ATIS-1000081

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

JOINT STANDARD

As a leading technology and solutions development organization, the Alliance for Telecommunications Industry Solutions (ATIS) brings together the top global ICT companies to advance the industry's most pressing business priorities. ATIS' nearly 200 member companies are currently working to address the All-IP transition, 5G, network functions virtualization, big data analytics, cloud services, device solutions, emergency services, M2M, cyber security, network evolution, quality of service, billing support, operations, and much more. These priorities follow a fast-track development lifecycle — from design and innovation through standards, specifications, requirements, business use cases, software toolkits, open source solutions, and interoperability testing.

ATIS is accredited by the American National Standards Institute (ANSI). The organization is the North American Organizational Partner for the 3rd Generation Partnership Project (3GPP), a founding Partner of the oneM2M global initiative, a member of the International Telecommunication Union (ITU), as well as a member of the Inter-American Telecommunication Commission (CITEL). For more information, visit www.atis.org.

The SIP Forum is a leading IP communications industry association that engages in numerous activities that promote and advance SIP-based technology, such as the development of industry recommendations; interoperability testing events and special workshops, educational activities, and general promotion of IP communications standards, services, and technology for service provider, enterprise, and governmental applications. The SIP Forum is also the producer of the annual SIPNOC conferences (for SIP Network Operators Conference), focused on the technical requirements of the service provider community. One of the Forum's technical activities is the development of the SIPconnect Technical Recommendation – a standards-based SIP trunking recommendation that provides detailed guidelines for direct IP peering and interoperability between IP PBXs and SIP-based service provider networks, and the SIPconnect Certification Testing Program, a unique certification testing program that includes a certification test suite and test platform, and an associated "SIPconnect Certified" logo program that provides an official "seal of certification" for companies products and services that have officially achieved conformance with the SIPconnect specification. Other important Forum initiatives include work in security, SIP and IPv6, and IP-based Network-to-Network Interconnection (IP-NNI). For more information about all SIP Forum initiatives, please visit:

< http://www.sipforum.org/ >

ATIS-1000081, ATIS Technical Report on a Framework for Display of Verified Caller ID

Is an ATIS & SIP Forum Joint Standard developed by the **ATIS/SIP Forum IP-NNI Task Force** under the **ATIS Packet Technologies and Systems Committee (PTSC)** and the **Technical Working Group (TWG)** under the **SIP Forum**.

Published by

Alliance for Telecommunications Industry Solutions
1200 G Street, NW, Suite 500
Washington, DC 20005

SIP Forum LLC
733 Turnpike Street, Suite 192
North Andover, MA 01845

ATIS-1000081

ATIS Standard on

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

Alliance for Telecommunications Industry Solutions

Approved May 2018

Abstract

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. The main goal is to provide display guidelines that help empower consumers in managing their calls, as per the Robocalling Strike Force recommendations.

Foreword

The Alliance for Telecommunication Industry Solutions (ATIS) serves the public through improved understanding between providers, customers, and manufacturers. The Packet Technologies and Systems Committee (PTSC) develops and recommends standards and technical reports related to services, architectures, and signaling, in addition to related subjects under consideration in other North American and international standards bodies. PTSC coordinates and develops standards and technical reports relevant to telecommunications networks in the U.S., reviews and prepares contributions on such matters for submission to U.S. International Telecommunication Union Telecommunication Sector (ITU-T) and U.S. ITU Radiocommunication Sector (ITU-R) Study Groups or other standards organizations, and reviews for acceptability or per contra the positions of other countries in related standards development and takes or recommends appropriate actions.

The SIP Forum is an IP communications industry association that engages in numerous activities that promote and advance SIP-based technology, such as the development of industry recommendations, the SIPit, SIPconnect-IT, and RTCWeb-it interoperability testing events, special workshops, educational seminars, and general promotion of SIP in the industry. The SIP Forum is also the producer of the annual SIP Network Operators Conference (SIPNOC), focused on the technical requirements of the service provider community. One of the Forum's notable technical activities is the development of the SIPconnect Technical Recommendation – a standards-based SIP trunking recommendation for direct IP peering and interoperability between IP Private Branch Exchanges (PBXs) and SIP-based service provider networks. Other important Forum initiatives include work in Video Relay Service (VRS) interoperability, security, Network-to-Network Interoperability (NNI), and SIP and IPv6.

Suggestions for improvement of this document are welcome. They should be sent to the Alliance for Telecommunications Industry Solutions, PTSC, 1200 G Street NW, Suite 500, Washington, DC 20005, and/or to the SIP Forum, 733 Turnpike Street, Suite 192, North Andover, MA, 01845.

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 an optional capability that could augment the standard. The standard is fully functional without the incorporation of this optional capability.

The **ATIS/SIP Forum IP-NNI Task Force** under the **ATIS Packet Technologies and Systems Committee (PTSC)** and the **SIP Forum Technical Working Group (TWG)** was responsible for the development of this document.

Table of Contents

Scope, Purpose, & Application 1
1.1 Scope 1
1.2 Purpose 1
2 Normative References 1
3 Definitions, Acronyms, & Abbreviations 2
3.1 Definitions 2
3.2 Acronyms & Abbreviations 2
4 Signaling of Verified Caller ID using Conventional Caller Name (CNAM) 3
4.1 Considerations during Transition to STIR/SHAKEN Caller Authentication & Signaling 4
5 Display Guidelines of Verified Caller ID on All-IP Networks & Screen-based Devices 5
5.1 Entities that shape the display 5
5.1.1 IP Network 6
5.1.2 Call Validation Treatment (CVT) or Analytics 6
5.1.3 User Equipment (UE) 6
5.2 Assumptions 6
5.3 Available Call-related Information 7
5.4 Preliminary Display Usability & Comprehension Studies 7
5.4.1 Study #1: Comprehension & Impact of Certified Call Markers 8
5.4.2 Study #2: Call Pickup Rate Test 8
5.4.3 Study #3: Warning Phrasing Test 9
5.4.4 Study #4: Iconography Impact Test 11
5.5 Recommended Data Treatment & Display Options 13
5.6 Example Displays 14
5.6.1 Full Attestation & Verification Passed (no analytics) 14
5.6.2 Gateway Attestation, Verification Passed, Subscribes to Analytics (Analytics Determine the Call is Suspicious) 15
5.6.3 Verification Failed 16
5.6.4 Basic Recommendations on the Display or Message Delivery to the UE 16
5.7 Americans with Disabilities Act (ADA) Considerations 16
6 Display Guidelines for Analog Devices 17
6.1 Analog Devices Connected to an IP Network 17
6.2 Analog Devices Connected to Circuit Switched (CS) Network 17
7 Related SDOs & Fora 17
7.1 3GPP 17
7.2 ATIS 17
7.3 IETF 18

Table of Figures

Figure 5.1: Entities Contributing to Ultimate Display 6
Figure 5.2: Change in Pickup Rates, Change in User Trust, Change in Block Percentages, & Ratio Between the Two 10
Figure 5.3: Test Images for “Possible Fraud” String 11
Figure 5.4: Impact on User Trust and block Rates, By Icon 12
Figure 5.5: Pickup, Trust, & Block Rates for all Text-only & Tested Text+Icon Combinations 13

Table of Tables

Table 5.1: Results of Warning Phrasing Test 9
Table 5.2: Summary of Proposed Displays to the User 13

ATIS Standard on –

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

1 Scope, Purpose, & Application

1.1 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. The main goal is to provide display guidelines that help empower consumers in managing their calls, as per the Robocalling Strike Force recommendations[1].

This report should be treated as a living document as the guidelines are expected to evolve. The deployment of verification methods, such as Secure Telephone Identity Revisited/Signature-based Handling of Asserted information using toKENs (STIR/SHAKEN), and application of call analytics are expected to occur in stages over an extended period of time. Hence, the operations experience gained over time is expected to provide feedback and input to future issues of this report.

Results of usability studies are expected to contribute to the evolution of the recommendations in this report, as they become available.

More research is needed to identify the types of displays that empower end users with messages that are easy to interpret. At this time, such research is outside the scope of this report.

1.2 Purpose

The guidelines presented in this document are best practices based on a review of industry standards and studies on the effectiveness of warning signs and human factors related to the reading and comprehension of variable messages (text and symbolic). These guidelines help meet the goals of regulators and consumer protection agencies for empowering consumers with simple and effective call information.

This report recommends that these guidelines be taken into consideration by all stakeholders (service providers, equipment manufacturers, and analytics providers) in the deployment of verified Caller ID displays and the composition of its related messages.

Variations may exist, subject to local policy.

2 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.

[Ref 1] ATIS-1000074, *Signature-based Handling of Asserted Information using toKENs (SHAKEN)*.[2]

---

[1] *Industry Robocall Strike Force Report,* FCC, April 28, 2017; This document is available from the Federal Communications Commission at < https://www.fcc.gov/file/12311/download >.

[2] This document is available from the Alliance for Telecommunications Industry Solutions (ATIS) at < https://www.atis.org/docstore/product.aspx?id=28297 >.

[Ref 2] 3GPP TS 22.173, *IP Multimedia Core Network Subsystem (IMS) Multimedia Telephony Service and supplementary services*.[3]

[Ref 3] 3GPP TS 24.196, *Technical Specification Group Core Network and Terminals; Enhanced Calling Name*.[4]

[Ref 4] IETF RFC 8224: "*Authenticated Identity Management in the Session Initiation Protocol (SIP)*".[5]

[Ref 5] 3GPP TS 24.229: *"IP Multimedia call control protocol based on Session Initiation Protocol (SIP) and Session Description Protocol (SDP); Stage 3".*[6]

[Ref 6] 3GPP TS 29.165: *"Inter-IP Multimedia System (IMS) Network to Network Interface (NNI) (Release 15)".*[7]

3 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 >.

3.1 Definitions

Caller ID: The originating phone number included in call signaling 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.

End user/consumer: Used interchangeably to refer to a customer of telecommunications service that is not a carrier or a device, and for whom the service was ultimately created or intended.

Normal call profile: The display of all identity information/services the end user subscribes to, outside the mitigation services that include analytics.

'verstat' tel URI: a parameter used in either the P-Asserted Identity header field or From header field (in a SIP request) to convey the status of calling number verification performed by the home network.

3.2 Acronyms & Abbreviations

ADA	Americans with Disabilities Act
ATA	Analog Terminal Adapters
ATIS	Alliance for Telecommunications Industry Solutions
CNAM	Conventional Caller Name
CVT	Call Validation Treatment
eCNAM	Enhanced Caller Name
IP	Internet Protocol
IP-NNI	ATIS and SIP Forum IP Network-to-Network Joint Task Force
ITU-T	U.S. International Telecommunication Union Telecommunication Sector
ITU-R	U.S. ITU Radiocommunication Sector

[3] This document is available from the Third Generation Partnership Project (3GPP) at: < http://www.3gpp.org/specs/specs.htm >

[4] This document is available from the Third Generation Partnership Project (3GPP) at: < http://www.3gpp.org/specs/specs.htm >

[5] This document is available from the Internet Engineering Task Force (IETF). < http://www.ietf.org >

[6] This document is available from the Third Generation Partnership Project (3GPP) at: < http://www.3gpp.org/specs/specs.htm >

[7] This document is available from the Third Generation Partnership Project (3GPP) at: < http://www.3gpp.org/specs/specs.htm >

NNI	Network-to-Network Interoperability
PBXs	IP Private Branch Exchanges
PTSC	The Packet Technologies and Systems Committee
SHAKEN	Signature-based Handling of Asserted information using toKENs
SIP	Session Initiation Protocol
SIPNOC	SIP Network Operators Conference
STIR	Secure Telephone Identity Revisited
TDM	Time-Division Multiplexing
TN	Telephone Number
TTL	Time to Live
UE	User Equipment
UI	User Interface
VRS	Video Relay Service

4 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. It is quite likely, however, that as STIR/SHAKEN caller authentication standards are implemented, there will be millions of UE that won't initially be able to support 'verstat'. In particular, analog devices connected to IP networks are not expected to support 'verstat'.

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/Time-Division Multiplexing (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. The following two approaches incorporate use of conventional CNAM with or without the implementation of the STIR/SHAKEN caller authentication standards:

- In the absence of STIR/SHAKEN implementation, a terminating IP/TDM switch, before completing a call to the associated UE, issues a conventional CNAM query to an authoritative 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 textual message (e.g., "FRAUDULENT 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 the CVT service 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 the UE that does 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 relaying verification status to the consumer. 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.

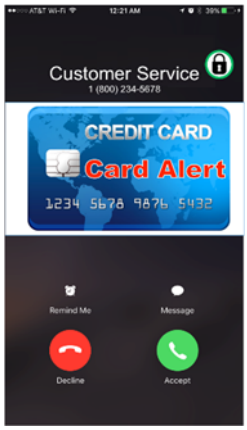
There is a range of implementation options that can be considered. Two simple examples are:

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. The service provider prepends a designated alphanumeric character to 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 relay the verification of the calling number in the associated SIP URI and not the displayed CNAM. There are 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.

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 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 below (i.e., the black padlock):



4.1 Considerations during Transition to STIR/SHAKEN Caller Authentication & Signaling

When signaling Verified Caller ID status using conventional CNAM, the following items should be considered:

1. As with any signaling approach, use of the conventional CNAM display field for relaying the Verified Caller ID status to the UE 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 and the existing CNAM of record is already 15 characters long, then the name needs to be reviewed according to the service provider's truncation rules. Further, the selected character should not be used in existing CNAMs of record. Lastly, it is important to understand that the idea of appending/prepending a special character 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 is trained to trust that symbol, then some subscribers may be affected.
3. This approach relies on ubiquitous network switching support by the service provider for conventional CNAM queries and device support to display 15-character CNAMs.
4. This approach may be extensible in the future to not just relaying the verification status of Caller ID but also the associated CNAM. For example, if the current SHAKEN identity claim is extended to cases where the name is signaled from the originating network, then both the verification of Caller ID and its associated CNAM can potentially be relayed to the consumer using this approach.

5. The ‘verstat’ tel URI parameter has been standardized with three potential values to signal Verified Caller ID status. However, there may be a need to signal more information to the UE about the verification status. Any such extensions would need to go back through the standardization process and UEs would then need to make changes to support these extensions. The near-term approach to use conventional CNAM can be an option to accelerate implementations, as well as signal more verification status information to UEs. A 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. A transition plan to a more standards-based approach needs to address implementation changes, subscriber education (re-education), and the results of their call experience with this approach.
7. 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, 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, CNAM is extensible in multiple ways enabling it to support a number of innovative ways to further enhance the subscriber call experience. Moreover, it allows companies to respond to accelerated timelines from regulators for addressing illegal robocalls and spoofing.

5 Display Guidelines of Verified Caller ID on All-IP Networks & 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 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 clause 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 Clause 6.

5.1 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.

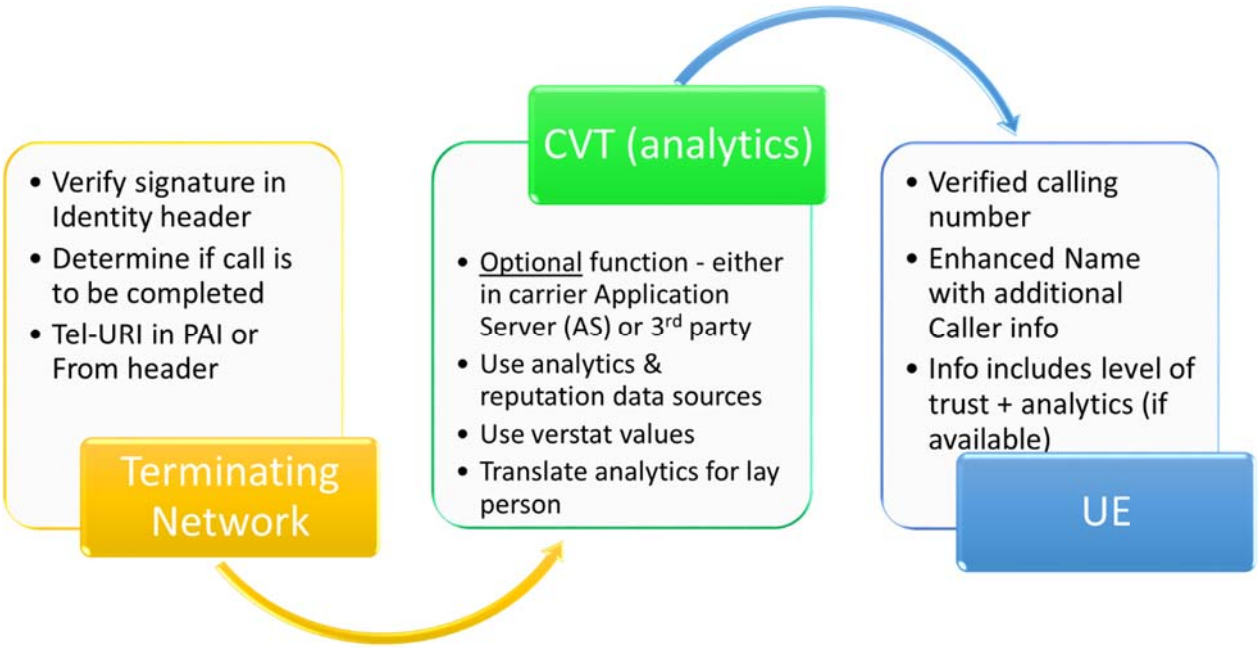


Figure 5.1: Entities Contributing to Ultimate Display

5.1.1 IP Network

The originating network is responsible for signaling the Identity header containing the pertinent claims and attestations about the calling number, per IETF RFC 8224 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.

5.1.2 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), 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 Telephone Number (TN) in question. CVTs typically access a multitude of data sources on each TN to improve the accuracy of its results.

5.1.3 User Equipment (UE)

This clause assumes a wireless handset with a screen display that is compliant with 'verstat' requirements in 3GPP standards TS 24.229, TS 29.165, and TS 24.196.

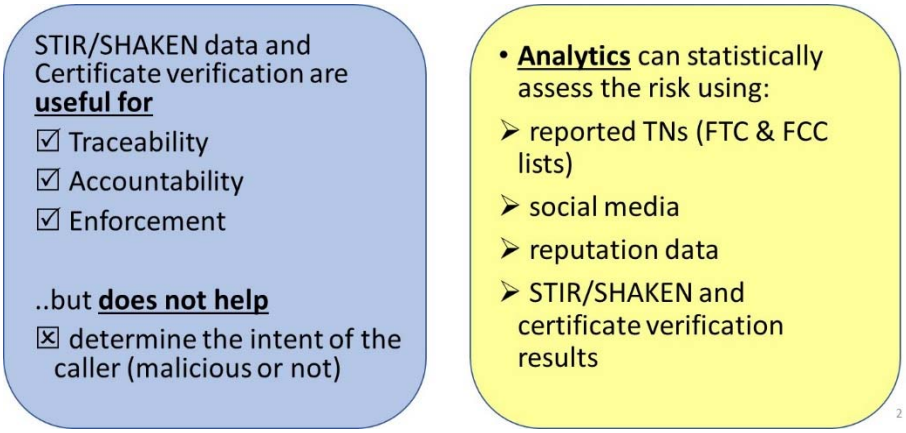
5.2 Assumptions

1) The guidelines herein are limited in scope to empowering end users in managing their identity services, not business verification services.
2) Network data and/or analytics may not always be available/implemented in all networks.
3) The analytics operation is predicated on the statistical evaluation of data available on the current call along with data on other similar calls. When end users subscribe to or are provided an analytic service, they will be informed that they may receive false positive and false negative messages on some of their incoming calls.

4) It is expected that some service providers will delegate the delivery of the final call information display (including TN, calling name, and the results of verification) to an analytics provider. For those cases, the analytics provider is expected to adhere to the application of privacy rules for the calling number and name portions of the display; i.e., an "Anonymous" message would be displayed for name and TN.
    a. The terms of agreement between the service provider and the analytics provider are expected to require preservation of the caller's privacy.
    b. Further clarification and/or safe harbors are needed to determine whether the name and TN could be anonymized while additional call information, such as call category and potential fraud risk, could be delivered to help empower the end user.
5) Where delivery of the final call information display is not delegated to an analytics provider, the service provider is expected to adhere to the application of privacy rules for the calling number and name portions of the display; i.e., an "Anonymous" message would be displayed for name and TN.
6) In the absence of clarification or any special allowances on handling private calls, the guidelines herein call for anonymizing ALL call information if the received calling number is anonymous. The determination of the authentication of the call is NOT “call information” in the traditional sense and should be presented to the user independent of legitimate privacy uses.
7) The end user may subscribe to multiple mitigation services. Order and preference of display may be determined by the service provider. Variations in operating systems and the plethora of available applications make it impractical to set interoperability or prioritization guidelines. Therefore, it is the responsibility of end users to select the mitigation service that best meets their needs.

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



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

5.4 Preliminary Display Usability & Comprehension Studies

Over the course of Q2 and Q3 2017, Hiya Inc. conducted several usability studies targeted at the display guidelines of the STIR/SHAKEN protocol. The studies and their results are provided later in this clause.

The goals of the study were twofold:

1. To measure the potential impact of a positive assurance indication for verified calls (the “green checkmark”).
2. To assess various textual and iconographic display options for caution indicators on suspicious calls.

Hiya conducted three brief usability studies on different audiences:

1. A user comprehension and influence study on robust caller profiles and certified call markers.
2. A user impact analysis of various phrasings and iconography for suspicious call messaging.
3. A call pickup rate impact analysis of a “certified” checkmark icon against existing Hiya users.

5.4.1 Study #1: Comprehension & Impact of Certified Call Markers

5.4.1.1 Study Description

Hiya interviewed 11 randomly chosen individuals among a pool of volunteers to participate in a paper-based usability study.

Participants were offered no context or explanation of STIR/SHAKEN or the purpose of the study.

Participants were presented with a sequence of incoming call User Interface (UI) mockups and asked a series of questions:

- What do you notice about this screen?
- What confidence or trust do you have in this caller information?
- What effect does this have on your opinion of previous screens (if any)?

The mockups were designed to enhance the incoming call experience with expanded caller profile information, with the final mockup showing a “certified call” confirmation reflective of STIR/SHAKEN validation.

Interviews lasted an average of 35 minutes per participant.

5.4.1.2 Results

In nearly all cases (10/11), participants showed a “strong” or “very strong” indication that additional caller profile information strengthened their confidence in the legitimacy of the theoretical phone call.

This applied across all mockups, prior to “certified call” marker.

For the “certified call” mark,

- A significant number of participants (8/11) identified the mark as reassurance to the legitimacy of the call, and all who identified this also expressed future doubts to the legitimacy of any future call lacking the indication.
- Some (6/11) expressly stated that they would become less likely to answer any unknown call lacking certification, once the certification marker was seen.

5.4.1.3 Conclusions

Hiya has concluded that the use of such a marker with clear context would negatively impact all calls lacking this marker.

It remained unclear from the study if the marker would have a positive impact on pickup rates for marked numbers. (Hiya has previously demonstrated that extended call profile information positively influences call pickup rates, without any “certified call” indication.)

5.4.2 Study #2: Call Pickup Rate Test

5.4.2.1 Study Description

Hiya selected 70 high-volume (in excess of 600 monthly observed calls) legitimate business phone numbers from Canada with varying pre-existing caller profile information. These numbers were chosen because of Hiya’s subscription rate in Canada.

Call creation rates and user pickup rates were monitored for these numbers over a two-week period, during which Hiya caused the display of a simple white checkmark to be shown for any Smart Call user.

After two weeks, the checkmark was removed, and call volume and pickup rates were measured for an additional two weeks.

5.4.2.2 Results

It is important to note that Hiya could not identify or control the individuals receiving phone calls from the selected businesses. Therefore, it is not possible to confirm the results of Study #1 (that individual pickup rates would drop as users become familiar with expecting a checkmark on legitimate calls).

On average, Hiya did observe a 4.89% increase in call pickup rates overall while the checkmark was present.

5.4.2.3 Conclusions

Further analysis is needed to determine if the number's existing call profile (a "caller ID" name) or business industry was more effective than others.

However, overall, this is taken to reinforce the positive impact a certified marker can potentially have on pickup rates for verified calls.

5.4.3 Study #3: Warning Phrasing Test

5.4.3.1 Study Description

Hiya has crafted 7 near-identical mockups of an incoming call screen. The only delta between the screen mockups was the presence of a warning phrase, expressing reasonable doubt about the legitimacy of the caller. Study participants were shown this screen for 5 seconds, then asked a series of questions:

1. Would you answer this call?
2. Was this call from a trustworthy source?
3. Would you block this number from calling in the future?
4. Why do you think you're receiving this call?

The following phrases were used, each shown to 400 unique participants (no overlap between phrases):

- Phone number only (baseline).
- "Fake Phone Number", with phone number.
- "Possible Fraud" with phone number.
- "Private Number" with no phone number.
- "Unknown Caller" with phone number.
- "Caller Not Verified" with phone number.
- "Spoofed Number" with phone number.

5.4.3.2 Results

The results of the study are:

Table 5.1: Results of Warning Phrasing Test

Display	Pickup Rate	Block Rate	User Trust
Phone number only	30%	29%	46%
"Private Number" (no phone number)	28%	43%	38%

Display	Pickup Rate	Block Rate	User Trust
“Fake Phone Number”	21%	49%	30%
“Possible Fraud”	11%	57%	20%
“Unknown Caller”	24%	33%	42%
“Caller Not Verified”	24%	39%	40%
“Spoofed Number”	19%	51%	29%

5.4.3.3 Conclusions

One main caveat is that these percentages should be validated against actual user behavior. A 33% block rate for unknown callers seems unexpectedly high. This should be verified via other means before concluding this reflects real-world behavior. However, while totals may not be actionable, the belief is the deltas between levels are valid.

“Private Number” was included in this study only as an anecdotal comparison and is not a recommended display string. From this we can see minimal change in pickup rates, but a large increase in block rates. It was otherwise excluded from analysis.

The main goal of the study is to find how different messaging affects users’ level of caution for an incoming call, while separately measuring their likelihood to block the number in the future. The ideal message would greatly increase caution level, with minimal impact on block rates (as spoofed calls may impersonate legitimate numbers).

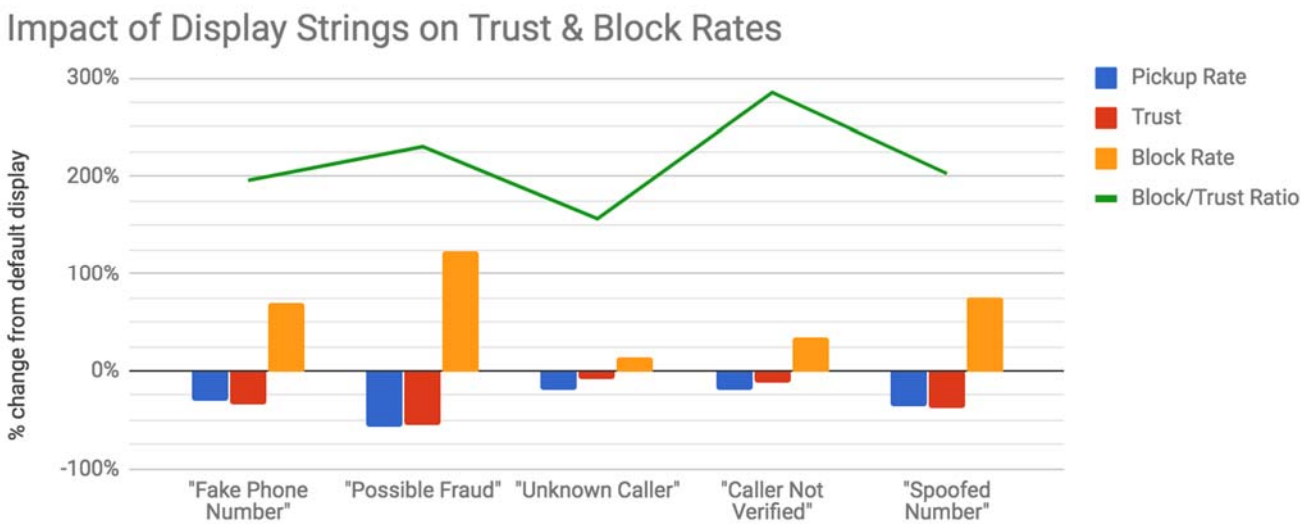


Figure 5.2: Change in Pickup Rates, Change in User Trust, Change in Block Percentages, & Ratio Between the Two

Overall, some variation was observed in the delta of user trust as it relates to the delta in block rates. Less aggressive message “Unknown Caller” has a lower block/trust ratio, but overall has negligible impact on both. Overall, all strings tested had significant impact on the claimed block rate from users.

Similar results between “Fake Phone Number” and “Spoofed Number” indicates user general understanding of the term “spoof”.

5.4.4 Study #4: Iconography Impact Test

5.4.4.1 Study Description

Hiya selected two test strings “Possible Fraud” and “Fake Number” and created eight mockups of an incoming call screen, four with each string. Each string was paired with one of three possible flagged icons: a red stop sign, a yellow triangle, and an “unknown person” icon. These were to be compared against the results of these strings with no icon, tested in Study #2.

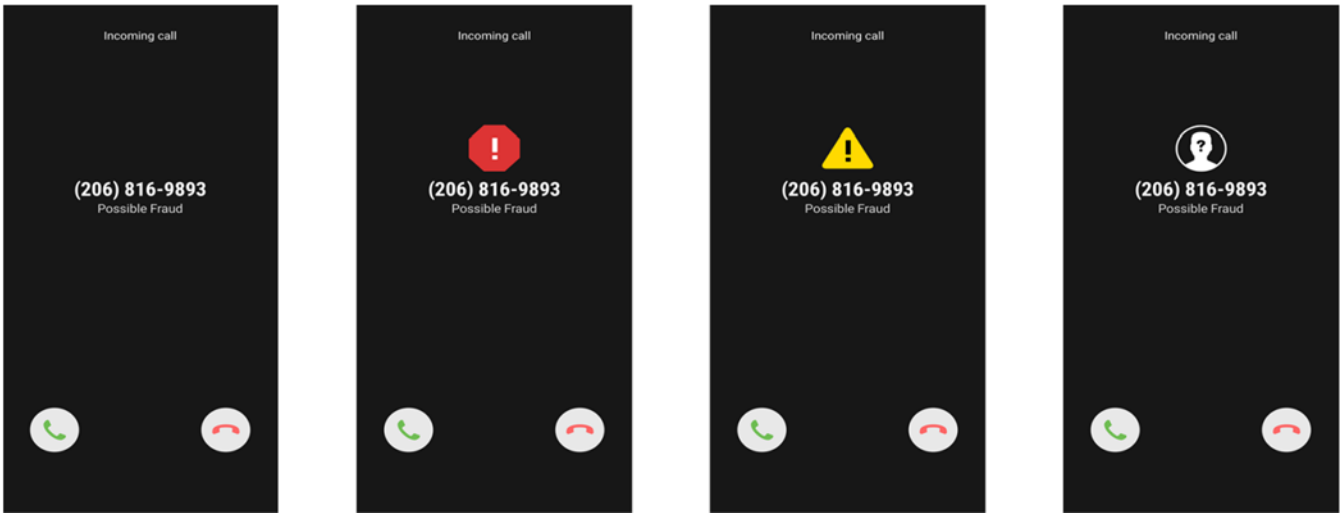


Figure 5.3: Test images for “Possible Fraud” string

Each participant (400 per mockup with no overlap) was asked the same questions as Study #2:

1. Would you answer this call?
2. Was this call from a trustworthy source?
3. Would you block this number from calling in the future?
4. Why do you think you’re receiving this call?

5.4.4.2 Results

The results of this analysis are:

Display	Pickup Rate	Block Rate	User Trust
“Possible Fraud” + no icon	11%	57%	20%
“Fake Number” + no icon	21%	49%	30%
“Possible Fraud” + stop sign	9%	58%	18%
“Fake Number” + stop sign	17%	51%	25%
“Possible Fraud” + warning sign	10%	60%	21%
“Fake Number” + warning sign	17%	54%	25%
“Possible Fraud” + unknown sign	13%	62%	20%
“Fake Number” + unknown sign	18%	50%	30%

5.4.4.3 Conclusions

Further analysis is recommended based on these results. Initial observations:

- The addition of icons has relatively minor impact on block rates, beyond that from text alone. However, in all cases, block rates increased further.
- With the less severe “fake number” string, a supporting icon more strongly reduces pickup rates and overall perception of trustworthiness of the caller.
- With the more severe “possible fraud” string, the less-severe “unknown” icon actually improved pickup rates, tempering the impact of the warning message.

Figure 5.4: Impact on User Trust & Block Rates, By Icon

Looking at all results together as deltas from the default unidentified call result, Hiya arrived at this summary:

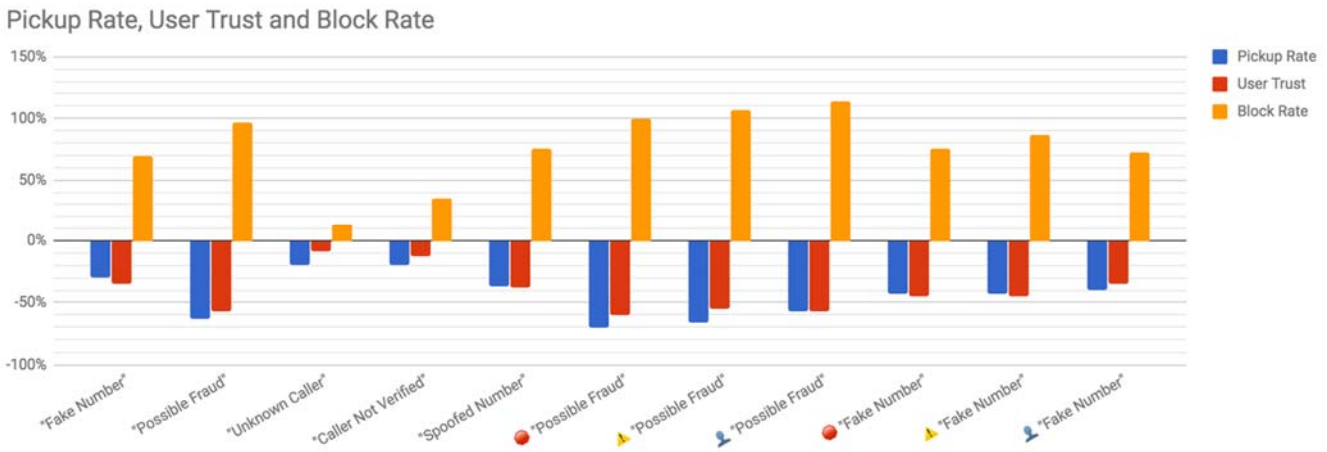


Figure 5.5: Pickup, Trust, & Block Rates for all Text-only & Tested Text+Icon Combinations

5.5 Recommended Data Treatment & Display Options

1) In the absence of an analytics service, and subject to local policy, 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) STIR/SHAKEN and verification information should be made available to the CVT (analytics) service, when available.

The following table summarizes the types of messages that should be displayed to the user based on the results of the STIR/SHAKEN identity verification methodology (ATIS-1000074). This table does not account for other factors, such as operational failures. It may be necessary to define more granular indicators reflecting different causes of failure [e.g., connectivity issues, certificate Time to Live (TTL) expiration] in ATIS-1000074.

Table 5.2: Summary of Proposed Displays to the User

Attestation (by the originating end)	Verification (by the terminating network) of the originator's signature	Availability of Analytics	Message presented to the User
A - Full	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*
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

Attestation (by the originating end)	Verification (by the terminating network) of the originator's signature	Availability of Analytics	Message presented to the User
		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	Not Available	Normal call profile
		Available	Display analytics results*

[1] Delivery of a warning indicator upon verification failure is subject to local policy.

* 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.

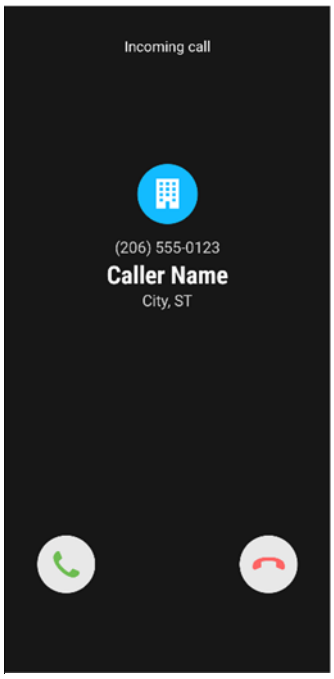
** Some service providers may – based on consumer choice and consent – block these marked calls instead of completing them with a warning.

5.6 Example Displays

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

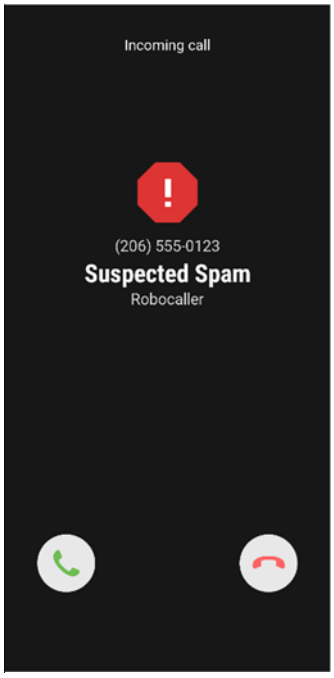
5.6.1 Full Attestation and Verification Passed (No Analytics)

In this scenario, the user does not subscribe to a CVT service. The call, with the 'verstat' tel URI parameter (TN validation passed), is delivered 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).



5.6.2 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 for the caller, but an analytics service has flagged the caller as a known scammer. Therefore, a warning is provided to the user.

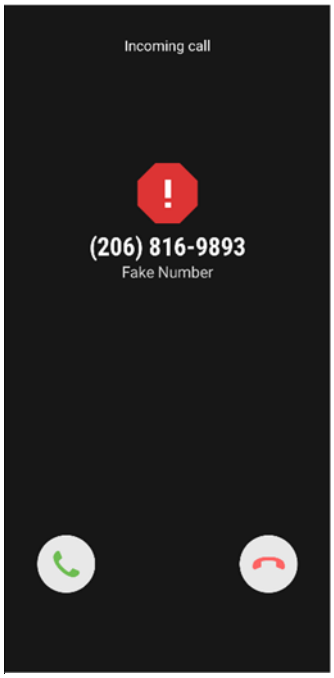


5.6.3 Verification Failed

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

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

Alternatively, a warning would be provided along with an explanation of the reason behind the warning. The end user 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.



5.6.4 Basic Recommendations on the Display or Message delivery to the UE

As a result of the above studies, it is recommended (as supported by the results of Study #1, outlined in Clause 5.4.1), the following display/messaging behavior be adopted:

1. On validation failure, recommend use of words “Fake Number” to inform the user not to trust the number being presented. If an icon can be presented, use of a “stop sign” or warning triangle further increases user caution with negligible impact on block rates. Such a string is short enough to fit in CNAM fields.
2. 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).
3. 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.
4. Displaying status symbols, such as checkmarks, on calls with "full attestation – verification passed", is not recommended (studies show it leads to consumer confusion).
5. It is recommended that only warning symbols be provided when warranted.
6. Audible special ringing/tones may be applied on calls that fail verification as a consumer option.

5.7 Americans with Disabilities Act (ADA) Considerations

- Eight percent of the male population are color-blind. Therefore, the display should not rely heavily on coloration to convey results.

- Ensure messages are clearly understood without industry knowledge (e.g., “spoof”) or strict dependence on sight and/or sound.
- Consider audio announcements for the visually impaired before the call is completed (within the limits of post-dial delays).

6 Display Guidelines for Analog Devices

6.1 Analog Devices Connected to an IP Network

Analog Terminal Adapters (ATA) convert analog voice signals into digital IP packets. ATAs support many features including Caller ID, Call Waiting, and Call Forwarding. ATAs support multiple protocols, including SIP. They also support detection of call progress tones. However, there are no guidelines or standards requiring ATAs to support STIR/SHAKEN authentication and verification functions.

Given that the end user is served by an IP network, the available STIR/SHAKEN information may be relayed to an analytics service that could provide a useful text-based message reflecting the results of the analytics in the conventional CNAM or extended display of the analog device - to the extent allowed by the device display capabilities.

Icons may not be supported by analog devices.

6.2 Analog Devices Connected to Circuit Switched (CS) Network

Efforts at reducing spoofing are likely to increase end user trust in the caller identity information (name and number) and to help empower them in managing their calls. However, end users served by the CS network are less likely to benefit from verification. Effective solutions for this segment of users may be better delivered in consumer devices.

It is recommended that devices allow one or more of the following:

- Storage and management of high volume black and white lists (10,000+ entries).
- End users to manage the lists via simple "button" presses to add/delete numbers from the list.
- A mechanism that screens and reduces robocalls by requiring callers to proactively press a digit through an interactive request to prove the caller is not a robot.
- Optional updates from more diverse reputation sources (e.g., FTC and FCC lists). This could be downloaded periodically to the device, based on end user's subscription.

For this population of users, the available conventional CNAM display – albeit limited – should be used to maximize the caller information delivered/displayed. In addition to the calling number, the end users are encouraged to subscribe to a Name Delivery service. This will help improve their chances of receiving some benefits of analytics about the caller.

7 Related SDOs & Fora

7.1 3GPP

TS 24.229 and TS 29.165 have been modified to support and include syntax for the 'verstat' tel URI parameter.

eCNAM is described in TS 24.196. Stage 1 service description is provided in TS 22.173.

7.2 ATIS

Enhanced Calling Name is described in ATIS-1000067.

7.3 IETF

Authenticated Identity Management in SIP (also referred to as STIR) is described in IETF RFC 8224.