



Open Verifiable Communications

A GSMA Foundry Project

Webinar for One Consortium

Rich Connexions Ltd

GSMA™



A tsunami of fraud

- According to the “Global State of Scams (2024)”, consumers lost \$1Tn to scams. A significant proportion of this is driven by telecommunications
- In the UK 45% of APP fraud started with a call or text
- Nearly half the global population encounters a scam attempt every week

Calling party impersonation is a \$1Tn problem

- This is only the beginning
- The cost of fraud is about to drop to zero
- Fraud is no longer artisanal – it is industrial

Our goals

Prevent Impersonation ✓

Ensure legitimate number use ✓

Enable enforcement ✓

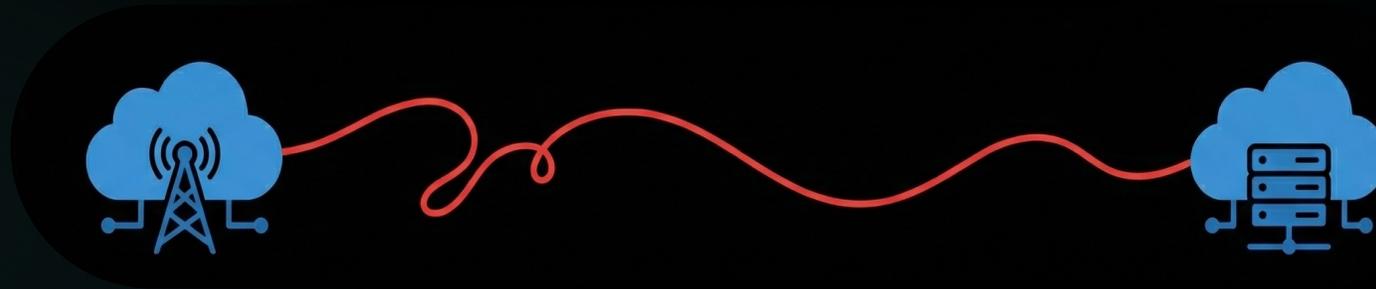
Protect citizens – without breaking legitimate services ✓

***** through decentralised identity *****

Restoring trust – a split focus

Originating Carrier

Terminating Carrier



But who is the caller?



Originating carrier controls

- KYC requirements
- Attestation levels (STIR/SHAKEN)
- Number allocation controls (for example – non-suballocation)
- Information disappears on the first hop



Terminating carrier controls

- Obligations to protect from harm
- Obligations on domestic numbering
- No information comes with the call



Why we fail



Evidence



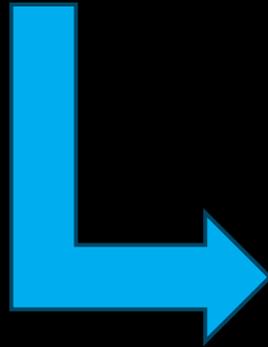
Inference

The Accountable Party



Portable Evidence

- Who am I?
- What assets can I claim?
- What obligations have I accepted?
- What services may I use?



Accepted by:

- All operators
- All services
- All geographies
- Any originator

Accountability vs Inference

10

Inference (today)

- ✗ Traffic patterns
- ✗ Heuristics
- ✗ Post-event
- ✗ Probabilistic

Accountability (OVC)

- ✓ Explicit Identity
- ✓ Cryptographic proof
- ✓ With the call
- ✓ Deterministic

Vetting the Accountable Party

Legal existence

Telecoms-specific rights

Intellectual Property

Rights to originate

Regulated rights



Following GLEIF guidance

Phone numbers

Brand name, logo

RCS chatbots, Phone calls

Financial offers, healthcare

The vetting ecosystem

GSMA™

Defines the appropriate outcomes of vetting
Reviewed with industry
Discussed with regulators

Policy
Administrator
(an Auditor)

Assesses Vettors fitness as vetting providers
Reviews Vettors' processes against GSMA criteria
Monitors Vettors' performance in-life

Authorised
Vetting Agent

Builds vetting processes to determine KYC and RTU
Submits processes and vetting results for audit review
Audits and re-audits enterprises against specific services

Accountable
Body (the brand)

Contracts with Authorised Vetter to gain the rights to use
a particular service
Delegates their credential to an aggregator/platform

MNO

- Lightweight for each MNO
- Evidence of the rights of an originator along with the communication
- A clear feedback loop



Governance as a root of trust



The proof platform



Policy Administrator (an Auditor)

Authorised Vetting Agent

Accountable Body (the brand)



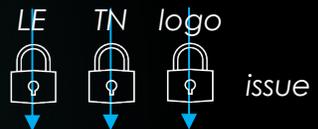
Root of Trust



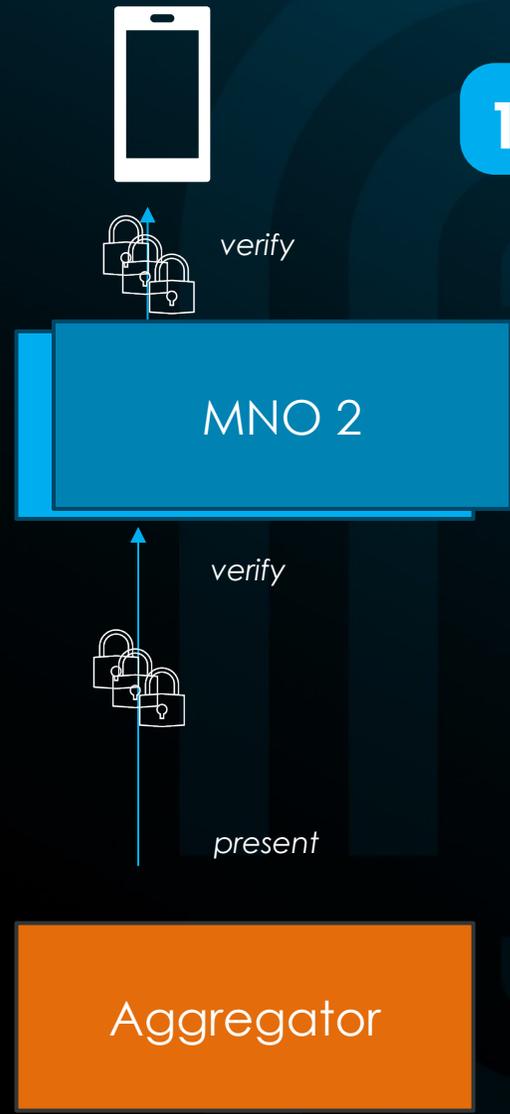
I am authorised to qualify vetters

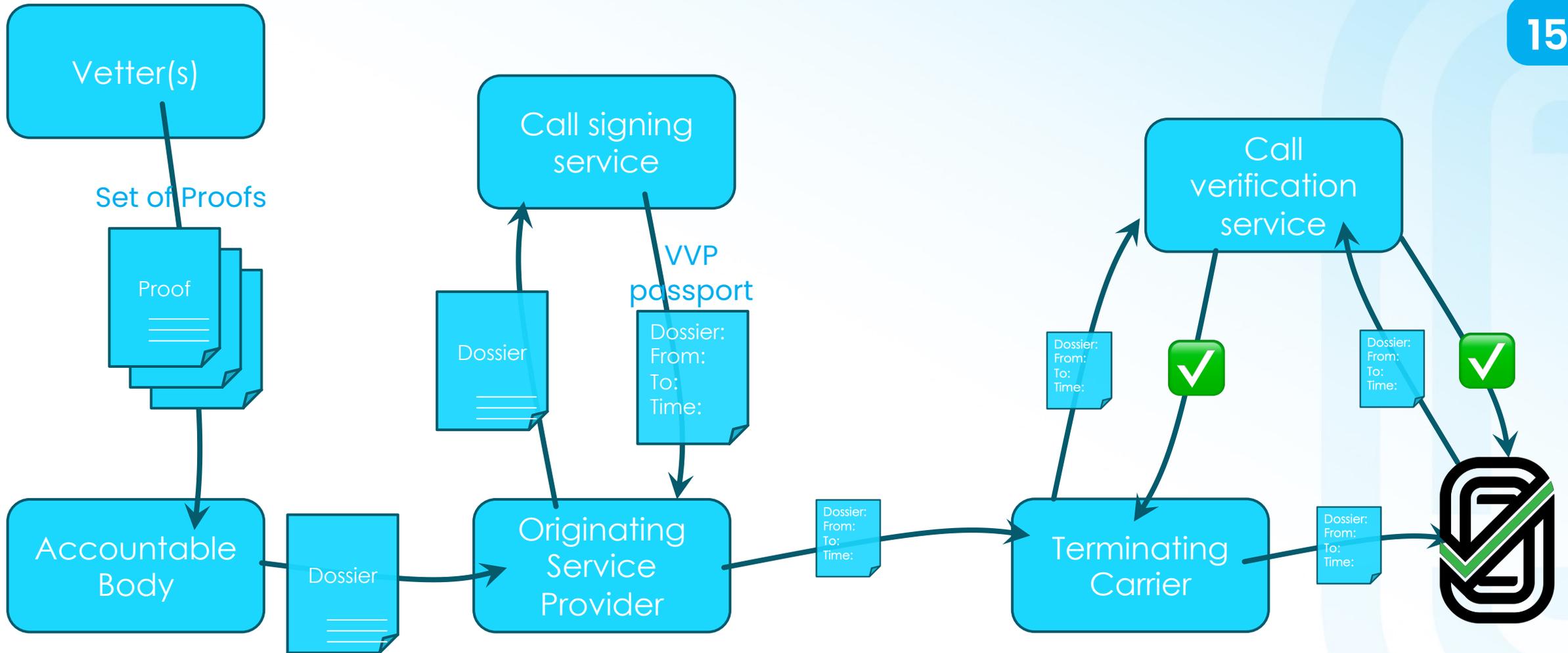


I am authorised to vet for Service X in territory Y



I am ACME Ltd
Using phone number +444 XXX
With Logo **A**





Vetting needs:

Identity+rights

- Who is the originating party
- Are they authorised to undertake this specific communication
- Are the assets they are using appropriately granted to them

Proof

- Binding the identity to the contracting party
- Signing the rights to the party
- Making the proofs available anywhere
- Stable, simple to manage proofs
- Display of the rights to the appropriate party

Verification

- Appropriate carriers should be able to verify all their traffic
- End users should see the results of verification
- Privacy and consent are critical



Worked Examples



Defeating the fraudster



- Robust vetting makes fraud difficult to start
- Robust evidence supports traceability
- Cryptographic assets enable immediate revocation

Supporting good callers



- Robust vetting assesses Right to Use
- Robust evidence supports appropriate action
- Cryptographic assets enable historical analysis

Implications for enforcement of laws

20

Today



With OVC





Panel Discussion

Moderated by Eric Drury

Panelists – aftertnoon session

Name	Affiliation
Glyn Povah	Telefonica Tech
Arifur Rahaman	Nextgen Clearing Ltd.
Victor Shisterov	Vonage
Peter Nilsson	Microsoft
Randy Warshaw	Provenant



On the internet, nobody knows you're a dog.



"ON THE INTERNET, NOBODY KNOWS YOU'RE A DOG."

The New Yorker cartoon, Peter Steiner,
July 1993

On the phone, nobody knows you're a dog.

The New Yorker cartoon, Peter Steiner,
July 1993



"ON THE INTERNET, NOBODY KNOWS YOU'RE A DOG."

Question for Panelists

How does *the lack of verifiable identity* impact your business specifically?

Q&A

Questions and comments from webinar attendees.



What does this all mean?

28

From fragmented controls → shared evidence

- Accountability moves from networks to callers
- Proof replaces inference – end-to-end
- Fraud becomes hard to start and impossible to scale
- Legitimate communications stop being collateral damage
- Regulation, enforcement, and operations align on the same facts



*Open Verifiable Communications –
evidence that travels with the message*

- LEI/vLEI
- Digital IDs



Identity



Trust
Technology



Verifiable Credentials



Rights
and
Authority

- Phone numbers
- Brand name
- Logos
- Delegation

Handset
Support

- Deployment across a wide range of devices
- Consistent support from major OEMs
- Full visibility to the consumer

Vetting and
Governance

- Governance Authority
- Rules for Vetting
- Audit and Revocation

Monetisation
Support

- Success-based
- Supports settlement agents
- Built on existing monetisation models
- Supports free/freemium and chargeable

Multiple
Deployment
Models

- In-band for full MNO visibility
- In-network OOB for simple MNO deployment
- Out of network, OOB for trials and demonstrators