**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 a framework for display of verified Caller ID.

**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 using Conventional Caller Name (CNAM)

In its simplest form, a service provider performing STIR/SHAKEN verification, 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 Equipment (UE) via a single alphanumeric character. The ‘verstat” tel URI parameter has been standardized to signal Verified Caller ID status but for UE that can support it. It is quite likely that as STIR/SHAKEN caller authentication standards are implemented, there will be millions of UE that won’t be able to support “verstat”. In particular, analog devices connected to IP networks.

Today, network switching support to query 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 existing 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.

Combatting illegal robocalls will require a range of mitigation techniques. Consider the following two approaches for incorporating use of conventional CNAM today and more importantly as STIR/SHAKEN caller authentication standards are implemented:

* A terminating IP/TDM switch, before completing a call to the associated UE, issues a conventional CNAM query to an authoritative 3rd party CNAM service. Prior to returning any CNAM of record, Call Validation Treatment (CVT) or “analytics” and policy are applied to determine if the CNAM of record should be overwritten with another name (e.g., “FRAUD CALL”). The policy-applied CNAM is then returned to the querying switch and transparently signaled to the UE.
* As STIR/SHAKEN is implemented, the result of verification can first be sent to CVT to determine if a CNAM of record should be returned or overwritten. The policy-applied CNAM can then be returned to the terminating IP switch through the STIR/SHAKEN verification process and be transparently signaled to UE that do not yet support “verstat”.

Therefore, in an effort to accelerate the reach of Verified Caller ID across analog devices in IP networks, service providers can evaluate the use of conventional CNAM as a vehicle for signaling verification status. 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 STIR/SHAKEN implementations are established.

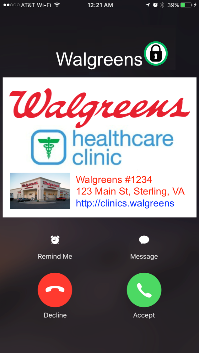
There is a range of implementation options that can be considered. Two simple examples are:

1. The service provider performing the STIR/SHAKEN verification process appends a designated alphanumeric character to the end of the 15 character CNAM of record for a verified Caller ID (e.g., JOHN DOE\*)
2. This service provider appends a designated alphanumeric character to the beginning of the 15 character CNAM of record 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 identity) 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 3rd party 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 analog 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 could simplify the subscriber education process)
2. A device operating system or application vendor can interpret the “\*” and enhance a screen-based display to the subscriber as illustrated in the below (i.e., the black padlock within the green circle):



Given the above description and explanation, the following highlights items to consider when signaling Verified Caller ID status using conventional CNAM:

1. As with any signaling approach, use of conventional CNAM for Verified Caller ID status to UEs needs to be secure and not easily imitated by scammers. For example, a service provider should override any included CNAM from another network with this approach.
2. If a single alphanumeric character is used from conventional CNAM instead of overwriting the CNAM of record with a different name like “FRAUD CALL”, existing 15 character CNAMs need to be addressed. Further, the selected character should not be used in existing CNAMs of record.
3. This approach doesn’t assume that a 3rd party CNAM service is used. What is key is the ubiquitous network switching support for conventional CNAM queries and device support to display 15 character CNAMs.
4. A 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 signaling verifying Caller ID but also the associated, displayed CNAM.
5. ATIS IP-NNI continues to discuss the desire to signal more information to the UE about the verification status. However, at this time, it seems like any such approach would require changes by UEs to interpret and act on such information (e.g., any extensions to the “verstat” tel URI parameter). The near term approach to use conventional CNAM can be an option to accelerate implementations and signal the most critical piece of information to UEs. 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.
6. Any display approach to UEs will require 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 a uniform industry approach is agreed to.
7. If conventional CNAM to signal Verified Caller ID status is considered for use as a near term approach, then a transition plan to any more standards-based approach needs to address implementation changes, subscriber education (re-education) and their call experience.
8. Accurate CNAM, along with Verified Caller ID, forms a foundation for building a much better subscriber call experience. Coupling these together is intuitive as many business to consumer calls are not identifiable enough today to be consistently answered. Further, analytics and policy rules, which are increasingly becoming more commercially supported, can be defined and used to modify the signaled CNAM based on the caller verification status. For example, a non-Verified Caller ID on an IP network could be signaled as “UNVERIFIABLE” to analog devices.

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 a broad set of existing subscriber devices as STIR/SHAKEN caller authentication standards are implemented in IP networks. Although positioned as a near term approach, it is extensible in multiple ways to support innovative ways to further enhancing the subscriber call experience.

## Considerations during Transition to STIR/SHAKEN Caller Authentication and Signaling

Using conventional CNAM to convey the Verified Caller ID status until STIR/SHAKEN caller authentication standards and “verstat” UE support become more widely deployed can benefit subscribers in the interim, especially those served on analog devices.

It is important to understand that during this transition, the use of any special character that may be appended/ prepended to the 15 character CNAM could be misused by bad actors. As the concept is implemented with some service providers, scammers could insert it on calls to other networks that do not offer this service securely. If the public, in general, is trained to trust that symbol, then some subscribers may be affected.

# Display Guidelines of Verified Caller ID on All-IP Networks and Screen-based Devices

With the implementation of STIR/SHAKEN and certificate governance models on All-IP Networks, 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 guidelines in this section are provided for screen-based devices, such as smartphones, operating on an all-IP network. Considerations for other scenarios of analog devices served by all-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.

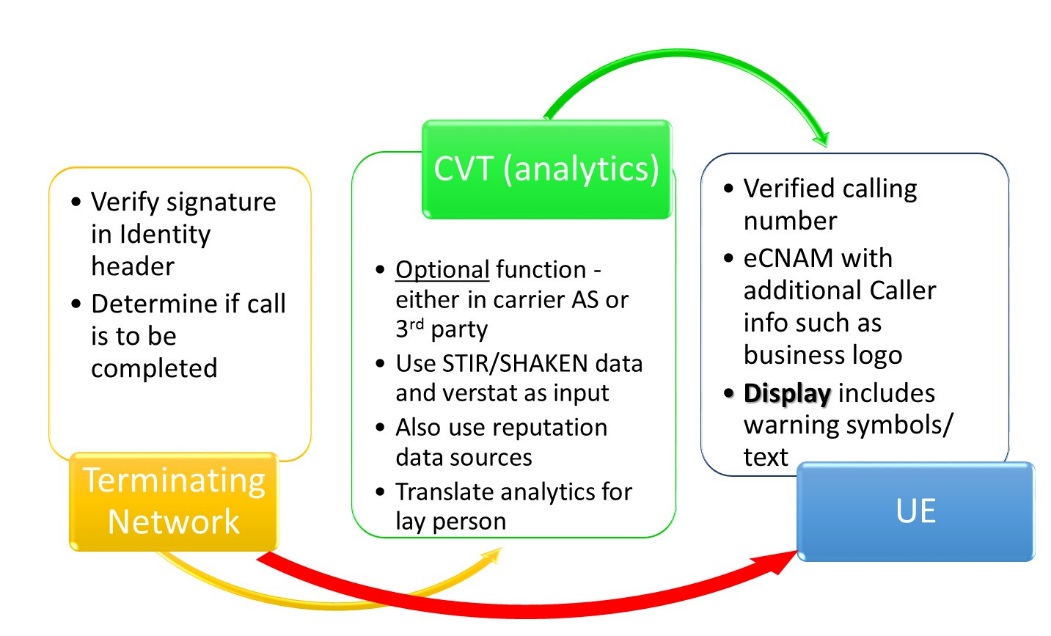


Figure 1. Entities Contributing to Ultimate Display

### 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 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 application server) 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” parameter 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 or is provided 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 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.

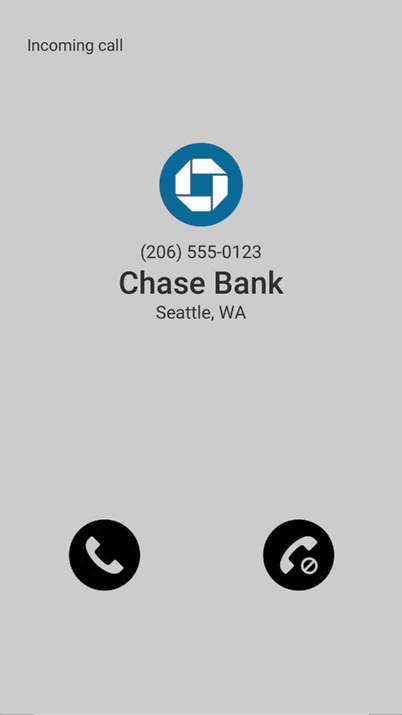
\*\* Some service providers may – based on consumer choice and consent - block these marked calls instead of completing them with a warning.

## Example Displays

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

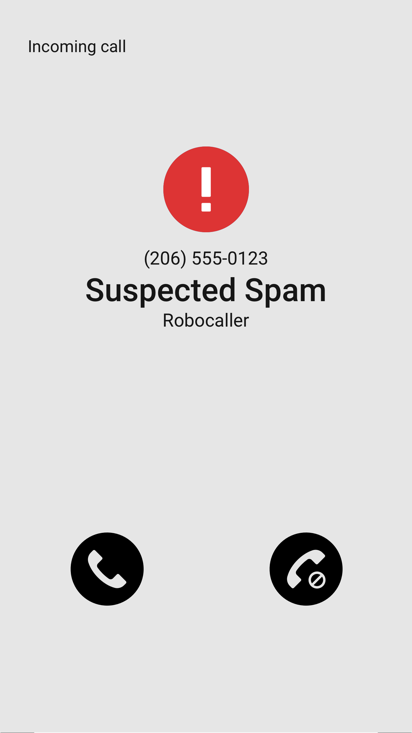
### Full Attestation and Verification Passed (no analytics)

In this scenario, the user does not subscribe to a CVT service. The delivery of the verstat parameter (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 enhanced CNAM (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.

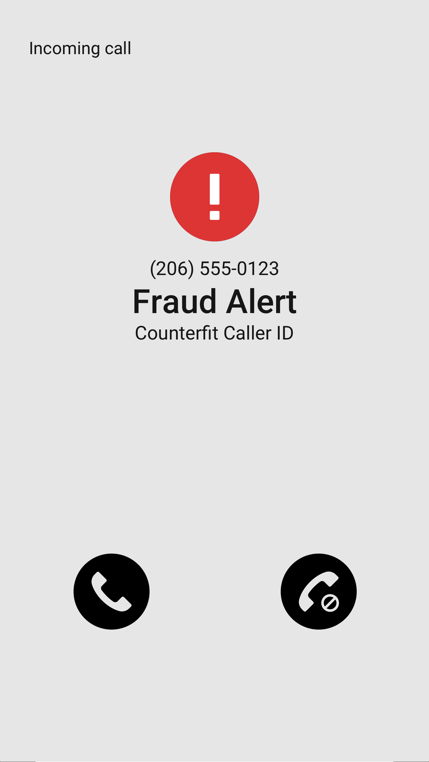


### Verification Failed

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. 
   3. *Other*
6. Audible special ringing/tones may be applied on calls that fail verification as a 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)