Enterprise Identity on Distributed Ledger for Authenticated Caller Use Cases

ATIS-I-0000076 | December 2019
Abstract

This document provides a description for using distributed ledger technology to provide enterprise identity verification to authenticate originating party caller information in IP communication networks. It describes problems associated with the attestation of a telephone number (TN) due to enterprise multi-homing with originating service providers that are not the allocation provider of the TN, within IP communication networks.
As a leading technology and solutions development organization, the Alliance for Telecommunications Industry Solutions (ATIS) brings together the top global ICT companies to advance the industry’s business priorities. ATIS’ 150 member companies are currently working to address 5G, cybersecurity, robocall mitigation, IoT, artificial intelligence-enabled networks, the all-IP transition, network functions virtualization, smart cities, emergency services, network evolution, quality of service, billing support, operations, and much more. These priorities follow a fast-track development lifecycle – from design and innovation through standards, specifications, requirements, business use cases, software toolkits, open source solutions, and interoperability testing.

ATIS is accredited by the American National Standards Institute (ANSI). ATIS is the North American Organizational Partner for the 3rd Generation Partnership Project (3GPP), a founding Partner of the oneM2M global initiative, a member of the International Telecommunication Union (ITU), and a member of the Inter-American Telecommunication Commission (CITEL). For more information, visit www.atis.org.
Notice of Disclaimer and Limitation of Liability

The information provided in this document is directed solely to professionals who have the appropriate degree of experience to understand and interpret its contents in accordance with generally accepted engineering or other professional standards and applicable regulations. No recommendation as to products or vendors is made or should be implied.

NO REPRESENTATION OR WARRANTY IS MADE THAT THE INFORMATION IS TECHNICALLY ACCURATE OR SUFFICIENT OR CONFORMS TO ANY STATUTE, GOVERNMENTAL RULE OR REGULATION, AND FURTHER, NO REPRESENTATION OR WARRANTY IS MADE OF MERCHANTABILITY OR FITNESS FOR ANY PARTICULAR PURPOSE OR AGAINST INFRINGEMENT OF INTELLECTUAL PROPERTY RIGHTS. ATIS SHALL NOT BE LIABLE, BEYOND THE AMOUNT OF ANY SUM RECEIVED IN PAYMENT BY ATIS FOR THIS DOCUMENT, AND IN NO EVENT SHALL ATIS BE LIABLE FOR LOST PROFITS OR OTHER INCIDENTAL OR CONSEQUENTIAL DAMAGES. ATIS EXPRESSLY ADVISES THAT ANY AND ALL USE OF OR RELIANCE UPON THE INFORMATION PROVIDED IN THIS DOCUMENT IS AT THE RISK OF THE USER.

NOTE - The user’s attention is called to the possibility that compliance with this standard may require use of an invention covered by patent rights. By publication of this standard, no position is taken with respect to whether use of an invention covered by patent rights will be required, and if any such use is required no position is taken regarding the validity of this claim or any patent rights in connection therewith. Please refer to https://www.atis.org/01_legal/patent-assurances/ to determine if any statement has been filed by a patent holder indicating a willingness to grant a license either without compensation or on reasonable and non-discriminatory terms and conditions to applicants desiring to obtain a license.
# Contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Pages</th>
</tr>
</thead>
<tbody>
<tr>
<td>ABSTRACT</td>
<td>2</td>
</tr>
<tr>
<td>FOREWORD</td>
<td>3</td>
</tr>
<tr>
<td>01: INTRODUCTION</td>
<td>9</td>
</tr>
<tr>
<td>1.1: PROBLEM STATEMENT</td>
<td>9</td>
</tr>
<tr>
<td>02: DISTRIBUTED LEDGER TECHNOLOGY</td>
<td>12</td>
</tr>
<tr>
<td>03: ENTERPRISE IDENTITY DISTRIBUTED LEDGER PROJECT GOALS</td>
<td>14</td>
</tr>
<tr>
<td>3.1: GOAL #1: GOVERNANCE MODEL FOR THE DL SOLUTION</td>
<td>15</td>
</tr>
<tr>
<td>3.2: GOAL #2: ENTERPRISE KYC VETTING AND IDENTITY ASSIGNMENT</td>
<td>15</td>
</tr>
<tr>
<td>3.3: GOAL #3: ALLOCATING A TN TO A VETTED ENTERPRISE</td>
<td>16</td>
</tr>
<tr>
<td>3.4: GOAL #4: ENABLE ANY ORIGINATING SERVICE PROVIDER TO ATTEST A VETTED ENTERPRISE CALL</td>
<td>16</td>
</tr>
<tr>
<td>3.5: GOAL #5: VERIFICATION OF THE TN ON THE DL AT CALL TERMINATION</td>
<td>16</td>
</tr>
<tr>
<td>3.6: GOAL #6: ‘BRAND’ ENTERPRISE DELEGATES A TN TO A BPO ENTERPRISE</td>
<td>16</td>
</tr>
<tr>
<td>3.7: GOAL #7: THE ORIGINATING SERVICE PROVIDER, CAN VERIFY THE TN WHEN USED BY A DELEGATED ‘TRUSTED’ ENTERPRISE</td>
<td>17</td>
</tr>
<tr>
<td>04: DEFINITIONS OF THE ACTORS AND THEIR ROLES IN THE SERVICE</td>
<td>18</td>
</tr>
<tr>
<td>4.1: ACTORS AND ROLES</td>
<td>18</td>
</tr>
<tr>
<td>4.2: ASSUMPTIONS</td>
<td>18</td>
</tr>
<tr>
<td>05: USER STORIES</td>
<td>22</td>
</tr>
<tr>
<td>5.1: GOVERNANCE AUTHORITY</td>
<td>22</td>
</tr>
<tr>
<td>5.2: KYC VETTER</td>
<td>23</td>
</tr>
<tr>
<td>5.3: TN PROVIDER</td>
<td>23</td>
</tr>
<tr>
<td>5.4: ‘BRAND’ ENTERPRISE</td>
<td>24</td>
</tr>
<tr>
<td>5.5: ‘BPO’ ENTERPRISE</td>
<td>25</td>
</tr>
<tr>
<td>5.6: ORIGINATING SERVICE PROVIDER</td>
<td>26</td>
</tr>
<tr>
<td>5.7: TERMINATING SERVICE PROVIDER</td>
<td>27</td>
</tr>
<tr>
<td>06: GOVERNANCE</td>
<td>28</td>
</tr>
</tbody>
</table>
6.1: NETWORK GOVERNANCE ............................................................... 31
  6.1.1: QUALIFICATIONS FOR NODE HOSTING ................................. 31
  6.1.2: IDENTITY MANAGEMENT OF NODES ..................................... 31
  6.1.3: QUALIFICATIONS FOR KYC VETTER TO ASSIGN ACCOUNTS. . . . 31
  6.1.4: TN PROVIDER ACCOUNT MANAGEMENT AND ADMIN. ................ 31
  6.1.5: TN DATA RIGHTS, RESPONSIBILITIES, TERMS OF USE. .......... 31
  6.1.6: NETWORK TRANSACTION VALIDATION ..................................... 31
  6.1.7: TN WITHDRAWAL FROM ENTERPRISE ACCOUNT ....................... 32
  6.1.8: ACCOUNT REPUTATION AND REVOCATION ............................ 32
  6.1.9: NODE REPUTATION AND REVOCATION .................................... 32
  6.1.10: DISPUTE RESOLUTION ...................................................... 32

07: IDENTITY MANAGEMENT ............................................................. 33
  7.1: DISTRIBUTED LEDGER NODE IDENTITIES ..................................... 33
  7.2: ACTOR ACCOUNT IDENTITIES ................................................. 34
    7.2.1: BLOCKCHAIN ACCOUNT IDENTITIES OVERVIEW ..................... 34
    7.2.2: ENTERPRISE IDENTITY DL ACCOUNT IDENTITIES .................... 35
      7.2.2.1: ‘BRAND’ & ‘BPO’ ENTERPRISE IDENTITY ......................... 35
      7.2.2.2: TN PROVIDER IDENTITY ............................................. 36

08: DATA MODEL ............................................................................. 37

09: SOLUTION – FUNCTIONAL ARCHITECTURE AND FLOWS ..................... 39
  9.1: FUNCTIONAL FLOWS ............................................................. 39
  9.2: GOVERNANCE AUTHORITY FLOWS ......................................... 39
    9.2.1: NEW DL NODE CREATION AND AUTHORIZATION: EIDL-001 ....... 39
    9.2.2: NEW TN PROVIDER ACCOUNT: EIDL-005 ............................ 40
    9.2.3: REVOCATION OF A BAD ACTOR NODE: EIDL-002 ................ 41
  9.3: ENTERPRISE FLOWS ............................................................. 42
    9.3.1: ENTERPRISE REGISTRATION WITH A KYC VETTER: EIDL-007,EIDL-011 .... 42
    9.3.2: ‘BRAND’ ENTERPRISE – ATTAIN TN: EIDL-008 .................... 42
    9.3.3: DELEGATE A TN TO A ‘BPO’ ENTERPRISE: EIDL-010 .......... 43
  9.4: SERVICE PROVIDER FLOWS ................................................... 44
    9.4.1: SIGNING AND AUTHENTICATING AN ORIGINATING CALL: EIDL-009,EIDL-012,EKYC-014 ... 44
    9.4.2: OSP ATTESTING OF THE ORIGINATING CALL: EIDL-015 .......... 45
    9.4.3: TSP ATTESTING OF THE ORIGINATING CALL: EIDL-017 .......... 45
Introduction

The objective of the ATIS DLT project is to validate key aspects of distributed ledger technology as it applies to real-world challenges facing today’s communications industry. Through the analysis of a specific use case, it will assess if the unique characteristics of DLT can be a game-changer by enabling innovative solutions to difficult problems experienced today in the communications space.

The basic idea behind the “enterprise identity use case” that the focus group has identified is to study how to leverage a distributed ledger to provide communications service providers with a better mechanism to validate that calling parties are entitled to use the telephone number (TN) that they are using. This is especially difficult – and valuable – in complex calling scenarios. One example is a call center that’s originating calls on behalf of an enterprise, using third-party calling platforms and multiple originating service providers (OSPs), for a short-term calling campaign such as a product recall. This real-world scenario is not adequately addressed by any solution today.

1.1 Problem Statement

The Federal Trade Commission (FTC) and Federal Communications Commission (FCC) regularly cite “unwanted and illegal robocalls” as their No. 1 complaint category. Caller ID spoofing increases the harm from these unwanted calls. The ATIS-SIP Forum IP-NNI Task Force developed a specification designed specifically to mitigate unwanted robocalls by reducing the impact of caller ID spoofing. This specification, SHAKEN (Signature-based Handling of Asserted information using tokens), is based on the STIR (Secure Telephone Identity Revisited) protocol developed by IETF. SHAKEN allows the OSP to generate a digital signature, which securely signals the terminating service provider (TSP) that the caller has the right to use that phone number.

When a call is originated, the OSP will use the originating caller ID to create a digital signature, or token, that will accompany the call as it is being completed. At call termination, the TSP verifies that nothing was tampered with and ensures that the call came from an entity that has a legitimate right to use that number. The verification from SHAKEN can be displayed directly to the user or fed into a “call-blocking app,” which provides a rating system that essentially identifies calls as good, questionable or likely fraudulent. The call-blocking app can take
action, on behalf of the user, to stop unwanted calls from getting through.

SHAKEN was never intended to be a complete solution for addressing the robocalling problem. It is an important tool in a multi-layered approach. What SHAKEN specifically does is to provide “full attestation.” In the SHAKEN framework, ATIS 1000074¹, Full Attestation is defined as follows:

**A. Full Attestation:** The signing provider shall satisfy all of the following conditions:

1. Is responsible for the origination of the call onto the IP-based service provider voice network.
2. Has a direct, authenticated relationship with the customer and can identify the customer.
3. Has established a verified association with the TN used for the call.

Many scenarios today will not satisfy these conditions and will therefore receive “partial attestation” (Attestation B) at most. Third-party call centers are a great example of a situation that will not allow full attestation by SHAKEN today, nor in any planned evolution of the specification.

SHAKEN does not define what service providers should do with the delivery of a call. This is governed by existing regulations that generally (with a few exceptions) require that telephone service providers complete all calls. Note that this does not apply to call-blocking apps, which allow the end user to opt-in and have the app screen, characterize and potentially block, calls on the user’s behalf. In June 2019, the FCC issued a Declaratory Ruling allowing service providers to apply call blocking at the network level on an opt-out basis.²

SHAKEN does not characterize calls, and therefore it cannot identify calls correctly or incorrectly. SHAKEN merely creates a digital signature at the origin with the information the OSP knows about the call (customer, and potentially their right to use the number). It then sends this signature to the TSP, which verifies that no one has tampered with the information. SHAKEN does not identify calls as spam. Call-blocking apps are the entity that tries to identify the call intent, and as a result, sometimes mislabel legitimate calls as spam.

Robocalls can sometimes be quite valuable to customers in communicating important, need-to-know information that otherwise may not have been received in real time. A few examples include flight or school cancellations, appointment reminders and credit card fraud alerts. However, current analytics deployments can label these legal callers as FRAUD/SCAM.

As previously mentioned, these typical call scenarios are complex. An enterprise will contract with a call center provider, which will:

- Use another vendor (or vendors) for the calling platform.
- Obtain phone numbers for the campaign from a number reseller(s).
- Originate the calls using multiple OSPs (some examples actually use a

---

¹ [https://www.atis.org/sti-qa/resources/docs/ATIS-1000074.pdf](https://www.atis.org/sti-qa/resources/docs/ATIS-1000074.pdf)

dozen OSPs) based on time of day and other factors to minimize costs. With this scenario, the OSP has absolutely no confidence in the phone number in the caller ID, or anything else about the call and can only provide partial attestation. A solution is needed to enable an OSP to associate the calling number of a call with the verified Enterprise identity, which is responsible for, or sponsoring the content of, the call.

FIGURE 1.1 PROBLEM TO ATTEST A TELEPHONE NUMBER
Distributed Ledger Technology

Blockchain/distributed ledger technologies (DLT) are currently being used to power and secure a cryptocurrency market worth over US$250 billion (as of June 2019).3

The ledger is the core storage for the information, which can include cryptocurrency transactions, property ownership, proof of existence and more. The original design intent of the underlying Bitcoin blockchain was to give full transparency to all transactions and make them time ordered and fixed once entered into the ledger. The term “blockchain” originates from this process, where a number of transactions are combined into a block which is added to a chain of existing blocks in a way that creates a strong (cryptographic) signature of all chained blocks.

The foundation for how blockchain cryptography functions uses public-private key pairs, also known as “asymmetric cryptography.” The system uses key pairs to eliminate the need for third-party verification. Private keys, which are used to sign messages, are known only by the owner, while public keys can be distributed to anyone. The public key is used to verify the received message is from the holder of a specific private key. The private key can decrypt the message that was originally encrypted with the public key. This method eliminates the need for personal data to be used to provide verified and authenticated access.

The blockchain ledger by nature enables recording of information, messages, transaction and data, all of which cannot be changed once committed to the ledger. This mechanism provides a tamper-resistant record that can lock in variables that authenticate identity, making it consistently accurate even with the passage of time. This tamper-resistant record reduces the need for repetition and constant verification and authentication across various platforms. Unaltered information on the blockchain is what makes the concept of a universal blockchain ID incredibly sound, reducing the need for sprawling data stores and protects against identity theft. There is no need to repeatedly enter personal information when we can securely authenticate identity once.

A know your customer (KYC) process can benefit from the same approach. With distributed ledgers, a person’s or enterprise’s KYC process can be expedited because everyone on the blockchain network can affirm the new entrant’s identity. Blockchain technology’s security is a major reason why blockchain is

3 https://coinmarketcap.com/charts/
renowned globally. Customers can be assured that their information is secured on an organization’s ledger using cryptography to provide enhanced security. Once an enterprise has been vetted by a KYC process and has been granted permission to access the blockchain via a particular account (public-private key pair), all members of the network can rely on this identity for all subsequent transactions.

The distribution is where the complexity is added. The original Bitcoin blockchain was designed to store transactions with no trust requirements, which effectively means many distributed copies of the ledger are required. Truth is determined by majority vote, and all ledgers are kept up to date through a consensus mechanism. Now if this consensus mechanism were trivial, it would be possible to subvert truth by creating a 51 percent vote in favor of your desired outcome (Sybil Attack). Here is where consensus mechanisms come into play. For example, in Bitcoin’s proof of work (PoW), the cost of performing the validation process is kept high, requiring significant power and computing resources where the effort required to subvert the truth is cost prohibitive. Other consensus techniques can be used that require the validators to vote through an incentivized “proof of stake” algorithm, where the validator submits a large financial stake to the community. If they subvert the trust, they lose the stake. But if they’re truthful, they’ll receive a reward.

Smart contracts are computer programs that directly control the transfer of digital assets between parties under certain conditions. A smart contract defines the rules and penalties related to an agreement in the same way that a traditional contract does. A smart contract can also automatically enforce those obligations. DLTs/blockchains are ideal for storing smart contracts because of the technology’s immutability.

A non-fungible token (NFT) is essentially a unique representation of an asset or good in the form of a virtual token. NFTs are used to create verifiable digital scarcity. They are used in several specific applications that require unique digital items such as collectibles, game props, digital ticketing, identity authentication and digital certificates, which are immutably stored on a distributed ledger/blockchain.

**DLT and its cryptographic principles can be applied to provide a verified enterprise identity for all communications service providers to use to attest originating TNs. This enterprise identification and authentication process could prove key to greatly enhancing capability for STIR/SHAKEN.**
Enterprise Identity Distributed Ledger Project Goals

The objective of this project is to address the current issues identified within the problem statement described in section 1 of this document. Specifically, the scope of the project is to implement a technical solution that utilizes DLT and its capabilities to address these problems.

A number of specific goals have been identified for this project in the ATIS DLT Project group. The following diagrams illustrate the key goals.

FIGURE 3.1 KEY GOALS FOR ENTERPRISE IDENTITY ON DISTRIBUTED LEDGER

FIGURE 3.2 KEY GOALS FOR ENTERPRISE IDENTITY – DELEGATED TN
3.1 Goal No. 1: Governance Model for the Distributed Ledger Solution

The enterprise identity distributed ledger solution will require governance to control the service. This solution also will need to consider how aspects of the service are supported by a decentralized organization, including:

- **DL governance, central authority or decentralized organization**
  - What aspects of the solution will be controlled by a central governing authority and how will this be enforced on the DL actors?
  - If the project allows for multiple governing entities (decentralized), what controls are required to ensure that there is a consensus across the entities?
  - Which actors will have access to the service, under what terms and how will they be policed?

- **Funding governance**
  - Under what economic model will the service be funded to support the operations of the network?

- **Project governance**
  - Who will make the decisions on governance, changes, and priorities?
  - How will decisions about changes be made and agreed amongst the community?
  - How will agreement be reached on priorities?

- **Operational governance**
  - Who will maintain and make updates and fixes to the network?

3.2 Goal No. 2: Enterprise KYC Vetting and Identity Assignment

The key aspect of this project is predicated upon a trusted enterprise identity that can be used to authenticate an enterprise, when allocating a TN and attesting to an originating a call through any OSP or TSP.

KYC is the process of a business verifying the identity of its clients and assessing their suitability, along with the potential risks of illegal intentions towards the business relationship, regulation and governance of the activity. An enterprise actor will provide detailed due diligence information to be verified by a "KYC Vetter" according to the rules of the governance authority.

There are two types of enterprise actor roles:

1. The brand enterprise, which is the company representing the content of the call. An example is Toyota informing customers of a recall.

2. The business processing outsourcing (BPO) enterprise, which performs the outgoing calls on behalf of the brand actor. The BPO actor will make and sign the outgoing calls.

Once an enterprise actor has been KYC vetted, the enterprise is allocated a digital identity. This digital identity is used to authenticate the enterprise when transacting with other actors on the distributed ledger. It must be secure,
allowing only the authorized enterprise to be authenticated with this digital identity and not to enable spoofing by an unauthorized party.

3.3 Goal No. 3: Allocating a TN to a Vetted Enterprise

Once an enterprise has been KYC vetted and has an identity on the distributed ledger, it can request the allocation of a TN from a TN provider indicating the purpose and intended use of the number. Note that for the purpose of this document, TN provider can be a TN service provider (TNSP) or TN reseller.

The TN provider will be able to verify and authenticate the enterprise’s digital identity from the distributed ledger before allocating the number to the enterprise. When approved, the TN provider allocates the number to the enterprise identity on the distributed ledger, along with the details of the intended use and the terms and conditions of its use. These terms and conditions can be incorporated into a smart contract to ensure that all actors accessing the distributed ledger can verify that the TN is being used by the legitimate assignee and in accordance with the agreed terms and purpose.

3.4 Goal No. 4: Enable Any Originating Service Provider to Attest a Vetted Enterprise Call

When the vetted enterprise places an originating call, the SIP header is encoded with information to convey proof of the enterprise identity and that it is the legitimate assignee of the number. This enables any originating service provider to authenticate from the distributed ledger.

The proof information proof could be a digital signature, token or hash of specific attributes of the SIP call. It is suggested that this proof be created by using an asymmetric key pair native to the distributed ledger. The enterprise will sign the call using its private key, enabling any originating service provider to authenticate the signature using the public key on the distributed ledger. If the proof of identity is valid for the enterprise and the number being used, the originating service provider can attest to the call for STIR/SHAKEN.

3.5 Goal No. 5: Verification of the TN on the DL at Call Termination

When a STIR/SHAKEN call is received at a TSP, this is authenticated to be from the OSP according to the STIR/SHAKEN specification. The TSP can query the distributed ledger regarding the originating number to extract the details of the originating enterprise, the call content and its intended use. These details can be used to enable the TSP to perform analytics on these calls and establish if they are adhering to the rules and terms of use within the smart contract.

3.6 Goal No. 6: Brand Enterprise Delegates a TN to a BPO Enterprise

A brand enterprise may not always be the originator of the call. Instead, it may
use a BPO enterprise to perform the outgoing calls on its behalf. These outgoing calls could be performed in one of two ways:

- The BPO enterprise obtains the number from the TN provider on behalf of the brand and is allocated the number as per goal No. 2.
- The brand is able to delegate its allocated TN to a BPO to perform the outgoing calls according to the rules and terms of the smart contract.

If the second way is used, a BPO enterprise must be vetted as defined by goal No. 2 to be able to perform delegated calls on behalf of the brand enterprise. The brand enterprise can delegate a number by updating the information on the distributed ledger relating to the allocated TN. This allows all actors on the ledger to know that the BPO identity is now the originating party for the number. Considerations for a single smart contract to identify these two scenarios could include the following attributes/fields:

- “Provider” identifies the TN provider that manages this TN.
- “Assignee” identifies the enterprise and is set once the TN has been allocated to an enterprise by a provider. This is set by the provider.
- “Delegate” identifies the enterprise to which the TN has been delegated or is null if not delegated. This is set by the assignee.

3.7 Goal No. 7: The OSP can Verify the TN When Used by a Delegated Trusted Enterprise

Using the same mechanism as goal No. 4, the OSP can use the distributed ledger to authenticate the proof of the originating call and identify that the BPO identity is authorized to originate calls from the delegated number.
Definitions of the Actors and Their Roles in the Service

The enterprise identity service on the distributed ledger has a number of actors that play a role. The following section describes these actors and their roles.

4.1 Actors and Roles

The enterprise identity service has the following actors defined. Each actor has a specific role in participating in the delivery of the service.

- **Governance Authority**
  - Defines the framework and properties of the network.
  - Identifies and approves the technology and the implementer.
  - Identifies and approves trusted actors including the KYC veters, TN providers, OSPs and TSPs.
  - Identifies and authenticate nodes on the distributed ledger.
  - Defines the mechanism to police the actors operating a node of the distributed ledger to ensure trust across the network. This includes how accounts and transactions are verified.

- **Enterprise Identity Allocation Actors**
  - **KYC Vetter**
    - Is a trusted actor managed by the governance authority to perform verification service according the rules and agreements of the enterprise identity service.
- Vets and verifies enterprise actors based on the defined KYC policies (out of scope for PoC).
- Provides a qualified enterprise identity to be used across the system.
- Custodian for the enterprise identity (private key)

**Brand Enterprise**
- Is the enterprise that is communicating the content to the called parties.
- Represents the intent and purpose of the contact to the called parties.
- Requests the use of a TN to deliver the indented content/intent.
- Originates the calls using the assigned TN.
- Delegates the use of the assigned TN for a BPO enterprise to be the originator of the calls.

**BPO Enterprise**
- Originates calls on behalf of a brand enterprise for a delegated TN.

**Service Provider Actors**

- **TN Provider**
  - Verifies the enterprise identity requesting a TN.
  - Provides and provisions TNs to a vetted enterprise according to its intended use.

- **OSP**
  - Provides originating network for the call.
  - Verifies the call originator identity and the authority to use the TN.
  - Signs calls with STIR/SHAKEN.

- **TSP**
  - Provides the terminating network for the call.
  - Validates the STIR/SHAKEN token.
  - Checks the call intent and content type to filter for blocking unwanted calls.

- **Called Party**
  - Receives calls verified and screened by the enterprise identity service.

4.2 Assumptions

For the enterprise identity PoC, the following assumptions are made regarding each actor and its role.

- **Governance Authority**
  - For the PoC, the governance authority is a single entity.
  - The governance authority function must be able to support multiple Trust Authorities to support a global solution.
  - Processes the requests from network contributors and authorizes their node identities.
• **Enterprise Identity Allocation Actors**
  
  › **KYC Vetter**
  - Is verified, authorized and policed by the governance authority to perform the vetting function.
  - Can provide secure safe storage for an enterprise’s private keys (custodian).
  - Is a contributory node of the distributed ledger network.
  
  › **Brand Enterprise**
  - Provides identity information for the purpose of being KYC vetted (out of scope for the POC).
  > Example would be proof of business name and address.
  - Has the ability to provide safe storage of a private key.
  - Has the ability to sign originating calls with the private key.
  
  › **BPO Enterprise**
  - Provides identity information for the purpose of being KYC vetted (out of scope for the POC).
  > Example would be proof of business name and address.
  - Has the ability to provide safe storage a private key.
  - Has the ability to sign originating calls with the private key.

• **Service Provider Actors**
  
  › **TN Provider**
  - Is verified, authorized and policed by the governance authority to perform the TN provider function.
  - Is trusted to only provide legitimate and valid numbers for use by the enterprise identity service.
  - Can only assign TNs for which they are the original assignee.
  - Is able to revoke a TN from being used, if identified as being used inappropriately.
  - Can reassign a TN to another enterprise, if no longer in use.
  - Is a contributory node of the distributed ledger network.
  
  › **OSP**
  - Is verified, authorized and policed by the governance authority to perform the OSP function.
  - Will provide an indication within STIR/SHAKEN header that the call has been signed by the enterprise identity distributed ledger service.
  - Is a contributory node of the distributed ledger network.
  
  › **TSP**
  - Is verified, authorized and policed by the governance authority to perform the TSP function.
  - Can verify that a call indicated as enterprise identity in the STIR/SHAKEN header has been signed by the enterprise identity distributed ledger service.
  - Has the capability to screen TNs from being forwarded to the called party based on global and called party specific opt-in policies (out of scope for the POC).
» NOTE: If the Called Party is roaming, then the opt-in policy needs to be collected from the called party service provider.

- Is a contributory node of the distributed ledger network.

\textbf{Called Party}

- Has the ability to register their opt-in preferences with their service provider to receive signed calls (out of scope for the POC).
- The UE of the called party will indicate that call is signed and trusted (out of scope for the POC).
User Stories

The following section provides a description of the user stories for each actor. User stories are descriptions of desirable system features, ideally describing some customer-visible functionality.

A useful format for expressing user stories is:

As a <actor/role>, I want <goal/desire> so that <benefit/value>

The third part (so that <benefit/value>) is often clear from the context and does not have to be explicitly stated.

5.1 Governance Authority

<table>
<thead>
<tr>
<th>ID</th>
<th>EIDL-001</th>
</tr>
</thead>
<tbody>
<tr>
<td>Actor</td>
<td>As the governance authority</td>
</tr>
<tr>
<td>I want/Goal</td>
<td>I want to control which actors can be a node of the enterprise identity network by only allocating DL node identities to trusted contributors.</td>
</tr>
<tr>
<td>Value/Benefit</td>
<td>Ensure that only trusted actors have access to the enterprise identity DL network nodes</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>ID</th>
<th>EIDL-002</th>
</tr>
</thead>
<tbody>
<tr>
<td>Actor</td>
<td>As the governance authority</td>
</tr>
<tr>
<td>I want/Goal</td>
<td>I want to prevent an actor from using the enterprise identity network by revoking their identity.</td>
</tr>
<tr>
<td>Value/Benefit</td>
<td>Prevent a bad actor access the enterprise identity network</td>
</tr>
</tbody>
</table>
### 5.2 KYC Vetter

<table>
<thead>
<tr>
<th>ID</th>
<th>EIDL-003</th>
</tr>
</thead>
<tbody>
<tr>
<td>Actor</td>
<td>As the KYC vetter</td>
</tr>
<tr>
<td>I want/Goal</td>
<td>I want to register with the governance authority to be an approved KYC vetter of the enterprise identity network</td>
</tr>
<tr>
<td>Value/Benefit</td>
<td>As an approved KYC Vetter, I can authenticate brand and BPO enterprise actors to use the network.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>ID</th>
<th>EIDL-004</th>
</tr>
</thead>
<tbody>
<tr>
<td>Actor</td>
<td>As the KYC vetter</td>
</tr>
<tr>
<td>I want/Goal</td>
<td>I can authorize a vetted brand/BPO enterprise actor account and provide it a trusted identity to be used on the network.</td>
</tr>
<tr>
<td>Value/Benefit</td>
<td>Enable a vetted enterprise to use its trusted identity to transact and use the enterprise identity data with other actors on the network.</td>
</tr>
</tbody>
</table>

### 5.3 TN Provider

<table>
<thead>
<tr>
<th>ID</th>
<th>EIDL-005</th>
</tr>
</thead>
<tbody>
<tr>
<td>Actor</td>
<td>As a TN provider</td>
</tr>
<tr>
<td>I want/Goal</td>
<td>I want to register with the governance authority to be an approved TN provider of the enterprise identity network.</td>
</tr>
<tr>
<td>Value/Benefit</td>
<td>As an approved TN provider, I can issue trusted TNs to vetted brand and BPO enterprise actors to be authenticated by the network.</td>
</tr>
<tr>
<td>ID</td>
<td>Description</td>
</tr>
<tr>
<td>--------</td>
<td>----------------------</td>
</tr>
<tr>
<td>EIDL-006</td>
<td>As a TN provider</td>
</tr>
<tr>
<td>ID</td>
<td>I want/Goal</td>
</tr>
<tr>
<td>EIDL-006</td>
<td>I can assign a TN to a KYC vetted enterprise account ID, indicating the terms of use for the TN, its intended use and content type.</td>
</tr>
<tr>
<td>Value/Benefit</td>
<td>Allow any actor that has access to the network to know which is the authorized holder of the TN, including the terms and purpose of its use.</td>
</tr>
</tbody>
</table>

5.4 Brand Enterprise

<table>
<thead>
<tr>
<th>ID</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>EIDL-007</td>
<td>As a brand enterprise</td>
</tr>
<tr>
<td>ID</td>
<td>I want/Goal</td>
</tr>
<tr>
<td>EIDL-007</td>
<td>I want to connect and register with a KYC vetter to have my KYC identity data validated, and to be assigned a trusted enterprise identity for my account ID.</td>
</tr>
<tr>
<td>Value/Benefit</td>
<td>I will be able to prove my identity when transacting on the enterprise identity network with other actors. My assigned enterprise identity can be used by TN providers to verify my identity.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>ID</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>EIDL-008</td>
<td>As a brand enterprise</td>
</tr>
<tr>
<td>ID</td>
<td>I want/Goal</td>
</tr>
<tr>
<td>EIDL-008</td>
<td>I can use my authenticated account ID to request/obtain TNs from a TN provider, providing details of the intended use and call content when requesting a TN.</td>
</tr>
<tr>
<td>Value/Benefit</td>
<td>I can reuse my enterprise identity data to attain TN's.</td>
</tr>
<tr>
<td>ID</td>
<td>EIDL-009</td>
</tr>
<tr>
<td>------</td>
<td>---------------------------</td>
</tr>
<tr>
<td>Actor</td>
<td>As a brand enterprise</td>
</tr>
<tr>
<td>I want/Goal</td>
<td>I can use my assigned enterprise identity to sign originating calls I place with an OSP.</td>
</tr>
<tr>
<td>Value/Benefit</td>
<td>Any OSP can verify my enterprise identity and that I am authorized to use the TN.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>ID</th>
<th>EIDL-010</th>
</tr>
</thead>
<tbody>
<tr>
<td>Actor</td>
<td>As a brand enterprise</td>
</tr>
<tr>
<td>I want/Goal</td>
<td>I can delegate my authorized TN to a BPO enterprise to make originating calls on my behalf.</td>
</tr>
<tr>
<td>Value/Benefit</td>
<td>Any OSP can verify that the specific BPO enterprise identity is authorized to use the TN.</td>
</tr>
</tbody>
</table>

5.5 BPO Enterprise

<table>
<thead>
<tr>
<th>ID</th>
<th>EIDL-011</th>
</tr>
</thead>
<tbody>
<tr>
<td>Actor</td>
<td>As a BPO enterprise</td>
</tr>
<tr>
<td>I want/Goal</td>
<td>I want to connect and register with a KYC vetter to have my KYC identity data validated, and to be assigned a trusted enterprise identity for my account ID.</td>
</tr>
<tr>
<td>Value/Benefit</td>
<td>I will be able to prove my identity when transacting on the enterprise identity network. My assigned enterprise identity can be used by brand enterprises to verify my identity.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>ID</th>
<th>EIDL-012</th>
</tr>
</thead>
<tbody>
<tr>
<td>Actor</td>
<td>As a BPO enterprise</td>
</tr>
<tr>
<td>I want/Goal</td>
<td>I can use my assigned enterprise identity to sign originating calls I place with an OSP.</td>
</tr>
<tr>
<td>Value/Benefit</td>
<td>Any OSP can verify my identity and that I have authorization to use the TN.</td>
</tr>
</tbody>
</table>
### 5.6 Originating Service Provider

<table>
<thead>
<tr>
<th>ID</th>
<th>EIDL-013</th>
</tr>
</thead>
<tbody>
<tr>
<td>Actor</td>
<td>As an OSP</td>
</tr>
<tr>
<td>I want/Goal</td>
<td>I want to register with the governance authority be an approved OSP of the enterprise identity network.</td>
</tr>
<tr>
<td>Value/Benefit</td>
<td>As an approved OSP, I can check and sign authentic originating calls being placed using the enterprise identity network.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>ID</th>
<th>EIDL-014</th>
</tr>
</thead>
<tbody>
<tr>
<td>Actor</td>
<td>As an OSP</td>
</tr>
<tr>
<td>I want/Goal</td>
<td>I can authenticate an originating call from an enterprise by using the originating TN and enterprise ID signature (within the SIP header) to verify the call’s authenticity.</td>
</tr>
<tr>
<td>Value/Benefit</td>
<td>I am able to verify any originating call placed from an authorized enterprise Identity/TN registered on the enterprise identity network.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>ID</th>
<th>EIDL-015</th>
</tr>
</thead>
<tbody>
<tr>
<td>Actor</td>
<td>As an OSP</td>
</tr>
<tr>
<td>I want/Goal</td>
<td>I can indicate in the STIR/SHAKEN header that the call is authenticated/attested to using the enterprise identity network.</td>
</tr>
<tr>
<td>Value/Benefit</td>
<td>I can notify any TSP that it can use the enterprise identity network to screen the call from the stored TN profile data.</td>
</tr>
</tbody>
</table>
### 5.7 Terminating Service Provider

<table>
<thead>
<tr>
<th>ID</th>
<th>EIDL-016</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Actor</strong></td>
<td>As a TSP</td>
</tr>
<tr>
<td><strong>I want/Goal</strong></td>
<td>I want to register with the governance authority be an approved TSP of the enterprise identity network.</td>
</tr>
<tr>
<td><strong>Value/Benefit</strong></td>
<td>As an approved TSP, I can check calls being placed using the enterprise identity network.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>ID</th>
<th>EIDL-017</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Actor</strong></td>
<td>As a TSP</td>
</tr>
<tr>
<td><strong>I want/Goal</strong></td>
<td>I can query a TN verified by the network to screen the TN before forwarding the call to the called party based on my own and called party opt-in preferences.</td>
</tr>
<tr>
<td><strong>Value/Benefit</strong></td>
<td>I have information about the intended use and content type to screen the call before forwarding to the called party.</td>
</tr>
</tbody>
</table>
Governance

Governance refers to all actions, such as decision-making processes, that are involved in creating, updating and abandoning formal and informal system rules. These rules can be code (e.g., smart contracts), laws (e.g., fees for malign actors), processes (what must be done when X happens) or responsibilities (who must do what).

The current STIR/SHAKEN governance model is based on a central representation of a consortium of non-discriminatory representation members managing the governance rules over the roles, access and operation of members having access to the STIR/SHAKEN network. Each STIR/SHAKEN network member is authenticated and authorized to operate under the trust of the governing authority. The rules for operation and implementation of the protocol are managed and verified by this consortium. Member access can be revoked when these rules are broken.

The enterprise identity distributed ledger acts as an extension of the STIR/SHAKEN network. So it is the working assumption that the enterprise identity distributed ledger governance be aligned, operating as a consortium. The key areas for governance to be defined for the enterprise identity network are described below.

**Organizational Governance Authority**

The organizational governance authority is where member organizations control what is shared and with whom it is shared. Most likely, the member organizations involved have different goals and priorities. They may be in direct competition with each other in one area and partners in others. None of the organizations involved is willing to cede total control of the consortium to one of the others. To function efficiently, the consortium needs to have a governance model in place. A governing body will be needed as the network grows and the organizations change. In the first instance, the consortia must agree on how the consortium organization will be formed, and managed, covering areas such as:

- Qualifications for membership.
- Member management and administration.
- Data rights and responsibilities.
- Withdrawal of consortium members.
- Term, removal and termination.
• Warranties.
• Dispute Resolution.

It is important to decide what will be the legal framework and jurisdiction that will cover the governance and consortium members. The selection of the type and the jurisdiction of this entity structure will be driven by the location of the founding members and prospective members, as well as tax issues. This should be considered carefully for the future growth and scope of the distributed ledger project, as the project may span geographies and market sectors in the future.

As this area will be subject to the long-term viability and scope of a production solution, the organizational governance is out of scope for definition of the PoC.

**Funding Governance**

Funding governance regulates how projects manage collected funds:

• Funding source and amount: i.e., where do funds come from. A blockchain project is typically funded in one of two ways:
  › By the community of the distributed ledger project, either as membership fees for the consortium and/or subscription fees to participate on the distributed ledger network. These models are typical for private and consortia distributed ledger projects.
  › The distributed ledger is self-funding through transaction fees, created within the protocol of the distributed ledger itself. These are typically performed within the economic modeling of public distributed ledger projects, where a portion of the generated fees can be set aside to manage the operation and change of the network. (e.g., 10 percent of all mining rewards).
• Funds Administrator: Defines who collects, spends and keeps the funds.
• Fund usages: Defines what should be done with the funds.
• Reporting process: Defines how the fund usage should be communicated to the outside (e.g., through quarterly financial statements).

As this area will align with the organizational governance of any production solution, this area is out of scope for definition with the PoC.

**Project Governance**

Project governance deals with all topics related to the technology (i.e., the code), distributed ledger/network governance, funding governance and meta-governance (i.e., changing the governance process itself). Technology-related topics include, among other things, distributed ledger parameters (e.g., changing block size or gas prices), fixing bugs or adding new features.

The management of the project governance and the priorities is typically included within the control of the consortia governance.

As projects grow in size, the use of the distributed ledger protocol itself can
allow all participants to have voting rights in the network’s project direction. Voting may be implemented using tokens that are directly proportionate to the member’s interest in the network. The token holders can vote using the tokens in the form of a liquid democracy to cast votes on decisions and preventing voting centralization.

In a changing world, speed of change is critical to improving services or reacting to potential cyber-attacks. Project governance should be able to deal with change using a controlled but effective mechanism, i.e., without the need for monthly meetings and consensus agreement across attending members. This is an area where using on-chain governance can add value for the distributed ledger project.

As this area will align with the organizational governance of any production solution, it is out of scope for definition with the PoC.

**Operational Governance**

The operational governance deals with ensuring the network continues to run correctly and can be upgraded and improved over time. The key areas covering this include:

- Fix bugs and vulnerabilities of the network.
- Upgrade the underlying network technology.
- Repair damages from attacks on the network.

The majority of distributed ledger projects deal with these aspects through a contracted entity that is responsible for the operational maintenance of the platform and its service.

As this area will align with the organizational governance of any production solution, this area is out of scope for definition with the PoC.

**Network Governance**

This area deals with controls over the network infrastructure, access participation and security. The scope of network governance for enterprise identity distributed ledger covers the following:

- Qualifications for node hosting.
- Identity management of nodes.
- Qualifications for KYC vetter to assign accounts to an enterprise.
- TN provider account management and administration.
- TN data rights, responsibilities and terms of use.
- Network transaction validation.
- TN withdrawal from enterprise account.
- Account reputation and revocation.
- Node reputation and revocation.
- Dispute resolution.
6.1 Network Governance

The following sections provide information regarding the enterprise identity network governance.

6.1.1 Qualifications for Node Hosting

The governance authority will ultimately decide which individual actor can be a contributing node to the enterprise identity network. Through an approval process (out of scope for the PoC), the governance authority will satisfy itself that the actor can conform to the agreed policies and procedures to be a participating node. Once the governance authority is satisfied that the individual actor is compliant, it will authorize the actor by issuing a digital certificate as described in section 7.

6.1.2 Identity Management of Nodes

The enterprise identity network node's identity will be authenticated using digital certificates to provide access controls and access preventions as outlined in section 7.

6.1.3 Qualifications for KYC Vetter to Assign Accounts

The KYC vetter will ultimately decide which individual enterprise actor can be assigned an account on the enterprise identity network. Through an approval process set out by the governance authority (out of scope for the PoC), the KYC vetter will determine whether the enterprise actor can conform to the agreed policies and procedures to be a participating enterprise of the network and assign it an account identity. Once the KYC vetter is satisfied that the individual enterprise actor is compliant, the KYC vetter will authorize it by issuing an enterprise identity with its private key as described in section 7.

6.1.4 TN Provider Account Management and Admin

The TN provider account administration will be a governance authority function. The governance authority will control whether each entity is a trusted provider of TN identities to enterprise accounts. The governance authority will have an application that will enable it to provide TN providers with account identities on the enterprise identity network with a private key that they can use to transact on the network, as described in section 7.

6.1.5 TN Data Rights, Responsibilities and Terms of Use

The rights for the TN allocation to an enterprise and its terms of use will be defined within a contractual agreement between the enterprise and the TN provider. The terms of use for the TN will be incorporated within a smart contract allocated with the TN assignment to the enterprise on the enterprise identity network.

6.1.6 Network Transaction Validation

The network nodes will provide the consensus mechanism used to validate transactions on the enterprise identity network. A governance authority consortium will control the network, so the most appropriate mechanism in
this scenario would be a Byzantine Fault-Tolerant (BFT) protocol. The BFT protocol allows each of the nodes to be a validator and enables policing of one another. As no specific distributed ledger technology platform has been decided for the PoC, the specific consensus protocol will be decided by the PoC implementation.

### 6.1.7 TN Withdrawal from Enterprise Account

The withdrawal of a TN from an enterprise account will occur in one of the following scenarios:

1. The term of use has expired by the contract. In this case the process is automated as part of the smart contract term. The TN is released by the TN provider.

2. The enterprise no longer requires the TN and has requested its end of use. In this case, the enterprise will request that the TN assignment is removed and a transaction is generated, mutually signed between the TN provider and the enterprise so that the network is updated with the change.

3. The terms of use have been violated and the TN revoked. In this case, a feedback mechanism is implemented on the network to provide reputation scoring for the terms of use. Where the reputation is deemed to be compromised, the smart contract can revoke the use of the TN and return it to the TN provider. This mechanism is for future study and out of scope for this stage of the PoC.

### 6.1.8 Account Reputation and Revocation

A feedback mechanism is implemented on the network to provide reputation scoring for the terms of use of enterprise TNs. If the reputation of the TNs assigned to an enterprise is deemed to be compromised, the TN smart contract can revoke the use of the TN and return it to the TN provider. The enterprise account can also be revoked as part of this mechanism. This mechanism is for future study and out of scope for this stage of the PoC.

### 6.1.9 Node Reputation and Revocation

As part of the agreed governance authority policy for a node provider and the consensus mechanism, if a node provider is observed to not be performing its functions to the agreed procedures, its participation into the network will be revoked according to the process in section 7.

### 6.1.10 Dispute Resolution

The governance authority will provide a dispute resolution process for node providers and enterprise actors to report and challenge a dispute. This is out of scope for the PoC.
Identity Management

The following section covers identity management of the enterprise identity network. Each actor will require a permissioned identity to be either:

1. A distributed ledger node identity, permissioned to be a contributor node within the enterprise identity distributed ledger network that other nodes use to verify the access and communications.
2. An account identity used by an individual enterprise and the TN provider actors to authenticate themselves while transacting with the enterprise identity service.

7.1 Distributed Ledger Node Identities

A public blockchain is a permission-less blockchain. Anyone can join a public blockchain network, meaning that they can read, write or participate. Public blockchains are decentralized: No single entity has control over the network, and all entities are immutable because their data cannot be changed once validated on the blockchain.

On the other hand, a private blockchain is a permissioned network of nodes. This means restrictions are placed on who can participate, what functions they can perform and with which transactions they can interact.

**Enterprise Identity DL Private Network**

The enterprise identity distributed ledger will be a private blockchain, enabling the governance and control over access to the nodes and the data to be controlled by the relative trust authority. Communication for each node of the distributed ledger network is authenticated using a private key/digital certificate verified by all other network nodes. The authorization and allocation of the distributed ledger node private key/digital certificate will be the role of the governance authority.

NOTE: It is possible to implement virtual private distributed ledger networks on public blockchain using enterprise implementations of existing public network technologies, such as Ethereum, EoS, etc. No specific distributed ledger technology is decided at this stage.
The actors that can be an authorized network node are:

- **KYC Vetter**
  - It is mandatory for a KYC vetter to be a network node because it provides the authoritative function for vetting all enterprise identities.
- **TN Provider**
  - It is mandatory for a TN provider to be a network node because it is the trusted source of approved TNs.
- **OSP**
  - It is not mandatory for an OSP actor to be a network node if it is a TN Provider, but it must be authorized by the governance authority to do so.
- **TSP**
  - It is mandatory for the TSP to be a network node because it will contribute termination quality reports to the network.

### 7.2 Actor Account Identities

#### 7.2.1 Blockchain Account Identities Overview

Address, private key, public key and digital signatures are elements of managing an account identity used in the blockchain and distributed ledger technologies.

**Blockchain Address**

At the core of a distributed ledger, everything is transacted between account addresses. These addresses are typically a string of characters. For example, Bitcoin addresses are a sequence of letters and digits, such as 171gLtPShdVXdkjieiG786WmeAyTVWXFA4q. Once an address has been created, it is unique on the blockchain and cannot be created a second time; it exists forever on the distributed ledger. As with an email address, once an entity knows the other party’s address, it can use that address to transact with it.

Typically, an address is created with an endpoint application, such as a wallet application used to manage cryptocurrencies. The application will allow users to create an account, where a public-private key pair is generated. The public key is then used with a hash function to create the public address that Bitcoin users use to send and receive funds. The private key is kept secret and is used to sign a digital transaction to make sure the origin of the transaction is legitimate.

**Public-Private Key**

Public key cryptography, or asymmetric cryptography, is a cryptographic system that uses pairs of keys. Public key cryptography is an essential part of a blockchain protocol and is used in several places to ensure the integrity of messages transferred using the protocol.

**Digital Signatures**

Digital signatures are core to the security of distributed ledger technologies,
where every message/transaction has a different digital signature that is created by the user’s private key. By using the public key of the user account identity and the signature, it is possible to prove the signature is authentic.

- **Sign (Message, Private Key) -> Signature.** Given the message we want to sign and a private key, this function produces a unique digital signature for the message.
- **Verify (Message, Public Key, Signature) -> True/False.** Given the message we want to verify, the signature and the public key, this function gives a binary output depending on whether the signature is authentic.

**NOTE:** This is the same process used by STIR/SHAKEN by the OSP to sign originating calls, and for the TSP to verify that it came from the trusted origin.

### 7.2.2 Enterprise Identity DL Account Identities

Each actor of the enterprise identity distributed ledger must provide a proven, trusted, unique identity when interacting with other actors on the enterprise identity network. To verify the identity of the actor, it is proposed to use private-public key digital signatures for transacting between actors.

All actors that are communicating or transacting using the enterprise identity network will have a unique address on the distributed ledger that can identify the individual actor. Public-private keys associated with the account identity are used to digitally sign messages and transactions to authenticate the account identity.

Not all actors on the network will require an account, as they may only be using the network to read and validate identities, TN associations and or TN profile data.

**NOTE:** The specific distributed ledger address format will be defined by the DLT choice used for the PoC. It would be proposed that any unique identifier should be a globally unique string corresponding to a Universally Unique Identifier (UUID) (RFC 4122), making it compatible with STIR/SHAKEN PASSport Encoding.

#### 7.2.2.1 Brand and BPO Enterprise Identity

When a brand or BPO enterprise actor registers with a KYC vetted on the network, a unique account identity is generated on the distributed ledger by the KYC vetter node with a corresponding public-private key pair.

This address is the identity used by the enterprise actor to perform all transactions on the enterprise identity distributed ledger. Together with the private key, the identity can be proven and authenticated when interacting with all actors on the network.

**NOTE:** The specific distributed ledger address format will be defined by the DLT choice used for the PoC. It would be proposed that any unique identifier should be a globally unique string corresponding to a UUID (RFC 4122), making it compatible with STIR/SHAKEN PASSport Encoding.

The enterprise actor account identity can be used by the network when
performing the following actions:

- Initial identity verification of the enterprise by the KYC vetter.
- Send and upload ID data for vetting (securely stored on distributed ledger for future use).
- Request TN from a TN provider, including the intended use.
- TN assignment to the enterprise for its intended use.
- Brand delegate a TN to a 'BPO.
- Sign originating calls placed to an OSP.
- OSP authenticate call and sign STIR/SHAKEN header.
- TSP authenticate the call signature and determine call screening.

7.2.2.2 TN Provider Identity

When a TN provider actor registers on the network, a unique account identity is generated by the governance authority on the distributed ledger with a corresponding public-private key pair.

This address is the identity used by the TN provider actor to perform all transactions on the enterprise identity distributed ledger. Together with the private key, the identity can be proven and authenticated when interacting with all actors on the network.

NOTE: The specific distributed ledger address format will be defined by the DLT choice used for the PoC. It would be proposed that any unique identifier should be a globally unique string corresponding to a UUID (RFC 4122), making it compatible with STIR/SHAKEN PASSport Encoding.

The TN provider actor account identity can be used by the network when performing the following actions:

- Assign a TN to the brand enterprise for its intended use.
- Revoke an assigned TN from being used, in the event of misuse (TBD).
- OSP to verify that the TN provider is a legitimate source of the TN.
- TSP to verify that the TN provider is a legitimate source of the TN.
Data Model

The following section describes the basic enterprise identity data model required for a PoC.

The enterprise identity Object Class diagram below is the basic meta-format for each enterprise identity actor and the TN relationship. The syntax used in the diagram is to model an XML schema definition (XSD) as an UML diagram.
The enterprise identity object attributes are described as follows:

### TABLE 8.1 ENTERPRISE IDENTITY DATA MODEL – ATTRIBUTE DEFINITION

<table>
<thead>
<tr>
<th>Attribute Name</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>name</td>
<td>Name descriptor of the actor identity/business identity</td>
</tr>
<tr>
<td>Uuid</td>
<td>Globally unique string corresponding to a UUID (RFC 4122)</td>
</tr>
<tr>
<td>publicKey</td>
<td>The public key generated and assigned to the actor account</td>
</tr>
<tr>
<td>tn</td>
<td>The unique telephone number identity</td>
</tr>
<tr>
<td>use_intent</td>
<td>The intended use of the telephone number</td>
</tr>
</tbody>
</table>

The following instance diagram illustrates an example of the TN “+14085551234” assignment by the TN provider “DC Telecom” to the brand enterprise “Global Airlines” for the intended use of notifying customers about “Delayed Flight Notification.” Global Airlines delegates the TN to the BPO enterprise “Calls RUs” to make outgoing calls. Both Global Airlines and Calls RUs have been vetted by “TrustyCorp.”

![Instance Diagram](image)
Solution – Functional Architecture and Flows

The following section provides a high-level functional architecture of the enterprise identity and the flows between each of the actors of the service.

![Diagram of Trust Authority/Certificate Authority, Governance Authority, DL Network Nodes, Brand Enterprise, BPO Enterprise, TN Provider, TSP, Register/Verify, Transact, Authenticate, Authorize, Governance, Audit]  

**FIGURE 9.1 ENTERPRISE IDENTITY HIGH LEVEL FUNCTIONAL ARCHITECTURE**

9.1 Functional Flows

The following section describes the function flows that address the specific user stories described in section 9.

NOTE: This section is described at a level of abstraction, specifically, so as not to define a DLT protocol.

9.2 Governance Authority Flows

The following flows apply to the governance authority user stories.

9.2.1 New Distributed Ledger Node Creation and Authorization: EIDL-001, EIDL-003, EIDL-005, EIDL-0013, EIDL-0016

The governance authority will have a delegated trust authority to perform the actor vetting and authentication to provide a node of the distributed ledger. When an actor requests to be a distributed ledger node of the enterprise
identity network, it must perform the following steps:

- Download a copy of the enterprise identity network node software from a trusted source (trust authority).
- Register to be a node contributor of the network, indicate the actor role the node will perform and provide evidence of the ability to perform the function as part of the network.
- Be validated to the satisfaction of the governance authority to perform the role as the actor.
- Generate a private-public key pair and distribute to the relevant parties.
- Connect and synchronize the node data from the network.

**FIGURE 9.2 NEW DISTRIBUTED LEDGER NODE CREATION AND AUTHORIZATION**

NOTE: This flow allows for the registration of all actors providing a contributory node to the enterprise identity network.

### 9.2.2 New TN Provider Account: EIDL-005

A TN provider requires an enterprise identity distributed ledger account ID in order to allocate TNs for Enterprise use on the ledger. The trust authority acting on behalf of the governance authority will generate an account for the TN provider with the node approval.
9.2.3 Revocation of a Bad Actor Node: EIDL-02

When the governance authority has a reason to revoke a node from accessing the enterprise identity distributed ledger (e.g., bad actor), the TA, acting on the governance authority’s behalf, will revoke the bad actor node certificate. The TA also will notify all network nodes to prevent the bad actor connecting with the network.
9.3  Enterprise Flows

The following flows apply to the enterprise user stories.

9.3.1  Enterprise Registration with A KYC Vetter: EIDL-007, EIDL-011

When either a brand or a BPO enterprise wants to connect and register to be KYC vetted for access to the distributed ledger network, it must connect with an approved KYC vetter using a registration application (portal/wallet application) to create an application with the KYC vetter. The application will include the relevant documented identity evidence to satisfy the KYC vetter to be granted approval.

Once the application is approved (vetted), the registration application can generate an enterprise account ID on the KYC vetter node and the corresponding key pair for the account. The enterprise identity account ID with the public key is distributed across the enterprise identity distributed ledger network of nodes.

**NOTE:** The Enterprise will be responsible for the safe storage of the private key.

![Figure 9.5 Enterprise Registration with the KYC Vetter](image)

9.3.2  ‘Brand’ Enterprise – Attain TN: EIDL-008

When a brand enterprise wishes to attain a TN from a TN provider, it must make that request through an application (portal/wallet) to the TN provider. This request must include the TN’s intended use and nature of the content the TN will be used for.

The TN provider will create a smart contract representing the TN asset on the distributed ledger, including the terms of use agreed with the brand enterprise.
ID. This is signed with the TN provider's private key and recorded on the ledger. The brand enterprise will counter sign the smart contract using its private key. The TN is now assigned to the brand enterprise for use according to the contract terms.

**FIGURE 9.6 ATTAINMENT OF A TN BY THE ‘BRAND’ ENTERPRISE FROM THE TN PROVIDER**

### 9.3.3 Delegate a TN to a BPO Enterprise: EIDL-010

When a brand enterprise wishes to delegate a TN asset to a BPO enterprise to make and sign outgoing calls on the brand’s behalf, they must agree to the terms of use for delegating the TN.

The brand enterprise will add a new record into the TN asset smart contract to indicate that the BPO enterprise account ID is now originating the calls on its behalf. The brand enterprise signs this with its private key.

The BPO enterprise accepts the contract terms and signs with its account private key.
9.4  Service Provider Flows

The following flows apply to the OSP and TSP user stories.

9.4.1  Signing and Authenticating an Originating Call: EIDL-009, EIDL-012, EKYC-014

When a brand or BPO enterprise makes an outgoing call to the OSP, it will sign the outgoing call with its private key.

NOTE: For investigation, the enterprise will encode the SIP header using RFC 3325: Private Extensions to the Session Initiation Protocol (SIP) for Asserted Identity within Trusted Networks to sign an outgoing call.

Further information regarding the specific encoding to align with the STIR/SHAKEN protocol is defined in section 12 of this document.

The OSP will query the smart contract for the TN asset to get the enterprise ID that is authorized to originate this TN. The OSP will use the public key for the enterprise ID account to validate the SIP signature. If the signature is valid, the OSP can attest to the call with STIR/SHAKEN. If not valid, the OSP will not attest to the call.
9.4.2 OSP Attesting of the Originating Call: EIDL-015

When the OSP can attest the originating call is from the authorized enterprise ID.

NOTE: Assuming same process as current STIR/SHAKEN for OSP, where the SIP header is replaced with the STIR/SHAKEN header created using the OSP token.

9.4.3 TSP Attesting of the Originating Call: EIDL-017

The OSP forwards the call to the TSP using STIR/SHAKEN. The TSP will verify the call using the SIP header according to STIR/SHAKEN. If the TSP can verify the originating call, then the TSP will query the smart contract for the TN asset on the enterprise identity distributed ledger to determine the intended use and content of the call.

NOTE: This could include the brand enterprise name (i.e. Global Airlines).

Based on the network preferences and/or called party preferences for receiving calls, the call may or may not be forwarded to the called party.
Proposed Interworking with STIR/SHAKEN

The following section describes how the enterprise identity will interwork with the STIR/SHAKEN infrastructure to support the enterprise identity trusted originating call flows.

It is proposed for the purpose of the PoC that a vetted enterprise originating a call to an OSP will create a SIP header that is consistent with the ATIS-1000074 SHAKEN specification, section 5.4. Specifically, the encoding of the SIP header by the STI-AS conveys to the TSP an authenticated and trusted originating call. The enterprise originating a call will include a signed enterprise PASSPort token in the SIP header to enable the OSP to authenticate and attest to the call.

It is proposed for the enterprise identity PoC that the enterprise PASSPort shall be encoded by an enterprise actor and validated by the STIR/SHAKEN infrastructure as defined in the draft-ietf-stir-rfc4474bis document.

Note: It is assumed for the interworking with the STIR/SHAKEN infrastructure that the STI-AS and STI-VS function will need adaptation to verify the enterprise PASSPort token conveyed in the SIP header from the enterprise identity distributed ledger. This is described later in this section.

10.1 Interworking Call Scenarios

The following table identifies four basic call scenarios that indicate where the interworking of enterprise identity with STIR/SHAKEN would be used.

<table>
<thead>
<tr>
<th>Scenario</th>
<th>Enterprise PASSPort</th>
<th>OSP Verification</th>
<th>TSP Verification</th>
<th>Result</th>
</tr>
</thead>
<tbody>
<tr>
<td>A</td>
<td>No</td>
<td>No</td>
<td>Non Possible</td>
<td>Call not verified</td>
</tr>
<tr>
<td>B</td>
<td>Yes</td>
<td>Yes</td>
<td>Shaken PASSPort</td>
<td>Call is verified</td>
</tr>
<tr>
<td>C</td>
<td>Yes</td>
<td>Yes</td>
<td>Shaken PASSPort</td>
<td>Call is verified</td>
</tr>
<tr>
<td>D</td>
<td>Yes</td>
<td>Shaken PASSPort</td>
<td>Shaken PASSPort</td>
<td>Call is verified</td>
</tr>
</tbody>
</table>

This specification will outline call scenarios C and D where the enterprise will provide an enterprise PASSPort token encoded SIP header.

### 10.2 Call Scenario C: OSP STI-AS Enterprise Identity Attested

This call scenario illustrates where a KYC vetted enterprise originates a call to an OSP including an enterprise PASSPort token, and the OSP is able to attest to the originating call with a SHAKEN token. The OSP is able to identify the SIP header as an enterprise vetted call and will authenticate the enterprise PASSPort token as follows:

![Diagram of call scenario C](image)

**FIGURE 10.1 CALL SCENARIO C – OPTION 1 (TSP NO CONNECTION WITH ENTERPRISE IDENTITY DISTRIBUTED LEDGER)**

1. The OSP will identify that the originating call is a signed enterprise PASSPort by the encoded SIP header. The enterprise PASSPort is forwarded to the STI-AS for authentication.

2. The adapted STI-AS will have a function to authenticate the enterprise PASSPort from the enterprise identity distributed ledger to authenticate the enterprise and the authorized use of the TN.
   a. Using the public key for the enterprise “origid” to verify the token.
   b. The TN has assignment to this enterprise to make outgoing calls.

3. If the enterprise PASSPort is authenticated, then the STI-AS can attest to the originating call, encoding the SIP header according to the SHAKEN Specification ATIS-1000074 to the TSP.

4. The TSP will verify the SHAKEN SIP header according to the SHAKEN Specification ATIS-1000074.

5. **NOTE:** in the above example, the TSP has no connection with the enterprise identity distributed ledger to collect information regarding the TN Intended use to indicate to the end user UE.
Where the TSP is also connected with the enterprise identity distributed ledger, the STI-VS is adapted to query the TN intended use data, included in the following additional steps.

- When the STI-VS has verified the SHAKEN PASSPort, it will query the originating TN on the enterprise identity distributed ledger to identify the brand enterprise assignee of the TN and the intended purpose of the TN.
- Extended caller ID information can be provided to the end user UE, indicating the brand identity and intended purpose.

### 10.3 Call Scenario D: OSP STI-AS No Attestation

In this call scenario, the OSP is unable to attest to the originating call and provide a SHAKEN passport to the TSP. For example, the TSP is not part of the SHAKEN network. The OSP will forward the originating call with the original enterprise PASSPort to the TSP. The TSP can authenticate the originating call using the enterprise PASSPort as follows:
FIGURE 10.3 CALL SCENARIO D – OSP STI-AS NO ATTESTATION

1. The OSP will identify that the originating call is a signed enterprise PASSPort by the encoded SIP header. The enterprise PASSPort is forwarded to the STI-AS for authentication.

2. The STI-AS will not attest to the enterprise PASSPort. For example, the destination TSP is not included in the SHAKEN network, so the OSP will forward the originating call to the TSP with the original enterprise PASSPort in the SIP header.

3. The TSP will send the enterprise PASSPort to the adapted STI-VS to authenticate the enterprise PASSPort from the enterprise identity distributed ledger, as well as authenticate both the enterprise and the authorized use of the TN, which was used to originate the call. At the same time, the TN brand identity and the TN intended use can be retrieved.

4. If the enterprise PASSPort is authenticated, then the call will be completed to the end user UE with the extended caller ID indicating the brand identity and intended purpose.
10.4 Enterprise PASSPort Token Encoding

It is proposed that the enterprise PASSPort token will be encoded as follows.

Protected Header
{
  "typ":"passport",
  "alg":"ES256",
  "ppt": ( PASSPORT TYPE TO BE DEFINED AS PART OF THE PoC )
  "x5u":https://cert.example.org/passport.crt
}

Payload
{
  "dest":{"tn":["12125551213 "]},
  "iat":1443208345,
  "orig":{"tn":["12155551212"],
  "origid":["123e4567-e89b-12d3-a456-426655440000"

Origination Identifier ("origid")

The Enterprise Identifier Originating the Call. As outlined in section 9.2, "Actor Identities," it is proposed that an enterprise unique identifier should be a globally unique string corresponding to a UUID (RFC 4122), making it compatible with STIR/SHAKEN PASSPort encoding. The ‘orig’ claim and ‘dest’ claim shall be of type ‘tn’.

The “iat” to an encoding of the value of the SIP Date header field

10.5 Enterprise Identity Distributed Ledger Network Integration with STIR/SHAKEN Entities

As indicated previously, for interworking with the enterprise identity distributed ledger, both the STI-AS and STI-VS will need to be adapted to connect with the enterprise identity distributed ledger to verify the enterprise PASSPort. The following diagram illustrates the physical network architecture for the STIR/SHAKEN Interworking with the enterprise identity nodes.
An enterprise identity node can be a separate physical entity from the STI-AS and STI-VS or a software function running inside the STI-AS and STI-VS entities.

A single enterprise identity node could service one or more STI-AS and or STI-VS entities at an OSP/TSP entirely or at individual switch locations. The number and locality of enterprise identity nodes required to support STI-AS and STI-VS entities will depend on the CSP size and call volumes.
New Business Models and Value Creation

Distributed ledger technology can be used across many areas of the telecom service provider business. It can create new business models by:

- Improving current operational processes to increase productivity and quality.
- Increasing speed and transparency of communications amongst parties.
- Creating new opportunities to reinvent products and services.

Some of the key attributes distributed ledger technology brings to the enterprise identity service are:

- Full traceability of any information on the ledger.
- Ability to ensure data has not been tampered with.
- Distributed nature of the technology.
- Smart contracts and automation.
- Increased speed and efficiency.
- Increased security.
- A holistic view with transparency for all appropriate parties.
- New business products or services.

The Accenture Blockchain Value Framework provides a structured approach when building business cases to evaluate the blockchain opportunity. The value drivers can become the prime benefits or opportunities that organizations need to assess.

---

5 Accenture – Building Value from Blockchain Technology – May 2019
Using this model, we have identified how the enterprise identity network will create new value for participating businesses and consumers.

**Auditability**

Blockchain provides a shared ledger of transactions to all parties, with full traceability of any assets and associated activity. As a result, organizations can cut their auditing costs and raise levels of confidence in the data they are producing without having to manually validate the data.

**Enterprise Identity Value Creation:**

- TN reputation can be shared and trusted across all telephone service providers to enable them to quickly identify bad actors or misappropriated use.
  - Increasing TN audit effectiveness and productivity.
- Telecom regulators can view enterprise use of TN and compliance with terms of use at any given time, removing the need for SPs to produce reports.
  - Reducing cost of compliance with audit regulation, increasing productivity.

**Compliance**

Processes involving manual checks for compliance that currently take weeks can be accelerated through a distributed ledger of all relevant information.

**Enterprise Identity Value Creation:**

- Telecom regulator to view enterprise use of TN and compliance with terms of use at any given time, removing the need for SPs to produce reports.
  - Reducing cost of compliance with audit regulation, increasing productivity.
- All transaction data recorded on the blockchain. Each actor can prove that it’s compliant with regulation and or governance terms for the service.
Improving effectiveness for proof of compliance, removing risk of disputes.

**Data management**

Blockchain can improve the management of data in three main areas:

1. Data provenance and accuracy through knowing more about digital assets and accompanying data.
2. Data integrity through access/authentication to the network and easy identification of manipulation or tampering.
3. Data aggregation and organization, as blockchain enables the seamless sharing of real-time data from a single data source. An example metric is improved product forecasting.

**Enterprise Identity Value Creation:**

- TN assets used by an enterprise can include additional data about its intended use and purpose. The data is not static and can change over time (i.e., porting, enterprise assignment, multiparty assignments) change in scope of use. Each actor has full visibility of the TN asset, its current data, history and who made the changes, to qualify how to manage calls. Integrity checking and reputation are shared across all participants in real time so that service integrity is optimal.
  - Increased visibility of information, to provide more effective validation and call management.
  - Improvements in fraud detection capabilities, process effectiveness and cost to manage.

**Data Security**

According to new Accenture research, poor data security could cost companies US$5.2 trillion over the next five years, yet only 30 percent of organizations are confident in their data security. Blockchain technology makes use of military-level cryptography that creates a more secure environment for sharing and storing data, reducing the risk of a data breach and limiting the damage should it occur.

**Enterprise Identity Value Creation:**

- Enterprise identity data, network profiles, and potentially consumer opt in/out profiles can be stored either on or off chain by using encryption to protect this data from breach. This approach also restricts data use to intended parties with permissible keys.
  - Improve security compliance, breach protection, and flexibility to access data securely.

**Ownership**

Distributed ledger technology can enable true digital ownership of both real-world goods and digital assets by creating improved intellectual property and...

---

6 Accenture research, poor data security could cost companies $5.2 trillion over the next five years
personalized data profiles without the need to check the history or current state of the item. Distributed ledger technology can draw on the single, shared data source to ensure asset assignments are accurate and remove the need to manually audit and track down ownership.

**Enterprise Identity Value Creation:**

- Enables any TN to be traced through the supply chain from range holder through subsequent retailers, the attainer/enterprise and any associated BPOs making calls on behalf of the enterprise.
  - Improve productivity and quality of asset tracking and trace back of calls.
  - Increase visibility for TN provider to control quality of supply chain and increase value.

**Process automation**

Distributed ledger enables business processes to be executed automatically via rules-based algorithms. Organizations can use blockchain to look for improvements in efficiency, cost savings and increased worker productivity and retention by shifting the focus of the service to higher engagement and satisfaction.

**Enterprise Identity Value Creation:**

- Using smart contracts to execute TN assignment duration terms, the smart contract will automate the release of the number back into the pool automatically at the end of the used term. All parties will know about this activity in real time. TNs can go back into circulation immediately for resale or the contract duration can be extended with no ambiguity.
  - Improve productivity and quality of asset tracking and assignment.
  - Optimizing TN reuse, more effective use of the assets, increasing value per TN.
  - Improve renewals payment process, eliminate nonpayment exposure.

**Reconciliation**

Inaccurate or missing information, or fragmented communication between multiple parties, are often magnified year after year as unreconciled items get pushed forward. Additional complexities arise due to duplicate entries, post-event changes from cancellations or returns, or conversion from analog to digital inputs. Distributed ledger technology can significantly reduce the overall cost of reconciliation while reducing errors and the accumulation of unreconciled items.

**Enterprise Identity Value Creation:**

- Ensuring that each enterprise identity, TN asset and smart contract has one version of trust on the ledger, so there are no issues for reconciliation of data across internal systems, external partners, or geographic borders.
› Improve productivity and quality of data across the whole ecosystem.

**Standardization**

For multiple organizations to work together in a blockchain system, they must agree on common terms, business logic and business flow as they share access to the same data and apply the same smart-contract-enabled business logic. All participants must agree to the set of rules by which they will work together. This task is often daunting for many industries that have minimal experience of driving this level of agreement.

_Enterprise Identity Value Creation:_

- Using a distributed ledger, everyone performs the rules in exactly the same way according to the rules of the governance authority and smart contracts. If the governance authority changes the rules that need to be updated within the business logic of the ledger, these are automatically adopted across the network at the same time, no impact for version compatibility between interconnecting parties.
- Improve speed to market for improved features and services.
- Ensures interworking compatibility when rolling out changes
- Ease of inclusion of parties across national borders.

**Track and Trace**

The management and tracking of supply chains as it stands today is cumbersome, costly and susceptible to human error, and vulnerable to criminal activities. Distributed ledger technology allows trading organizations to view each step of the supply-chain process. Each party can verify the current state and trail of assets without depending upon direct communication with others in the network.

_Enterprise Identity Value Creation:_

- This allows each party to know instantly if an enterprise is authorized to attain a TN, or a whether TN asset is valid and assigned to an enterprise for use as a verified call. Decisions can be made immediately about how to handle a transaction/call without the need to wait for replies from third parties.
- Increased productivity and reduced costs, having a single consistent view of data and not needing accrual data from various parties.
- Optimizing network resources and costs for the OSP, only process verified calls that are assigned in the ledger but are also not going to be blocked due to TSP or consumer opt-out preferences.

**Data Sharing**

When retained in isolated systems – often fragmented and rarely shared between organizations – data starts to lose its value and verifiability. Without distributed ledger technology, a receiving organization must trust the validity of any data it receives before being able to capture its value. With blockchain, however, trading partners can share real-time data, as well as the history of that
data and any modifications to it.

**Enterprise Identity Value Creation:**

- Data on enterprise onboarding, current identity approval status, their trading history, reputation, historical TN transactions and opt-out preferences can be shared on the ledger. This provides enormous potential to create value and new business models across the supply chain.
  - New revenue opportunities and improved business insights on customer value.
  - Increased data accuracy, always working with current view of information.
  - Process optimization and costs efficiencies, though shared data.

**Resiliency**

Organizations that manage and maintain on-site and central data systems are at risk of malicious or incompetent employees, natural disasters and other situations that can irreparably destroy data. Existing in a distributed form, blockchain creates a highly resilient network with multiple shared copies of the data, all of which mitigates the risk of an isolated attack or incident. An example metric is decreased downtime.

**Enterprise Identity Value Creation:**

- Using a distributed ledger to provide an accurate source of data across the network of participants mitigates any issue from internal fraud, malicious or coordinated attacks. Data can only be introduced or modified onto the network ledger with the agreement and verification by the network consensus.
  - Improved resilience of the system from single point of failure.

**Transparency**

Distributed ledger technology allows all designated parties to view the data in real time. With unlimited transparency, organizations can identify opportunities, improve decision-making and track and trace the outcome of those decisions.

**Enterprise Identity Value Creation:**

- Call validation by the OSP and TSP can be shared across the network using the ledger to determine the reputation of enterprises and the use of the TNs for their intended purpose. Where an individual party has not observed a TN or enterprise previously it can use the ledger reputation score and intelligence to be more effective in screening and processing transactions.
  - Reduce exposure to the business when transacting with unfamiliar enterprises or TNs.
  - Improve incident/fraud response ensuring network has a real-time collective view.
Trust

Trust is being challenged in the digital world, with organizations unable to verify basic essentials. Blockchain helps enable and even automate trust by cryptographically securing information and providing transparency to the state and trail of data. An example metric is mitigated business risk.

Enterprise Identity Value Creation:

- The enterprise identity enables any participant connected to the network the ability to verify the digital identity and signature of an originating call and know if the originator has the right to make a call with the associated TN using the ledger. As TN allocations change ownership from range holder, TN service provider, resellers, carriers and different enterprises, the TN allocation and its permissible use are instantly available for any participating business to verify.
  - Mitigate business risk from inaccurate records or latency on updated systems.
  - Improved level of trust across the ecosystem from a single source of fact.

Authentication

A core function of blockchain technology is its public and private key cryptography, which can serve as a basis for authenticating one user across multiple networks, resulting in increased confidence in the overall network and participants. An example metric is prevention of attacks by bad actors.

Enterprise Identity Value Creation:

- Using the built-in public and private key cryptography enables the network to assign trusted digital identities to all parties at scale. Each participant has its own public-private key pair that is not controlled by the issuing party. The keys do not need to be reissued if the enterprise has multiple TNs, multiple OSPs, ports a TN or if the issuing party root key has been compromised.
  - Improve productivity managing digital identities across the ecosystem.
  - New business opportunity for the service provider to be a custodian for the enterprise.
  - Reduced complexity, managing revocation lists at scale.

Identity management

With more and more business transactions being conducted online, it no longer makes sense to rely upon physical documents as the only means of establishing the identity of a user or object. Distributed ledger technology enables enhanced characteristics in how digital identity is both managed and used, while moving beyond the limitations of being operated by one institution. An example metric is improved retention rate.
Enterprise Identity Value Creation:

- Enterprises are able to upload and sign digital documents for KYC verification, where the hash of the signed documents is stored on the ledger, enabling any KYC vetter to authorize them. Once authorized, the enterprise is able to use its digital identity to conduct business transactions (e.g., attain TNs, telecom capacity) while also verify originating calls being placed into carriers’ networks.
  - Creates new business models, using the enterprise digital identity across the whole supply chain to transact in business services not only call verification.

Marketplace Creation

Distributed ledger technology improves confidence in products and services in the marketplace, while also using a shared ledger, smart contracts and digital assets to facilitate real-time peer-to-peer transactions. An example metric is new markets created.

Enterprise Identity Value Creation:

- Using the distributed ledger enables enterprises to transact with any TN vendor or business partner to place calls and connect with any OSP while maintaining the integrity of the service for all. This creates an open marketplace to securely verify and trade across the network of parties.
  - Increase adoptions through network effect of parties connected on the ledger.
  - Increases value and integrity of the service by mass adoption.
  - Creates new revenue opportunities leveraging open marketplace.

New and Enhanced Products and Services

The technology’s unique capabilities are creating the foundations to enhance existing products and services and create new ones. New digital assets can exist beyond the umbrella of one organization, company or government. How organizations offer and manage those products and services is evolving, giving power back to the creators and consumers.

Enterprise Identity Value Creation:

- The enterprise identity network of digital identity, verification service and unique assets can easily support other services using telephone numbers such as SMS messaging and RCS, marketing and contact services. Other assets can be managed by the enterprise identity network, including IoT trusted data, consumer KYC data and opt-in preferences. The same platform can support carrier network identity verification and virtual asset trading including, NFV, SDN and grid networks.
  - Enhanced Identity across all telecom services.
  - New value creation from consumer identity and consent services.
  - Open marketplace for secure trading of telecom virtual assets.
New and Expanded Partnerships

With the increased confidence in data afforded by distributed ledger, new partnerships can be formed more easily. Many of these partnerships can have automated components, as well, by exploiting digital assets and smart contracts. An example metric is new distribution channels.

Enterprise Identity Value Creation:

- The enterprise identity network is not limited by national borders. Through managed governance controls, the network can provide a global service. For example, when consumers are roaming abroad, they want to experience the same secure contact service as at home. Likewise, the same governance controls enable the network to include new enterprise business types looking to trade trusted identity and secure virtual assets from a carrier.
  - Increases the reach of services capabilities, to incorporate new customers and partners.
  - Improves customer affinity, with seamless user experience.
ATIS Distributed Ledger Technology Project

The ATIS Distributed Ledger Technology (DLT) project was initiated to validate key aspects of DLT as it applies to real-world challenges facing today’s communications industry. From a number of potential use cases, one was selected for a more in-depth analysis and proof of concept. This specific use case defined as Enterprise Identity Network addresses the current challenges with trusted Enterprise Identities and their legitimate use of a Telephone Number (TN) in complex Enterprise call scenarios.

For more information about the ATIS DLT project, visit https://www.atis.org/01_strat_init/dlt/.