**ATIS-0x0000x**

ATIS Standard on

**Signature-Based Handling of Asserted Information Using Tokens (SHAKEN):**

**Campaign Tokens**

**Alliance for Telecommunications Industry Solutions**

Approved Month DD, YYYY

**Abstract**

This technical report defines mechanisms that enable a Service Provider to delegate STI authentication authority for a subset of its TNs to another entity. This delegation capability is needed to support STI for cases such as multi-homed SIP-PBXs, where the authorized owner of a TN does not provide originating call services for that TN.

**Foreword**

The Alliance for Telecommunications Industry Solutions (ATIS) serves the public through improved understanding between carriers, customers, and manufacturers. The [**COMMITTEE NAME**] Committee [**INSERT MISSION**]. [**INSERT SCOPE**].

The mandatory requirements are designated by the word *shall* and recommendations by the word *should*. Where both a mandatory requirement and a recommendation are specified for the same criterion, the recommendation represents a goal currently identifiable as having distinct compatibility or performance advantages. The word *may* denotes a optional capability that could augment the standard. The standard is fully functional without the incorporation of this optional capability.

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

At the time of consensus on this document, [**COMMITTEE NAME**], which was responsible for its development, had the following leadership:

[**LEADERSHIP LIST**]

The **[SUBCOMMITTEE NAME]** Subcommittee was responsible for the development of this document.

**Revision History**

| **Date** | **Version** | **Description** | **Author** |
| --- | --- | --- | --- |
| Jun 13, 2019 | Initial | Baseline | Tolga Asveren |

**Table of Contents**

1 Scope, Purpose, & Application 1

1.1 Scope 1

1.2 Purpose 1

2 Normative References 2

3 Definitions, Acronyms, & Abbreviations 2

3.1 Definitions 2

3.2 Acronyms & Abbreviations 2

4 Overview 3

4.1 Strategy 3

4.2 Operational Steps 3

Campaigner applies at the Authority for permission to place robocalls for a specific campaign. 3

The application is either approved or denied. 3

If approved, tokens are provided to the Campaigner. Multiple tokens may be provided for a single campaign. For example, 240 tokens may be provided for a 10 day campaign with each having a validity period of 1 hour. 3

These steps could be automated or performed out-of-band. 3

This procedure is similar to approval process for a credit card application. 3

4.3 Mechanism 3

4.3.1 Verification Procedure 3

4.3.2 Security Concerns 4

4.3.3 Non-Supporting entities 4

4.3.4 Call Flow 5

A Annex Title 5

**Table of Figures**

Figure 1 High Level Flow of Events 5

**Table of Tables**

# Scope, Purpose, & Application

## Scope

## Purpose

The purpose of this document is enabling Network Analytics (NA) use of a “legitimate robocall/campaign call indicator” (LRC-id)during its analysis. In general NA can be modeled as a function with various input parameters. These may include originating calling party information, whether the originating calling party information is successfully verified through STIR/SHAKEN procedures, signaling message content/patterns, media content, information about the path taken by the signaling message etc… “. LRC-id would be another parameter which may be utilized by NA. This mechanism is not meant to be a strongly secure procedure to rely on but is expected to increase the quality of analysis when it is used.

# Normative References

# Definitions, Acronyms, & Abbreviations

## Definitions

The following provides some key definitions used in this document.

**Campaigner:** The entity placing robocalls for a legitimate reason.

**Authority:** The entity deciding whether a Campaigner is entitled for placing legitimate robocalls. An Authority’s decision is limited to its own domain. It does not need to be the central regulating organization in a jurisdiction domain. For example, an Operator-A can act as Authority for its own domain and Operator-B can act as Authority for its own domain. Federation among multiple operators to form a single Authority domain is also possible.

**Verifier:** The entity verifying that “legitimate robocall indicator” is valid

## Acronyms & Abbreviations

**LRC-Id:** Legitimate Robocall Identifier

|  |  |
| --- | --- |
| A-JWT | Authority generated JSON Web Token for Legitimate Robocall Identification |
| C-JWT | Campaigner generated JSON Web Token for Legitimate Robocall Identification |
| LRC-Id | Legitimate Robocall Identifier |

# Overview

## Strategy

The mechanism relies on temporary delegation of trust through use of “long term tokens” to the Campaigner. Furthermore “short term tokens” generated by Campaigner are used to decrease possibility of abusive reuse of tokens.

## Operational Steps

### Campaigner applies at the Authority for permission to place robocalls for a specific campaign.

### The application is either approved or denied.

### If approved, tokens are provided to the Campaigner. Multiple tokens may be provided for a single campaign. For example, 240 tokens may be provided for a 10 day campaign with each having a validity period of 1 hour.

A Campaigner may get tokens for the same campaign from multiple Authorities. This could be used for cases where the call can be verified in different Authority domains.

### These steps could be automated or performed out-of-band.

### This procedure is similar to approval process for a credit card application.

## Mechanism

Two JWT tokens are used

A-JWT: JWT generated by the Authority

- More than one token can be generated for the same campaign splitting it into multiple periods.

C-JWT: JWT generated by the Campaigner

A-JWT Content:

- Authority id

- Campaigner id

- Campaign id

- Campaigner public key (matching the Campaigner private key. This key pair is generated by Campaigner)

- Validity period

- Quota (optional)

- Signature (signed by Authority private key)

C-JWT Content:

- Timestamp (signed by Campaigner private key)

- Orig-id

- Dest-id

### Verification Procedure

Verifier possesses Authority public key.

#### - A-JWT signature is verified by using the public key of the Authority

#### - A-JWT validity period is verified

#### - C-JWT signature is verified by using the public key provided in A-JWT Campaigner public key field

#### - C-JWT Timestamp is verified against local time. It would be considered as valid for a duration of 60s.

#### - C-JWT Orig-id is verified against calling party information

- C-JWT Dest-id is verified against called party information

#### - Optionally, Quota can be checked against locally kept usage metric to prevent excessive abuse

#### - Optionally token is sent to an Authority Aggregation Point. There, all tokens associated with a campaign can be aggregated and verified that they didn’t exceed the allocated quota. The result of this operation can be used as input when granting/denying future applications from the same Campaigner.

### Security Concerns

An attacker can reuse a token pair during its validity period/60s period after its timestamp. It needs to place the call with the calling party information matching the orig-id/dest-id though. Considering that the easiest way for the attacker to obtain the token is to be the “target” of a campaign, i.e. attacker gets the token which is not stripped off by the network as the destination party of the call, dest-id check adds significant value.

Call diversion related semantics/security concerns which are applicable for STIR/SHAKEN calling party identification apply (To be studied further…)

### Non-Supporting entities

If a Campaigner does not use LR-I then its calls would be subject to existing analysis functionality which does not make use of LR-I.

If a Verifier does not make use of LR-I then it would use existing parameters for verification.

In other words, everything would be the same as before for non-supporting entities.

If a Verifier, which is able to use LR-I, does not receive LR-I then it would apply existing procedures as is. There won’t be a degradation in quality of call classification.

### Event Flow



Figure High Level Flow of Events

# A Annex Title

Xxx