SIPPING
Internet-Draft
Expires: April 16, 2006

S. Fries
H. Tschofenig
Siemens

October 13, 2005

SIP Identity Usage in Enterprise Scenarios
draft-fries-sipping-identity-enterprise-scenario-01.txt

Abstract

This document describes a scenario for the SIP identity work involving certificate management in enterprise environments. A discussion of possible solutions is included.

Table of Contents

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 infrastructure is based on device and software properties and characteristics.

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.

2. Scenario Overview

The scenario, which is the focus of this discussion, can be described as follows.

- o A user is connected to the corporate LAN with his destop PC or laptop and may possess a user certificate for certain applications.
- o Additionally, the user has been assigned a hardware-based phone. The hardware-based phone is equipped with an appropriate device certificate in order to enable secure communication and maintainance.
- o Using the phone requires the user to authenticate himself based on a username and a password for VoIP service access, instead of a user certificate. The reason why it is assumed that the user cannot authenticate himself based on a certificate is the lack of appropriate interfaces in order to accomplish the necessary certificate provision to the phone (e.g. using smart cards or

secure USB tokens). Additionally, as the user might not have complete control over the phone, and as the phone may be shared among multiple user, it is not desireable to expose private keys to the phone.

3. Problem Description

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 approach works nicely in many environments but suffers from the following limitations.

- Users may not want to download their credentials to end hosts over which they do not have administrative control. This restricts the applicability of the approach of storing credentials in an enterprise environment where IP-based phones might not be associated with a single person.
- 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 apporach may not be feasible for all enterprises, as there are certain regulations regarding the safeguarding of employee information. Usually the corporate directory is not accessible by people outside the enterprise.

[I-D.ietf-sip-identity] introduces a new entity, called the authentication server, which provides assurance about the identity in the FROM field of a SIP request (such as an INVITE). The authentication service adds an assertion to the SIP header field in a SIP request. This assertion also provides integrity protection for certain header fields and the body of the SIP request. This

assertion is added after authenticatiing and authorizing the signaling session initiator.

The combination of both concepts, namely SIP Identity and SIPPING-CERTS, provides the possiblity 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 precondition is that the UA and the authentication server trust the same root CA.

This latter approach would not work when a UA uses device certificates, as the receiving UA would not be able to match the AOR value, which must be checked according to Section 10.6 of [I-D.ietf-sipping-certs]. The approach of using device certificates could serve as an option to provide security services during the session. Devices certificates may not be used for user authentication.

Users might not want to provide certicates and corresponding private keys to a hardware based phone using SIPPING-CERT [I-D.ietf-sipping-certs]. Even if the credentials are ephemeral it may not be desirable to store them at a device that is not under the control of the user. Severely limiting the lifetime of the credentials (e.g., just for the duration of the session) is often not an option since the user may not know in advance how long the credentials are needed (i.e., how long a session may last).

4. Solution Approaches

4.1. Associating user identity and device credentials for session duration

As devices may already possess device certificates, a UA may want to bind these credentials to the identity of the registering user for the duration of the registration. During the registration, the registrar may authenticate the device in addition to the user. The registrar is therefore able to associate the user authentication (e.g. using SIP digest authentication) with the certificate-based device authentication which has beed performed as part of the TLS

handshake. If the authentication server and the registrar are co-located then the authentication server has access to the credentials that were used during authentication. The authentication server may then be in a position to assert the identity used in the FROM header. SIP Identity [I-D.ietf-sip-identity] can fulfill this task.

Furthermore, if certificates are carried inside the SIP/SDP payload (as part of the end-to-end communication) then the assertion added by the authentication service can also cover it. The signature of the authentication service would enable the receiving UAC to verify that the body and thus the certificate has not been tampered with while in transit, and that it was provided by a particular entity (as indicated in the assertion).

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 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.

In any case, using the approach decribed 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. According to [I-D.ietf-sip-identity] the authentication service is responsible to make sure that the user is allowed to use the stated identity in the FROM field within the domain of the server's authority.

4.2. Associating user identity and device credentials upfront

Another approach would be that the UA uploads the credentials to the credential server also for the duration of the registration, which enables other UAs to fetch the certificate upfront, before starting communication with the target UA. This approach is supported by the usage of [I-D.ietf-sipping-certs]. A limitation, which has been stated in the Overview section above is that it might not be suitable for external parties as they may not be allowed to obtain the

appropriate certificates from a corporate server.

4.3. Potential enhancements to SIP Identity

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, the 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 would not be possible with the current [I-D.ietf-sip-identity] draft and would require further specification. SIP-SAML [I-D.tschofenig-sip-saml] enables SAML assertions and artifacts to be carried in SIP. This draft offers a mechanism to deliver additional information about previously executed authentication.

5. Conclusion

In this draft we propose to use the scenario described in section 4.1 above, and thereby enables in-band certificate exchange, as a best current practice use case for [I-D.ietf-sip-identity] in enterprise environments. It would require a UACs to store an association of FROM field 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. This creates a binding (identity, device-based certificate) at the receiver side. The approach of Section 4.3 may enhance this solution but requires further specification.

6. Security Considerations

Storing device certificates on a credential server may lead to additional effort for certificate revocation, as the device certificate may be compromised during a session with user A and should therefore not be used in a later communication session with user B. Usually, the binding of a device certificate to an identity would be valid only for the duration of the registration, i.e. a UAC

would provide the certificate related to the user's AoR to the certificate server upon registration with the SIP registrar. In order to prevent impersonation attacks, after de-registration the certificate should be withdrawn from the certificate server.

If a device certificate is compromised, systems management is responsible to revoke it and issue a new certificate to that device. Following the approach of [I-D.ietf-sipping-certs] the notifier sends a notification with an empty body to indicate that the device 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].

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.ietf-sip-identity]
Peterson, J. and C. Jennings, "Enhancements for Authenticated Identity Management in the Session Initiation Protocol (SIP)", draft-ietf-sip-identity-05 (work in progress), May 2005.

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-00 (work in progress), July 2005.

[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.

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

Disclaimer of Validity

Copyright Statement

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.