, 19]. In consumer scenarios, eSIM adoption shifts many attacks toward end users and retail processes: SIM swap fraud, phishing with malicious QR codes, and opaque travel eSIM offers exploit user-

facing flows and customer support procedures rather than purely cryptographic weaknesses [11, 19]. Enterprises, by contrast, typically centralize eSIM lifecycle management through mobile device management (MDM) systems and direct integrations with operator APIs, which reduces individual user exposure but concentrates risk in a small number of highly privileged management platforms [19].

IoT deployments operate at much larger scale with unattended devices and increasingly rely on SGP.32-based provisioning and external eIM platforms, so the main attack vectors shift toward the provisioning and management layer: a single compromise of the eIM or misconfiguration of profile policies can simultaneously affect thousands of devices, and remediation is complicated by limited physical access and constrained interfaces [10, 5, 24]. Across all three domains, signalling-plane attacks and implementation flaws in baseband and core components remain a shared concern, but eSIM-specific lifecycle and supply-chain issues determine how easily attackers can translate those lower-layer weaknesses into persistent identity compromise or large-scale service disruption [14, 18, 13, 10].

5 Methodology: Use of AI Assistants

This report was prepared with the assistance of Artificial Intelligence (AI) tools to enhance the efficiency of the literature review and synthesis process. The use of AI was strictly limited to the following scopes:

5.1 Literature Discovery and Parsing

AI tools were utilized to parse large volumes of conference proceedings, specifically the Table of Contents for the *34th USENIX Security Symposium* (2025). The AI assisted in keyword matching and semantic analysis to identify relevant papers operating within the specific domain of mobile security (e.g., 5G signaling, eSIM, and baseband fuzzing) from a dataset of hundreds of unrelated submissions [22].

5.2 Report Structuring and Polishing

The report was created using Latex overleaf, to ease the use of this tools in creating the report we used AI in helping generating Latex-ready format such as citation, picture, table, etc. We also use AI to help translate our idea to power point format or Latex-power point format.

5.3 Summarization and Technical Synthesis

Given the technical density of the selected primary sources, AI was employed to generate initial summaries of long-form research papers. This included:

- Extracting core threat models from complex architectural diagrams in papers such as *CORECRISIS* and *SNI5GECT* [8, 18].

- Synthesizing disparate vulnerabilities—ranging from physical layer fuzzing in *LLFUZZ* [13] to logic flaws in IoT management—into cohesive categories.

References

[1] General data protection regulation (gdpr). https://gdpr-info.eu/. Accessed: 2023.

[2] GSMA sgp.22: Remote sim provisioning (rsp) architecture for consumer devices. Technical Report SGP.22, GSMA, 2023. Defines the normative consumer eUICC remote provisioning architecture.

[3] GSMA esim architectures: Consumer and iot. Technical report, GSMA, 2024. Provides conceptual illustrations of eSIM device connectivity and eUICC integration.

[4] John Ardis and et al. Security architecture for gsm networks. *IEEE Communications Magazine*, 41(2):90–96, 2003.

[5] BICS. Sgp.32 explained: Next-gen esim for enterprise iot. White paper, September 2025.

[6] Cavli Wireless. What is isim? 2025 guide to integrated sim vs. traditional sim cards, March 2025.

[7] Counterpoint Research. Over 9 billion esim-capable devices to be shipped by 2030. https://counterpointresearch.com/en/insights/over-9-billion-esim-capable-devices-to-be-shipped-by-2030, 2024. Accessed: 13 January 2026.

[8] Yilu Dong, Tianchang Yang, Abdullah Al Ishtiaq, Syed Md Mukit Rashid, Ali Ranjbar, Kai Tu, Tianwei Wu, Md Sultan Mahmud, and Syed Rafiul Hussain. CORECRISIS: Threat-guided and context-aware iterative learning and fuzzing of 5g core networks. In *Proceedings of the 34th USENIX Security Symposium*, 2025.

[9] Simon Erni, Martin Kotuliak, Richard Baker, Ivan Martinovic, and Srdjan Capkun. GLaDOS: Location-aware denial-of-service of cellular networks. In *Proceedings of the 34th USENIX Security Symposium*, 2025.

[10] European Union Agency for Cybersecurity. Embedded sim ecosystem: Security risks and measures. Technical report, ENISA, March 2023. Used for architectural illustration only.

[11] Federal Communications Commission. Protecting consumers from sim swap and port-out fraud (report and order and further notice of proposed rulemaking). https://docs.fcc.gov/public/attachments/DOC-397990A1.pdf, October 2023. WC Docket No. 21-341, FCC-CIRC2311-04.

[12] GSMA. esim-only has arrived: what operators do next will define their future. https://www.gsma.com/solutions-and-impact/industry-services/gsma_resources/esim-only-has-arrived-what-operators-do-next-will-define-their-future/, 2025. Accessed: 13 January 2026.

[13] Tuan Dinh Hoang, Taekkyung Oh, CheolJun Park, Insu Yun, and Yongdae Kim. LL-FUZZ: An over-the-air dynamic testing framework for cellular baseband lower layers. In *Proceedings of the 34th USENIX Security Symposium*, 2025.

[14] Syed Rafiul Hussain, Mitziu Echeverria, Omar Chowdhury, Ninghui Li, and Elisa Bertino. Privacy attacks to the 4g and 5g cellular paging protocols using side channel information. *Network and distributed systems security (NDSS) symposium2019*, 2019.

[15] International Telecommunication Union. Recommendation itu-t e.164: The international public telecommunication numbering plan. Recommendation, ITU-T, November 2010.

[16] IoT Analytics. The role of esim for iot: Better security, simplified roaming, and easier provisioning. https://iot-analytics.com/role-of-esim-for-iot-better-security-simplified-roaming-easier-provisioning/, 2024. Accessed: 13 January 2026.

[17] Peter Jarich and Pablo Iacopino. Travel esim: a passport to growth for esim among mnos? https://www.gsmaintelligence.com/blogs/travel-esim-a-passport-to-growth-for-esim-among-mnos, 2024. Accessed: 13 January 2026.

[18] Shijie Luo, Matheus Garbelini, Sudipta Chattopadhyay, and Jianying Zhou. SNI5GECT: A practical approach to inject anrchy into 5g nr. In *Proceedings of the 34th USENIX Security Symposium*, 2025.

[19] Mohammad Motallebighomi, Amir Houmansadr, and Mathy Vanhoef. Security analysis of the esim ecosystem. In *Proceedings of the USENIX Security Symposium*, 2025.

[20] EDPB Recommendations. 01/2020 on measures that supplement transfer tools to ensure compliance with the eu level of protection of personal data. *European Data Protectin Board*, 2020.

[21] Secure-IC. Introduction to side-channel attacks (sca) on socs, 2021. Foundational reference for SoC side-channel risks.

[22] USENIX Association. Proceedings of the 34th usenix security symposium: Table of contents, 2025. Source document used for AI-assisted literature discovery.

[23] WDS Sicap. What european mnos can learn from us carriers' esim strategies. https://wds-sicap.com/news-events/what-european-mnos-can-learn-from-us-carriers, 2024. Accessed: 13 January 2026.

[24] Yang Yang, Guomin Yang, Yingjiu Li, Minming Huang, Zilin Shen, Imtiaz Karim, Ralf Sasse, David Basin, Elisa Bertino, Jian Weng, Hwee Hwa Pang, and Robert H.

Deng. AKMA+: Security and privacy-enhanced and standard-compatible akma for 5g communication. In *Proceedings of the 34th USENIX Security Symposium*, 2025.