JANEIRO DIGITAL

Stopping the Exploitation of Internetwork Signaling

Justin Bingham

Janeiro Digital

Solid Core Team

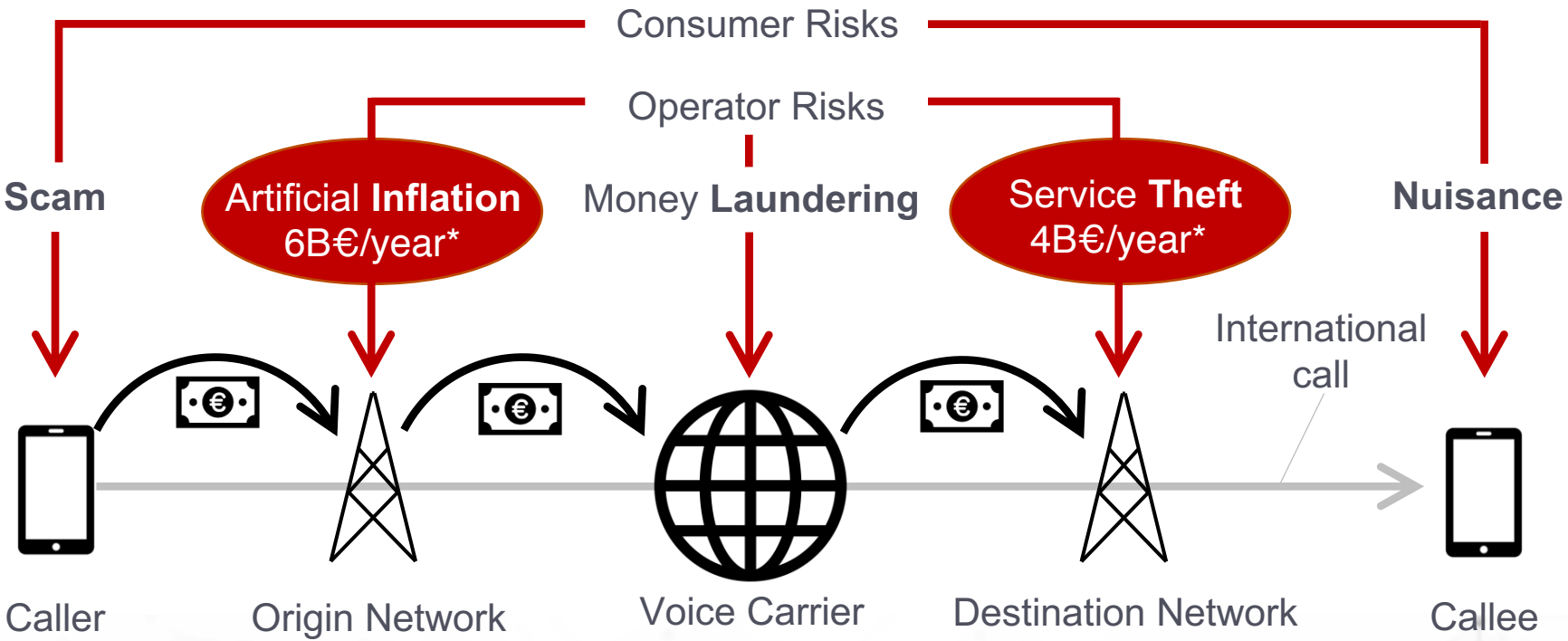
Agenda

1. Problem
2. Solutions
3. SEISMIC
4. Implementation
5. Demonstration

Problem

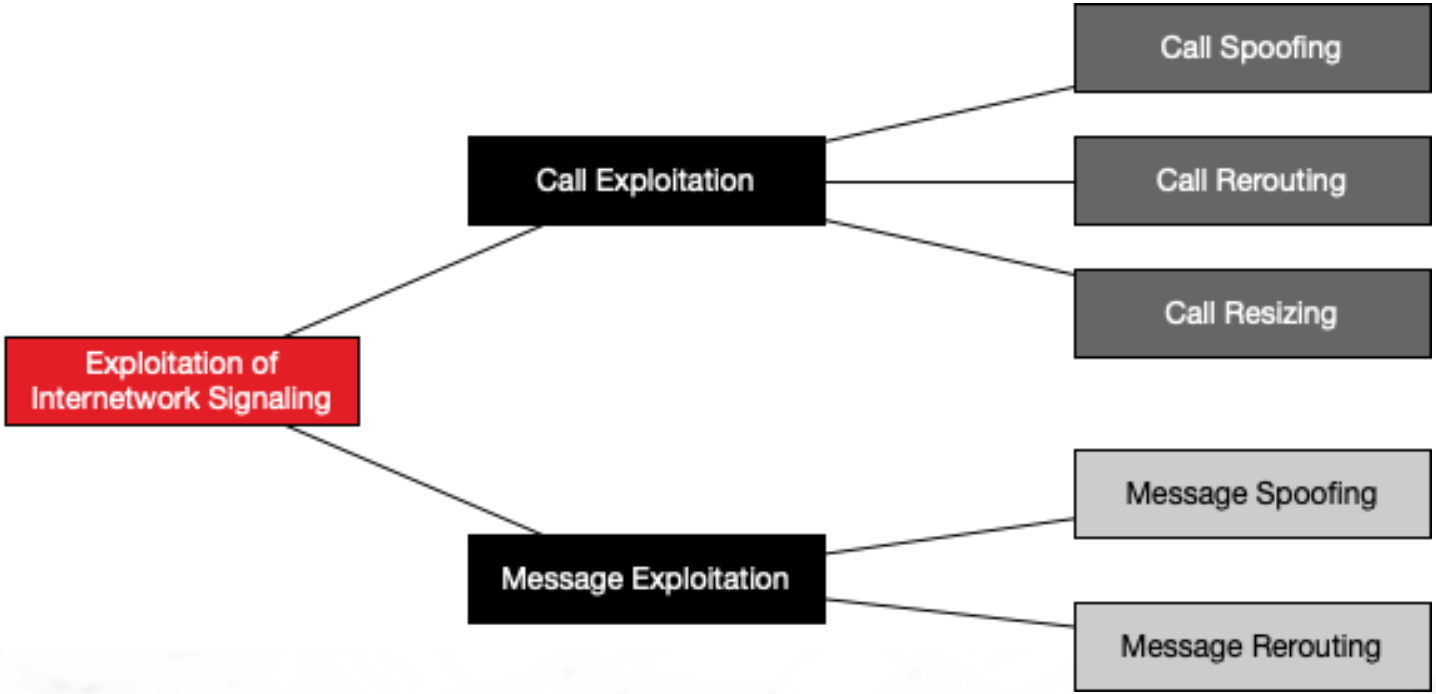
Internetwork Fraud is pervasive, hard to prevent, and **costing the victims a lot of money**.

International Call Risks



* CFCA worldwide survey

Exploitation of Internetwork Signaling



CLI Spoofing

The ability to impersonate a caller number is a primary or contributing factor in numerous types of fraudulent activity.

- Robocalling
- Wangiri
- Scam Calls
- OBR Spoofing
- VM Brute Force
- Call Bombing

…And a contributing factor to other fraud categories

CLI Spoofing

The ability to impersonate a caller number is a primary or contributing factor in numerous types of fraudulent activity.

Prevention:

- **Trust in the CLI is paramount**
- **Validate the Origin Network, who in turn can attest to the validity of the Caller Identity.**

Call Rerouting

Short Stopping

A rogue carrier diverts a call from it's proper destination through number range hijacking or route manipulation, receiving money from the upstream entities.

A prominent mechanism for *International Revenue Share Fraud*.

Call Rerouting

Interconnect Bypass

Illegitimate carriers bypass the legitimate destination network gateway to avoid international termination fees.

- Sim Box
- OTT

Call Rerouting

Interconnect Bypass

Illegitimate carriers bypass the legitimate destination network gateway to avoid international termination fees.

Prevention of both:

Prove to the Origin that the intended Destination network has received the call

Call Resizing

Fraudulent carriers manipulate the duration of a given call in transit to influence the associated charges.

- Call Stretching
- False Answer Supervision

Call Resizing

Fraudulent carriers manipulate the duration of a given call in transit to influence the associated charges.

Prevention:

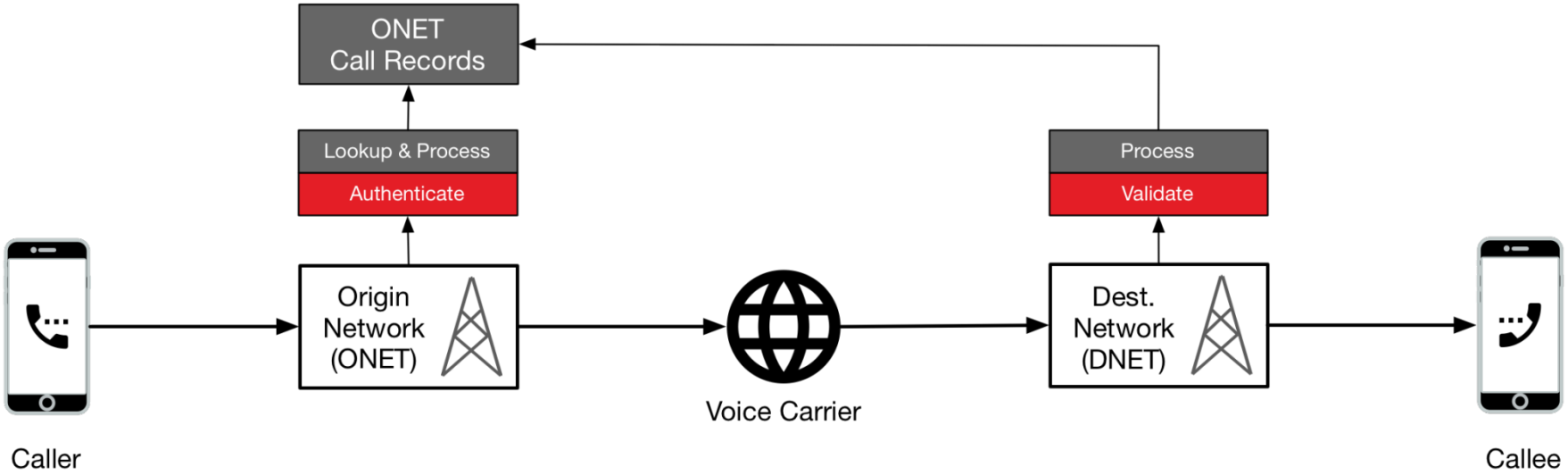
- **Verified call record shared by the Origin and Destination Networks**
- **Includes timestamped events for accurate duration times**

New Solutions Required

Conservative estimates project annual losses in excess of **10+ billion dollars per year**.

Our Goal

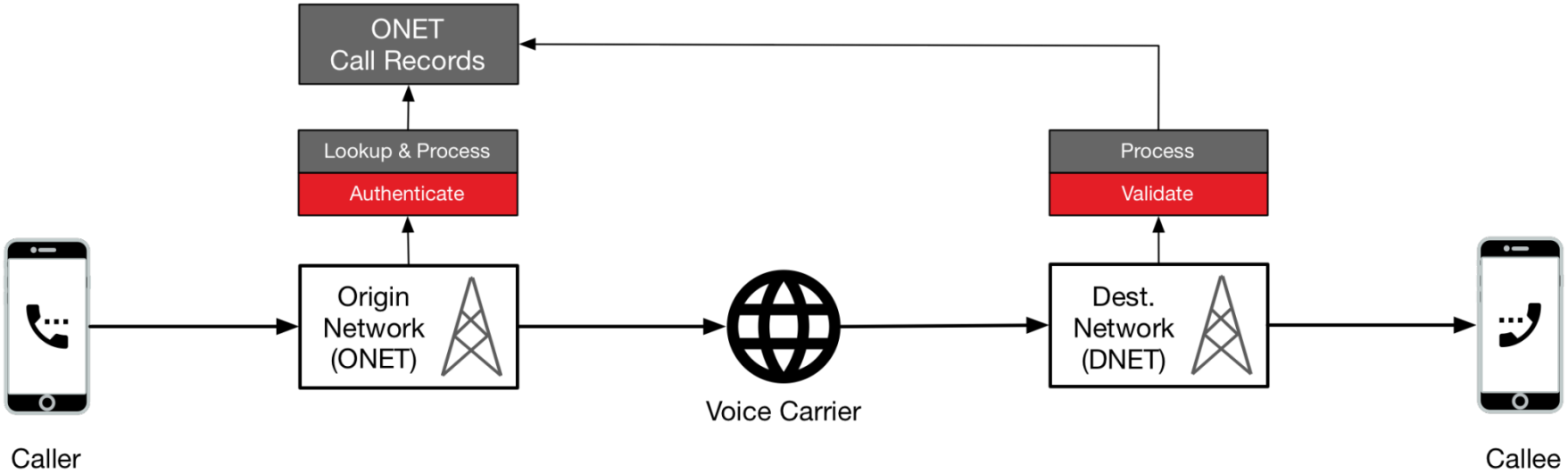
Prevent Internetwork Signaling Fraud in a manner that's **flexible enough to be adopted universally**, and **effective enough to seriously reduce fraudulent activity**.



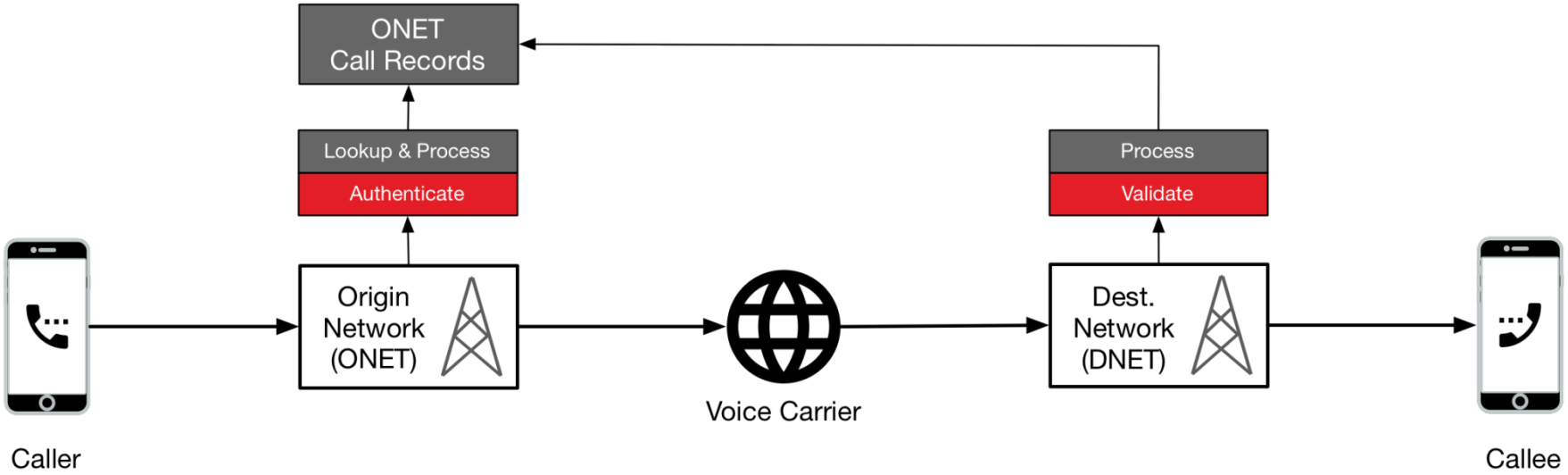
SEISMIC

Stopping Exploitation of Internetwork Signaling by Mitigating Illegitimate Communications

JANEIRO DIGITAL

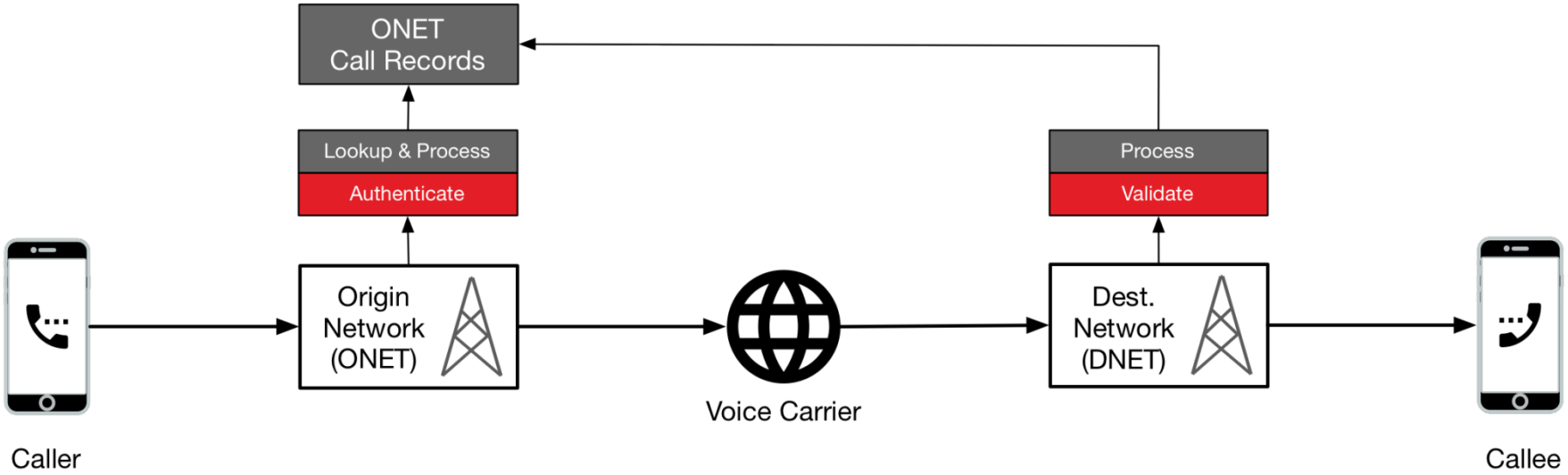


1. Caller initiates a call via Origin Network
2. Origin Network authenticates the source of the call
3. Origin Network looks up the Destination, checks participation

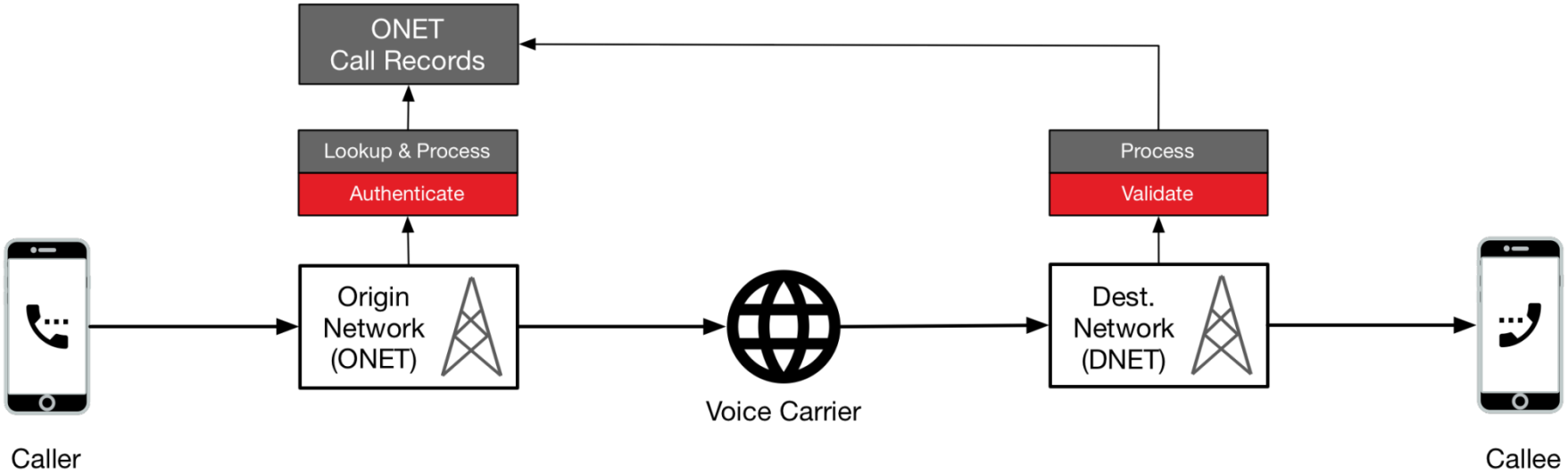


4. Origin Network creates a Call Record

5. Networks, Caller ID, Callee ID, and Initiate Event stored with associated Timestamp.

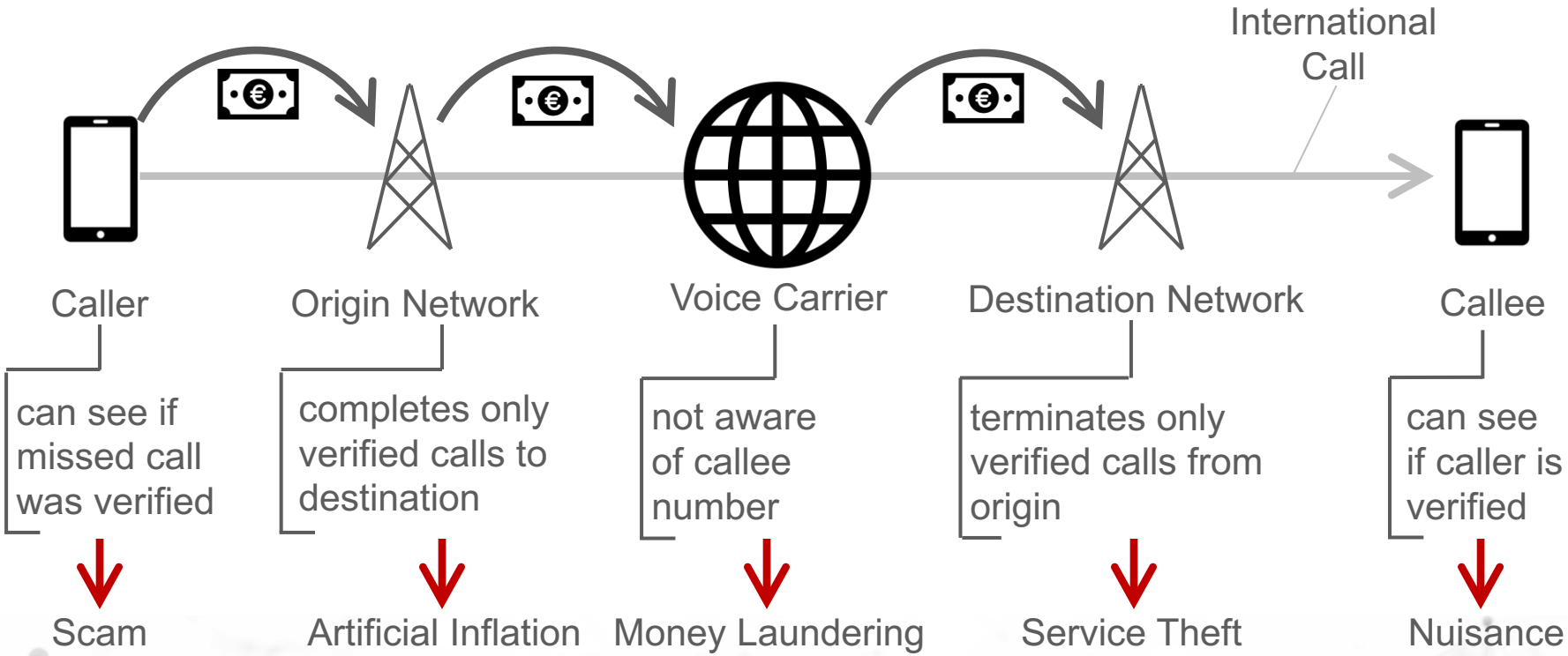


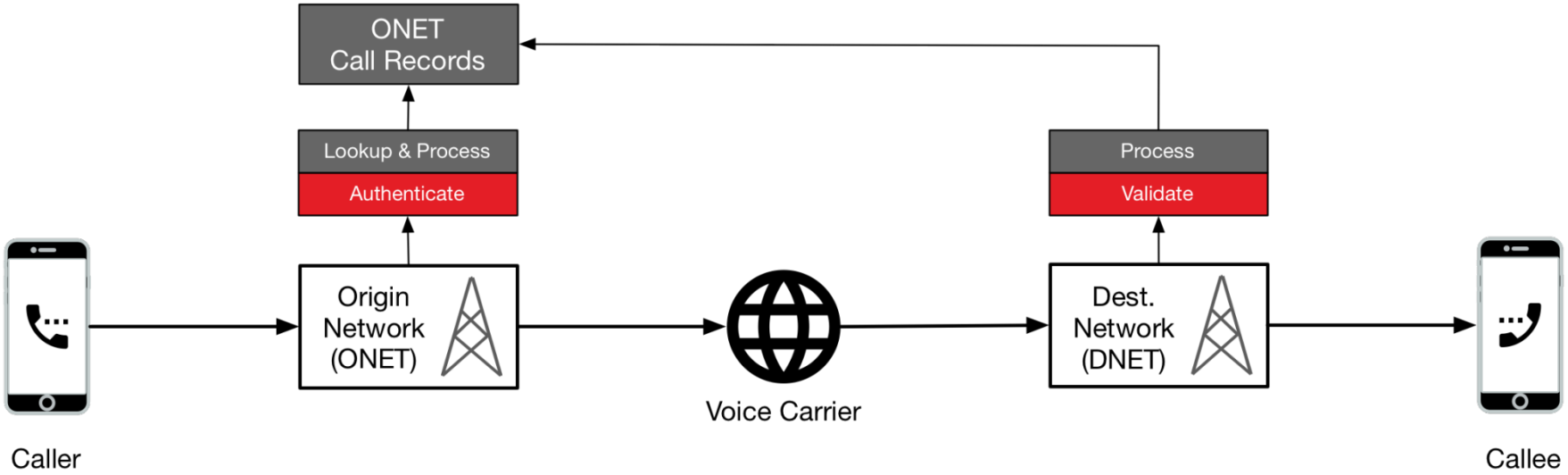
6. Origin Network anonymizes the callee by changing “To” to the Callee Routing Number (gateway of the Destination Network), and the “From” to a Caller Temporary Number.



7. Destination Network receives the call and validates the Origins
8. Destination Network looks up the call record and gets the callee
9. Destination Network completes the call and updates the Call Record

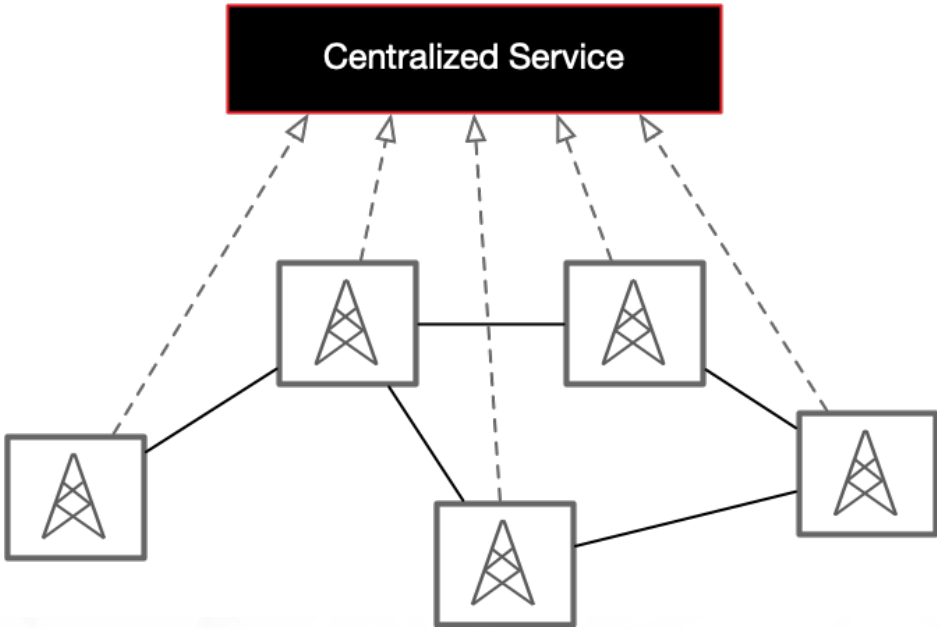
SEISMIC Benefits



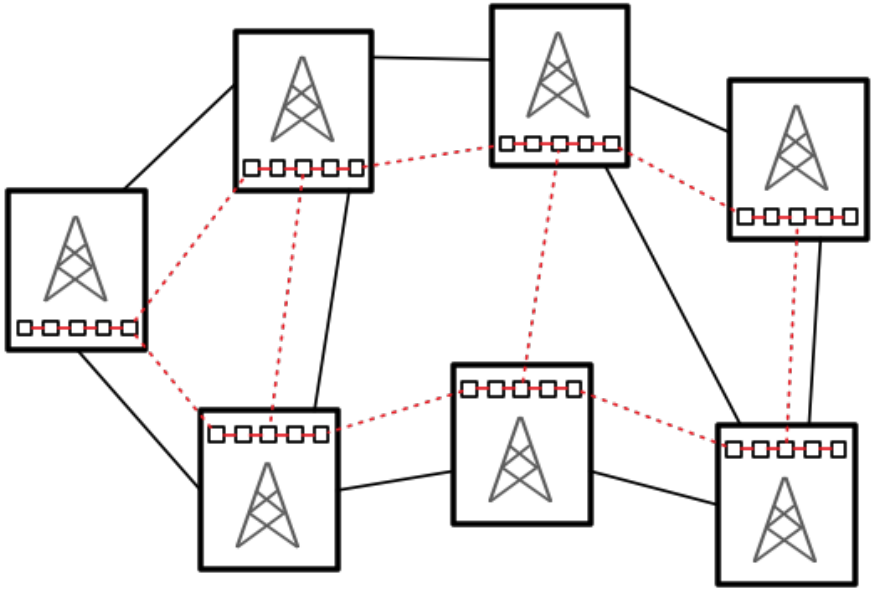


What approach do we take to implement this?

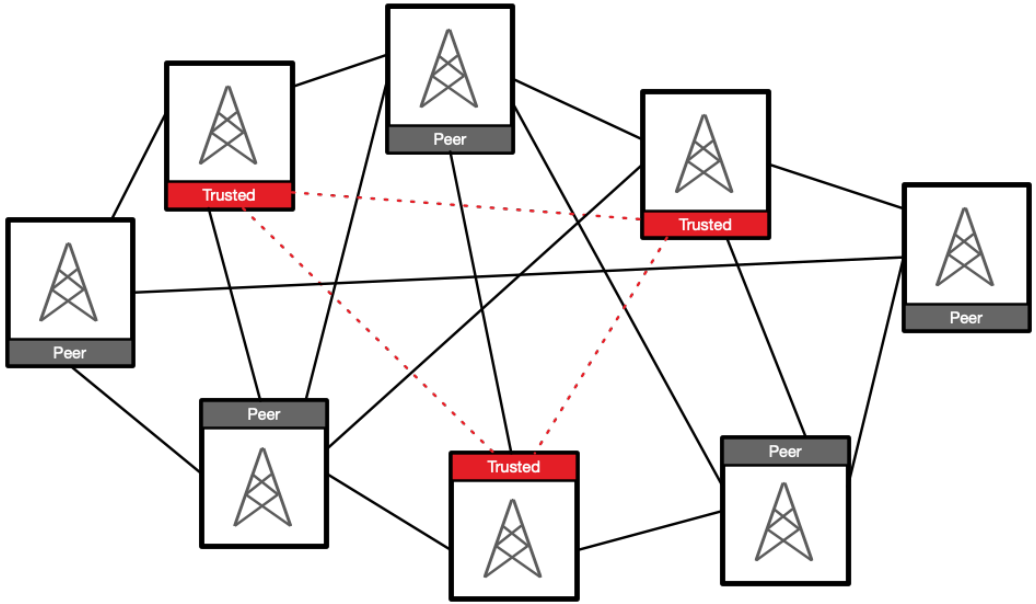
Centralized Service



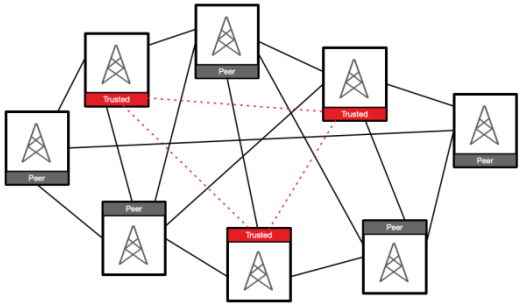
Distributed Blockchain



Distributed Peer to Peer



Distributed Peer to Peer



Recommended Approach

STIR / SHAKEN

Call origin validation and for the secure transport of call meta-data between networks

SOLID

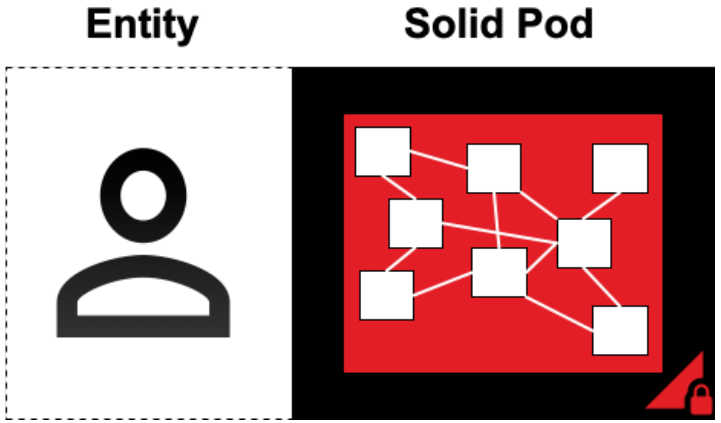
Decentralized infrastructure for flexible and secure data sharing between networks built on open web standards.

STIR / SHAKEN

Validate the caller and prove the identity of the Origin Network

- SIP Identity Header used passes the URL of the call record to the Destination Network.
- Destination Network knows meta data hasn't been tampered with in transit.

Solid



Individual entities separate their data from the systems and applications that leverage it into decentralized data stores (***pods***)

Built on the Web. Solid extends HTTP with a set of open standards and protocols.

Created by the inventor of the Web, Sir Tim Berners-Lee.

Solid

Built on the web with open standards, Solid provides a common backend for decentralized applications and system infrastructure.

Identity – **WEBID**
Authentication – **OPENID CONNECT**
Authorization – **WEB ACCESS CONTROL**
Transport - **HTTPS**
Interface – **LINKED DATA PROTOCOL**
Messaging – **LINKED DATA NOTIFICATIONS**
Data Model – **RDF / LINKED DATA**
Graph Search – **TPF / SPARQL / GRAPHQL**

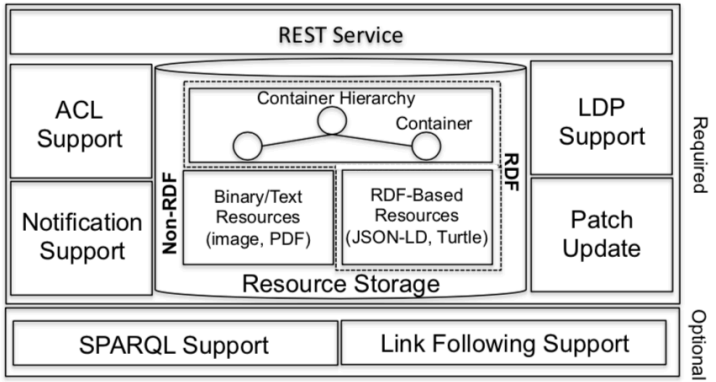
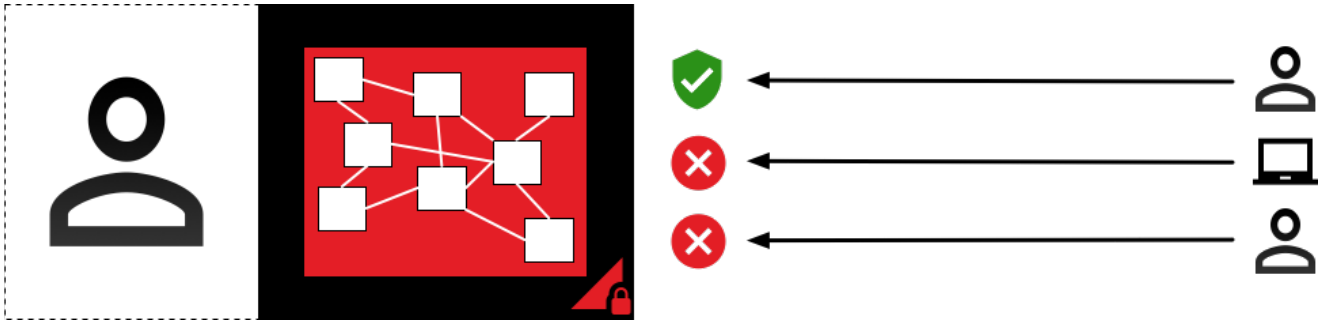


Figure 2: Overview of a pod server. A pod stores RDF and non-RDF resources. The server support LDP, patching resources, access control, live updates, and optionally SPARQL.

Solid

Each individual entity controls the data in its pod, and chooses which other entities it will share that data with.

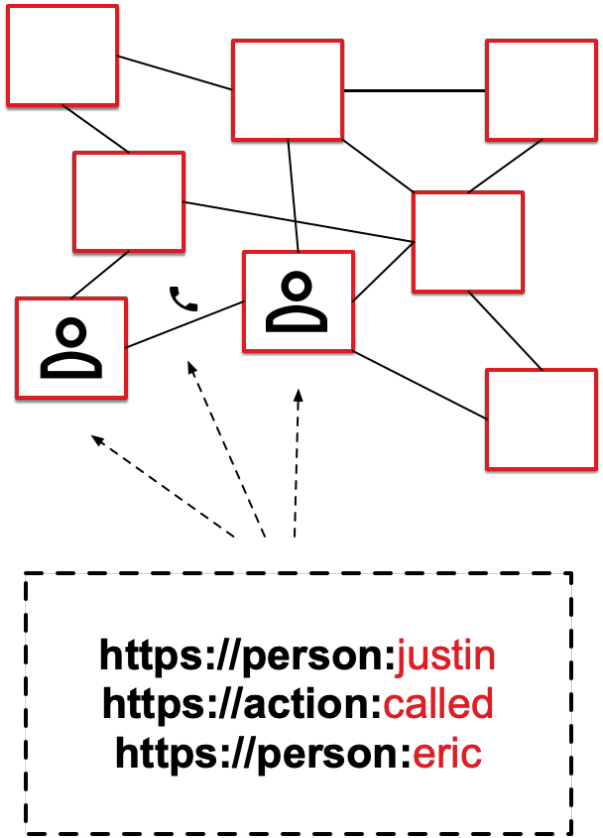


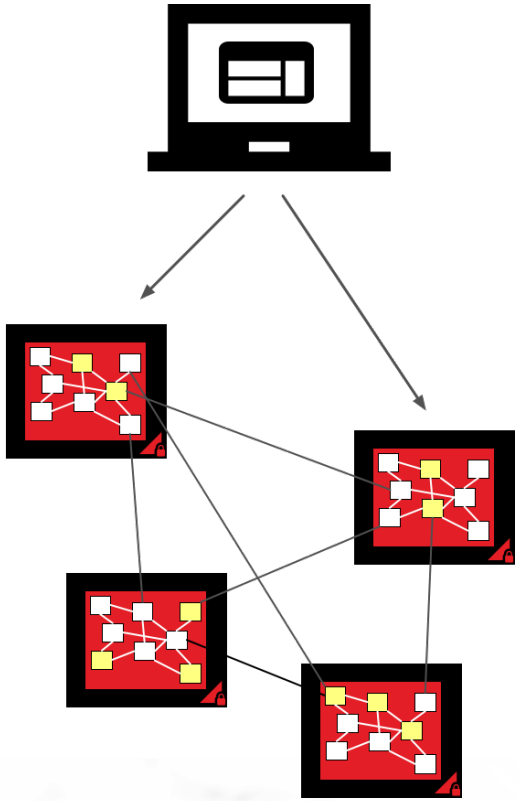
Powered by Linked Data

You can store any kind of files or data in a Solid pod. It falls into two categories…

- **Arbitrary Files**
- **Linked Data**

Every linked data item has a URL – and can be interlinked, creating a globally distributed graph where you can represent and link any kind of “thing”.



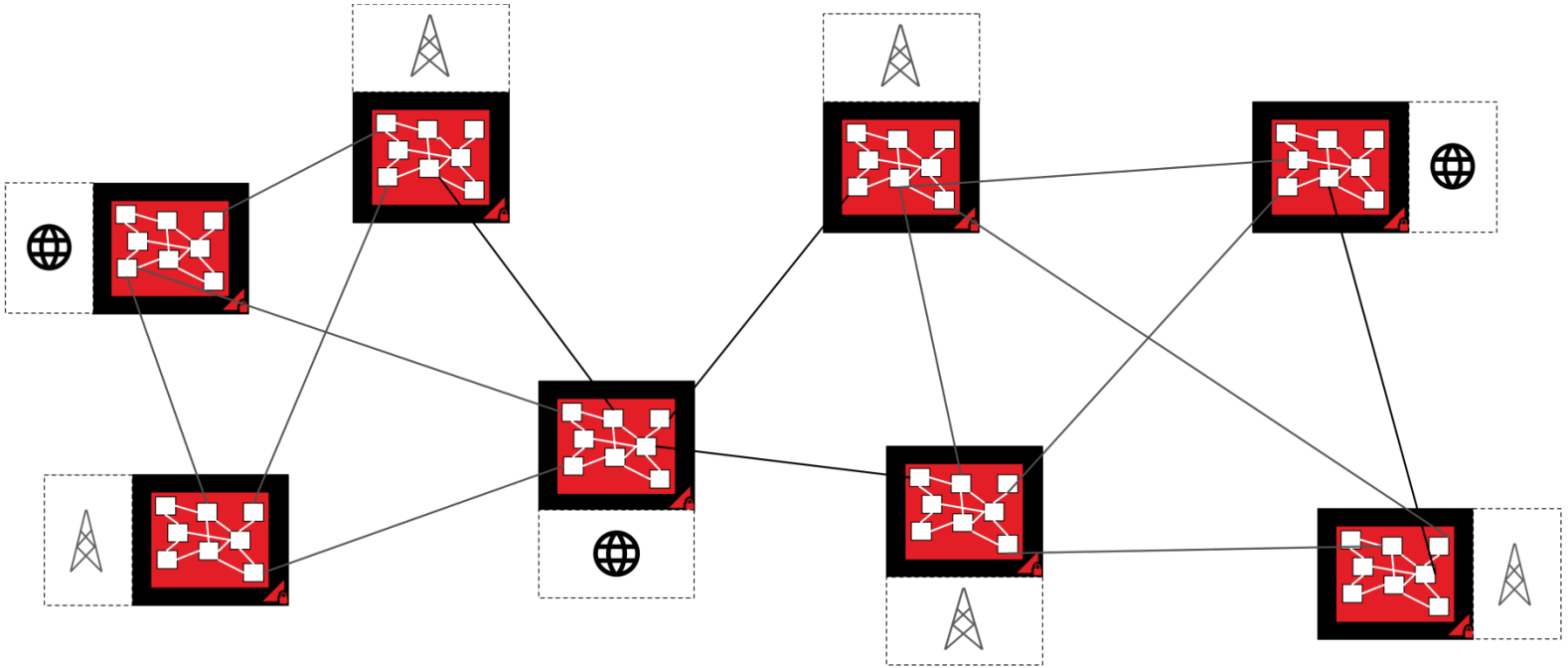


Inherent Interoperability

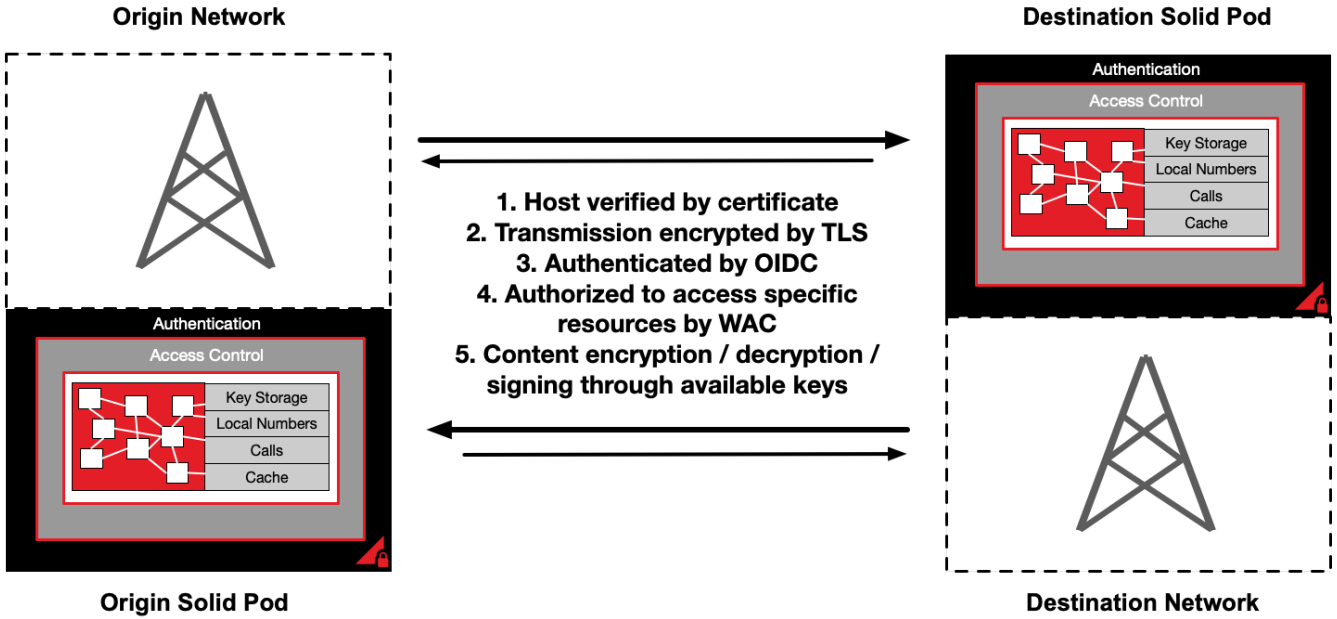
Things in linked data are defined by **shared vocabularies** and **data shapes**.

Vocabularies and shapes provide **native interoperability of data** even when it is stored in different places or read / written to by other applications.

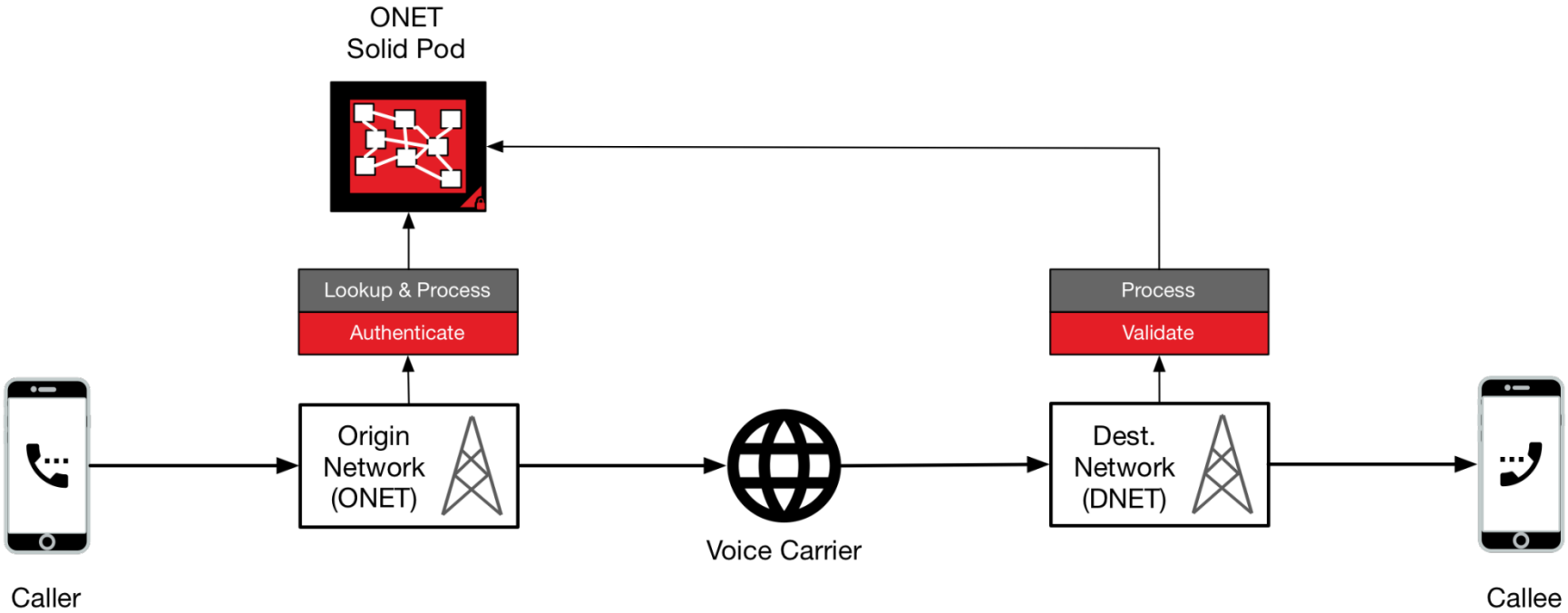
As a result, any credentialed application can safely manipulate any kind of thing in any pod.



Decentralized graph data model maps perfectly to the real-world data model of internetwork communications.



Decentralized Identity and Security Model provides Peer to Peer Authentication, Authorization, and Crypto.

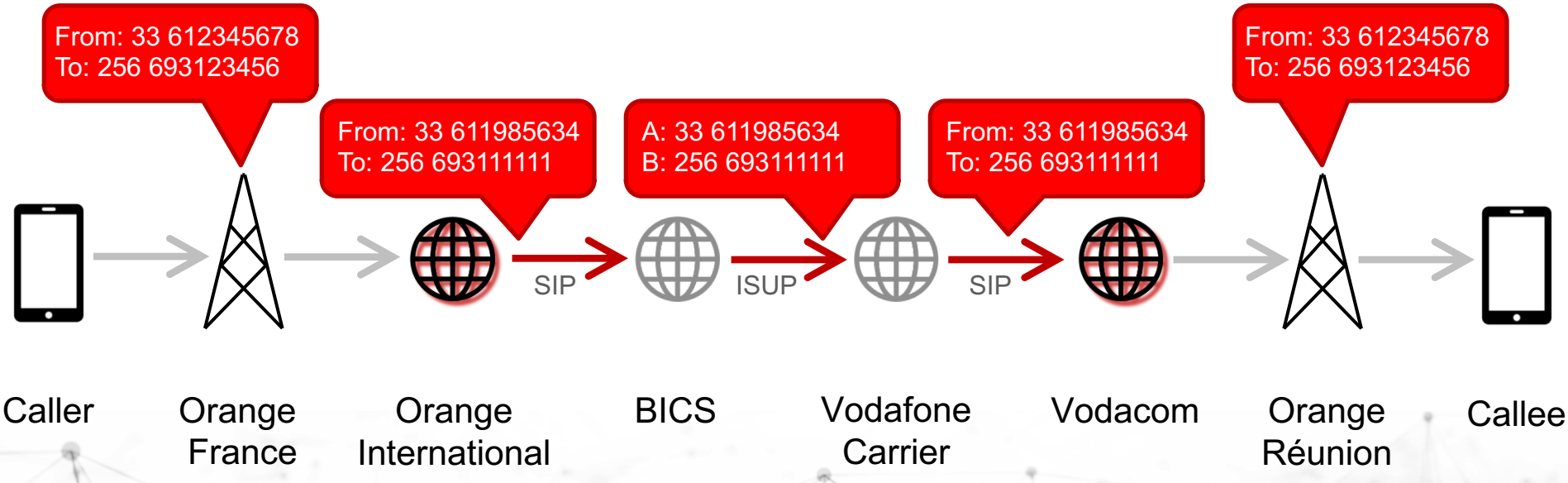


Mitigates all target fraud scenarios without any disruption to the legitimate eco-system of operators, carriers, callers, and callees

DEMONSTRATION

SEISMIC Call

- Caller number swapped by a temporary number identifying the call
- Callee number swapped by a number identifying the destination network



Caller Temporary Number Format

GUID possible using 15 digit CID + Reference Clock

- YYYYMMDDHH prepended to E.164 CID using syncronized time source (NTP, GPS, etc).
- 6 digits for HNI (MCC+MNC) or fixed network identifier to identify which ONET pod to request the call record from.
- 9 digits for unique call identifier (unique for given hour on a given pod).

Allows for one billion unique call IDs/hour/network

Callee Routing Number

Routable Destination Number

- Number does not represent a special carrier route and should be routable to DNET via existing networks.
- DNET treats all inbound caller IDs on the SEISMIC routing number as SEISMIC call reference identifiers.
- Full SEISMIC CRI can be embedded in SIP headers but is recoverable if lost during routing using ref clock + CID.