**ATIS-xxxxxxx**

ATIS Technical Report on

**VoIP Interconnection over the Public Internet**

**using UDP and IPsec**

**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 using UDP and IPsec.

**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](#_Toc55840110)

[ATIS Technical Report on i](#_Toc55840111)

[VoIP Interconnection over the Public Internet i](#_Toc55840112)

[Alliance for Telecommunications Industry Solutions i](#_Toc55840113)

[Abstract i](#_Toc55840114)

[1 Executive Summary 1](#_Toc55840115)

[1.1 Scope 1](#_Toc55840116)

[1.2 Purpose 1](#_Toc55840117)

[2 References 1](#_Toc55840118)

[3 Definitions, Acronyms, & Abbreviations 1](#_Toc55840119)

[3.1 Definitions 1](#_Toc55840120)

[3.2 Acronyms & Abbreviations 1](#_Toc55840121)

[4 Overview 2](#_Toc55840122)

[4.1 Reference Architecture 2](#_Toc55840123)

[5 NON-FACILITIES-BASED VoIP Interconnection Procedures 3](#_Toc55840124)

[5.1 Preconfigured Information to support OTT VoIP Interconnection 3](#_Toc55840125)

[5.2 Procedures to Establish/Use the NON-FACILITIES-BASED VoIP Interconnection Interface 3](#_Toc55840126)

[5.2.1 Location Discovery 4](#_Toc55840127)

[5.2.2 Signaling Transport, Security and Authentication 4](#_Toc55840128)

[5.2.3 Media and Session Interactions 4](#_Toc55840129)

**Table of Figures**

[Figure 4.1 – NON-FACILITIES-BASED VoIP Interconnection Reference Architecture 2](#_Toc55840130)

[Figure 4.2 – NON-FACILITIES-BASED VoIP Interconnection Using VPN Gateways 3](#_Toc55840130)

**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 interconnect over the public internet. It recommends mechanisms for establishing IP connectivity using UDP transport, securing the signaling via IPsec ([RFC 4301] and related specifications), securing the media using Secure Real-time Transport Protocol (SRTP) [RFC 3711] or RTP encapsulated in an IPsec tunnel, 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, encryption/authentication and telephone number ranges exchanged is out of scope of this document.

## Purpose

This report is to coexist with ATIS-1000063 as well as expand on options available for carriers to leverage the public internet for VoIP Interconnection described in IPNNI-2021-00059r000. 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.

ATIS-1000063, *Joint ATIS/SIP Forum Technical Report – IP NNI Profile*

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

RFC 3711 Secure Real-time Transport Protocol

RFC 4733 RTP Payload for DTMF Digits, Telephony Tones, and Telephony Signals

RFC 4303 IP Encapsulating Security Payload (ESP)

RFC 4301 Security Architecture for IP

RFC 2409 The Internet Key Exchange (IKE)

RFC 4306 Internet Key Exchange (IKEv2) Protocol

RFC 4568 SDP Security Descriptions

# 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

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 shall be encrypted and optionally media may be encrypted to protect 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

Figure 4.1 shows the reference architecture for the non-facilities-based VoIP Interconnection model. 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 4.1 – Non Facilities-Based VoIP Interconnection Reference Architecture

For some SPs, implementing IPsec tunnels for SIP signaling and/or RTP in a separate VPN gateway may simplify deployment and security policy. Figure 4.2 shows a reference architecture for this implementation.

****

Figure 4.2 – Non Facilities-Based VoIP Interconnection using VPN Gateways

# 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. For example, each SP must provide to its interconnection partner the IP addresses of the SBCs that terminate the Non-Facilities-Based VoIP interconnect interface to care for geo-redundancy as well as capacity distribution.

Furthermore, the traffic to be exchanged over the interconnection must be agreed upon. Identification of subject traffic should use existing numbering plan and portability correction databases. This information exchange should occur via bi-lateral communications and mutual agreement.

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

### Locating SIP Servers

SPs shall exchange the public IP addresses of their SBCs that terminate the Non-Facilities-Based VoIP Interconnection interface. This allows for geo-redundancy as well as capacity planning. VoIP SPs may choose to leverage public DNS to maintain active IPs that have been pre-established for interoperability.

### Signaling Transport, Security and Authentication

ATIS-1000063 Clause 6.0 Call Features describes general guidelines to be followed for SIP session interactions. In addition to those guidelines, implementations conforming to this standard 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.

#### Minimum IPsec Support

The following table lists the minimum set of IPsec and Internet Key Exchange (IKE) [RFC 2409] 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.



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] 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**.**0General Procedures describes guidelines to be followed with regard to media and session interactions.

#### Media Transport

Under this profile, either SRTP or RTP through tunnel-mode IPsec may be used by bilateral agreement between SPs for media encryption, authentication, and integrity.

#### Audio Profile

ATIS-1000063 Clause 5.5.1 applies to SP Non-Facilities-Based VoIP interconnections. Codecs that are widely used in IP-based SP voice networks are listed in the table below. Codecs in the Group 1 column shall be supported for both transmission and reception across the NNI. Codecs in the Group 2 columns should be supported for both transmission and reception across the NNI, however the set of non-mandatory codecs that will be offered and accepted on a specific NNI are subject to bilateral agreement. To tolerate the potential of varying congestion levels encountered on the public internet, SPs may utilize modern codec technology that incorporates the use of adaptive bit-rate support and forward error correction techniques.

|  |  |
| --- | --- |
| **Group 1: Mandatory Codecs** | **Group 2: Optional** |
| G.711 μ-law 64 kbit/s | G.711 a-law 64 kbit/s |
|  | G.726, G.729, G.729a, G.729b, G.729ab 8kbit/s |
|  | Adaptive MultiRate (AMR) |
|  | G.722 (Wideband) |
|  | G.722.2 (AMR-Wideband) |

ATIS-1000063 Clause 5.5.3 applies to this profile and provides the guidelines for codec choice and transcoding responsibility. 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.

Editor's note: Table is from ATIS 1000063 Clause 5.5.1. Transcoding rules/recommendations are found in ATIS1000063 Clause 5.5.3.

#### 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.



Editor’s note [figure above]: Check whether GCM is sufficiently widely used.

NNI elements supporting SRTP shall support negotiation of SRTP keys and cryptography attributes via SDP in the IPsec-protected SIP signaling channel per [RFC 4568]. RTP encryption via tunnel-mode IPsec as described for SIP signaling in Clause 5.2.2 may be supported by 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.