**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.

Editor’s Note: This is a living document and the guidelines will evolve with deployment and operational experience. It is anticipated that output from usability studies will be contributed to this work.

## 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.

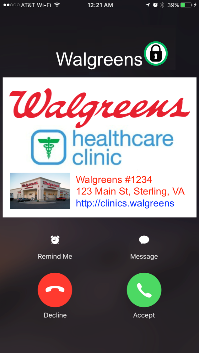
There is a range of implementation options that can be considered. Two simple examples are:

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 Guidelines for All IP Networks and Devices

With the implementation of STIR/SHAKEN and certificate governance models, specific data will be signaled between networks which could help assess the risk associated with each call.

It is important to realize that this information signaled between networks (such as attestation levels and certification information) is **not meaningful or suitable to be displayed to the end user**. However, when further analytics are applied to that information, a more useful "communication" can be formulated and presented to the end user.

The factors contributing to the final display and the possible display options are the subject of the present document.

The guidelines in the present section are provided for screen-based devices, such as smartphones, operating an all-IP network.Considerations for other scenarios of analog devices served by IP networks, or by circuit-switched networks will be discussed in Section 7.

## Entities that shape the display

Multiple entities contribute to the ultimate message delivered to the user about the trust level of incoming calls.

Each entity may be responsible for specific data that is signaled, processed, or displayed at different points in the call setup.

Editor's Note: This section proposes the following entities as the key contributors to the ultimate display and the role each one plays. Other entities may be added in the future, if deemed necessary.

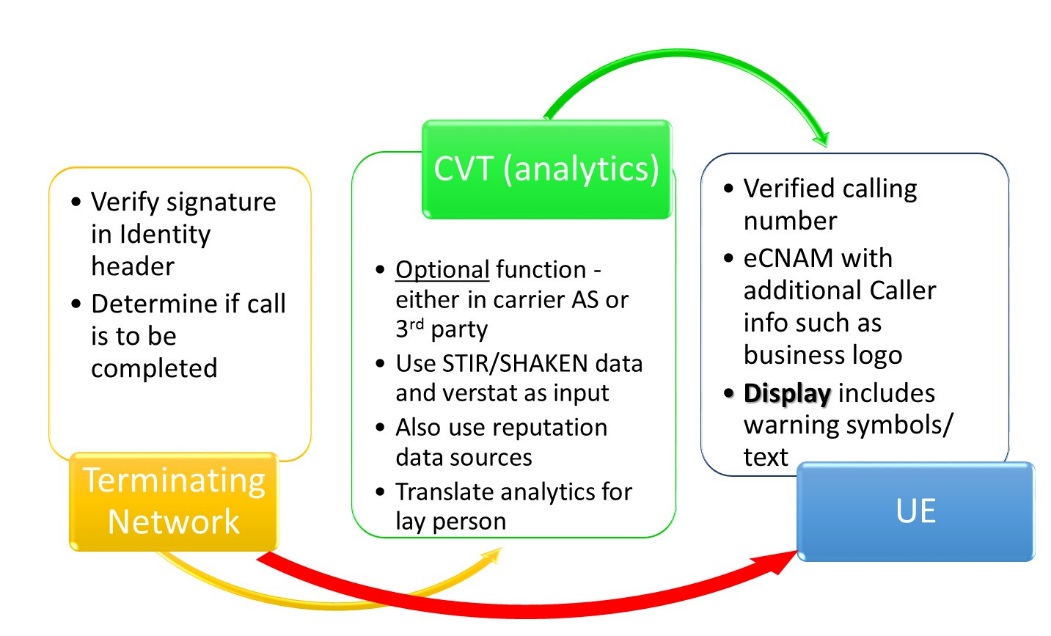


Figure 2. Entities Contributing to Ultimate Display

### IP Network

The originating network is responsible for signaling the Identity header containing the pertinent claims and attestations about the calling number, per draft-ietf-stir-rfc4474bis and ATIS-1000074.

The terminating network is responsible for verifying the received claims. Results of the verification are inserted by the AS in the "verstat" tel URI parameter (defined in 3GPP TS 24.229) to provide the UE with the calling identity number verification status in an initial INVITE request.

### Call Validation Treatment (CVT) or Analytics

CVT is a function that analyzes data to ascertain the level of risk associated with the incoming call. CVT may be implemented as part of the terminating network (e.g., in an AS) or by a third-party that partners with the service provider, or in association with a UE application. CVT applies different algorithms to data it obtains on the TN in question. CVTs typically access a multitude of data sources on each TN to improve the accuracy of its results.

### User Equipment (UE)

This section assumes a wireless handset with a screen display that is compliant with Verstat requirements in 3GPP standards.

## Assumptions

1. The guidelines herein are limited in scope to consumer services, and not business verification services.
2. Network data and/or analytics may not be available/implemented at all times in all networks.
3. When an end user subscribes to an analytics service, the end user understands that the assessment is predicated on the statistical evaluation of data available on the current call along with data on other similar calls. Consequently, he/she may receive false positive and false negative messages on some of their incoming calls.

Editor’s Note: add assumption on privacy issues

## Available Call-related Information

The data outputs from the network and CVT will be at the center of the message delivered to the user (e.g., warning or other). The CVT or analytics function may be in a better position to process and assess the trust level of incoming calls.



Therefore, it is recommended that attestation levels and identifiers from SHAKEN be made available to the CVT function by the appropriate carrier and according to local policies.

Making more information available to the CVT algorithms is likely to yield more accurate results for the user.

## Recommended Data Treatment and Display Options

1. In the absence of an analytics service, a warning (symbols and text) should be displayed to the user if verification fails, independent of the attestation level. Otherwise, for other values of verification, the user should receive a normal call profile based on the services they subscribe to.
2. If an analytics service is available/used, a warning should be displayed to the user if verification fails, independent of the attestation level.
3. STIR/SHAKEN and verification information should be made available to the CVT (analytics), when available.

Editor’s Note: add that it is subject to local policy

Table X+1: Summary of Proposed Displays to the User

|  |  |  |  |
| --- | --- | --- | --- |
| Attestation (by the originating end) | Verification (by the terminating network) of the originator's signature/cert | Availability of Analytics | Message presented to the User |
| A - Full | Passed | Not Available | Normal call profile[[1]](#footnote-1) |
|  | Available | Display analytics results\* |
| Failed | Not Available | Warning\*\*[[2]](#footnote-2) |
|  | Available | Display analytics results\* |
| No Verification performed | Not Available | Normal call profile |
|  | Available | Display analytics results\* |
| B - Partial | Passed | Not Available | Normal call profile |
|  | Available | Display analytics results\* |
| Failed | Not Available | Warning\*\* |
|  | Available | Display analytics results\* |
| No Verification performed | Not Available | Normal call profile |
|  | Available | Display analytics results\* |
| C - Gateway | Passed | Not Available | Normal call profile |
|  | Available | Neutral display with analytics results |
| Failed | Not Available | Warning\*\* |
|  | Available | Display analytics results\* |
| No Verification performed | Not Available | Normal call profile |
|  | Available | Display analytics results\* |
| Not A, B or C. No Attestation performed (e.g., early stages when carrier hasn't implemented STIR/SHAKEN) | *Nothing to sign – is that a "Fail"* | Not Available | Normal call profile |
|  | Available | Display analytics results\* |

\* This assumes the STIR/SHAKEN data was provided as input to the analytics service. Analytics results include additional information on the caller, and may include a warning.

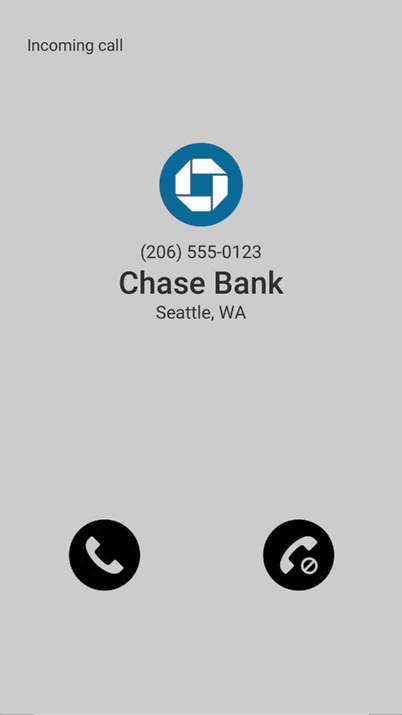
\*\* Some service providers may – based on consumer choice and consent - block these marked calls instead of completing them with a warning.

## Example Displays

These examples are provided for the illustration and enhancement of the scenarios listed in the above table.

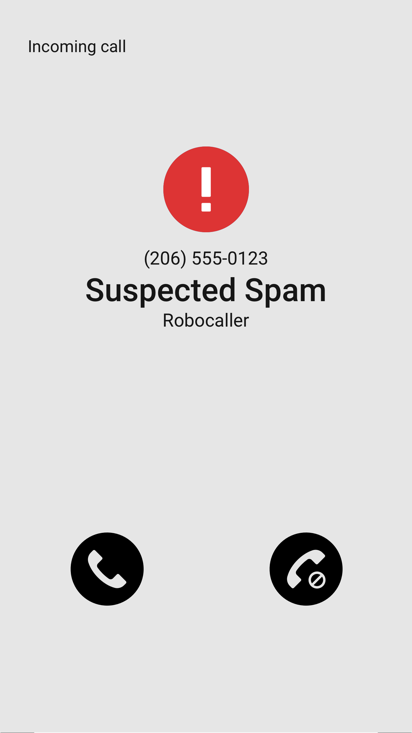
### Full Attestation and Verification Passed (no analytics)

In this scenario, the user does not subscribe to a CVT service. The delivery of the Verstat (TN validation passed) delivers the call to the UE without warnings (or affirmations). The logo and location (city and state) of the caller is retrieved and delivered by eCNAM.



### Gateway Attestation, Verification Passed, subscribes to analytics (analytics determine the call is suspicious)

In this scenario, the user subscribes to a CVT service that provides analytics. A gateway attestation is inconclusive to the caller, but an analytics service has flagged the caller as a known scammer. Therefore, a warning is provided to the user.

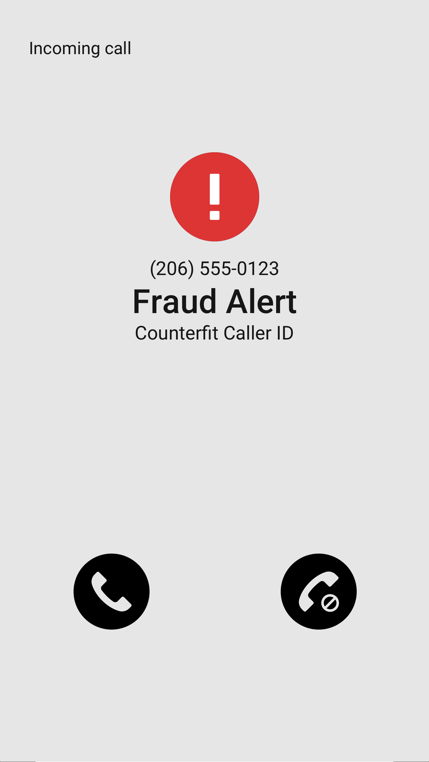


### Verification Failed

If the verification failed, CVT may not be necessary or be used. There are several possible outcomes.

The service provider may simply block the call from terminating to the end user, per the subscriber's request.

Alternatively, a warning would be provided along with an explanation of the reason behind the warning. The subscriber is then forewarned and empowered to manage incoming calls based on all the information made available. A CVT service may be able to provide more useful reasoning, but is not expected to.



## User Perspective

### Usability Studies

Background and size of study groups

What did users prefer in terms of symbols and verbal messages, colors, order of display?

Other human factors [TBD].

### Basic recommendations on the Display or Message delivery to the UE

As a result of the above studies, it is recommended that [ the following are examples of recommendations for further discussion]:

1. eCNAM delivers the aggregate of all the information available about the TN (caller identity, results of CVT analytics, and information queried by the terminating provider)
2. The use of multiple symbols in a given display is not recommended because the consumer's interpretation of different symbols may result in confusion and detract from the value the service is providing.
3. Displaying status symbols, such as checkmarks, on calls with "full attestation – verification passed", is not recommended (studies show it leads to consumer confusion).
4. It is recommended that only warning symbols be provided when warranted.
5. For displays where a warning symbol should be displayed, the following are suggested symbols to choose from:
   1. 
   2. 
6. Audible special ringing/tones may be applied on calls that fail verification as an consumer option.
7. Minimize length of verbal messages to a choice of tested, effective phrases (the following are examples for further discussion):
   1. Caution: possible scam
   2. Fraud Alert
   3. Possible Scam
   4. Warning: do not give personal information
   5. *More from human factors experts*

### ADA Considerations

* 8% of the male population are color-blind. Therefore, the display should not rely heavily on red and green to convey results.
* Ensure messages are clearly understood without relying on colors (e.g., via text or sound)
* Consider audio announcements for the visually impaired before the call is completed (within the limits of post-dial delays)

# Display Guidelines for Analog Devices

## Analog Devices connected to an IP Network

Limited Screen display

Are these devices capable of handling

a) PASSport's attestation levels

b) results of verification (Verstat), and

c) displaying analytics results?

## Analog Devices connected to CS Network

### Available Solutions

Devices that apply black and white lists with updates from FTC and FCC registries.

Devices that apply simultaneous ringing and block suspect calls, per the user's request.

More.

# Related SDOs and Fora

## 3GPP

## GSMA

## Cable Labs

## Consumer Electronics

# Conclusions

**Annex A**

(normative/informative)

# A Illustrative Examples

This annex will document supportive material





1. Define normal call display. [↑](#footnote-ref-1)
2. Whether a warning indicator is sent will be left up to local policy. [↑](#footnote-ref-2)