

SIPPING
Internet-Draft
Expires: August 23, 2006

S. Fries
H. Tschofenig
Siemens
February 19, 2006

SIP Identity Usage in Enterprise Scenarios
draft-fries-sipping-identity-enterprise-scenario-02.txt

Status of this Memo

By submitting this Internet-Draft, each author represents that any applicable patent or other IPR claims of which he or she is aware have been or will be disclosed, and any of which he or she becomes aware will be disclosed, in accordance with [Section 6 of BCP 79](#).

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF), its areas, and its working groups. Note that other groups may also distribute working documents as Internet-Drafts.

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."

The list of current Internet-Drafts can be accessed at <http://www.ietf.org/ietf/1id-abstracts.txt>.

The list of Internet-Draft Shadow Directories can be accessed at <http://www.ietf.org/shadow.html>.

This Internet-Draft will expire on August 23, 2006.

Copyright Notice

Copyright (C) The Internet Society (2006).

Abstract

This document describes a use case for the SIP Identity document involving certificate management with the focus on enterprise environments. It provides a best current practice document for binding an identity to a certificate for the duration of a session. The certificate may then be used to bootstrap further security parameters, e.g., for securing media data. A discussion of possible enhancements is included in the appendix.

Table of Contents

- [1.](#) Introduction [3](#)
- [2.](#) Terminology [4](#)
- [3.](#) Existing Building Blocks [4](#)
- [4.](#) Scenario and Profile [5](#)
- [5.](#) Conclusion [6](#)
- [6.](#) Security Considerations [7](#)
- [7.](#) IANA Considerations [7](#)
- [8.](#) Acknowledgments [7](#)
- [9.](#) References [7](#)
 - [9.1.](#) Normative References [7](#)
 - [9.2.](#) Informative References [8](#)
- [Appendix A.](#) Alternative Approaches [8](#)
 - [A.1.](#) Associating user identity and credentials upfront [8](#)
 - [A.2.](#) Enhancements to SIP Identity using SIP SAML [9](#)
- Authors' Addresses [11](#)
- Intellectual Property and Copyright Statements [12](#)

1. Introduction

In current enterprise environments certificates are used to provide secure access to web servers, to protect server-to-server communication, and for administrative purposes. In certain scenarios, authentication of the access device as well as the user is important. In order to support such scenarios, IP-based enterprise systems may be equipped with device certificates. Several enterprise networks already have a device authorization infrastructure.

This security often is restricted to the perimeter of the corporate network, as peers outside the corporate network may not be able to verify a certificate given by a corporate CA.

For user-to-user communication, the receiving side needs to be able to validate a certificate as belonging to the sending side. A device certificate is not ideally suited to this purpose since it contains a device specific identifier. Although user certificates would seem to be a better alternative, there are certain difficulties with this at present. Users often use different devices at different times, and to facilitate this (and also prevent unauthorised use of a certificate in the absence of a user), private keys and certificates may be provided on smart cards. However, this almost rules out the simultaneous usage of this card in two devices (e.g., hard phone and PC). As a complete role out of a PKI providing server and user certificates that are globally usable is not likely in the near future (at least for user certificates), intermediate steps need to be taken.

This document discusses the usage of certificates with a limited applicability, e.g., device certificates or self-signed certificates in an enterprise environment in the context of SIP. In particular, this document focuses on the session binding of these certificates to user identities.

The scenario, which is the focus of this document, can be described as follows. Note that the applicability of the approach is not restricted to this example use case.

A user in a corporate environment has been assigned a hardware-based phone. With this phone the user may initiate and receive calls inside the corporate environment and also to/from the outside. Since the corporate policy requires certain security services to be in place, e.g., media encryption, for internal as well as external calls, the phone needs to support security parameter negotiation between the participants of a call. To achieve this negotiation securely, the phone typically needs to be equipped with an appropriate certificate. Note that since the phone may be shared by

several users, the phone may even be able to generate certificates for the user currently associated with this phone.

Using the phone, i.e., the voice service, requires the user to authenticate himself, often based on a username and a password. One reason why it is assumed that the user does not authenticate using a certificate and corresponding private key is the lack of an appropriate interface in order to accomplish the necessary certificate provision to the phone (e.g., using smart cards or secure USB tokens). Even with such an interface, the enterprise may not be able to issue globally resolvable certificates due to technical or financial reasons.

A certificate based on the phone can be used to secure the exchange of security parameters. The problem to be solved here is the binding of available certificate material to a user identity for the duration of the session concerned.

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. Existing Building Blocks

[RFC 3261](#) [[RFC3261](#)] already describes the transport of certificates within the SDP body of a message using the S/MIME Key Exchange approach described in [Section 23.2 of \[RFC3261\]](#). Here, a user may submit a self-signed certificate. It is even allowed that the subjectname field be different from the AoR submitted in the From header field. The drawback is that the receiver may not be able to verify the validity of the embedded key and associate it with a particular user identity.

[I-D.ietf-sip-identity] introduces a new entity, called the authentication service, which provides assurance about the identity in the From header field of a SIP request (such as an INVITE request). The authentication service does this by adding an assertion to the SIP header in a SIP request. This assertion provides integrity protection for certain header fields and also for the body of the SIP request. The assertion is added after authenticating (and authorizing) the request initiator, e.g., by HTTP digest authentication.

4. Scenario and Profile

Subsequently, a profile is described for a BCP providing an implicit binding of a user identity to the available certificate for the duration of a session. The profile ensures interoperability of different vendor's products regarding the described scenario. The profile does not define any new messages or parameters. It rather takes existing options from [RFC 3261](#) and appropriate SIP extensions to achieve the binding.

Devices may already possess certificates or may generate self-signed certificates on logon of a new user or on request. A UA may want to bind these credentials to the identity of the registering user for the duration of the registration or just for the duration of a session. When the UA issues a SIP request, the outbound proxy / registrar will authenticate the UA as having the credentials associated with the user identified in the From header field. For example, the UA may be challenged to provide HTTP digest authentication. Alternatively, if the request is received over a TLS connection on which the UA has been authenticated previously, then further authentication may not be necessary. Having authenticated the UA, any certificate conveyed in that request can be implicitly associated with that UA and hence with the authenticated user, provided the request has been integrity protected (e.g., through the use of TLS). An authentication service, as defined in [I-D.ietf-sip-identity], can then verify that the URI in the From header field corresponds to an AoR that the authenticated user is allowed to use, and on this basis can provide an assertion in the forwarded request that the From header field URI does indeed identify the origin of the request. This assertion is in the form of an inserted Identity header field in the INVITE message. This provides a signature over some of the header fields in the forwarded request and over the entire body, using the domain's private key. Thus, if a certificate is included in a body, it will be integrity protected and any recipient of the request can be sure that the certificate originated at a device having the credentials of the user identified in the From header field, provided the signature can be verified and validated. This can be facilitated if the authentication service uses a certificate signed by a well know CA.

An extension, allowing the authentication service to add a fingerprint of a certificate used during the user authentication is described in [Appendix A](#) of this document. The signature of the authentication service enables the receiving UAC to verify that the body and thus the certificate has not been tampered with while in transit from the authentication server to the recipient, and that it was provided by a particular entity stated in the FROM field (as indicated in the assertion). The message integrity together with the

assertion create a temporary binding (identity, certificate) at the receiver side.

This is important, as the receiving client may not be able to verify the certificate provided by the initiator of the communication (for example, because it was created by an enterprise CA and the root certificate of the issuing CA cannot be validated). In-band certificate provision may be done as described in [RFC 3261](#) [[RFC3261](#)] for self-signed certificates or by using the recently proposed new MIKEY option [[I-D.ietf-msec-mikey-rsa-r](#)] for key management, allowing the certificate transport as part of a MIKEY message, which in turn can be transmitted in SIP using the [[I-D.ietf-mmusic-kmgmt-ext](#)] approach.

After verifying the signature, the receiving client can store the certificate associated with the identity stated in the FROM header field for the duration of the session. After the session ends the receiving UA SHOULD delete the association.

In any case, using the approach described in [[I-D.ietf-sip-identity](#)], the authentication service, through the signature over the body, implicitly asserts that the identity in the FROM field is somehow connected to a certificate in the body.

Note that the authentication service may not be held responsible for attacks on the path between the UAC and the authentication server via the SIP proxy. As this approach is provided in-band it only requires an [[I-D.ietf-sip-identity](#)] compliant authentication service to be in place as additional component.

5. Conclusion

In this document we propose to use the scenario and profile described above to enable in-band certificate exchange and association with an identity in the FROM header field as a best current practice use case for [[I-D.ietf-sip-identity](#)]. It would require a UACs to store an association of identity and certificate for the duration of a session. This is done in order for the receiver to ensure that during the entire session the same certificate/private key is used for cryptographic purposes with the calling UA. This creates a temporary binding (identity, certificate) at the receiver side. Alternative approaches are described in [Appendix A](#). These alternatives, however, suffer from some limitations or require protocol extensions.

6. Security Considerations

To avoid the use of a dedicated certificate and private key pair from several users, the device needs to ensure that a fresh key pair is generated upon user login. The lifetime of the certificate may be rather short. A new certificate may be generated during the period of registration if a certificate expires.

If a certificate is compromised, it needs to be revoked and a new certificate has to be issued to the device. Following the approach in [[I-D.ietf-sipping-certs](#)] a notification with an empty body is sent to indicate that the certificate is no longer valid.

Response identity, e.g., for the mutual exchange of certificates, cannot be achieved using the approach described in [[I-D.ietf-sip-identity](#)]. Here, a the recently submitted ID handling connected SIP identity [[I-D.elwell-sip-connected-identity](#)] may provide a solution. This ID describes an approach for targeting the authenticated connected identity provisioning using [[I-D.ietf-sip-identity](#)].

7. IANA Considerations

This document does not require actions by IANA.

8. Acknowledgments

The authors would like to thank Jon Peterson and Cullen Jennings as well as John Elwell and Francois Audet for the discussions in context of SIP identity. Additionally, we would like to thank Andreas Pashalidis for his comments.

9. References

9.1. Normative References

[[I-D.elwell-sip-connected-identity](#)]
Elwell, J., "Connected Identity in the Session Initiation Protocol (SIP)", [draft-elwell-sip-connected-identity-00](#) (work in progress), October 2005.

[[I-D.ietf-sip-identity](#)]
Peterson, J. and C. Jennings, "Enhancements for Authenticated Identity Management in the Session Initiation Protocol (SIP)", [draft-ietf-sip-identity-06](#) (work in progress), October 2005.

- [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.

[9.2. Informative References](#)

- [I-D.ietf-mmusic-kmgmt-ext]
Arkko, J., "Key Management Extensions for Session Description Protocol (SDP) and Real Time Streaming Protocol (RTSP)", [draft-ietf-mmusic-kmgmt-ext-15](#) (work in progress), June 2005.
- [I-D.ietf-msec-mikey-rsa-r]
Ignjatic, D., "An additional mode of key distribution in MIKEY: MIKEY-RSA-R", [draft-ietf-msec-mikey-rsa-r-02](#) (work in progress), February 2006.
- [I-D.ietf-sipping-certs]
Jennings, C. and J. Peterson, "Certificate Management Service for The Session Initiation Protocol (SIP)", [draft-ietf-sipping-certs-02](#) (work in progress), July 2005.
- [I-D.tschofenig-sip-saml]
Tschofenig, H., "Using SAML for SIP", [draft-tschofenig-sip-saml-04](#) (work in progress), July 2005.
- [RFC3830] Arkko, J., Carrara, E., Lindholm, F., Naslund, M., and K. Norrman, "MIKEY: Multimedia Internet KEYing", [RFC 3830](#), August 2004.

[Appendix A. Alternative Approaches](#)

[A.1. Associating user identity and credentials upfront](#)

SIPPING-CERTS [[I-D.ietf-sipping-certs](#)] and SIP Identity [I-D.ietf-sip-identity] are two promising approaches that help to deal with the problem that deployment of end user certificates and a global PK infrastructure is not available.

[I-D.ietf-sipping-certs] is suitable for an enterprise environment to provide certificate information to the end hosts and end users via a credential server. UAs can fetch certificates and use them as

necessary. UAs may also store their own credentials on the credential server. This may be done also (only) for the duration of a registration, which enables other UAs to fetch the certificate upfront, before starting communication with the target UA. This approach requires that both parties have sufficient access to a credential server. Besides the credential server, also an authentication server may be needed to support certain scenarios.

This approach works nicely in many environments but there may be limitations is others

In order to use the credential server in a way in which certificates are globally accessible it is necessary to put the credential server on the public Internet. This is in order to enable persons from outside to access the certificate information before making or answering a call. This approach may not be feasible for all enterprises, as there are certain company based regulations regarding the safeguarding of employee information. A corporate directory for instance is normally not accessible by people outside the enterprise.

The combination of both concepts, namely SIP Identity and SIPPING-CERTS, provides the possibility to route a NOTIFY, which contains a certificate from the credential server, via the authentication service to the UA. As stated in [[I-D.ietf-sipping-certs](#)], if the identity asserted by the authentication service matches the AOR that the UA subscribed to, the certificate in the NOTIFY can be treated as valid and may be used for the protection of subsequent communication. A general precondition is that the UA and the authentication server trust the same root CA.

This latter approach requires the certificate SubjectAltName to match a given AoR, as described in [Section 8.10](#) of [[I-D.ietf-sipping-certs](#)], thus leaving certain device certificates or certain self-signed certificates outside the possible solution.

[A.2.](#) Enhancements to SIP Identity using SIP SAML

As required by [[I-D.ietf-sip-identity](#)], the authentication server has to authenticate the user whose identity appears in the FROM field of the SIP request by some means, e.g., by challenging the user.

Additionally, an authentication server may also check and assert, that a dedicated certificate was used during registration over a TLS protected link for the authentication on the TLS level. This approach is currently not be possible with [[I-D.ietf-sip-identity](#)] and would require further specification.

A document supporting this approach is provided in SIP-SAML [[I-D.tschofenig-sip-saml](#)], which enables SAML assertions and artifacts to be carried in SIP. This document offers a mechanism to deliver additional information about previously executed authentication.

Authors' Addresses

Steffen Fries
Siemens
Otto-Hahn-Ring 6
Munich, Bavaria 81739
Germany

Email: steffen.fries@siemens.com

Hannes Tschofenig
Siemens
Otto-Hahn-Ring 6
Munich, Bavaria 81739
Germany

Email: Hannes.Tschofenig@siemens.com

Intellectual Property Statement

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.

Disclaimer of Validity

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 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.

Copyright Statement

Copyright (C) The Internet Society (2006). 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.

Acknowledgment

Funding for the RFC Editor function is currently provided by the Internet Society.

