WHITE PAPER

A Strategic Shift: Certificate-Based Authentication (CBA)

Modernizing 4G/5G and Private Cellular Core Authentication Architecture

---

Prepared by

Open Device Alliance

July 2026

Table of Contents

Executive Summary

Traditional 4G/5G authentication ties every device to a SIM or eSIM — a model built for consumer handsets on a handful of national carriers, not for the fast-growing set of Enterprises, Private Cellular Operators, CableCos, and Satellite Providers now building their own commercial 4G/5G infrastructure. For these operators, SIM-based identity creates real friction: per-transaction eSIM provisioning fees, IT organizations that can't manage a SIM the way they manage a laptop, brittle IoT onboarding, single points of failure during disaster response, and per-carrier roaming agreements that don't scale to neutral host deployments.

Certificate-Based Authentication (CBA), delivered via EAP-TLS, offers a standards-supported alternative. 3GPP TS 33.501 documents EAP-TLS as a primary 5G authentication method, and Release 17's Credentials Holder using AAA Server (CH-AAA) model lets a network authenticate a device against credentials owned by an outside entity — the enterprise, the device manufacturer, or a federated identity provider — rather than a SIM tied to the network operator itself.

This paper examines five business cases for CBA adoption: direct cost reduction versus eSIM provisioning fees, convergence with enterprise IT for private 5G, zero-touch IoT provisioning at scale, resilient authentication for first responder and disaster deployments, and federated identity for neutral host and non-SIM assets. Each case is grounded in current 3GPP standards; where a claim goes beyond what is standardized today, it is flagged as such rather than presented as settled fact.

Introduction

Traditional cellular networks are structurally bound to SIM/eSIM-based authentication (5G-AKA). However, as non-traditional Operators (Enterprises, Private Cellular Operators, CableCos, and Satellite Providers) deploy their own 4G/5G infrastructure for commercial use, relying on legacy SIM architecture introduces massive structural friction.

By utilizing Certificate-Based Authentication (CBA via EAP-TLS) within their owned and managed 5G cores, Operators can decouple identity from cellular hardware, seamlessly integrate with corporate enterprise IT ecosystems, and unlock a highly scalable, asset-light, zero-trust network topology.

This is a standards-supported path, not a workaround: **3GPP TS 33.501 (Annex B)** formally documents EAP-TLS as a primary authentication method for private/non-public networks, and **Release 17** introduced the "Credentials Holder using AAA Server" (CH-AAA) model, letting a Standalone Non-Public Network (SNPN) authenticate a device using credentials issued and owned by a separate enterprise entity rather than a subscription tied to the network operator. That is the specific mechanism that makes everything below possible.

1. Direct Cost Reduction: Bypassing the eSIM "Provisioning Tax"

While eSIM technology eliminates physical plastic, it does not eliminate vendor lock-in. Managing eSIMs requires a complex, GSMA-certified Remote SIM Provisioning (RSP) infrastructure driven by third-party platform vendors.

The Financial Leakage of eSIM

- **Per-Transaction Fees:** Every time an eSIM profile is generated, updated, or downloaded via an SM-DP+ server, operators pay an intermediate transaction fee. For an operator managing millions of consumer devices, high-density corporate campuses, or rotating IoT profiles, these transactional micro-fees scale into significant recurring operational cost.
- **Core Network Overhead:** Maintaining a traditional cellular core database (HLR/HSS/UDM) to track SIM cryptographic keys requires specialized telecom engineers and heavy licensing costs.

The CBA Business Case

- **Fractional-Cost PKI Scaling:** Standardizing on X.509 digital certificates allows operators to route authentication through cloud-native Public Key Infrastructure (PKI) and AAA/RADIUS servers. Once the PKI infrastructure is built, generating, rotating, or revoking large volumes of digital certificates costs a small fraction of a comparable SIM transaction.
- **Standards Legitimacy:** Because EAP-TLS is a documented 3GPP primary authentication method (TS 33.501 Annex B) and Release 17's CH-AAA model is purpose-built for exactly this "credentials owned outside the network operator" scenario, this is a supported architectural pattern — not a proprietary bolt-on that risks interop or compliance issues.
- **Directional Cost Impact:** Shifting authentication from complex, specialized cellular core infrastructure to standard cloud-native IT infrastructure (PKI/RADIUS, which most IT organizations already run) removes an entire specialized cost center. Industry vendors managing large-scale remote device provisioning report cost reductions in the range of 40–60% versus traditional SIM logistics and management, though figures are vendor- and deployment-specific.

2. Unlocking Private 4G/5G: Total Convergence with Enterprise IT

Companies are aggressively positioning themselves as Managed Service Providers of Private 4G/5G networks for enterprise clients (factories, hospitals, airports, and universities). However, corporate IT departments heavily resist traditional SIM cards.

The Barrier of the SIM in the Enterprise

- **Siloed Identity:** Corporate IT cannot track or manage SIM cards using standard enterprise identity providers (like Microsoft Entra ID, Okta, or Active Directory). A SIM card treats a device like a phone line, whereas corporate IT needs to treat it like a secure computer network asset.

- **Logistical Friction:** Provisioning private physical SIMs or pushing private eSIM profiles to corporate laptops, tablets, and ruggedized scanners requires manual onboarding by IT staff.

The CBA Business Case

- **Zero-Trust LAN/WAN Alignment:** Because 3GPP TS 33.501 supports EAP-TLS natively for 5G primary authentication in private/non-public network deployments, Private 5G networks can behave exactly like secure corporate Wi-Fi.
- **Leveraging Existing Infrastructure:** Enterprises don't need to issue new credentials. An Operator can deploy a Private 5G network that authenticates client devices using the same X.509 certificates already pushed to those devices by the company's existing Mobile Device Management (MDM) platform via SCEP/Intune-style enrollment — the identical mechanism already used to secure enterprise Wi-Fi (802.1X/EAP-TLS) today.
- **Unified Enterprise Policy:** This enables a single, unified security policy across Wi-Fi, Ethernet, and Private 5G, turning Private Cellular into a friction-free extension of the corporate Local Area Network (LAN).

3. Massive IoT Simplicity: True Zero-Touch Provisioning

The modern IoT market presents massive recurring revenue, but scaling via SIMs introduces severe operational bottlenecks.

The Friction of SIM-Based IoT

- Deploying thousands of remote devices requires managing regional SIM variants or configuring complex multi-IMSI roaming tables.
- If a fleet of devices changes network ownership or requires a credential rotation, pushing remote over-the-air (OTA) SIM updates to battery-constrained IoT devices often results in high packet-drop failures and severe power drain.

The CBA Business Case

- **"In-Factory" Identity Embedding:** Devices can be manufactured with a root cryptographic certificate securely provisioned into a secure element or TPM at the factory level (the same device-identity model — e.g., IEEE 802.1AR — already used for zero-touch onboarding in AWS IoT and Azure IoT deployments).
- **Zero-Touch on the Operator's Footprint:** When an industrial IoT device or satellite terminal powers up for the first time, it can locate and authenticate against the operator's own private/SNPN network — or any partner network with which the operator has a certificate-trust (CH-AAA) relationship — presenting its certificate without needing local carrier activation, SIM profile queues, or physical staging.
- **Seamless Lifecycle Management:** Device certificates can be rolled over or renewed automatically during routine software and firmware updates, eliminating cellular carrier profile management entirely.

4. Mission-Critical Resilience: First Responder & Disaster Deployment

During First Responder and Natural Disaster events, public commercial cellular infrastructure frequently collapses due to damage, power, backhaul, or congestion. Operators providing and deploying mobile tactical cells require resilient, instant-on access control.

The Failure of SIMs in Disaster Scenarios

- If a first responder team brings an un-activated device or an off-network asset to a disaster zone, activating a new eSIM profile requires a stable, active internet connection back to an eSIM RSP. This requires a stable internet connection which may not be readily available, so the device remains unconnected and offline.

The CBA Business Case

- **Local Edge Autonomy:** CBA authenticates via a cryptographic chain of trust rooted in a certificate authority (CA) that can be pre-positioned at the edge. The 5G network forwards the EAP-TLS exchange to a co-located AAA/RADIUS server, which validates a first responder's device certificate — provided that certificate was already issued before deployment — against a locally cached root/intermediate CA and revocation list, requiring no live link back to a central authentication server. SIM-based deployable cores with a locally cached HSS/UDM can likewise authenticate previously known devices offline; CBA's real advantage is that certificates can be pre-positioned and validated locally without depending on a live path back to a specific carrier's centralized HLR/HSS.
- **Phishing & Intercept Resistance:** Because EAP-TLS is mutual — the device validates the network's certificate and the network validates the device's certificate — a first responder's device will only connect to a verified, trusted network, protecting operational security during a crisis. This is a meaningfully stronger guarantee than SIM-based 5G-AKA, which authenticates the device to the network but historically has been more exposed to rogue base-station (IMSI-catcher style) attacks at the RAN layer.

5. Uniform Cross-Carrier Connectivity: The Neutral Host Multiplier

Neutral Host operators (venue owners, enterprises, and infrastructure investors) don't need to build a dense, nationwide macro-cellular footprint. Instead, they deploy hyper-localized infrastructure (campus-scale private networks, in-building small cells, and shared-RAN systems) in the high-traffic zones where data demand is most concentrated: stadiums, airports, hospitals, office campuses, transit hubs. Rather than every visitor depending on whatever macro signal happens to reach that location, the NH Operator stands up a dedicated local network and makes it available to everyone on-site, regardless of which national carrier they normally subscribe to. Operating as a Neutral Host means allowing subscribers from Public MNOs to seamlessly attach to and use that local network as if it were a native extension of their own carrier's footprint.

How This Actually Works Today (Important Correction)

For a standard consumer smartphone, this already works — and it works because of the SIM, not in spite of it. In a CBRS MOCN neutral host deployment, the phone attaches to the shared RAN using its existing carrier SIM; the neutral host operator routes that session back to the subscriber's home MNO core over a commercial roaming agreement, and the MNO authenticates it with standard 5G-AKA. No new credential is issued to the phone. CBA does not replace this mechanism for a consumer's primary carrier line — a mainstream phone isn't going to accept an NH Operator-issued certificate as a substitute for its home carrier's SIM authentication.

Where CBA Genuinely Changes the Picture

The class of devices that don't carry a public-MNO SIM at all — enterprise-managed laptops, tablets, ruggedized handhelds, and IoT/OT equipment, plus non-3GPP access — is where CBA changes the picture. For that population, per-carrier roaming agreements and SIM issuance don't scale, and a certificate-based model does:

- **A Federated Identity Passport for 5G:** 3GPP Release 17 already defines the "Credentials Holder using AAA Server" (CH-AAA) model allowing an SNPN to authenticate a device using credentials owned by a separate trusted entity rather than a subscription tied to that specific network. This makes a CBA-issued certificate a federated identity in its own right: any network with a trust relationship to that same Credentials Holder can recognize it. An enterprise or IoT certificate issued once can therefore validate against an NH Operator's own network and any partner SNPN or neutral host network sharing that Credentials Holder relationship, without a new certificate, a new SIM, or a bilateral roaming agreement for each hop. This is standards-grounded federation on the 5G side; it does not extend to a consumer's Public MNO session, which remains governed by SIM/5G-AKA and commercial roaming agreements.
- **Unified Policy for Non-SIM Assets:** For the enterprise/IoT device population, a single certificate-based profile lets a device move between an NH Operator's private enterprise network and its public neutral-host footprint (and any federated partner networks), authenticating consistently everywhere without a carrier relationship or MOCN roaming agreement for each hop.

Conclusion

Continuing down the path of traditional cellular SIM cards means accepting structural margins and onboarding workflows controlled by legacy telecom paradigms. Supporting Certificate-Based Authentication (CBA) for strategic Public and Private 4G/5G infrastructure — grounded in 3GPP TS 33.501's EAP-TLS support and the Release 17 CH-AAA model — transitions these companies from hardware-bound utility operators into highly agile, asset-light, cloud-native connectivity platforms that speak the native security language of modern enterprise IT.

References

- 3GPP TS 33.501 — Security architecture and procedures for 5G systems (Annex B: EAP-TLS for private network primary authentication) — https://itecspec.com/3gpp/33.501
- 3GPP — Security features for Non-Public Networks (Release 17 Credentials Holder / AAA Server model) — https://www.3gpp.org/technologies/sec-npn
- 3GPP — Non-Public Networks (NPN) overview — https://www.3gpp.org/technologies/npn
- RCR Wireless — MOCN vs MORAN, neutral-host systems in CBRS — https://www.rcrwireless.com/20251010/fundamentals/mocns-versus-moran-cbrs
- OnGo Alliance — CBRS Neutral Host Networks for enterprises — https://ongoalliance.org/cbrs-neutral-host-networks-a-new-option-for-enterprises/
- Smallstep — Deploy EAP-TLS Wi-Fi to Windows via Intune (MDM/SCEP certificate issuance model) — https://smallstep.com/docs/tutorials/intune-mdm-setup-guide/