

IETF 127 · EMU WG · NOVEMBER 2026

EAP-WSIM

SIM-based EAP for Wi-Fi with no live MNO backend: the missing link for seamless mobility between Wi-Fi and 5G/6G

Praveen Gupta · MobileStack, Inc.

draft-gupta-emu-eap-wsim-01

THE PROBLEM · IN NUMBERS

The traffic is on Wi-Fi. The SIM is not.

82–89%

of US smartphone data is offloaded to Wi-Fi, on every major operator (Opensignal)

~80%

of calls are made indoors, where Wi-Fi is the coverage [confirm survey source]

- Operator devices join venue Wi-Fi with PSK or guest access. The SIM is used only inside the IPsec tunnel.
- The Wi-Fi cannot see that the device belongs to an operator, so it cannot treat the call as a call.
- The Wi-Fi stack is outside operator device compliance, so handover between APs varies by device.

THE PROBLEM · WHY TODAY'S TOOLS FALL SHORT

OpenRoaming and Passpoint do not close the gap

60%

invest in OpenRoaming or Passpoint to get seamless access between Wi-Fi and 5G/LTE

70%

have deployed one of them, or plan to in 2026

What they deliver

Automatic, secure onboarding and a roaming federation across venues.

What they leave open

- The operator's device is not visible to the Wi-Fi as an operator device.
- SIM authentication still needs the operator's AAA on every attach.
- Voice handover between APs, and inbound and outbound roaming, are not solved.

EAP-WSIM Authentication completes at the venue

Device + SIM
The subscriber's existing SIM credential (WSIM-Card)

→

Wi-Fi AP
Receives PMK-R1 and per-subscriber WMM policy

→

WSIM-AS
Venue EAP server; MASTER KEY in tamper-resistant hardware

MNO core
Provisions key material once per venue. Not in the authentication path

MILENAGE + ML-KEM-768

Mutual authentication from the SIM. A fresh KEM exchange per session adds post-quantum forward secrecy.

The MSK stays local

PMK-R0 and PMK-R1 are derived at the venue, so 802.11r fast transition works for SIM-authenticated devices.

Identity at association

The Wi-Fi knows which operator's subscriber it is serving before any tunnel exists.

WHY EAP-WSIM · THE MISSING LINK

The gap sits between four standards bodies

Body	What exists for Wi-Fi and cellular	What it still depends on
3GPP	N3IWF, TNGF and ATSSS anchor Wi-Fi in the core	A reachable core for every authentication
IEEE 802.11	802.11r fast transition; 802.11bn roaming	An MSK at the venue, bound to the subscriber
WBA	Passpoint and OpenRoaming federation	The home AAA answering on every attach
IETF EMU	EAP-AKA′, EAP-AKA′ FS, PQC drafts for AKA′	An offline SIM-based method: EAP-WSIM

MobileStack is leading this discussion in WBA. WBA, 3GPP and IEEE can specify deployment;

only the IETF can define the EAP method.

USE CASES

Where SIM authentication at the Wi-Fi matters

01 · In-building

Wi-Fi DAS

Venue Wi-Fi as indoor coverage for every operator's subscribers: SIM onboarding, no portal, voice-grade roaming between APs.

02 · Aircraft cabin

In-flight Wi-Fi

Authentication completes on board: no home-AAA round trips over the satellite link, and it survives backhaul outages.

03 · Campus, hospital, stadium

Enterprise VoWiFi

Visitors' phones authenticate with the SIM, with no PKI enrolment. Calls survive AP changes with per-subscriber voice QoS.

04 · Operator to operator

Inbound and outbound roaming

Roaming on Wi-Fi requires the operator's device to be visible at the Wi-Fi layer. Today it is anonymous behind a tunnel.

3GPP DISCUSSION · SA2 FS_6G_ARC · TR 23.801-01

3GPP is deciding now how Wi-Fi fits into 6G

v0.9.0

Draft of the 6G architecture study after SA2#176, September 2026

Mar 2027

SA2 target for concluding the study

Rel-21

Expected first normative 6G specifications

- Non-3GPP access is a key issue of the study: untrusted access, Wi-Fi offload, service continuity.
- SA2 is coordinating with SA3 on authentication for non-3GPP access.
- CT1's work on the secure tunnel for non-3GPP access is waiting on SA2 and SA3.

An IETF WG item during the study window gives SA2 and SA3 an offline SIM-based method they can cite.

3GPP DISCUSSION · WI-FI LOCAL BREAKOUT FOR 6G TRAFFIC

Local breakout needs an authenticated subscriber

Today

- The tunnel to the ePDG or N3IWF is used in practice for Wi-Fi Calling only.
- Everything else breaks out locally with no operator identity, policy or QoS attached.
- Home-routing all traffic would hairpin venue traffic through the core.

With EAP-WSIM

- SIM authentication at Layer 2, completed at the venue.
- Data breaks out locally under a known subscriber identity and per-subscriber WMM policy.
- Only services that need the core, such as IMS voice, are tunnelled.
- 802.11r keeps the session across APs.

Offload and service continuity over Wi-Fi are in the 6G study scope. Both start with knowing who is on the Wi-Fi.

THE ASK

Adopt EAP-WSIM, or name the steps to adoption

1 · Scope

Chairs and AD: is an offline SIM-based EAP method within the EMU charter? If not, which charter text or dispatch path applies?

2 · Review

Two or three WG reviewers for the draft, and a cryptographic review of the MILENAGE-ML-KEM-FWD construction.

3 · Coordination

Raise it at IETF–3GPP coordination while the 6G study is open. Keep WBA and IEEE 802.11 informed.

4 · Adoption call

A call for adoption on the list after WG review. Comments to emu@ietf.org.