

ATIS-I-0000084

ATIS Technical Report on

ATIS-I-0000084: Enterprise Identity Distributed Ledger Network

Providing Enterprise and Telephone Number Allocation Authentication for Originating Service Provider SHAKEN Attestation



Alliance for Telecommunications Industry Solutions

Approved July 15th, 2021

Abstract

Consumers worldwide have been inundated with illegal robocalls and other unwanted calls to the point that by some estimates, a large percentage no longer answer their phones. This makes it difficult for legitimate businesses to reach consumers in a timely manner with important information, alerts and reminders. Those businesses also bear the expense of follow-up calls and other outreach. Meanwhile, service providers bear costs such as fielding customer complaints and investigating sources of fraudulent traffic.

This Technical Report describes a specification that extends the capabilities of SHAKEN to provide the ecosystem with new options for mitigating illegal robocalls. In addition, it features a distributed ledger infrastructure called the enterprise identity network.

The specification enables an enterprise to establish enterprise identity credentials by applying distributed ledger technology and its cryptographic principles. The enterprise then can place calls signed with its enterprise identity credentials, enabling any originating service provider (OSP) receiving the call to authenticate the enterprise identity of the calling enterprise. When the OSP can authenticate the calling enterprise identity and the originating TN is authorized for use, the OSP can apply SHAKEN A-level attestation to the call.

Foreword

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 most pressing business priorities. ATIS' nearly 200 member companies are currently working to address the all-internet protocol (IP) transition, 5G, network functions virtualization, big data analytics, cloud services, device solutions, emergency services, M2M, cyber security, 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). The organization is the North American Organizational Partner for the 3rd Generation Partnership Project (3GPP), a founding partner of the oneM2M global initiative, a member of and major U.S. contributor to the International Telecommunication Union (ITU), as well as a member of the Inter-American Telecommunication Commission (CITEL). For more information, visit www.atis.org.

The Alliance for Telecommunications Industry Solutions (ATIS) serves the public through improved understanding between carriers, customers, and manufacturers. The ATIS DLT Focus Group 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. The Enterprise Identity Network use case addresses current challenges differentiating robocalls from legitimate calls placed by enterprises.

Suggestions for improvement of this document are welcome. They should be sent to the Alliance for Telecommunications Industry Solutions, [DLT Focus Group], 1200 G Street NW, Suite 500, Washington, DC 20005.

Table of Contents

1	Scope & Problem Statement	1
1.1	Scope	1
1.2	Problem Statement	1
2	References	3
3	Definitions, Acronyms & Abbreviations	4
3.1	Definitions	4
3.2	Acronyms & Abbreviations	6
4	Overview	8
4.1	Enterprise Identity Distributed Ledger Network Interworking with SHAKEN Architecture	13
4.2	Overview of Self-Sovereign Identity (SSI)	13
4.3	Overview of Decentralized Identifier	14
4.4	Overview of Verifiable Credentials	16
5	Enterprise Identity Management on Distributed Ledger	17
5.1	Creation of a Decentralized Identifier DID and recording of the EIDL	17
5.1.1	Identity Creation API	18
5.2	Identity Vetting Trust Authority Hierarchy	19
5.3	Identity Vetting Authorization Verifiable Credential	20
5.3.1	Enterprise Identity Vetting Status	23
5.3.2	Organization 'rcd' Identifiable Information Verifiable Credential	24
5.3.3	Organization Vetting API	27
5.3.4	Organization rcd Claims Vetting API	27
6	TN Authorizations	28
6.1	Assignment of a TN by TNSP to TNR or Brand	32
6.2	Delegation of a TN by TNR to Brand / Brand to BPO	36
6.2.1	Delegation of a TN by Brand to BPO	40
6.2.2	TN Authorization API	46
6.3	TN Cancel and Revocation - Credential Claim Status	47
7	OSP Attestation of a call using EIDLN	48
7.1	Enterprise PASSporT Encoding	50
7.1.1	Use of a Modified Base PASSporT Encoding for Enterprise Identity	50
7.1.2	Use of a Modified "rcd" PASSporT Encoding for Enterprise Identity	51
7.2	Enterprise PASSporT Verification Procedure	52
7.2.1	OSP Verification using a modified base PASSporT	52
7.2.2	OSP Caller Verification API	54
7.2.3	OSP Verification Using a modified "rcd" PASSporT	55
7.2.4	OSP Caller Verification API	57
8	Traceback using Enterprise Identity	58
8.1	Principle #5. Confirm the Identity of Commercial Customers	58
8.2	Principle #6. Require Traceback Cooperation in Contracts	60
9	ANNEX A: Example of Open API for EIDL	61
9.1	Organization Accounts	61
9.1.1	createAccount	61
9.1.2	getAccount	63

ATIS-I-0000084

9.2	Vetter.....	65
9.2.1	createVettedOrganizationOnDLT	65
9.2.2	getVettedOrganizationAuthorization	68
9.2.3	createOrganizationVettedRcdOnDLT	70
9.3	TNAuthorization	71
9.3.1	createTnAuthrizationOnDLT.....	71
9.4	OSP Verification	75
9.4.1	callerVerification	75
9.4.2	verifyOrganizationVettedRcd.....	78
Contributors to this report.....		79

Table of Figures

Figure 4.1	EIDLN Services Supporting SHAKEN Attestation	8
Figure 4.2	EIDLN to Attest a TN.....	10
Figure 4.3	EIDLN Organization Actors	11
Figure 4.4	EIDLN Interworking with SHAKEN Architecture	13
Figure 4.5	DID Format - Example Sovrin Network Method) Compared to URN Format.....	14
Figure 5.1	Creation of DID on EIDLN	17
Figure 5.2	API Flow Creation of DID on EIDLN	18
Figure 5.3	EIDLN Trust Hierarchy	19
Figure 5.4	Request Org to be KYC Vetted and Create Vetted VC Claim	21
Figure 5.5	API Flow for OOB Request to be Vetted.....	27
Figure 5.6	API Flow for OOB Request for rcd Claims to be Vetted.....	27
Figure 6.1	TN Authorization Hierarchy	30
Figure 6.2	TN Authorization VC on EIDLN.....	31
Figure 6.3	TNSP-to-TNR TN Assignment.....	32
Figure 6.4	TNR-to-Brand TN Delegation – VC.....	36
Figure 6.5	Brand-to-BPO TN Delegation	40
Figure 6.6	API Flow for TN Authorization	46
Figure 7.1	Enterprise Identity from EIDLN to Provide OSP A-Level Attestation	49
Figure 7.2	OSP Verification of an Originating Caller Using a Modified Base PASSporT	53
Figure 7.3	API Flow for OSP Caller Verification from Modified Base PASSporT.....	54
Figure 7.4	OSP Verification of an Originating Caller Using a Modified rcd PASSporT	56
Figure 7.5	API Flow for OSP Caller Verification from Modified rcd PASSporT.....	57
Figure 8.1	KYC Vetter Creation of Commercial Identity Credential Claim.....	59
Figure 8.2	Using the VC Commercial Identity to Prove with Multiple Actors	59
Figure 8.3	Traceback of Robocaller Identity Using EIDLN	60