ATIS-1000100

VoIP Interconnection over the Public Internet

TECHNICAL REPORT

As a leading technology and solutions development organization, the Alliance for Telecommunications Industry Solutions (ATIS) brings together the top global ICT companies to advance the industry's most pressing business priorities. ATIS' nearly 200 member companies are currently working to address the All-IP transition, 5G, network functions virtualization, big data analytics, cloud services, device solutions, emergency services, M2M, cyber security, network evolution, quality of service, billing support, operations, and much more. These priorities follow a fast-track development lifecycle — from design and innovation through standards, specifications, requirements, business use cases, software toolkits, open source solutions, and interoperability testing.

ATIS is accredited by the American National Standards Institute (ANSI). The organization is the North American Organizational Partner for the 3rd Generation Partnership Project (3GPP), a founding Partner of the oneM2M global initiative, a member of the International Telecommunication Union (ITU), as well as a member of the Inter-American Telecommunication Commission (CITEL). For more information, visit www.atis.org.

ATIS-1000100, *VoIP Interconnection over the Public Internet*

Published by

Alliance for Telecommunications Industry Solutions
1200 G Street, NW, Suite 500
Washington, DC 20005

ATIS-1000100

ATIS Technical Report on

VoIP Interconnection over the Public Internet

Alliance for Telecommunications Industry Solutions

Approved December 12, 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) is a global standards development and technical planning organization that develops and promotes worldwide technical and operations standards for information, entertainment, and communications technologies. ATIS' diverse membership includes key stakeholders from the Information and Communications Technologies (ICT) industry – wireless and wireline service providers, equipment manufacturers, broadband providers, software developers, VoIP providers, consumer electronics companies, public safety agencies, and internet service providers. ATIS is also a founding partner and the North American Organizational Partner of the Third Generation Partnership Project (3GPP), the global collaborative effort that has developed the Long-Term Evolution (LTE) and LTE-Advanced wireless specifications.

ATIS' Packet Technologies and Systems Committee (PTSC) develops standards related to services, architectures, signaling, network interfaces, next generation carrier interconnect, cybersecurity, lawful intercept, and government emergency telecommunications service within next generation networks. As networks transition to all-IP, PTSC will evaluate the impact of this transition and develop solutions and recommendations where necessary to facilitate and reflect this evolution.

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

Table of Figures

Table of Tables

ATIS Standard on –

VoIP Interconnection over the Public Internet

1 Executive Summary

1.1 Scope

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

The report does not describe the Session Initiation Protocol (SIP) call control signaling interworking procedures between interconnected VoIP SPs. The scope is limited to IP transport aspects only. Furthermore, automation regarding network discovery, including points of interconnection and telephone number ranges exchanged, is out of scope of this document.

1.2 Purpose

This report is intended to coexist with ATIS-1000063, *Joint ATIS/SIP Forum Technical Report – IP NNI Profile*, and expand on options available for SPs to leverage the public Internet for VoIP interconnection. The expansion of options available with the "non-facilities-based VoIP Interconnection" model described in this document that can be agreed to on a bilateral basis facilitates adoption of VoIP interconnect as well as support for STIR/SHAKEN protocols to combat robocalling.

2 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]

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

[Ref 3] RFC 3711 *Secure Real-time Transport Protocol*.[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]

[1] This document is available from the Alliance for Telecommunications Industry Solutions (ATIS) at: < https://www.atis.org/ >.

[2] Available from the Internet Engineering Task Force (IETF) at: < https://www.ietf.org/ >.

[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]

3 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 >.

3.1 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.

Secure Telephone Identity (STI) Certificate: A public key certificate used by a service provider to sign and verify the PASSporT.

3.2 Acronyms & Abbreviations

ATIS	Alliance for Telecommunications Industry Solutions
CA	Certification Authority
CRL	Certificate Revocation List
DNS	Domain Name System
DTLS	Datagram Transport Layer Security
FQDN	Fully-Qualified Domain Name
IKE	Internet Key Exchange
IP	Internet Protocol
IPsec	IP Security
LERG	Local Exchange Routing Guide
LRN	Location Routing Number
NAPTR	Naming Authority Pointer
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
SIPS	SIP Secure
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

4 Overview

VoIP 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 need to be taken so that calls are delivered securely and with adequate quality. First, strong authentication mechanisms need to be in place to ensure that interconnected SPs can identify each other. Second, call signaling and media need to 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 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.

4.1 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.

4.1.1 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 interconnection point to support SIP signaling and media on the non-facilities-based VoIP Interconnection interface. SIP signaling across the interconnection interface is protected by 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.

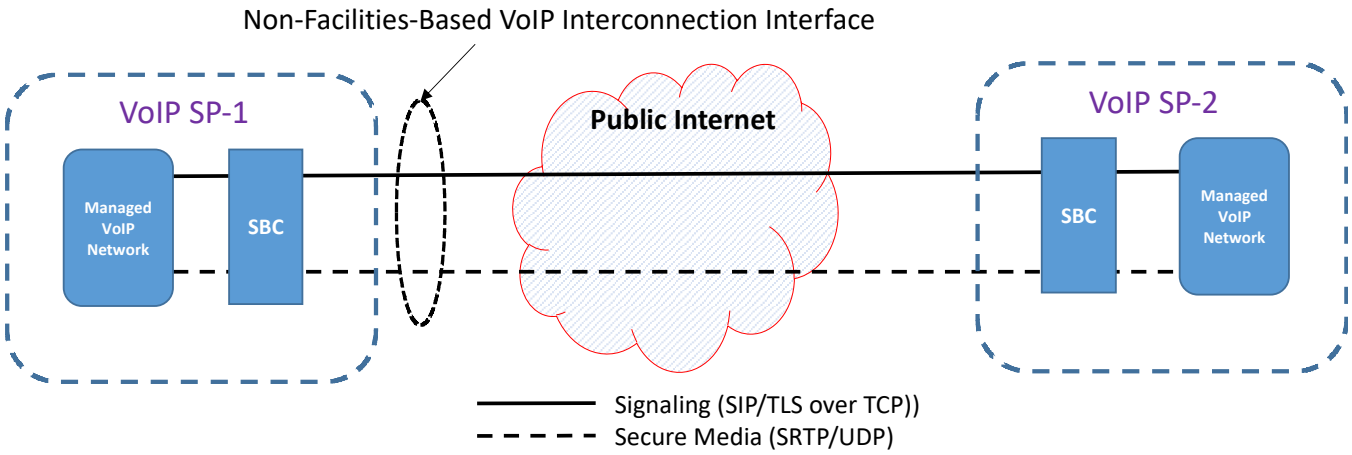

Figure 4.1 – Non-Facilities-Based VoIP Interconnection Reference Architecture for TLS Option

4.1.2 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 an 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 is used for signaling or by using SRTP if outside the IPsec tunnel. How media is handled is subject to bilateral communications and mutual agreement between the two SPs.

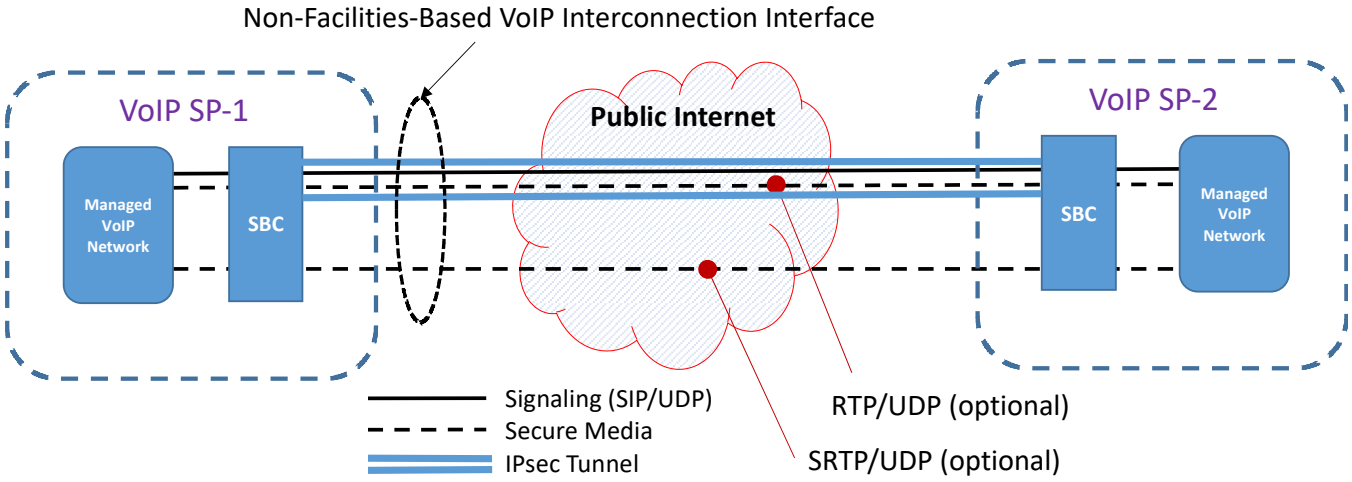

Figure 4.2 – Non-Facilities-Based VoIP Interconnection Reference Architecture for IPsec Option

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.

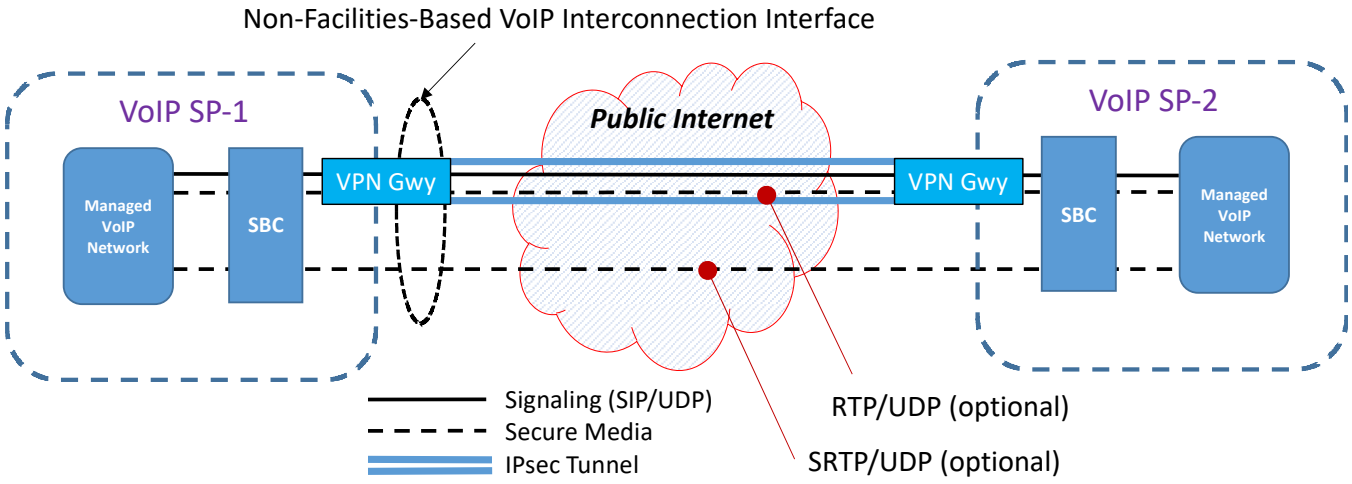

Figure 4.3 – Non-Facilities-Based VoIP Interconnection using VPN Gateways for IPsec Option

5 Non-Facilities-Based VoIP Interconnection Procedures

5.1 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 bilateral 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 interconnection 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 Operating Company Numbers (OCNs) or Location Routing Numbers (LRNs). The peering SP then updates its local routing database so that calls destined to the subject Telephone Numbers (TNs) obtained from industry routing data, such as the Local Exchange Routing Guide (LERG™ Routing Guide), are routed to the VoIP SP. The originating SP shall portability-correct the called TN before routing the call to the terminating interconnection service.

5.1.1 Additional Information Exchanged for TLS Option

5.1.1.1 Interconnect Interface SIP Signaling Address

Peering SPs shall exchange domain name information that can be resolved via Domain Name System (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 fully-qualified domain name (FQDN) such as “my-peering-interface.VoIP-SPa.com” that is resolvable via DNS SeRVice record (SRV) or A/AAAA records.

5.1.1.2 TLS Certificates

Each SP shall obtain a TLS end-entity certificate from a bilaterally agreed Certification Authority (CA). The TLS certificate shall contain the a domain name pattern (individual FQDN, multiple FQDNs, or name with a wildcard value (‘*’) in the left-most tag) covering the domain name that the VoIP SP shared with its peer SPs as described in clause 5.1.1.1.1. The domain name pattern 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.

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

5.2.1 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 IP addresses that have been pre-established for interoperability.

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

5.2.2 Signaling Transport, Security and Authentication

Clause 6.0, *Call Features*, of ATIS-1000063 [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.

5.2.2.1 TLS Option

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

SPs shall support the requirements for TLS over the Transmission Control Protocol (TCP) to transport all SIP signaling messages exchanged over the non-facilities-based VoIP interconnection interface as detailed in the following specifications. 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 the SIP Secure (SIPS) Uniform Resource Identifier (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 decreasing 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 Naming Authority Pointer (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 clause 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 clause 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 clause 7.4 of RFC 5922 [Ref 11].

5.2.2.2 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 to the SIP signaling. SIP signaling over TCP transport encapsulated in tunnel-mode IPsec may be implemented by bilateral agreement.

Error! Reference source not found. 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

Phase 1 (Main Mode) - IKE Policy	
IKE Version	Version 1
Message Encryption	AES-128
Message Integrity - Hash Algorithm	SHA2-256
Peer Authentication Method	Preshared Key - min length 64 characters, high-entropy alphanumeric with special characters
Diffie-Hellman Group ID Number	Group 14 (2048-bit)
IKE Lifetime	min 8 Hours; max 24 hours
Phase 2 (Quick Mode) - IPSec Parameters	
Encryption Algorithm	AES-128
Authentication Algorithm	SHA2-256
Perfect Forwarding Secrecy	Diffie-Hellman Group 14 (2048-bit)
Protocol Mode	Encapsulating Security Protocol (ESP) Tunnel Mode
Security Association (SA) Lifetime	1 Hour (3600 seconds)

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.

5.2.3 Media Transport, Security and Audio Profile

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

5.2.3.1 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.

5.2.3.2 Audio Profile

The support of codecs as specified in clause 5.5.1 of ATIS-1000063 [Ref 1] applies to SP non-facilities-based VoIP interconnections.

Clause 5.5.3 of ATIS-1000063 [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 varying congestion levels encountered on the public Internet. Codec support and transcoding at the IP-NNI should be agreed to on a bilateral basis. Absent a specific arrangement, SPs shall at a minimum support negotiation of G.711 μ-law at the NNI and shall provide any needed transcoding capability within their network.

5.2.3.3 Media Security

SRTP may be supported by bilateral agreement, and if so, the following algorithms should be supported, with the strongest possible encryption supported by both sides preferred. Table 5.2 lists algorithms from top to bottom in order of decreasing security.

Table 5.2 – SRTP Parameters

Crypto Suite	Master Key Length (bits)	Salt Value (bits)	Cipher	Key Derivation Function	Encryption key (bits)	Message Authentication Code	Authentication tag length (bits)	Authentication key length (bits)
AEAD-AES-256-GCM	256	96	AES-CM	AES_256_CM_PRF [RFC6188]	256	Galois Message Authentication Code (GMAC)	128	N/A
AEAD-AES-128-GCM	128	96	AES-CM	AES_128_CM PRF [RFC3711]	128	Galois Message Authentication Code (GMAC)	128	N/A
AES-CM-256-HMAC-SHA1-80	256	112	AES-CM	AES_256_CM_PRF	256	HMAC_SHA1	80	160
AES-CM-256-HMAC-SHA1-32	256	112	AES-CM	AES_256_CM_PRF	256	HMAC_SHA1	32	160
AES-CM-192-HMAC-SHA1-80	192	112	AES-CM	AES_192_CM_PRF	192	HMAC_SHA1	80	160
AES-CM-192-HMAC-SHA1-32	192	112	AES-CM	AES_192_CM_PRF	192	HMAC_SHA1	32	160
AES-CM-128-HMAC-SHA1-80	128	112	AES-CM	AES_128_CM_PRF	128	HMAC-SHA1	80	160
AES-CM-128-HMAC- SHA1-32	128	112	AES-CM	AES_128_CM_PRF	128	HMAC-SHA1	32	160

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 Data Transport Layer Security (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.