# Unlocking the Potential of Private 6G Networks: Converging OpenRoaming and Cellular Connectivity for Public Safety and Emergency Response

IIT RTC 2025

Charles Eckel, Cisco Systems
eckelcu@cisco.com

October 8, 2025

# Agenda

01 OpenRoaming

02 Cellular roaming and private networks

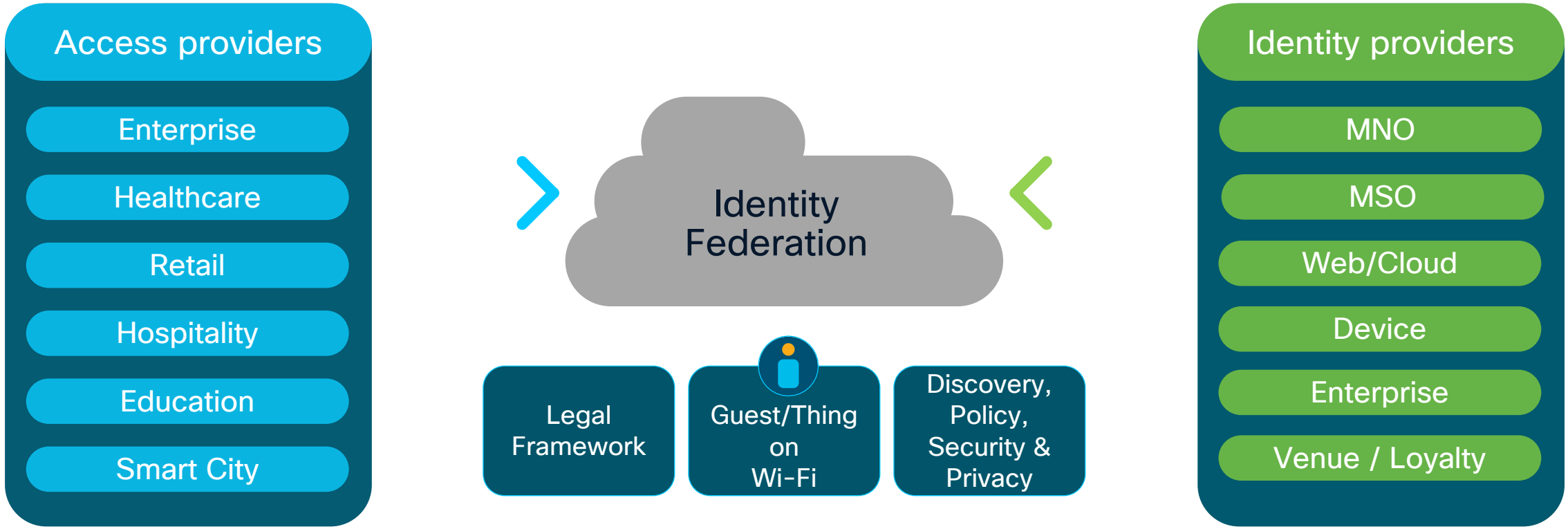
03 SNPN cellular hotspots

04 Public safety and emergency response

05 Key takeaways and next steps

# OpenRoaming

# OpenRoaming: A standardized approach to federated roaming, covering technical, legal, and (optional) financial aspects

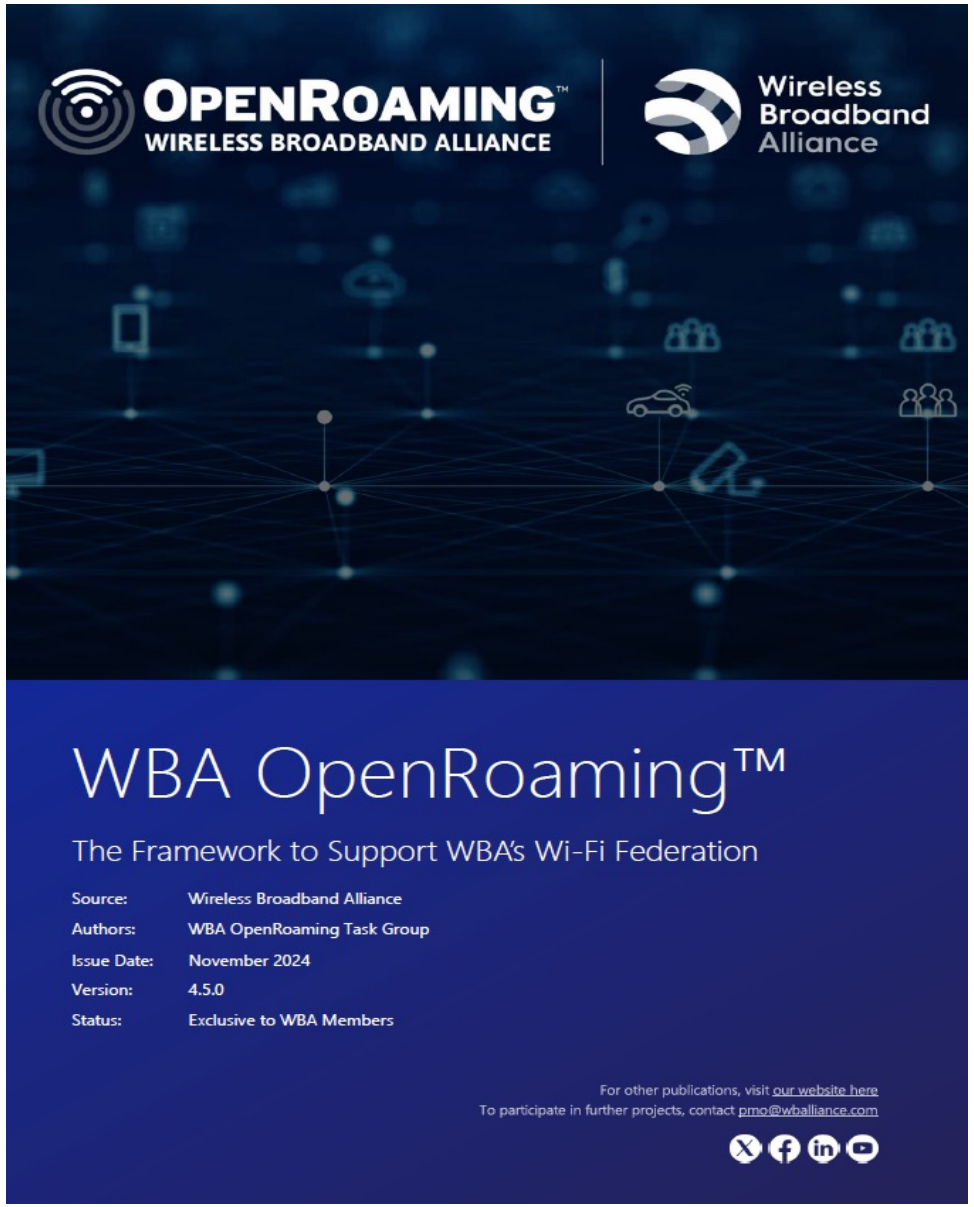



OpenRoaming is a federation of identity & access providers to enable automatic, seamless, and secure roaming

# Legal framework


- Privacy policy
- End-user terms and conditions
- Database operations
- Templated agreements with some immutable terms
  - Settlement free
    - Broker-to-ANP
    - Broker-to-IDP
  - OpenRoaming settled
    - Broker-to-Broker
    - Broker-to-ANP
    - Broker-to-IDP

# Technical framework




- Passpoint profiles and Roaming Consortium Organization Identifiers (RCOIs)
- DNS discovering, including special handling of 3GPP realms
- PKI, certificate chains, and mTLS
- RADIUS attributes
- Service Level Requirements (Bronze/Silver/Moving)
- Published as an IETF Internet-Draft

# OpenRoaming: Top Level Architecture Framework

1) Agree legal terms between WBA and brokers including required use of templates with providers

WBA: Federation Policy Authority
Publishes PKI certificate policy and templated legal terms. Operates private CR root and policy I-CA. Assigns primary WBAIDs to members.

Ecosystem Brokers:
Operates Issuing I-CA/RA and assigns subordinate WBAIDs under primary namespace

2) Agree legal terms including those regarding privacy. Issue certificate to provider.

3) Agree legal terms including those regarding end user prohibited conduct. Issue certificate to provider

Access Provider:
Configure RCOI (s) according to policy, installs PKI certs

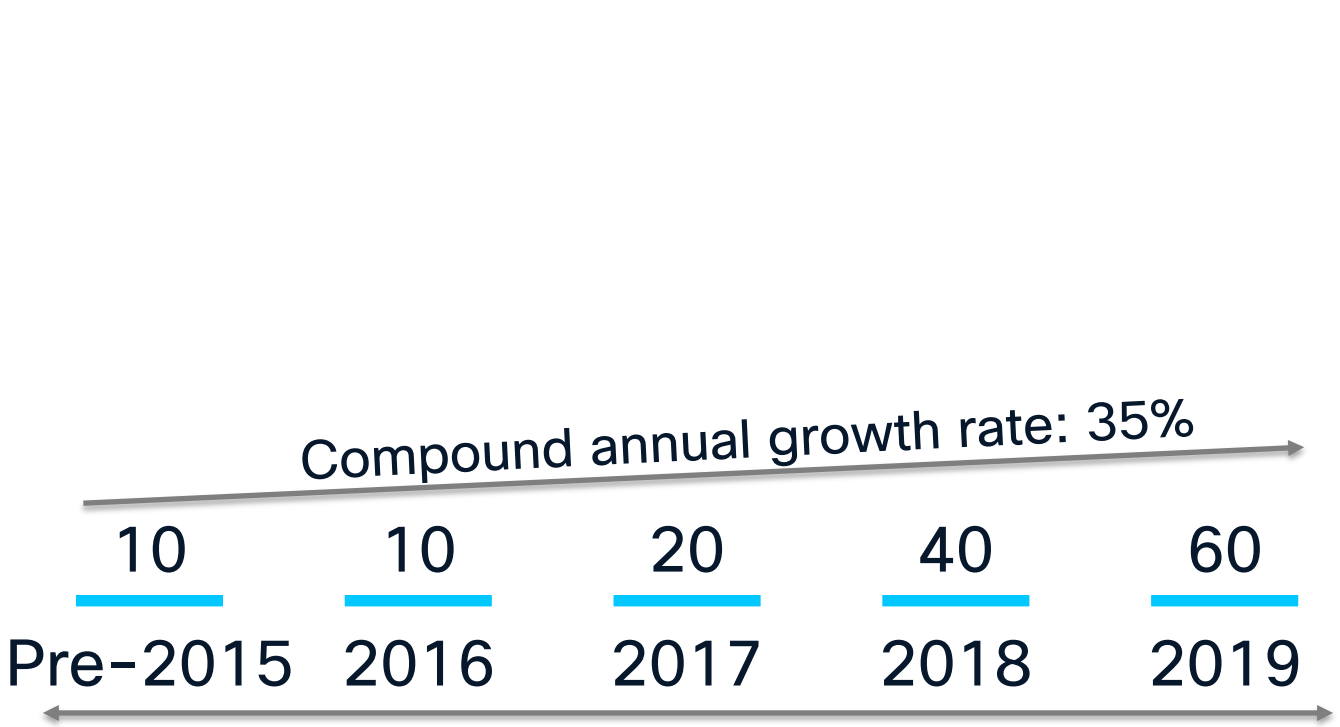
EAP/AAA/TLS

DNS

Identity Provider:
Configure RCOI polices in Passpoint profile, configure DNS for dynamic discovery, install PKI certs

# Federation to scale private network roaming

## Estimated total number of individual private networks enabled for Wi-Fi roaming



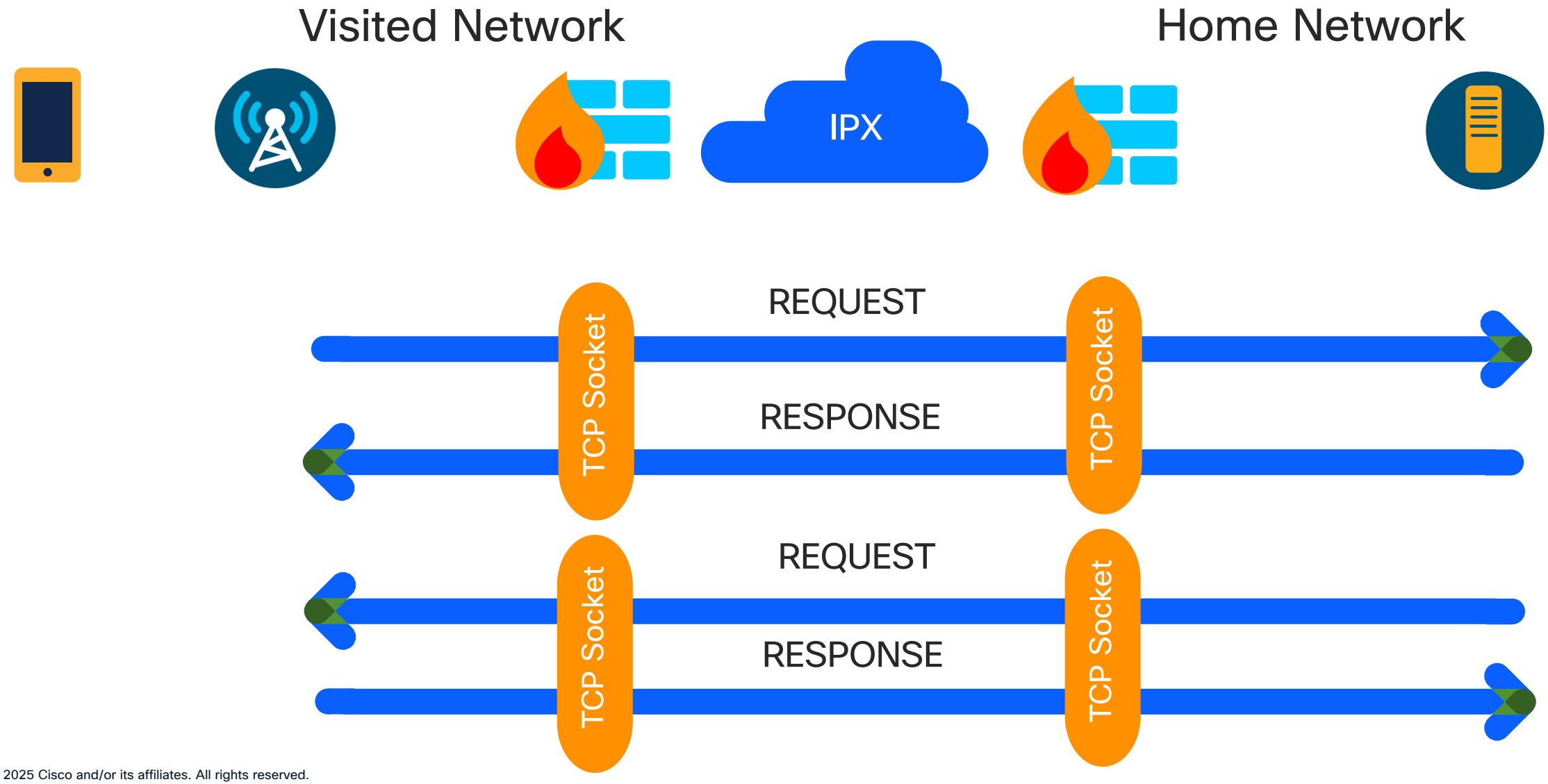

Roaming deployments mostly based on bilateral carrier agreements


Federation approach accelerates adoption of roaming by private networks

# Cellular roaming and private networks

# Inter-Carrier Roaming: Bi-directional Signaling

## Security Edge Protection Proxy (SEPP)



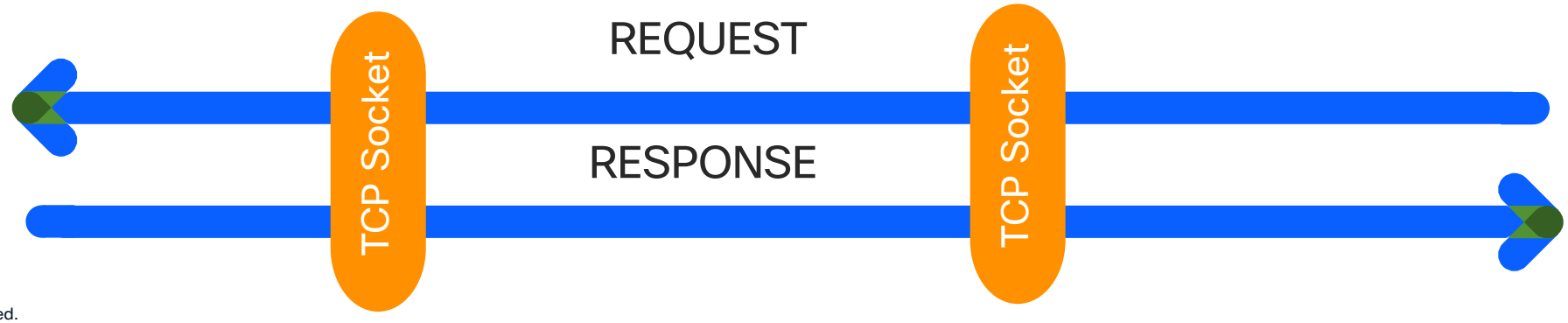
# Inter-Carrier Roaming: Bi-directional Signaling

## Security Edge Protection Proxy (SEPP)


1. REGISTER OWN IP@
2. RECOVER PARTNER IP@
3. CONFIGURE FIREWALL

1. REGISTER OWN IP@
2. RECOVER PARTNER IP@
3. CONFIGURE FIREWALL

Central database of signaling endpoint IP@
(GSMA:IR.21)



# Scaling for Private Networks

## Public Networks Signaling

- 100,000 active roaming agreements
- 120 Billion roamer records exchanged per year
- ~120 Million roamer records per network per year
- ~1.2 Million records/year per agreement

(Source: GSMA)

## Private Networks Signaling

- Sample private OpenRoaming network delivers 235 in-bound client auths/day
- ~1/1000th of typical public network roaming volume
- Roaming procedures need to be radically simplified to be relevant to private networks

## Scaling Number of Networks

- ~800 public cellular networks
- Globally, there will be nearly 628 million public Wi-Fi hotspots by 2023 (Cisco)
- By end of decade, there will be over 1 million private cellular networks in Europe (Vodafone)

1000 times more networks, each with 1/1000$^{th}$ of the signaling load

# SNPN cellular hotspots

# Release 19 SA1 study and work item on interconnection of Standalone Non-Public Networks (SNPNs)

3GPP TS 22.261 V19.6.0 (2024-03)

*Technical Specification*

**3rd Generation Partnership Project;**
**Technical Specification Group Services and System Aspects;**
**Service requirements for the 5G system;**
**Stage 1**
**(Release 19)**

5G ADVANCED

3GPP A GLOBAL INITIATIVE

The present document has been developed within the 3rd Generation Partnership Project (3GPP™) and may be further elaborated for the purposes of 3GPP..
The present document has not been subject to any approval process by the 3GPP Organizational Partners and shall not be implemented.
This Specification is provided for future development work within 3GPP only. The Organizational Partners accept no liability for any use of this Specification.
Specifications and Reports for implementation of the 3GPP™ system should be obtained via the 3GPP Organizational Partners' Publications Offices.

## 6.25.4 SNPN cellular hotspots

- The following requirements apply to support of Stand-alone Non-Public Network (SNPN) cellular hotspots:
  - NOTE 1: SNPN hotspot refers to a connectivity hotspot based on 3GPP 5G network technology that **provides services in a similar way as provided by WLAN hotspots.** Charging requirements are considered out of scope for this functionality.
- Based on the SNPN configuration, the 5G network shall support a mechanism for an **SNPN to be able to interconnect with a large number of SNPN Credential Providers** with which the SNPN might **not have preconfigured information** detailing the IP addresses used by these SNPN Credential Providers to interconnect with the SNPN.
- Based on the SNPN configuration, the 5G network shall support a mechanism for an **SNPN Credential Provider to be able to interconnect with a large number of SNPNs** with which the SNPN Credential Provider might **not have preconfigured information** detailing the IP addresses used by these SNPNs to interconnect with the SNPN Credential Provider.
- Based on the SNPN configuration, the 5G network shall support a mechanism for an SNPN to be able to determine how to connect to an SNPN Credential Provider capable of verifying the identity presented by a user attempting to connect to that SNPN.
- **Based on the SNPN configuration, the 5G network shall support a mechanism for an SNPN to be able to securely interconnect with an SNPN Credential Provider in deployments where the required security information is not preconfigured.**
- Based on the SNPN configuration, the 5G network shall support a mechanism for an SNPN to enable an SNPN Credential Provider to securely notify events (e.g., a user's subscription ending) to the SNPN.



cisco

# Alignment with architectures defined in Release 17 by SA2

- SNPN Credentials Holder functionality is subset of that of Credentials Holder, as defined in 3GPP TS 23.501, “System architecture for the 5G System (5GS)”

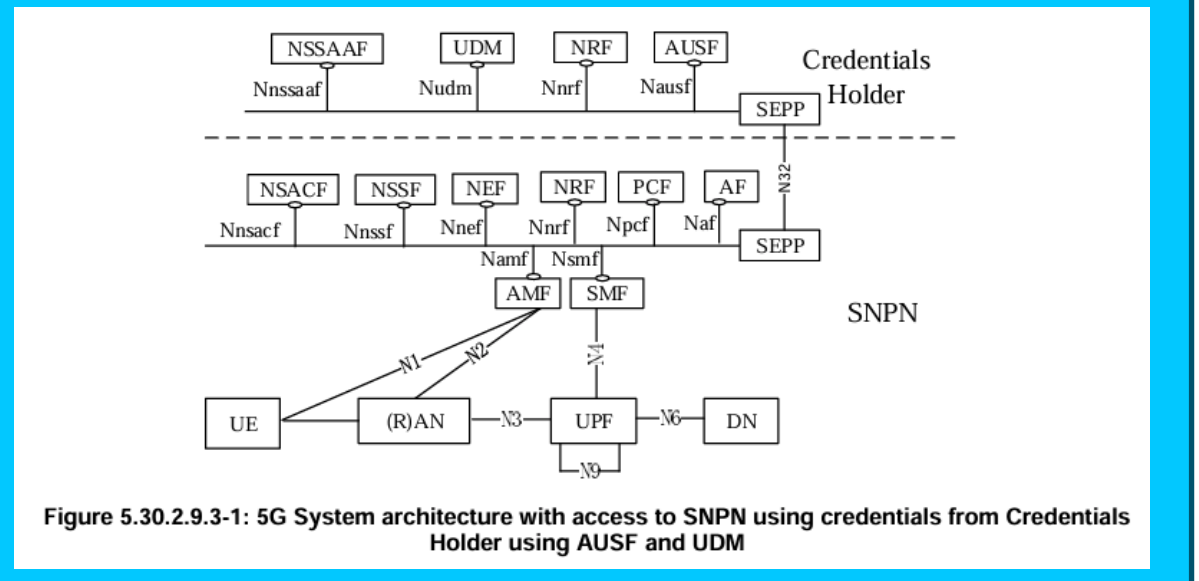



Figure 5.30.2.9.3-1: 5G System architecture with access to SNPN using credentials from Credentials Holder using AUSF and UDM

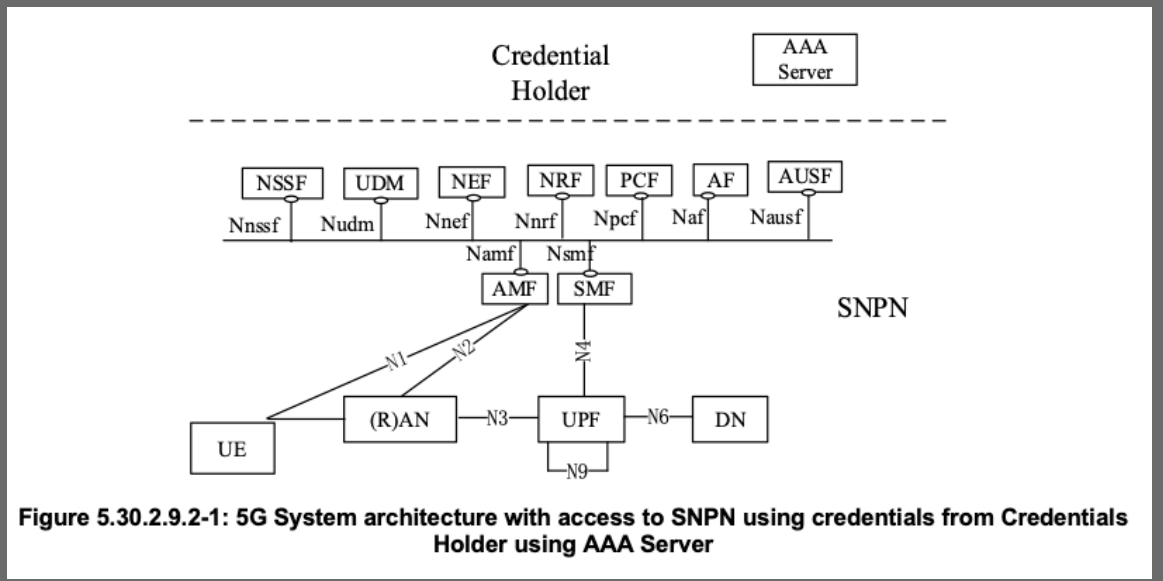
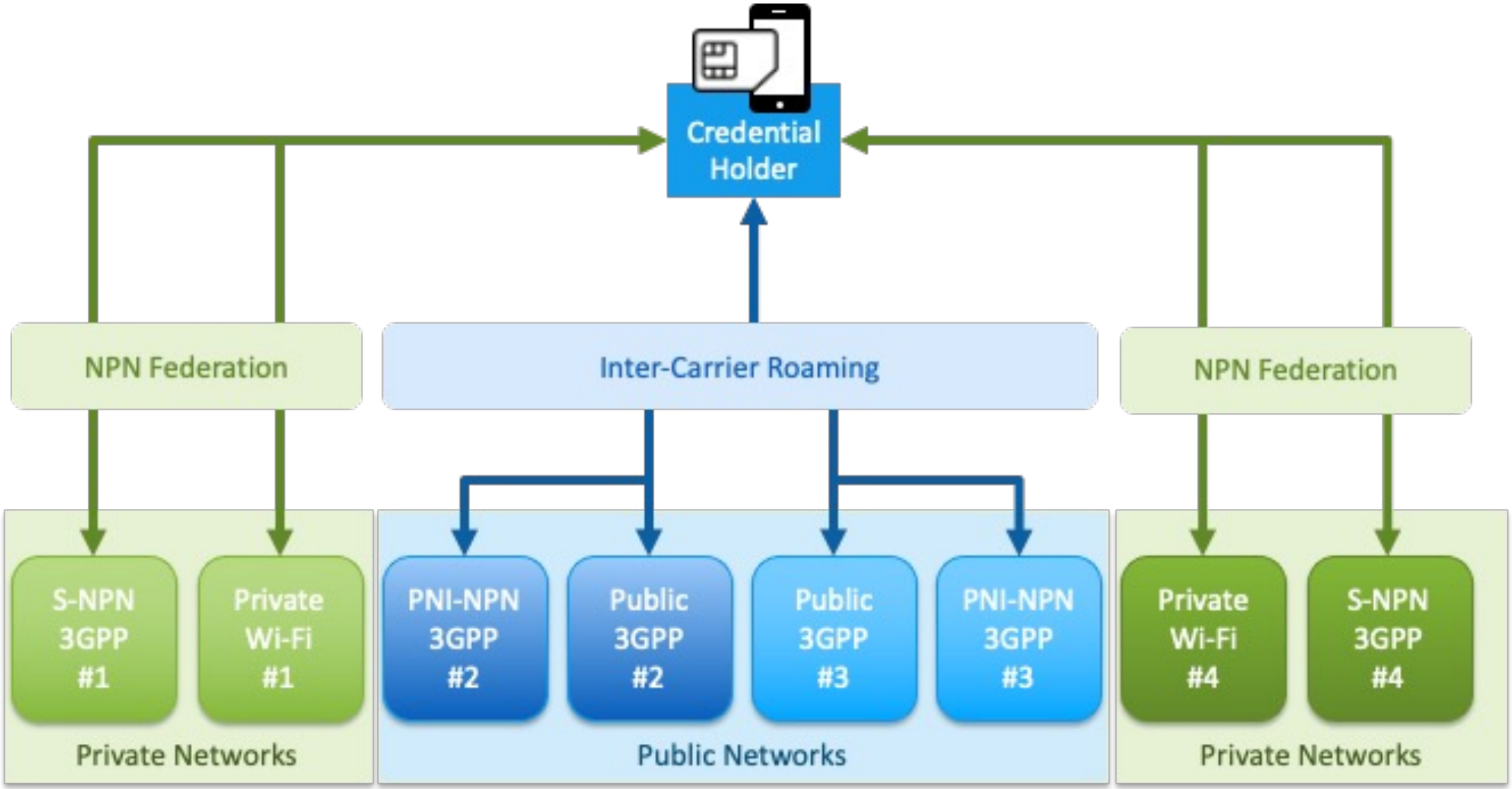



Figure 5.30.2.9.2-1: 5G System architecture with access to SNPN using credentials from Credentials Holder using AAA Server

- Primary authentication and authorization of UEs that use credentials from a Credentials Holder using AUSF and UDM seems better aligned with role of an Identity Provider.

# Extend public roaming model to private networks



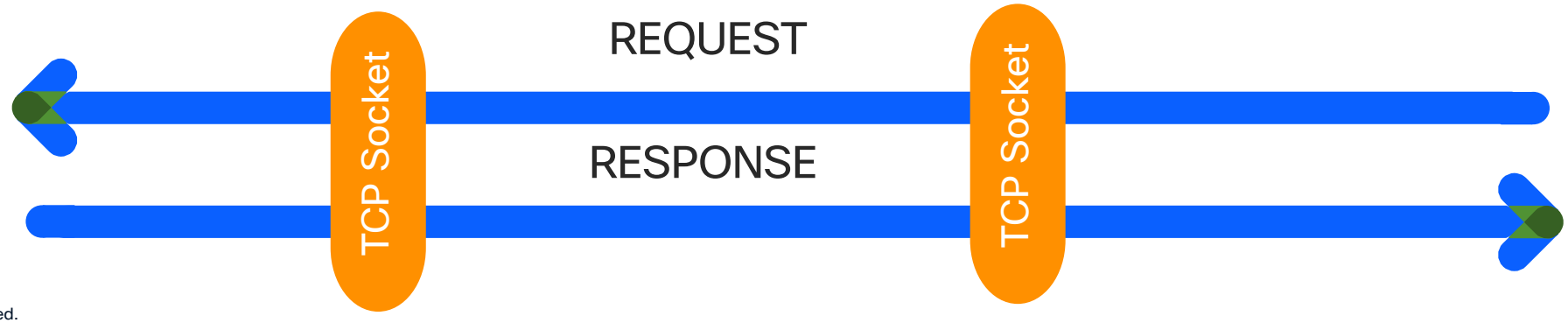
# Inter-Carrier Roaming: Bi-directional Signaling

## Security Edge Protection Proxy (SEPP)


1. REGISTER OWN IP@
2. RECOVER PARTNER IP@
3. CONFIGURE FIREWALL

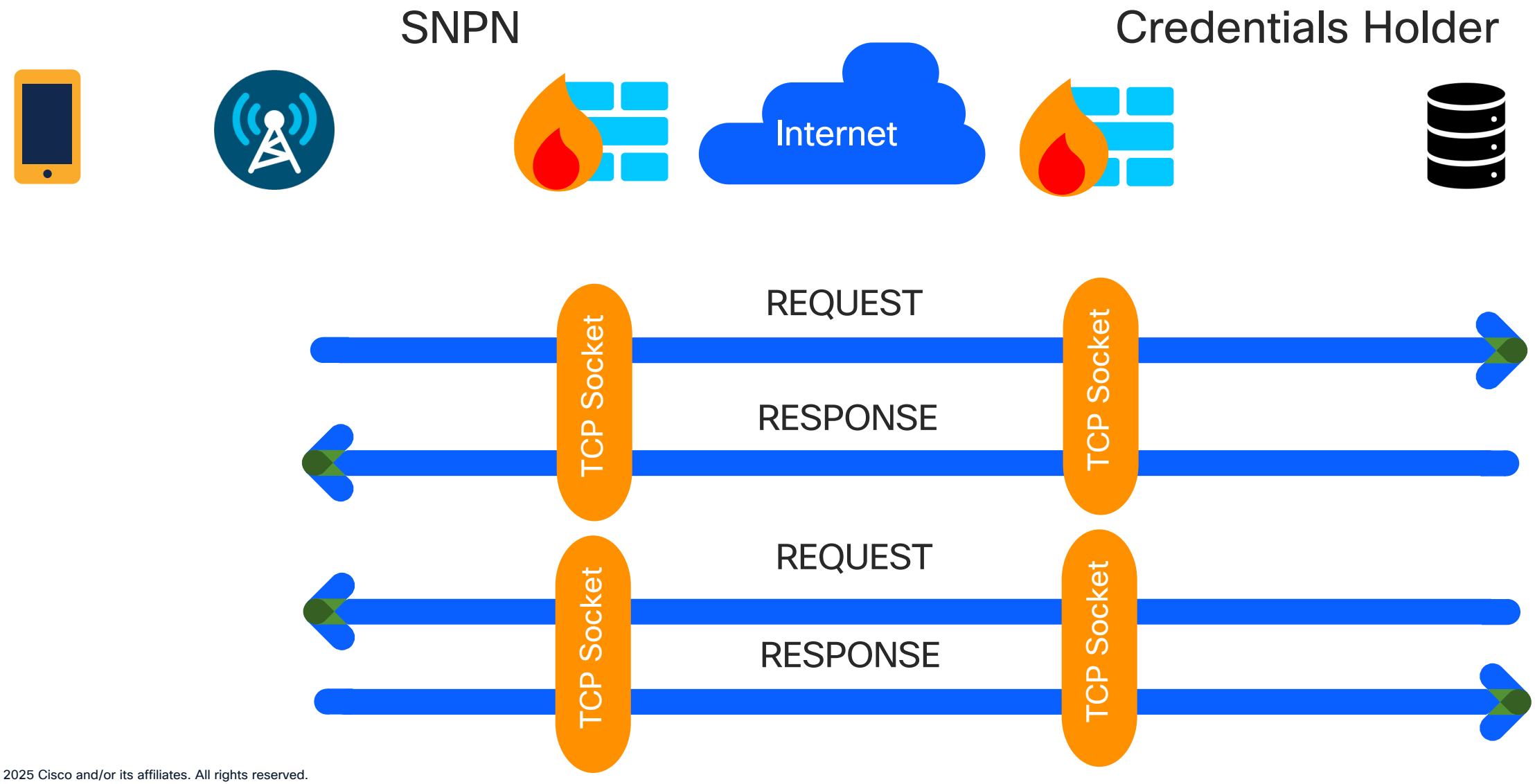
1. REGISTER OWN IP@
2. RECOVER PARTNER IP@
3. CONFIGURE FIREWALL

Central database of signaling endpoint IP@
(GSMA:IR.21)



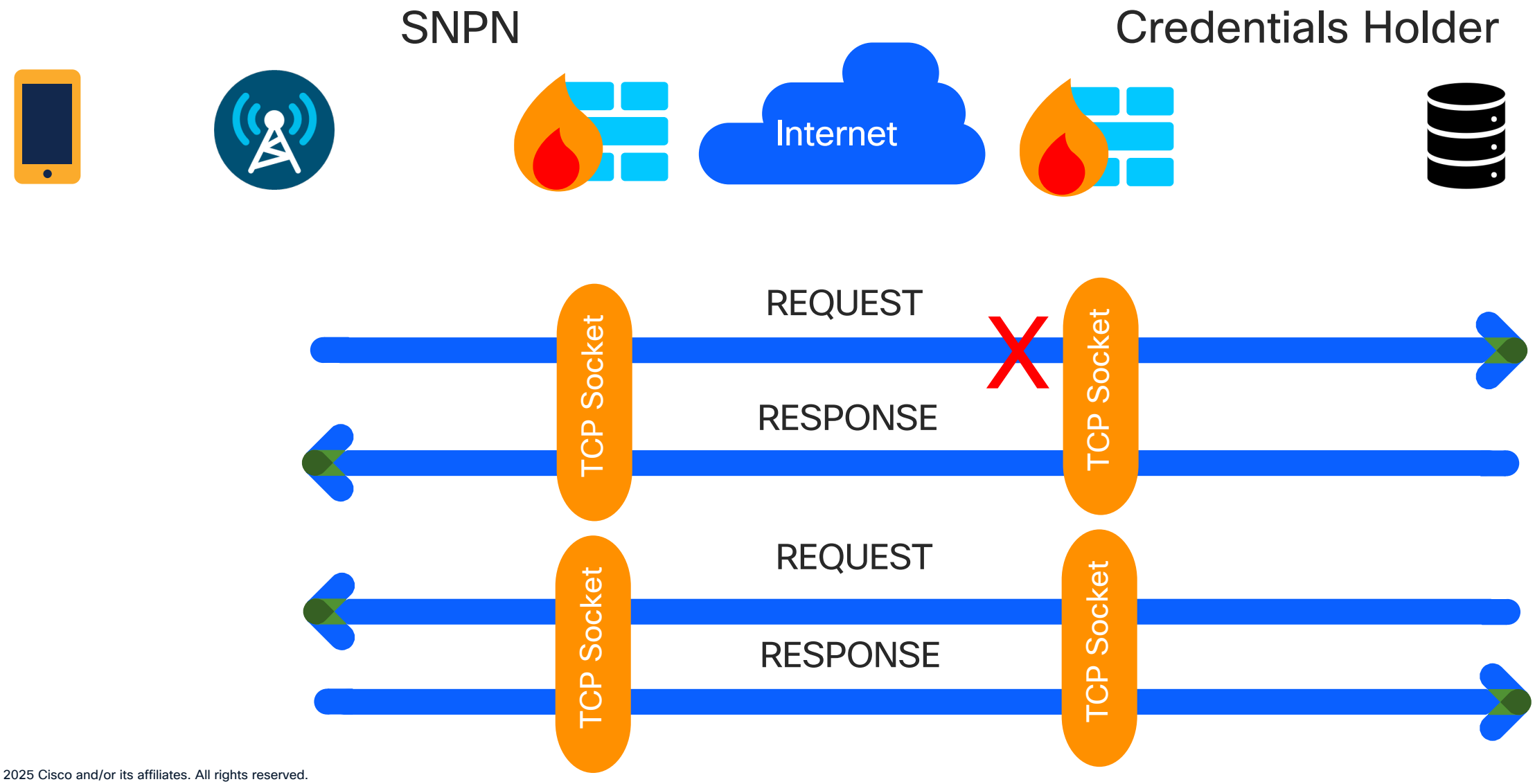
# SNPN Cellular Hotspot: Bi-directional Signaling

## Security Edge Protection Proxy (SEPP)



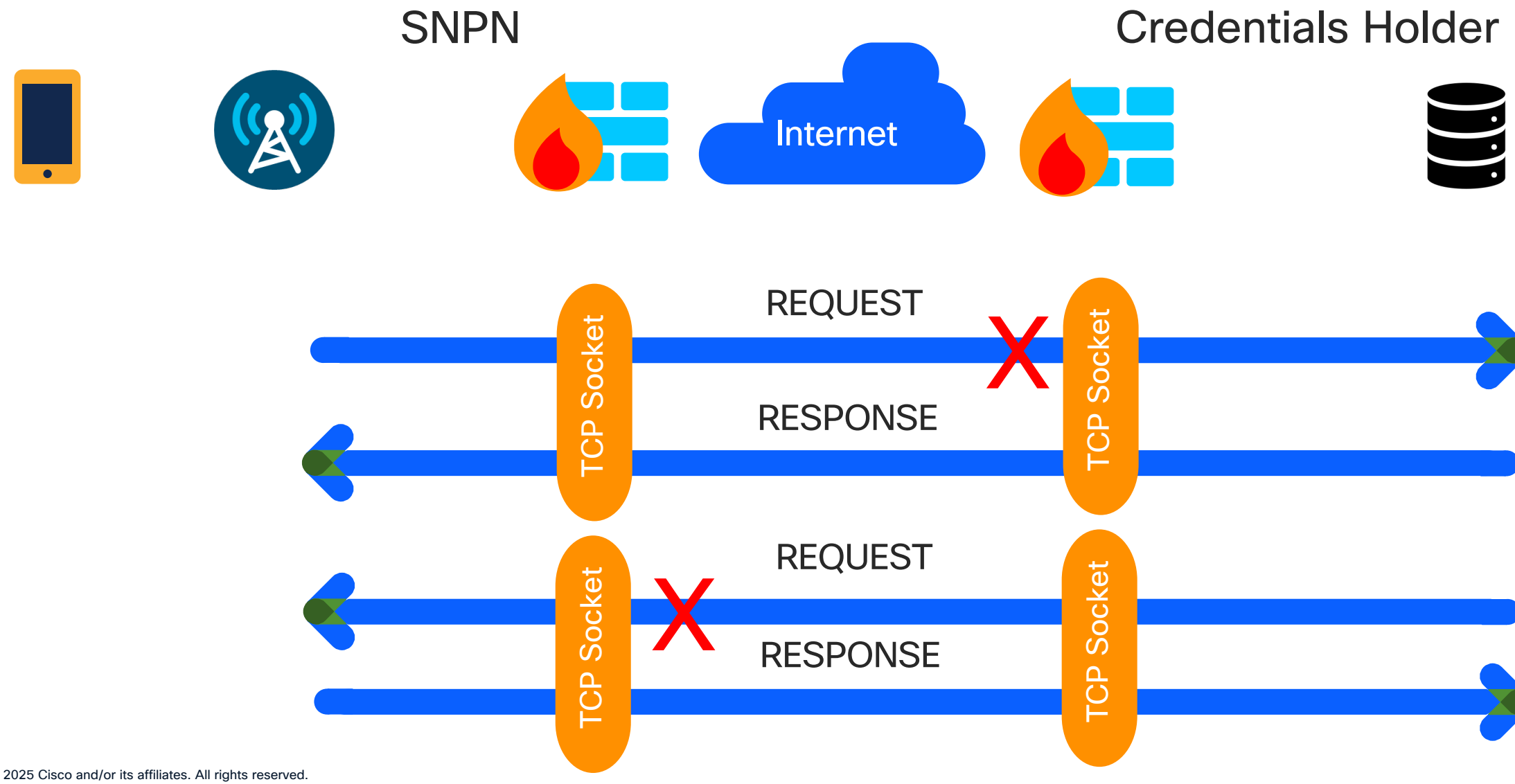
# SNPN Cellular Hotspot: Bi-directional Signaling

## Security Edge Protection Proxy (SEPP)

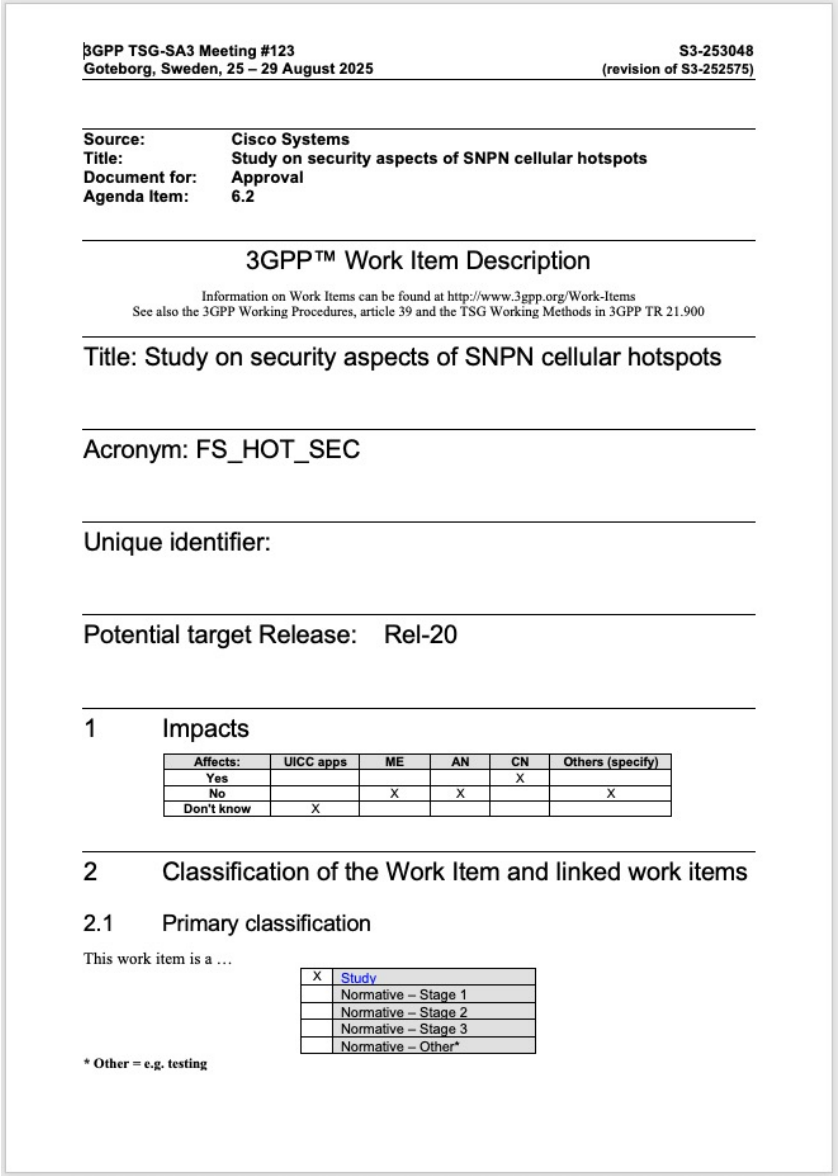


# SNPN Cellular Hotspot: Bi-directional Signaling

## Security Edge Protection Proxy (SEPP)



# Release 20 5G-Advanced, Study item proposal in SA3



3GPP TSG-SA3 Meeting #123 — S3-253048
Goteborg, Sweden, 25 – 29 August 2025 — (revision of S3-252575)

**Source:** Cisco Systems
**Title:** Study on security aspects of SNPN cellular hotspots
**Document for:** Approval
**Agenda Item:** 6.2

3GPP™ Work Item Description

Information on Work Items can be found at http://www.3gpp.org/Work-Items
See also the 3GPP Working Procedures, article 39 and the TSG Working Methods in 3GPP TR 21.900

Title: Study on security aspects of SNPN cellular hotspots

Acronym: FS_HOT_SEC

Unique identifier:

Potential target Release: Rel-20

1 Impacts

| Affects: | UICC apps | ME | AN | CN | Others (specify) |
|---|---|---|---|---|---|
| Yes | | | | X | |
| No | | X | X | | X |
| Don't know | X | | | | |

2 Classification of the Work Item and linked work items

2.1 Primary classification

This work item is a …

| | |
|---|---|
| X | Study |
| | Normative – Stage 1 |
| | Normative – Stage 2 |
| | Normative – Stage 3 |
| | Normative – Other* |

* Other = e.g. testing

- WT#1: Study and propose mechanisms that address the security aspects of SA1 requirements for SNPN cellular hotspots.

# Public safety and emergency response

# SNPNs can complement 3GPP's mission critical capabilities

## Emergency Services

IMS location routing to PSAP and PSAP recovering of dispatchable address.

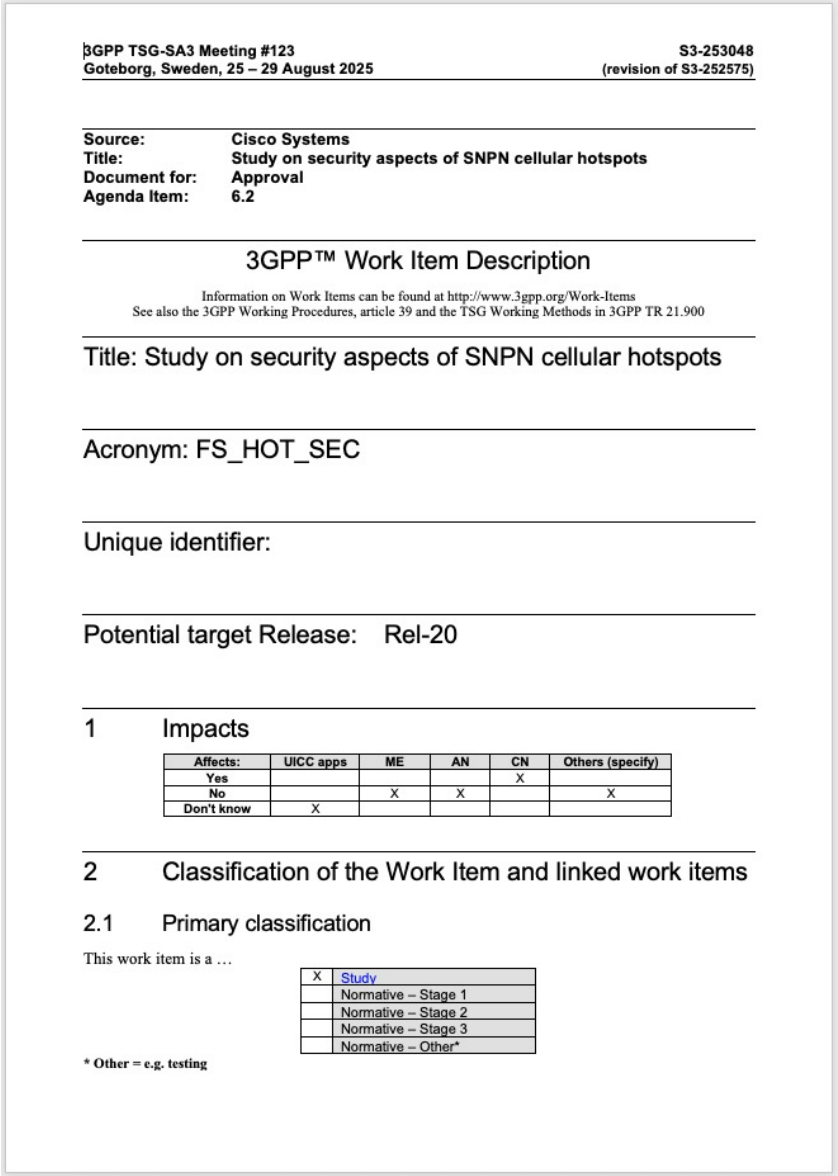
## Mission Critical Communications

Serving public safety organizations to ensure reliable and secure communications during emergencies.

## Public Warning Systems

Scaling communications of emergency alerts to the public.

# Original, and potential future/6G, study item



3GPP TSG-SA3 Meeting #123 — S3-253048
Goteborg, Sweden, 25 – 29 August 2025 — (revision of S3-252575)

**Source:** Cisco Systems
**Title:** Study on security aspects of SNPN cellular hotspots
**Document for:** Approval
**Agenda Item:** 6.2

3GPP™ Work Item Description

Information on Work Items can be found at http://www.3gpp.org/Work-Items
See also the 3GPP Working Procedures, article 39 and the TSG Working Methods in 3GPP TR 21.900

Title: Study on security aspects of SNPN cellular hotspots

Acronym: FS_HOT_SEC

Unique identifier:

Potential target Release: Rel-20

1 Impacts

| Affects: | UICC apps | ME | AN | CN | Others (specify) |
|---|---|---|---|---|---|
| Yes | | | | X | |
| No | | X | X | | X |
| Don't know | X | | | | |

2 Classification of the Work Item and linked work items

2.1 Primary classification

This work item is a …

| | |
|---|---|
| X | Study |
| | Normative – Stage 1 |
| | Normative – Stage 2 |
| | Normative – Stage 3 |
| | Normative – Other* |

* Other = e.g. testing

- WT#1: Study and propose mechanisms that enable dynamic connections between SNPN and CH other than current pre-configuration of addresses and certificates, and specifically the following aspects:
  - Establishment of secure connection(s) for bidirectional signaling between an SNPN and a CH with no pre-established relationships between the SNPN and CH.
  - Required lifetime (if any) of this/these connection(s).

- WT#2: Study security aspects of SNPN cellular hotspots being used to support:
  - Basic internet access.
  - Emergency service and public safety services, including IMS.

# Key takeaways and next steps

- OpenRoaming facilitates automatic, secure, and seamless connections for Wi-Fi hotspots
- Cellular roaming across public networks is complex and facilitated by GSMA IR.21
- SNPN cellular hotspots are technically supported by 3GPP architecture since Release 17
  - Connection establishment challenges exists for SNPN cellular hotspots
  - There is no GSMA IR.21 equivalent and scalability requirements are several orders of magnitude different
- SNPN cellular hotspots can complement 3GPP's mission critical capabilities
- Study item proposal in SA3 for SNPN cellular hotspots met with resistance
  - **Support form other member companies, especially large operators, would be most welcome!**

# Thank you!


CISCO