**ATIS-1x000xx**

ATIS Standard on

**SHAKEN Roadmap**

**Alliance for Telecommunications Industry Solutions**

Approved Month DD, YYYY

**Abstract**

This Technical Report provides a roadmap view of the subtending suite of ATIS standards, technical reports, and requirements documents showing the applicability of particular standard specifications in the context of enabling deployment of the needed National Security/Emergency Preparedness (NS/EP) priority related functions and capabilities supporting end-to-end priority communications in Next Generation Networks (NGNs). The ATIS set of standards includes national specific applications of 3GPP, IETF and ITU-T specifications for the support of ETS. This document includes a roadmap of the dependent 3GPP, IETF and ITU-T specifications and standards.

**Foreword**

**Revision History**

| **Date** | **Version** | **Description** | **Author** |
| --- | --- | --- | --- |
|  |  |  |  |

**Table of Contents**

[INSERT]

**Table of Figures**

[INSERT]

**Table of Tables**

[INSERT]

# Scope, Purpose, & Application

## Scope

There are numerous industry standards, technical reports, and requirements documents addressing various aspects for

This Technical Report (TR) provides a roadmap view of the subtending suite of IPNNI standards, technical reports, and requirements documents showing the applicability of particular standard specifications in the context of enabling deployment of Signature-Based Handling of Asserted Information Using Tokens (SHAKEN). This TR includes a roadmap of the dependent 3GPP, IPNNI and IETF specifications and standards.

## Purpose

The purpose of this TR is to provide a consolidated view of various SHAKEN related specifications and provide a roadmap view to enable SHAKEN deployment in NGNs. The objective is to provide a roadmap view showing the applicability of particular specifications to specific network layer, network procedure, interfaces or network element functional capabilities and segments making up the end-to-end NGN infrastructure.

## Application

This document is applicable to the support of SHAKEN in the public NGN infrastructure.

# Normative References

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

**ATIS**

[ATIS-1000074] *Signature-based Handling of Asserted Information using Tokens (SHAKEN)*

[ATIS-0300251.2007 (R2012)] *Codes for Identification of Service Providers for Information Exchange*

[ATIS-1000080] *Signature-based Handling of Asserted information using toKENs (SHAKEN): Governance Model and Certificate Management*

[ATIS-1000081] *Framework for Display of Verified Caller ID*

[ATIS-1000082]  *SHAKEN APIs for a Centralized Signing and Signature Validation Server*

[ATIS-1000084] *Operational and Management Considerations for SHAKEN STI Certification Authorities and Policy Administrators*

[ATIS-1000085] *SHAKEN Support of “div” PASSporT Token*

[ATIS-1000087] *Mechanism for Initial Cross-border Signature-based Handling of Asserted information using toKENs (SHAKEN)*

[ATIS-1000088] *SHAKEN Attestation and Origination Identifier*

[ATIS-100008x]*Study of Full Attestation Alternatives for Enterprises and Business Entities with Multi-Homing and Other Arrangements*

**3GPP**

[TR xx.yyy]

**IETF**

RFC 2986, *PKCS #10: Certification Request Syntax Specification Version 1.7*

RFC 3325, *Private Extensions to SIP for Asserted Identity within Trusted Networks.*1

RFC 3261, *SIP: Session Initiation Protocol.*1

RFC 3326, *The Reason Header Field for the Session Initiation Protocol (SIP).*1

RFC 3647, *Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework*

RFC 3966, *The tel URI for Telephone Numbers*

RFC 4949, *Internet Security Glossary, Version 2*

RFC 5217, *Memorandum for Multi-Domain Public Key Infrastructure Interoperability*

RFC 5280, *Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile.*1

RFC 5905, *Network Time Protocol Version 4 (NTPv4)*

RFC 7159, *The JavaScript Object Notation (JSON)*

RFC 7231, *Hypertext Transfer Protocol (HTTP/1.1): Semantics and Content”*

RFC 7375, *Secure Telephone Identity Threat Model*

RFC 7515, *JSON Web Signatures (JWS)*

RFC 7516, *JSON Web Algorithms (JWA)*

RFC 7517, *JSON Web Key (JWK)*

RFC 7519, *JSON Web Token (JWT)*

RFC 8225, PASSporT: *Personal Assertion Token.*[[1]](#footnote-1)

RFC 8224, *Authenticated Identity Management in the Session Initiation Protocol.*1

RFC 8226, *Secure Telephone Identity Credentials: Certificates.*1

RFC 8555, *Automatic Certificate Management Environment (ACME).*

RFC 8588, *Personal Assertion Token (PASSporT) Extension for Signature-based Handling of Asserted information using toKENs (SHAKEN)*

draft-ietf-acme-authority-token, *ACME Challenges Using an Authority Token.*

draft-ietf-acme-authority-token-tnauthlist, *TNAuthList profile of ACME Authority Token*

draft-ietf-stir-passport-divert*, PASSporT Extension for Diverted Calls*

# 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

See References.

## Acronyms & Abbreviations

|  |  |
| --- | --- |
| 3GPP | 3rd Generation Partnership Project |
| ACME | Automated Certificate Management Environment (Protocol) |
| CA | Certification Authority |
| CP | Certificate Policy |
| CPS | Certification Practice Statement |
| CSR | Certificate Signing Request |
| DN | Distinguished Name |
| DNS | Domain Name System |
| HTTPS | Hypertext Transfer Protocol Secure |
| IETF | [Internet Engineering Task Force](http://www.ietf.org/rfc.html) |
| JSON | JavaScript Object Notation |
| JWA | JSON Web Algorithms |
| JWK | JSON Web Key |
| JWS | JSON Web Signature |
| JWT | JSON Web Token |
| NECA | National Exchange Carrier Association |
| NNI | Network-to-Network Interface |
| NRRA | National/Regional Regulatory Authority |
| OCN | Operating Company Number |
| OCSP | Online Certificate Status Protocol |
| PASSporT | Personal Assertion Token |
| PKI | Public Key Infrastructure |
| PKIX | Public Key Infrastructure for X.509 Certificates |
| PSTN | Public Switched Telephone Network |
| SHAKEN | Signature-based Handling of Asserted information using toKENs |
| SIPREST | Session Initiation ProtocolRepresentational state transfer (REST) |
| SKS | Secure Key Store |
| SMI | Structure of Management Information |
| SP | Service Provider |
| SP-KMS | SP Key Management Server |
| STI | Secure Telephone Identity |
| STI-AS | Secure Telephone Identity Authentication Service |
| STI-CA | Secure Telephone Identity Certification Authority |
| STI-CR | Secure Telephone Identity Certificate Repository |
| STI-GA | Secure Telephone Identity Governance Authority |
| STI-PA | Secure Telephone Identity Policy Administrator |
| STI-VS | Secure Telephone Identity Verification Service |
| STIR | Secure Telephone Identity Revisited |
| TLS | Transport Layer Security |
| TN | Telephone Number |
| URI | Uniform Resource Identifier |
| VoIP | Voice over Internet Protocol |

# Roadmap Overview

This document provides an overview of the specifications that comprise the Signature-based Handling of Asserted Information using Tokens (SHAKEN) Framework. It describes the ATIS specifications and related IETF dependencies in section 5 and 3GPP contributions in section 6. Section 7 of this document provides a summary of the IETF specifications, along with the key dependencies on other IETF specifications.

## Reference Model

The following diagram provides an overview of the SHAKEN framework, highlighting the specifications that provide the protocol details supporting the functionality.



Figure 4.1 –Reference Model

# ATIS/SIP Forum IP Network-Network Interface (IPNNI) Task Force

The ATIS/SIP Forum IPNNI Task Force has developed specifications defining an ecosystem to support the SHAKEN framework in VoIP networks as follows:

* [ATIS-1000074] Signature-based Handling of Asserted Information using Tokens (SHAKEN)
* [ATIS-1000080] Signature-based Handling of Asserted information using toKENs (SHAKEN): Governance Model and Certificate Management
* [ATIS-1000081] Framework for Display of Verified Caller ID
* [ATIS-1000082] SHAKEN APIs for a Centralized Signing and Signature Validation Server
* [ATIS-1000084] Operational and Management Considerations for SHAKEN STI Certification Authorities and Policy Administrators
* [ATIS-1000085] SHAKEN Support of “div” PASSporT Token
* [ATIS-1000087] Mechanism for Initial Cross-border Signature-based Handling of Asserted information using toKENs (SHAKEN)
* [ATIS-1000088] SHAKEN Attestation and Origination Identifier
* [ATIS-1000089]Study of Full Attestation Alternatives for Enterprises and Business Entities with Multi-Homing and Other Arrangements
* IPNNI-2020-00032Rxxx Mechanism for International Signature-based Handling of Asserted information using toKENs (SHAKEN)
* [IPNNI-2020-00025Rxxx] SHAKEN Calling Name and Rich Calling Data Handling Procedures
* [IPNNI-2020-00010Rxxx] SIP RPH Signing in Support of Emergency Calling
* [IPNNI-2020-00021Rxxx] Signature-based Handling of SIP RPH Signing using PASSporT Tokens
* [IPNNI-2020-00022Rxxx] Delegate certificates
* [IPNNI-2020-00026Rxxx] LEveraging MOdels for Enterprise dialiNg - TNauthlist With an enterprise Identity Secured Token (Lemon-Twist)
* [IPNNI-2020-00035Rxxx] Methods to Determine SHAKEN Attestation Levels Using Enterprise-Level Credentials and Telephone Number Letter of Authorization Exchange
* [IPNNI-2020-00023Rxxx] Central TN Database Approach to Full Attestation for Enterprises with Multi-Homing and/or Multi-Tenancy
* [IPNNI-2020-00074Rxxx] Extending STIR/SHAKEN over TDM Interconnects
* [IPNNI-2020-00058Rxxx] Signature-Based Handling of Asserted Information Using Tokens (SHAKEN): Out-of-Band Token Transmission
*

An overview of each of the specifications, along with IETF dependencies are provided in the following sections.

## SHAKEN Framework (ATIS-1000074) and related documents

The Signature-Based Handling of Asserted Information using toKENs (SHAKEN) framework provides a model for deployment of Secure Telephone Identity (STI) technologies to provide end-to-end cryptographic authentication and verification of the telephone identity for calling parties in Voice over IP service provider networks. Additional information about the call origination is also captured at call origination and transported to the terminating network. The SHAKEN framework is based on the use of Session Initiation Protocol (SIP) extensions to sign and validate the calling party identity.

### IETF dependencies

* RFC 3261: SIP: Session Initiation Protocol
* RFC 3325: Private Extensions to SIP for Asserted Identity within Trusted Networks.
* RFC 3326: The Reason Header Field for the Session Initiation Protocol (SIP)
* RFC 3966: The tel URI for Telephone Numbers
* RFC 5280 Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile
* RFC 8224: Authenticated Identity Management in the Session Initiation Protocol*.*
* RFC 8225: Persona Assertion Token
* RFC 8226: Secure Telephone Identity Credentials: Certificates
* RFC 8588 SHAKEN PASSporT extensions

### Related SHAKEN Framework documents

The following proposal, referred to as “AT&T’s Tagging Optimization”, is premised on the fact that many calls originating in a service provider’s network stay within that network:

  <https://access.atis.org/apps/group_public/download.php/33957/IPNNI-2017-00037R000.pdf>

So, rather than signing the calls at origination, the information that would be required to build the PASSporT is captured at the time of call in origination in SIP P- headers. If, and when, the call leaves the service provider’s network, the P- headers are used to populate the fields in the PASSporT by invoking the Signing and Signature Validation Server (SSVS) API described in section 5.2.

## Authentication/Verification Service API  (ATIS-1000082)

This document introduces an optional API between the Authentication and Verification Services and a centralized signing and signature validation server to the SHAKEN Framework [ATIS-1000074]. In many cases the signing and validation of the signature require cryptographic processors such as Hardware Security Modules (HSMs) for optimal performance. This API facilitates a model whereby the core AS functionality is deployed on an existing application server in the service provider’s network as opposed to a standalone AS server.

The following diagram highlights the functional model introduced to support the API:



## Display Framework (ATIS-1000081)

This document provides guidelines related to the display of verified Caller ID information on the User Equipment (UE) in a uniform manner. The guidelines are in the form of 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). The guidelines are not prescriptive, but rather are recommendations for consideration by all stakeholders (service providers, equipment manufacturers and analytics providers) in the deployment of verified Caller ID displays and composition of its related messages.

## SHAKEN: Governance and Certificate Management (ATIS-1000080)

This specification expands the SHAKEN framework to introduce a governance model and X.509 Public Key Infrastructure (PKI) certificate management procedures. The certificate management procedures provide mechanisms for creating and validating certificates as well as a means for verification of the associated digital signature to allow identification of illegitimate use of the

The following diagram identifies the functional elements and interfaces involved in the Certificate Management Procedures:



### IETF dependencies

* RFC 5280: Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile
* RFC 7231:Hypertext Transfer Protocol (HTTP/1.1): Semantics and Content
* RFC 7519:JSON Web Token (JWT*)*
* RFC 8226: Secure Telephone Identity Credentials: Certificates
* RFC 8555: Automatic Certificate Management Environment (ACME)

draft-ietf-acme-authority-token: *ACME Challenges Using an Authority Token.*

* draft-ietf-acme-authority-token-tnauthlist: *TNAuthList profile of ACME Authority Token*

### Certificate Management informational documents

* RFC 4949: Internet Security Glossary, Version 2
* RFC 5217: Memorandum for Multi-Domain Public Key Infrastructure Interoperability
* RFC 5905:Network Time Protocol Version 4 (NTPv4)
* RFC 7375: Secure Telephone Identity Threat Model.

The following presentations provide overviews related to the SHAKEN Certificate Management Framework:

[Editor’s note; It’s probably a useful exercise to update these overviews to reflected published ACME specs, new model for ACME challenge response mechanism and other changes in ATIS-1000080-v002 and ATIS-1000084]

* Overview of SHAKEN Certificate Management framework as defined in ATIS-1000080:

[https://access.atis.org/apps/group\_public/download.php/35614/IPNNI-2017-00085R001.pdf](https://access.atis.org/apps/group_public/download.php/35614/IPNNI-)

* ACME Protocol Overview:

<https://access.atis.org/apps/group_public/download.php/35615/IPNNI-2017-00084R001.pdf>

* Overview of SHAKEN's use of ACME:

[https://access.atis.org/apps/group\_public/download.php/35605/IPNNI-2017-00091R000.pdf](https://access.atis.org/ap)

##  Operational and Management Considerations for SHAKEN STI Certification Authorities and Policy Administrator (ATIS-1000084)

This document introduces operational and management considerations for STI Certification Authorities (STI-CAs) within the context of the SHAKEN framework [ATIS-1000074] and the SHAKEN: Governance Model and Certificate Management framework [ATIS-1000080]. This document focuses on the operational and management aspects that impact the authentication and verification services, as well as general Certification Authority (CA) practices and policies. The document addresses the STI-PA operational aspects of managing the list of STI-CAs and authorization of Service Providers to obtain STI certificates.

The following diagram highlights the functional elements and interfaces described in this document:



The following diagram illustrates the Trust Model for the SHAKEN Certificate Management framework, underlying the functionality that is provided by the STI-PA:



### IETF dependencies

* RFC 3647:Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework
* RFC 5280: Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile
* RFC 7231:Hypertext Transfer Protocol (HTTP/1.1): Semantics and Content
* RFC 7519:JSON Web Token (JWT*)*
* RFC 8224: Authenticated Identity Management in the Session Initiation Protocol (SIP)
* RFC 8226: Secure Telephone Identity Credentials: Certificates

### Operational and Management Considerations for SHAKEN STI-CAs and STI-PAs informational documents

* RFC 4949: Internet Security Glossary, Version 2
* RFC 5217: Memorandum for Multi-Domain Public Key Infrastructure Interoperability
* RFC 5905:Network Time Protocol Version 4 (NTPv4)

The following document provides an overview of the Operational and Management Considerations for SHAKEN STI-CAs and STI-Pas document:

<http://access.atis.org/apps/group_public/document.php?document_id=35562&wg_abbrev=ipnni>

## SHAKEN Support of “div” PASSporT Token (ATIS-1000085)

The base SHAKEN specification provides replay-detection mechanisms to identify cases where a malicious entity attempts to masquerade as another user by replaying parts of a legitimate INVITE request. However, these mechanisms don’t cover cases where the INVITE is replayed within the short Date freshness window. This technical report describes how the mechanisms defined by [draft-ietf-stir-passport-divert] can be integrated within the SHAKEN framework to close this replay attack window.

### IETF Dependencies

### Informational Documents

## Mechanism for Initial Cross-border Signature-based Handling of Asserted information using toKENs (SHAKEN) (ATIS-1000087)

This document provides an Initial mechanism to extend the SHAKEN trust environment to include more than one country without requiring service providers to make changes to their current standard SHAKEN interfaces. Note that a longer term solution is described in section 5.10.

### IETF Dependencies

### Informational Documents

## A Framework for SHAKEN Attestation and Origination Identifier (ATIS-1000088)

This technical report provides a framework for SHAKEN (ATIS-1000074) attestation and granularity of the Origination Identifier. The population of attestation indicator and origination identifier in the SHAKEN Identity header relies on decisions the originating service provider (originating SP) makes based on the type of interface at the ingress to its network, knowledge of the customer or SP entity it has received the call from, and knowledge or agreements as to the calling party telephone numbers (calling TNs) used on the interface. These determinations are made both through administrative and security management procedures as well as security services applied at call processing time. The resulting values are provided to the SHAKEN Secure Telephone Identity Authentication Service (STI-AS) function to be passed with the protected call data. This report documents the characteristics of the security services applied at the User-to-Network Interface or Network-to-Network Interface of an originating SP, and some guidelines for the population of SHAKEN attestation indicator and origination identifier based on these services. The material and guidelines presented here should be considered informative, as practice and norms can be expected to evolve with deployment and industry experience.

### IETF Dependencies

### Informational Documents

## Study of Full Attestation Alternatives for Enterprises and Business Entities with Multi-Homing and Other Arrangements (ATIS-1000089)

Several solution proposals have been developed and defined as baselines to allow for the authentication of the calling party for various enterprise models and other scenarios whereby the TN customer and calling party is not the TN owner. IPNNI-2019-00075R005 provides an overview of the problem space and a summary of the characteristics of the various solution options, which includes the following:

* Delegate certificates: IPNNI-2020-00022Rxxx
* LEveraging MOdels for Enterprise dialiNg - TNauthlist With an enterprise Identity Secured Token (Lemon-Twist): IPNNI-2020-00026Rxxx
* Enterprise Certificates: IPNNI-2019-00086R0xx
* Methods to Determine SHAKEN Attestation Levels Using Enterprise-Level Credentials and Telephone Number Letter of Authorization Exchange: IPNNI-2020-00035Rxxx
* Central TN Database Approach to Full Attestation for Enterprises with Multi-Homing and/or Multi-Tenancy: IPNNI-2020-00023Rxxx

### IETF Dependencies

### Informational Documents

##  Mechanism for International Signature-based Handling of Asserted information using toKENs (SHAKEN)

This document (IPNNI-2020-00032Rxxx) provides telephone service providers with a framework and guidance on how to use Secure Telephone Identity (STI) technologies on IP-based service provider voice networks (also to be referred to as Voice over Internet Protocol [VoIP] networks) in scenarios where a call originates in one country and terminates in a different country. ATIS-1000087 “*Mechanism for Initial Cross-Border Signature-based Handling of Asserted information using toKENs (SHAKEN)*” provides an initial mechanism for cross-border SHAKEN calls, but it recognizes that it is only the first step, and that a more general approach is required to accommodate the general cases of international SHAKEN calls. In particular, it is not scalable for all countries to execute bilateral agreements. That is a 1932 problem. The purpose of this document is to detail how to extend SHAKEN while maintaining the SHAKEN trust framework. This document does not require any changes to the existing SHAKEN specifications but does identify new interfaces and functions to exchange information between countries.

### IETF Dependencies

### Informational Documents

## SHAKEN Calling Name and Rich Calling Data Handling Procedures

This document (IPNNI-2020-00025Rxxx) introduces a set of procedures for the use of calling name (CNAM) and Rich Call Data (RCD) in the SHAKEN framework [ATIS-1000074] and [ATIS-1000080] and with TN certificates using certificate delegation [ATIS delegate-cert document]. The SHAKEN framework establishes an end-to-end architecture that allows a telephone service provider to authenticate and assert a telephone identity and provides for the verification of this telephone identity by a terminating service provider. The SHAKEN framework defines a profile, using protocols standardized in the IETF Secure Telephone Identity Revisited (STIR) Working Group (WG), providing recommendations and requirements for implementing these IETF specifications, [RFC 8225], [RFC8224], and [RFC 8226], to support management of Service Provider-level certificates within the SHAKEN framework.

This document extends the SHAKEN framework beyond authentication of only the telephone number identity to include more traditional CNAM data, typically in the form of a string, of the name of the calling party displayed to the called party. It also discusses the use of draft-ietf-stir-passport-rcd which defines a PASSporT [RFC8225] extension for enhanced calling party data such as name, address, photos, logos, and other extensible information that may be extended in the future to enable the secure, verified transport of data relevant to the calling party that can be displayed or passed to the called party.

### IETF Dependencies

### Informational Documents

## SIP Resource Priority Header Signing in Support of Emergency Calling

This document (IPNNI-2020-00010Rxxx) defines how extension to the IETF STIR PASSporT and the associated STIR mechanisms are used to sign the Session Initiation Protocol Resource Priority Header (SIP RPH) header field and convey assertions of authorization for Resource-Priority. This standard provides a procedure for providing cryptographic authentication and verification of the information in the Session Initiation Protocol Resource Priority Header (SIP RPH) field in Internet Protocol (IP)-based service provider communication networks in support of National Security / Emergency Preparedness Next Generation Priority Services (NS/EP NGN-PS). Specifically, this document provides a mechanism for a originating NS/EP NGN-PS Service Provider to cryptographically-sign the SIP RPH and allow a receiving NS/EP NGN-PS Service Provider to verify the validity of the authorization for Resource-Priority and act on the information with confidence (i.e., verifying that the RPH information have not been spoofed or compromised).

Editor’s note: This description is appropriate for the other document on SIP RPH, IPNNI-2020-00021Rxxx, which needs to be added.

### IETF Dependencies

In addition to the dependencies identified for [ATIS-1000074] in section 5.15.1, this document also has the following IETF dependencies:

* RFC 4412 Communications Resource Priority for the Session Initiation Protocol (SIP)
* RFC 7135 Registering a SIP Resource Priority Header Field Namespace for Local Emergency Communications
* RFC 8225 PASSporT: Personal Assertion Token
* RFC 8224 Authenticated Identity Management in the Session Initiation Protocol
* RFC 8226 Secure Telephone Identity Credentials: Certificates
* RFC 8443 PASSporT Extension for Resource-Priority Authorization
* draft-ietf-stir-rph-emergency-services Assertion Values for a Resource Priority Header Claim in Support of Emergency Services Networks.
	+ Keep for RPH for Emergency Calling; don’t move to RPH for NSEP

### Informational Documents

[Editor’s note: Is there any overviews that we should point to?]

##  Extending STIR/SHAKEN over TDM Interconnects

This document (IPNNI-2020-00074Rxxx) the current SHAKEN framework to enable transferring verified attestation levels over TDM interconnects.

### IETF Dependencies

In addition to the dependencies identified for [ATIS-1000074] in section 5.15.1, this document also has the following IETF dependencies:

* RFC 4122: A Universally Unique IDentifier (UUID) URN Namespace
* RFC 7044: An Extension to the Session Initiation Protocol (SIP) for Request History Information
* draft-ietf-stir-oob: STIR Out-of-Band Architecture and Use Cases
* draft-peterson-stir-servprovider-oob: Out-of-Band STIR for Service Providers

### Informational Documents

##  Signature-Based Handling of Asserted Information Using Tokens (SHAKEN): Out-of-Band Token Transmission

This document (IPNNI-2020-00058Rxxx) extends the STIR/SHAKEN framework to enable an originating service provider to send caller identity PASSporTs to the terminating service provider out-of-band, that is, separate from the telephone network signaling. The mechanisms described in this specification are based on the STIR Out-of-Band Architecture and Use Cases defined in [draft-ietf-stir-oob] and Out-of-Band STIR for Service Providers in [draft-peterson-stir-servprovider-oob].

### IETF Dependencies

In addition to the dependencies identified for [ATIS-1000074] in section 5.15.1, this document also has the following IETF dependencies:

* RFC 4122: A Universally Unique IDentifier (UUID) URN Namespace
* RFC 7044: An Extension to the Session Initiation Protocol (SIP) for Request History Information
* draft-ietf-stir-oob: STIR Out-of-Band Architecture and Use Cases
* draft-peterson-stir-servprovider-oob: Out-of-Band STIR for Service Providers

### Informational Documents

# 3GPP

The table below list the 3GPP CT1 Agreed CRs:

|  |  |  |  |
| --- | --- | --- | --- |
| C1-164324 | Robo-Calling and Spoofing of Telephone Numbers and Need for Verification Tel URI Parameter | Discussion Paper |  |
| C1-164851 | New WID on User Controlled Spoofed Call Treatment (SPECTRE-CT) | Work Item |  |
| C1-164863 | Indication of calling number verification | Procedures are added, allowing the home network to inform UEs about its support of calling number verification during registration, and allowing the home network to inform UEs about the calling number verification status (or to inform the UE that calling number verification has not been performed) in an initial INVITE request and MESSAGE request.Reference to draft-ietf-stir-rfc4474bis is added. | TS 24.229 |
| C1-170132 | Robo-Calling and Spoofing of Telephone Numbers and Need for draft RFC 4474bis and “666” | Discussion Paper |  |
| C1-170421 | Addition of the Unwanted response | The response code 666 (Unwanted) is specified in draft-ietf-sipcore-status-unwanted for the user to be able to indicate that an incoming call is unwanted. This information can then be used by the network to take further actions.Adding a Reason header with protocol SIP and cause unwanted for call release.Adding support for the unwanted response code to annex A. | TS 24.229 |
| C1-170487 | Identity verification using the Identity header procedures | A new subclause 5.7.1.x is added.New originating procedures added to this subclause.Text added in Guilin to 5.7.1.4 for terminating procedures is moved to this new subclause.Support for authenticated identity management added to Annex A | TS 24.229 |
| C1-171062 | Presence of a "verstat" tel URI parameter in the From header field | A "verstat" tel URI parameter in a tel URI or a SIP URI with a user=phone parameter may be present in the P-Asserted-Identity header field or in the From header field in the initial INVITE and MESSAGE requests.However, in subclauses 5.1.2A.2 and 7.2A.20.1 the presence of the "verstat" tel URI parameter is indicated only in the P-Asserted-Identity header field.Subclauses 5.1.2A.2 and 7.2A.20.1: added that the "verstat" tel URI parameter can be present in the From header field. | TS 24.229 |
| C1-171326 | Addition of missing 4xx response codes for SPECTRE to profile tables | SIP failure response codes 428, 436, 437 and 438 are added to the Annex A profile tables.the UA major capability related to draft-ietf-stir-rfc4474bis is also made applicable to the MGCF, MSC server enhanced for ICS, SRVCC or DRVCC roles. | TS 24.229 |
| C1-172576 | Profile Table Correction for 666 | Currently support for 666 (Unwanted) response is not correctly shown in the profile tables in Annex A.Table A.162 and Table A.164 don’t have entries for 666 (Unwanted) | TS 24.229 |
| C1-172256 | Usage of sip.666 | Network to use the feature capability indicator to indicate to UE in 200 (OK) to REGISTER to UE that it supports 666.UE to take this information into account. | TS 24.229 |
| C1-171999 | Reference update: draft-ietf-stir-rfc4474bis | The version number of draft-ietf-stir-rfc4474bis is updated to reflect the latest draft version. | TS 24.229 |
| C1-172921 | RFC 8197 available | RFC 8197 replaces draft-ietf-sipcore-status-unwanted-06. No technical changes that would impact 24.229 are made. | TS 24.229 |
| C1-174986 | IANA registration for “verstat” complete |  | TS 24.229 |
| C1-174987 | IANA registration for “verstat” complete |  | TS 24.229 |
| C1-180374 | Enhancements to SPECTRE | Discussion Paper for eSPECTRE WID |  |
| C1-180637 | Enhancements to Call spoofing functionality | eSPECTRE WID |  |
| C1-181109 | Reference update: RFC 8224 | IETF draft-ietf-stir-rfc4474bis has now been published as RFC 8224, and therefore the specification requires updating to the published version. | TS 24.229 |
| C1-181110 | Reference update: RFC 8224 | IETF draft-ietf-stir-rfc4474bis has now been published as RFC 8224, and therefore the specification requires updating to the published version. | TS 24.229 |

The table below list the 3GPP CT3 Agreed CRs:

|  |  |  |  |
| --- | --- | --- | --- |
| C3-171045 | Robo-Calling and Spoofing of Telephone Numbers | Discussion Paper |  |
| C3-171072 | Support of "Calling number verification” | Support of a "Calling number verification" feature in accordance to procedures defined in TS 24.229 needs to be included in TS 29.163.If a "Calling number verification" feature is supported, and if the I-MGCF received a "verstat" tel URI parameter within the P-Asserted-ID and From SIP header fields in the initial INVITE request the I-MGCF may map the verstat" tel URI parameter to the Screening Indicator field of the ISUP Calling Party Number and Generic (Additional Calling Party Number parameters.If a "Calling number verification" feature is supported, then the called UE can send a 666 (Unwanted) response to the initial INVITE request or a BYE request with a Reason header field with a protocol value set to "SIP" and a "cause" header field parameter set to "666" to indicate that an incoming call is unwanted. If the MGCF receives the 666 (Unwanted) response to the initial INVITE request or the BYE request with the Reason header field with the protocol value set to "SIP" and a "cause" header field parameter set to "666" then the MGCF should map SIP status code "666 (Unwanted)" to the cause value "21 (Call rejected)" of the cause value field. | TS 29.163 |
| C3-171221 | Support of "Calling number verification” | Support of a "Calling number verification" feature over the II-NNI in accordance to procedures defined in TS 24.229 needs to be included in TS 29.165.Support of the "Calling number verification" added in:- subclause 6.1.1.3.4 - added applicability of the Identity header field;- subclause 6.1.3. - major capabilities;- new clause X;- annex A – added support of the Identity header field;- annex B– added support of the Identity header field in the INVITE and MESSAGE requests; and- subclause C.3.1. | TS 29.165 |
| C3-171137 | Reception of 666 (Unwanted) response | If a "Calling number verification" feature is supported, then the called UE can send a 666 (Unwanted) response to the initial INVITE request or a BYE request with a Reason header field with a protocol value set to "SIP" and a "cause" header field parameter set to "666" to indicate that an incoming call is unwanted.If the MSC Server receives the 666 (Unwanted) response to the initial INVITE request or the BYE request with the Reason header field with the protocol value set to "SIP" and a "cause" header field parameter set to "666" then the MSC Server should map SIP status code "666 (Unwanted)" to the cause value "21 (Call rejected)" of the cause information element. | TS 29.292 |
| C3-172035 | Mapping of additional 4xx response codes for SPECTRE | SIP failure response codes 428, 436, 437 and 438 are mapped to ISUP Cause Value No 127 (Interworking, unspecified).IETF draft-ietf-stir-rfc4474bis introduces the following SIP failure response codes in subclause 6.2.2:  A 428 response will be sent (per Section 6.2) when an Identity header field is required, but no Identity header field without a "ppt" parameter, or with a supported "ppt" value, has been received. In the case where one or more Identity header fields with unsupported "ppt" values have been received, then a verification service may send a 428 with a human-readable reason phrase like "Use Supported PASSporT Format". Note however that this specification gives no guidance on how a verification service might decide to require an Identity header field for a particular SIP request. Such authorization policies are outside the scope of this specification.  The 436 'Bad Identity Info' response code indicates an inability to acquire the credentials needed by the verification service for validating the signature in an Identity header field. Again, given the potential presence of multiple Identity header fields, this response code should only be sent when the verification service is unable to deference the URIs and/or acquire the credentials associated with all Identity header fields in the request. This failure code could be repairable if the authentication service resends the request with an 'info' parameter pointing to a credential that the verification service can access.  The 437 'Unsupported Credential' is sent when a verification service can acquire, or already holds, the credential represented by the 'info' parameter of at least one Identity header field in the request, but does not support said credential(s), for reasons such as failing to trust the issuing CA, or failing to support the algorithm with which the credential was signed.  The 438 'Invalid Identity Header' response indicates that of the set of Identity header fields in a request, no header field with a valid and supported PASSporT object has been received. Like the 428 response, this is sent by a verification service when its local policy dictates that a broken signature in an Identity header field is grounds for rejecting a request. Note that in some cases, an Identity header field may be broken for other reasons than that an originator is attempting to spoof an identity: for example, when a transit network alters the Date header field of the request. Sending a full form PASSporT can repair some of these conditions (see Section 6.2.4), so the recommended way to attempt to repair this failure is to retry the request with the full form of PASSporT if it had originally been sent with the compact form. The alternative reason phrase 'Invalid PASSporT' can be used when an extended full form PASSporT lacks required headers or claims, or when an extended full form PASSporT signaled with the "ppt" parameter lacks required claims for that extension. Sending a string along these lines will help humans debugging the sending system. All those errors are network internal and SIP-specific and do not have an equivalent ISUP cause. | TS 29.163 |
| C3-172036 | Mapping of additional 4xx response codes for SPECTRE | SIP failure response codes 428, 436, 437 and 438 are mapped to cause information element value No 127 (Interworking, unspecified) in the CC DISCONNECT message.IETF draft-ietf-stir-rfc4474bis introduces the following SIP failure response codes in subclause 6.2.2:  A 428 response will be sent (per Section 6.2) when an Identity header field is required, but no Identity header field without a "ppt" parameter, or with a supported "ppt" value, has been received. In the case where one or more Identity header fields with unsupported "ppt" values have been received, then a verification service may send a 428 with a human-readable reason phrase like "Use Supported PASSporT Format". Note however that this specification gives no guidance on how a verification service might decide to require an Identity header field for a particular SIP request. Such authorization policies are outside the scope of this specification.  The 436 'Bad Identity Info' response code indicates an inability to acquire the credentials needed by the verification service for validating the signature in an Identity header field. Again, given the potential presence of multiple Identity header fields, this response code should only be sent when the verification service is unable to deference the URIs and/or acquire the credentials associated with all Identity header fields in the request. This failure code could be repairable if the authentication service resends the request with an 'info' parameter pointing to a credential that the verification service can access.  The 437 'Unsupported Credential' is sent when a verification service can acquire, or already holds, the credential represented by the 'info' parameter of at least one Identity header field in the request, but does not support said credential(s), for reasons such as failing to trust the issuing CA, or failing to support the algorithm with which the credential was signed.  The 438 'Invalid Identity Header' response indicates that of the set of Identity header fields in a request, no header field with a valid and supported PASSporT object has been received. Like the 428 response, this is sent by a verification service when its local policy dictates that a broken signature in an Identity header field is grounds for rejecting a request. Note that in some cases, an Identity header field may be broken for other reasons than that an originator is attempting to spoof an identity: for example, when a transit network alters the Date header field of the request. Sending a full form PASSporT can repair some of these conditions (see Section 6.2.4), so the recommended way to attempt to repair this failure is to retry the request with the full form of PASSporT if it had originally been sent with the compact form. The alternative reason phrase 'Invalid PASSporT' can be used when an extended full form PASSporT lacks required headers or claims, or when an extended full form PASSporT signaled with the "ppt" parameter lacks required claims for that extension. Sending a string along these lines will help humans debugging the sending system. All those errors are network internal and SIP-specific and do not have an equivalent cause information element value. | TS 29.292 |
| C3-172091 | Support of feature capability indicator "sip.666" | Currently, the specification does not contain a requirement to support a feature capability indicator "sip.666", defined in IETF in draft-ietf-sipcore-status-unwanted.If the network supports a SIP response code "666 (Unwanted)" the S-CSCF will include the "sip.666" feature-capability indicator in a 200 (OK) final response to a REGISTER request.If the UE is roaming, the "sip.666" feature-capability indicator when included in a Feature-Caps header field in the 200 (OK) response to the REGISTER request should be supported at the roaming II-NNI.Added that a "sip.666" feature-capability indicator when included in a Feature-Caps header field in a 200 (OK) response to a REGISTER request shall be supported at the roaming II-NNI. | TS 29.165 |
| C3-173190 | Reference update: draft-ietf-sipcore-status-unwanted | The version number of draft-ietf-sipcore-status-unwanted is updated to reflect the latest draft version.Response code value for unwanted calls (reason phrase "Unwanted") changed from "666" to "607". | TS 29.163 |
| C3-173191 | Reference update: draft-ietf-sipcore-status-unwanted | The version number of draft-ietf-sipcore-status-unwanted is updated to reflect the latest draft version.Response code value for unwanted calls (reason phrase "Unwanted") changed from "666" to "607". | TS 29.292 |
| C3-173192 | Support of feature capability indicator "sip.607" | Added that a "sip.666" feature-capability indicator when included in a Feature-Caps header field in a 200 (OK) response to a REGISTER request shall be supported at the roaming II-NNI.Changes from CT3 #89 meeting agreed version in C3-172091:- the version number of draft-ietf-sipcore-status-unwanted is updated to reflect the latest draft version;- response code value for unwanted calls (reason phrase "Unwanted") changed from "666" to "607"; and- name of the feature-capability indicator changed from "sip.666" to "sip.607". | TS 29.165 |
| C3-173021 | Reference update: draft-ietf-stir-rfc4474bis | The version number of draft-ietf-stir-rfc4474bis is updated to reflect the latest draft version. | TS 29.163 |
| C3-173022 | Reference update: draft-ietf-stir-rfc4474bis | The version number of draft-ietf-stir-rfc4474bis is updated to reflect the latest draft version. | TS 29.165 |
| C3-173072 | Mapping of additional 4xx response codes for SPECTRE | SIP failure response codes 428, 436, 437 and 438 are mapped to cause information element value No 127 (Interworking, unspecified) in the CC DISCONNECT message.Changes from CT3 #89 meeting agreed version in C3-172036:the version number of draft-ietf-stir-rfc4474bis is updated to reflect the latest draft version. | TS 29.292 |
| C3-174101 | Reference update from draft-ietf-sipcore-status-unwanted-06 to RFC 8197 | RFC 8197 replaces draft-ietf-sipcore-status-unwanted-06.There are no technical changes between the draft and the RFC.Rel 14 | TS 29.163 |
| C3-174102 | Reference update from draft-ietf-sipcore-status-unwanted-06 to RFC 8197 | RFC 8197 replaces draft-ietf-sipcore-status-unwanted-06.There are no technical changes between the draft and the RFC.Rel 14 | TS 29.165 |
| C3-174103 | Reference update from draft-ietf-sipcore-status-unwanted-06 to RFC 8197 | RFC 8197 replaces draft-ietf-sipcore-status-unwanted-06.There are no technical changes between the draft and the RFC.Rel 15 | TS 29.165 |
| C3-174104 | Reference update from draft-ietf-sipcore-status-unwanted-06 to RFC 8197 | RFC 8197 replaces draft-ietf-sipcore-status-unwanted-06.There are no technical changes between the draft and the RFC. | TS 29.292 |
| C3-174224 | Added the profile status in proxy role regarding “A SIP Response Code for Unwanted Calls” | The profile status in proxy role about “A SIP Response Code for Unwanted Calls” was specified in TS 24.229. For alignment between 3GPP specifications, it should be reflected to TS 29.165.In Addition, there are editorial errors in TS 29.165. - In subclause 3.3, there is capital letter(misspell) about MCData.- In item 83 of table 6.1.3.1, there is wrong reference name. | TS 29.165 |
| C3-181048 | Reference update: RFC 8224 | IETF draft-ietf-stir-rfc4474bis has now been published as RFC 8224, and therefore the specification requires updating to the published version. Rel 14 | TS 29.163 |
| C3-181049 | Reference update: RFC 8224 | IETF draft-ietf-stir-rfc4474bis has now been published as RFC 8224, and therefore the specification requires updating to the published version. Rel 15 | TS 29.163 |
| C3-181050 | Reference update: RFC 8224 | IETF draft-ietf-stir-rfc4474bis has now been published as RFC 8224, and therefore the specification requires updating to the published version. Rel 14 | TS 29.165 |
| C3-181051 | Reference update: RFC 8224 | IETF draft-ietf-stir-rfc4474bis has now been published as RFC 8224, and therefore the specification requires updating to the published version. Rel 15 | TS 29.165 |
| C3-181052 | Reference update: RFC 8224 | IETF draft-ietf-stir-rfc4474bis has now been published as RFC 8224, and therefore the specification requires updating to the published version. Rel 14 | TS 29.292 |
| C3-181053 | Reference update: RFC 8224 | IETF draft-ietf-stir-rfc4474bis has now been published as RFC 8224, and therefore the specification requires updating to the published version. Rel 15 | TS 29.292 |
|  |  |  |  |

# IETF

This section provides a roadmap of dependent IETF RFCs. The SHAKEN framework [ATIS-1000074] is dependent upon IETF Session Initiation Protocol (SIP) RFCs as well as the RFCs developed in the Secure Telephone Identity Revisited (STIR) WG. The SHAKEN Certificate Management framework is dependent upon core Public Key Infrastructure (PKI) specifications as well as those in the Automated Certificate Management (ACME) WG specifications. Note that this is not a complete list of RFCs required as each of the RFCs identified below also has dependencies – a complete list of these can be found for each document in the IETF datatracker.

The IETF RFCs are organized into two tables as follows:

* Documents providing normative requirements and/or protocols for support of SHAKEN Framework and SHAKEN Governance and Certificate Management Framework

|  |  |  |  |
| --- | --- | --- | --- |
| Document | Title | Description | Key Dependencies |
| RFC3325 | *Private Extensions to SIP for Asserted Identity within Trusted Networks.* | Defines the P-Asserted-Identity header field that allows a Service Provider to assert an Identity other than what’s in the To Header field. In the context of SHAKEN, the P-Asserted-Identity header field, if present, is used to populate the PASSporT “orig” field .  | RFC 3261 |
| RFC 3261 | *SIP: Session Initiation Protocol.* | Core SIP Protocol specification |  |
| RFC 3326 | *The Reason Header Field for the Session Initiation Protocol (SIP).* |  | RFC 3261 |
| RFC 3966 | *The tel URI for Telephone Numbers* | The STIR/SHAKEN is premised on the use of tel URIs in the TO, FROM and PAI header fields in the SIP signaling.  | RFC 3261 |
| RFC 5280 | *Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile.*1 | Defines the including the format for the PKI certificate extended by STIR per  |  |
| RFC 7159 | *The JavaScript Object Notation (JSON)* | The format for the contents of the PASSporT is based on JSON. | Obsoleted by RFC 8259 |
| RFC 7231 | *Hypertext Transfer Protocol (HTTP/1.1): Semantics and Content”* | The interfaces between the Service Provider and the STI-PA and STI-CA are based on HTTP.  |  |
| RFC 7515 | *JSON Web Signatures (JWS)* | JSON Web Signature (JWS) represents content secured with digital signatures using JSON-based data structures.  | RFC 7159, RFC 7518 |
| RFC 7516 | *JSON Web Encryption (JWE)* | JSON Web Encryption (JWE) represents encrypted content using JSON-based data structures. | RFC 7159, RFC 5280, RFC 7518 |
| RFC 7517 | *JSON Web Key (JWK)* | A JSON Web Key (JWK) is a JavaScript Object Notation (JSON) data structure that represents a cryptographic key. This specification also defines a JWK Set JSON data structure that represents a set of JWKs.  | RFC 7159, RFC 7518 |
| RFC 7518 | *JSON Web Algorithm* | This specification registers cryptographic algorithms and identifiers to be used with the JSON Web Signature (JWS), JSON Web Encryption (JWE), and JSON Web Key (JWK) specifications. | RFC 7159 |
| RFC 7519 | *JSON Web Token (JWT)* | The PASSporT included in the SIP Identity header field is encoded as a JWT.  | RFC 7159, RFC 7515, RFC 7516, RFC 7517, RFC 7518 |
|  |  |  |  |
| RFC 8224 | *Authenticated Identity Management in the Session Initiation Protocol.*1 | Defines the syntax and semantics for the SIP Identity header field, updating RFC 4447. | RFC 8226 |
| RFC 8225  | *Persona Assertion Token.*[[2]](#footnote-2) | Defines the syntax and semantics for the PASSporT field in the SIP Identity header field. | RFC 8224, RFC 7519 |
| RFC 8226 | *Secure Telephone Identity Credentials: Certificates.*1 | Defines the procedures for the use of PKI in the context of STIR. Defines an extension to the RFC 5280 Certificate format to include TNs and Service Provider codes.  | RFC 5280 |
| RFC 8259(Obsoletes RFC 7519) | *The JavaScript Object Notation (JSON)* | The format for the contents of the PASSporT is based on JSON. |  |
| RFC 8588  | PASSporT SHAKEN Extension (SHAKEN) | Defines the syntax and semantics for the SHAKEN specific extensions to the PASSporT.  | RFC 8225, ATIS-1000074 |
| RFC 8555 | *Automatic Certificate Management Environment (ACME).*  | Defines the protocol used by the Service Provider to request certificates from the STI-CA.  | RFC 2986  |
| draft-ietf-acme-authority-token | *ACME Challenges Using an Authority Token* | Defines the generic mechanism for the ACME challenge response using an Authority Token | RFC 8555, ATIS-1000080 |
| draft-ietf-acme-authority-token-tnauthlist | *TNAuthList profile of ACME Authority Token* | Defines the SHAKEN specific mechanism for the ACME challenge using the Authority Token | RFC 8555, ATIS-1000080, draft-ietf-acme-authority-token |

* Documents providing general reference material and informational guidelines, related to the normative SHAKEN specifications.

|  |  |  |
| --- | --- | --- |
| Document | Title | Description |
| RFC 3647 | *Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework* | Provides a framework and details for Certificate Policies (CPs) to be established by the STI-PA and Certification Practice Statements (CPSs) to be provided by STI-CAs during the approval process.  |
| RFC 4949 | *Internet Security Glossary, Version 2*  | Defines terminology used for PKI, certificates, etc. that provide the baseline for terminology used in ATIS-1000074, ATIS-1000080 and ATIS-1000084. |
| RFC 5217 | *Memorandum for Multi-Domain Public Key Infrastructure Interoperability* | Defines a model for Multi-domain PKI that defines considerations for the SHAKEN Trust Domain model introduced in ATIS-1000080 and ATIS-1000084. |
| RFC 5905 | *Network Time Protocol Version 4 (NTPv4)* | Recommended to be implemented by the STI-PA, STI-CA and Service Providers to ensuring time is aligned to ensure consistency and predictability with regards to the expiry of certificates, Service Provider Code tokens along with various timestamps (e.g., IAT in the PASSporT).  |
| RFC 7375 | *Secure Telephone Identity Threat Model* | Introduces the threat model for STIR, which imposes some requirements on the signaling solution and certificate management procedures.  |

1. Available from the Internet Engineering Task Force (IETF) at: < <https://www.ietf.org/> >. [↑](#footnote-ref-1)
2. Available from the Internet Engineering Task Force (IETF) at: < <https://www.ietf.org/> >. [↑](#footnote-ref-2)