Best Practices for SIP Security

IMTC SIP Parity Group

Version 21

November 9, 2011

Table of Contents

1. Overview

This document describes best practices for implementing security in SIP-based video conferencing end devices. The document is written in the spirit of a "Best Current Practices" RFC. It does not describe any new functionality, but instead describes the best current practices for implementing security in SIP-based video conferencing end devices based on current IETF RFCs and drafts. A video conferencing end device is defined as a video endpoint incorporating a SIP User Agent (UA).

Furthermore, this document is focused on protecting SIP signaling and session media, and not on securing the video conferencing end devices themselves against network-based or other types of attacks.

2. Security Profile

This document defines a "Best Practices" Profile for security. The profile is focused on providing security for videoconferencing sessions and interoperability with current implementations of videoconferencing devices.

Function	"Best Practices" Profile
UAC Authentication to Registrar/Proxy	SIP Digest authentication
Identity Protection	Hop-by-hop asserted identity
Certificates	Use CA certificates to validate identity of peer in TLS connections
Protection of Signaling	SIP-over-TLS SIPS URI (optional)
Protection of Media	SRTP encryption, integrity protection and replay protection
Key Exchange for protection of media	Security Descriptions
SRTP negotiation	Mandatory and best effort options in SDP

Table 2.1 Functions and mechanisms used in the Security "Best Practices" Profile

The remainder of this document describes the approach for each functional aspect of this profile and specifies requirements on video conferencing end devices.

3. Authentication & Identity Protection

In video conferencing, identity verification through authentication lays the foundation for other security mechanisms used to protect confidentiality and availability. Authentication involves proving the identity of the person, or people using an end device. Endpoints must authenticate to their call servers to prove they can use the system. This authentication usually involves a well-known challenge/response mechanism. Video conferencing end devices MUST implement the Digest authentication mechanism for SIP (RFC 3261 Section 22.4) for authentication to a call server.

When establishing a TLS connection for protecting signaling (see Section 4) a video conferencing end device, acting as TLS client, MUST validate the certificate received from the registrar/proxy to which it is connecting (i.e., the TLS server). In particular, the video conferencing end device MUST check that the certificate identifies the target entity that it is trying to connect to, i.e., the registrar/proxy. The video conferencing end device MUST first check the contents of the subjectAltName field (Subject Alternative Name, RFC 5280, Section 4.2.1.6). However, for compatibility with older forms of certificate, if the subjectAltName field is not present the video conferencing end device MUST instead check the contents of the subject field (Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile [RFC 5280], section 4.1.2.6), specifically the commonName (CN) attribute. When checking the contents of these fields, the video conferencing end device MUST be able to accept either a SIP URI or a DNS name that matches the target entity that the device is trying to connect to (i.e., the target of the SIP request to be submitted over the established TLS connection) or a host name obtained by applying RFC 3263 procedures to that target.

To achieve validation of a received certificate, a video conferencing end device MUST be capable of installing and using certification authority (CA) certificates, including CA certificates from authorities (such as Verisign) and customer CA certificates. A video conferencing end device MUST support revocation and updating of certificates. That is, it MUST periodically use a mechanism such as OCSP to determine whether the CA certificates it has installed have been revoked (X.509 Internet Public Key Infrastructure Online Certificate Status Protocol – OCSP [RFC 2560]). In addition, video conference endpoints MUST check whether any server certificate they receive has been revoked, also using a mechanism such as OCSP. A video conferencing device MUST be capable of validating received certificates using certificate chains. It is recommended that video conferencing endpoints not accept self-signed certificates from servers unless they have an out-of-band mechanism for validating the server certificate.

Endpoints need to be able to trust the claimed identity of those with whom they are communicating, especially across domains. The “SIP Identity” mechanism defined in Enhancements for Authenticated Identity Management in SIP [RFC 4474] provides a means to securely identify originators of SIP messages, even when those messages have traversed different domains. Identity trust is accomplished in a transitive manner. The basic idea is that if the end domains trust each other, and end devices are authenticated to their respective end domains, then the end devices can trust each other. The “SIP Identity” mechanism provides the highest level of authentication and integrity protection mechanisms for sensitive information such as end-to-end key exchange because messages are not susceptible to modification by malicious intermediaries. The absence of any significant deployment of this mechanism, coupled with known difficulties with signatures being invalidated by certain types of SIP intermediary, means that this mechanism cannot be specified as part of the "Best Practices" Profile. Instead, reliance has to be placed on hop-by-hop assertion of identity, as provided by Private Extensions to SIP for Asserted Identity within Trusted Networks [RFC 3325] and Updates to Asserted Identity in SIP [RFC 5876]. Specifically, video conferencing end devices:

- MUST support the SIP "Asserted Identity" mechanism as specified in RFC 3325 and updated by RFC 5876;

- MAY use either the P-Asserted-Identity header field in every request except ACK or CANCEL (RFC 5876 Section 3.3) when sending the request to a proxy or registrar in its own trust domain, or send the P-Preferred-Identity header in every request to a proxy or registrar in its own trust domain if it wishes that the proxy insert the P-Asserted-Identity header on the endpoint's behalf;
- MAY use the privacy mechanisms for P-Asserted-Identity (RFC 3325 Section 7 and RFC 5876 Section 4.5); and
- MUST adhere to rules in RFC 5876 (Section 4.5) when rendering any P-Asserted-Identity information it receives in a SIP request.

4. Protecting Signaling

In SIP sessions, call signaling should be kept confidential to protect user identities, as well as to protect the network topology and call routing information which could be used to gain unauthorized access to services. When Security Descriptions key exchange is used, SIP signaling MUST be kept confidential to protect the key information.

To protect SIP signaling, video conferencing end devices MUST support SIP over TLS in accordance with SIP: Session Initiation Protocol [RFC 3261] as updated by The Use of the SIPS URI Scheme in SIP [RFC 5630] and MAY support the SIPS URI scheme in accordance with RFC 3261 as updated by RFC 5630.

SIP-over-TLS: In The Use of the SIPS URI Scheme in SIP [RFC 5630], two models for SIP-over-TLS are described. In the "Server Supplied Certificate" model, only the TLS server provides a certificate during the TLS handshake. This is applicable only between a UA and a proxy, where the UA is the TLS client and the proxy is the TLS server, and hence the UA uses a certificate to authenticate the proxy but the proxy does not use a certificate to authenticate the UA. If the proxy needs to authenticate the UA, SIP Digest authentication is used. This directionality implies that the TLS connection always needs to be setup by the UA (e.g., during the registration phase). Since SIP allows for requests in both directions (e.g., an incoming call), the TLS connection needs to be kept alive so that it is available for both incoming and outgoing requests.

In the "Mutual Authentication" model, both the TLS client and the TLS server provide a certificate in the TLS handshake phase. This has proven to be impractical in many environments, in particular for SIP UAs, because of the difficulties of setting up a certificate infrastructure for a wide population of users or devices. For these reasons, video conferencing end devices need only to support the "Server Supplied Certificate" model.

A video conferencing end device MUST support TLS to protect signaling in SIP using the "Server Supplied Certificates" model. The video conferencing end device MUST authenticate the TLS server by validating a received certificate as specified in Section 3. After establishing a TLS connection, the video conferencing end device MUST take steps to keep it alive, as specified in Managing Client Initiated Connections in SIP [RFC 5626].

Use of TLS between a video conferencing end device and the first proxy does not necessarily mean that TLS will be used on the entire signaling path to the remote endpoint. If a video conferencing end device wants to use "best-effort TLS" when sending a SIP request, in an attempt to achieve SIP on all hops, it

SHOULD use a SIP URI, and send the request over a TLS connection to its own proxy. The subsequent hops are all "best-effort" TLS. Using SIP over TLS in this manner is very simple. A video conferencing end device opens a TLS connection and uses SIP URIs (instead of SIPS URIs) for all the header fields in a SIP message (From, To, Request-URI, Contact header field, Route, etc.). When TLS is used, the Via header field indicates TLS. Managing Client Initiated Connections in SIP [RFC 5626] describes how to establish and maintain a TLS connection in environments where it can only be initiated by the UA.

SIPS URI: Use of the SIPS URI scheme when sending a request helps to achieve TLS on all hops by indicating that the request should be rejected if TLS is not available. However, this still provides no guarantee. In The Use of the SIPS URI Scheme in SIP [RFC 5630], the meaning and usage of the SIPS URI is clarified. First, the SIPS scheme implies transitive trust. While SIPS is useful to request that a resource be contacted securely, it is not useful as an indication that a resource was in fact contacted securely, since there is nothing that prevents proxies from "cheating". Therefore, it is not appropriate to infer that because an incoming request had a Request-URI (or even a To header field) containing a SIPS URI, that it necessarily guarantees that the request was in fact transmitted securely on each hop. Likewise, if a request is sent using a SIPS Request-URI, acceptance of the request does not guarantee that all hops are secure. For this reason, the SIPS URI is not required in the Best Practices Profile. Video conferencing end devices MAY support use of the SIPS URI scheme in accordance with RFC 3261, as updated by RFC 5630.

There is currently no mechanism to provide an indication of end-to-end security for SIP. Other mechanisms can provide a more concrete indication of security. For example, Enhancements for Authenticated Identity Management in SIP [RFC4474] provides an authenticated identity mechanism and a domain-to-domain integrity protection mechanism.

In the past, using TLS on the last hop of a SIPS session was not required when using SIPS. However, The Use of the SIPS URI Scheme in SIP [RFC 5630] deprecates the last hop exception by requiring that the target end device use the mechanisms in Managing Client Initiated Connections in SIP [RFC 5626] to support TLS on the last hop. This improves the chances that TLS is used on all hops all the way up to the remote target.

5. Protecting Media

5.1 SRTP

Secure RTP (or SRTP) is the primary mechanism used for media encryption. It is a RTP profile which provides:

- Media Confidentiality through fast AES encryption (a stream cipher)
- Media Packet Integrity using message authentication codes
- Media Packet Replay Protection (protects against DoS packet flooding attacks)
- Key Management Framework (which provides forward security)

Video conferencing end devices MUST use the confidentiality mechanisms in SRTP and SRTCP to ensure media confidentiality.

Video conferencing end devices MUST use the integrity mechanisms in SRTP and SRTCP to ensure media integrity.

Video conferencing end devices which are acting as receivers MUST maintain the indices of previously received packets and compare them with the index of each new received packet and admit the new packet only if it has not been played (i.e. sent) before. Such an approach relies on integrity protection being enabled (to make it impossible to spoof packet indices).

Video conferencing end devices MUST utilize the session key management framework to prevent an attacker from collecting large amounts of packets encrypted with one single session key. Re-derivation of the encryption key also provides backwards and forward security because a compromised session key does not compromise other session keys derived from the same master key.

Once SRTP is negotiated and operating for a stream, video conferencing end devices MUST continue to encrypt the channel even in the presence of dynamic codec switches for the channel.

5.1.1 Key Exchange for SRTP

The use of SRTP for media encryption requires that a secure session key be exchanged between the end instruments involved in the secure session. The IETF has standardized several key exchange mechanisms for SRTP. The “Best Practices” Profile requires use of SDP Security Descriptions for Media Streams [RFC 4568]. Although this has several limitations, and does not provide true end-to-end security, this is the only mechanism that has seen relatively widespread deployment. Datagram Transport Layer Security (DTLS) (DTLS Protocol for Protection of Media Traffic Established with SIP [RFC 5763] and DTLS Extension to Establish Keys for SRTP [RFC 5764]) has superior security properties, but has seen far too little deployment to be recommendable at present. Key exchange using Security Descriptions MUST be supported by video conferencing end devices following the “Best Practices” Profile.

In Security Descriptions, the keys are transported in the clear in the SDP attachment of a SIP message. Therefore, the transport layer for SIP must make sure that no unauthorized entity can see or modify the SDP attachment. This can be done by using TLS. By using TLS, an end device assumes that all hops in the SIP proxy chain can be trusted, although there is no mechanism in SIP which can guarantee this. The big advantage of Security Descriptions is that it is extremely simple.

5.1.2 Negotiation of SRTP

Negotiation of SRTP for media channels is accomplished using SDP. The “Best Practices” Profile takes a pragmatic approach that reflects common practice at the time of writing and is in line with the mechanism used in [Bandwidth and Flow Control Profile] for negotiating the use of feedback. The use of SDP Capability Negotiation [RFC 5939] for addressing more complex negotiation scenarios is outside the scope of this document.

There are three separate use cases:

- Where the offerer requires the use of SRTP (and will not accept RTP);
- Where the offerer prefers to use SRTP (but will accept RTP); and
- Where the offerer requires the use of RTP.

Offerer requires the use of SRTP: If the offerer requires the use of SRTP for a medium, the offerer MUST indicate transport protocol SRTP by including either SAVP or SAVPF in the 'proto' field of the SDP m= line and MUST include a=crypto attribute in the description of that medium.

If the answerer receives an SDP offer with SAVP or SAVPF in the 'proto' field of the m=line and an a=crypto attribute in the description of that medium and is prepared to accept the medium with SRTP, the answerer MUST include in the corresponding description in the SDP answer 'proto' value SAVP or SAVPF (as appropriate) and an a=crypto attribute (Extended Secure RTP Profile for RTCP-based Feedback (RTP/SAVPF) [RFC 5124]). If the answerer is not prepared to accept the medium using SRTP the answerer MUST reject the medium or the entire SDP offer.

An example of an SDP offer which mandates SRTP encryption support is:

```
m=video 50004 RTP/SAVP 34 97 101
a=crypto:2 AES_CM_128_HMAC_SHA1_80 inline:Oi0nVM8eJZ2bkLVNeRaqtUeqjXwGMXo0s0IrmoKh|2^31|1:1
```

An example SDP when the Peer responding to the request is capable of supporting, and does support, SRTP encryption, is:

```
m=video 50014 RTP/SAVP 34 97 101
a=crypto:2 AES_CM_128_HMAC_SHA1_80 inline:v0ncVM8eKP2bkOINeRaqcFeqjXwGMXo0sRalidZc|2^31|1:1
```

Offerer prefers the use of SRTP: If the offerer prefers the use of SRTP for a medium but will also accept RTP, the offerer MUST indicate transport protocol RTP by including either AVP or AVPF in the 'proto' field of the SDP m= line and MUST include attribute a=crypto in the description of that medium.

If the answerer receives an SDP offer with AVP or AVPF in the 'proto' field of the m=line and an a=crypto line in the description of that medium and is prepared to accept the medium with SRTP, the answerer MUST include in the corresponding description in the SDP answer 'proto' value AVP or AVPF (as appropriate) and an a=crypto attribute. If the answerer is prepared to accept the medium using RTP the answerer MUST include in the corresponding description in the SDP answer 'proto' value AVP or AVPF (as appropriate) and no a=crypto attribute.

An example of an SDP offer from a Peer which specifies that it can support SRTP encryption, but that the support is not mandatory, is:

```
m=video 50004 RTP/AVP 34 97 101
a=crypto:2 AES_CM_128_HMAC_SHA1_80 inline:Oi0nVM8eJZ2bkLVNeRaqtUeqjXwGMXo0s0IrmoKh|2^31|1:1
```

An example SDP when the Peer responding to the request is capable of supporting, and does support, SRTP encryption, is:

```
m=video 50014 RTP/AVP 34 97 101
a=crypto:2 AES_CM_128_HMAC_SHA1_80 inline:v0ncVM8eKP2bkOINeRaqcFeqjXwGMXo0sRalidZc|2^31|1:1
```

An example SDP when the Peer responding to the request is not capable of supporting or does not support SRTP encryption, is:

m=video 50104 RTP/AVP 43 97 101

An offerer that prefers the use of SRTP SHOULD be lenient when receiving an answer. It SHOULD interpret either: 1) RTP/AVP with the crypto attribute or 2) RTP/SAVP with the crypto attribute as indicating that the answerer is capable of supporting, and does support, SRTP encryption.

Offerer requires the use of RTP: If the offerer requires the use of RTP for a medium, the offerer MUST indicate transport protocol RTP by including either AVP or AVPF in the 'proto' field of the SDP m= line and MUST NOT include attribute a=crypto in the description of the medium.

If the answerer receives an SDP offer with AVP or AVPF in the 'proto' field of the m=line and no a=crypto line in the description of that medium and is not prepared to accept the medium with RTP, the answerer MUST reject the medium or the entire SDP offer.

5.2 Security for the BFCP Control Channel

Role-based video stream (RBVS) functionality in SIP is comparable to H.239 for H.323 systems. H.239 is the ITU standard for implementing role management of multiple streams in H.323 and H.320. It specifies mechanisms for:

1. Adding additional media channels to conferences,
2. Designating roles of video media channels (“Live” or “Presentation”) and
3. Controlling the presenter of the “Presentation” video stream during a conference.

In Role-Based Video Streams the "Presentation" channel is controlled by a token. The holder of the token is the presenter and all of the endpoints in the conference typically display the presenter’s stream on their content rendering display. In a centralized, multipoint conference, the MCU manages the token. SIP-based video elements implement token management and control using the Binary Floor Control Protocol (BFCP), which is specified in The Binary Floor Control Protocol (BFCP) [RFC 4582]. SIP-based video elements must use a UDP-based BFCP channel to conform to the IMTC SIP Parity Group’s RBVS “Best Practices” Profile.

This Security “Best Practices” Profile does not mandate that the UDP-based BFCP channel be secured because the value of the information which could be obtained from the BFCP channel is considered insignificant if the SIP signaling channel and media channels are secured as mandated by this profile. The threat risks against the UDP–based BFCP channel are summarized here:

Confidentiality: The BFCP messages FloorRequest, FloorRequestStatus, FloorRelease, FloorQuery and FloorStatus are used in RVBS. There are two attributes in these messages which could potentially reveal an actual user’s identity information: USER-URI and USER-DISPLAY-NAME. It is recommended that implementations do not use these attributes when the BFCP channel is not secured. If these attributes are not used, then the lack of confidentiality protection of the content of the BFCP messages is not considered to be critical.

Integrity: Without integrity protection, BFCP messages could be spoofed so that they would appear to be coming from a different user by a man-in-the-middle attack. This attack is only a concern in a multipoint conference where there are more than two participants. Under this attack, the attacker could request the presentation token with a false User ID. However, in order to actually inject false content into the presentation channel, the attacker would also have to be connected to the conference. Thus the attacker would need to be authenticated and would need to send/receive encrypted media and SIP signaling. Under most circumstances, the participants would quickly become aware of the spoofed ID.

Availability: Without integrity and replay protection mechanisms, false BFCP messages could be injected into a system and be used to bring down endpoints or bridges with flooding attacks. However, these devices could protect themselves from these attacks using techniques which don't rely on securing the channel.

6. Best Practices for Availability Protection

Availability refers to the ability to use information or resources. The most obvious example of an attack against availability in IP video conferencing is when a denial of service attack is used to take down, or slow down, a network so that video conferencing becomes unusable.

Availability of SIP-based video conferencing end devices is protected as an indirect result of deploying the authentication, integrity and confidentiality protection mechanisms listed in the previous sections.

- Authentication of users ensures that only authorized users gain access to video services. Since unauthorized users cannot gain use of system resources, availability is protected.
- Identity mechanisms can be used to ensure that unwanted calls can be blocked thus ensuring resources are only available to authorized users.
- SRTP integrity and replay protection protects video conferencing end devices from DoS attacks because they can readily reject packets that are not valid or valid packets that are being re-played.

7. List of Relevant IETF RFCs and Drafts

Normative references are listed in Table 7.1 and informative references are listed in Table 7.2

Normative References		
RFC or Draft	Title	Usage
RFC 3263	**Session Initiation Protocol (SIP): Locating SIP Servers**	The Session Initiation Protocol (SIP) uses DNS procedures to allow a client to resolve a SIP Uniform Resource Identifier (URI) into the IP address, port, and transport protocol of the next hop to contact. It also uses DNS to allow a server to send a response to a backup client if the primary client has failed.

RFC 3325	**Private Extensions to the Session Initiation Protocol (SIP) for Asserted Identity within Trusted Networks**	Describes private extensions to SIP that enable a network of trusted SIP servers to assert the identity of authenticated users, and the application of existing privacy mechanisms to the identity problem. The use of these extensions is only applicable inside an administrative domain with previously agreed-upon policies for generation, transport and usage of such information.
RFC 3711	**The Secure Real Time Transport Protocol (SRTP)**	Describes the Secure Real-time Transport Protocol (SRTP), a profile of the Real-time Transport Protocol (RTP), which can provide confidentiality, message authentication, and replay protection to the RTP traffic and to the control traffic for RTP, the Real-time Transport Control Protocol (RTCP).
RFC 4568	**Session Description Protocol (SDP) Security Descriptions for Media Streams**	Defines a Session Description Protocol (SDP) cryptographic attribute for unicast media streams. The attribute describes a cryptographic key and other parameters that serve to configure security for a unicast media stream in either a single message or a roundtrip exchange. The attribute can be used with a variety of SDP media transports, and this document defines how to use it for the Secure Real-time Transport Protocol (SRTP) unicast media streams. The SDP crypto attribute requires the services of a data security protocol to secure the SDP message.
RFC 5124	**Extended Secure RTP Profile for RTCP-based Feedback (RTP/SAVPF)**	Both SRTP and AVPF are RTP profiles and need to be negotiated. This implies that either one or the other may be used, but both profiles cannot be negotiated for the same RTP session (using one SDP session level description). However, using secure communications and timely feedback together is desirable. Therefore, this draft specifies a new RTP profile ("SAVPF") that combines the features of SAVP and AVPF.
RFC 5280	**Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile**	Profiles the X.509 v3 certificate and X.509 v2 certificate revocation list (CRL) for use in the Internet.
RFC 5626	**Managing Client Initiated Connections in the Session Initiation Protocol (SIP)**	Defines behaviors for User Agents, registrars and proxy servers that allow requests to be delivered on existing connections established by the User Agent. It also defines keep-alive behaviors needed to keep NAT bindings open and specifies the usage of multiple connections from the User Agent to its Registrar.
RFC 5630	**The use of the SIPS URI Scheme in the Session Initiation Protocol (SIP)**	This document provides clarifications and guidelines concerning the use of the SIPS URI scheme in the Session Initiation Protocol (SIP). It also makes normative changes to SIP (including both [RFC3261] and [RFC3608]). The meaning and usage of the SIPS URI scheme and of TLS (RFC4346) is underspecified in SIP (RFC3261) and has been a source of confusion for implementers and this document provides clarification.

RFC 5876	**Updates to Asserted Identity in SIP**	RFC 3325 does not specify the insertion of the P-Asserted-Identity header field by a trusted User Agent Client (UAC), does not specify the use of P-Asserted-Identity and P-Preferred-Identity header fields with certain SIP methods such as UPDATE, REGISTER, MESSAGE, and PUBLISH, and does not specify how to handle an unexpected number of URIs or unexpected URI schemes in these header fields. This document extends RFC 3325 to cover these situations.

Table 7.1 Relevant RFCs and Drafts for Security - Normative References

Informative References		
RFC or Draft	Title	Usage
RFC 2560	**X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP**	Specifies a protocol useful in determining the current state of a digital certificate without requiring CRLs.
RFC 4474	**Enhancements for Authenticated Identity Management in the Session Initiation Protocol (SIP)**	The existing security mechanisms in the Session Initiation Protocol (SIP) are inadequate for cryptographically assuring the identity of the end users that originate SIP requests, especially in an inter-domain context. This RFC defines a mechanism for securely identifying originators of SIP messages. It does so by defining two new SIP header fields, Identity, for conveying a signature used for validating the identity, and Identity-Info, for conveying a reference to the certificate of the signer.
RFC 4582	**The Binary Floor Control Protocol (BFCP)**	Specifies the Binary Floor Control Protocol (BFCP) which is used for token control.
RFC 5763	**Datagram Transport Layer Security (DTLS) Protocol for Protection of Media Traffic Established with the Session Initiation Protocol**	Specifies how to use the Session Initiation Protocol (SIP) to establish secure media sessions using or over the Datagram Transport Layer Security (DTLS) protocol. It describes a mechanism of transporting a fingerprint attribute in the Session Description Protocol (SDP) that identifies the key that will be presented during the DTLS handshake. It relies on the SIP identity mechanism to ensure the integrity of the fingerprint attribute. This allows the establishment of media security along the media path.
RFC5764	**Datagram Transport Layer Security (DTLS) Extension to Establish Keys for Secure Real-time Transport Protocol (SRTP)**	Describes a Datagram Transport Layer Security (DTLS) extension to establish keys for secure RTP (SRTP) and secure RTP Control Protocol (SRTCP) flows. DTLS keying happens on the media path, independent of any out-of-band signaling channel present.

RFC 5939	**SDP Capability Negotiation**	SDP does not address an increasingly important problem: the ability to negotiate one or more alternative transport protocols (e.g., RTP profiles). This document defines a mechanism that enables SDP to provide limited support for indicating capabilities and their associated potential configurations, and negotiate the use of those potential configurations as actual configurations.
IMTC SIP Parity Best Practices	**Role-Based Video Streams Best Practices**	This document describes the best practices for implementing role-based video stream (RBVS) functionality in SIP which is comparable to H.239 for H.323 systems.

Table 7.2 Relevant RFCs and Drafts for Security - Informative References

8. Glossary

Certificate Authority (CA) Certificates: A Certificate Authority certificate is a digital credential that validates the identity of the Certificate Authority (CA) that owns the certificate. The Certificate Authority's certificate contains identifying information about the Certificate Authority, as well as its public key. Others can use the CA certificate's public key to verify the authenticity of the certificates that the CA issues and signs. A Certificate Authority certificate can be signed by another CA, such as VeriSign, or can be self-signed if it is an independent entity.

Source: http://publib.boulder.ibm.com/infocenter/iseries/v5r3/index.jsp?topic=/rzahu/rzahutypesofcerts.htm

Server or Client Certificates: A server or client certificate is a digital credential that identifies the server or client application that uses the certificate for secure communications. Server or client certificates contain identifying information about the organization that owns the application, such as the system's distinguished name. The certificate also contains the system's public key. A server must have a digital certificate to use TLS for secure communications. Applications that support digital certificates can examine a server's certificate to verify the identity of the server when the client accesses the server. The application can then use the authentication of the certificate as the basis for initiating a TLS-encrypted session between the client and the server.

Source: http://publib.boulder.ibm.com/infocenter/iseries/v5r3/index.jsp?topic=/rzahu/rzahutypesofcerts.htm