FIRST ORION
TRANSPARENCY IN COMMUNICATION

THE STIR/SHAKEN GAP FACING ENTERPRISES

AND HOW TO ADDRESS IT WITH DISTRIBUTED LEDGER TECHNOLOGY

A FIRST ORION WHITE PAPER

Table Of Contents

The Challenge: Enterprise Identities are Complicated in a STIR/SHAKEN World

Illegal and spoofed robocalls are distressing the telecommunications industry. In 2019 the Federal Trade Commission received 1.7 million fraud complaints for a reported total loss of $1.9 billion USD[1]. Over 74% of these frauds reported were through phone calls. In an attempt to combat illegal robocalls, the Federal Communications Commission (FCC) outlined plans requiring the industry to implement a call-authentication system called STIR/SHAKEN by June 2021[2] (with some exemptions). The SHAKEN standards, short for Signature-based Handling of Asserted Information Using toKENs, enables carriers to "sign" calls originating from their network with information about the calling party, which then allows for verification of the signature by the terminating network before reaching users' phones.

STIR/SHAKEN does not innately prevent robocalls; however, SHAKEN does establish a framework whereby carriers can use additional techniques to identify, track, and mitigate illegal, spoofed, and fraudulent robocalls. Many current STIR/SHAKEN implementation strategies focus on the ability of originating service providers (OSPs) and terminating service providers (TSPs) to assert the caller's authenticity.

However, enterprises have a vested interest in ensuring their calls are verified as well, as do call centers who support those business calls. Without **Enterprise STIR/SHAKEN** to verify a business identity, many businesses and call centers are at risk. This technical white paper reviews a breakthrough approach to verifying enterprise identities with distributed ledger technology (DLT).

Enterprise STIR/SHAKEN Strategies Being Considered Include:

- **Delegate Certificates, Enterprise Certificates, and Lemon-Twist** – all extend the baseline SHAKEN framework by providing additional data to aid in determining attestation prior to presenting the call to the subscriber.
- **Enterprise-Level Credentials and Telephone Number Letter of Authorization Exchange** – a business process whereby an electronically signed document establishes the enterprise identity, and the "right to use" telephone number is used to issue cryptographic credentials.
- **Central Telephone Number Database** – a central authority maintains a repository of telephone numbers, uniquely identifiable respective owners, and delegation artifacts that the OSPs and TSPs query during the call setup.
- **Distributed Ledger Technology (DLT)** – distributed ledgers provide a decentralized immutable ledger and guarantee a single source of truth, allowing all stakeholders to validate enterprise identities to meet full attestation requirements and deliver verified calls.

1 https://www.ftc.gov/system/files/documents/reports/consumer-sentinel-network-data-book-2019/consumer_sentinel_network_data_book_2019.pdf
2 https://www.fcc.gov/call-authentication

Why Do We Need Distributed Ledger Technology for Enterprise STIR/SHAKEN?

While the alternative approaches have their unique advantages and disadvantages, most fall short of developing a new, strategic ecosystem that addresses all the challenges faced by enterprises. There are multiple calling scenarios where distributed ledger technology (DLT) may be the best fit for enterprises and call centers, such as:

ONE-TO-MANY USES

Enterprises often provide the same telephone number to multiple 3rd party call centers and will make calls with one number for many reasons (e.g., customer service, application processing, account alerts).

LEGITIMATE SPOOFING

A national enterprise may use local numbers, sometimes in rapid succession, on behalf of a local franchise or establishment. Conversely, a local agency may use the national enterprise number (e.g., toll-free) to initiate outbound calls from their own lines.

RAPID RE-USE

Mobile app developers and businesses (such as a ride-share app or vacation rental marketplace) may access a pool of temporary phone numbers to make short-lived, temporary assignments for quick consumer communication.

Distributed ledger technology solves these use cases by validating the telephone number's "right to use" on a per call basis. These immutable records serve as a single source of truth so the OSP can cryptographically validate and authenticate the enterprise identity originating the call and verify the use of the telephone number.

The STIR/SHAKEN Gap Facing Enterprises

Enterprises often use multiple service providers from which they originate calls, and the OSPs do not always know if the business placing the call has a legitimate right to use of the number. Additionally, each service provider must already undertake its own “Know Your Customer” (KYC) vetting process to onboard businesses.

While some KYC processes are handled via internal business practices, some 3rd party KYC vendors will verify the identities of businesses registering phone numbers. OSPs use the information collected during KYC vetting processes to authenticate the caller and sign the calls under the STIR/SHAKEN framework. Since the KYC processes can be internal or 3rd party, there’s often little standardization around the process and a lack of portability when KYC vendors are working with multiple service providers.

Even with this process in place, attesting to phone number ownership poses a variety of other challenges. Telephone number assignments can come from multiple sources for any given enterprise business caller, including telephone number service providers (TN Providers) and telephone number resellers (TN Resellers). In addition, the business may not actually make calls themselves, but instead rely on 3rd party call centers to originate calls on their behalf using a telephone number assigned to the business, but not the call center.

Not to mention, a 3rd party call center may use a variety of OSPs for call origination in order to optimize its outbound traffic cost. Furthermore, a strict “traceback” process is mandated by existing regulation to be sure each phone call can be traced to its originating party.

FULL ATTESTATION IS REQUIRED FOR PRESENTING VERIFIED CALLER DETAILS

The process of asserting the identity of outbound numbers is called “attestation” as defined by the FCC[3]. Using trusted public key networks, originating carrier networks provide information about outbound calls by signing it in one of three levels:

- A-Level - Full attestation – The OSP is responsible for call origination, has a direct authenticated (KYC vetted) relationship with the customer, and has established a verified association with the telephone number used for the call.
- B-Level - Partial attestation – The OSP is responsible for call origination, has a direct authenticated relationship with the customer, but has NOT established a verified association with the telephone number used for the call.
- C-Level - Gateway attestation – The OSP is an entry point (or gateway) for the call onto its network but possesses no direct authenticated relationship with the originator.

3 https://docs.fcc.gov/public/attachments/DOC-362932A1.pdf

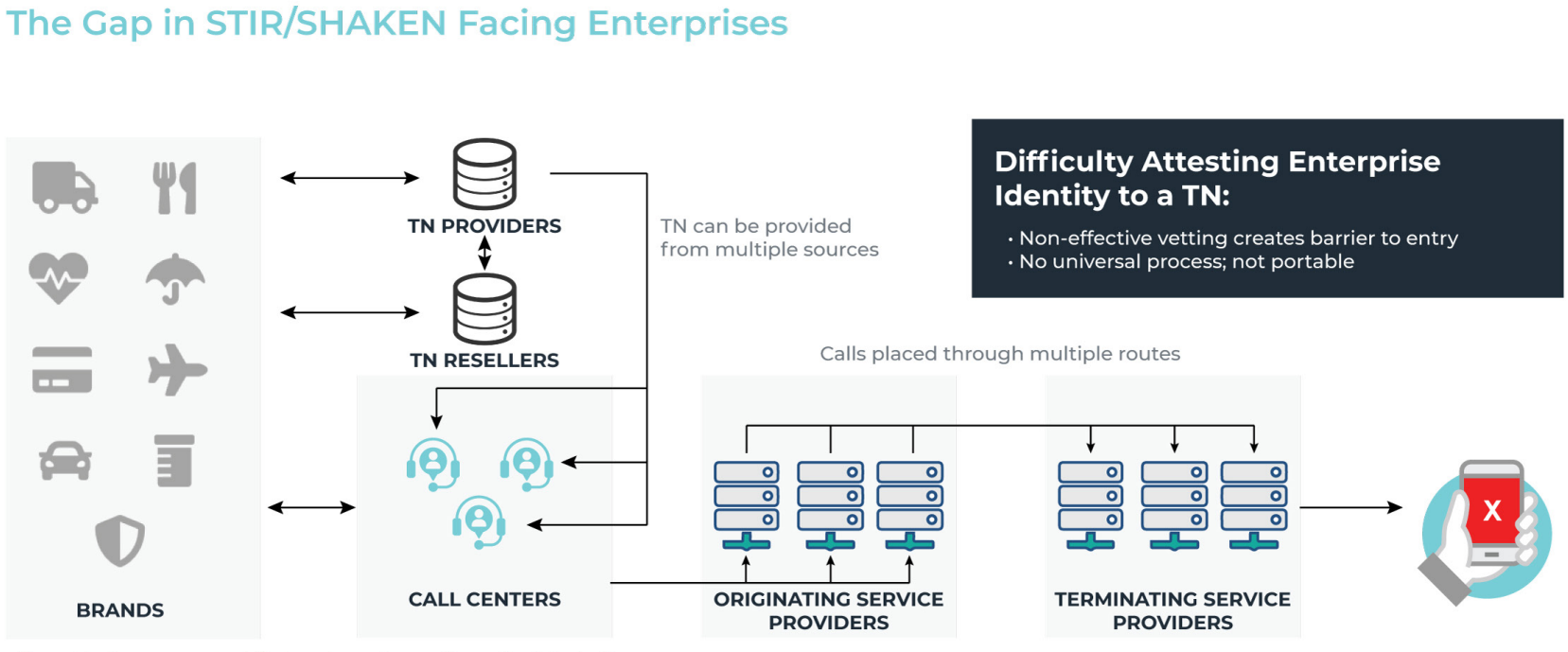
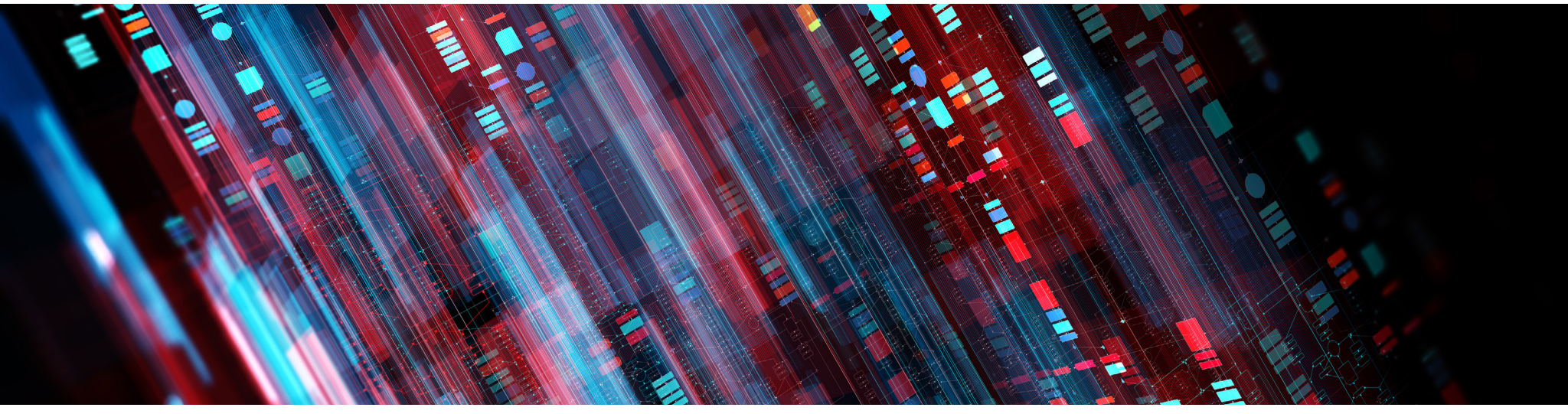


FIGURE 1

The combination of all of these practices makes standardization incredibly complex. Enterprises need a way to make sure, regardless of their size and existing business ecosystem, that they can effectively and securely make phone calls. Enterprise STIR/SHAKEN will provide the ability for enterprises to participate and ensure their calls are authenticated and verified regardless of where they acquire their telephone numbers and what entity/service provider they use to place the calls.

An Enterprise STIR/SHAKEN implementation could be achieved using any of the core Enterprise STIR/SHAKEN strategies described above, but this research explores how authentication is most successful when unique enterprise identities are easily available across all carriers.



Distributed Ledger Technology is Transforming Business Calling

Distributed ledger technology is specifically built to easily store, process, and transmit unique identity information. First Orion is leveraging this functionality to support an Enterprise STIR/SHAKEN use case with distributed ledgers. After deploying STIR/SHAKEN for two Tier 1 carriers in the US, First Orion continues a natural progression toward helping carriers and enterprises navigate the regulatory world of STIR/SHAKEN to ensure compliance and robocall mitigation through our world-class solutions.

Distributed ledger technology systems are built upon proven methodologies including distributed computing, cryptographic encryption, and hashing. Distributed ledgers provide a **decentralized immutable ledger** managed by multiple participants across multiple nodes. Each node always contains the same version of the ledger and guarantees that synchronization forms a **single source of truth**.

Cryptographic algorithms ensure immutability and non-repudiation to preserve the integrity of the data, whereas cryptographic links (hashes) ensure full audit trail chaining all blocks (transactions) together and making it apparent to all users when a change has taken place. All actions on the data executed via smart contracts are also cryptographically signed, making sure no transactions can take place unless the code performing them is explicitly allowed to do so.

Thus, distributed ledgers allow for unique enterprise digital identities to be created, presented, and validated as a global identity network, expanding the ability for all stakeholders to validate enterprise identities.

DISTRIBUTED LEDGER TECHNOLOGY WORLDWIDE

Distributed ledger technology is currently being used worldwide across many industries, including telecommunications and government services, to increase the security of information being shared and accountability of parties handling such information. Almost every single major US Tier 1 carrier and most EU Tier 1 carriers have been using distributed ledger technology to settle roaming charges.

The ATIS Distributed Ledger Technology Initiative[4] was launched to validate key aspects of distributed ledger technology as it applies to real-world challenges facing today's communications industry. The International Telecommunications Union has issued guidance[5] on distributed ledger standardization, use cases and reference architectures. Global System for Mobile Communications Association followed suit by providing a paper on the Operator opportunities[6] and regulatory overview[7].

4 https://www.atis.org/initiatives/distributed-ledger-technology/
5 https://www.itu.int/en/ITU-T/focusgroups/dlt/Pages/default.aspx
6 https://www.gsma.com/newsroom/wp-content/uploads/IG.03-v1.0_Whitepaper.pdf
7 https://www.gsma.com/identity/wp-content/uploads/2018/09/Distributed-Ledger-Technology-Blockchains-and-Identity-20180907ii.pdf

Enterprise STIR/SHAKEN Identity Management Using Distributed Ledger Technology

While distributed ledger technologies play a huge role in the future of computing, implementing an enterprise identity with distributed ledger technology in the existing STIR/SHAKEN ecosystem is a viable approach that enables SHAKEN to meet its full potential. In December 2019, ATIS outlined how the telecom industry might employ distributed ledger technologies to overcome these issues of enterprise caller attestation in the ATIS-I-0000076 'Enterprise Identity on Distributed Ledger for Authenticated Caller Use Cases' technical report[8].

As mentioned previously, for multiple enterprise calling scenarios distributed ledgers would be more efficient than other strategies: one-to-many uses, legitimate spoofing, and rapid re-use of telephone numbers. Distributed ledger technology solves these use cases by making telephone number's "right to use" on a per call basis.

First Orion quickly saw the advantages of distributed ledgers in the telecommunications space and began working with ATIS and the other participating vendors to create a proof-of-concept environment to validate key aspects of the technology and provide an effective industry demonstration.

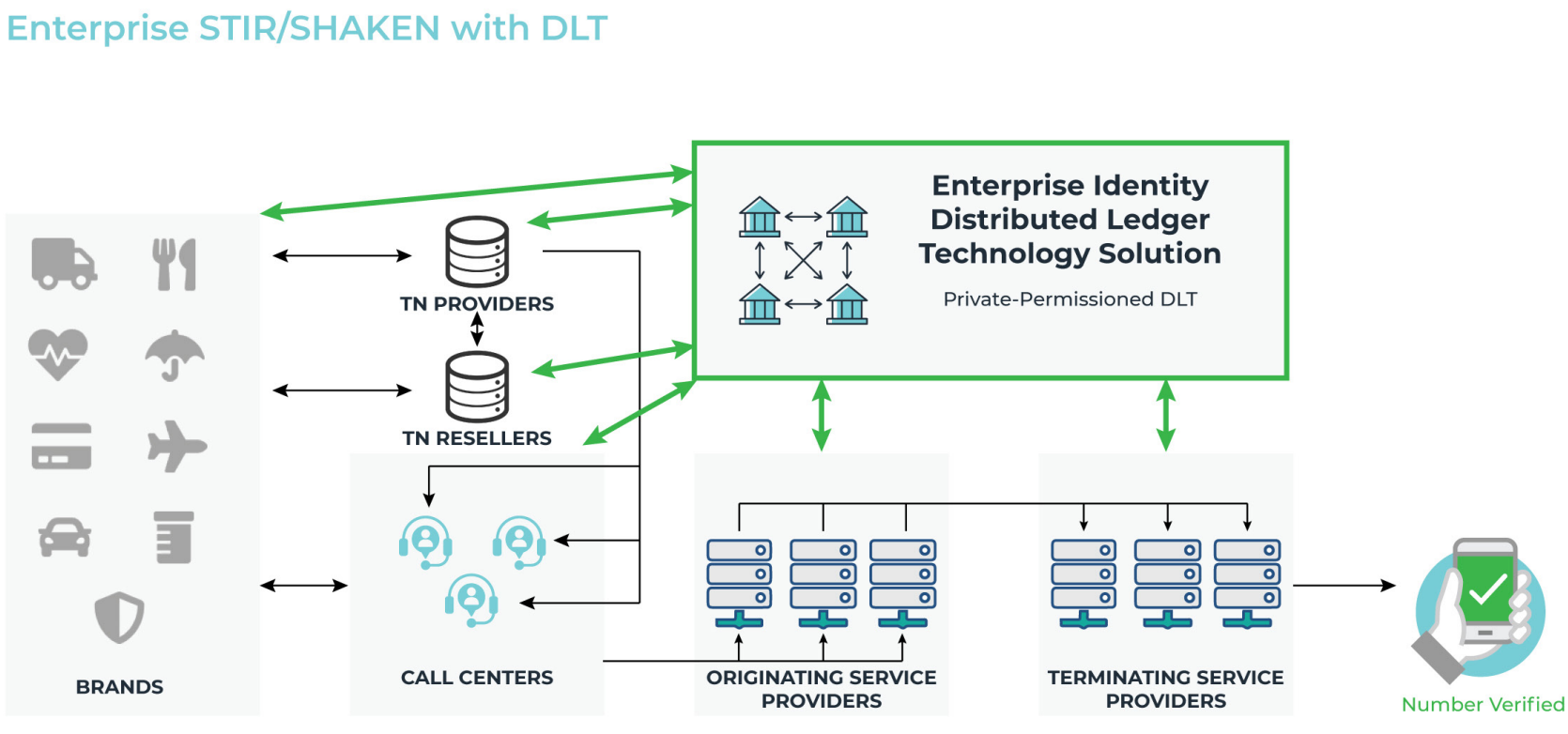


FIGURE 2

8 https://access.atis.org/apps/group_public/download.php/50787/ATIS-I-0000076.pdf

DLT provides business enterprise callers with an immutable digital identifier recorded on a distributed permissioned ledger, using cryptographic public/private key credentials to verify and authenticate proof of their enterprise identity.

In order for a business to be KYC-vetted they must:

1. verify they are who they say they are,
2. authorize use of their enterprise digital identity on the distributed ledger, and
3. prove their identity when being onboarded by a service provider or being assigned a telephone number's "right to use".

Once KYC-vetted, the business' enterprise identity can be assigned a telephone number "right to use", indicating the intended purpose of the calls being placed from the number.

The telephone number "right to use" is recorded on the DLT network, ensuring all stakeholders of the network instantly know who has the right to place a call using the telephone number and for what reason. Regardless of whether the phone number is from a service provider or reseller, and regardless of where the call originates, it can now be attested to the owning enterprise.

Furthermore, a business may use a 3rd party call center entity to place calls on their behalf without verification issues. The business may delegate the telephone number "right to use" to the call center with DLT, so any OSP will know the call center has the right to place calls using the specific telephone number on behalf of the business.

With the call authenticated, enhanced caller information such as brand name and intended purpose of the call can be presented, so the consumer can rest assured who is calling them and the purpose of the call before answering. Enhanced caller information with "Branded Phone Calls" is crucial for businesses looking beyond base STIR/SHAKEN authentication to an Enterprise STIR/SHAKEN identity. With DLT approach, businesses can increase brand awareness and maintain trust with their customers.

PRIVATE VS. PUBLIC DISTRIBUTED LEDGERS

Distributed ledgers can be public (permissionless), or private (permissioned). The distinction between the two is much like the Internet versus an intranet.

An enterprise identity network uses a permissioned distributed ledger in order to:

- Limit the ability to connect and transact to a set of users who have been given permission and issued cryptographic credentials by a centralized authority.
- Restrict access to view records (or even fields within them) to specific users based on their role.
- Ensure user updates to the data stored on the ledger occur based on rules set forth by the trust authority administering the ledger.

Whereas permissionless ledgers (e.g., Bitcoin):

- Allow anyone to transact on the ledger and hold identical copies of the full ledger.
- Allow anyone to access the network and view all transactions.
- Allow updates to the data stored on the ledger based on consensus reached by a number of nodes.

While most STIR/SHAKEN solutions focus around service providers, DLT provides immediate value for enterprises who want to ensure their telephone numbers are authenticated and verified, guaranteeing they connect with their consumers in a more trusted way.

The First Orion Proof of Concept Innovation Lab

First Orion collaborated with ATIS in a proof-of-concept initiative along with other working group members to deliver a fully integrated, minimal viable solution to validate key aspects of the approach and demonstrate to the industry its effectiveness, use, and ease of integration. The goal was to help advance the DLT solution and validate an effective blueprint for a real-world STIR/SHAKEN distributed ledger solution implementation.

First Orion implemented a proof-of-concept innovation lab environment to provide an end-to-end session initiation protocol (SIP) call validation infrastructure to authenticate caller identity and telephone number “right to use” at each stage in the SIP call process. The proof of concept validated the process during each step - from the business enterprise caller, through OSP and TSP - to verify consumer call scenarios.

A decentralized enterprise identity was created while having a non-repudiated and immutable record of it authenticated/vetted by representations of the real-world STIR/SHAKEN ecosystem. Elements of the enterprise identity were then used to represent the various aspects of the enterprise, such as its outbound telephone numbers for phone calls.

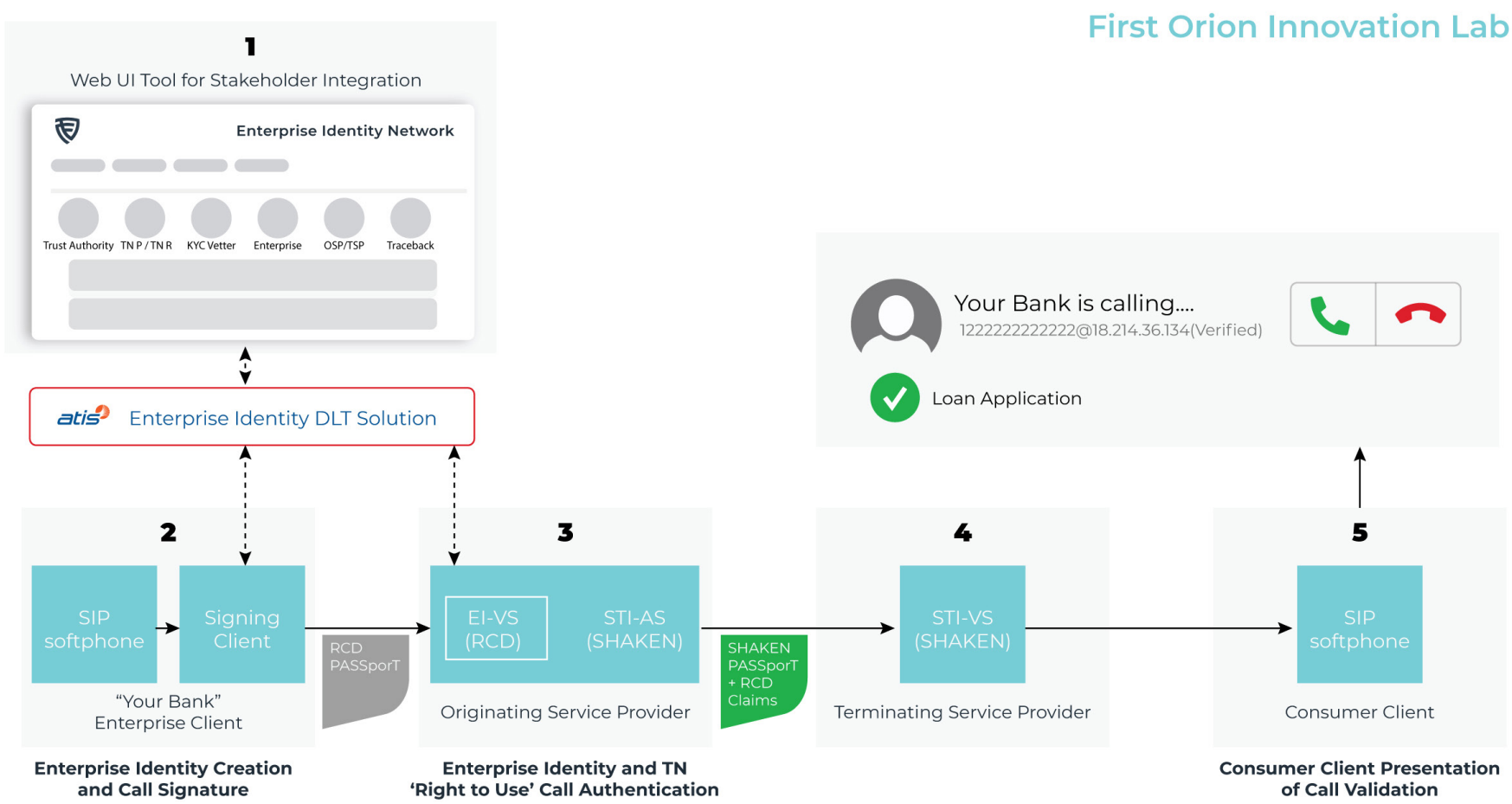


FIGURE 3

Illustrates key components of the ecosystem created in the First Orion Proof of Concept Innovation Lab

1. **Stakeholder User Interface:** Provided a user interface enabling each of the enterprise identity actors to perform operations on the ledger to KYC verify and authenticate enterprise identities, granting the telephone number "right to use" across the ecosystem of actors.

2. **Enterprise Identity SIP Client:** Implemented an "Enterprise SIP Client" that can register and create an enterprise identity on the distributed ledger, generating a digital identity with a corresponding private/public key pair. Provided a SIP signing function, using the private key to sign the identity header of outgoing SIP calls.

3. **Enhanced STI-AS Distributed Ledger Technology Verification Function:** Implemented a distributed ledger technologies verification function typically found within an OSP to interface with the DLT solution to verify the SIP identity header signature, using the public key registered on the ledger for the callers' enterprise identity. The function ensures the enterprise identity is KYC-vetted and authorized to be "trusted" including the enterprise "brand" name. If so, the telephone number being used has the telephone number's "right to use" signed by the authorized TN Provider. With the authenticated enterprise identity and telephone number's "right to use". The STI-AS then applies the appropriate SHAKEN attestation and signing of the SIP call after creating the claims for the base PASSPorT as well as additional Rich Call Data (RCD) claims. The RCD claims are used to pass through "Branded Phone Calls" with information regarding the enterprise "brand" name and the intended reason for the call.

4. **STI-VS:** The STI-VS performs verification of the SHAKEN-signed SIP identity header and converts the RCD data into SIP headers the B-party can display.

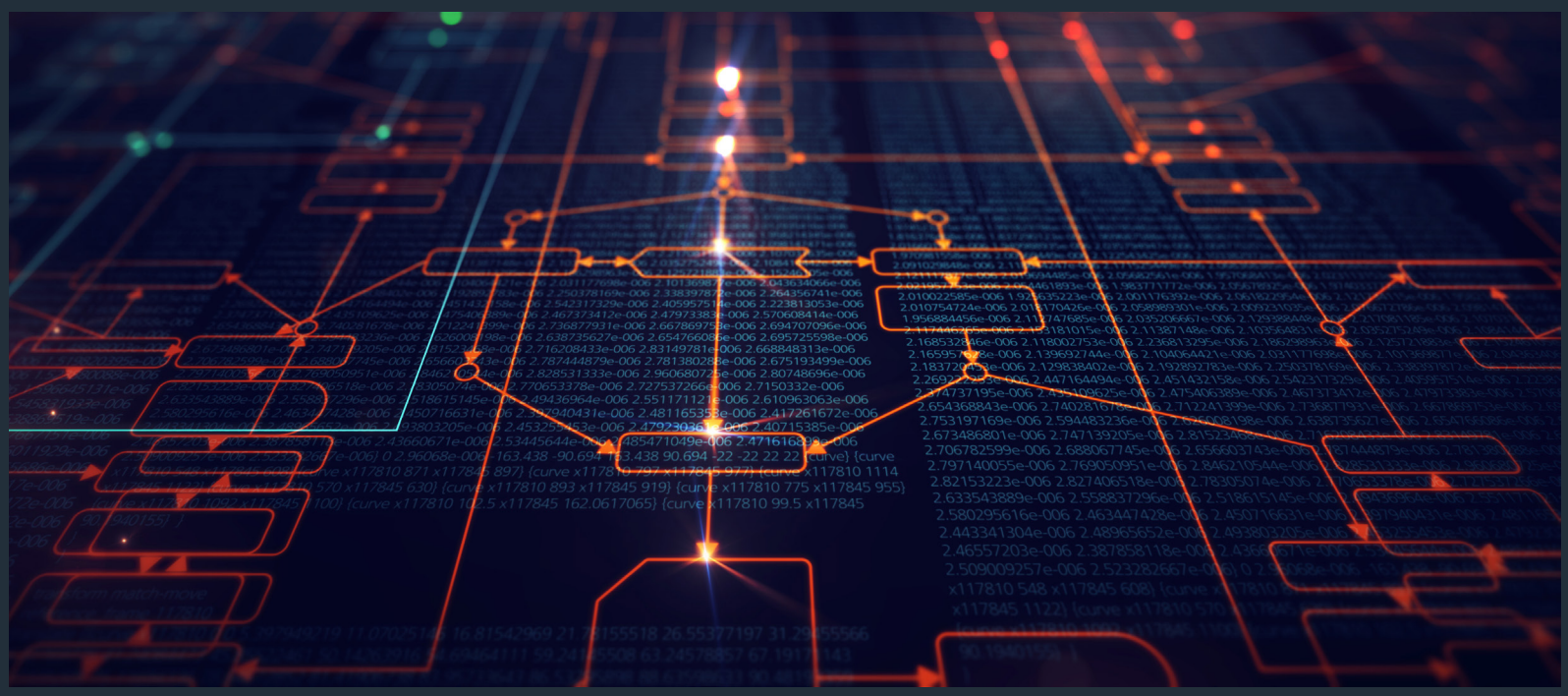
5. **Consumer SIP Client:** A SIP client is able to present the verified details of the caller to the call recipient. In the case of a fully verified call this will be the SHAKEN attestation presented as a check mark, the caller brand name (e.g. "Your Bank"), and the intended reason for the call (e.g. "Loan Application").

DLT Solution Validation

The First Orion Innovation Lab simulates the existing telecom ecosystem for VoIP calls and verifies the feasibility of implementing a DLT solution at scale. The solution offers many benefits and advantages when compared to other strategies, while using a different method for recording and verifying the source of truth for participating service providers.

The resulting infrastructure consists of a series of components providing the signaling network functionality for SIP-based call origination and termination:

- SIP-based A party UA with a SIP signing function
- SIP-based element representing an OSP STI-AS function, interfaced with an SP-KMS
- SIP-based element representing a TSP, complete with an STI-VS function
- SIP-based B party UE with enhanced caller presentation



Furthermore, the lab provided the requisite IP-based elements needed by the signaling nodes:

- An SP-KMS solution supporting STIR/SHAKEN including an SKS and STI-CR
- A bridging function within the SP-KMS providing access to the API layer for transacting on with DLT

In order to represent an “off-ledger” part of the solution, more specifically the business interaction between the entities already occurring today, the following auxiliary functions were added to the lab:

- A web-based user interface allowing full management of all processes for each actor within the model ecosystem
- An API layer middleware to allow SP-KMS to access the DLT solution hosted by another working group member via the API endpoints
- A set of APIs used by the web-interface to request processes such as telephone number request, KYC vetting, and others to take place
- A tracing and logging mechanism to demonstrate the under-the-covers mechanics of the ecosystem

Results and Learnings

First Orion's team has been pioneering the most advanced data, AI, ML, and computing solutions for our clients for years, so we immediately saw the benefit of using distributed ledger technologies for telecommunication use cases. A DLT model has potential value for legitimate enterprises, 3rd party calling entities, and of course telecom service providers who have a lot to gain from immutable, unique identifiers for enterprises and telephone numbers.

The First Orion Innovation Lab set out to further demonstrate that when applied to the STIR/SHAKEN problem domain, the DLT approach has some advantages over other approaches. A distributed ledger approach allows for specific use cases to be solved that are not always easily solved by other STIR/SHAKEN strategies.

Portable Enterprise KYC Vetting Efficiencies

Portable KYC vetting makes it easier for a business to use an existing KYC vetted and approved enterprise identity to be used with any other service providers for proof during onboarding, minimizing the friction for the enterprise and the carrier. This also means it is easier for entities providing telephone numbers to prove their identities when assigning them telephone numbers.

Reducing barriers to onboard new telephone numbers is especially important for mobile apps and marketplaces who might be using a pool of temporary numbers to make business calls (rapid re-use of telephone numbers use case). For instance, when drivers are placing phone calls they are able to use enterprise telephone numbers delegated to them for the purpose of performing their duties and distinctly differentiating from the telephone number of their personal device.

Flexible and Immutable Telephone Number with "Right to Use"

Not only does this mean everyone leveraging DLT solution knows enterprises are correctly being identified as having the proper authorized "right to use" for their numbers, but it will also indicate when phone number permissions have been revoked. An enterprise identity signed calls will be correctly verified even if the enterprise uses multiple call centers (internal, 3rd party, or both) or has remote call centers placing calls using local store/branch numbers (one-to-many uses and legitimate spoofing). Having these numbers labeled as "right to use" makes the calls verified with a checkmark and details of the caller to consumers.

Improved Efficacy of SHAKEN Attestation

Fulfilling the requirements set forth by the regulatory bodies and benefitting service providers, distributed ledger technology ensures a single source of truth determines the authenticity of calling enterprises using specific telephone numbers across all participating entities in the network. The identity of every phone number can be authenticated, and all calls can be traced back to their point of origin.

IMMEDIATE BENEFITS OF A DLT SOLUTION

Portable Enterprise KYC-vetting Efficiencies

- √ KYC-vetted once, then used by any entity within the DLT solution
- √ Lower barrier to entry for onboarding and proving telephone number ownership
- √ Accessible by TN Providers and TN Resellers when assigning "right to use"

Flexible and Immutable Telephone Number "Right to Use"

- √ Proof of telephone number "right to use" exists on the enterprise identity distributed ledger
- √ Proof of 3rd party delegated telephone number "right to use" on behalf of a business
- √ Immediate record for any network participant once telephone number "right to use" is assigned, delegated, or revoked

Improved Efficacy of SHAKEN Attestation

- √ A single source of truth for the authenticity of a calling business and their right to originate calls from the telephone number being used
- √ All OSPs connected to the DLT solution can authenticate the true identity of the business placing and signing a call

DLT Addresses the Enterprise Gap in STIR/SHAKEN

Unlike other approaches to solving the attestation gap, the DLT option makes it easier for enterprises of any size to have their calls authenticated and verified. Regardless of whether enterprise calls are originated internally or from 3rd party call centers, DLT benefits everyone involved.

As demonstrated through First Orion's proof of concept, distributed ledgers provide many advantages over traditional database and public key infrastructures when managing telephone number allocations to trusted enterprises. Distributed ledger technology ensures stakeholders always have access to a trusted single source of truth about the status of an enterprise's identity. Furthermore, using the DLT solution ensures all participants of the ecosystem know the "right to use" credentials for a telephone number.

Distributed ledger technology is a proven, robust, scalable, and secure technology that is transforming the way businesses securely manage identity information across global telecom, financial services, and governments. First Orion believes DLT is a viable solution for providing trusted enterprise caller identities and maximizes the full potential of SHAKEN across a broader set of enterprise scenarios. DLT would fill the gap for verifying enterprise identities across all stakeholders in the network, enabling the implementation of Enterprise STIR/SHAKEN solutions.

First Orion has been pioneering solutions for STIR/SHAKEN since it was first mandated, and we continue to innovate in this space. We have helped service providers, call centers, carriers, enterprises, and 3rd party vendors all understand how to make sure they are in compliance while doing everything we can to bring value to their customers. Our world-class team of technologists and data scientists are dedicated to call transparency and helping customers trust their phone calls again.

Although additional steps need to be taken and industry stakeholders must come together, this complex enterprise problem can be solved with DLT. This technology is available now and leading the industry into the future. First Orion continues to work closely with industry partners and through industry forums furthering approaches such as Delegate Certificates, Rich Call Data, and Central Telephone Number Registry to successfully bring enterprises and call centers into the SHAKEN ecosystem.

Next Steps for OSPs, Contact Centers, and Enterprises

First Orion offers a number of call protection and call enhancement solutions for enterprises. For more information about STIR/SHAKEN and Enterprise calling options or to request a consultation with our team of experts, contact us at info@firstorion.com

By First Orion
Key Contributors:
Mark Himelfarb, CTO, First Orion
Ian Deakin, Principal Technologist, ATIS

FIRSTORION

520 MAIN STREET, NORTH LITTLE ROCK, 72114

P: +1-501-358-4061 | **W:** FIRSTORION.COM | **E:** info@firstorion.com