**ATIS-1000100**

ATIS Technical Report on

**VoIP Interconnection over the Public Internet**

**Alliance for Telecommunications Industry Solutions**

Approved xxxx xx, 2022

**Abstract**

This document describes a “non-facilities-based VoIP Interconnection" profile, where IP connectivity between VoIP Service Providers is established over the public internet.

**Foreword**

The Alliance for Telecommunications Industry Solutions (ATIS) serves the public through improved understanding between carriers, 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.

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.

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.

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**

[1 Executive Summary 1](#_Toc118900678)

[1.1 Scope 1](#_Toc118900679)

[1.2 Purpose 1](#_Toc118900680)

[2 References 1](#_Toc118900681)

[3 Definitions, Acronyms, & Abbreviations 2](#_Toc118900682)

[3.1 Definitions 2](#_Toc118900683)

[3.2 Acronyms & Abbreviations 2](#_Toc118900684)

[4 Overview 4](#_Toc118900685)

[4.1 Reference Architecture 4](#_Toc118900686)

[4.1.1 Architecture for TLS Option 4](#_Toc118900687)

[4.1.2 Architecture for IPsec Option 5](#_Toc118900688)

[5 Non-Facilities-Based VoIP Interconnection Procedures 6](#_Toc118900689)

[5.1 Information to support Non-Facilities-Based VoIP Interconnection 6](#_Toc118900690)

[5.1.1 Additional Information Exchanged for TLS Option 6](#_Toc118900691)

[5.2 Procedures to Establish/Use the Non-Facilities-Based VoIP Interconnection Interface 6](#_Toc118900692)

[5.2.1 Locating SIP Servers 6](#_Toc118900693)

[5.2.2 Signaling Transport, Security and Authentication 6](#_Toc118900694)

[5.2.3 Media Transport, Security and Audio Profile 9](#_Toc118900695)

**Table of Figures**

[Figure 4.1 – Non-Facilities-Based VoIP Interconnection Reference Architecture for TLS Option 4](#_Toc118900696)

[Figure 4.2 – Non-Facilities-Based VoIP Interconnection Reference Architecture for IPsec Option 5](#_Toc118900697)

[Figure 4.3 – Non-Facilities-Based VoIP Interconnection using VPN Gateways for IPsec Option 5](#_Toc118900698)

**Table of Tables**

[Table 5.1 – IPSec/IKE Configuration Parameters – Recommended Minimum 8](#_Toc118883291)

[Table 5.2 – SRTP Parameters 9](#_Toc118883292)

# Executive Summary

## Scope

This Technical Report describes an interconnect profile for VoIP Service Providers who choose to interconnect over the public internet. It recommends mechanisms for establishing IP connectivity, securing the signaling and media, and proposing bilateral agreements with respect to codec selection to address QoS impacts as well as resources for real-time media traversing the unmanaged public internet.

The report does not describe the SIP interworking procedures between interconnected VoIP Service Providers. Furthermore, automation regarding network discovery – including points of interconnection and telephone number ranges exchanged is out of scope of this document.

## Purpose

This report is to coexist with ATIS-1000063, *Joint ATIS/SIP Forum Technical Report – IP NNI Profile*, as well as expand on options available for carriers to leverage the public internet for VoIP Interconnection. The expansion of options that can be agreed to on a bilateral basis will accelerate adoption of VoIP interconnect as well as support for STIR-SHAKEN protocols to combat Robocalling.

# References

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

[Ref 1] ATIS-1000063 *Joint ATIS/SIP Forum Technical Report – IP NNI Profile*.[[1]](#footnote-2)

[Ref 2] RFC 3711 *Secure Real-time Transport Protocol*.[[2]](#footnote-3)

[Ref 3] RFC 2409 *The Internet Key Exchange (IKE)*.2

[Ref 4] RFC 4306 *Internet Key Exchange (IKEv2) Protocol*.2

[Ref 5] RFC 4568 *SDP Security Descriptions*.2

[Ref 6] RFC 4949 *Internet Security Glossary, Version 2*.2

[Ref 7] RFC 5246 *The Transport Layer Security (TLS) Protocol, Version 1.2*.2

[Ref 8] RFC 5280 *Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile*.2

[Ref 9] RFC 5763 *Framework for Establishing a Secure Real-time Transport Protocol (SRTP) Security Context Using Datagram Transport Layer Security (DTLS)*.2

[Ref 10] RFC 5764 *Datagram Transport Layer Security (DTLS) Extension to Establish Keys for the Secure Real-time Transport Protocol (SRTP)*.2

[Ref 11] RFC 5922 *Domain Certificates in the Session Initiation Protocol (SIP)*.2

[Ref 12] RFC 8446 *The Transport Layer Security (TLS) Protocol, Version 1.3*.2

[Ref 13] RFC 9162 *Certificate Transparency Version 2.0*.2

# 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

**Certification Authority (CA):** An entity that issues digital certificates (especially X.509 certificates) and vouches for the binding between the data items in a certificate [RFC 4949, *Internet Security Glossary, Version 2*].

**(Digital) Certificate:** Binds a public key to a Subject (e.g., the end-entity). A certificate document in the form of a digital data object (a data object used by a computer) to which is appended a computed digital signature value that depends on the data object [Ref 6]. See also STI Certificate.

**End-Entity:** An entity that participates in the Public Key Infrastructure (PKI). Usually a Server, Service, Router, or a Person. In the context of SHAKEN, it is the Service Provider on behalf of the originating endpoint.

**Non-Facilities-Based VoIP Interconnection**: refers to the case where the Network-to-Network Interface (NNI) interconnection between two Service Providers is over the public internet.

## Acronyms & Abbreviations

|  |  |
| --- | --- |
| ATIS | Alliance for Telecommunications Industry Solutions |
| CA | Certificate Authority |
| CRL | Certificate Revocation List |
| DNS | Domain Name System |
| DTLS | Datagram Transport Layer Security |
| IKE | Internet Key Exchange |
| IP | Internet Protocol |
| IPsec | IP Security |
| LERG | Local Exchange Routing Guide |
| LRN | Location Routing Number |
| NAPTR | Naming Authority Pointer Record |
| NNI | Network-to-Network Interface |
| OCN | Operating Company Number |
| PKI | Public Key Infrastructure |
| QoS | Quality of Service |
| RTCP | Real-time Transport Control Protocol |
| RTP | Real-time Transport Protocol |
| SBC | Session Border Controller |
| SHAKEN | Signature-based Handling of Asserted information using toKENs |
| SIP | Session Initiation Protocol |
| SP | Service Provider |
| SRTCP | Secure RTCP |
| SRTP | Secure RTP |
| SRV | SeRVice record |
| STIR | Secure Telephone Identity Revisited |
| TCP | Transmission Control Protocol |
| TLS | Transport Layer Security |
| TN | Telephone Number |
| UDP | User Datagram Protocol |
| URI | Uniform Resource Identifier |
| VoIP | Voice over IP |
| VPN | Virtual Private Network |

# Overview

VoIP Service Providers (“SPs”) traditionally interconnect through a carrier hotel, where the managed IP networks of the two SPs are connected via private dedicated facilities. The carrier hotel model has good security and quality-of-service characteristics due to the physical security provided by the carrier hotel building and the direct non-shared facilities connecting the managed networks of the two SPs.

This document describes a “non-facilities-based VoIP Interconnection" model, where IP connectivity between SPs is established over the public internet. Since calls traverse the public internet in this case, special measures must be taken so that calls are delivered securely and with adequate quality. First, strong authentication mechanisms must be in place to ensure that Interconnected SPs can identify each other. Second, call signaling and media shall be encrypted to protect them from eavesdropping or manipulation via man-in-the-middle attacks while traversing the open internet. Finally, while the use of fixed-rate codecs (e.g., G.711 µ-law) with jitter adaptation and packet-loss concealment in the media endpoints may provide adequate voice quality within certain public network routing paths and conditions, SPs may choose to utilize modern codec technology that incorporates the use of adaptive bit-rate support and forward error correction techniques to tolerate the potential of varying congestion levels encountered on the public internet. When it is not possible to use these codecs on an end-to-end transcoder-free basis, which would provide the highest voice quality and least use of resources in both SP networks, SPs may bilaterally agree to a transcoding scheme that distributes the resource usage and minimizes the number of transcoding operations on the same media stream as described in Clause 5.2.3.2 below.

## Reference Architecture

This document describes two options for securing call traffic exchanged between peering VoIP Service Providers (SP) over the non-facilities-based VoIP Interconnection:

**TLS Option:** Call signaling is secured using Transport Layer Security (TLS), while media is secured using Secure Real-time Transport Protocol (SRTP).

**IPsec Option:** Call signaling is secured using Internet Protocol Security (IPsec), while media is secured either using SRTP or by conveying the media in the same IPsec tunnel that secures the signaling.

### Architecture for TLS Option

Figure 4.1 shows the reference architecture for the non-facilities-based VoIP Interconnection interface when the peering partners choose the TLS option. Peering partners VoIP SP-1 and SP-2 each deploy a Session Border Controller (SBC) at their peering interconnect point to support SIP signaling and media on the non-facilities-based VoIP Interconnection interface. SIP signaling across the interconnection interface is protected by Transport Layer Security (TLS) with mutual authentication. The media on the interconnection interface is anchored at the Media Endpoint of each SBC. The media is protected by SRTP.



Figure 4.1 – Non-Facilities-Based VoIP Interconnection Reference Architecture for TLS Option

### Architecture for IPsec Option

Figure 4.2 shows the reference architecture for the non-facilities-based VoIP Interconnection model when the peering partners choose the IPsec option. SP-1 and SP-2 each deploy a Session Border Controller (SBC) at their interconnect point to support SIP signaling and media on the non-facilities-based VoIP Interconnect interface. SIP signaling across the interconnect interface is protected by IPsec with mutual authentication. Media may be protected by streaming within the same IPsec tunnel as used for signaling or using SRTP if outside the IPsec tunnel. How media is handled is subject to bilateral communications and mutual agreement between the two SPs.



Figure 4.2 – Non-Facilities-Based VoIP Interconnection Reference Architecture for IPsec Option

For some SPs, implementing IPsec tunnels for SIP signaling and/or RTP in a separate VPN gateway may simplify deployment and security policy. Figure 4.3 shows a reference architecture for this implementation.

****

Figure 4.3 – Non-Facilities-Based VoIP Interconnection using VPN Gateways for IPsec Option

# Non-Facilities-Based VoIP Interconnection Procedures

## Information to support Non-Facilities-Based VoIP Interconnection

Some level of information exchange must occur between two SPs who wish to establish a VoIP interconnection over the public internet. This information exchange should occur via bi-lateral communications and mutual agreement.

Each SP shall provide to its interconnection partner the signaling and media IP addresses of the SBCs that terminate the Non-Facilities-Based VoIP interconnect interface. Based on local policy, the SPs can use these addresses for access control.

Each VoIP SP shall provide to its interconnection partner information that identifies its subject traffic, such as a list of assigned OCNs or LRNs. The peering SP then updates its local routing database so that calls destined to the subject TNs obtained from the LERG are routed to the VoIP SP. The originating SP shall portability correct the called TN before routing the call to the terminating interconnection service.

### Additional Information Exchanged for TLS Option

#### Interconnect Interface SIP Signaling Address

Peering SPs shall exchange domain name information that can be resolved via DNS to identify the SIP signaling IP addresses:ports of the SBCs that terminate the Non-Facilities-Based interconnection interface. For example, the domain name could be in the form of a sub-domain such as “my-peering-interface.VoIP-SPa.com” that is resolvable via DNS SRV or A/AAAA records.

#### TLS Certificates

Each SP shall obtain a TLS end entity certificate from a bilaterally agreed Certificate Authority (CA). The TLS certificate shall contain the same domain name that the VoIP SP shared with its peer SPs as described in clause 5.1.1. The domain name shall be carried in either the Subject Alternate Name extension using the dNSName form [RFC 5280, *Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile*], or in the Common Name (CN=) attribute of the Subject field of the TLS certificate.

The SP shall be configured with the trusted root certificate of all CAs that issued TLS certificates to its peer SPs.

## Procedures to Establish/Use the Non-Facilities-Based VoIP Interconnection Interface

### Locating SIP Servers

SPs supporting the TLS option shall determine the SIP signaling IP addresses:ports of a peering SP by resolving the domain name information received from the peering SP as described in clause 5.1.1.1

SPs supporting the IPsec option shall exchange the public IP addresses of their SBCs that terminate the Non-Facilities-Based VoIP Interconnection interface. VoIP SPs may choose to leverage public DNS to maintain active IPs that have been pre-established for interoperability.

Traffic should be balanced across SBCs to care for geo-redundancy as well as capacity planning.

### Signaling Transport, Security and Authentication

ATIS-1000063 Clause 6.0, *Call Features*, [Ref 1] describes general guidelines to be followed for SIP session interactions. In addition to those guidelines, implementations conforming to this standard shall support the requirements specified in this clause.

#### TLS Option

The requirements specified in this clause apply only to SPs that choose the TLS option.

SPs shall support the requirements Transport Layer Security (TLS) over the Transmission Control Protocol (TCP) to transport all SIP signaling messages exchanged over the non-facilities-based VoIP interconnection interface. TLS version 1.2 [RFC 5246, *The Transport Layer Security (TLS) Protocol, Version 1.2*] shall be supported, and higher TLS versions may be supported (e.g., TLS version 1.3 defined in RFC 8446, *The Transport Layer Security (TLS) Protocol, Version 1.3*). The VoIP SP shall be capable of supporting both TLS client and server roles; i.e., the VoIP SP shall be capable of initiating a TLS session to a peer SP using the domain name information that it received from the peer SP as described in clause 5.1.1.1, and accepting a TLS session establishment request from a peer SP. The VoIP SP shall avoid TLS protocol version intolerance; i.e., if only TLS 1.2 is supported, TLS handshakes with peers that try to negotiate higher – yet unknown – versions (e.g., TLS 1.3) shall succeed (in this case negotiating TLS 1.2). While support for TLS at the peering SIP signaling interface is mandatory for the TLS option, support for SIPS URI scheme is not required.

SPs shall support the following TLS cipher suite when negotiating TLS 1.2:

* TLS\_ECDHE\_RSA\_WITH\_AES\_128\_GCM\_SHA256.

SPs may support the following TLS cipher suites when negotiating TLS 1.2:

* TLS\_RSA\_WITH\_AES\_128\_GCM\_SHA256
* TLS\_RSA\_WITH\_AES\_256\_GCM\_SHA384
* TLS\_ECDHE\_RSA\_WITH\_AES\_256\_GCM\_SHA384

An SP compliant with this specification shall identify the TLS\_ECDHE\_RSA\_WITH\_AES\_128\_GCM\_SHA256 cipher suite as its first choice, followed by any optional cipher suites that it supports in order of preference. During the TLS session handshake, peering SPs shall negotiate the most preferred cipher suite that is supported by both SPs, as described in RFC 5246 [Ref 7].

An SP shall not advertise support for other transports (UDP or TCP), via configuration of DNS NAPTR and/or SRV resource records.

An SP shall not initiate sessions with other transports (e.g., UDP or TCP), even if the peer indicates that these are available via configuration of DNS NAPTR and/or SRV resource records.

When exchanging SIP signaling messages with a peer, the VoIP SP should reuse an existing TLS connection if available.

During the TLS session handshake, the peering SPs shall perform mutual TLS authentication as described in the IETF RFC associated with the TLS version being used (e.g., RFC 5246 [Ref 7] for TLS 1.2, or RFC 8446 [Ref 12] for TLS 1.3). The peering SPs shall perform the certificate transparency validation procedures defined in RFC 9162, *Certificate Transparency Version 2.0*. The profile specified in this document extends the RFC 9162 [Ref 13] procedures to mandate that the TLS server shall perform certificate transparency validation of the TLS client certificate. Each SP shall extract the SIP domain name from the peer’s TLS certificate, as defined in section 7.1 of RFC 5922, *Domain Certificates in the Session Initiation Protocol (SIP)*. The SP acting as TLS client shall verify that one of the domain names obtained from the certificate matches the domain name it used to initiate the TLS session, as described in section 7.3 of RFC 5922 [Ref 11]. The SP acting as TLS server shall verify that one of the domain names obtained from the certificate matches a trusted SIP domain name obtained from one of its peer SPs (see clause 5.1.1.1), as described in section 7.4 of RFC 5922 [Ref 11].

#### IPsec Option

The requirements specified in this clause apply only to SPs that choose the IPsec option.

SPs shall support SIP signaling over UDP transport, encapsulated within tunnel-mode IPsec to provide encryption, authentication, and integrity services. SIP signaling over TCP transport encapsulated in tunnel-mode IPsec may be implemented by bilateral agreement.

Table 5‑1 lists the minimum set of IPsec and Internet Key Exchange (IKE) [RFC 2409, *The Internet Key Exchange (IKE)*] protocols, security algorithms, and configuration parameters that shall be supported for Non-Facilities-Based VoIP Interconnection. Stronger algorithms and alternative IPsec/IKE versions may be implemented per bilateral agreement.

Table 5.1 – IPSec/IKE Configuration Parameters – Recommended Minimum



NNI elements implementing IPsec shall support IPv4 with public addresses for both the inner and outer IP headers. It is recommended to use an IP address for the IPsec tunnel endpoint that is separate from the addresses used for encapsulated SIP/UDP packets as this can simplify routing and policy configuration. It is also recommended that IPsec (phase 2) security associations be identified by individual host addresses and/or subnet prefixes without including protocol and port specifications as this simplifies negotiation. The use of IPv6 incorporating tunnel-mode IPsec and the use of IKEv2 [RFC 4306, *Internet Key Exchange (IKEv2) Protocol*] may be agreed-to on a bilateral basis. The associated parameters for these protocols are outside the scope of this document.

### Media Transport, Security and Audio Profile

ATIS-1000063 Clause 5.0,*General Procedures* [Ref 1], describes guidelines to be followed with regard to media and session interactions.

#### Media Transport

SPs that select the IPsec option shall support either SRTP/SRTCP [RFC 3711, *Secure Real-time Transport Protocol*] or RTP through tunnel-mode IPsec based on bilateral agreement between SPs for media encryption, authentication, and integrity. SPs that support the TLS option shall support SRPT/SRTCP.

#### Audio Profile

The support of codecs as specified in ATIS-1000063 Clause 5.5.1 [ Ref 1] applies to SP Non-Facilities-Based VoIP interconnections.

ATIS-1000063 Clause 5.5.3 [Ref 1] applies to this profile and provides the guidelines for codec choice and transcoding responsibility. In addition, SPs may utilize modern codec technology that incorporates the use of adaptive bit-rate support and forward error correction techniques to tolerate the potential of varying congestion levels encountered on the public internet, Codec support and transcoding at the IP-NNI should be agreed to on a bi-lateral basis. Absent a specific arrangement, SPs shall at a minimum support negotiation of G.711 µ-law at the NNI and provide any needed transcoding capability within its network.

#### Media Security

SRTP may be supported by bilateral agreement, and if so, the following algorithms should be supported, with highest possible encryption supported by both sides preferred. Table 5.2 is listed bottom to top in order of increasing security.

Table 5.2 – SRTP Parameters



NNI elements supporting SRTP shall support negotiation of SRTP keys and cryptography attributes via SDP in the TLS- or IPsec-protected SIP signaling channel per RFC 4568, *SDP Security Descriptions*. By bilateral agreement NNI elements supporting SRTP may utilize DTLS-based SRTP key and cryptography attribute negotiation per RFC 5763, *Framework for Establishing a Secure Real-time Transport Protocol (SRTP) Security Context Using Datagram Transport Layer Security (DTLS)* and RFC 5764, *Datagram Transport Layer Security (DTLS) Extension to Establish Keys for the Secure Real-time Transport Protocol (SRTP)*. Such elements shall also utilize TLS or IPsec protection of the SIP signaling channel for integrity protection of the SDP-based certificate fingerprint exchange.

SPs that select the IPsec option may support RTP encryption via tunnel-mode IPsec as described for SIP signaling in Clause 5.2.2.2 based on bilateral agreement as an alternative to SRTP. This method requires pre-exchange of media IP addresses to be configured in the IPsec and routing policies in both SP networks.

1. This document is available from the Alliance for Telecommunications Industry Solutions (ATIS) at: < https://www.atis.org/ >. [↑](#footnote-ref-2)
2. Available from the Internet Engineering Task Force (IETF) at: < <https://www.ietf.org/> >. [↑](#footnote-ref-3)