**ATIS-xxxxxxx**

ATIS Technical Report on

**VoIP Interconnection over the Public Internet using TLS**

**Alliance for Telecommunications Industry Solutions**

Approved xxxx xx, 2020

**Abstract**

This document describes an "non-facilities-based Interconnection" model, where IP connectivity between peer SPs 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**

[ATIS-xxxxxxx i](#_Toc113884955)

[ATIS Technical Report on i](#_Toc113884956)

[VoIP Interconnection over the Public Internet using TLS i](#_Toc113884957)

[Alliance for Telecommunications Industry Solutions i](#_Toc113884958)

[Abstract i](#_Toc113884959)

[1 Executive Summary 1](#_Toc113884960)

[1.1 Scope 1](#_Toc113884961)

[1.2 Purpose 1](#_Toc113884962)

[2 References 1](#_Toc113884963)

[3 Definitions, Acronyms, & Abbreviations 1](#_Toc113884964)

[3.1 Definitions 1](#_Toc113884965)

[3.2 Acronyms & Abbreviations 1](#_Toc113884966)

[4 Overview 2](#_Toc113884967)

[4.1 Reference Architecture 2](#_Toc113884968)

[5 Non-facilities-based VoIP Interconnection Procedures 3](#_Toc113884969)

[5.1 Preconfigured Information to support non-facilities-based VoIP Interconnection 3](#_Toc113884970)

[5.1.1 Interconnect Interface SIP Signaling Address 3](#_Toc113884971)

[5.1.2 TLS Certificates 3](#_Toc113884972)

[5.1.3 OCNs 3](#_Toc113884974)

[5.1.4 SRTP 3](#_Toc113884975)

[5.2 Procedures to Establish/Use the non-facilities-based VoIP Interconnection Interface 3](#_Toc113884976)

[5.2.1 Locating SIP Servers 3](#_Toc113884977)

[5.2.2 Signaling Transport, Security and Authentication 3](#_Toc113884978)

[5.2.3 Media and Session Interactions 4](#_Toc113884979)

**Table of Figures**

[Figure 4.1 – Non-Facilities-Based VoIP Interconnection Reference Architecture 2](#_Toc113884980)

**Table of Tables**

**No table of figures entries found.**

# Executive Summary

## Scope

This Technical Report describes an interconnect profile for VoIP Service Providers who choose to peer over the public internet. It recommends mechanisms for establishing IP connectivity, securing the signaling and media, and providing reliable quality-of-service for real-time media traversing the unmanaged public internet. The report does not describe the SIP interworking procedures on the VoIP interconnection between peering Service Providers.

## Purpose

# 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.

ATIS-1000074, *Signature-based Handling of Asserted Information using Tokens (SHAKEN).*

# 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

**<term>:** <meaning>.

## Acronyms & Abbreviations

|  |  |
| --- | --- |
| ATIS | Alliance for Telecommunications Industry Solutions |

# Overview

Peering VoIP Service Providers traditionally interconnect through a carrier hotel, where the managed IP networks of the two peering partners 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 facility connecting the managed networks of the two peering partners.

This document describes an alternative "non-facilities-based VoIP Interconnection" model, where IP connectivity between peer 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 peering partners can identify each other. Second, call signaling and media must be protected from eavesdropping or manipulation via man-in-the-middle attacks while traversing the open internet. Finally, media encode/decode across the non-facilities-based VoIP interconnection interface may utilize modern codec technology that incorporate the ability to survive packet-loss and packet congestion with 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.

## Reference Architecture

Figure 4.1 shows the reference architecture for the non-facilities-based VoIP Interconnection model. 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

# Non-facilities-based VoIP Interconnection Procedures

This section describes the procedures that shall be supported when SIP signaling on the non-facilities-based VoIP interconnection is protected using TLS.

## Preconfigured Information to support non-facilities-based VoIP Interconnection

### Interconnect Interface SIP Signaling Address

Peering VoIP 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. A VoIP SP shall consider the domain name obtained from a peer SP as the trusted identity of that peer SP.

As a default or interim option, service provides through a bilateral agreement can exchange the specific IP addresses of the VoIP SP’s non-facilities-based VoIP interconnection interface

### TLS Certificates

Each VoIP SP shall obtain a TLS end entity certificate from an authorized 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), or in the Common Name (CN=) attribute of the Subject field of the TLS certificate.

Before issuing the TLS certificate to the VoIP SP, the CA shall verify that the VoIP SP has authority over the domain name identified in either the Subject Alternate Name extension or the Common Name attribute of the Subject field of the certificate.

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

Editor’s note: Companies need to review Clause 5.1.2 and explicitly approve this proposed text.

### Signaling Security

The VoIP SP shall be configured to always use TLS to initiate a session to a peer SP, and to require use of TLS when accepting TLS sessions initiated to it by a peer.

### OCNs

The VoIP SP shall provide its list of assigned OCNs to its peering SP. The peering SP then updates its local routing database so that calls destined to the set of OCNs and associated LRNs obtained from the LERG are routed to the VoIP SP. The peering SP must portability correct the called TN during call origination processing before routing the call to the terminating interconnection service.

Editor’s note: Time needed for further examination and review by participant companies.

### Media Security

The VoIP SP shall be configured to always negotiate SRTP for the media session on the non-facilities-based interconnection interface.

## Procedures to Establish/Use the non-facilities-based VoIP Interconnection Interface

### Locating SIP Servers

The VoIP SP 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.

### Signaling Transport, Security and Authentication

#### Transport

Transport Layer Security (TLS) over the Transmission Control Protocol (TCP) shall be used to transport all SIP signaling messages exchanged over the non-facilities-based VoIP interconnection interface.

#### Security

A VoIP SP shall use Transport Layer Security (TLS) to provide privacy and integrity protection of SIP messages exchanged over the non-facilities-based VoIP interconnection interface. TLS version 1.2 (RFC 5246) shall be supported, and higher TLS versions may be supported (e.g., TLS version 1.3 defined in RFC 8446). 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 trusted domain name information that it received from the peer SP as described in clause 5.1.1, 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, support for SIPS URI scheme is not required.

The VoIP SP shall support the following TLS cipher suite:

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

The VoIP SP may support the following TLS cipher suites for backwards compatibility:

* TLS\_RSA\_WITH\_AES\_128\_GCM\_SHA256
* TLS\_RSA\_WITH\_AES\_128\_CBC\_SHA
* TLS\_RSA\_WITH\_AES\_256\_GCM\_SHA384

A VoIP 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 VoIP SPs shall negotiate the most preferred cipher suite that is supported by both VoIP SPs, as described in RFC 5246.

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

The VoIP 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.

Editor’s note: Review the set of cipher suites that need to be supported.

#### Authentication

During the TLS session handshake, each VoIP SP shall send its TLS certificate to the peer VoIP SP. Each VoIP SP shall validate the certificate received from its peer as described in [RFC 5280], including the path validation procedure to verify that the certificate chains to a trusted root certificate. If the certificates are valid, the performEach VoIP SP shall extract the SIP domain name from the peer’s TLS certificate, as defined in section 7.1 of RFC 5922. The VoIP SP acting as TLS client shall verify that the SIP domain name obtained from the certificate matches the trusted domain name used to initiate the TLS session with the peer SP, as described in section 7.3 of RFC 5922. The VoIP SP acting as TLS server shall verify that the SIP domain name obtained from the certificate matches a trusted SIP domain name obtained from one of its peer SPs (see clause 5.1.1), as described in section 7.4 of RFC 5922.

Editor’s note: Consider addition of certificate transparency, and also review these authentication procedures.

### Media and Session Interactions

This section describes the procedures related to support of media on the non-facilities-based VoIP interconnection interface.

#### Media Transport

A Media Endpoint shall send and receive voice samples using the real-time transport protocol (RTP) as described in [RFC 3550] and shall support SRTP [RFC 3711] using SDP security descriptions [RFC 4568] for the key exchange, as specified in clause 5.2.3.4.

RTP itself comprises two parts: the RTP data transfer protocol, and the RTP control protocol (RTCP). RTCP is a fundamental and integral part of RTP, and shall be supported.

Any Media Endpoint that originates and/or terminates SRTP traffic over UDP shall use the same UDP port for sending and receiving session media (i.e. symmetric RTP).

Any Media Endpoint that originates and/or terminates RTP traffic shall be capable of processing RTP packets with a different packetization rate than the rate used for sending.

#### Audio Profile

A VoIP SP shall support G.711 and optional support a variable bit rate codec (e.g., AMR, OPUS), based on bilateral agreement.

The variable bit rate audio codec Opus as specified in [RFC6716], with the payload format specified in [RFC7587]. Since Opus provides its own Comfort Noise (CN) mechanism, the use of [RFC3389] CN with Opus is not recommended.

Editor’s note: Align the audio codec requirements here with the equivalent IPsec document (IPNNI-2022-00007R004).

#### Media Security

Secure RTP [RFC 3711] is an RTP profile which provides confidentiality, authentication and replay protection for both RTP and RTCP.

A VoIP SP shall secure the media using SRTP [RFC 3711] and shall use SDP Security Descriptions [RFC 4568] for the necessary key exchange.

SDP Security Descriptions allows for negotiation of various crypto-suites and SRTP parameters in the a=crypto: attribute as defined in [RFC 4568]. As a least common denominator that allows for successful interoperability, the Offerer shall include at least one a=crypto: attribute that uses the following values:

* crypto-suite: AES\_CM\_128\_HMAC\_SHA1\_80
* key||salt: dynamically and randomly calculated for each new offer, unique to the entire SDP message and unique per direction. This means that in case of a new SDP offer/answer exchange, the Offerer should include a new master key and master salt that is unique and generated independently from the key and salt provided during the previous SDP offer/answer exchange.

The Offerer shall not include the following elements in the above a=crypto: attribute:

* lifetime:
* MKI:length
* Any session parameters, e.g., KDR, UNENCRYPTED\_SRTP, UNENCRYPTED\_SRTCP, UNAUTHENTICATED\_SRTP, FEC\_ORDER, FEC\_KEY and WSH.

Media Endpoints should use the confidentiality mechanisms in SRTP and SRTCP to ensure media confidentiality as described in [RFC 3711].

Media Endpoints should use the integrity mechanisms in SRTP and SRTCP to ensure media integrity as described in [RFC 3711].

Media Endpoints should use the replay protection mechanism for protecting both SRTP and SRTCP as described in [RFC 3711].

Subject to the above recommendations, the SDP offer may include further a=crypto: attributes allowing for other crypto-suites or carrying any valid combination of optional elements that were disallowed for the mandatory a=crypto: attribute from above. The recommendation for using new key material in subsequent SDP offer/answer exchanges remains valid also when one of these further a=crypto: attributes is negotiated. Usage of new key material is motivated due to SIP forking and due to Transfer, in which case the offerer’s key is distributed to several peers.

Editor’s note: Review the set of cipher suites that need to be supported.

#### Transport of DTMF Tones

A VoIP SP shall advertise support for telephone-events [RFC 4733] in its SDP. Media Endpoint shall support [RFC 4733] procedures. Media Endpoints shall use the [RFC 4733] procedures to transmit DTMF tones using the RTP telephone-event payload format, provided that the other side has advertised support for receiving [RFC 4733] in the offer/answer exchange.

For any local Media Endpoint that supports receiving telephone-event packets, the VoIP SP shall include the supported events in an "a=fmtp:" line as is described as mandatory in [RFC 4733].

To provide backward compatibility with [RFC 2833] implementations, a Media Endpoint shall be prepared to receive telephone-event packets for all events in the range 0-15. A VoIP SP shall be prepared to accept SDP with a payload type mapped to telephone-event, even if it does not have an associated "a=fmtp" line.