SIMPLE Working Group	C.H. Holmberg
Internet-Draft	S.B. Blau
Intended status: Standards Track	Ericsson
Expires: April 07, 2012	E.W. Burger
	Georgetown University
	October 05, 2011

Connection Establishment for Media Anchoring (CEMA) for the Message Session Relay Protocol (MSRP)

draft-ietf-simple-msrp-cema-03.txt

Abstract

This document defines a Message Session Relay Protocol (MSRP) extension, Connection Establishment for Media Anchoring (CEMA). Support of the extension is optional. The extension allows middleboxes to anchor the MSRP connection, without the need for middleboxes to modify the MSRP messages, and thus also enables a secure end-to-end MSRP communication in networks where such middleboxes are deployed. The document also defines a Session Description Protocol (SDP) attribute, 'msrp-cema', that MSRP endpoints use to indicate support of the CEMA extension.

Status of this Memo

Copyright Notice

Table of Contents

*1. Introduction

*2. Conventions

*3. Applicability Statement

*4. Connection Establishment for Media Anchoring Mechanism

*4.1. General

*4.2. MSRP SDP Offerer Procedures

*4.3. MSRP SDP Answerer Procedures

*4.4. Address Information Matching

*4.5. Usage With the Alternative Connection Model

*5. The SDP 'msrp-cema' attribute

*5.1. General

*5.2. Syntax

*6. Middlebox Assumptions

*6.1. General

*6.2. MSRP Awareness

*6.3. TCP Connection Reuse

*6.4. SDP Integrity

*6.5. TLS

*7. Security Considerations

*7.1. Man in the Middle

*7.2. TLS Usage

*7.3. TLS and Insecure Signaling

*8. IANA Considerations

*8.1. IANA Registration of the SDP 'msrp-cema' attribute

*9. Acknowledgements

*10. Change Log

*11. References

*11.1. Normative References

*11.2. Informative References

*Authors' Addresses

1. Introduction

The Message Session Relay Protocol (MSRP) [RFC4975] expects to use MSRP relays [RFC4976] as a means for Network Address Translation (NAT) traversal and policy enforcement. However, many Session Initiation Protocol (SIP) [RFC3261] networks, which deploy MSRP, contain middleboxes. These middleboxes anchor and control media, perform tasks such as NAT traversal, performance monitoring, lawful intercept, address domain bridging, interconnect Service Layer Agreement (SLA) policy enforcement, and so on. One example is the Interconnection Border Control Function (IBCF) [GPP23228], defined by the 3rd Generation Partnership Project (3GPP). The IBCF controls a media relay that handles all types of SIP session media such as voice, video, MSRP, etc.

MSRP, as defined in RFC 4975 [RFC4975] and RFC 4976 [RFC4976], cannot anchor through middleboxes. The reason is that MSRP messages have routing information embedded in the message. Without an extension such as CEMA, middleboxes must read the message to change the routing information. This occurs because middleboxes modify the address:port information in the Session Description Protocol (SDP) [RFC4566] c/m-line in order to anchor media. An "active" [RFC6135] MSRP UA establishes the MSRP TCP or TLS connection based on the MSRP URI of the SDP 'path' attribute. This means that the MSRP connection will not be routed through the middlebox, unless the middlebox also modifies the MSRP URI of the topmost SDP 'path' attribute. In many scenarios this will prevent the MSRP connection from being established. In addition, if the middlebox modifies the MSRP URI of the SDP 'path' attribute, then the MSRP URI comparison procedure [RFC4975], which requires consistency between the address information in the MSRP messages and the address information carried in the MSRP URI of the SDP 'path' attribute, will fail.

The only way to achieve interoperability in this situation is for the middlebox to act as an MSRP back-to-back User Agent (B2BUA). Here the MSRP B2BUA acts as the endpoint for the MSRP signaling and media, performs the corresponding modification in the associated MSRP messages, and originates a new MSRP session towards the actual remote endpoint. However, the enabling of MSRP B2BUA functionality requires substantially more resource usage in the middlebox, that normally result in negative performance impact. In addition, the MSRP message needs to be exposed in clear text to the MSRP B2BUA, which violates the end-to-end principle [RFC3724] .

This specification defines an MSRP extension, Connection Establishment for Media Anchoring (CEMA). CEMA in most cases allows MSRP endpoints to communicate through middleboxes, as defined in Section 2, without a need for the middleboxes to be an MSRP B2BUA. In such cases, middleboxes, that want to anchor the MSRP connection simply modify the SDP c/m-line address information, similar to what it does for non-MSRP media types. MSRP endpoints that support the CEMA extension will use the SDP c/m-line address information for establishing the TCP or TLS connection for sending and receiving MSRP messages.

The CEMA extension is fully backward compatible. In scenarios where MSRP endpoints do not support the CEMA extension, an MSRP endpoint that supports the CEMA extension behaves in the same way as an MSRP endpoint that does not support it. The CEMA extension only provides an alternative mechanism for negotiating and providing address information for the MSRP TCP connection. After the creation of the MSRP connection, an MSRP endpoint that supports the CEMA extension acts according to the procedures for creating MSRP messages, performing checks when receiving MSRP messages defined in RFC 4975 and, when it is using a relay for MSRP communications, RFC 4976.

2. Conventions

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in BCP 14, RFC 2119 [RFC2119].

Definitions:

Fingerprint Based TLS Authentication: An MSRP endpoint that uses a self-signed TLS certificate and sends a certificate fingerprint in SDP.

Name Based TLS Authentication: An MSRP endpoint that uses a certificate from a well known certificate authority and the other endpoint matches the hostname in the received TLS communication SubjectAltName parameter towards the hostname received in the MSRP URI in SDP.

B2BUA: This is an abbreviation for back-to-back user agent.

MSRP B2BUA: A network element that terminates an MSRP connection from one MSRP endpoint and reoriginates that connection towards another MSRP endpoint. Note the MSRP B2BUA is distinct from a SIP B2BUA. A SIP B2BUA terminates a SIP session and reoriginates that session towards another SIP endpoint. In the context of MSRP, a SIP endpoint initiates a SIP session towards another SIP endpoint. However, that INVITE may go through, for example, an outbound Proxy or inbound Proxy to route to the remote SIP endpoint. As part of that SIP session an MSRP session, that may follow the SIP session path, is negotiated. However, there is no requirement to co-locate the SIP network elements with the MSRP network elements.

TLS B2BUA: A network element that terminates security associations (SAs) from endpoints, and establishes separate SAs between itself and each endpoint.
Middlebox: A SIP network device that modifies SDP media address:port information in order to steer or anchor media flows described in the SDP, including TCP and TLS connections used for MSRP communication, through a media proxy function controlled by the SIP endpoint. In most cases the media proxy function relays the MSRP messages without modification, while in some circumstances it acts as a MSRP B2BUA. Other SIP related functions, such as related to routing, modification of SIP information etc, performed by the Middlebox, and whether it acts a SIP B2BUA or not, is outside the scope of this document. Section 5 describes additional assumptions regarding how the Middlebox handles MSRP in order to support the extension defined in this document.
This document reuses the terms answer, answerer, offer and offerer as defined in RFC 3264.

3. Applicability Statement

This document defines a Message Session Relay Protocol (MSRP) extension, Connection Establishment for Media Anchoring (CEMA). Support of the extension is optional. The extension allows Middleboxes to anchor the MSRP connection, without the need for Middleboxes to modify the MSRP messages, and thus also enables a secure end-to-end MSRP communication in networks where such Middleboxes are deployed. The document also defines a Session Description Protocol (SDP) attribute, 'msrp-cema', that MSRP endpoints use to indicate support of the CEMA extension.
The CEMA extension is primarily intended for MSRP endpoints that operate in networks in which Middleboxes that want to anchor media connections are deployed, without the need for the Middleboxes to enable MSRP B2BUA functionality. An example of such network is the IP Multimedia Subsystem (IMS) defined by the 3rd Generation Partnership Project (3GPP), which also has the capability for all endpoints to use Name-based TLS Authentication. The extension is also useful for other MSRP endpoints operating in other networks, but that communicate with MSRP endpoints in networks with such Middleboxes, unless there is a gateway between the networks that by default always enable MSRP B2BUA functionality.
This document assumes certain behaviors on the part of Middleboxes, as described in Section 6. These behaviors are not standardized. If Middleboxes do not behave as assumed, then the CEMA extension does not add any value over base MSRP behavior. MSRP endpoints that support CEMA are required to use RFC 4975 behavior in cases where they detect that the CEMA extension cannot be enabled.

4. Connection Establishment for Media Anchoring Mechanism

4.1. General

This section defines how an MSRP endpoint that supports the CEMA extension generates SDP offers and answers for MSRP, and which SDP information elements the MSRP endpoint uses when creating the TCP or TLS connection for sending and receiving MSRP messages.
In the following cases, where there is a Middlebox in the network, the CEMA extension cannot be used, and there will be a fallback to the MSRP connection establishment procedures defined in RFC 4975 and RFC 4976:
- A non-CEMA-enabled MSRP endpoint becomes "active" [RFC6135] (no matter whether it uses a relay for its MSRP communication or not), as it will always establish the MSRP connection using the SDP 'path' attribute, which contains the address information of the remote MSRP endpoint, instead of using the SDP c/m-line which contains the address information of the Middlebox.
- A non-CEMA-enabled MSRP endpoint that uses a relay for its MSRP communication becomes "passive" [RFC6135], as it cannot be assumed that the MSRP endpoint inserts the address information of the relay in the SDP c/m-line.
- A CEMA-enabled MSRP endpoint that uses a relay for its MSRP communication becomes "active", since if it adds the received SDP c/m-line address information to the ToPath header field of the MSRP message (in order for the relay to establish the MSRP connection towards the Middlebox), the session matching [RFC4975] performed by the remote MSRP endpoint will fail.

4.2. MSRP SDP Offerer Procedures

When a CEMA-enabled offerer sends an SDP offer for MSRP, it generates the SDP offer according to the procedures in RFC 4975. In addition, the offerer follows RFC 4976 if it is using a relay for MSRP communication. The offerer also performs the following additions and modifications:
1. The offerer MUST include an SDP 'msrp-cema' attribute in the MSRP media description of the SDP offer.
2. If the offerer is not using a relay for MSRP communication, it MUST include an SDP 'setup' attribute in the MSRP media description of the SDP offer, according to the procedures in RFC 6135 [RFC6135].
3. If the offerer is using a relay for MSRP communication, it MUST, in addition to including the address information of the relay in the topmost SDP 'path' attribute, also include the address information of the relay, rather than the address information of itself, in the SDP c/m-line associated with the MSRP media description. In addition, it MUST include an SDP 'setup:actpass' attribute in the MSRP media description of the SDP offer.
When the offerer receives an SDP answer, if the MSRP media description of the SDP answer does not contain an SDP 'msrp-cema' attribute, the offerer MUST check the criteria below. If either or all of the criteria

is met, the offerer MUST fallback to RFC 4975 behavior, by sending a new SDP offer according to the procedures in RFC 4975 and RFC 4976. The new offer MUST NOT contain an SDP 'msrp-cema' attribute.

1. The SDP c/m-line address information associated with the MSRP media description does not match Section 4.4 the information in the MSRP URI of the 'path' attribute(s) (in which case is assumed that the SDP c/m-line contains the address to a Middlebox), and the MSRP endpoint will become "passive" (if the MSRP media description of the SDP answer contains an SDP 'setup:active' attribute).

NOTE: If an MSRP URI contains a domain name, it needs to be resolved into an IP address and port before it is checked against the SDP c/m-line address information, in order to determine whether there address information matches.

2. The offerer uses a relay for its MSRP communication, the SDP c/m-line address information associated with the MSRP media description does not match the information in the MSRP URI of the SDP 'path' attribute(s) (in which case is assumed that the SDP c/m-line contains the address to a Middlebox), and the offerer will become "active" (either by default or if the MSRP media description of the SDP answer contains an SDP 'setup:passive' attribute).

3. The remote MSRP endpoint, acting as an answerer, uses a relay for its MSRP communication, the SDP c/m-line address information associated with the MSRP media description does not match the information in the MSRP URI of the SDP 'path' attributes (in which case is assumed that the SDP c/m-line contains the address to a Middlebox), and the MSRP offerer will become "active" (either by default or if the MSRP media description of the SDP answer contains an SDP 'setup:passive' attribute).

NOTE: As described in section 5, in the absence of the SDP 'msrp-cema' attribute in the new offer, it is assumed that a Middlebox will act as an MSRP B2BUA in order to anchor MSRP media.

The offerer can send the new offer within the existing early dialog [RFC3261], or it can terminate the early dialog and establish a new dialog by sending the new offer in a new initial INVITE request.

The offerer MAY choose to terminate the session establishment if it can detect that a Middlebox acting as an MSRP B2BUA is not the desired remote MSRP endpoint.

If the answerer uses a relay for its MSRP communication, and the SDP c/m-line address information associated with the MSRP media description matches one of the SDP 'path' attributes, it is assumed that there is no Middlebox in the network. In that case the offerer MUST fallback to RFC 4975 behavior, but it does not need to send a new SDP offer.

In other cases, where none of the criteria above is met, and where the MSRP offerer becomes "active", it MUST use the SDP c/m-line for establishing the MSRP TCP connection. If the offerer becomes "passive", it will wait for the answerer to establish the TCP connection, according to the procedures in RFC 4975.

4.3. MSRP SDP Answerer Procedures

If the MSRP media description of the SDP offer does not contain an SDP 'msrp-cema' attribute, and the SDP c/m-line address information associated with the MSRP media description does not match the information in the MSRP URI of the SDP 'path' attribute(s), the answerer MUST either reject the offered MSRP connection (by using a zero port value number in the generated SDP answer), or reject the whole SDP offer carrying SIP request with a 488 Not Acceptable Here [RFC3261] response.

NOTE: The reasons for the rejection is that the answerer assumes that a middlebox, that do not support the CEMA extension, has modified the c/m-line address information of the SDP offer, without enabling MSRP B2BUA functionality.

NOTE: If an MSRP URI contains a domain name, it needs to be resolved into an IP address and port before it is checked against the SDP c/m-line address information, in order to determine whether there address information matches.

If any of the criteria below is met, the answerer MUST fallback to RFC 4975 behavior and generate the associated SDP answer according to the procedures in RFC 4975 and RFC 4976. The answerer MUST NOT insert an SDP 'msrp-cema' attribute in the MSRP media description of the SDP answer.

1. Both MSRP endpoints are using relays for their MSRP communication. The answerer can detect if the remote MSRP endpoint, acting as an offerer, is using a relay for its MSRP communication if the MSRP media description of the SDP offer contains multiple SDP 'path' attributes.
2. The offerer uses a relay for its MSRP communication, and will become "active" (either by default or if the MSRP media description of the SDP offer contains an SDP 'setup:active' attribute). Note that a CEMA-enabled offerer would include an SDP 'setup:actpass' attribute in the SDP offer, as described in Section 4.2.
3. The answerer uses a relay for MSRP communication and is not able to become "passive" (if the MSRP media description of the offer contains an SDP 'setup:passive' attribute. Note that an offerer is not allowed to include an SDP 'setup:passive' attribute in an SDP offer, as described in RFC 6135.

In all other cases, the answerer generates the associated SDP answer according to the procedures in RFC 4975 and RFC 4976, with the following additions and modifications:

1. The answerer MUST include an SDP 'msrp-cema' attribute in the MSRP media description of the SDP answer.
2. If the answerer is not using a relay for MSRP communication, it MUST include an SDP 'setup' attribute in the MSRP media description of the answer, according to the procedures in RFC 6135.
3. If the answerer is using a relay for MSRP communication, it MUST, in addition to including the address information of the relay in the topmost SDP 'path' attribute, also include the address information of the relay, rather than the address information of itself, in the SDP c/

m-line associated with the MSRP media description. In addition, the answerer MUST include an SDP 'setup:passive' attribute in the MSRP media description of the SDP answer.

If the answerer included an SDP 'msrp-cema' attribute in the MSRP media description of the SDP answer, and if the answerer becomes "active", it MUST use the received SDP c/m-line for establishing the MSRP TCP or TLS connection. If the answerer becomes "passive", it will wait for the offerer to establish the MSRP TCP or TLS connection, according to the procedures in RFC 4975.

4.4. Address Information Matching

When comparing address information in the SDP c/m-line and an MSRP URI, for address and port equivalence, the address and port values are retrieved in the following ways:

- SDP c/m-line address information: The IP address is retrieved from the SDP c- line, and the port from the associated SDP m- line for MSRP.
- In case the SDP c- line contains a Fully Qualified Domain Name (FQDN), the IP address is retrieved using DNS.
- MSRP URI address information: The IP address and port are retrieved from the authority part of the MSRP URI.
- In case the authority part of the MSRP URI contains a Fully Qualified Domain Name (FQDN), the IP address is retrieved using DNS, according to the procedures in section 6.2 of RFC 4975.

NOTE: According to RFC 4975, the authority part of the MSRP URI must always contain a port.

NOTE: Before IPv6 addresses are compared for equivalence, they need to be converted into the same representation, e.g. using the mechanism defined in RFC 5952 [RFC5952].

NOTE: In case the DNS returns multiple records, each needs to be compared against the SDP c/m- line address information.

NOTE: If the authority part of the MSRP URI contains special characters, they are handled according to the procedures in section 6.1 of RFC 4975.

4.5. Usage With the Alternative Connection Model

An MSRP endpoint that supports the CEMA extension MUST support the mechanism defined in RFC 6135, as it extends the number of scenarios where one can use the CEMA extension. An example is where an MSRP endpoint is using a relay for MSRP communication, and it needs to be "passive" in order to use the CEMA extension, instead of doing a fallback to RFC 4975 behavior.

5. The SDP 'msrp-cema' attribute

5.1. General

The SDP 'msrp-cema' attribute is used by MSRP entities to indicate support of the CEMA extension, according to the procedures in Sections 4.2 and 4.3.

5.2. Syntax

This section describes the syntax extensions to the ABNF syntax defined in RFC 4566 required for the SDP 'msrp-cema' attribute. The ABNF defined in this specification is conformant to RFC 5234 [RFC5234].

```
attribute          /= msrp-cema-attr
;attribute defined in RFC 4566
msrp-cema-attr     = "msrp-cema"
```

6. Middlebox Assumptions

6.1. General

This document does not specify explicit Middlebox behavior, even though Middleboxes enable some of the procedures described here. However, as MSRP endpoints are expected to operate in networks where Middleboxes that want to anchor media are present, this document makes certain assumptions regarding to how such Middleboxes behave.

6.2. MSRP Awareness

In order to support interoperability between UAs that support the CEMA extension and UAs that do not support the extension, the Middlebox is MSRP aware. This means that it implements MSRP B2BUA functionality. The Middlebox enables that functionality in cases where the offerer does not support the CEMA extension. In cases where the SDP offer indicates support of the CEMA extension, the Middlebox can simply modify the SDP c/m-line address information for the MSRP connection.
In cases where the Middlebox enables MSRP B2BUA functionality, it acts as an MSRP endpoint. If it does not use the CEMA procedures it will never forward the SDP 'msrp-cema' attribute in SDP offers and answers. If the Middlebox does not implement MSRP B2BUA functionality, or does not enable it when the SDP 'msrp-cema' attribute is not present in the SDP offer, CEMA-enabled MSRP endpoints will in some cases be unable to interoperate with non-CEMA-enabled endpoints across the Middlebox.

6.3. TCP Connection Reuse

Middleboxes do not need to parse and modify the MSRP payload when endpoints use the CEMA extension. A Middlebox that does not parse the

MSRP payload probably will not be able to reuse TCP connections for multiple MSRP sessions. Instead, in order to associate an MSRP message with a specific session, the Middlebox often assigns a unique local address:port combination for each MSRP session. Due to this, between two Middleboxes there might be a separate connection for each MSRP session.

If the Middlebox does not assign a unique address:port combination for each MSRP session, and does not parse MSRP messages, it might end up forwarding MSRP messages towards the wrong destination.

6.4. SDP Integrity

This document assumes that Middleboxes are able to modify the SDP address information associated with the MSRP media. Middleboxes cannot be deployed in environments that require end-to-end SDP integrity protection or SDP encryption.

NOTE: Eventhough the CEMA extension as such works with end-to-end SDP protection, the main advantage of the extension is in networks where Middleboxes are deployed.

If the Middlebox is unable to modify SDP payloads due to end-to-end integrity protection, it will be either unable to anchor MSRP media, or the SIP signaling might fail due to integrity violations.

6.5. TLS

When UAs use the CEMA extension, this document assumes that Middleboxes relay MSRP media packets at the transport layer. The TLS handshake and resulting security association (SA) can be established peer-to-peer between the MSRP endpoints. The Middlebox will see encrypted MSRP media packets, but is unable to inspect the clear text content.

When UAs fall back to RFC 4975 behavior Middleboxes act as TLS B2BUAs. The Middlebox decrypts MSRP media packets received from one MSRP endpoint, and then re-encrypts them before sending them toward the other MSRP endpoint. Middleboxes can inspect and modify the MSRP message content. As CEMA does not require a Middlebox to modify the MSRP content, this can be prevented if TLS is used for the MSRP communication, assuming that the SIP signalling channel is end-to-end integrity protected.

7. Security Considerations

7.1. Man in the Middle

In some cases, where MSRP B2BUA functionality does not need to be enabled, the CEMA extension makes it easier for a man in the middle (MiTM) to transparently insert itself in the communication between MSRP endpoints in order to monitor or record unprotected MSRP communication. It does not however make it easier for a MiTM to monitor TLS protected MSRP, or in any significant way modify TLS protected MSRP content or even find out that the packets contain MSRP messages, since that would require the MiTM to implement MSRP B2BUA functionality, no matter if UAs support the CEMA extension or not. It would thus require the MiTM to terminate the TCP/TLS/MSRP connection in both directions. MSRP endpoints SHOULD use encrypted channels, if possible. For backward compability, a CEMA-enabled MSRP endpoint MUST implement TLS.

7.2. TLS Usage

The CEMA extension supports the usage of name-based authentication for TLS in the presence of Middleboxes.

If a Middlebox acts as a TLS B2BUA, MSRP endpoints will be able to use fingerprint based authentication and name-based authentication for TLS, no matter if they support the CEMA extension or not. In such cases, as the Middlebox acts as TLS endpoints, MSRP endpoints might be given an incorrect impression that there is an end-to-end security association (SA) between the MSRP endpoints.

If a Middlebox does not act as a TLS B2BUA, fingerprint based authentication will not work, as the "SIP Identity" based integrity protection of SDP will break. Therefore, in addition to the authentication mechanisms defined in RFC 4975, it is RECOMMENDED that a CEMA-enabled MSRP endpoint also support one one of the following authentication mechanisms, that do not rely on peer-to-peer SDP integrity:

1. TLS certificates together with support of interacting with a Certificate Management Service [RFC6072], to which it publishes the public version of its own self-signed certificate and from which it fetches on demand the public certificates of other endpoints.
2. TLS-PSK managed by MIKEY-TICKET Based Key Management and Key Management Service [RFC6043]. Note that 3GPP has specified the MIKEY-TICKET based Key Management and Key Management Service authentication mechanism for the IP Multimedia Subsystem (IMS). Thus it will be available in that environment.

When an MSRP endpoint generates an SDP offer for MSRPS, in addition to the SDP attributes associated with the TLS authentication mechanisms described in RFC 4975, it MUST include any information elements associated with the other authentication mechanisms that it supports.

If possible, MSRP endpoints MUST use name-based authentication. If not possible, if the MSRP endpoints support a common authentication mechanism, they MUST use that mechanism. If the MSRP endpoints do not support such common authentication mechanism, they MUST try fingerprint-based authentication, which will succeed if there are no Middleboxes present. If that also fails, the MSRP endpoints MUST either:

1. Consider the TLS authentication as failed, in accordance with RFC 4975; or
2. If the SIP signaling is integrity protected between the endpoint and network elements on a hop-by-hop basis, typically through use of IPsec or TLS transport, then an endpoint can depending on local policy choose

to trust the network endpoints in the signalling path for SDP integrity and accept fingerprint based TLS authentication without requiring end-to-end SDP integrity.

NOTE: As defined in RFC 4975, if TLS authentication fails, the user needs to be able to decide whether to try anyway to establish a connection with unprotected MSRP media.

7.3. TLS and Insecure Signaling

One of the side effects of relieving Middleboxes from manipulating message content in CEMA provides an environment necessary for end-to-end integrity of MSRP media.

CEMA recommends using an integrity-protected media channel, such as TLS. As defined in RFC 4975, all MSRP endpoints MUST support TLS. That applies also to CEMA-enabled endpoints.

One issue with usage of TLS is the availability of a certificate infrastructure. Endpoints can always provide self-signed certificates. However, this is problematic in that any endpoint can masquerade as another, by providing a self-signed certificate with the victim's information.

One of the target deployments for CEMA is the 3GPP IMS SIP network. In this environment service providers provision signed certificates or manage signed certificates on behalf of their subscribers. This does require trusting the service provider, but those issues are beyond the scope of this document.

Alternate key distribution mechanisms, such as DANE [DANE], PGP [RFC6091], or some other technology, might become ubiquitous enough to solve the key distribution problem in the future.

Even with seemingly end-to-end media integrity, at the time of the publication of this document there are other vulnerabilities in MSRP, due to vulnerabilities in the SIP signaling. If there are no integrity protections on the SIP signaling, it is easy to insert malicious middleboxes to alter, record, or otherwise harm the media. With insecure signaling, it can be difficult for an endpoint to even be aware the remote endpoint has any relationship to the expected endpoint. Securing the SIP signaling does not solve all problems. For example, in a SIPS environment, the endpoints have no cryptographic way of validating that one or more SIP Proxies in the proxy chain are not, in fact, malicious.

8. IANA Considerations

8.1. IANA Registration of the SDP 'msrp-cema' attribute

This document instructs IANA to add a attribute to the 'att-field (media level only)' registry of the SDP parameters registry, according to the information provided in this section.

This section registers a new SDP attribute, 'msrp-cema'. The required information for this registration, as specified in RFC 4566, is:

Contact name: Christer Holmberg

Contact e-mail: christer.holmberg@ericsson.com

Attribute name: msrp-cema

Type of attribute: media level

Purpose: This attribute is used to indicate support of
         the MSRP Connection Establishment for Media
         Anchoring (CEMA) extension defined in
         RFC XXXX. When present in an MSRP media
         description of an SDP body, it indicates
         that the creator of the SDP supports the CEMA
         mechanism.

Values: The attribute does not carry a value

Charset dependency: none

9. Acknowledgements

Thanks to Ben Campbell, Remi Denis-Courmont, Nancy Greene, Hadriel Kaplan, Adam Roach, Robert Sparks, Salvatore Loreto, Shida Schubert, Ted Hardie, Richard L Barnes, Inaki Baz Castillo, Saul Ibarra Corretge, Cullen Jennings, Adrian Georgescu and Miguel Garcia for their guidance and input in order to produce this document.

10. Change Log

[RFC EDITOR NOTE: Please remove this section when publishing]
Changes from draft-ietf-simple-msrp-cema-02

*Changes based on WGLC comments.

*- Editorial changes based on comments from Nancy Greene.

*- Editorial changes based on comments from Saul Ibarra Corretge.

*- Editorial changes based on comments from Christian Schmidt.

*- Editorial changes based on comments from Miguel Garcia.

*Changes based on MMUSIC SDP impact review.

*- Editorial changes based on comments from Miguel Garcia.

Changes from draft-ietf-simple-msrp-cema-01

*Changes based on comment from Ben Campbell.

*- TLS B2BUA added to definitions section.

*- Middlebox added.

*- Editorial changes.

Changes from draft-ietf-simple-msrp-sessmatch-13

*Changed the draft name, as was suggested by our AD and work group.

*Clean up language use, clarify language, and clean up editorial and style issues.

*Formally defined an MSRP B2BUA.

Changes from draft-ietf-simple-msrp-sessmatch-12

*Extension name changed to Connection Establishment for Media Anchoring (CEMA).

*Middlebox definition added.

*ALG terminology replaced with Middlebox.

*SDP attribute name changed to a=msrp-cema.

*Applicability Statement section expanded.

*Re-structuring of MSRP Answerer section.

*Changes based on comments from Saúl Ibarra Corretgé (1406111).

Changes from draft-ietf-simple-msrp-sessmatch-11

*Modification of the sessmatch mechanism.

*- Extension name changed to Alternative Connection Establishment (ACE)

*- Session matching procedure no longer updated.

*- SDP c/m-line used for MSRP TCP connection.

*- sessmatch option-tag removed.

*- a=msrp-ace attribute defined.

*- Support of RFC 6135 mandatory.

Changes from draft-ietf-simple-msrp-sessmatch-10

*Sessmatch option-tag added, based on WG discussions and concensus.

Changes from draft-ietf-simple-msrp-sessmatch-08

*OPEN ISSUE regarding the need for a sessmatch option-tag removed.

Changes from draft-ietf-simple-msrp-sessmatch-07

*Sessmatch defined as an MSRP extension, rather than MSRP update

*Additional security considerations text added

11. References

11.1. Normative References

[RFC2119]	Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.
[RFC3261]	Rosenberg, J., Schulzrinne, H., Camarillo, G., Johnston, A., Peterson, J., Sparks, R., Handley, M. and E. Schooler, "SIP: Session Initiation Protocol", RFC 3261, June 2002.
[RFC4566]	Handley, M., Jacobson, V. and C. Perkins, "SDP: Session Description Protocol", RFC 4566, July 2006.
[RFC4975]	Campbell, B., Mahy, R. and C. Jennings, "The Message Session Relay Protocol (MSRP)", RFC 4975, September 2007.
[RFC4976]	Jennings, C., Mahy, R. and A.B. Roach, "Relay Extensions for the Message Sessions Relay Protocol (MSRP)", RFC 4976, September 2007.
[RFC5234]	Crocker, D. and P. Overell, "Augmented BNF for Syntax Specifications: ABNF", STD 68, RFC 5234, January 2008.
[RFC6072]	Jennings, C. and J. Fischl, "Certificate Management Service for the Session Initiation Protocol (SIP)", RFC 6072, February 2011.
[RFC6135]	Holmberg, C. and S. Blau, "An Alternative Connection Model for the Message Session Relay Protocol (MSRP)", RFC 6135, February 2011.

11.2. Informative References

, "

[RFC3724]	Kempf, J., Austein, R., IAB, "The Rise of the Middle and the Future of End-to-End: Reflections on the

	Evolution of the Internet Architecture", RFC 3724, March 2004.
[RFC5952]	Kawamura, S. and M. Kawashima, "A Recommendation for IPv6 Address Text Representation", RFC 5952, August 2010.
[RFC6043]	Mattsson, J. and T. Tian, "MIKEY-TICKET: Ticket-Based Modes of Key Distribution in Multimedia Internet KEYing (MIKEY)", RFC 6043, March 2011.
[RFC6091]	Mavrogiannopoulos, N. and D. Gillmor, "Using OpenPGP Keys for Transport Layer Security (TLS) Authentication", RFC 6091, February 2011.
[GPP23228]	3GPP, "IP Multimedia Subsystem (IMS); Stage 2", 3GPP TS 23.228 10.5.0, June 2011.
[DANE]	DNS-based Authentication of Named Entities Work Group", .

Authors' Addresses

Christer Holmberg Holmberg Ericsson Hirsalantie 11 Jorvas, 02420 Finland EMail: christer.holmberg@ericsson.com

Staffan Blau Blau Ericsson Stockholm, 12637 Sweden EMail: staffan.blau@ericsson.com

Eric Burger Burger Georgetown University Department of Computer Science 37th and O Streets, NW Washington, DC 20057-1232 United States of America EMail: eburger@standardstrack.com URI: http://www.standardstrack.com