5G/6G Academy
TELECOM CERTIFICATIONS · SINCE 2009

Technical Whitepaper
N° 06 · June 2026

TECHNICAL WHITEPAPER

5G Security: What Got Fixed, What Got Deferred

Beyond the key ladder: how 5G repaired the interconnect's original sin, how zero trust was retrofitted onto the core, why nine 256-bit algorithms sit unused, where post-quantum actually stands — and what the first 5G-core CVEs teach.

AUTHOR
5G/6G Academy Research

VERSION
1.0

DATE
June 2026

SEPP · N32 | ZERO TRUST | 256-BIT · PQC | CVE REALITY | EU · FCC

© 2026 5G/6G Academy · by TELCOMA Global

5G/6G ACADEMY · TECHNICAL WHITEPAPER · N° 06 June 2026 · 5g6gacademy.com

5G Security: What Got Fixed, What Got Deferred

5G/6G Academy Research

a TELCOMA Global publication · Telecom Certifications · Since 2009

***Abstract*—5G's security story is usually told at the SIM: mutual authentication, the key ladder, concealed identities. This paper covers the half that decides real-world outcomes. On the interconnect, 5G finally fixed attribution — signed inter-operator messaging through SEPPs — yet the GSMA concluded plain TLS, not the celebrated PRINS, for its first roaming phase, and 3GPP itself concedes the ecosystem "still needs to fully embrace" the new model, while legacy fallback can drop a roamer's signalling from HTTP to Diameter to SS7. Inside the core, mTLS and OAuth machinery exist in the spec, but 3GPP's own zero-trust studies name monitoring and dynamic policy as the gaps. Nine 256-bit algorithms have been fully specified since March 2024 — and the system specification still references none of them, a fact verifiable by grep. We close with the first real 5G-core CVEs, the EU and US regulatory positions, and a checklist that starts where the key ladder ends.**

1. The Interconnect's Original Sin

The global signalling network was built on a politeness assumption: any operator that could reach the interconnect was trusted to say who it was. SS7 has no attribution — a message claims a sender, and the network believes it. What that costs was demonstrated conclusively in May 2017, when O2 Telefónica Germany confirmed that attackers, having obtained access through a foreign operator's network months earlier, used SS7 to redirect customers' banking one-time codes and drain their accounts — the canonical, press-documented incident of the legacy era [16]. The flaws had been publicly described by researchers back in 2014; ENISA's 2018 assessment rated interconnect signalling risk across SS7, Diameter and early 5G as "medium to high" for European communications [15]. Diameter, 4G's replacement, inherited the same class of weaknesses — location tracking and interception remained practical, per research reported alongside the ENISA work [17].

Every security property inside a network — the strongest SIM authentication, the tallest key ladder — sits behind this border. 5G's most consequential security decision was finally to fortify it.

2. What 5G Actually Fixed: Attribution

3GPP's security group states the goal plainly: 5G standalone roaming security "aims to address the root cause of a wide range of attacks that have taken and continue to take place over the roaming infrastructure in the past decades: the lack of attribution" [1]. The mechanism is the SEPP — the Security Edge Protection Proxy that terminates every signalling exchange between operators. Its interconnect, N32, splits in two: N32-c, where the SEPPs mutually authenticate and negotiate security mechanisms, and N32-f, which carries the actual signalling [1].

For N32-f there are two models (Fig. 1). The direct model wraps everything in TLS between the two SEPPs — one encrypted, authenticated pipe. The mediated model exists because real roaming traffic often crosses intermediaries (IPX carriers) that legitimately read or adjust certain fields: PRINS protects messages at the application layer (with a JOSE profile), letting intermediaries touch only the elements that negotiated protection and modification policies allow, with a maximum of two such intermediaries permitted when they do more than route IP [1], [3].

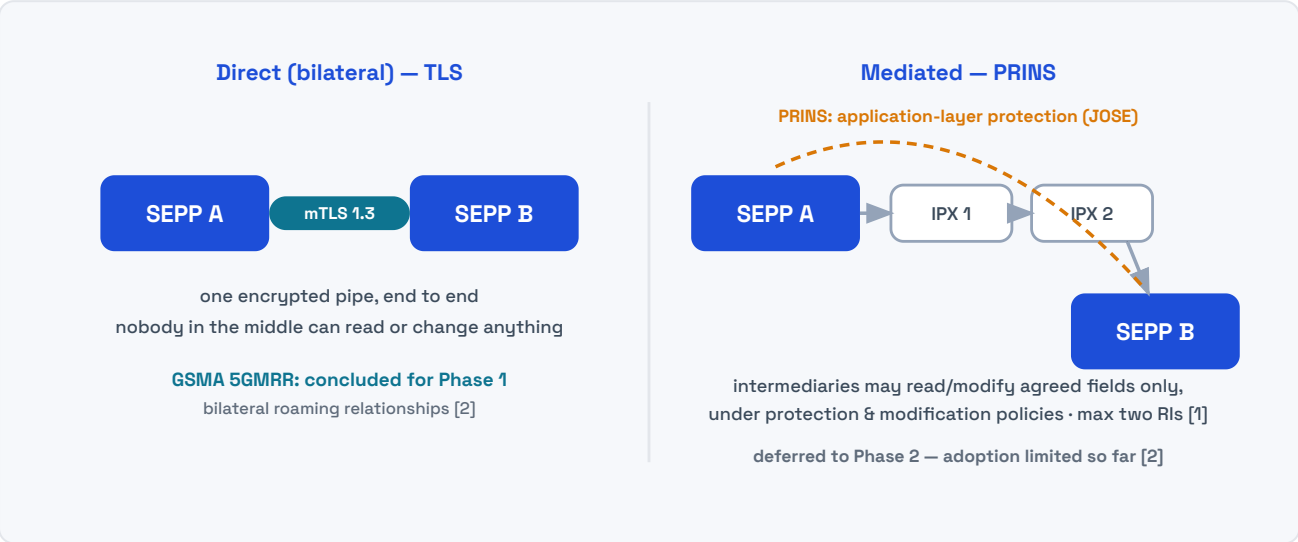

Fig. 1. Two ways to secure the inter-operator border (TS 33.501 cl. 13.1–13.2 [3]; 3GPP SA3 [1]). The GSMA's 5G roaming program concluded TLS for Phase 1 bilateral roaming and deferred the intermediary cases to Phase 2 [2] — the pragmatic model shipped first.

Here is the part the conference slides skip. The GSMA's 5G Mobile Roaming Revisited program, weighing "simplest model per use case," concluded **TLS — not PRINS — as the connection model for Phase 1** bilateral roaming, deferring the intermediary scenarios (IPX, hosted SEPPs, roaming hubs) to Phase 2 [2]. PRINS adoption, accordingly, remains limited and in progress rather than the norm. And 3GPP's own February 2025 assessment is refreshingly honest: the end-to-end approach "represents a fundamental change," and the roaming ecosystem "still needs to fully embrace this approach at the time of writing" [1]. The user plane got its own border control: GSMA requires Inter-PLMN UP Security on N9 between all operators [2]. Attribution is fixed in the spec; the ecosystem is still moving in.

3. The Fallback Problem

One sentence in the GSMA's roaming report deserves a section of its own. Discussing roamers whose devices move across generations in a visited network, it warns that signalling between visited and home networks "switches from HTTP to Diameter to SS7 in case there are parallel links. This may involve security risks for 5G users during roaming" [2]. Read it again: the strongest interconnect security 3GPP ever built can be bypassed not by breaking it, but by stepping around it — a subscriber drops to 4G or 2G coverage, and the conversation about that subscriber drops to the protocols of Section 1.

This is the same lesson the 2017 mTAN heist taught at the subscriber layer, now one layer up: **a security architecture is only as strong as its weakest coexisting generation**. For operators, the practical consequences are unglamorous — inventory which legacy interconnect links still run in

parallel, apply GSMA's legacy signalling controls there, and treat 2G/3G sunset plans as security projects, not just spectrum-refarming projects.

4. Zero Trust, Retrofitted

Inside the core, 5G's service-based architecture turned network functions into web services — and inherited the web's security toolbox. TS 33.501's clause 13, verified directly against the current specification (V20.1.0, March 2026), mandates the machinery: TLS protection on the service-based interfaces (cl. 13.1); the N32 application-layer protection of Section 2 (cl. 13.2); network-function authentication including Client Credentials Assertion (cl. 13.3.8); and OAuth 2.0 authorization in which **the NRF acts as the authorization server**, issuing access tokens per RFC 6749 (cl. 13.4.1) [3]. On paper, that is most of a zero-trust stack.

3GPP then did something rare: it graded its own homework. TR 33.894 (Rel-18) assessed the 5G core against the tenets of NIST SP 800-207, the canonical zero-trust framework [7], [10], [11]; TR 33.794 (Rel-19) followed, focused on the enablers the first study found wanting — **security monitoring and dynamic policy enforcement** [8], [11]. Table 1 summarizes the picture as we read it: communications security and token-based authorization are specified; continuous monitoring, telemetry-driven policy and assume-breach verification are, by 3GPP's own program of work, still under construction. Zero trust in the 5G core is genuinely underway — and genuinely unfinished.

TABLE 1 · Zero trust vs. the 5G SBA — the machinery and its gaps

NIST SP 800-207 expectation	What the 5G core has today (TS 33.501, cl. 13)	Status
All communication secured, regardless of network location	TLS on every SBI hop (cl. 13.1); N32 protection between operators (cl. 13.2)	in the spec [3]
Per-session, least-privilege access to resources	OAuth 2.0 authorization with the NRF as token server (cl. 13.4.1, per RFC 6749); Client Credentials Assertion (cl. 13.3.8)	in the spec; scope granularity still coarse in practice [3], [19]
Integrity and security posture of all assets monitored	vendor tooling; SCAS-hardened NFs	partial — the admitted gap [7], [8]
Dynamic policy, informed by telemetry	management-plane enablers under study	Rel-19 study (TR 33.794) [8]
Assume breach; verify continuously	no standardized continuous-verification machinery yet	open [7], [8]

5. The 256-bit Paradox

If you want one fact that captures the distance between "standardized" and "deployed," it is this. 3GPP has fully specified **three complete 256-bit algorithm suites** — SNOW 5G (256-NEA4/NIA4/NCA4, TS 35.240–242), AES-256-based (TS 35.243–245), and ZUC-256-based (TS 35.246–248) — all Release 18, first published in March 2024 [4]. Nine algorithm specifications, designed with ETSI SAGE, sitting on the shelf.

And the shelf is where they sit: a direct grep of TS 33.501 V20.1.0 — the 5G security architecture as of March 2026 — finds **zero occurrences** of any 256-bit algorithm identifier; the normative annex still lists NEA0 and the 128-bit sets, nothing more [3]. The machinery for negotiating and transitioning to

256-bit operation is a Rel-19 *study* (TR 33.700-41), descended from a groundwork study that began back in 2018 (TR 33.841) [5], [6]. No committed release wires the new algorithms into the system, and we will not invent a date (Fig. 2). The honest framing: 5G's cryptographic upgrade path exists as components, not as a system — and the transition machinery, not the cryptography, is the long pole.

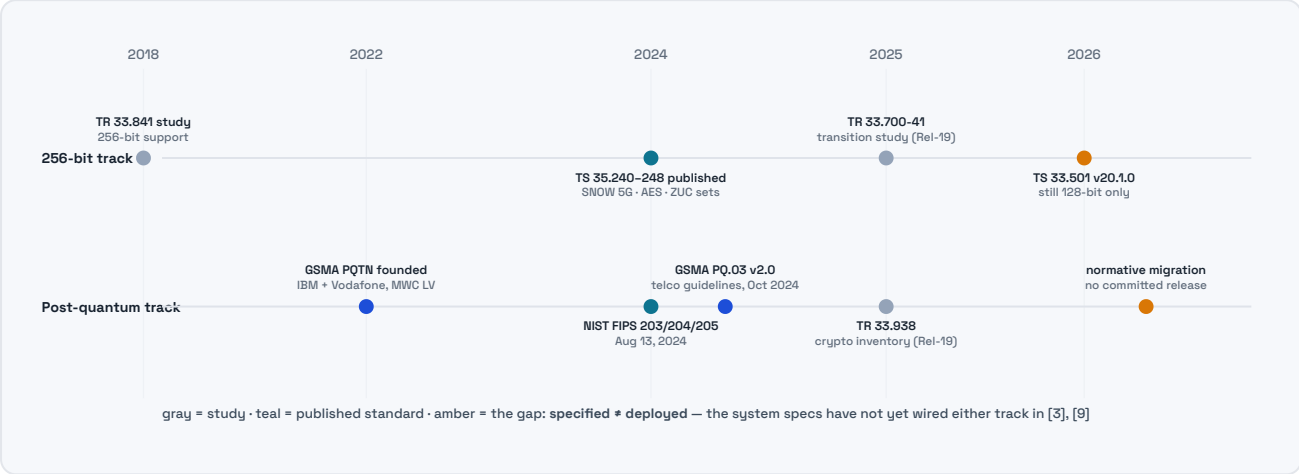

Fig. 2. Two cryptographic upgrade tracks, one pattern: the algorithms arrive years before the system adopts them. The 256-bit suites have been published since March 2024, yet the security architecture references none of them; post-quantum has standards (NIST) and guidelines (GSMA) but, in 3GPP, an inventory study. Sources: [3]–[6], [9], [12]–[14].

6. Post-Quantum on a Telco Timetable

The post-quantum clock started properly on August 13, 2024, when NIST finalized FIPS 203 (ML-KEM), 204 (ML-DSA) and 205 (SLH-DSA) — the algorithms every serious migration now builds on [12]. The telecom industry's coordination vehicle predates them: the GSMA's Post-Quantum Telco Network task force, initiated by IBM and Vodafone at MWC Las Vegas in 2022, had grown past fifty companies and twenty major operators by late 2023 [14], and published the second version of its telco migration guidelines (PQ.03) in October 2024 — phased migration, use-case prioritization, hybrid key exchange for transport links first [13].

3GPP's contribution so far is deliberately unexciting: TR 33.938, a Rel-19 **cryptographic inventory** — a systematic map of every place cryptography lives in 3GPP systems, under change control since mid-2025 [9]. Unexciting is correct: you cannot migrate what you have not enumerated, and the inventory is the precondition for every later decision. What does not yet exist, anywhere in 3GPP, is normative post-quantum integration — no PQC SUCI concealment, no PQC-ready N32 profile in the published architecture. As with the 256-bit suites, the pieces are assembling in the order large systems actually change: algorithms, guidelines, inventory, then — on a timetable nobody has committed to paper — the system itself. Plan procurement accordingly: ask vendors about crypto-agility (the ability to swap algorithms without forklift upgrades) rather than about "quantum-safe 5G" badges.

7. When the Core Became Software

The service-based core is software, and in 2025 it started accumulating software's most honest artifact: CVE numbers. CVE-2025-63288 documents a denial of service in Open5GS — a malformed NGSetupRequest crashes the AMF; network-reachable, no privileges required, scored 7.5 by the reporting authority [18]. Deeper and more instructive: researchers examining free5GC — the only

public open-source core with a Rel-17-compliant OAuth implementation on the SBI — found eight vulnerabilities, all acknowledged by the project and mostly patched. The worst was a token-scope check whose failure was silently swallowed by a wrapped-error bug, letting a token issued for one network-function service access others: privilege escalation *inside* the SBA, through exactly the OAuth machinery Section 4 praised [19]. Independent work has reported further parser crashes in open-source cores [20].

Three lessons, stated carefully. First, these are open-source implementations, not documented attacks on production operator cores — the public record of incidents remains SS7/Diameter-era, and we found no citable breach of a production 5G SBA or SEPP. Second, that is precisely why these CVEs matter: they are the first empirical look at how SBA security fails, and the failure modes are classic software — input parsing and authorization edge cases, not broken cryptography. Third, the defense is operational, not architectural: the spec's machinery was sound in both cases; implementations and their patch cadence were the gap. If your core is software — and it is — your security program needs the disciplines of software: fuzzing in acceptance, CVE watch on every component, and assurance schemes (SCAS, NESAS) treated as floors rather than achievements.

8. The Regulatory Layer, and What To Do

Two regulatory facts frame every operator's room for maneuver. In Europe, the 5G Toolbox (January 2020) established risk-mitigation measures including restrictions on high-risk suppliers, and the Commission sharpened it on June 15, 2023: Huawei and ZTE "represent in fact materially higher risks than other 5G suppliers," with the Commission applying that judgment to its own communications and funding [21], [22]. In the United States, the rip-and-replace ledger reads, per the FCC's December 2025 report to Congress: $1.9 billion appropriated against $4.98 billion in approved cost estimates; the $3.08 billion shortfall borrowed in full from the Treasury in March 2025 after Congress authorized it; roughly $1.4 billion spent by mid-2025 [23]. Vendor trust, once a procurement preference, is now a funded — and expensively underfunded — matter of law.

The engineering checklist that falls out of this paper: **(1)** at the border, demand TLS-mode N32 with every bilateral partner and treat PRINS as the exception requiring explicit policy review [1], [2]; **(2)** inventory parallel legacy interconnect links — your fallback exposure is your real exposure (§3); **(3)** inside the core, enable user-plane integrity where device policy allows, and audit OAuth token scopes against least privilege — the free5GC finding shows exactly where that fails [19]; **(4)** start your own cryptographic inventory now, mirroring TR 33.938's logic, so the 256-bit and PQC transitions are migrations rather than archaeology [9]; **(5)** put SCAS/NESAS requirements and CVE-response SLAs into every core procurement. None of it is glamorous. Neither was the SEPP — and the SEPP is the most important security box 5G ever shipped.

References

[1] 3GPP SA3, "5G roaming security" (Y. Targali, A. Jerichow, A. Pashalidis), 3GPP technology article, Feb. 2025. 3gpp.org/technologies/roaming-security-sa3

[2] GSMA, NG.132, "5G Mobile Roaming Revisited (5GMRR)," v5.0, Feb. 2024 (Phase-1 TLS conclusion; v4.0 conclusions retained). gsma.com/newsroom

[3] 3GPP, TS 33.501, "Security architecture and procedures for 5G System," V20.1.0, Mar. 2026, cl. 13, Annex D. 3gpp.org/ftp/Specs/archive/33_series/33.501

[4] 3GPP, TS 35.240–35.248: SNOW 5G, AES-based and ZUC-based 256-bit algorithm sets (Rel-18, first published Mar. 2024). 3gpp.org/DynaReport/35240.htm

[5] 3GPP, TR 33.841, "Study on the support of 256-bit algorithms for 5G." 3gpp.org/DynaReport/33841.htm

[6] 3GPP, TR 33.700-41, "Study on enabling a cryptographic algorithm transition to 256 bits" (Rel-19). 3gpp.org/DynaReport/33700-41.htm

[7] 3GPP, TR 33.894, "Study on applicability of the zero trust security principles in mobile networks" (Rel-18). 3gpp.org/DynaReport/33894.htm

[8] 3GPP, TR 33.794, "Study on enablers for Zero Trust Security" (Rel-19). 3gpp.org/DynaReport/33794.htm

[9] 3GPP, TR 33.938, "3GPP Cryptographic Inventory" (Rel-19; under change control since Jun. 2025). 3gpp.org/DynaReport/33938.htm

[10] NIST, SP 800-207, "Zero Trust Architecture," Aug. 2020. csrc.nist.gov/pubs/sp/800/207/final

[11] Ericsson, "Zero trust architecture enabled by 3GPP security," blog, Feb. 2025. ericsson.com/en/blog

[12] NIST, "NIST releases first 3 finalized post-quantum encryption standards" (FIPS 203/204/205), Aug. 13, 2024. nist.gov

[13] GSMA, PQ.03, "Post Quantum Cryptography — Guidelines for Telecom Use Cases," v2.0, Oct. 4, 2024. gsma.com/newsroom/gsma_resources

[14] GSMA, "Readying the mobile industry for a post-quantum future" (PQTN task force). gsma.com/newsroom

[15] ENISA, "Signalling security in telecom SS7/Diameter/5G," Mar. 28, 2018. enisa.europa.eu/publications

[16] Help Net Security, "Attackers exploited SS7 flaws to empty Germans' bank accounts," May 4, 2017 (operator confirmation via Süddeutsche Zeitung). helpnetsecurity.com

[17] BleepingComputer, "Newer Diameter telephony protocol just as vulnerable as SS7." bleepingcomputer.com

[18] NVD, CVE-2025-63288 (Open5GS AMF DoS; CVSS 3.1 7.5, CNA-supplied), Nov. 10, 2025. nvd.nist.gov/vuln/detail/CVE-2025-63288

[19] "Cross-service token: finding attacks in 5G core networks," arXiv:2509.08992, 2025 (vendor-acknowledged; 7 of 8 issues patched at submission). arxiv.org/abs/2509.08992

[20] P1 Security, "Open5GS vulnerabilities uncovered by P1 Security," blog. p1sec.com/blog

[21] European Commission / NIS Cooperation Group, "Cybersecurity of 5G networks — EU toolbox of risk-mitigating measures," Jan. 2020. digital-strategy.ec.europa.eu

[22] European Commission, "Communication on the implementation of the 5G cybersecurity toolbox," Jun. 15, 2023. digital-strategy.ec.europa.eu

[23] FCC Wireline Competition Bureau, "Secure and Trusted Communications Networks Reimbursement Program," Seventh Report to Congress, Dec. 2025. docs.fcc.gov