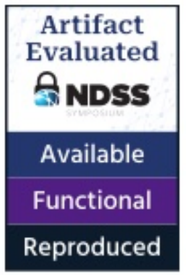


AnonyCall: Enabling Native Private Calling in Mobile Networks

Bridging the gap between subscriber anonymity and essential network functionality

Hexuan Yu Chaoyu Zhang Yang Xiao Angelos D. Keromytis Y. Thomas Hou Wenjing Lou

Virginia Tech • University of Kentucky • Georgia Tech

NDSS 2026, San Diego

Mobile Networks Rely on Persistent Identity

THE REALITY:
Default Tracking of Identity & Location.

THE RISK:
Data selling, leaks, and profiling.

$200M FCC FINE:
CARRIERS SOLD LOCATION DATA

Mobile Network Operators (**MNOs**) manage infrastructure and sensitive subscriber data by design. To provide service, they rely on long-term identifiers:

- Phone Numbers: Publicly reachable but permanently tied to identity.
- SUPI/IMSI: Permanent identifiers used for network authentication.

These identifiers create a permanent trail.
The root issue is not just policy, but the architectural reliance on static IDs to route calls and bill users

Motivation: Anonymous Access Is Not Enough

Current State: Cellular Access Anonymity

protecting subscriber's identity and location privacy from **untrusted MNOs**

- **Hides Permanent Identifiers (SUPI/IMSI, IMEI, Phone #) and other long-term identifiers (IP, SIP URI, etc)**
- **Masks Phone Numbers**
- **Protects Fine-grained Location**

Recent research [1-5] enable users to authenticate anonymously using cryptographic pseudonyms (e.g., PGPP, AAKA, LOCA, PGUS...)

- Cryptographic techniques, e.g., Blind Signatures, Anonymous Credentials (AC) ...
- Some approaches [1,3] rely on trusted third-party components, e.g., dedicated Mobile Virtual Network Operators (MVNOs) brokers

[1] Schmitt et al. *Pretty Good Phone Privacy.* USENIX Sec' 21
[2] Yu et al. *AAKA: An Anti-Tracking Cellular Authentication Scheme Leveraging Anonymous Credentials.* NDSS' 24
[3] Luo et al. *LOCA: A Location-Oblivious Cellular Architecture.* NSDI' 24
[4] Alnashwan et al. *Strong Privacy-Preserving Universally Composable AKA Protocol with Seamless Handover Support for Mobile Virtual Network Operator.* CCS'24
[5] Yang et al. *PGUS: Pretty Good User Security for Thick MVNOs with a Novel Sanitizable Blind Signature.* IEEE S&P' 25

Anonymous access protects identity but breaks native cellular services

Current State: Cellular Access Anonymity

protecting subscriber's identity and location privacy from untrusted MNOs

- **Hides Permanent Identifiers (SUPI/IMSI, IMEI, Phone #) and other long-term identifiers (IP, SIP URI, etc)**
- **Masks Phone Numbers**
- **Protects Fine-grained Location**

Safe from tracking

Anonymity requires unlinkability.

The Broken Utility : Routing & Billing

- **Unreachable: Native VoLTE/VoNR calls fail (No Routing Path)**

Routing requires fixed ID-to-location mapping. Network cannot route calls without a Phone #.

- **Unbillable: Operators cannot charge usage (No session Linkage)**

Billing (prepaid&postpaid) requires session linkability.

THE GAP:
Anonymous access without calling and charging is technically interesting but undeployable.

We need a system that preserves Unlinkability (Privacy) while enabling Reachability and Billing (Utility).

AnonyCall reconciles privacy with deployable cellular functionality

Goal 1 – Anonymous Callee Discovery

- Anonymous users remain reachable
- Native VoLTE / VoNR compatibility
- User remain discoverable only by authorized caller

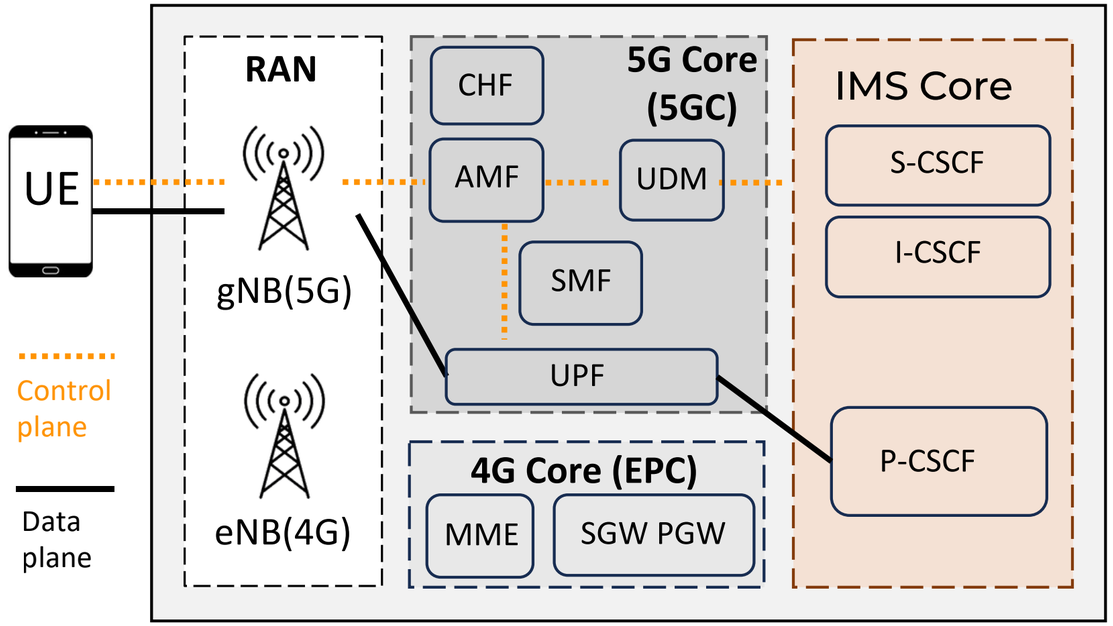
Goal 2 – Anonymous but Accountable Charging

- Real-time prepaid support
- Postpaid aggregation
- No cross-session linkability
- Double-spending detection

Design constraints:

- No new network entities
- Compatible with existing 4G/5G IMS
- No modification to
  - SIP signaling
  - IMS core logic
  - Radio access network (RAN)

Modifications restricted strictly to Home Network logic.

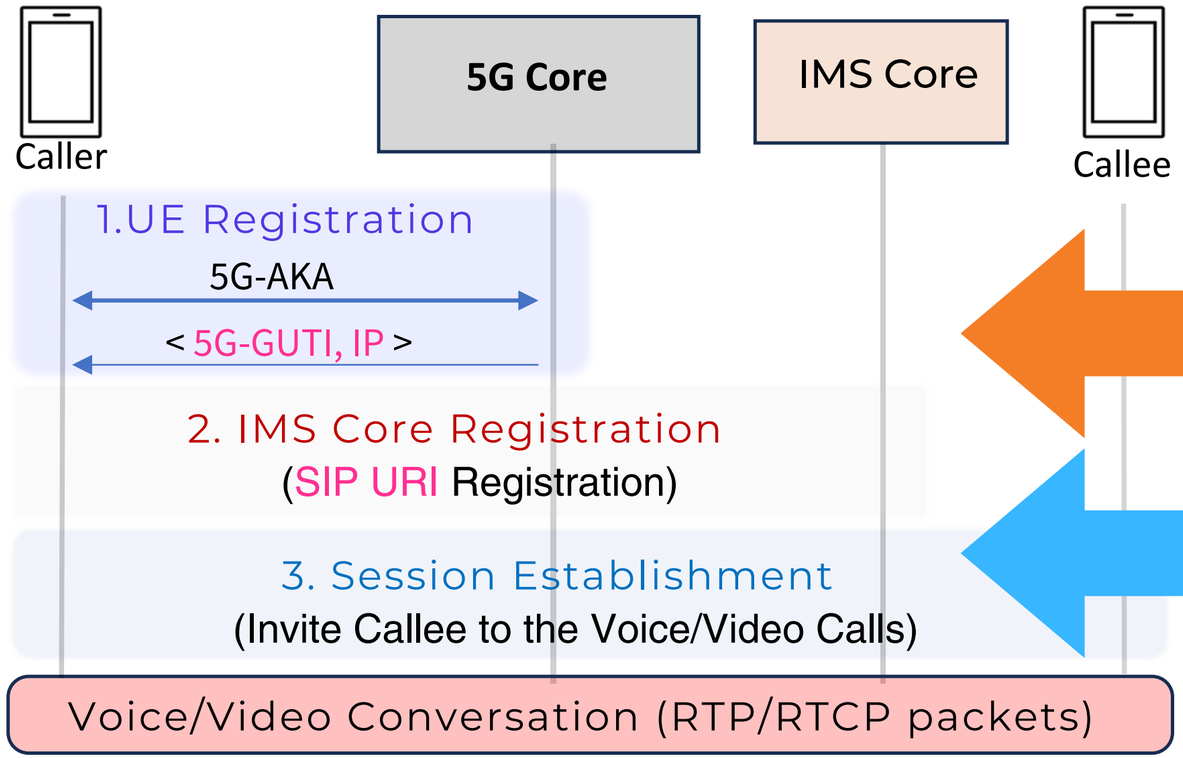


Standard 5G calling involves RAN, 5GC, and IMS

A UE connects through:

- RAN for radio access
- 5GC for mobility and IP assignment
- IMS (IP Multimedia Subsystem) for SIP-based call routing

AnonyCall is a complementary layer built on top of existing anonymous access schemes



Existing anonymous cellular access methods can accomplish steps 1, 2

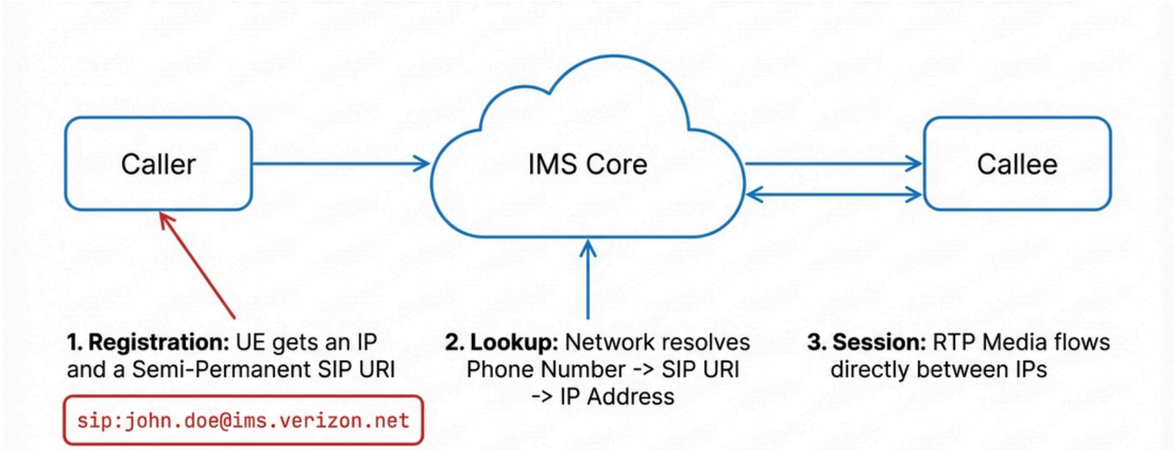
Existing Anonymous Cellular Access Methods
(Blinded SUPI/IMSI during AKA)

AnonyCall Layer

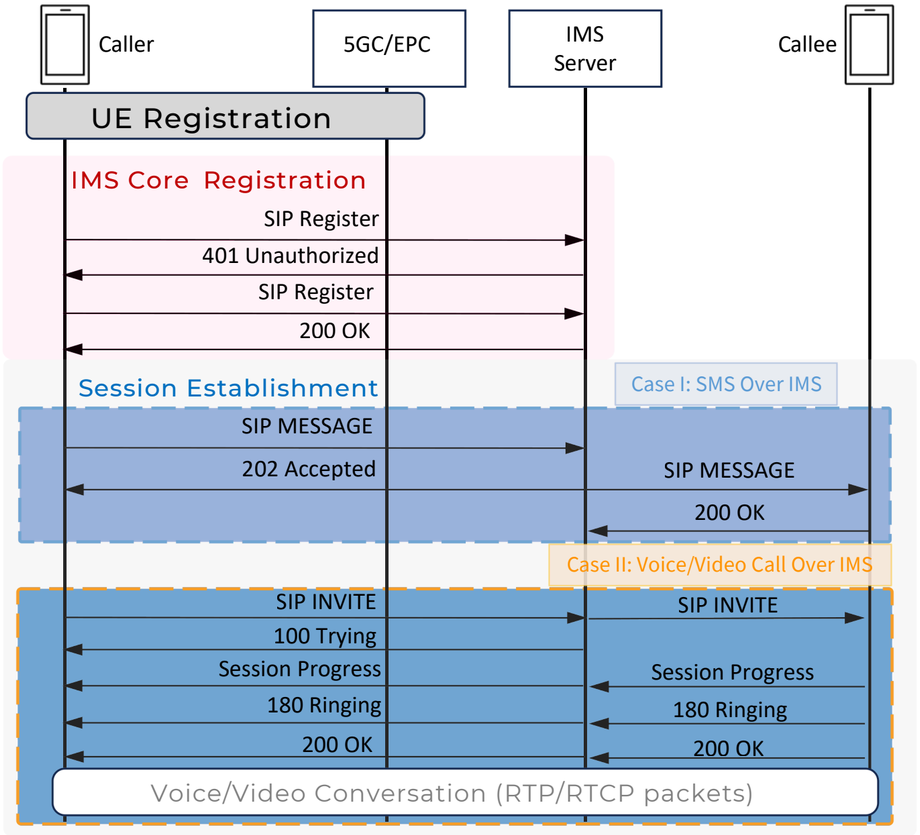
Reachability Module (Anonymous Callee Discovery)

Privacy-preserving Charging Module

Standard IMS routing inherently binds SIP identity to permanent identity



Standard Callee Discovery Process (5G Core omitted)



Standard SIP Call Flow

In VoLTE and VoNR, a device:

1. obtains a dynamic IMS IP address,
2. registers a SIP URI,
3. receives calls via SIP URI resolution.

In standard networks, the SIP URI is static and linked to user's permanent identity (e.g., SUPI, Phone #).

Key Idea : Decoupling Identity from Reachability

Core insight: A user can be reachable without being identifiable.

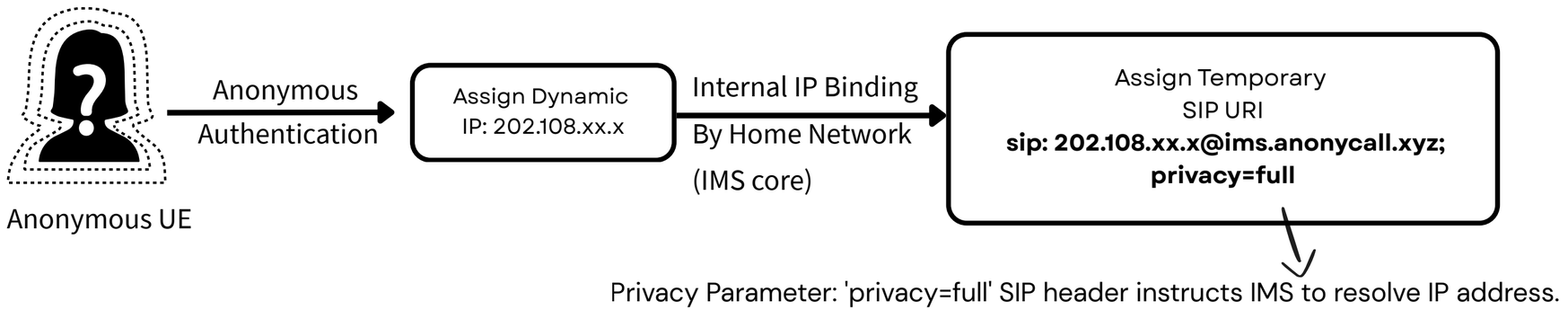
We introduce **temporary SIP URIs** that are:

- Short-lived
- Bound to IMS IP address
- Automatically invalid on DHCP release
  – Expires once the IP lease ends
- Fully resolved by IMS

Mechanism

- Home Network assigns a Temporary SIP URI dynamically.
- URI is valid only as long as the IP address is active.
- Result: Reachable via IP, but identity is Unlinkable.
- URI rotates every 10-60 minutes

Standard SIP URI	**sip:1870123456@ims.mnc480.mcc311.3gppnetwork.org sip: john.doe@ims.verzion.net**	**Reveals Phone # / Identity**
AnonyCall SIP URI	**sip: 202.108.xx.x@ims.anonycall.xyz**	**Reveals only ephemeral IP Address**



Out-of-band authentication restricts SIP URI disclosure

The temporary SIP URI is not publicly visible.

Instead, the caller authenticates through an callee-side **authentication agent** before receiving the routing information.

- the caller proves authorization
- the policy is verified
- the SIP URI is securely released

Authentication is:

- Policy-driven
- Automated
- Asynchronous

AnonyCall does not introduce a new PKI or identity authority.
Out-of-band authentication leverages already deployed trust infrastructures:

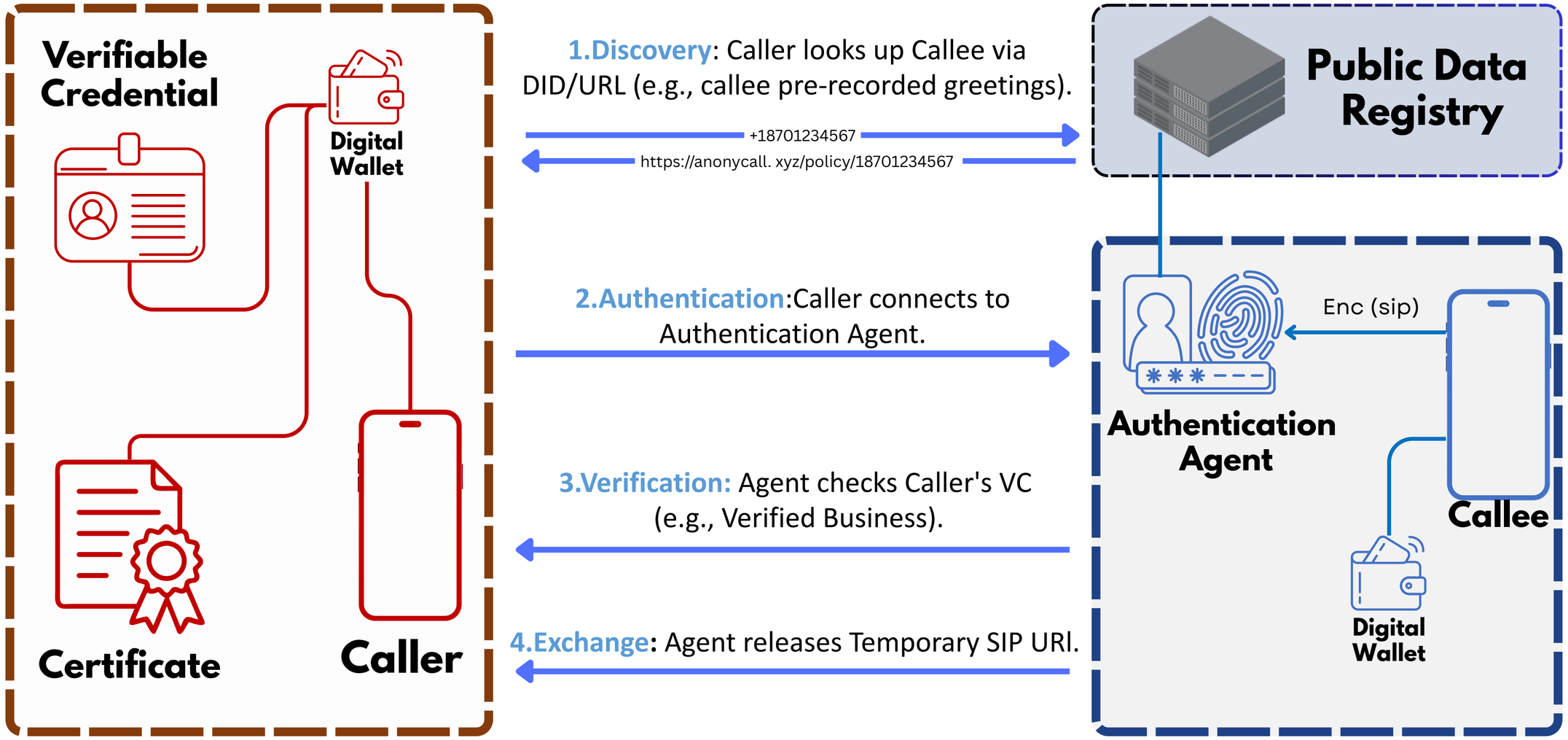
• **Telecom PKI** (e.g., STIR/SHAKEN under 3GPP/GSMA standards)
– mandated in the United States
– adopted in the UK, France, and other regions

• **W3C Decentralized Identifiers (DID) and Verifiable Credentials (VC)**
– supported by government and enterprise identity systems
– eIDAS 2.0, Entra ID, and similar federated identity frameworks

Only callers who satisfy the callee’s policy obtain the temporary SIP URI.

The network routes the call, but discovery happens completely outside the network's view.

Out-of-band Authentication Workflow



Out-of-band authentication decouples discovery from the cellular core.

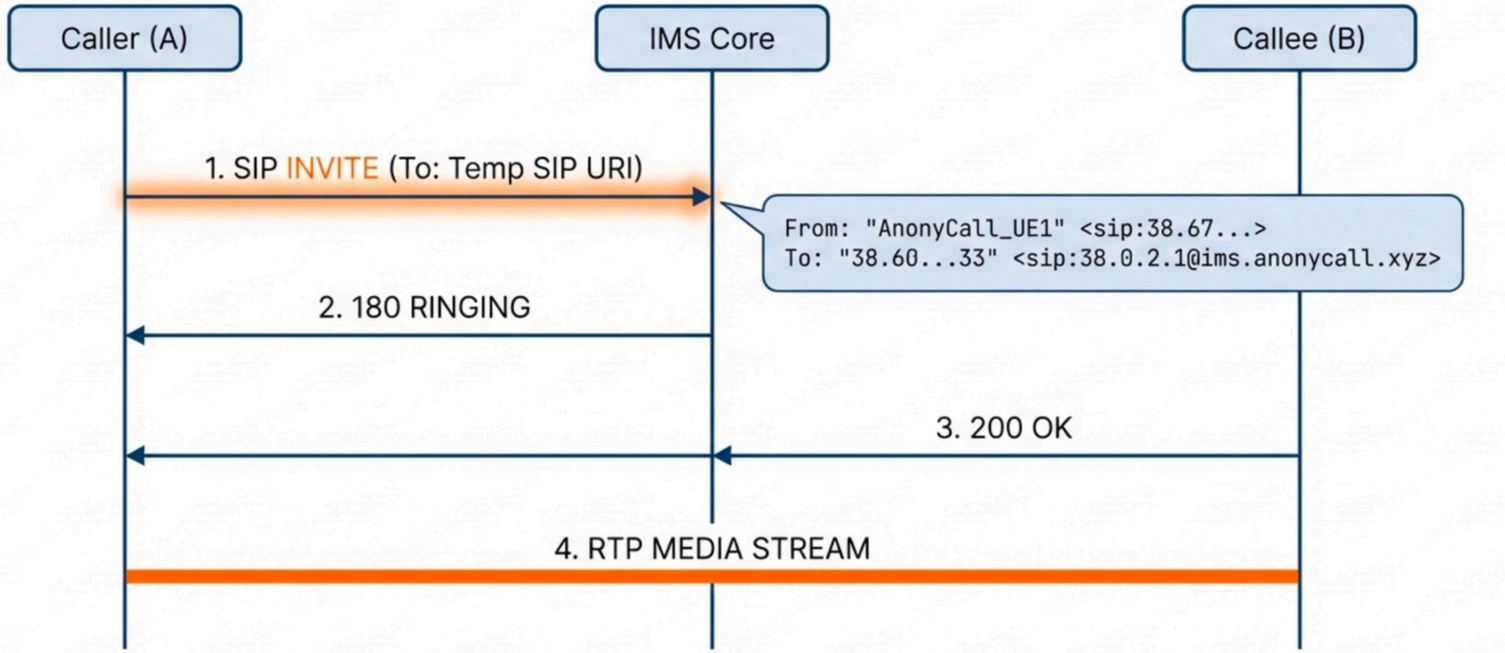
Native Call Establishment

Once the caller receives the temporary SIP URI, the call proceeds via standard SIP routing.

The IMS core:

- resolves the URI to the dynamic IP address,
- detects the privacy flag,
- forwards the call normally.

No inter-operator protocol changes are required.



No changes to:

- **SIP protocol**
- **Call routing**
- **Roaming architecture**

The network processes the call normally. It routes to an IP, not an Identity.

The Charging Paradox

Cellular billing requires real-time, fine-grained charging.

The challenge: How to bill an anonymous user?

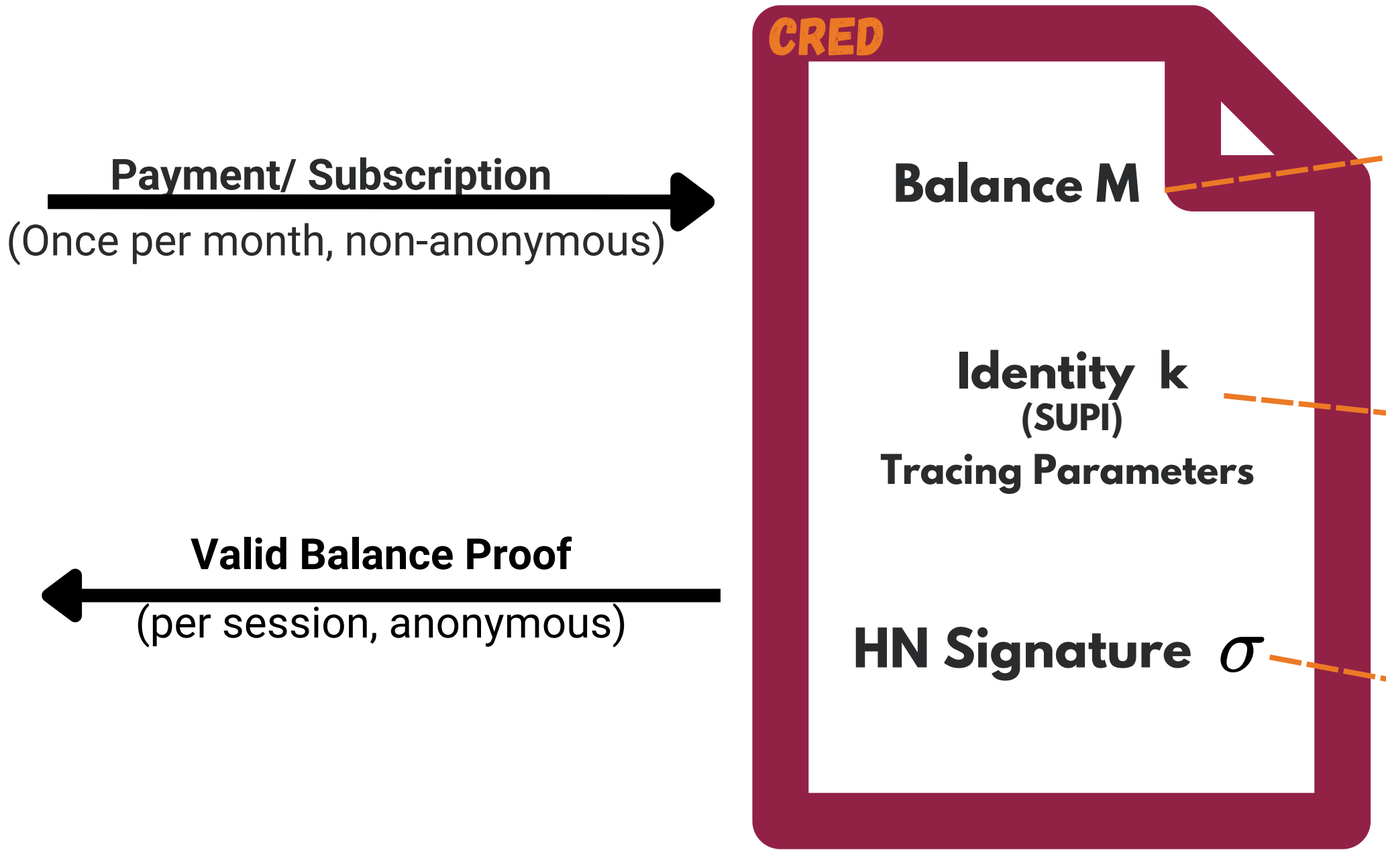
- Prepaid: Must deduct balance without knowing which account.
- Postpaid: Must aggregate usage without linking sessions.
- The Threat: Fingerprinting via balance history.

However:

- fixed-value tokens do not support per-minute billing,
- standard blind signatures do not support unlinkable state updates,
- billing requires continuous balance mutation.

We therefore need a new subscription credential design.

The Anonymous Balance Credential



Hidden balance with homomorphic update capability
(Pedersen commitment)

Committed and re-randomized per session

Identity recovery is triggered only upon double-spending (accountability)

SPS-EQ Signatures
(Structure-preserving Signatures on Equivalence Classes)
Allows signature re-randomization (unlinkable credential refresh) **without re-issuance**

The Home Network verifies the validity of the credential and updates the balance homomorphically, without seeing the values inside.

Anonymous balance credentials enable private stateful billing

1. Anonymous Session Start

UE proves Balance $\geqslant$ threshold (e.g., 5 mins) via Zero-knowledge Range Proof.

ZK-Proof : $ Balance $\geqslant$ 5 min;
cred is valid

SPS-EQ ensures the new credential is cryptographically unlinkable to the old one.

MNOs updates the balance without ever knowing the balance or identity

2. Session Grants

1. Verify the ZK-Proof
2. MNO deducts usage homomorphically from hidden balance.
3. MNO updates the credential.

$ Balance_new = Balance_old - Usage
cred -> cred'

3. Refresh

UE adapts credential *cred'* to new random state *cred''*

Conditional Unlinkability Deters Double-Spending

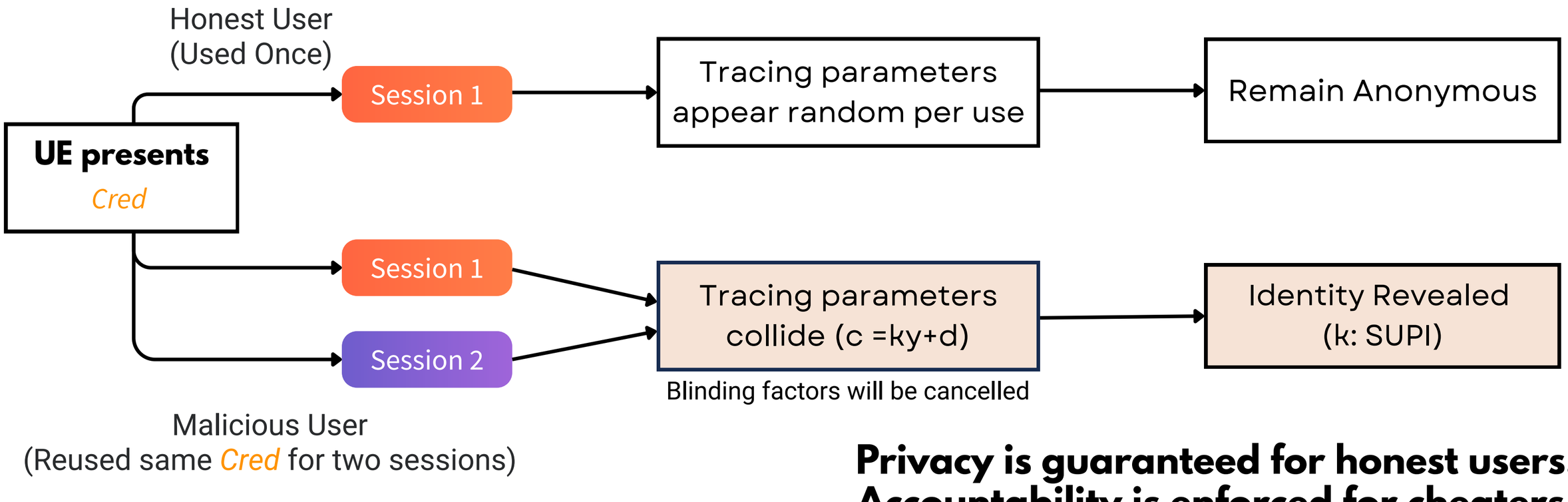
For honest users:

- **Credentials appear fresh and unlinkable**
- **Sessions cannot be correlated**

If a credential is reused:

- **a mathematical collision occurs**
- **the hidden identity can be recovered**

Anonymity is conditional on honest behavior



Privacy is guaranteed for honest users.
Accountability is enforced for cheaters.

System Implementation and Evaluation

Part I: End-to-End OOB Authentication

Two auth modes:
1) **Simple** mode - standard x.509 digital certificate (OpenSSL) – emulates Telcom PKI
2) **Flexible** mode - DID + Verifiable Credentials – customizable callee policies

DID and VCs implemented using the standard DID open-source projects (e.g., Microsoft Entra)

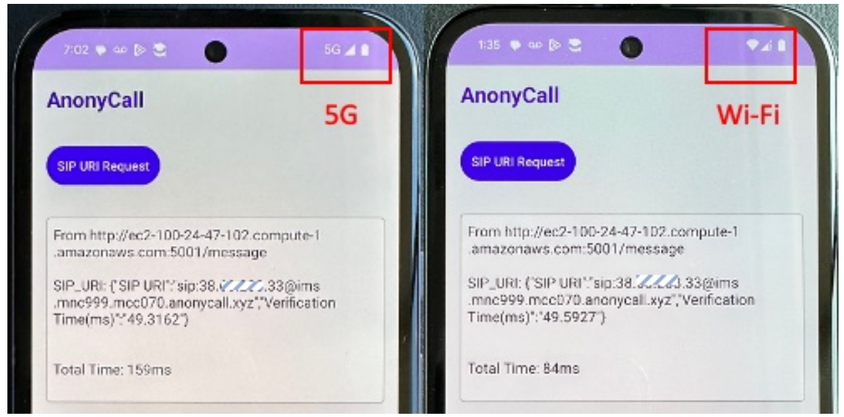
Part II: Call Routing and Charging

Evaluated on Standard Cellular SIP Process (*Linphone SIP client App*)

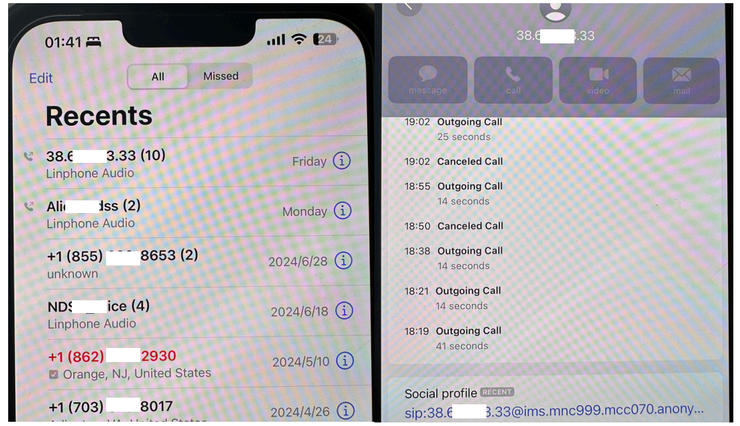
We evaluate both:

- end-to-end call establishment latency
- cryptographic overhead of the charging protocol

Functionality Evaluation



OOB Auth Latency



Call Histories with an Anonymous Callee

Dial SIP URIs through SIP Dialer Apps (e.g., Linphone/Zopier) on iPhone
Callee's temporary SIP URI: 38.XXX.XX.33@domain.name

```
Session Initiation Protocol (180)
  Status-Line: SIP/2.0 180 Ringing
  Message Header
    Via: SIP/2.0/UDP 38.6[redacted]7.173;branch=z9hG4bK928e.c9eb69c8ddf46d53abd7b67
    Via: SIP/2.0/UDP 38.6[redacted]3.34:63121;received=38.6[redacted]3.34;branch=z9hG4bK.
    From: "AnonyCall_UE1" <sip:38.68.233.34@ims.mnc999.mcc070.anonycall.xyz>;
    To: "38.6[redacted]3.33" <sip:38.68.233.33@ims.mnc999.mcc070.anonycall.xyz>;tag
Session Initiation Protocol (BYE)
  Request-Line [truncated]: BYE sip:38.6[redacted].34@38.6[redacted]3.34:63121;pn-prid=18
  Message Header
    Via: SIP/2.0/UDP 38.6[redacted].173;branch=z9hG4bKc53d.08f3881618a77b61ae5ceb3
    Via: SIP/2.0/UDP 38.6[redacted].33:55719;received=38.68.233.33;branch=z9hG4bK.
    From: "38.6[redacted].33" <sip:38.6[redacted].33@ims.mnc999.mcc070.anonycall.xyz>;t
    To: "AnonyCall_UE1" <sip:38.6[redacted].34@ims.mnc999.mcc070.anonycall.xyz>;ta
```

Caller:"AnonyCall_UE1"

Callee:"38.XX.XXX.33@domain.name"

Captured SIP Messages during Call Establishment (via Wireshark)

- SIP Packets 180 Ringing and BYE
- IMS domain name: ims.mnc999.mcc070.anonycall.xyz
- Caller does not need to be anonymous

***Note on Direct SIP URI dialing:**
Some providers support direct SIP URI dialing (e.g., Verizon, AT&T)
Most mobile devices support placing and receiving calls using registered SIP URIs through either native dialers or third-party Apps

Performance Evaluation

Part I.a: Out-of-band authentication (one-time and cached) takes:

- 50–180 ms using PKI,
- 650–780 ms using DID/VC.

Part I.b: SIP URI Retrieval Latency (per-call)

Note: A caller does not need to authenticate itself to the same callee for each phone call.
i.e., Once a caller has been authenticated, the Auth Agent can provide it access rights to the SIP URI for a longer duration, e.g., 1 year.

Performance Evaluation (cont'd)

Part I.a: Out-of-band authentication (one-time and cached) takes:

- 50–180 ms using PKI,
- 650–780 ms using DID/VC.

Part I.b: SIP URI Retrieval Latency (per-call)

Stage	UE time (ms)	HN time (ms)	Description
Setup (obtain cred)	8.0	4.6	Issue new balance credential (once per month)
Spend (prepaid)	27.3	49.1	cred verification and update
Spend (postpaid)	26.7	47.9	*cred* verification and update (w/o range check)

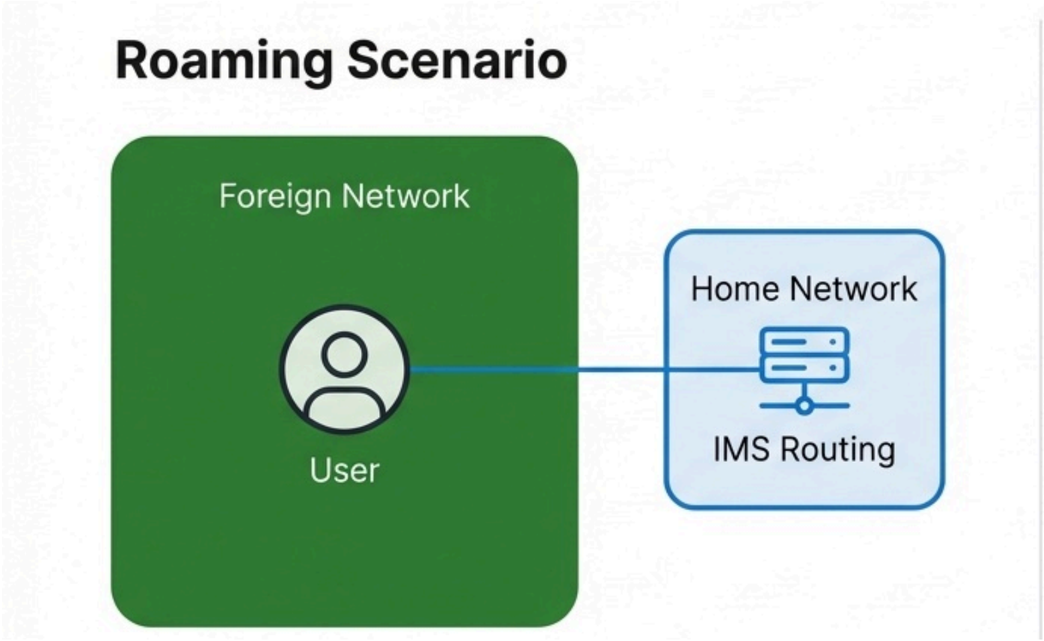
- HN's heaviest step: SPS-EQ signature verification (4 pairings).
- Prepaid slightly costlier due to an extra range proof (balance ≥ usage).
- Latency can be further optimized: UE pre-computes the ZK proof of balance offline, i.e., before call setup

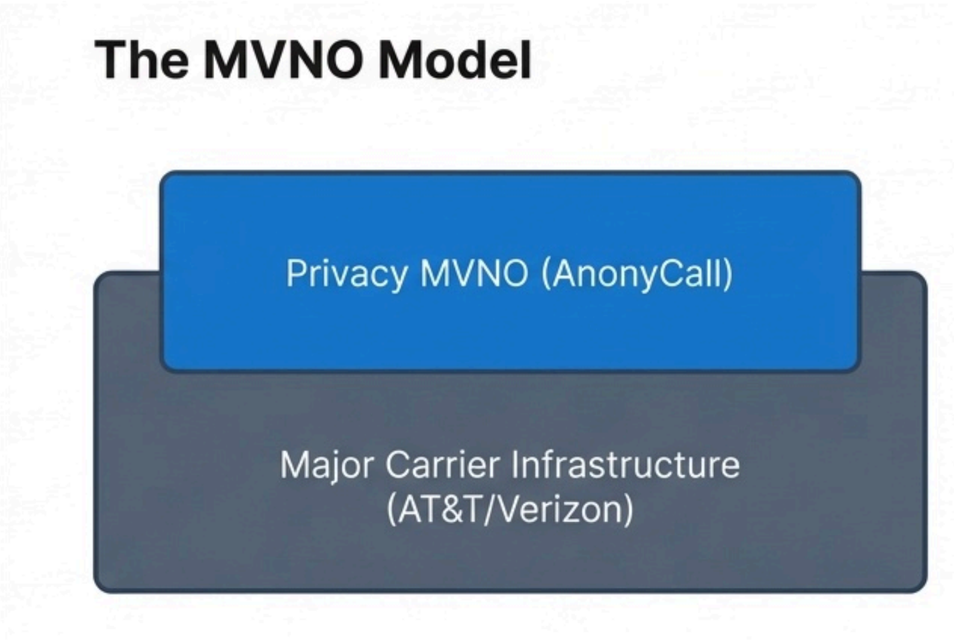
Part II: Charging Protocol (per-call)

Charging overhead < 80 ms per session without precomputation.

Effective total call setup overhead of AnonyCall (on top of standard VoLTE):
80 ms (SIP URI retrieval) + 76 ms (charging) ≈ < 200 ms total
Negligible impact on user experience.

Compatibility & Deployment





ANONYCALL requires no changes to roaming networks.
Foreign networks only observe:

- temporary IP addresses
- standard SIP routing traffic

Compatible with 5G Home-Routed Archictecture

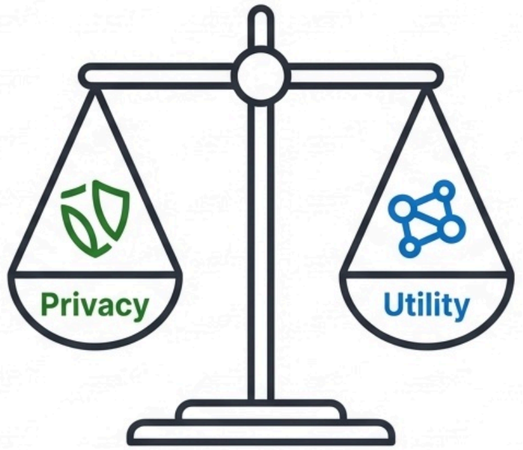
Can be deployed as an overlay service without major changes to the underlying carrier.

All privacy logic is handled within the home network.

Summary

Reconciled Privacy & Utility

- Enabled native VoLTE/VoNR calls for anonymous users.
- Reachability without Permanent Identity.
- Billing without Explicit Usage Tracking.



Key Results

- Supports both prepaid and postpaid charging with conditional accountability for double-spending
- Computation localized in HN — no change to SN
- End-to-end overhead < 200 ms, imperceptible to users
- Demonstrates real-time anonymous billing feasibility for mobile calls

AnonyCall paves the way for privacy-preserving yet functional mobile communication.

Questions?