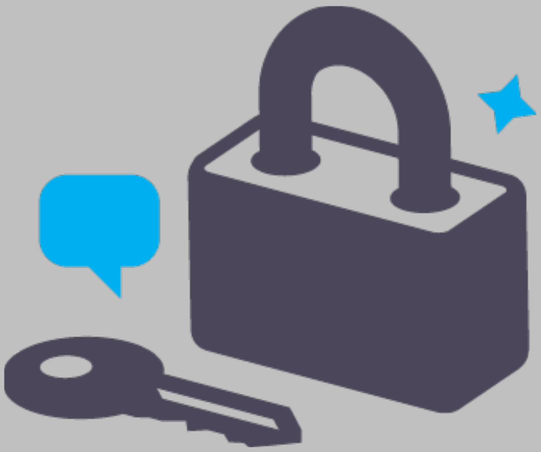
TLS and SRTP for Skype Connect™

Technical Datasheet



Introducing TLS and SRTP

Protocols help protect enterprise communications

Skype Connect now provides Transport Layer Security (TLS) and Secure RTP (SRTP) protocols for encrypting both SIP messages and RTP (media streams) between your IP-PBX, Media Gateway, or UC (Unified Communications) platform and Skype Connect. The addition of these two native protocols provides increased protection from “man in the middle” attacks that can include eavesdropping, wiretapping, or threats to the security and privacy of Skype Connect.

TLS provides an encrypted connection between your UC platform and Skype Connect while SRTP encrypts voice media.

Once configured for use by your certified gateway and SIP-enabled PBX, TLS and SRTP are automatically enabled for Skype Connect customers; no additional configuration or provisioning is required.

Protocol overview

Transport Layer Security (TLS) is a cryptographic protocol that provides authentication and encryption of signalling over the Internet. TLS encrypts connections above the Transport Layer, using asymmetric cryptography for privacy and keyed message authentication codes for message reliability.

By encrypting SIP signalling (protocol exchanges), TLS ensures that parameters (numbers, Skype user names, and others) negotiated between your UC platform and Skype Connect cannot be captured. TLS also helps prevent third parties from eavesdropping or tampering with messages.

The Secure Real-time Transport Protocol (SRTP) defines a profile of RTP (Real-time Transport Protocol) providing encryption, message authentication and integrity, and replay protection to RTP data for both unicast and multicast applications. Developed by the IETF (Internet Engineering Task Force) as a standard for transporting encrypted media, SRTP only encrypts the payload, making it a highly efficient protocol for transporting media packets. An SRTP-encrypted packet is distinguished from an RTP packet by the addition of a 4-byte authentication tag.

SRTP secures your conversations by encrypting voice traffic. Even if unauthorized users were able to capture your audio packets, they would be unable to recognize it as speech. SRTP uses the keys exchanged within the SIP SDP (SDES) during the SIP signalling dialog.

The Skype implementation of TLS relies on an X.509 secure key exchange mechanism issued by Verisign®. A standard for public key infrastructure, X.509 defines a standard certificate format for public key certificates and certification validation.

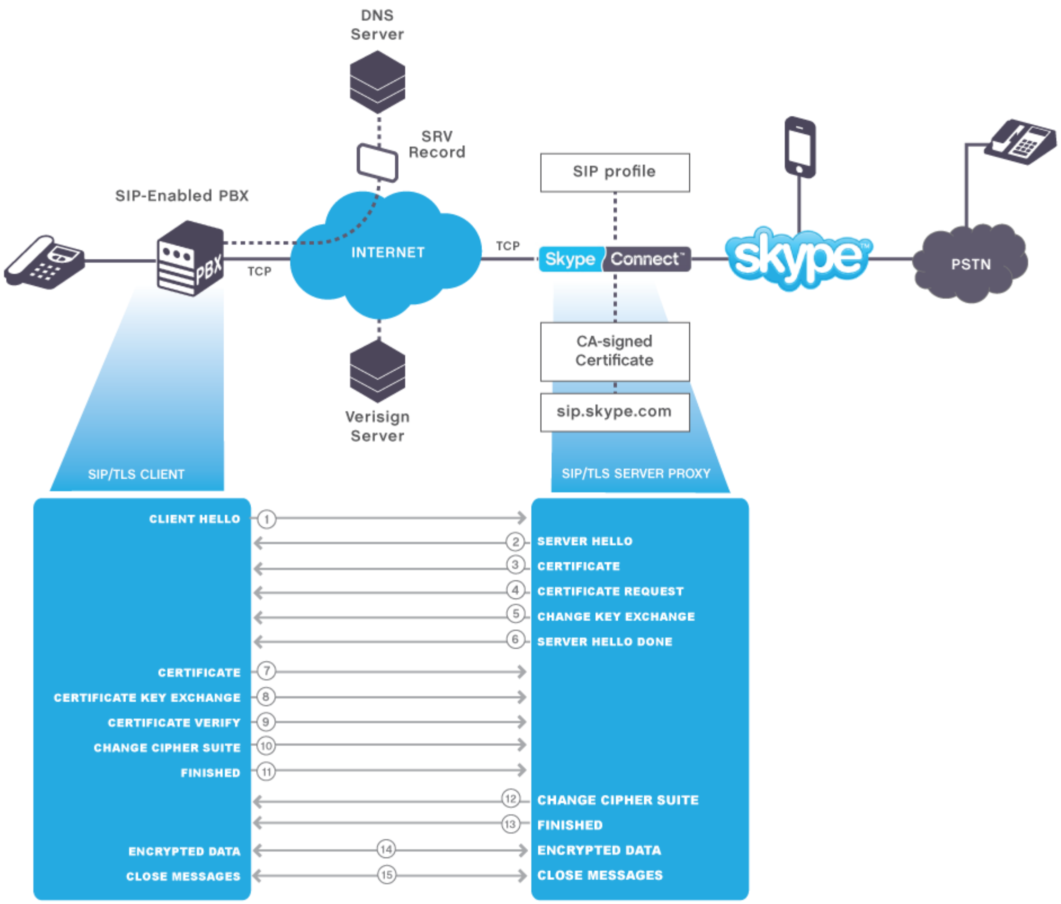
How TLS authenticates connections

The security model of TLS is based on digital certificate verification and closely resembles the HTTPS process used for secure web mail and online banking. Skype Connect TLS connections are verified by CA-signed certificates from Verisign. When your device—a SIP-enabled PBX, Gateway or SBC (Session Border Controller)—attempts to make a secure connection, it receives a CA-signed certificate that verifies it is connecting to Skype Connect.

Your device then performs a DNS SRV lookup on the domain sip.skype.com to get a gateway IP address and port assignment. After a TCP connection is set up, the TLS client negotiates a connection with Skype Connect through a standard handshaking procedure in which the client and Skype Connect agree on the parameters they will use to make the connection secure.

The TLS handshake starts with a client request for a secure connection to Skype Connect on port 5061 and presents a list of supported ciphers and hash functions. Skype Connect identifies itself by sending a CA-signed digital certificate to the client, which can contact the issuing Verisign (CA) server to confirm the validity of the certificate.

If the client accepts the certificate as valid, it generates session keys for the connection by encrypting a random number with Skype Connect's public key and sends the result to Skype Connect, which uses its public key to decrypt the result.



Skype Connect TLS Handshake

1 **Client Hello**. The client sends a Client Hello message specifying the TLS version and a list of cipher suites it supports.

2 **Skype Connect Hello**. Skype Connect responds with a Hello message specifying the TLS version and a chosen cipher suite.

3 **Certificate**. As part of the initial TLS handshake, Skype Connect presents an X.509 certificate or certificate chain to the client for verification.

4 **Certificate Request**. Skype Connect requests a certificate from the client so the connection can be mutually authenticated. (optional)

5 **Skype Connect Key Exchange**. Skype Connect sends the client a Skype Connect Key Exchange message with the Public Key information supplied in step 3.

6 **Skype Connect Hello Done**. Skype Connect sends a Hello Done message that lets the client know the initial negotiations are finished.

7 **Certificate**. If Skype Connect requested a certificate, the client sends the certificate or certificate chain.

8 **Certificate Key Exchange.** The client sends a Certificate Key Exchange message which, depending on the choice of cipher suite,,contains a PreMasterSecret, a Public Key, or is empty.

9 **Certificate Verify**. This message is sent when the client presents a certificate. Receipt of this message allows Skype Connect to complete the process of authenticating the client.

10 **Change Cipher Suite.** The client sends this message to tell Skype Connect to change to encrypted mode.

11 **Finished**. The client tells Skype Connect it is ready for secure data communication to begin.

12 **Change Cipher Spec.** Skype Connect sends a message to the client telling it to change to encrypted mode.

13 **Finished**. Skype Connect tells the client it is ready for secure data communication to begin. (This completes the TLS handshake.)

14 **Encrypted data.** The client and Skype Connect communicate using the symmetric encryption algorithm and a cryptographic hash function negotiated in Steps 4 and 5 and the secret key the client sent to Skype Connect in Step 12.

15 **Close Messages**. When the connection ends, each side sends a *close_notify* message informing the peer that the connection is closed.

How do I prepare my network to use TLS and sRTP?

Firewall

Configure your firewall to allow:

- outbound DNS SRV requests by Skype to the domain sip.skype.com
- inbound request for DNS SRV records by Skype
- outbound TCP/IP connections from your public interface to the IP addresses provided in the DNS SRV record from Skype
- inbound TCP/IP requests from Skype Connect

PBX or SIP UA

Configure your SIP-enabled voice platform to use TLS and secure RTP (optional).

Some SIP-enabled platforms require the CA-signed certificate to be pre-installed. Contact Skype Connect technical support to confirm your PBX, Gateway or SBC certificate requirements.

SIP profile

Use the Username/Password option (Registration Authentication) in Skype Manager to set up a working SIP Profile .

CA certificate

Contact Skype Connect technical support to obtain Skype's CA certificate (for certain platforms only).

Device configuration

Configure Skype devices for TLS and SRTP. Assign TLS to port 5061. SDES is used to register SRTP in the SIP session.

Configure devices to perform DNS SRV requests to sip.skype.com.

Technical specifications of TLS

Protocol	TLS V1.2 (SSL-3.2), RFC 5249-compliant
IP transport	TCP
Authentication method	Single-sided asymmetric, or public key, cryptography. Client authenticates Skype Connect.
Certificate format	X.509
Root certificate authority	Verisign

Technical specifications of SRTP

Protocol	SRTP RFC 1889, RFC 3711, RFC 3830-compliant
Key Negotiation Method	SDES (Session Description Protocol Security Descriptions for Media Streams)
Encryption Algorithm	AES (Advanced Encryption Standards)
IP transport	UDP
Authentication method	SHA-1 cryptographic hash function

Learn more about Skype Connect at skypeconnect.com

Need more information?

We have a comprehensive set of support documentation to help you get the most out of Skype Connect, available from **support.skype.com**.

It includes:

- **Skype Connect IT Requirements Guide**
- **Skype Connect Quick Start Guide**
- **Skype Connect User Guide**
- **Skype Connect Troubleshooting Guide**

Skype is not a replacement for traditional telephone services and cannot be used for emergency calling. Skype Connect is meant to complement existing traditional telephone services used with a corporate SIP-enabled PBX, not as a stand-alone solution. Skype Connect users need to ensure all calls to emergency services are terminated through traditional fixed line telephone services, connected to the local exchange, or through other emergency calling capable telephone services.