**IPNNI-2016-00009R001**

**ATIS-0x0000x**

ATIS Standard on

**Verification Token Use Cases**

**Alliance for Telecommunications Industry Solutions**

Approved Month DD, YYYY

**Abstract**

Abstract text here.

**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** |
| --- | --- | --- | --- |
|  |  |  |  |

**Table of Contents**

[INSERT]

**Table of Figures**

[INSERT]

**Table of Tables**

[INSERT]

# Scope, Purpose, & Application

## Scope

xxx

## Purpose

xxx

## Application

xxx

# Normative References

The following standards contain provisions which, through reference in this text, constitute provisions of this Standard. At the time of publication, the editions indicated were valid. All standards are subject to revision, and parties to agreements based on this Standard are encouraged to investigate the possibility of applying the most recent editions of the standards indicated below.

ATIS-0x0000x, *Technical Report*.

ATIS-0x0000x.201x, *American National Standard*.

# Definitions, Acronyms, & Abbreviations

For a list of common communications terms and definitions, please visit the *ATIS Telecom Glossary*, which is located at < <http://www.atis.org/glossary> >.

## Definitions

**AAA**: xxxx.

**Bbbb**: xxxx.

## Acronyms & Abbreviations

|  |  |
| --- | --- |
| ATIS | Alliance for Telecommunications Industry Solutions |

# Main Body of Standard

Figure X illustrates authentication relationships that may utilize the Verified Token capability.



Editor’s Note: Add subsection for Gaps

## Use Cases

Xxx

All the scenarios discussed in this document are of calls originating and terminating within the US; i.e., not addressing calls from outside the country.

### Verification of Calling Party Number

Xxx

Phone scams that target consumers for banking information are surging. The scammers are exploiting the vulnerabilities of IP caller ID – namely spoofing. Spoofing allows the fraudster originating the call to send a caller ID that the recipient trusts, such as their bank’s phone number. With the trust established, the fraudster is able to collect sufficient personal information and answers to security questions. Mobile users are lured into divulging this information via text messages that appear to come from their bank(s).

Armed with the necessary information of the victim, the fraudster places a call to the bank with the caller ID of that victim. That results in tricking the bank Customer Relations Management (CRM) systems into treating the fraudster as the real customer. Most of these systems were designed to recognize the incoming caller ID (not ANI), and launch the customer’s account information to improve the customer experience and to reduce wait times. Spoofers armed with the correct answers to security questions will be able to trick the bank employees into transferring money to the spoofers’ accounts.

1. Role of Originating SP

The role of the originating SP is critical in the chain of authentication and verification of the call.

* The originating SP must ensure that the telephone address inserted in the outgoing INVITE is authorized to initiate that call, utilizing the knowledge in its operations support systems, etc.
* The originating SP must employ a PKI certification process and use it to sign authorized outgoing calls, as described in [RFC 4474bis-07]

Similarly, SIP-based softphone packages installed on mobile phones should be expected to adhere to the same guidelines of RFC 4474-bis. These applications typically assign a dedicated TN to each user, since most users use those numbers for business purposes even if the call is launched from a cellphone with a separate TN.

The entity assigning these numbers is expected to employ a PKI certification process to sign the outgoing caller identification information, if it is to be treated as a trusted player.

The banking example is only one of many spoofing scenarios, but one of the more detrimental since most banks do not cover the losses for those defrauded customers.

Editor’s Note: Consider new use case for delegation

1. Role of Terminating SP

The terminating SP plays an important role in the final stage of the caller ID service – delivering and displaying the caller’s information. In an IP environment, the terminating SP has a new role.

* The terminating SP must be able to verify that the signature of the received VT header is valid based on the provided credentials in the VT claim. If the signature is valid, the data in the “orig” field of the VT Claim should be delivered as the Calling Party Number to the end user.
* The terminating SP must employ a method for assessing the level of confidence in the received calling number information and conveying that assessment to the called user in a meaningful form,
* The terminating SP will need to educate its customers on this new spoofing assessment tool and how customers should interpret the display to reduce their exposure to fraud.
  + *Author’s note: Expand on suggested categories from Pierce Gorman’s suggestions: no credentials, carrier signed but no authentication of CgPN, carrier signed but semi authenticated, carrier signed and authenticated.*
* The terminating SP also has the option to query authoritative, trusted databases to request information on the received TN, such as type of service and the service provider responsible for that number (account owner), to bolster its overall assessment.

#### SIP

#### WebRTC

### Verification of Call Delivery

The caller typically recognizes the TN of the party they are trying to reach and trusts he/she will reach the intended party. Exceptions would include a classified call where the caller needs to ensure the station/device they reach is the intended one. This is not a verification of the identity of the person answering the call but verification that the call was terminated to the station/device authorized to use that called TN.

To assist in verifying the called party, the response to the INVITE could either be:

* A 18x response (e.g., 183 Session Progress) Reason-Phrase, or message body that conveys:
  + The called party’s authorization to use that TN, and, optionally,
  + The disposition of completing the call to the called TN. For example, if the called party does not accept the credentials of the calling party because of suspected spoofing, the 183 response would communicate the status back to the calling party.

Editor’s Note: address forwarding scenario

Xxx

#### SIP

#### WebRTC

### Verification of Originating Service Provider

xxx

### Verification of Terminating Service Provider

xxx

### Verification of Transit Service Provider

xxx

### Verification of Emergency Telecommunication Services (ETS) Authenticating Service Provider

#### Description

National Security/Emergency Preparedness (NS/EP) is made up of two service access types GETS and WPS. GETS authentication uses PIN verification and WPS is a subscription based service where the service is invoked on a per session basis triggering on a prefixed feature code.

NS/EP provides priority of network resources on a per call basis in order to a select group of Government users. When call/sessions transverse two service providers, there is a need for the receiving network to verify that the user was authenticated by a valid NS/EP service provider.

Once authenticated the Resource Priority Header (RPH) is added to the SIP INVITE. It is proposed that the RPH is signed with the token.

#### Call Flow

Tbp

### Verification of Information Service Provider

Information Services are provided by Application Providers, as shown in Figure 1.

#### Call/Session Associated

Examples of an Information Services are Calling Name, LIDB, Toll Free, etc ….

TN-based data related to CNAM, eCNAM or Identity Verification services, is not always stored in the same network as the end user authorized to use that TN. Therefore, verifying the service provider responsible for that TN does not provide any verification of the information provider that stores and manages user data for that TN.

However, in most scenarios, the data exchange takes place via a private or virtual private connection. The relationship between the information provider and the data requester is governed by contractual agreements. The IP addresses and identifiers of both entities (information provider and data requester) are exchanged to verify the access rights of the requester to the data source. Unlike a call or media session where no prior identification is needed to place the call, this type of data exchange operates securely without the need for a Verified Token.

#### Non-Call/Session Associated

zzz

### Verification of Messaging

xxx

#### SIP

#### SMS

### Verification of SIP Subscribe/Notify

xxx

### Verification of SIP PUBLISH

xxx

#### Subclause Heading 4

Xxx

### Conference Calling

xxx

### Toll Free

Xxx

### E911

Xxx

### Alternate Caller-ID

#### Description

A caller places a call; the caller ID of the outbound call is replaced by a different number, such as the caller’s office number, a toll-free number, or a pre-set string. The originating service provider is able to verify the authority of the caller to use the requested displayed caller ID and provides the attestation that the caller is authorized to use the number for caller identity. The terminating network uses the caller identity credentials provided by the originating operator to verify that the caller identity is a valid use.

**Annex A**

(normative/informative)

# A Annex Title

Xxx