Abstract

The end-to-end security properties of DTLS-SRTP depend on the authenticity of the certificate fingerprint exchanged in the signalling channel. In current approaches the authenticity is protected by SIP-Identity or SIP-Identity-Media. These types of signatures are broken if intermediaries like Session Border Controllers in other domains change specific information of the SIP header or the SIP body. The end-to-end security property between the originating and terminating domain is lost if these intermediaries...
re-sign the SIP message and create a new identity signature using their own domain credentials.

This document defines a new signature type ‘Fingerprint-Identity’ which is exchanged in the signalling channel. Fingerprint-Identity covers only those elements of a SIP message necessary to authenticate the certificate fingerprint and to secure media end-to-end. It is independent from SIP-Identity and SIP-Identity-Media and can be applied in parallel to them.

Table of Contents

1. Introduction .................................................. 3
2. Terminology .................................................. 4
3. Identity Signatures ............................................ 4
   3.1. SIP-Identity ............................................... 5
   3.2. SIP-Identity-Media ........................................ 6
4. Fingerprint-Identity .......................................... 7
   4.1. Overview ................................................ 7
   4.2. Operation ............................................... 7
   4.3. Syntax ................................................ 9
5. IANA Considerations ........................................... 10
6. Security Considerations ..................................... 10
7. Acknowledgments .............................................. 11
8. References .................................................. 11
   8.1. Normative References .................................... 11
   8.2. Informative References .................................. 12
Author’s Address ................................................. 13
Intellectual Property and Copyright Statements .......... 14
1. Introduction

DTLS-SRTP [I-D.ietf-avt-dtls-srtp] specifies a key management protocol for SRTP [RFC3711] based on DTLS. The SRTP master key is derived from a common DTLS master secret established during the DTLS handshake. In contrast to other key management protocols like MIKEY [RFC3830] or Security Descriptions [RFC4568], the keys are exchanged within the media channel and not in the signalling channel. In most scenarios the DTLS handshake is authenticated mutually by certificates. In principle it is possible that DTLS-SRTP endpoints are authenticated by certificates issued by trusted PKI providers, but typically the endpoints use self-signed certificates since the deployment and management of official signed PKI credentials is complex and expensive. Unfortunately, an endpoint cannot be authenticated by a self-signed certificate - the certificate is only a container for a public key without a trusted identity binding.

[I-D.ietf-sip-dtls-srtp-framework] addresses the problem by transferring the fingerprint of the self-signed certificate as attribute in the SDP offer/answer exchange [RFC4572] and protecting the SIP request by means of SIP-Identity [RFC4474], which provides cryptographic evidence from the user’s domain that the request (and hence the fingerprint) originate from a UA having the credentials of the user identified in the From header field. However, this approach fails in inter-domain scenarios in which a SIP message traversed multiple domains and was modified during transit. The signature is broken and needs to be renewed by the intermediate domain, e.g. a service provider domain. This renewal process necessitates changing the From header field URI to something based on the intermediate domain’s name. The receiving partner is not able to detect if the request really originated in the domain indicated by the From header field URI or elsewhere.

Another approach [I-D.ietf-wing-sip-identity-media] addresses the limitations of SIP-Identity by specifying an Identity-Media signature, which signs less information than the Identity signature. However, there are still problems with intermediate domains which modify specific information in the SIP header, e.g. the URI in the From header field. This results in a need to renew the Identity-Media signature and again a loss of the end-to-end security property of DTLS-SRTP between the originating and terminating domains.

This document defines a new signature type ‘Fingerprint-Identity’ which covers only those elements of a SIP message necessary to authenticate the certificate fingerprint and to secure media end-to-end. Modifications of the SIP message by intermediate domains do not affect the Fingerprint-Identity signature. The original identity information of the From header is kept and transferred to the
terminating domain along with the signature. This mechanism is independent from SIP-Identity and SIP-Identity-Media and can be applied in parallel to them. The focus of this document is to provide a solution for securing DTLS-SRTP end-to-end. However, since the fingerprint attribute is originally specified and used in [RFC4572], the Fingerprint-Identity mechanism is also applicable to the Comedia scenarios.

2. Terminology

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 RFC 2119 [RFC2119].

3. Identity Signatures

The following diagram shows an inter-domain scenario, in which the UA of domain A (UA-A) calls the UA of domain B (UA-B). Both domains have deployed an outgoing SBC (SBC-A and SBC-B). The call is routed over two service provider domains S1 and S2. An SBC is deployed in each service provider domain, e.g. to hide topologies between service providers. For simplicity one SBC per domain is shown only. Each of these SBCs may change information in the SDP body, such as the IP address in a c-line and the port in an m-line. Each of these SBCs may also change certain SIP header fields (e.g. Contact URI, From URI) that are signed in accordance with [RFC4474] or [I-D.ietf-wing-sip-identity-media]. The present document makes no judgment as to whether such changes to SIP requests are necessary or good practice, but simply takes account of widespread current practice in SIP deployments.

```
     Domain A   Domain S1   Domain S2   Domain B
+-----+   +-----+    +-----+    +-----+   +-----+
|UA-A|---|SBC-A|----|SBC-S1|----|SBC-S2|----|SBC-B|---|UA-B|
+-----+   +-----+    +-----+    +-----+   +-----+
```

Figure 1: Inter-domain scenario

Domain A can populate the From header using general SIP-URIs (e.g. ‘sip:alice@domaina.com’) or E.164 telephone numbers (e.g. ‘sip:+1234567890@domaina.com;user=phone’). The fingerprint of UA-A’s certificate used during the DTLS-handshake is inserted as a separate SDP attribute in the body. Two mechanisms exist to protect the authenticity of the certificate fingerprint ([RFC4474] and [I-D.ietf-wing-sip-identity-media]). The next two sub-sections describe the limitations of these approaches in providing an end-to-

Fischer                   Expires July 25, 2008                 [Page 4]
end security property between A and B. In this context end-to-end security means security between the two end domains A and B, so that neither service provide S1 nor S2 is able to intercept the call.

### 3.1. SIP-Identity

SIP-Identity generates a signature over specific SIP headers and the whole SIP body [RFC4474]. The signature is added as an Identity header field to the SIP message and the link to the associated certificate is added as an Identity-Info header. Relating to the example depicted above, the following high-level steps are executed:

- **UA-A** generates a SIP INVITE message.
- **SBC-A** modifies the private IP address of UA-A to a public one and afterwards generates a Identity signature using credentials of domain A.
- **SBC-S1** validates domain A’s Identity signature and modifies the IP addresses according to the service provider’s policy, thus invalidating the signature. **SBC-S1** can renew the Identity signature with the credentials of domain S1, but only if the From header field URI domain name matches the domain name of S1. This means either the From header field URI has to be changed or the signature cannot be renewed (in which case it either has to be removed or left as invalid). The following steps assume the signature has been renewed.
- **SBC-S2** validates domain S1’s Identity signature, modifies the IP addresses according to the service provider’s policy and needs to renew the Identity signature with the credentials of domain S2 (again assuming the From header field URI can be changed).
- **SBC-B** sends the SIP INVITE message to UA-B after successful validation of domain S2’s Identity signature.

In this example scenario the authenticity of the fingerprint is not protected end-to-end. It is only a hop-by-hop protection, since every traversed domain creates a new signature. Each traversed domain is principally able to exchange the certificate fingerprint with a fingerprint of the certificate of a media device within its own domain and thus intercept the media traffic.

Note, that a SBC may not only change the IP address in the SDP body, but may also change certain SIP header fields covered by the Identity signature like Contact URI, Call-ID or CSeq [I-D.ietf-sipping-sbc-funcs].
In order to renew a signature, an intermediate service provider domain must also change the From header field URI so that the domain part is its own domain, i.e., a domain for which it possesses a private key and certificate. An E.164 telephone number as mentioned above (‘sip:+1234567890@domaina.com;user=phone’) can be changed in a way that the domain part representing domain A is replaced by the domain of the service provider (‘sip:+1234567890@domains1.com;user=phone’). Even SIP-URIs in the From header field like ‘sip:alice@domaina.com’ can be changed by an SBC in the service provider domain. Due to possible name conflicts between different domains, a SBC cannot simply exchange the domain part, but can move the original domain part into the user-info part, e.g. ‘sip:alice%domaina.com@domains1.com’. In both cases, a change of the From header field URI breaks the Identity signature. In the case of E.164 telephone numbers the receiving domain is not even able to determine the originating domain of UA-A.

3.2. SIP-Identity-Media

SIP-Identity-Media works similar as SIP-Identity and generates a signature over specific SIP headers and parts of the SIP body [I-D.ietf-wing-sip-identity-media]. In contrast to SIP-Identity the Identity-Media signature includes less information. It omits those parts of the SIP message which are probably subject to change. All body information is omitted apart from certain SDP attributes needed for cryptographic purposes like the certificate fingerprint, so that a change of the IP address in SDP does not break the Identity-Media signature. Moreover, certain SIP header fields are omitted too, like the Contact URI, Call-ID and Cseq. The signature is added as an Identity-Media-Signature header field and the link to the associated certificate is added as an Identity-Info header field.

SIP-Identity-Media improves the mechanism of SIP-Identity, since a change of SDP information (e.g. IP addresses in the c-line) does not break the signature and still provides an end-to-end security property between the originating and terminating domains. However, this approach has an issue with the From header field URI. As mentioned above a service provider may change the domain part of an E.164 telephone number or may even change the domain part of other types of SIP-URI by manipulating the original information. A change of the From header field URI breaks the signature and necessitates a renewal by intermediaries. In the case of E.164 telephone numbers the receiving part (in the example domain B) is not able to determine the originating domain (here domain A).
4. Fingerprint-Identity

4.1. Overview

Fingerprint-Identity protects the authenticity of the certificate fingerprint SDP attribute between the originating and terminating domains. Fingerprint-Identity is a signature over specific SIP header and body elements. In contrast to the approaches described in Section 3 the Fingerprint-Identity signature covers only that information in a SIP message that is necessary for authenticating the fingerprint (and hence the source and destination of media) without introducing new security threats (refer to Section 6 for an analysis of the security properties). This information comprises:

- the SDP fingerprint attribute representing the fingerprint of the certificate used in the DTLS handshake,
- the original identity information of the From header field and
- the Date header field.

As described in Section 3 intermediaries may change the From header field URI. Therefore, the signature is not generated over the From header field URI of the SIP message, but rather a copy of the addr-spec part that is preserved between the originating and terminating domains. A change of the From header field URI does not invalidate it.

The signature is added as a new SIP header field ‘Fingerprint-Identity’ and the link to the domain certificate with which the signature was generated is inserted as new header field ‘Fingerprint-Identity-Cert’.

4.2. Operation

The operation of Fingerprint-Identity is similar to [RFC4474] and likewise uses an authentication service and a verifier. Figure 2 shows the same inter-domain example as in Section 3.

```
    Domain A         Domain S1       Domain S2       Domain B
    +-----+   +-----+    +-----+    +-----+   +-----+   +-----+
    |UA-A|--|SBC-A|--SBC-S1|--SBC-S2|--SBC-B|--UA-B|
    +-----+   +-----+    +-----+    +-----+   +-----+
                |Auth.-       |Verifier-
                |Service      |Service
```

Figure 2: Inter-domain scenario (Fingerprint-Identity)
Here, the SBC in domain A acts as authentication service and the SBC in domain B as verifier. Note, that the authentication service and verifier need not to be realized necessarily on the SBC, they can be deployed also on a SIP proxy in domain A and/or domain B.

UA-A wants to call UA-B and the call is routed through the domains of service provider S1 and S2. As in Section 3.1 each of these SBCs may change information in the SDP body like the IP address in a c-line or the port in an m-line. SBCs may also change certain SIP header fields (e.g. Contact URI, From header field URI). Following steps are performed:

Step 1:

UA-A generates a SIP INVITE message. The From header field URI expresses the identity of UA-A. The SIP request MUST contain an SDP fingerprint attribute representing the certificate used in the DTLS handshake.

Step 2:

The authentication service MUST determine whether or not the sender of the request is authorized to claim the identity given in the identity field. In order to do so, the authentication service MUST authenticate the sender of the message. After successful verification, the authentication service copies the identity information of the From header field into a new SIP header field ‘Original-Identity’. The authentication service SHOULD ensure that any preexisting Date header in the request is accurate. If no Date header is present then it MUST be added to the SIP request.

The authentication service calculates a hash over the ‘Original-Identity’ header field, the ‘Date’ header field and the fingerprint attribute in the SDP body. The fingerprint attribute can be included on session-level as well as on media-level [RFC4572]. If specified on media-level this may result in multiple fingerprint attributes. The fingerprints might be equal for each media streams if the same certificate is used or they might differ by using different certificates (e.g. the media streams are terminated on different devices). The hash calculation considers in either case all fingerprint attributes included in the SDP body. The hash is signed with domain A’s private key whereas the public key is associated with domain A in a certificate. The signature is added as new SIP header field ‘Fingerprint-Identity’ and the URI from which the domain certificate can be obtained is added as new SIP header field ‘Fingerprint-Identity-Cert’. Note, that Identity-Info is not used for this purpose, since Fingerprint-Identity is independent of SIP-Identity and SIP-Identity can be applied in parallel. Moreover an
intermediate domain can introduce or renew SIP-Identity and will thus place a different certificate in the Identity-Info header field.

Dependent on the scenario and the requirements the authentication service may also add a SIP-Identity signature to the SIP request. However, for the end-to-end security property of the certificate fingerprint this is not necessary and is omitted in this description.

Step 3:

The SIP request traverses the domain S1, in which the SDP body or SIP headers may be modified. An intermediate domain MUST NOT change the Date, Original-Identity, Fingerprint-Identity and Fingerprint-Identity-Cert header fields or the SDP fingerprint attribute.

Step 4:

Same as step 3 but for domain S2.

Step 5:

The verifier MUST verify the Fingerprint-Identity signature. If the signature does not have the domain certificate with which the signature was created, he acquires the certificate for the signing domain using information in the 'Fingerprint-Identity-Cert' header field. A hash is calculated over the information listed in step 2 and compared with the signed hash in the Fingerprint-Identity header decrypted using the public key from the certificate of the originating domain. If the hashes match, the terminating domain B can be sure that the fingerprint originates from the domain included in the Original-Identity header field.

Note, that the authentication of the certificate fingerprint in the reverse direction from domain B to A works in a similar way applying the mechanisms specified in [RFC4916]. In this case the Fingerprint-Identity mechanism apply to the UPDATE request.

4.3. Syntax

This section defines the syntax of the new header fields according to [RFC4234].
5. IANA Considerations

To be done in a later version.

6. Security Considerations

Fingerprint-Identity protects the authenticity of the certificate fingerprint between the originating and terminating domain. It binds the fingerprint to an identity information described in the Original-Identity header field (copied from the From header field) by a domain signature. The associated domain certificate is signed by a trusted PKI provider, so that the targeting domain is able to verify and trust the Fingerprint-Identity signature. The targeting domain MUST assure that the authentication service of the originating domain is authorized to create a Fingerprint-Identity signature for the identity described in the Original-Identity header field, i.e. that the domain information of the domain certificate matches the domain in the Original-Identity header field.

In contrast to SIP-Identity the Fingerprint-Identity signature is not bound to a specific SIP request, because header fields like Cseq or Call-Id are omitted from the signature. However, a binding to a specific SIP request is not necessary to guarantee the authenticity of the certificate fingerprint and therewith the end-to-end security of DTLS-SRTP. Generally, the missing binding introduces possibilities for cut-and-paste attacks, i.e. the Fingerprint-Identity signature and the associated information are cut from a SIP request and pasted in another one. The inclusion of the Date header in the calculation of the hash and signature limits this possibility to a specific window size only. As specified in [RFC4474] implementations of this specification MUST NOT deem valid a request with an outdated Date header field (the RECOMMENDED interval is that the Date header must indicate a time within 3600 seconds of the
receipt of a message). But even a cut-and-paste attack is performed within this window size, the attacker cannot benefit from it and intercept a media call. He is able to retrieve the Fingerprint-Identity signature and associated information (Fingerprint-Identity-Cert, Date and Original-Identity header fields as well as the fingerprint attribute) of a valid SIP request and insert them into another SIP request within the windows size. But since the attacker does not own the private key belonging to the certificate represented by the fingerprint, the receiving party will recognize this by comparing the certificate fingerprint got during the DTLS-handshake and the one received in the SIP request.

The authentication service is a trusted entity within the originating domain. The authenticity of the certificate fingerprint is protected after creation of the signature only, i.e. the SIP request or more specific identity information or the SDP fingerprint attribute within the SIP request can be modified on the way between the UA and the authentication service. Therefore, the authentication service MUST authenticate the UA as described in step 2 of Section 4 and the connection between both parties MUST be integrity protected, e.g. using TLS.

The Fingerprint-Identity and Fingerprint-Identity-Cert header fields are not protected themselves, i.e. an attacker is able to remove these header fields during traversal. In this case the fingerprint is not protected anymore. This may lead in a Denial-of-Service attack if it is expected that the calling and called party want to have an encrypted call end-to-end. This may lead also in a bid-down attack falling back to RTP since the DTLS-SRTP handshake cannot be authenticated.

7. Acknowledgments

The author would like to thank John Elwell for the discussions and comments in the early phase of this document.

8. References

8.1. Normative References

[I-D.ietf-avt-dtls-srtp]
[I-D.ietf-sip-dtls-srtp-framework]


8.2. Informative References

[I-D.ietf-sipping-sbc-funcs]

[I-D.ietf-wing-sip-identity-media]


Author’s Address

Kai Fischer
Siemens Enterprise Communications GmbH & Co. KG
Schertlinstr. 8
Munich, Bavaria  80200
Germany

Email: kai.fischer@siemens.com
Full Copyright Statement

Copyright (C) The IETF Trust (2008).

This document is subject to the rights, licenses and restrictions contained in BCP 78, and except as set forth therein, the authors retain all their rights.

This document and the information contained herein are provided on an "AS IS" basis and THE CONTRIBUTOR, THE ORGANIZATION HE/SHE REPRESENTS OR IS SPONSORED BY (IF ANY), THE INTERNET SOCIETY, THE IETF TRUST AND THE INTERNET ENGINEERING TASK FORCE DISCLAIM ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO ANY WARRANTY THAT THE USE OF THE INFORMATION HEREIN WILL NOT INFRINGE ANY RIGHTS OR ANY IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

Intellectual Property

The IETF takes no position regarding the validity or scope of any Intellectual Property Rights or other rights that might be claimed to pertain to the implementation or use of the technology described in this document or the extent to which any license under such rights might or might not be available; nor does it represent that it has made any independent effort to identify any such rights. Information on the procedures with respect to rights in RFC documents can be found in BCP 78 and BCP 79.

Copies of IPR disclosures made to the IETF Secretariat and any assurances of licenses to be made available, or the result of an attempt made to obtain a general license or permission for the use of such proprietary rights by implementers or users of this specification can be obtained from the IETF on-line IPR repository at http://www.ietf.org/ipr.

The IETF invites any interested party to bring to its attention any copyrights, patents or patent applications, or other proprietary rights that may cover technology that may be required to implement this standard. Please address the information to the IETF at ietf-ipr@ietf.org.

Acknowledgment

Funding for the RFC Editor function is provided by the IETF Administrative Support Activity (IASA).