



Open Source Telecom Signaling

PAiCore Network API Platform

Technical Document

Reigniting telecom innovation and sustainable
profitability via open source signaling solutions

Main Benefits



Silent verification

Password-free, nothing to type, nothing to install on mobile data.



One platform

Same API style, credentials, onboarding, controls, reporting, and operations for every capability.



Operator in control

Decides who uses what, how much, and on which terms.



Use your existing network

Legacy and modern networks, with no new core infrastructure.



Built on open standards

No proprietary lock-in, and a path into the industry's open network API ecosystems.



Open-source expertise

Transparent, auditable foundations and years of carrier signaling experience, from open source to carrier-grade.

Key Features- CAMARA Aligned APIs



Silent Network Authentication

Authenticates a mobile user through the device's SIM, without passwords, SMS codes, or user interaction.



One-Time Password SMS

Sends a one-time password by SMS and verifies the submitted code.



SIM Swap

Checks whether a recent SIM change has occurred for a mobile subscription.



Know Your Customer Age

Checks whether a mobile subscriber's age exceeds a specified threshold.



Number Verification

Verifies that a mobile phone number belongs to the device accessing the service.



Location Retrieval

Retrieves the geographic area where a mobile device is located through integration with PAiCore GMLC.



Location Verification

Checks whether a mobile device is within a specified geographic area, through integration with PAiCore GMLC.



Geofencing Subscriptions

Provides notifications when a mobile device enters or leaves a defined geographic area through integration with PAiCore GMLC.

Silent Verification: Two Methods, One API

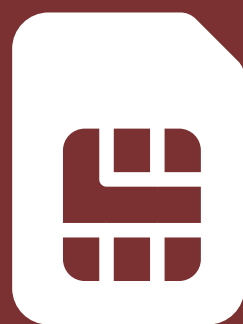
A business uses either method through the same API and chooses the one that fits each user.



Network-based (NV1)

From the mobile data session

Nothing to install. Works in any app or browser, even behind carrier-grade NAT.



SIM-based (NV2)

Silent Authentication

Via the phone's built-in capability, the PAiCore SDK or Google phone number verification.

 User needs	A phone on mobile data	An app on the phone
 Works in	Any app or web page	Inside an app
 Proves	The connection belongs to the number	The genuine SIM is in the device
 Network link	SS7 MAP or Diameter (Sh)	SS7 MAP or Diameter (STa + Sh)
 Platforms	Android or iOS	Android

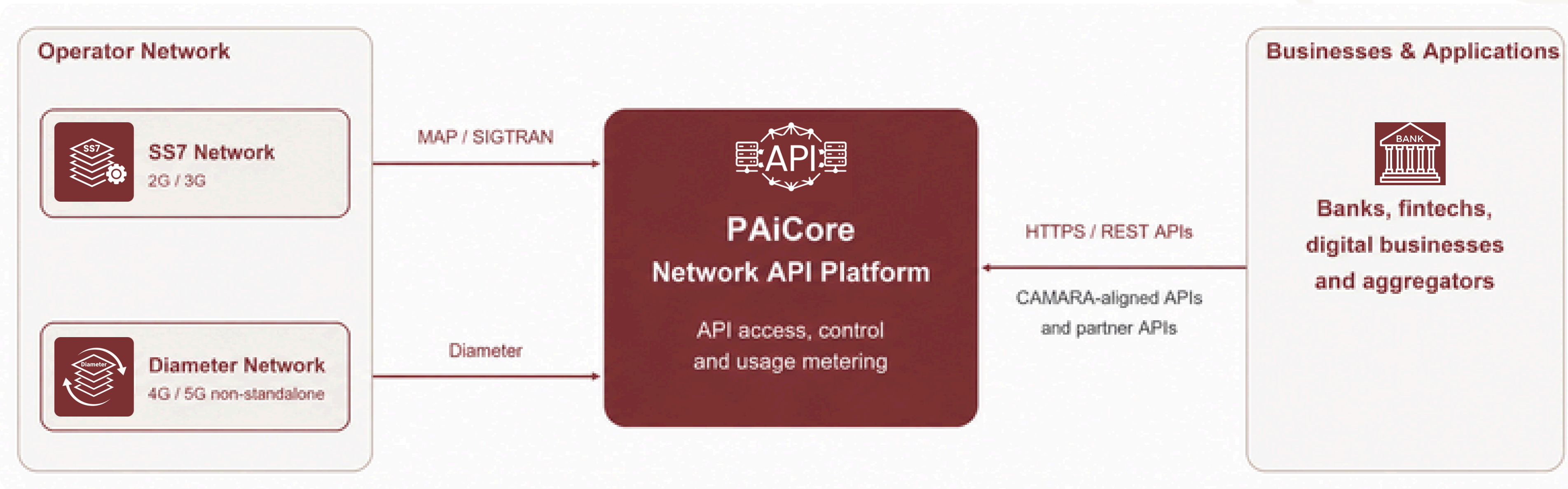


Open Source Telecom Signaling

Interconnections Points

Architecture

Interconnection Points



The operator's network remains the source of truth

Interfaces and connectivity requirements depend on the service and deployment

Recommended HW

Verifications per second	RAM	vCPU	Disk	Network	Sample AWS Instance
115	16 GB	4	250 GB SSD	1Gbps	m5.xlarge
175	32 GB	8	250 GB SSD	1Gbps	m5.2xlarge
280	64 GB	16	250 GB SSD	1Gbps	m5.4xlarge

Note: Measured for SIM-based number verification over SS7. One verification is a complete flow, not a single message. Network-based verification will be sized separately. Interconnection values below are examples only

For SS7 over SIGTRAN (SCTP/M3UA) interconnection

Description	Value	Comments
OPC	1001	Originating Point Code identifying the platform within the SS7 network over IP (carried in the M3UA routing label).
DPC	2002	Destination Point Code identifying the peer node (e.g., STP or core element) in the SS7 network over IP.
Global Title	919800123456	Signalling Connection Control Part (SCCP) Global Title digits assigned to the platform.
SSN	TBD	Signalling Connection Control Part (SCCP) Subsystem Number assigned to the platform.
Network Indicator	National (2)	International (0/1) or National network (2/3) determination for Signaling Point Codes (OPC/DPC).
IP and Port at peer side	1.1.1.1	Peer (usually SGW) SCTP endpoint IP address(es) and port number list.
IP and Port at host	2.2.2.2	Host (usually AS) SCTP endpoint IP address(es) and port number list.
SCTP mode	Host	Side that shall initiate the SCTP association and act as client: Host or Peer?
M3UA type	AS	Process that shall run on the platform host at M3UA: AS or SGW or IPSP?
Routing Context	101	The Routing Context assigned to the platform identifying its MTP3 routing key.
Network Appearance	12	Identifier of the SS7 network context for the routing key. Not required if SGW operates in the context of a single SS7 network, or if individual SCTP associations are dedicated to each SS7 network context.
Traffic mode	Override	Traffic mode type: Override or Loadshare. Override: ASP takes over all traffic overriding any currently active ASPs in the AS. Loadshare: The ASP will share in the traffic distribution with any other currently active ASPs.
Message Exchange	SE	IPSP model defining if each exchange of ASPTM or ASPSEM messages can be initiated by either IPSP (Double Exchange, DE) or not (Single Exchange). SE if unknown.
MUA ASP ID	1	Optional ASP ID (provide it only if it has been set by the operator).

For Diameter interconnection

Description	Value	Comments
Host IP	1.1.1.1	Diameter IP address(es) assigned to the PAiCore Technology platform (SMSC, GMLC, DRA, etc.).
Host Port	3868	Diameter port number(s) assigned to the PAiCore Technology platform (SMSC, GMLC, DRA, etc.).
Host Realm	epc.mcc748.mnc012.3gppnetwork.org	The string(s) in the Network Access Identifier (NAI) that immediately follows the "@" character assigned to the PAiCore Technology platform (SMSC, GMLC, DRA, etc.).
Host User Name	host_name.epc.mcc748.mnc012.3gppnetwork.org	The string(s) which contains the User-Name in a format consistent with the NAI specification assigned to the PAiCore Technology platform (SMSC, GMLC, DRA, etc.).
Host Number	861684684	ISDN (E.164) number assigned to the PAiCore Technology platform (SMSC, GMLC, DRA, etc.).
Peer IP(s)	2.222	Diameter IP address(es) of the peer side (DSC or DRA or DEA or IWF).
Peer Port(s)	3869	Diameter port number(s) of the peer side (DSC or DRA or DEA or IWF).
Peer Port Range	3868-3869	Port range to use for establishing SCTP associations.
Peer Realm	epc.mcc748.mnc01.3gppnetwork.org	The string in the DSC/DRA/DEA/IWF Network Access Identifier (NAI) that immediately follows the "@" character.
Peer User Name	peer_name.epc.mcc748.mnc01.3gppnetwork.org	The string which contains the DSC/DRA/DEA/IWF User-Name in a format consistent with the NAI specification.



Open Source Telecom Signaling

Web Management Overview

APIs, Messaging and USSD. One platform.

Publish telecom capabilities as governed products — signaling operations and CAMARA APIs, A2P SMS over SMPP or HTTP, and hosted USSD services — to the same customers, on the same terms, with one record of everything they used.

- SS7 MAP, Diameter and CAMARA APIs as products
- A2P SMS: SMPP binds, routing, sender IDs, receipts
- USSD short codes driven by the customer's own application
- One rate-limit tier per client, enforced on every channel
- One CDR feed across APIs, messages and sessions

Welcome back

Sign in to the Network API Platform.

Sign in as

Platform operator

Customer

Governs products, customers, terms, routing and the network side.

Email address

Password

☒ Remember this device [Forgot password?](#)

Sign in →

or continue with

Single Sign-On (SSO)

Conceptual prototype — credentials are pre-filled. Just click **Sign in**. The two audiences are separate user stores; this switch stands in for landing on either one.

- Dashboard
- NETWORK API
- Network API overview
- API Catalog
- Platform Auth & Keys
- SMS
- SMS overview
- Service providers
- Carriers
- Rules and Routing
- USSD
- USSD overview
- Short codes

Network API overview

What the Network APIs served today and how it went — requests, outcomes, latency, and the gate in front of the device-initiated ones. SMS and USSD have their own overviews.

Requests - 24h

68,310

Success rate

98.6%

Latency p95 - last hour

364ms

Failed or timed out - 24h

977 · 1.4%

Request volume — last 24h

Successful vs. timeout & failed responses

Request volume chart

Traffic by API

Share of today's requests - the APIs actually in use

Traffic by API chart

- Dashboard
- NETWORK API
- Network API overview
- API Catalog
- Platform Auth & Keys
- SMS
- SMS overview
- Service providers
- Carriers
- Rules and Routing
- USSD
- USSD overview
- Short codes
- Service Creation Environment
- PLATFORM EVENTS
- Platform clients
- Billing & Pricing
- FAQ
- Deployment & Onboarding
- CDR Feed
- Audit Log
- Console users

Platform Auth & Keys

Platform-wide: which authentication methods the platform accepts, the validity it applies, and the keys it signs with. Nothing here belongs to one customer — an individual credential lives on its client, under **Platform clients**.

Authentication methods

What the platform accepts, and how many credentials use each

OAuth2 client credentials

the primary method, a credential exchanges its id and secret for a short-lived scoped token, 0 of 0 credentials

enabled

Signed assertion (JWT-bearer)

For trusted providers they sign an assertion with a key we hold the public half of, so no shared secret exists, 0 of 0 credentials

enabled

Validity

What the platform applies to tokens and secrets

Access token

3000 s

Signing key lifetime

60 s

Retired key kept published

300 s

Assertion max lifetime

300 s

Clock skew tolerated

30 s

Client secret expiry

not enforced

Signing keys

Every consumer verifies our tokens against these

Rotate

KEY ID

TYPE

USED FOR

CREATED

STATUS

7f1a6114-3215

RSA-2048

Operator Token: RS256

6 days ago

Active

2a82f476-487

RSA-2048

Operator Token: RS256

38 days ago

Retired

Tokens

The three the platform deals in

TOKEN

ISSUED BY

TTL

SINGLE USE

Eligibility Token

Aggregator (third party)

1,300 s

yes

Operator Token

Operator auth-server

300 s

no

Service credential

Operator auth-server

300 s

no

Legal basis

What each scope may be called under, and until when

SCOPE - PURPOSE

BASIS

UNTIL

STATUS

number-verification-verify

ProauthFrontendContactCom

IDENTIFIABLE_PERSON

-

granted

device-location-verify

DeviceLocationVerification

CONSENT

2025-11-12

granted

ncs:device-user-info

ServiceFrontendCom

CONTRACT

-

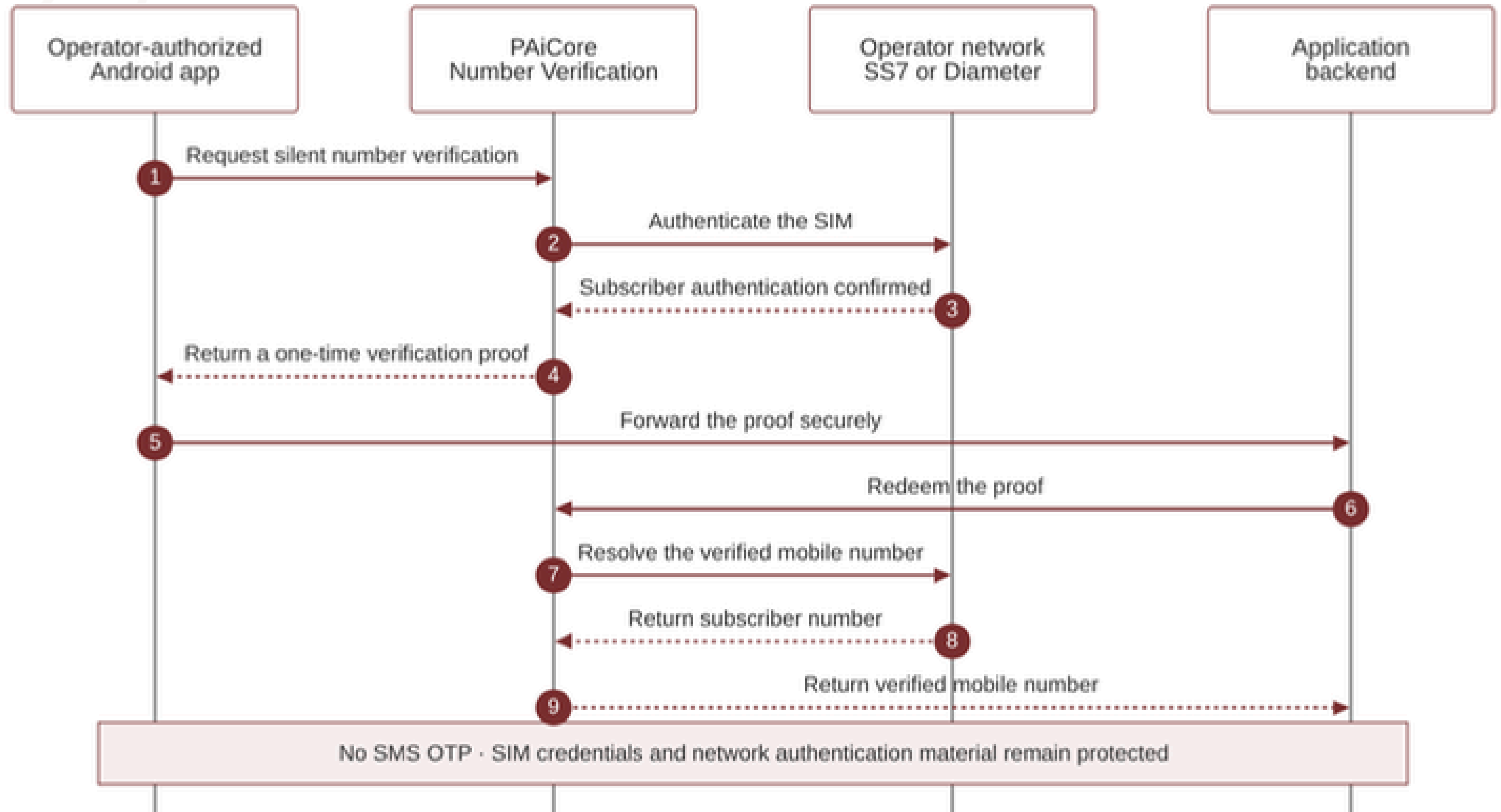
no check



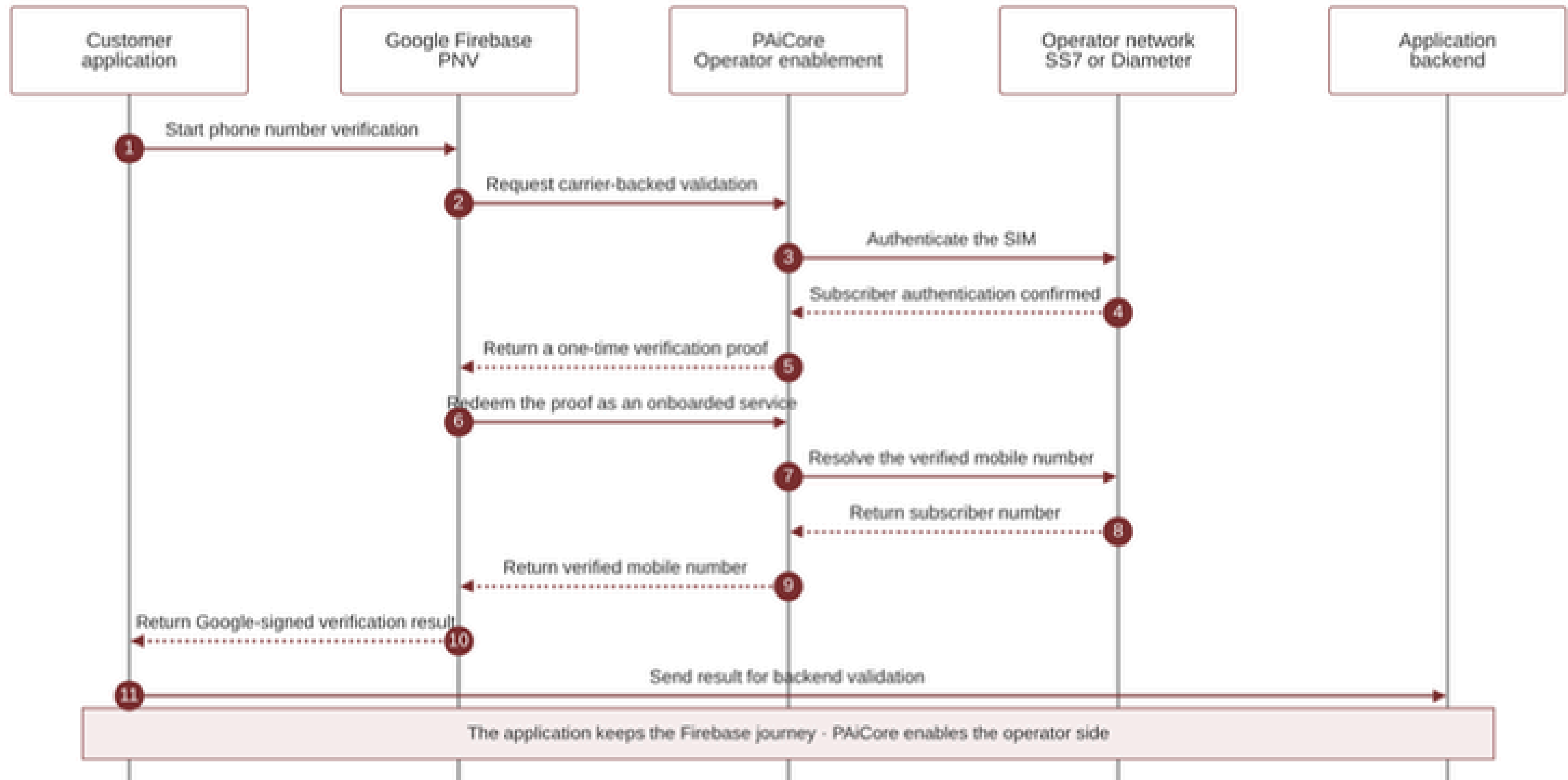
Open Source Telecom Signaling

Flow Diagrams

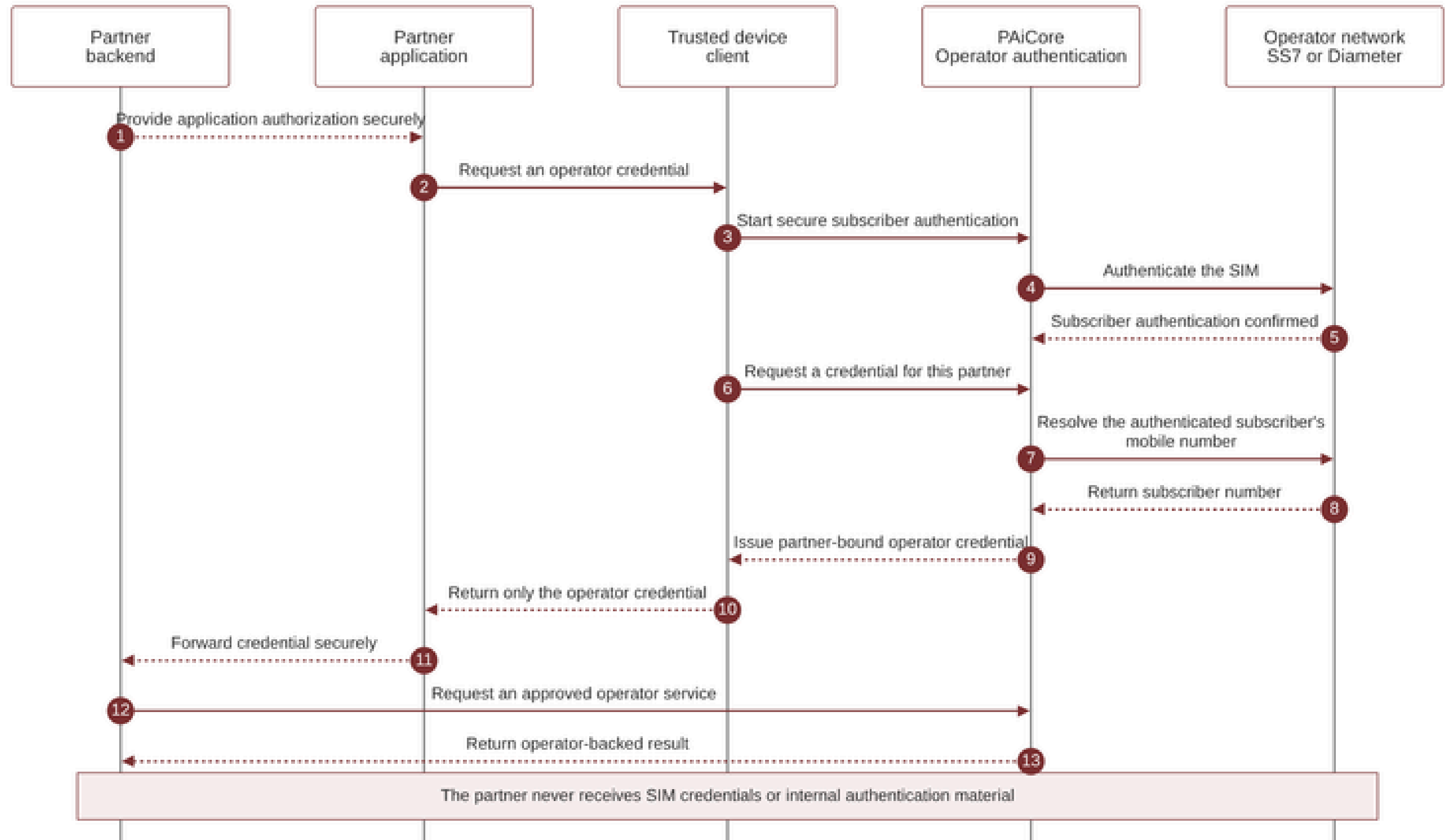
Number Verification: SIM-based, PAiCore SDK



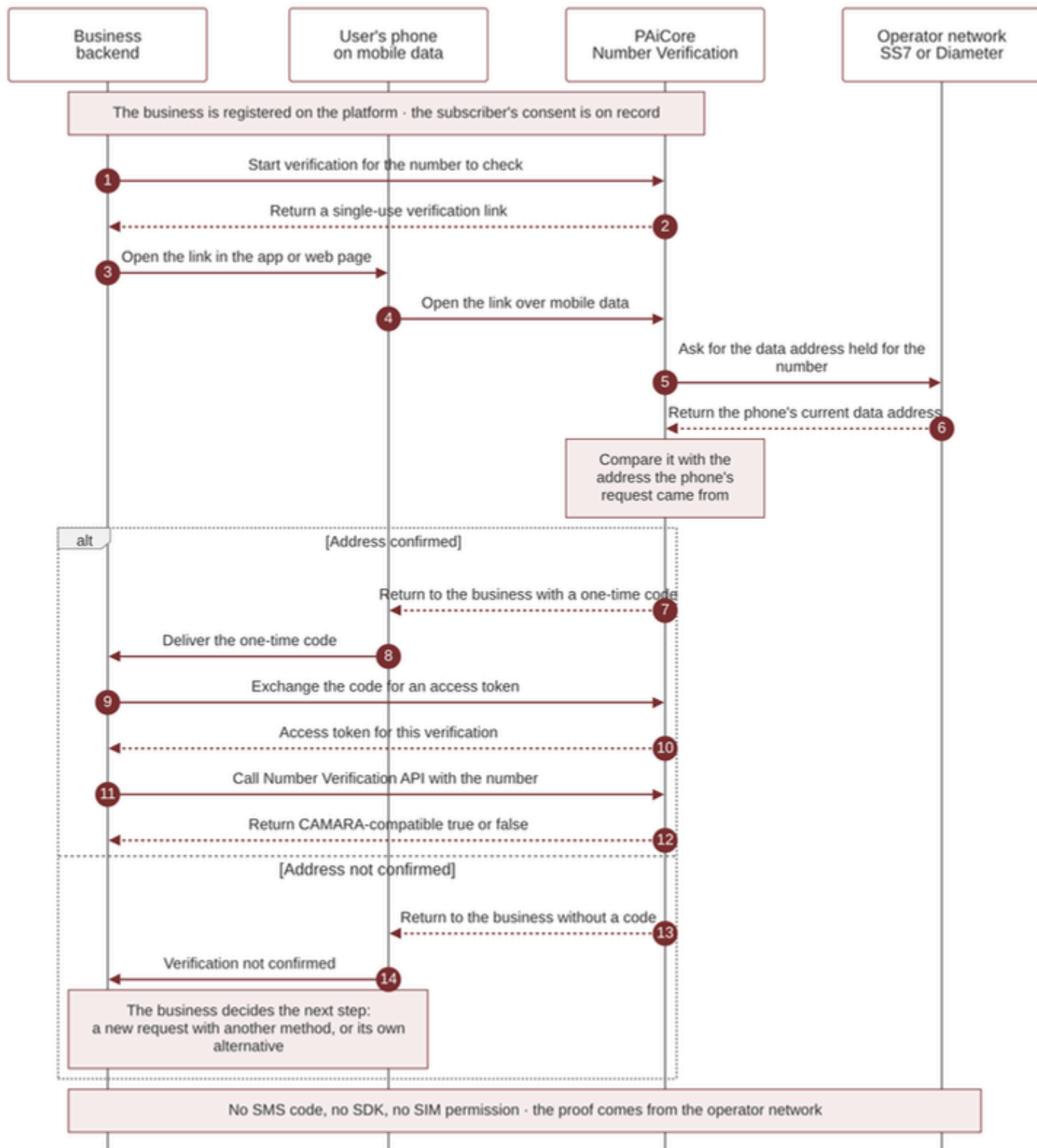
Number Verification: SIM-based, Google Firebase PNV



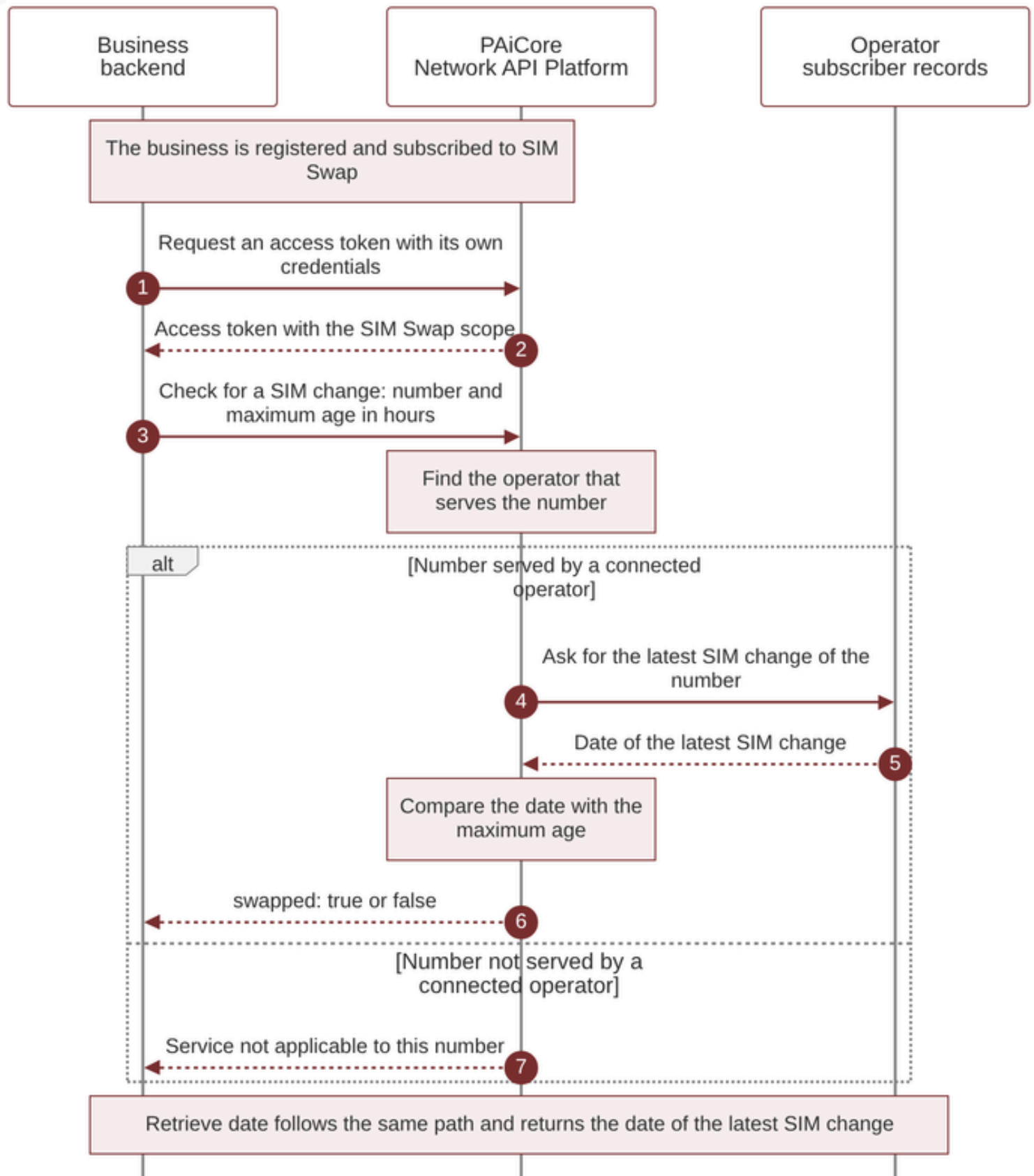
Number Verification: SIM-based, TS.43 standard



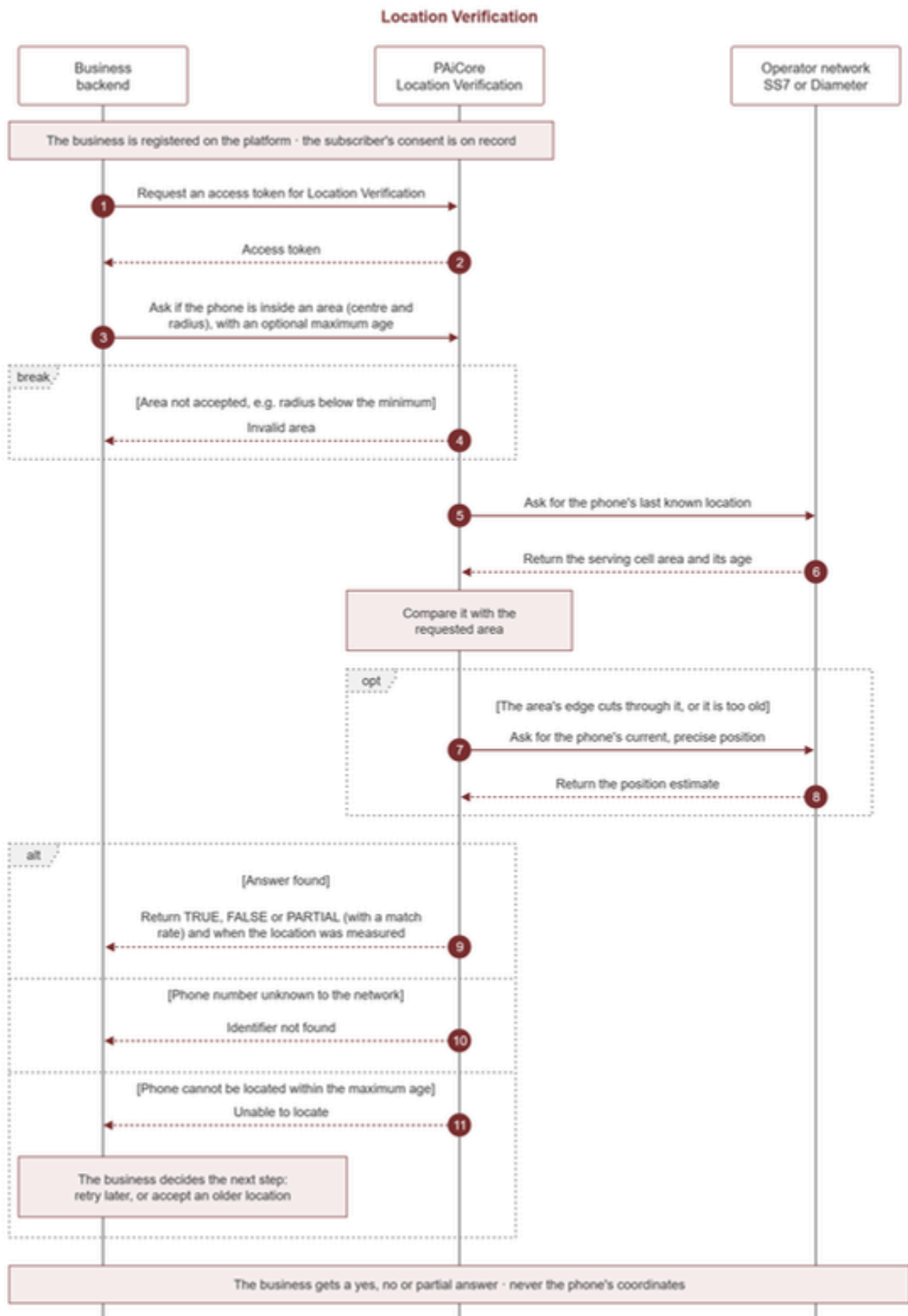
Number Verification: Network-based, mobile-data



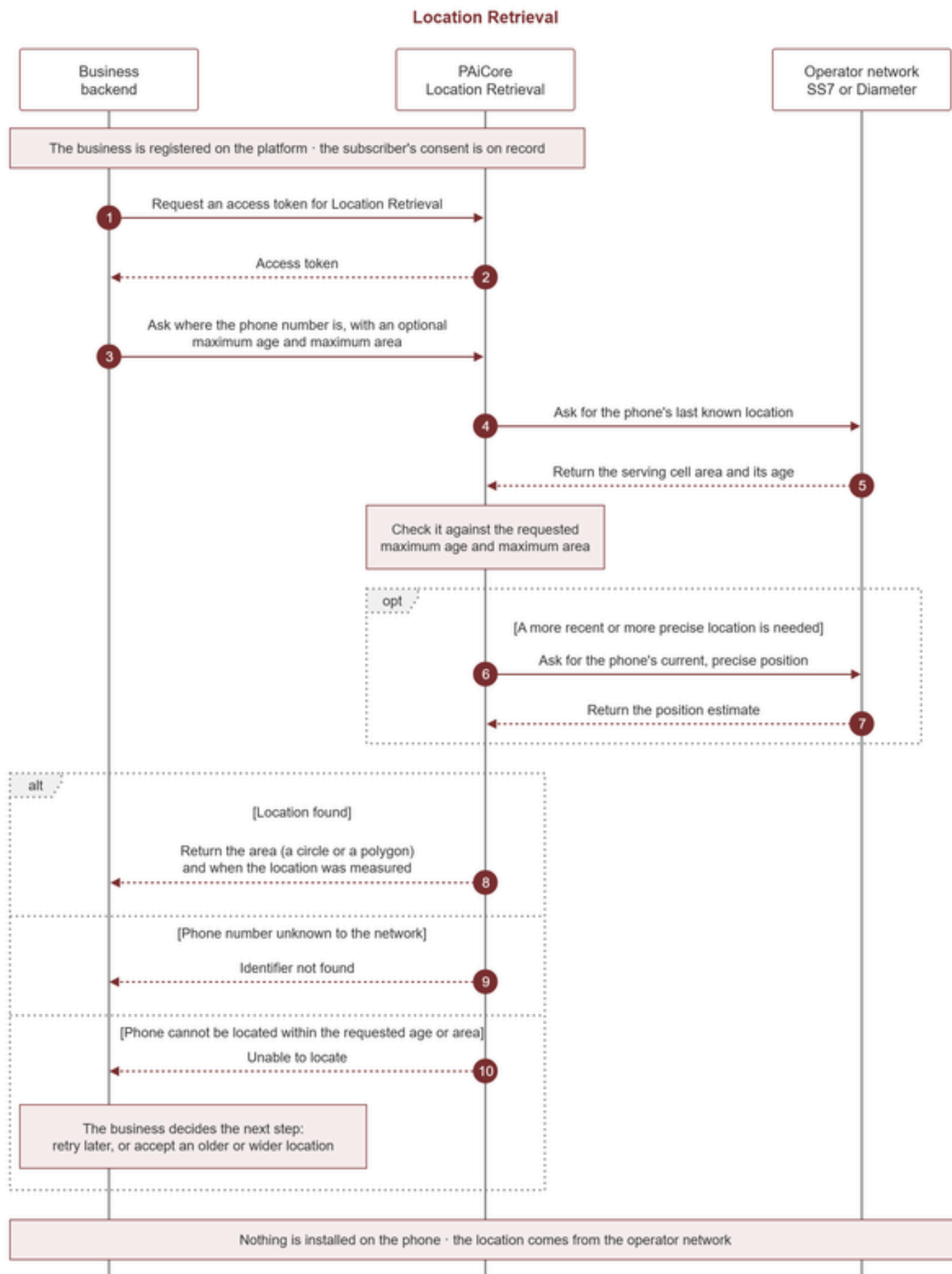
SIM Swap call flow



Location Verification call flow



Location Retrieval call flow





Open Source Telecom Signaling

Offering reliable open source signaling solutions with high quality 24/7 technical support, delivering ownership of the technology & the freedom to innovate while eliminating unnecessary license fees.

