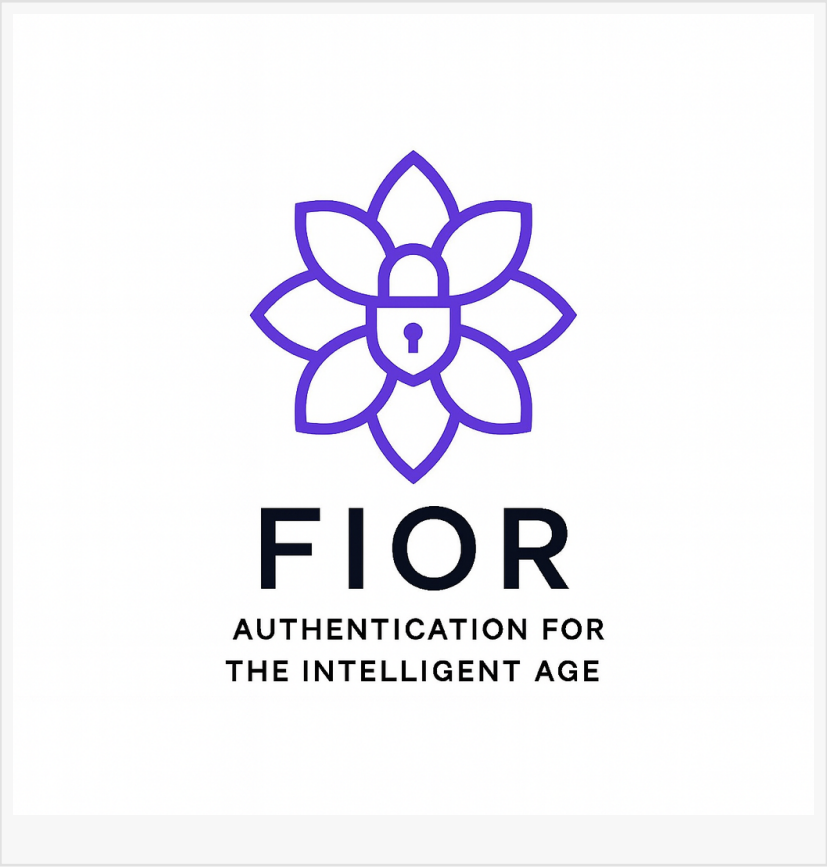
FIOR eSIM Identity Product Prevents Surging e-SIM Fraud

Hardware-rooted identity attestation solution delivers mutual device verification, anti-replay protection, and immutable audit trails with easy implementation.



BARCELONA, SPAIN, March 3, 2026 /EINPresswire.com/ -- Fior Group, a leader in identity infrastructure for autonomous systems, today announced the general availability of its eSIM Identity Verification Layer. It's a drop-in security overlay for the GSMA eSIM Open Gateway that adds application-layer identity attestation to the standard SM-DP+ provisioning flow.

SIM swap fraud cases exploded 1,055% in 2025 in the UK alone. According to a recently released Federal Trade Commission (FTC) report, U.S. consumers alone reported losing more than $12.5 billion to various types of fraud in 2024, including phone calls and text messages, a 25% increase over the prior year. The telecom industry loses at least $45bn to fraud.

The GSMA's eSIM Open Gateway specification defines how Mobile Network Operators (MNOs) remotely provision eSIM profiles to consumer and IoT devices at scale. While the standard mandates TLS for transport encryption, it does not include application-layer identity verification. This means any device that completes a TLS handshake can claim any identity without cryptographic proof. This architectural gap exposes carriers to a growing class of identity-based attacks: device impersonation, SM-DP+

> Fior creates cryptographic proof that every device is who it claims to be and every provisioning event is secure, immutable and auditable". This transforms eSIM security."
>
> *David Williams, Founder, Fior*

spoofing,
provisioning session replay, and eSIM identity cloning.

How it Works

Fior's eSIM Identity Layer integrates at the SM-DP+ API boundary, sitting between the carrier's provisioning infrastructure and the device without modifying the GSMA protocol or requiring new hardware. The solution delivers six layers of identity security:

• Hardware Device Binding: Cryptographically ties every eSIM profile to the device's TPM or Secure
Enclave.
• Mutual Identity Attestation: Both the device and SM-DP+ server prove their identity at the application layer.
• Nonce-Bound Sessions: Every provisioning session includes a unique cryptographic nonce against
replay.
• Cryptographically-Signed Profiles: Every eSIM profile is digitally signed enabling tampering detection.
• Offline Identity Verification: Devices verify signatures without network connectivity in under 5ms.
• Immutable Audit Trail: Every event generates a cryptographic proof hash for compliance and forensics.

CAMARA API Integration

The eSIM Identity Layer works in concert with Fior's existing GSMA CAMARA API security suite, including SIM
Swap Detection, Number Verification, and Device Status, to provide end-to-end identity protection across
the carrier ecosystem.

Carrier Business Impact

• Drop-in integration at the SM-DP+ API layer — no protocol changes required
• Less than 5ms verification overhead per provisioning event
• 100% identity attestation coverage across all provisioned devices
• New premium tier: "Verified Identity eSIM" as a value-added service
• Full compliance with EU Digital Identity Wallet and eIDAS 2.0

Commenting at Mobile World Live, David Williams, Fior Founder, said: "The GSMA eSIM Open Gateway
is a transformative standard for the carrier ecosystem, but it was rightly designed for

interoperability, not
identity verification. Fior completes the picture by adding the cryptographic proof that every device is who
it claims to be, every server is who it claims to be, and every provisioning event is secure, immutable and
auditable".
Come and see us at Hall 6, Stand G84 (6G84) at Mobile World Live from March 2nd to March 5th.

About Fior Group
FIOR Group provides cryptographic identity and governance infrastructure for the autonomous economy.
The company's platform secures AI agent identity, eSIM provisioning, CAMARA telecom APIs, enterprise AI
gateways and any network infrastructure with hardware-rooted trust using NIST AAL3 Certified quantum-safe cryptography, and zero-trust policy enforcement. FIOR is ISO 42001 aligned and serves carriers,
enterprises, and AI platform providers globally.
Media Contact
FIOR Group Press Office - thomas@fior.group - https://fior.group/
References
I. https://netnumber.com/phone-validation-blind-spot-report-2025/
II. https://www.ftc.gov/news-events/news/press-releases/2025/03/new-ftc-data-show-big-jump-reported-losses-fraud-125-billion-2024
III. https://arxiv.org/abs/2311.00724

David Williams
Fior Group Limited
email us here
Visit us on social media:
LinkedIn
