**A****TIS-1000XXX**

ATIS Standard on

**Signature-based Handling of Asserted information using toKENs (SHAKEN):
Calling Name and Rich Call Data Handling Procedures**

**Alliance for Telecommunications Industry Solutions**

Approved Month 00, 2019

**Abstract**

Signature-based Handling of Asserted information using toKENs (SHAKEN) is an industry framework for managing and deploying Secure Telephone Identity (STI) technologies with the purpose of providing end-to-end cryptographic authentication and verification of the telephone identity and other information in an IP-based service provider voice network. This specification expands the SHAKEN framework, introducing a mechanisms for authentication, verification, and transport of CNAM, Rich Call Data and how they a handled in various origination and termination proceedures.

**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

[**ATIS-1000XXX** i](#_Toc1226910)

[ATIS Standard on i](#_Toc1226911)

[**Signature-based Handling of Asserted information using toKENs (SHAKEN): Calling Name and Rich Call Data Handling Procedures** i](#_Toc1226912)

[**Alliance for Telecommunications Industry Solutions** i](#_Toc1226913)

[**Abstract** i](#_Toc1226914)

[Table of Figures iii](#_Toc1226915)

[1 Scope & Purpose 1](#_Toc1226916)

[1.1 Scope 1](#_Toc1226917)

[1.2 Purpose 1](#_Toc1226918)

[2 Normative References 1](#_Toc1226919)

[3 Definitions, Acronyms, & Abbreviations 2](#_Toc1226920)

[3.1 Definitions 2](#_Toc1226921)

[3.2 Acronyms & Abbreviations 2](#_Toc1226922)

[4 Overview 3](#_Toc1226923)

[5 SHAKEN CNAM and RCD Model 3](#_Toc1226924)

[5.1 Requirements for Governance of STI Certificate Management 3](#_Toc1226925)

[5.2 Certificate Governance: Roles & Responsibilities 4](#_Toc1226926)

[Appendix A – XXX 5](#_Toc1226927)

[Examples 5](#_Toc1226928)

# Table of Figures

[Figure 5.1 – Governance Model for Certificate Management 4](#_Toc1226929)

# Scope & Purpose

## Scope

This document expands the Signature-based Handling of Asserted Information using Tokens (SHAKEN) [ATIS-1000074] framework, introducing a governance model and defining certificate management procedures for Secure Telephone Identity (STI) technologies. The certificate management procedures identify the functional entities and protocols involved in the distribution and management of STI Certificates. The governance model identifies functional entities that have the responsibility to establish policies and procedures to ensure that only authorized entities are allowed to administer digital certificates within Voice over Internet Protocol (VoIP) networks. However, the details of these functional entities in terms of regulatory control and who establishes and manages those entities are outside the scope of this document.

## Purpose

This document introduces a governance model, certificate management architecture, and related protocols to the SHAKEN framework [ATIS-1000074]. The governance model defines recommended roles and relationships, such that the determination of who is authorized to administer and use digital certificates in VoIP networks can be established. This model includes sufficient flexibility to allow specific regulatory requirements to be implemented and evolved over time, minimizing dependencies on the underlying mechanisms for certificate management. The certificate management architecture is based on the definition of roles similar to those defined in “Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile”, [Internet Engineering Task Force](http://www.ietf.org/rfc.html) (IETF) [RFC 5280]. Per the SHAKEN framework, the certificates themselves are based on X.509 with specific policy extensions based on [RFC 8226]. The objective of this document is to provide recommendations and requirements for implementing the protocols and procedures for certificate management within the SHAKEN framework.

# 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-1000074, *Signature-based Handling of Asserted Information using Tokens (SHAKEN).*[[1]](#footnote-1)

RFC 3261, *SIP: Session Initiation Protocol.*4

RFC 7515, *JSON Web Signatures (JWS).*4

RFC 7516, *JSON Web Algorithms (JWA).*4

RFC 7517, *JSON Web Key (JWK).*4

RFC 7519, *JSON Web Token (JWT).*4

RFC 8224, *Authenticated Identity Management in the Session Initiation Protocol*.4

RFC 8225, *Personal Assertion Token (PASSporT)*.[[2]](#footnote-2)

RFC 8226, *Secure Telephone Identity Credentials: Certificates*4

# 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

The following provides some key definitions used in this document. Refer to IETF RFC 4949 for a complete Internet Security Glossary, as well as tutorial material for many of these terms.

**Caller ID:** The originating or calling party’s telephone number used to identify the caller carried either in the P-Asserted-Identity or From header fields in the Session Initiation Protocol (SIP) [RFC 3261] messages.

**Identity:** Either a canonical Address-of-Record (AoR) SIP Uniform Resource Identifier (URI) employed to reach a user (such as ’sip:alice@atlanta.example.com’), or a telephone number, which commonly appears in either a TEL URI [RFC 3966] or as the user portion of a SIP URI. See also Caller ID [RFC 8224].

**National/Regional Regulatory Authority (NRRA):** A governmental entity responsible for the oversight/regulation of the telecommunication networks within a specific country or region.

NOTE: Region is not intended to be a region within a country (e.g., a region is not a state within the US).

**Signature:** Created by signing the message using the private key. It ensures the identity of the sender and the integrity of the data [RFC 4949].

**Telephone Identity:** An identifier associated with an originator of a telephone call. In the context of the SHAKEN framework, this is a SIP identity (e.g., a SIP URI or a TEL URI) from which a telephone number can be derived.

## Acronyms & Abbreviations

|  |  |
| --- | --- |
| AoR | Address-of-Record |
| ATIS | Alliance for Telecommunications Industry Solutions |
| CNAM | Conventional Caller Name |
| eCNAM | Enhanced Caller Name |
| 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 |
| NNI | Network-to-Network Interface |
| OCN | Operating Company Number |
| PASSporT | Personal Assertion Token |
| PSTN | Public Switched Telephone Network |
| SHAKEN | Signature-based Handling of Asserted information using toKENs |
| SIP | Session Initiation Protocol |
| RCD | Rich Call Data |
| REST | Representational State Transfer |
| SP | Service Provider |
| STI | Secure Telephone Identity |
| STIR | Secure Telephone Identity Revisited |
| TN | Telephone Number |
| URI | Uniform Resource Identifier |
| VoIP | Voice over Internet Protocol |

# Overview

This document introduces a set of procedures for the use of calling name (CNAM) and Rich Call Data (RCD) in the SHAKEN framework [ATIS-1000074]. The SHAKEN framework establishes an end-to-end architecture that allows an originating 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 the telephone identity to include more traditional CNAM data typically 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.

There is various ways CNAM data is transmitted to the called party device today, these methods will be discussed and how the SHAKEN framework can provide validation of that data for each of these models. Additionally, for newer RCD types of data similar transmission and verification models will be discussed. Finally, a set of guidelines around how this data should be presented to the called party will be defined.

# SHAKEN CNAM and RCD Model Overview

Traditional CNAM which has been in use for many years in the telephone network from analog to digital telephones has provided the ability to show a 15-character string to the called party in a telephone call. The 15-character string is used to display a caller or company name corresponding to the calling party. This traditional CNAM is generally either passed through the call signaling or is inserted into the call at the terminating communications service provider (CSP) via a dip to a CNAM database.

Note: The 15-character string was derived from a limitation of SS7 Network and telephone user equipment limitations. However, recently, in ATIS and 3GPP, eCNAM was defined and described in [ATIS-1000067], [3GPP TS 22.173] and [3GPP TS 24.196]. eCNAM extends the ability to provide a longer name with 35 characters in the display-name SIP parameter plus additional data in one or more Call-Info headers.

As the industry moves away from string and text-based displays to more modern display of calling party information like mobile phone displays, Caller-ID to the TV services, and other enhanced displays capable of displaying more and different types of data like images, graphics at different sizes, using fonts and font sizes adapted to the device being displayed, a framework for the transport and authentication/verification of this rich data is required.

This document provides a model and framework to use the SHAKEN framework and extend it to provide both a model that can support both the security of traditional CNAM and eCNAM calling name strings transported in SIP as well as both the transport and security of RCD in an extensible way to support current and future needs and applications that want to pass identity and other information related to the calling party to the called party.

IETF has defined the RCD PASSporT extension in [draft-ietf-stir-passport-rcd] which defines the base STIR PASSporT claim ‘rcd’. This claim includes an extensible JSON object that has two specified key values. A ‘nam’ claim for validation of a CNAM string as well as a ‘jcd’ key value which is defined to support the jCard, the JSON format or vCard defined in [RFC7095] which is itself an extensible JSON object for the transport of personal identifiable types of information.

Using the RCD PASSporT extension and specifically the ‘rcd’ claim the following sections of this document will detail the use of ‘rcd’ claim depending on the call model either independently or as part of the ‘shaken’ PASSporT to validate CNAM and RCD data to the calling party.

# SHAKEN CNAM and RCD Framework Definition

This section will provide details of the procedures associated with the addition of inclusion of the ‘rcd’ PASSporT or inclusion of the ‘rcd’ claim into a ‘shaken’ PASSporT. Both of these procedures are used for supporting different service provider specific CNAM and RCD scenarios.

## ‘rcd’ claim construction overview

In [draft-ietf-stir-passport-rcd] there are three main key values possible as part of the ‘rcd’ claim. They are ‘nam’ which is a minimally required key value as part of the ‘rcd’ claim value JSON object, ‘jcd’ which is the key value that represents the direct inclusion of a jCard string in the ‘rcd’ claim, and ‘jcl’ which is the key value that represents an HTTPS URL link to a jCard file hosted on an HTTPS server. Both the ‘jcd’ and ‘jcl’ key values are optional, can only be included a maximum of one time in a ‘rcd’ claim, and are mutually exclusive where you can not have both key values. The following sections provide more details on how the ‘rcd’ JSON object is constructed.

### Traditional CNAM using ‘nam’

If a SIP INVITE contains a display-name parameter for From or P-Asserted-ID, the ‘rcd’ claim must contain a ‘nam’ key value that has a value with a string that matches exactly the ASCII values of the display-name parameter.

Example, for the following SIP INVITE

INVITE sip:+12155551213@biloxi.com SIP/2.0

Via: SIP/2.0/UDP pc33.atlanta.com;branch=z9hG4bK776asdhds

Max-Forwards: 70

To: “Bob” <sip:+12155551213@biloxi.com; user=phone>

From: “Alice” <sip:+12155551212@atlanta.com; user=phone>;tag=1928301774

Call-ID: a84b4c76e66710@pc33.atlanta.com

CSeq: 314159 INVITE

Date: Sat, 13 Nov 2015 23:29:00 GMT

Contact: <sip:alice@pc33.atlanta.com>

Content-Type: application/sdp

Content-Length: 142

This is an example of an ‘rcd’ extension PASSporT

Protected Header

{

 "alg":"ES256",

 "typ":"passport",

 “ppt”:”rcd”,

 "x5u":"https://biloxi.example.org/biloxi.cer”

}

Payload

{

 "dest":{“tn”:["12155551213"]}

 "iat":1443208345,

 "orig":{“tn”:"12155551212"},

 "rcd":{"nam":"Alice"}

}

This is an example of an ‘shaken’ extension PASSporT that includes an ‘rcd’ claim

Protected Header

{

 "alg":"ES256",

 "typ":"passport",

 “ppt”:”shaken”,

 "x5u":"https://biloxi.example.org/biloxi.cer”

}

Payload

{

 “attest”:”A”

 "dest":{“tn”:["12155551213"]}

 "iat":1443208345,

 "orig":{“tn”:"12155551212"},

 “origid”:”123e4567-e89b-12d3-a456-426655440000”,

 "rcd":{"nam":"Alice"}

}

### RCD using ‘jcd’ with an embedded jCard

A ‘jcd’ key value for a ‘rcd’ claim should be constructed with the value being equal to a jCard string. At a minimum the jCard should include a “fn” and one “tel” objects for SHAKEN. Note: Additional objects are optional but may be ignored or disregarded by the receiving entity depending on the rendering capabilities of the device and/or network local policy.

This is an example of an ‘rcd’ extension PASSporT with ‘jcd’

Protected Header

{

 "alg":"ES256",

 "typ":"passport",

 “ppt”:”rcd”,

 "x5u":"https://biloxi.example.org/biloxi.cer”

}

Payload

{

 "dest":{“tn”:["12155551213"]}

 "iat":1443208345,

 "orig":{“tn”:"12155551212"},

 "rcd":{"nam":"James Bond","jcd":["vcard",[["version",{},"text","4.0"],

 ["fn",{},"text", "James Bond"],

 ["n",{},"text",["Bond","James","","","Mr."]],

 ["adr",{"type":"work"},"text",

 ["","","3100 Massachusetts Avenue NW","Washington","DC","20008","USA"]

 ],

 ["email",{},"text","007@mi6-hq.com"],

 ["tel",{"type":["voice","text","cell"],"pref":"1"},"uri",

 "tel:+1-202-555-1000"],

 ["tel",{"type":["fax"]},"uri","tel:+1-202-555-1001"],

 ["bday",{},"date","19241116"],

 ["logo",{},"uri",

 "https://upload.wikimedia.org/wikipedia/en/c/c5/Fleming007impression.jpg"

 ]]]}}

}

This is an example of an ‘shaken’ extension PASSporT that includes an ‘rcd’ claim

Protected Header

{

 "alg":"ES256",

 "typ":"passport",

 “ppt”:”shaken”,

 "x5u":"https://biloxi.example.org/biloxi.cer”

}

Payload

{

 “attest”:”A”

 "dest":{“tn”:["12155551213"]}

 "iat":1443208345,

 "orig":{“tn”:"12155551212"},

 “origid”:”123e4567-e89b-12d3-a456-426655440000”,

 "rcd":{"nam":"James Bond","jcd":["vcard",[["version",{},"text","4.0"],

 ["fn",{},"text", "James Bond"],

 ["n",{},"text",["Bond","James","","","Mr."]],

 ["adr",{"type":"work"},"text",

 ["","","3100 Massachusetts Avenue NW","Washington","DC","20008","USA"]

 ],

 ["email",{},"text","007@mi6-hq.com"],

 ["tel",{"type":["voice","text","cell"],"pref":"1"},"uri",

 "tel:+1-202-555-1000"],

 ["tel",{"type":["fax"]},"uri","tel:+1-202-555-1001"],

 ["bday",{},"date","19241116"],

 ["logo",{},"uri",

 "https://upload.wikimedia.org/wikipedia/en/c/c5/Fleming007impression.jpg"

 ]]]}}

}

### RCD using ‘jcl’ with a URL to jCard

A ‘jcl’ key value for a ‘rcd’ claim should be constructed with the value being equal to an HTTPS URL of a file hosted on an HTTPS server containing a jCard string. At a minimum the linked jCard file should include a “fn” and one “tel” objects for SHAKEN. Note: Additional objects are optional but may be ignored or disregarded by the receiving entity depending on the rendering capabilities of the device and/or network local policy.

This is an example of an ‘rcd’ extension PASSporT with ‘jcl’

Protected Header

{

 "alg":"ES256",

 "typ":"passport",

 “ppt”:”rcd”,

 "x5u":"https://biloxi.example.org/biloxi.cer”

}

Payload

{

 "dest":{“tn”:["12155551213"]}

 "iat":1443208345,

 "orig":{“tn”:"12155551212"},

 "rcd":{"nam":"James Bond","jcl":"https://example.org/james\_bond.json"}

}

This is an example of an ‘shaken’ extension PASSporT that includes an ‘rcd’ claim

Protected Header

{

 "alg":"ES256",

 "typ":"passport",

 “ppt”:”shaken”,

 "x5u":"https://biloxi.example.org/biloxi.cer”

}

Payload

{

 “attest”:”A”

 "dest":{“tn”:["12155551213"]}

 "iat":1443208345,

 "orig":{“tn”:"12155551212"},

 “origid”:”123e4567-e89b-12d3-a456-426655440000”,

 "rcd":{"nam":"James Bond","jcl":"https://example.org/james\_bond.json"}

}

## Calling Name Authentication and Verification Scenarios

There are a number of methods that CNAM and RCD authentication and verification scenarios can be implemented in a VoIP network between the originating and terminating telephone service providers as part of a SHAKEN implementation. This section details the procedures involved in some of the common implementations of these scenerios. This isn’t intended to be a complete list, rather illustrating example deployments.

### Origination side ‘rcd’ authentication

For call scenarios where the rich call data authentication is performed at the origination of the call the following steps

1. Call is initiated by UE
2. The STI-AS constructs and signs the ‘shaken’ PASSporT that includes the ‘rcd’ claim including display-name and optionally jCard information about the telephone number account holder.
3. INVITE is sent over NNI to destination provider.
4. STI-VS receives INVITE with identity header containing ‘shaken’ PASSporT with ‘rcd’ claim
5. STI-CR is queried to get public key certificate associated with PASSport signature.
6. If verification is successful, verstat is added to PAID, identity header with ‘rcd’ claim is sent to UE.



#### Termination procedures for pass-thru ‘shaken’ with ‘rcd’ claim identity header

Option 1. Keep SHAKEN PASSporT with ‘rcd’ claim and UE can validate or use verstat indicator to determine verified status and displays CNAM/RCD

#### Termination procedures for new ‘rcd’ identity header

Option 2. Inspect ‘shaken’ identity header, extracts ‘rcd’ claim, and creates new ‘rcd’ identity header and signs with certificate that UE can validate and/or use verstat indicator to determine verified status and display CNAM/RCD

### Termination side ‘rcd’ authentication

Termination carrier receives call without SHAKEN ‘rcd’

Validates SHAKEN PASSporT

Adds verstat to PAID

Does CNAM/RCD lookup for verified TN

Creates new ‘rcd’ identity header and signs with certificate that UE can validate and/or use verstat indicator to determine verified status and display CNAM/RCD

## Calling Name Authentication and Verification Scenarios – Third-party service ‘rcd’ authentication

Text

## UE procedures

Provide basic guidelines for how CNAM and RCD are rendered to user. A framework that only has basic rules to make sure there is consistency in providing identity information to user, to the extent the display is capable of displaying information with different priority levels and clear indication of validation of the CNAM/RCD information.

In the jCard specification there is a large set of different identity information that is available, not all displays have either the ability or screen space to render an unlimited amount of data. The following is a suggested set of prioritized data to display for CNAM/RCD.

First priority: Calling Name

Second priority: Telephone number

Third priority: logo, image, City/State from address, full address, additional telephone numbers, email address

### Analog or Limited Text display procedures

Most analog or textual displays only have the ability to show CNAM information, possibly the telephone number. When the CNAM information is verified, the UE must render the “[V]” string before the Calling Name on the display for as many characters available for the display.

Optionally, UEs that read the CNAM using a text to speech synthesizer may interpret the “[V]” characters as the ability to announce “Verified Caller”.

### SIP enabled enhanced Text display procedures

In the case of future SIP based UEs that have textual displays, the use of “[V]” should follow the procedures defined above in the last section above. Optionally, a SIP enabled UE that understands verstat or can verify the ‘rcd’ claim in the identity header can provide a clear separate “verified” indicator or a dedicated LCD icon corresponding to the graphical display procedures defined in the next section below.

Optionally, UEs that read the CNAM using a text to speech synthesizer may interpret the inclusion of verstat or validation of the ‘rcd’ claim in an identity header directly as the ability to announce “Verified Caller”.

### Graphical display procedures

The CNAM and RCD data should be displayed to the extent possible in priority order. The verified CNAM/RCD icon, defined in Appendix B, should be displayed

If there is any logos or images included in a jCard, the verified icon should not ever be rendered in the same space as the image or logo to prevent any confusion of parts of the image/logo with the verified logo.

### Local address book procedures(?)

Optionally, define rules for providing validation of local/network address book entries based on comparing information passed in CNAM/RCD.

# Appendix A – CNAM and RCD Verified Text based Indicator

## Examples

Below shows photos of example usage of “[V]”

 

Figure 5.1 – Examples of Textual validated indicators

# Appendix B – CNAM and RCD Verified Graphical Indicator

## Graphics

The icon indicating CNAM and RCD information is verified is designed to be used on light and dark background as shown in the below figures. The size of the icons can be modified to be appropriate for the device, so the exact pixel sizes are for example only, however the proportions should remain exact and the icon should remain as consistent as possible to promote recognizability by consumers. The icon MUST not be combined with any other images or graphics where the icon could be spoofed in any way and should stand on its own or combined with reinforcing “verified” words to make a clear impression that the CNAM or RCD information is verified.



Figure 5.1 – 1024 px x 1024 px white background

  

Figure 5.1 – 128 px, 32 px, 16 px white background



Figure 5.1 – 1024 px x 1024 px white background

  

Figure 5.1 – 128 px, 32 px, 16 px white background

## SVG Source Code

The SVG representation of the icon is as follows.

<?xml version="1.0" encoding="UTF-8" standalone="no"?>

<!DOCTYPE svg PUBLIC "-//W3C//DTD SVG 1.1//EN" "http://www.w3.org/Graphics/SVG/1.1/DTD/svg11.dtd">

<svg width="100%" height="100%" viewBox="0 0 1024 1024" version="1.1" xmlns="http://www.w3.org/2000/svg" xmlns:xlink="http://www.w3.org/1999/xlink" xml:space="preserve" xmlns:serif="http://www.serif.com/" style="fill-rule:evenodd;clip-rule:evenodd;stroke-linecap:round;stroke-linejoin:round;stroke-miterlimit:1.5;">

 <path id="path" d="M512,13L419.05,134.885L280.103,70.158L254.442,221.277L101.331,228.536L148.838,374.271L16.638,451.853L126.43,558.817L45.427,688.948L192.352,732.637L181.102,885.507L331.501,855.912L392.582,996.5L512,900.401L631.418,996.5L692.499,855.912L842.898,885.507L831.648,732.637L978.573,688.948L897.569,558.817L1007.36,451.853L875.162,374.271L922.669,228.536L769.557,221.277L743.897,70.158L604.95,134.885L512,13Z" style="fill:rgb(61,166,0);fill-rule:nonzero;"/>

 <g transform="matrix(0.931161,0,0,0.931161,5.06784,64.0201)">

 <path d="M765.35,337.248L459.32,643.279L318.177,502.136" style="fill:none;stroke:white;stroke-width:128.87px;"/>

 </g>

</svg>

## Examples

Below shows examples of icon usage on graphical displays

1. This document is available from the Alliance for Telecommunications Industry Solutions (ATIS) at: < <https://www.atis.org/docstore/product.aspx?id=28297> >. [↑](#footnote-ref-1)
2. This document is available from the Internet Engineering Task Force (IETF) at: < <https://tools.ietf.org/> >. [↑](#footnote-ref-2)