**ATIS/SIP Forum IP NNI Task Force**

**Bellevue, WA**

**May 8-11, 2017**

**Contribution**

**TITLE: Proposed Guidelines for discussion on the Display of Verified Caller ID**

**SOURCE\*: Hala Mowafy (Ericsson)**

**ISSUE NUMBER:**

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**Abstract**

This contribution introduces basic display guidelines (as marked text) in sections 6 and 7 of the *“Technical Report on a Framework for Display of Verified Caller ID”* [IPNNI-2017-00019R2].

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**ATIS-0x0000x**

ATIS Standard on

**ATIS Technical Report on a Framework for Display of Verified Caller ID**

**Alliance for Telecommunications Industry Solutions**

Approved Month DD, YYYY

**Abstract**

This document provides a Technical Report on Originating Party Spoofing in IP Communication Networks. It describes problems associated with originating party spoofing in IP communication networks, identifies potential mitigation options, analyze pros and cons of mitigation options.

**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

This technical report provides a framework for signaling verified Caller ID information from the network to a User Equipment (UE), and displaying the information on the UE in a uniform manner, independent of technology.

## Purpose

## Application

.

# 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.

# 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

**Caller identity:** The originating phone number included in call signalling used to identify the caller for call screening purposes.In some cases this may be the Calling Line Identification or Public User Identity. For the purposes of this study, the caller identity may be set to an identity other than the caller’s Calling Line Identification or Public User Identity.

## Acronyms & Abbreviations

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

# Architecture

Editor’s note: add figure illustrating various access technologies and a variety of device types (UEs).

# Signaling of Verified Caller ID

## Signaling of Verified Caller ID using Conventional Caller Name (CNAM)

Editor’s Note: Items that need further consideration are trust in the source of the Caller ID data, security considerations, limitations on the 15 characters, impacts on current infrastructure, and consumer education.

In its simplest form, a service provider performing the 4474bis verification process, on behalf of one of their subscribers, will make a binary determination whether a call received is from a trusted source or not. Such a determination can be signaled from the network to a User Agent (UA) via a single alphanumeric character.

Today, infrastructure support for conventional Caller Name (CNAM) services across the United States is, for all practical purposes, ubiquitous. Conventional CNAM supports a 15 alphanumeric character field that is already signaled from IP/TDM networks and displayable on a broad range of wireline and wireless consumer and business devices today. In IP networks, CNAM is signaled in the Display Name portion of either the SIP From or P-Asserted-Identity header.

In an effort to accelerate adoption of Verified Caller ID, service providers should evaluate the use of conventional CNAM as a vehicle for signaling verification status to UAs. For service providers, this approach highly leverages an established ecosystem infrastructure. More importantly, it affords the opportunity to immediately begin signaling Verified Caller ID status to the broadest set of subscriber devices once network implementations are established.

There is a range of implementation options that can be considered. Two simple examples are:

1. The service provider performing the 4474bis verification process appends a designated alphanumeric character to the end of the “published” 15 character CNAM for a verified Caller ID (e.g., JOHN DOE\*)
2. This service provider appends a designated alphanumeric character to the beginning of the “published” 15 character CNAM for a verified Caller ID (e.g., \*JOHN DOE)

Note that the “\*” in the simple examples above is meant to verify the Caller ID (telephone number) in the associated SIP URI and not the displayed CNAM itself. There are other established commercial practices and policies around the subscriber information used in CNAM services, how it is obtained and how quickly it is updated in authoritative databases.

As validated through actual testing, the examples above afford at least two, immediate to near term device implementation approaches:

1. An existing device of a subscriber that supports conventional CNAM can just display what is signaled, e.g., “JOHN DOE\*” (as further discussed below, some agreement across service providers would simplify the subscriber education process)
2. A device operating system or application party can interpret the “\*” and enhance the display to the subscriber as illustrated in the below (i.e., the black padlock within the green circle):



Given the above introduction and explanation, the following addresses some questions that may arise:

1. If a single alphanumeric character is used from conventional CNAM, existing 15 character CNAMs need to be addressed. Further, the selected character should not be used in existing CNAMs or be used in only a small percentage of CNAMs. However, it would seem that receiving Verified Caller ID status adds much more value even though this impacts originating subscribers who, on the other hand, also receive calls.
2. This approach doesn’t assume that a “published” CNAM exists (e.g., “UNKNOWN NAME”) or that a subscriber wants to remain anonymous. Again, the approach leverages an established ecosystem infrastructure to quickly deliver Verified Caller ID status to the broadest set of subscriber devices.
3. An initial draft IETF document, “PASSporT Extension for Caller Name”, proposes a way to broaden the identity claim to include CNAM that may be inserted at call origination. Thus, this approach is extensible in the future to not just verifying Caller ID but also the associated, displayed CNAM.
4. ATIS IP-NNI has recently started discussing the desire to signal more information to the UA about the verification status. However, at this time, it seems like any such approach would require changes by UAs to interpret and act on such information. The near term approach above is meant to accelerate implementations and signal the most critical piece of information to the subscriber device. Note that another simple approach, for example, could be to use a single, numeric value between zero and nine, thus supporting up to ten possible statuses to be signaled.
5. Most any approach will require some subscriber education. For devices that simply display what is sent to them, subscribers will need to understand how their traditional display has changed. Such education can be greatly simplified if ATIS IP-NNI could agree on a uniform approach.
6. Accurate CNAM, along with Verified Caller ID, forms a foundation for building a much better subscriber phone experience. Coupling these together is intuitive as many business to consumer calls are not identifiable enough today to be consistently answered. Further, simple policy rules, which are increasingly being supported in the existing CNAM infrastructure, can be defined to modify the signaled CNAM based on the verification status. For example, a non-Verified Caller ID with an “UNKNOWN NAME” could be signaled as “UNVERIFIABLE” in the Display Name portion of either the SIP From or P-Asserted-Identity header

In summary, in response to accelerated timelines from regulators to address robocalling and spoofing, conventional CNAM affords service providers an opportunity to efficiently signal Verified Caller ID status to the broadest set of existing subscriber devices as soon as network implementations are deployed. Although positioned as a near term approach, it is extensible in multiple ways to support innovative ways to further enhancing the subscriber call experience.

## Pros and Cons of Signaling Special Indicators in Conventional Caller Name (CNAM) Display

While the intent of the proposal in 5.1 is to expedite the availability of a TN verification indicator reusing the existing infrastructure – a pro – the claimed benefits may produce some risks.

The proposal in 5.1 calls for the modification of the display-name portion, by appending or prepending the name with a special character. The drawbacks include the following:

* Extensive consumer education will be necessary for this idea to be of value to the consumer
* Despite the desire to expedite the availability of the verification information, this special character cannot be used until the STIR/SHAKEN methodology is implemented in the network. Therefore, the question is: what will this indicator expedite?
* The use of a visible character to convey a security status is not a good practice because it could be easily imitated by scammers.
* If consumers are taught to trust the ‘\*’ and an unverified number is received with a tampered name-display containing “\*NAME”, the contradictory information will only confuse the customer and lead to more service complaints to the carrier.
* If the proposal is intended for the short term, what is the expected time frame and would the short term value justify the extensive consumer education and the logic changes afterwards (when it is no longer needed)?

# Display Requirements

To harness the value of the SHAKEN STI mechanism and the related analytics, the summation or “rundown” about the caller should be delivered to the called party based on human factors and internationally accepted standards for design and colors (such as ISO Graphical Symbols) should be emulated / taken into consideration in the development of the new displays.

## Basic Display Rules

The following is a summary of good practices to follow in designing the message for display on the handset screen:

* Symbolic messages are more effective than verbal ones.
* Verbal messages should be succinct and easy to comprehend
	+ Simple imperatives are easier to follow for low-skilled readers
	+ *Carriers may consider providing such messages as : “do not answer” for unauthenticated calls, etc.*
* Colors and Suggested text:

|  |  |
| --- | --- |
|  | Symbolic Messages |
| A Yellow triangle serves as a warning sign | Image result for safety symbols |
| A Green square identifies safe conditions | Image result for green square |
| A Red ring with a diagonal bar serves as a general prohibition of some action that could result in harm  | Related image |

* Flashing text captures attention for important messages

## Proposed Guidelines

### Relaying Attestation Levels to End Users

The PASSport extension includes an attestation indicator provided by the originating network on the status of the calling number. Currently, there are three levels of attestation that should be part of the final assessment being presented to the user.

The levels of attestation are described below.



Signaling this information is described in 3GPP TS 24.229.

In the P-Asserted-Identity header, the "verstat" tel URI parameter may be mapped to the Screening Indicator as follows:

* “No-TN-Validation” to “user provided not verified”;
* “TN-Validation-Passed” to “user provided, verified and passed”; and
* “TN-Validation-Failed” to “user provided, verified and failed.”

Call management services have traditionally relied solely on the signaled information to determine what is presented to the end user. That information has typically been provided by the originating service provider and was based on “network” information.

In the new generation of IP-based services, the signaled information is not the only factor in determining what gets displayed to the end user. Customers may subscribe to services that take advantage of all available information about the caller. Big data algorithms draw on data from many sources, such as caller reputation, robocaller databases, black lists, white lists, and more.

#### Display based on Attestation Only

|  |  |  |
| --- | --- | --- |
| If the received Screening Indicator is… | The Symbolic Message should be… | Suggested Verbal Messages  |
| 1. user provided not verified
 |  | * Dubious
* Not confirmed
* Questionable
* Unreliable
 |
| 1. user provided, verified and passed”
 | Related imageRelated image | * Certified
* Authenticated
* Confirmed
* Ok! Answer
 |
| 1. user provided, verified and failed”
 |   | * Scam
* Risky
* Be wary
* Don’t Answer
* Decline
* Reject
 |

Table 1. Symbolic Messages

#### Display based on Attestation and Analytics Combined

* If the attestation level is **“User provided, verified and passed,”** the verified calling identity should be displayed with a symbolic message equivalent to the one listed in Table 1, item B. The additional information available from analytics (e.g., type of call) should be displayed along with the calling identity.

*Discussion: What if the caller is authorized to use this number, but is operating an illegal robocalling business? For the short term – until detected, reported and action is taken - analytics may assist with such scenarios. If analytics conflict with the attestation, which should take priority?*

* If the attestation level is **“user provided, not verified,”** the calling identity should be displayed with a symbolic message that alerts the user to the questionable nature of the call, along with a symbolic and verbal message equivalent to the one listed in Table 1, item A. The additional information available from analytics should be displayed along with the calling identity.
	+ If the results of analytics confirm that the caller is on a white list service for the called party, the symbolic and verbal messages should be changed to those shown in item B (
* If the attestation level is **“user provided, verified and failed,”**
	+ The call may be blocked, as part of the service the customer subscribes to, and therefore, no display would be needed.
	+ The call may be presented to the customers along with a symbolic and verbal message equivalent to the one listed in Table 1, item C. The additional information available from analytics should be displayed along with the calling identity.

#### Display based on Analytics Only

[TBD]

# Related SDOs and Fora

## 3GPP

### Enhanced CNAM

Enhanced CNAM (eCNAM) offers a standard vehicle for delivering the results of any independent analytics. eCNAM is described in ATIS-1000067.2015 and in 3GPP TS 22.173 V15.1.0 (2016-12).

Analytics provide a valuable, new source of call management data for the user. Therefore, to avoid incompatibility issues with different operating systems (OS) of different UEs, the enhanced CNAM service delivers the additional information from analytics in standard Call-Info headers instead of proprietary messages to each UE.

eCNAM Call-Info headers support the delivery of

* plain text that could be used to summarize the analytics results, and
* icons that could be used to display the symbolic messages

## GSMA

## Cable Labs

## Consumer Electronics

# Conclusions

**Annex A**

(normative/informative)

# A Illustrative Examples

This annex will document supportive material



