Machine Translated by Google
RCMOS – Multidisciplinary Scientific Journal The Knowledge.
ISSN: 2675-9128. São Paulo-SP.

Year VII, v.2 2026 | Submission: 09/30/2026 | Accepted: 10/03/2026 | Publication: 10/06/2026

International roaming on 5G standalone networks

International roaming in 5G standalone networks

International roaming on independent 5G networks

Danyell Teixeira Soares

Telecommunications engineer with 16 years of experience. MBA in Business Management from Fundação Getulio Vargas (FGV-SP, 2015). Bachelor's degree in Electrical Engineering with an emphasis in Telecommunications from Pontifícia Universidade Católica de São Paulo (PUC-SP, 2008).

Summary

This article investigates the architectural mechanisms, security protocols, and governance requirements necessary to ensure international service continuity in 5G Standalone (5G SA) networks.
This study examines the differentiation between Home Routed (HR) and Local Breakout (LBO) topologies, the role of the Security Edge Protection Proxy (SEPP) at the inter-PLMN edge, and the protection of the N32 interface via 3GPP TS 29.573 specifications. It also analyzes the subscriber identity privacy scheme based on SUPI encryption in SUCI, mitigating historical tracking vulnerabilities.
The methodology is based on an analytical review of 3GPP standards (Release 18), GSMA specifications (NG.113), ENISA reports, and peer-reviewed scientific articles. It concludes that the operational success of 5G roaming depends on a rigorously validated point-to-point trust chain through bilateral testing and partner-segmented observability.
Keywords: 5G Roaming. Home Routed. Location Breakout. SEPP. N32 interface. SUCI.

Abstract

This paper investigates the architectural mechanisms, security protocols, and governance frameworks required to ensure international service continuity in 5G Standalone (5G SA) networks. It details the operational differences between Home Routed (HR) and Local Breakout (LBO) topologies, the role of the Security Edge Protection Proxy (SEPP) at the inter-PLMN boundary, and the protection of the N32 interface according to 3GPP TS 29.573 specifications. It also analyzes subscriber identity privacy mechanisms based on encrypting the SUPI into a SUCI, mitigating legacy tracking vulnerabilities. The methodology relies on an analytical review of 3GPP Release 18 standards, GSMA guidelines (NG.113), ENISA threat reports, and peer-reviewed scientific literature. The study concludes that operational success in 5G roaming depends on an end-to-end chain of trust validated by bilateral testing and partner-segmented observability.
Keywords: 5G Roaming. Home Routed. Location Breakout. SEPP. N32 Interface. SUCI.

1. Introduction

International roaming in mobile telecommunications networks is the cornerstone that enables continuity. global range of voice, messaging, and data services for users on the move outside their networks. origin (Home Public Land Mobile Network - HPLMN). In legacy network generations (2G, 3G and 4G), signaling between partner networks relied heavily on the SS7 and Diameter protocols, transported by traffic exchange networks known as IPX (IP Exchange) (BASIN et al., 2018; ENISA, 2020).

This article is published in open access under the Creative Commons Attribution license, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Machine Translated by Google

Year VII, v.2 2026 | Submission: 09/30/2026 | Accepted: 10/03/2026 | Publication: 10/06/2026

However, the legacy signage architectures suffered from serious structural vulnerabilities.
The SS7 and Diameter protocols were originally conceived under the naive premise that the network of
IPX transport was an implicitly trusted environment. This vulnerability allowed malicious actors to access the service.
carried out attacks involving source spoofing, unauthorized interception of
Calls and SMS messages, and real-time tracking of subscribers' geographic location.
(ENISA, 2020).
The introduction of 5G Standalone (5G SA) radically alters this scenario by replacing the protocols.
legacies of Service-Based Architecture (SBA). In 5G SA, all communication of the plan of
Control between the visited network (Visited PLMN - VPLMN) and the home network (HPLMN) becomes
handled through RESTful API calls over HTTP/2, requiring new paradigms for the
protection of inter-operator borders (3GPP, 2024c; GSMA, 2024).
To ensure the security of the inter-PLMN roaming ecosystem, the 3GPP TS 29.573 standard defines
The Security Edge Protection Proxy (SEPP) is a mandatory edge function. SEPP acts as the...
Single entry and exit point for control plane signaling, protecting the internal topology.
from the operator and managing the encryption of messages transmitted through the N32 interface.
(3GPP, 2024c).
The N32 interface implements the PRINS (Protocol-specific Application Layer Security) protocol, a
A crucial innovation that resolves the impasse between end-to-end encryption and the need for intermediaries.
The IPX network allows users to modify certain transport headers. This ensures the integrity of the data.
and confidentiality of user data, allowing only explicitly stated modifications.
authorized by signage contracts.
The aim of this article is to thoroughly examine the roaming architecture in 5G SA, analyzing
data transport topologies, the role of SEPP in the N32 interface, the cryptographic scheme of
Identity privacy (SUPI/SUCI), multi-vendor interoperability and models of
Bilateral governance. The analysis relies strictly on the official 3GPP specifications and guidelines.
from GSMA and high-impact scientific literature.

2 Methodology

This study is based on an analytical and systematic review of the technical literature.
Standardized and scientific knowledge specializing in mobile network security and telecommunications architecture.
The selection process for the documentary corpus was guided by methodological rigor and verification.
authority of the sources.

This article is published in open access under the Creative Commons Attribution license, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Machine Translated by Google

Year VII, v.2 2026 | Submission: 09/30/2026 | Accepted: 10/03/2026 | Publication: 10/06/2026

The first axis of the survey covers the primary normative specifications published by
3GPP (Release 18). The TS 23.501 (general architecture) documents were analyzed in depth.
TS 23.502 (procedural flows), TS 29.573 (PLMN network interconnection via SEPP) and TS
33.501 (5G security architecture and procedures).
The second methodological axis encompasses the operational guidelines and orientations consolidated by
International Association of Mobile Operators (GSMA). The focus was on the GSMA NG.113 standard (5GS).
Roaming Guidelines), which establishes the practical requirements for the implementation of agreements
Bilateral roaming in fifth-generation networks.
The third axis includes technical threat assessment reports and frameworks for...
cybersecurity guidelines issued by governmental and international bodies, with particular emphasis on
Publications from the European Union Agency for Cybersecurity (ENISA - *5G Threat Landscape*)
and NIST (Cybersecurity Framework 2.0).
The fourth axis comprises peer-reviewed scientific articles presented at conferences.
A benchmark in the field of information security and mobile networks, such as the ACM SIGSAC Conference.
on Computer and Communications Security (CCS) and selected IEEE/Elsevier journals
through direct validation of the DOI.
The synthesis of the information was organized into an analytical matrix focused on four dimensions.
Operational aspects: user plane topology, control plane security on the N32 interface,
subscriber privacy encryption and bilateral governance requirements. The final text was
Fully standardized according to ABNT's scientific writing and citation guidelines.

3 Architectural Models for 5G Roaming

Establishing a roaming session in 5G SA requires precise coordination between functions.
control and transport networks located on the visited network (VPLMN) and on the subscriber's home network.
(HPLMN). 3GPP standardizes two architectural models for handling data traffic.
user: Home Routed (HR) and Local Breakout (LBO) (3GPP, 2024a; GSMA, 2024).
In the Home Routed (HR) model, the primary anchoring of the user plane remains in the network of
originates via the H-UPF (Home UPF). When the user accesses the network on the VPLMN, the traffic from
Data is received by the local V-UPF and encapsulated in a GTP-U tunnel that traverses the N9 interface.
inter-PLMN via the IPX network until reaching the H-UPF in the country of origin, from where the traffic is finally...
routed to the Internet (3GPP, 2024a).

This article is published in open access under the Creative Commons Attribution license, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Machine Translated by Google
RCMOS – Multidisciplinary Scientific Journal The Knowledge.
ISSN: 2675-9128. São Paulo-SP.

Year VII, v.2 2026 | Submission: 09/30/2026 | Accepted: 10/03/2026 | Publication: 10/06/2026

Figura 1 - Arquitetura de Interconexão e Segurança de Roaming 5G SA com SEPP

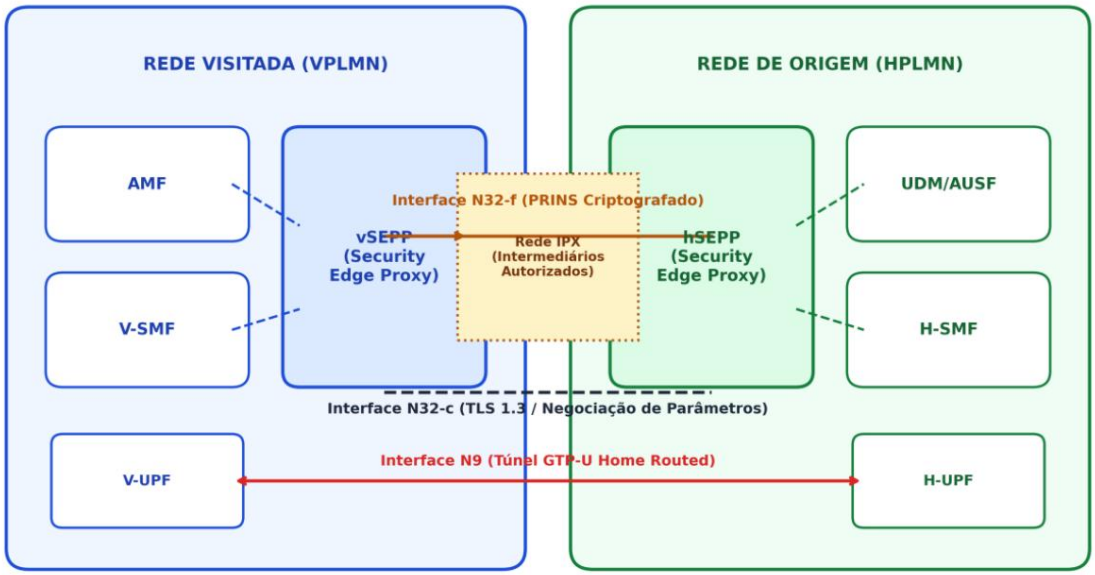


Figure 1 – 5G SA Roaming Interconnection and Security Architecture with SEPP.

Source: Prepared based on 3GPP TS 29.573 (2024).

HR architecture is the widely preferred choice for telecommunications operators for Conventional data services. Centralizing the user plan in HPLMN ensures control. absolute regarding the application of real-time pricing policies, consumption auditing and strict compliance with local regulatory requirements for lawful interception (*lawful interception*), without depending on the policies of the visited partner.

However, the main disadvantage of the Home Routed model is the additional latency introduced by Circular routing (*tromboning*). Data traffic is forced to travel geographically to the country. origin and return to destination, which may make real-time applications that require it unfeasible. Ultra-low latency (URLLC), such as advanced industrial automation and telemedicine (GSMA, 2024).

To overcome this limitation, 3GPP defines the Local Breakout (LBO) model. In LBO, traffic The PDU session data is downloaded directly to the destination data network from the V-UPF located at VPLMN, eliminating the need for traffic to travel to the country of origin. HPLMN maintains only control over policy rules and session authorization via H-PCF and H-SMF (3GPP, 2024a).

Despite its technical superiority in latency, the LBO model presents significant complexity. operational and commercial. It requires highly complex bilateral ticketing agreements for Cross-billing between operators poses regulatory challenges regarding liability. traffic offloaded onto the visited network, which is why its initial adoption is restricted to services. specific corporate (GSMA, 2024).

This article is published in open access under the Creative Commons Attribution license, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Machine Translated by Google
IRCMOS – Multidisciplinary Scientific Journal The Knowledge.
ISSN: 2675-9128. São Paulo-SP.

Year VII, v.2 2026 | Submission: 09/30/2026 | Accepted: 10/03/2026 | Publication: 10/06/2026

4 SEPP, N32 Interface and Interconnection Security

To eliminate the historical vulnerabilities of the SS7 and Diameter signaling networks, the 3GPP TS
Regulation 29.573 establishes the Security Edge Protection Proxy (SEPP) as the mandatory edge protection function.
In 5G SA, all signaling flows from the control plane between the VPLMN and the HPLMN are handled by any and all signaling.
must transit mandatorily through the SEPPs of both networks (vSEPP and hSEPP) (3GPP, 2024c;
ENISA, 2020).

SEPP plays vital cybersecurity roles at the inter-PLMN edge. It acts as
A signaling application firewall, performing the masking of the internal network topology.
(*topology hiding*), filtering of unauthorized messages, rate control for prevention of
Denial-of-service (DoS) attacks and strict format validation of JSON schemas (3GPP,
2024c).

The interconnection between vSEPP and hSEPP occurs through the N32 interface, which is logically...
subdivided into two operational channels with complementary roles: the N32-c interface (Control
Plane) and the N32-f (Forwarding Plane) interface (3GPP, 2024c).

The N32-c interface is used for the initial control phase. Through it, the two SEPPs perform the...
Mutual authentication via TLS 1.3 using x.509 digital certificates, negotiating capabilities.
Supported cryptographic methods, exchange session keys, and establish the parameters of the Association of
Security Association (SA) that will govern the exchange of application messages.

The N32-f interface is dedicated to the effective transmission of signaling messages from internal NFs.
(such as calls between V-SMF and H-SMF or AMF and UDM). To protect these messages while
For transit through the IPX network, the N32-f implements the PRINS protocol (Protocol-specific Application Layer).
Security) (3GPP, 2024c; BASIN et al., 2018).

The PRINS protocol elegantly solves the dilemma of roaming transportation. How?
Intermediate IPX network providers often need to modify certain headers.
For HTTP/2 routing, PRINS divides the message into blocks: the subscriber's sensitive data.
remain fully encrypted and inaccessible, while the modifiable headers can be
Modified by us with our authorization and cryptographically reassigned, guaranteeing complete auditability.
(BASIN et al., 2018).

5. Subscriber Identity, Authentication, and Privacy

One of the most severe weaknesses of second, third, and fourth generation mobile networks was...
Transmission of the subscriber's permanent identity (IMSI) in plain text over the radio channel.

This article is published in open access under the Creative Commons Attribution license, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Machine Translated by Google
RCMOS - Multidisciplinary Scientific Journal The Knowledge.
ISSN: 2675-9128. São Paulo-SP.

Year VII, v.2 2026 | Submission: 09/30/2026 | Accepted: 10/03/2026 | Publication: 10/06/2026

during the initial network connection procedures. This limitation facilitated the proliferation of malicious interception equipment known as *IMSI Catchers* (Stingrays) (BASIN et al., 2018; ENISA, 2020).

In 5G Standalone, the 3GPP TS 33.501 specification eliminates this vulnerability by redefining the User identity structure. The subscriber's permanent identity will now be called SUPI (Subscription Permanent Identifier). The regulation expressly prohibits the SUPI from being... transmitted in plain text on any radio interface (3GPP, 2024d).

Instead of directly sending SUPI data, the user's terminal SIM/eSIM card generates a A temporary, encrypted identity called SUCI (Subscription Concealed Identifier). The generation of SUCI relies on an asymmetric public-key cryptography scheme based on curves. elliptical (ECIES - Elliptic Curve Integrated Encryption Scheme) (BASIN et al., 2018).

The SIM card has the public key of its originating network stored in its secure memory. (HPLMN). When requesting access to the visited network (VPLMN), the terminal uses the public key to Encrypting SUPI produces SUCI. The corresponding private key is kept exclusively... Inside the HPLMN UDM, neither the radio network nor the VPLMN AMF can decipher the real identity of the user.

Upon receiving the SUCI sent by the terminal, the AMF in the VPLMN forwards this encrypted identity to The HPLMN hSEPP is accessed through the N32 interface. The HPLMN UDM uses its private key to... Decrypt the SUCI, retrieve the original SUPI, and initiate the 5G-AKA mutual authentication procedure. (or EAP-AKA') (3GPP, 2024d).

This mechanism ensures that subscriber privacy remains preserved end-to-end. Even that the visited radio network or the roaming partner's infrastructure be compromised by eavesdropping. Even with malicious activity, the user's permanent identity remains fully protected against tracking. undue (BASIN et al., 2018).

6. Interoperability and Signaling between Operators

Enabling international roaming on 5G SA networks requires strict technical compliance and semantics between network functions developed by different technology vendors (*multi-(vendor*). API calls exchanged in the SBA must strictly adhere to OpenAPI schemas. 3.0 standardized by 3GPP in the TS 29500 series (3GPP, 2024c; GSMA, 2024).

In real-world operational scenarios, minor discrepancies in the interpretation of optional parameters in JSON documents or specific HTTP/2 header handling may cause rejection.

This article is published in open access under the Creative Commons Attribution license, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Machine Translated by Google
RCMOS - Multidisciplinary Scientific Journal The Knowledge.
ISSN: 2675-9128. São Paulo-SP.

Year VII, v.2 2026 | Submission: 09/30/2026 | Accepted: 10/03/2026 | Publication: 10/06/2026

requests in the edge SEPP. This results in the premature termination of the connection attempt and in Loss of connectivity for subscribers while roaming.

To mitigate these interoperability risks, the GSMA NG.113 standard establishes a protocol. detailed instructions for conducting continuous bilateral testing (*IREG Testing*) prior to release. commercial roaming routes between two operators (GSMA, 2024).

Bilateral testing encompasses syntactic and semantic validation in SEPP, verifying whether the rules of Signaling firewalls are configured to allow the passage of authorized APIs without Improperly altering the payload of messages encrypted via PRINS.

Another critical aspect is the standardized mapping of error cause codes. When a PDU session request fails in HPLMN, H-SMF should return an error code. Standardized HTTP (e.g., `403 Forbidden` or `504 Gateway Timeout`) followed by the code of The corresponding 5GSM cause, according to TS 24.501, allows the AMF in VPLMN to guide the terminal correctly (GSMA, 2024).

Finally, network engineering teams must fine-tune the timers. TCP reconnection and HTTP/2 bus integrity check (*PING*) calls interface N32. This measure prevents small latency fluctuations in the IPX network from causing the mass dismantling of security associations among SEPPs (GSMA, 2024).

7. Quality, Continuity, and Experience in Roaming

The user's perceived experience in international roaming depends directly on the quality. The technique is maintained in both networks involved (VPLMN and HPLMN) and in the transport segment. interconnected via IPX. Continuous monitoring of this experience requires tracking by Highly specific Service Level Indicators (SLIs) (ITU, 2024; GSMA, 2024).

Quality assessment is divided between control plan metrics and risk plan metrics. user. In the control plan, the main indicator is the success rate in the procedures of 5G-AKA authentication and total response time for establishing PDU data sessions. in the Home Routed topology.

At the user level, metrics focus on the round-trip latency (RTT) of the GTP-U tunnel. interface N9, in the rate of change of packet delay (*jitter*) and in the percentage of accidental loss of packets during cross-border transmission.

Identifying performance bottlenecks in international networks requires the ability to segment. Observability data by roaming partner (identified by PLMN-ID). An elevation atypical latency observed exclusively on the N32 interface associated with a specific

This article is published in open access under the Creative Commons Attribution license, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Machine Translated by Google
RCMOS - Multidisciplinary Scientific Journal The Knowledge.
ISSN: 2675-9128. São Paulo-SP.

Year VII, v.2 2026 | Submission: 09/30/2026 | Accepted: 10/03/2026 | Publication: 10/06/2026

Partner operator indicates saturation in the remote SEPP or degradation in the contracted IPX network route. (GSMA, 2024).

The use of automated real-time experience monitoring systems allows that The originating operator performs proactive traffic switching (steering of roaming). In case the If the quality of a partner VPLMN falls below acceptable SLO limits, HPLMN advises dynamically connect its subscribers' terminals to another available partner network in same region.

In this way, the integration of quality metrics from the control plane and the data plane ensures the transparent continuity of services, minimizing browsing interruptions and guaranteeing the compliance with commercial service level agreements (SLAs) (ITU, 2024).

8 Bilateral Governance, Fraud and Incident Response

The reliable operation of roaming agreements in 5G SA goes beyond the deployment of solutions. purely technological. It requires a bilateral organizational and contractual governance structure. Highly disciplined among partner operators, aligned with NIST Cybersecurity principles. Framework 2.0 and GSMA recommendations (GSMA, 2024; NIST, 2024).

Roaming operational contracts should precisely define a responsibility matrix. (RACI) covering all technical contact points, scheduled maintenance windows and Standardized procedures for advance notification of software changes at the inter-PLMN edge.

One of the pillars of technical governance is the continuous management of the certificate lifecycle. x.509 digital signatures are used for TLS encryption on the N32-c interface and PRINS signing on the N32-f. lack of rigorous monitoring of key expiration dates or failures in key rotation.

PKI certificates can result in the complete and immediate interruption of roaming traffic between two networks.

In the context of fraud prevention, the migration to 5G SA requires new mechanisms for Monitoring in the SEPP. Signaling traffic must be continuously analyzed by algorithms. anomaly detection to identify attempts to bypass billing, phantom calls or API exploitation attacks aimed at the unauthorized consumption of data.

Additionally, the mutual exchange of billing and usage records should occur within shorter timeframes. through the standardized SDR (Standard Data Record) format, allowing for quick reconciliation of Inter-operator billing and agile containment of financial incidents (GSMA, 2024).

Finally, governance requires the establishment of direct communication channels for responding to Cybersecurity incident response (CSIRT). In case of compromise of private keys or

This article is published in open access under the Creative Commons Attribution license, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Machine Translated by Google

Year VII, v.2 2026 | Submission: 09/30/2026 | Accepted: 10/03/2026 | Publication: 10/06/2026

Identifying attack patterns originating from the partner network, and containment protocols.
Emergency measures and route isolation should be activated with response times measured in minutes.
(NIST, 2024).

Final Considerations

Enabling international roaming on 5G Standalone networks represents a historic transition.
at the level of security, privacy, and efficiency offered to users in global mobility. A
definitive replacement of legacy SS7 and Diameter networks with an infrastructure based on
Microservices and API calls over the HTTP/2 protocol address structural vulnerabilities of
Signaling that has affected the telecommunications sector for decades.
As demonstrated in this research, the mandatory presence of the Security Edge Protection Proxy
(SEPP) at the inter-PLMN edge constitutes the cornerstone of security in 5G SA. By acting as
By using the application firewall and managing the PRINS protocol on the N32 interface, SEPP ensures the integrity of the protocol.
and confidentiality of control plan messages even in the presence of intermediaries
on the IPX transport network.
Analysis of user plane topologies reveals that the Home Routed (HR) architecture
remains the predominant choice for operators in providing data services.
conventional. The ability to retain UPF anchoring in HPLMN ensures auditability.
Pricing and compliance with local regulations without depending on the partner being visited.
In turn, the Local Breakout (LBO) model is establishing itself as an indispensable strategic option.
to enable ultra-high-speed, ultra-low latency (URLLC) services. The download
Routing traffic directly on the visited network eliminates the delays inherent in circular routing, opening up...
A pathway for cross-border industrial and corporate applications.
With regard to user privacy, the advancement provided by the encryption scheme
The asymptotic SUPI/SUCI permanently eliminates the exposure of the subscriber identifier on the channel.
radio. The fact that SUCI is decrypted exclusively by the private key held in the UDM of
The origin network protects subscribers against malicious scans and improper tracking by
IMSI Catchers devices.
Ensuring seamless interoperability in multi-vendor environments.
This reinforces the importance of strictly adhering to the OpenAPI 3.0 schemas and testing routines.
bilateral adjustments as recommended by GSMA NG.113. The setting of HTTP/2 bus timers and the
Standardization of error cause codes is essential to avoid signaling failures.
intermittent.

This article is published in open access under the Creative Commons Attribution license, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Machine Translated by Google

Year VII, v.2 2026 | Submission: 09/30/2026 | Accepted: 10/03/2026 | Publication: 10/06/2026

In parallel, operational and contractual governance reaffirms itself as an inseparable element of Network architecture. Disciplined management of the PKI certificate lifecycle, monitoring. Fraud prevention in the SEPP and real-time cyber incident coordination are the conditions that ensure the stability of international partnerships.

In conclusion, the success of roaming in 5G SA depends on building a chain of trust. Technical and institutional end-to-end. The harmonious integration between cryptographic mechanisms. At the edge, partner-segmented observability and continuous bilateral governance are what ensure... delivering a truly robust, secure, and international connectivity experience resilient.

References

3GPP. TS 23.501: System architecture for the 5G System; Stage 2 (Release 18). Sophia Antipolis: 3GPP, 2024a. Available at: https://www.3gpp.org/dynareport/23501.htm.
3GPP. TS 23.502: Procedures for the 5G System; Stage 2 (Release 18). Sophia Antipolis: 3GPP, 2024b. Available at: https://www.3gpp.org/dynareport/23502.htm.
3GPP. TS 29.573: Public Land Mobile Network (PLMN) interconnection; Stage 3 (Release 18). Sophia Antipolis: 3GPP, 2024c. Available at: https://www.3gpp.org/dynareport/29573.htm.
3GPP. TS 33.501: Security architecture and procedures for 5G System (Release 18). Sophia Antipolis: 3GPP, 2024d. Available at: https://www.3gpp.org/dynareport/23501.htm.
BASIN, D. et al. A formal analysis of 5G authentication. In: Proceedings of the 2018 ACM SIGSAC CONFERENCE ON COMPUTER AND COMMUNICATIONS SECURITY (CCS '18), 2018, Toronto. Annals [...]. New York: ACM, 2018. p. 1383-1396. DOI: https://doi.org/10.1145/3243734.3243846.

ENISA. ENISA threat landscape for 5G networks. Athens: European Union Agency for Cybersecurity, 2020. DOI: https://doi.org/10.2824/49299.
GSMA. NG.113: 5GS roaming guidelines. Version 10.0. London: GSMA, 2024. Available at: https://www.gsma.com/newsroom/wp-content/uploads/NG.113-v10.0.pdf. Accessed on: September 10, 2026.
ITU. Measuring digital development: Facts and Figures 2024. Geneva: International Telecommunication Union, 2024. Available at: https://www.itu.int/itu-d/reports/statistics/facts-figures-2024/.

NIST. Cybersecurity Framework 2.0. https:// Gaithersburg: NIST, 2024. DOI: doi.org/10.6028/NIST.CSWP.29.

This article is published in open access under the Creative Commons Attribution license, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.