SIMPLE Working Group	C. Holmberg
Internet-Draft	S. Blau
Intended status: Standards Track	Ericsson
Expires: February 27, 2012	E. Burger, Ed.
	Georgetown University
	August 26, 2011

TOC

Connection Establishment for Media Anchoring (CEMA) for the Message Session Relay Protocol (MSRP) draft-ietf-simple-msrp-cema-00.txt

Abstract

This document defines an Message Session Relay Protocol (MSRP) extension, Connection Establishment for Media Anchoring (CEMA). MSRP endpoints implement this extension to enable secure, end-to-end MSRP communication in networks where Middleboxes anchor the MSRP connection. CEMA eliminates the need for Middleboxes to modify MSRP messages. Modifying MSRP messages requires the Middlebox to read the message in plain text, exposing the message to attack. The document also defines a Session Description Protocol (SDP) attribute, a=msrp-cema, that MSRP endpoints use to indicate support of the CEMA extension.

Status of this Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at http://datatracker.ietf.org/drafts/current/.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as “work in progress.”

This Internet-Draft will expire on February 27, 2012.

Copyright Notice

Table of Contents

---

1. Introduction

TOC

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. Since the active MSRP UA establishes the MSRP TCP connection based on the MSRP URI of the SDP a=path attribute, this means that the MSRP connection will not, unless the Middlebox also modifies the MSRP URI of the topmost SDP a=path attribute, be routed through the Middlebox. In many scenarios this will prevent the MSRP connection from being established. In addition, if the Middlebox modifies the MSRP URI of the SDP a=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 a=path attribute, will fail. Also the matching will fail if Middleboxes modify the address information in the MSRP URI of the SDP a=path attribute.

The only way to achieve interoperability in this situation is for the Middlebox to be a 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, this interoperability comes at the cost of exposing the MSRP message in clear text to the MSRP B2BUA. This is a serious violation of 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 without a need for the Middleboxes to be a 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 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 TCP 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

TOC

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 stream from a first MSRP endpoint and reoriginates that stream towards a second MSRP endpoint. Note the MSRP B2BUA is distinct from a SIP B2BUA. A SIP B2BUA terminates a SIP session and reoriginates that session towards the SIP endpoint. In the context of MSRP, a first SIP endpoint initiates a SIP session towards the remote SIP endpoint. However, that INVITE may go through, for example, an outbound Proxy or inbound Proxy to route to the remote SIP endpoint. That SIP session negotiates a MSRP session that may or may not follow the SIP session path. Although often the case, there is no requirement to co-locate the SIP network elements with the MSRP network elements.

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 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.

---

3. Applicability Statement

TOC

This document defines an MSRP extension, Connection Establishment for Media Anchoring (CEMA). Support of the extension is optional. MSRP endpoints implement the extension in order to allow MSRP communication in networks where Middleboxes anchor the MSRP connection, without the need for the Middleboxes to decode and rewrite MSRP messages and enabling end-to-end security. The document also defines a Session Description Protocol (SDP) **[RFC4566]** attribute, a=msrp-cema, that can be used by MSRP endpoints to indicate support of the CEMA extension.

An important use case for CEMA are Third-Generation Partnership Program Internet

Multimedia System (3GPP IMS) SIP networks. These networks use Middleboxes for various functions. Moreover, these networks have the capability for all endpoints to use Name-based TLS Authentication.

There is nothing special about 3GPP IMS SIP networks to indicate the use of CEMA. Rather, CEMA is an important update to MSRP that closes a number of existing security issues and creates a foundation for closing other security issues in the future. Therefore, CEMA is for all MSRP deployments that use Middleboxes. Moreover, because of the presence of secure transport, CEMA is for all MSRP deployments, including those without Middleboxes.

Section 6 describes this further.

---

4. Connection Establishment for Media Anchoring Mechanism

TOC

4.1. General

TOC

This section defines how an MSRP endpoint that supports the CEMA extension generates SDP offers and answers for MSRP, and what SDP information elements the MSRP endpoint uses when creating the TLS connection for the MSRP messages.

4.2. MSRP Offer Procedures

TOC

When a CEMA-enabled MSRP endpoint sends an SDP offer for MSRP, it generates the SDP offer according to the procedures in RFC 4975. In addition, the endpoint follows RFC 4976 if it is using a relay for MSRP communication. The endpoint also performs the following additions and modifications:

1. The MSRP endpoint MUST include an SDP a=msrp-cema attribute in the MSRP media description of the SDP offer.
2. If the MSRP endpoint is not using a relay for MSRP communication, it MUST include an SDP a=setup attribute in the MSRP media description of the SDP offer, according to the procedures in **RFC 6135** [RFC6135].
3. If the MSRP endpoint is using a relay for MSRP communication, it MUST include the address information of the relay (the MSRP URI of the topmost SDP a=path attribute), 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 a=setup:actpass attribute in the MSRP media description of the SDP offer.

The MSRP endpoint then receives the first SDP answer to the SDP offer above. The SDP answer indicates that the remote MSRP endpoint accepted the offered MSRP media if the port number of the MSRP media description is not zero. If the MSRP media description of the SDP answer does not contain an SDP a=msrp-cema attribute, the MSRP endpoint makes the following checks. If either or both of these checks fails, the MSRP endpoint 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 a=msrp-cema attribute.

1. The SDP c/m-line address information associated with the MSRP media description does not match the information in the MSRP URI of the topmost SDP a=path attribute, and the MSRP media description contains an SDP a=setup:active attribute (indicating that the remote MSRP endpoint is "active").
2. The MSRP media description contains multiple SDP a=path attributes, indicating the use of MSRP relays.

In the absence of the SDP a=msrp-cema attribute in the new offer, the Middlebox MUST act as an MSRP B2BUA to anchor MSRP media. Note the originating endpoint should reject the session if it can detect the MSRP B2BUA is not the desired remote endpoint.

The MSRP endpoint 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.

In all other cases, where the MSRP endpoint becomes "active", it MUST use the SDP c/m-line for establishing the MSRP TLS connection. If the MSRP endpoint becomes "passive", it will wait for the remote MSRP endpoint to establish the TLS connection, according to the procedures in RFC 4975.

TOC

4.3. MSRP Answer Procedures

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

1. Both MSRP endpoints are using relays for MSRP communication. An endpoint can detect the remote MSRP endpoint is using a relay for MSRP communication if the MSRP media description of the SDP offer contains multiple SDP a=path attributes.
2. The remote MSRP endpoint uses a relay for MSRP communication, and will become "active" either by default or if the MSRP media description of the SDP offer contains an SDP a=setup:active attribute. This case indicates the remote MSRP endpoint does not support the CEMA extension. A CEMA-enabled endpoint would include an SDP a=setup:actpass attribute in the SDP offer, as described in **Section 4.2**.
3. The MSRP endpoint uses a relay for MSRP communication and is not able to become "passive". The indication for this is the MSRP media description of the offer contains an SDP a=setup:passive attribute. This will not occur with a CEMA-enabled endpoint, as it cannot include an SDP a=setup:passive attribute in an SDP offer, as described in RFC 6135.
4. The MSRP media description of the SDP offer does not contain an SDP a=msrp-cema attribute, the SDP c/m-line address information associated with the MSRP media description does not match the information in the MSRP URI of the topmost SDP a=path attribute, and the remote MSRP endpoint will become "active", either by default, or if the MSRP media description of the SDP offer contains an SDP a=setup:active attribute.

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

1. The MSRP endpoint MUST include an SDP a=msrp-cema attribute in the MSRP media description of the SDP answer.
2. If the MSRP endpoint is not using a relay for MSRP communication, it MUST include an SDP a=setup attribute in the MSRP media description of the answer, according to the procedures in RFC 6135.
3. If the MSRP endpoint is using a relay for MSRP communication, it MUST include the address information on the relay (the MSRP URI of the topmost SDP a=path attribute), 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 a=setup:passive attribute in the MSRP media description of the SDP answer.

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

TOC

4.4. 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 a 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. Middlebox Assumptions

TOC

5.1. General

TOC

This document does not specify explicit Middlebox behavior, even though Middleboxes enable some of the procedures described here. However, as one rationale for the CEMA extension is to allow MSRP endpoints to communicate over end-to-end secure paths in networks where Middleboxes that want to anchor media are present, this document makes certain assumptions regarding to how such Middleboxes behave.

5.2. MSRP Awareness

TOC

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 remote endpoint does not support the CEMA extension. In cases where at least one MSRP endpoint supports the CEMA extension, the Middlebox can simply modify the SDP c/m-line address information for the MSRP connection.

5.3. TCP Connection Reuse

TOC

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.

5.4. SDP Integrity

TOC

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 protection using **SIP identity** [RFC4916].

5.5. TLS

TOC

The Middlebox relays MSRP media packets at the transport layer. The TLS handshake and resulting security association (SA) are 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.

6. Security Considerations

TOC

6.1. Man in the Middle

TOC

In some cases, the CEMA extension could make 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. Therefore, endpoints MUST use encrypted

channels. For base interoperability, a CEMA-enabled MSRP endpoint MUST implement TLS.

TOC

6.2. 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 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, an MSRP endpoint supporting the CEMA extension MAY support an authentication mechanism that does not rely on peer-to-peer SDP integrity.

It is RECOMMENDED that an MSRP endpoint support one of the following authentication mechanisms:

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.

Unless the MSRP endpoints are able to use name-based authentication, and they 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 something like SIPS protects the SIP signaling between the MSRP endpoints, use fingerprint based authentication without requiring peer-to-peer SDP integrity, and thus trust the network endpoints in the signaling path for SDP integrity.

As defined in RFC 4975, if TLS authentication fails, the user needs to be able to decide whether to try to establish an MSRP connection in the likely scenario of intercepted, altered, or forged connections

---

TOC

6.3. TLS and Insecure Signaling

MSRP is the only SIP-based media transport that has a layer violation. MSRP media includes routing information, including from and to URIs. Other SIP-based media can have separate paths for signaling and media and can have end-to-end integrity of the media. Except for MSRP, SIP-based media can flow through routers, NATs, **TURN servers** [RFC5766], **STUN servers** [RFC5389], and so on without modification.

CEMA provides an environment necessary for end-to-end integrity of MSRP media. CEMA makes it possible to route MSRP media without requiring modification of the media. This is what enables end-to-end, cryptographic integrity assurance. However, while CEMA is a

necessary prerequisite for end-to-end integrity, it is not sufficient.

CEMA mandates an integrity-protected media channel. At the base level, all CEMA endpoints MUST support TLS. Unless the CEMA endpoints negotiate a stronger communications mechanism, the endpoints MUST use TLS, even if they happen to not use a Middlebox for routing.

One issue with mandating 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.

The reason CEMA mandates TLS in light of such an obvious vulnerability is three-fold.

First, one of the target deployments for CEMA is the 3GPP IMS SIP network. In this environment it is trivially easy for the service provider to provide 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.

Second, alternate key distribution mechanisms, such as **DANE** [DANE], **PGP** [RFC6091], or some other technology may become ubiquitous enough to solve the key distribution problem.

Third, experiences with IETF protocols have been that when security is put on as an afterthought or is optional, it rarely gets deployed. There is a clear path over time for creating a key distribution mechanism. Thus mandating TLS at this time removes one of the recurring excuses to not deploy secure solutions build to Internet security norms. Namely, that one cannot deploy a secure solution because legacy endpoints do not have TLS capability.

Even with seemingly end-to-end media integrity, at the time of the publication of this document there are other vulnerabilities in MSRP that mean users may not have truly end-to-end security. These issues come from vulnerabilities in the SIP signaling. If there are no integrity protections on the SIP signaling, it is trivially easy for a bad actor to surreptitiously insert evil Middleboxes to alter, record, or otherwise harm the media. With insecure signaling, it can be very 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, evil.

In light of these vulnerabilities, why does CEMA mandate the more resource-intensive TLS instead of TCP for MSRP connections, and why does CEMA claim it has more security than deploying MSRP B2BUAs?

From a processing load perspective, the burden of TLS falls entirely on the endpoints. CPU capability and battery life of even low-end mobile devices are such that this is no longer a barrier for mandating TLS. Moreover, as an added bonus, CEMA removes the requirement for Middleboxes to decode, read, rewrite, and re-encrypting MSRP media. This means that Middleboxes can have much more scale and performance with CEMA.

From a framework perspective, the ubiquitous deployment of TLS, while to totally ensuring integrity in all cases, does enable the environment for further end-to-end integrity solutions. For example, one could envision mechanisms where the endpoints create security associations in the MSRP media stream. This, coupled with future end-to-end integrity protected or assured SIP signaling, will provide for true end-to-end MSRP integrity. By mandating TLS today, we eliminate the possibility of future downgrade attacks in light of more robust solutions.

This situation is comparable to **DNSSEC** [RFC4033]. DNSSEC does not solve all DNS integrity issues, but it does create an environment that immediately solves some problems and lays the groundwork for future, more robust solutions.

TOC

6.4. Downgrade Attacks

In order to ensure interoperability, CEMA clients can chose to conenct to non-CEMA clients. Whilst CEMA clients must use TLS, the CEMA client may connect to a pre-CEMA, RFC 4975 client. Although RFC 4975 mandates the implementation of TLS, RFC 4975 does not mandate the usage of TLS. Therefore, a pre-CEMA client may chose to use only TCP. In this case, in

the name of interoperability, a CEMA client MAY use a standard RFC 4975 TCP connection.

The security implication is that an evil client or middlebox could strip the CEMA information from the negotiation. In this case, the CEMA client would believe the other end when it claims not to implement TLS. CEMA clients SHOULD attempt to validate non-TLS requests via mechanisms such as by using secured signaling chanels, unless those mechansims are truly unavailable.

---

7. IANA Considerations

TOC

7.1. IANA Registration of the SDP a=msrp-cema Attribute

TOC

This section registers a new SDP attribute, a=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: a=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 sending UA supports the CEMA
         mechanism.

Values: The attribute does not carry a value

Charset dependency: none
```

---

8. Acknowledgements

TOC

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, and Adrian Georgescu for their guidance and input in order to produce this document.

---

9. Change Log

TOC

[RFC EDITOR NOTE: Please remove this section when publishing]

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

- Changed the draft name, as was suggested by our AD and work group.
- Reorient the draft from being about saving resources at a Middlebox to being about end-to-end security.
- Clean up language use, clarify language, and clean up editorial and style issues.
- TLS is mandated for all connections.
- Describe why, even though not perfect, CEMA mandates TLS in the Security Considerations section.
- Formally defined a MSRP B2BUA.

- Took out all of the TLS B2BUA language, as that is implied by an MSRP B2BUA.
- Describe signaling attacks in the Security Considerations section.
- Provide a roadmap for future work on end-to-end security.
- Added normative reference to RFC 6072.
- Added informative references to RFC 3724, RFC 4033, RFC 5389, RFC 5766, and RFC 6091

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

- Extension name changed to Connection Establishment for Media Anchoring (CEMA).
- Middlebox defintion 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

---

10. References

TOC

10.1. Normative References

TOC

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels," BCP 14, RFC 2119, March 1997 (TXT, HTML, XML).

[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 (TXT).

[RFC4566] Handley, M., Jacobson, V., and C. Perkins, "SDP: Session Description Protocol," RFC 4566, July 2006 (TXT).

[RFC4975] Campbell, B., Mahy, R., and C. Jennings, "The Message Session Relay Protocol (MSRP)," RFC 4975, September 2007 (TXT).

[RFC4976] Jennings, C., Mahy, R., and A. Roach, "Relay Extensions for the Message Sessions Relay Protocol (MSRP)," RFC 4976, September 2007 (TXT).

[RFC6072] Jennings, C. and J. Fischl, "Certificate Management Service for the Session Initiation Protocol (SIP)," RFC 6072, February 2011 (TXT).

[RFC6135] Holmberg, C. and S. Blau, "An Alternative Connection Model for the Message Session Relay Protocol (MSRP)," RFC 6135, February 2011 (TXT).

10.2. Informative References

TOC

[RFC3724] Kempf, J., Austein, R., and 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 (**TXT**).

[RFC4033] Arends, R., Austein, R., Larson, M., Massey, D., and S. Rose, "**DNS Security Introduction and Requirements**," RFC 4033, March 2005 (**TXT**).

[RFC4916] Elwell, J., "**Connected Identity in the Session Initiation Protocol (SIP)**," RFC 4916, June 2007 (**TXT**).

[RFC5389] Rosenberg, J., Mahy, R., Matthews, P., and D. Wing, "**Session Traversal Utilities for NAT (STUN)**," RFC 5389, October 2008 (**TXT**).

[RFC5766] Mahy, R., Matthews, P., and J. Rosenberg, "**Traversal Using Relays around NAT (TURN): Relay Extensions to Session Traversal Utilities for NAT (STUN)**," RFC 5766, April 2010 (**TXT**).

[RFC6043] Mattsson, J. and T. Tian, "**MIKEY-TICKET: Ticket-Based Modes of Key Distribution in Multimedia Internet KEYing (MIKEY)**," RFC 6043, March 2011 (**TXT**).

[RFC6091] Mavrogiannopoulos, N. and D. Gillmor, "**Using OpenPGP Keys for Transport Layer Security (TLS) Authentication**," RFC 6091, February 2011 (**TXT**).

[DANE] "**DNS-based Authentication of Named Entities Work Group**."

[GPP23228] 3GPP, "**IP Multimedia Subsystem (IMS); Stage 2**," 3GPP TS 23.228 10.5.0, June 2011.

Authors' Addresses

TOC

Christer Holmberg
Ericsson
Hirsalantie 11
Jorvas 02420
Finland
Email: **christer.holmberg@ericsson.com**

Staffan Blau
Ericsson
Stockholm 12637
Sweden
Email: **staffan.blau@ericsson.com**

Eric Burger (editor)
Georgetown University
Department of Computer Science
37th and O Streets, NW
Washington, DC 20057-1232
United States of America
Phone:
Fax: +1 530 267 7447
Email: **eburger@standardstrack.com**
URI: **http://www.standardstrack.com**