SIP
Internet-Draft
Intended status: Best Current Practice
Expires: June 13, 2007

S. Fries
Siemens AG
H. Tschofenig
Siemens Networks GmbH & Co KG
K. Fischer
Siemens Enterprise Communications GmbH & Co KG

December 10, 2006

SIP Identity Usage BCP
draft-fries-sip-identity-usage-bcp-01.txt

Status of this Memo

Copyright Notice

Abstract

This document describes a use case for RFC4474 (SIP Identity) for verifying a certificate that might not be publicly verifiable by traditional means. 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. Editors Note: The first version of this draft was discussed in the SIPPING WG. As the target of this draft is a BCP for current issues, the draft was updated and submitted to the SIP WG.

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 systems may be equipped with device certificates. Several enterprise networks already have a device authorization infrastructure, enforcing, that only dedicated devices have access to corporate resources. There can be benefits in re-using such device certificates in the context of SIP, e.g., for securing media.

The security provided by device certificates is 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. This also applies to non-corporate environments.

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 unauthorized use of a certificate in the absence of a user), private keys and certificates need to be provided to these devices. The dynamic provisioning of this can be facilitated using smart cards. However, this almost rules out the simultaneous usage of this card in two devices (e.g., hard phone and PC). Moreover, 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 limited applicability, e.g., device certificates or self-signed certificates 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 appropriate credentials. If in a targeted corporate environment device certificates are used, they may be reused here as well. Even a self-signed certificate could be used. The important thing is to be able to bind a certificate (e.g., device-based or self-signed) to the identity of the user of the device. Note that since the phone may be shared by several users, the phone may even be able to generate self-signed certificates for each user.

Using the phone, i.e., the voice service, requires the user to authenticate himself, most 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). Another appraoch is a central credential server that distributes the credentials as described in Appendix A.1. Even with such an interface, the enterprise may not be able to issue globally resolvable certificates due to technical or financial reasons. So again, a means to bind the certificate to the identity of the user would be beneficial.

A certificate available on an IP based 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.

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. This may be the case when the certificate is a device based certificate, i.e., reflecting the device identity and not necessarily the identity of the acting user. Another example is self-signed certificates, which may not be directly connectable to the user.

[RFC4474] 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 of 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

This document describes a procedure for providing an implicit binding of a user identity to a certificate available in the body of a request for the duration of a session. or parameters are defined. Instead, the procedure uses existing options from RFC 3261 and RFC 4474 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.

In the following subsections the forward and also the reverse direction for message exchange is considered. Note that forward denotes the direction from the caller to the callee, while reverse relates to the opposite direction. In both directions the recently published RFC4474 [RFC4474], describing a SIP Authentication Service, is applied for request messages.

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 [RFC4474] compliant authentication service to be in place as additional component.

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.

4.1. Forward Credential Processing

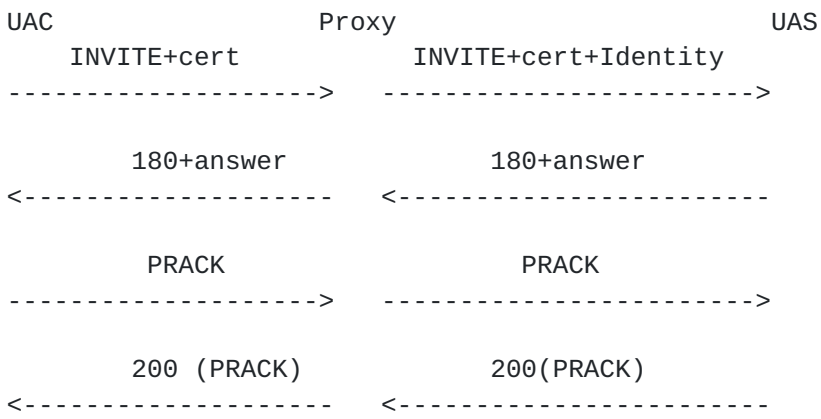
When the UA issues a SIP request, the outbound proxy / registrar will authenticate the UA as having the credentials associated with the user identified in the FROM header field. For example, the UA may be challenged to provide HTTP digest authentication. Alternatively, if the request is received over 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 [RFC4474], 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 request (e.g., INVITE) message, providing a signature over some of the header fields in the forwarded request and over the entire body, using the domain's private key. 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 can be facilitated as the authentication service uses a certificate signed by a well know CA and thus can be verified.

This is important, as the receiving client may not be able to verify the certificate provided by the initiator of the communication (for example, it is a self-signed certificate or the certificate was created by a corporate 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 [RFC4567] approach.

After verifying the signature, the receiving client stores 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.

Certificate (credential) provisioning using the SIP Identity approach may be achieved as shown in the following figure.



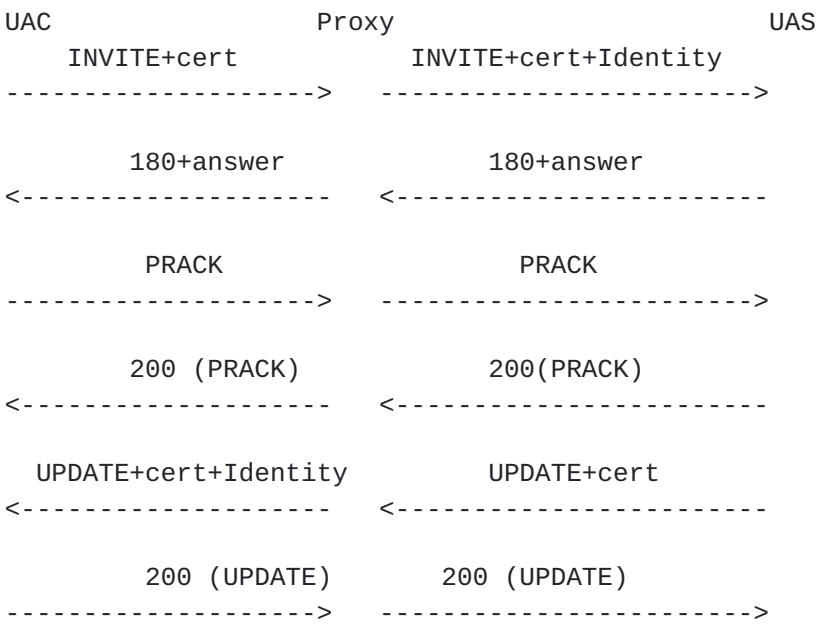
In any case, using the approach described in [RFC4474], the authentication service, through the signature over the body,

implicitly asserts that the identity in the FROM field is somehow connected to a certificate in the body.

4.2. Reverse Credential Processing

Response identity, e.g., for the mutual exchange of certificates, cannot be achieved using the approach described in [RFC4474]. Here, a the recently submitted ID handling connected SIP identity [I-D.ietf-sip-connected-identity] provides a solution. This ID describes an approach for targeting the authenticated connected identity provisioning using [RFC4474]. This approach can be leveraged to provide the credentials of the callee to the caller in a similar way as described in Section 4.1.

Certificate (credential) provisioning using the connected identity approach may be achieved as shown in the following figure.



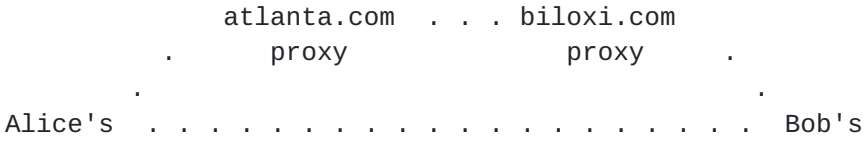
The offer is sent in the INVITE request and the answer is sent in a reliable response. However, the response, which may transport a certificate, cannot be signed with an Identity header field according to [RFC4474]. Consequently, the certificate has to be provided using a request in the reverse direction, in the figure above an UPDATE request, which is sent via the authentication service. Here, as in the forward direction, certain header fields and the body of the message of the request will be signed. The signature is provided using the Identity header field, which can then be used on the caller side as the credential to be used for the callee.

For the steps how the received credential is handled, we refer to

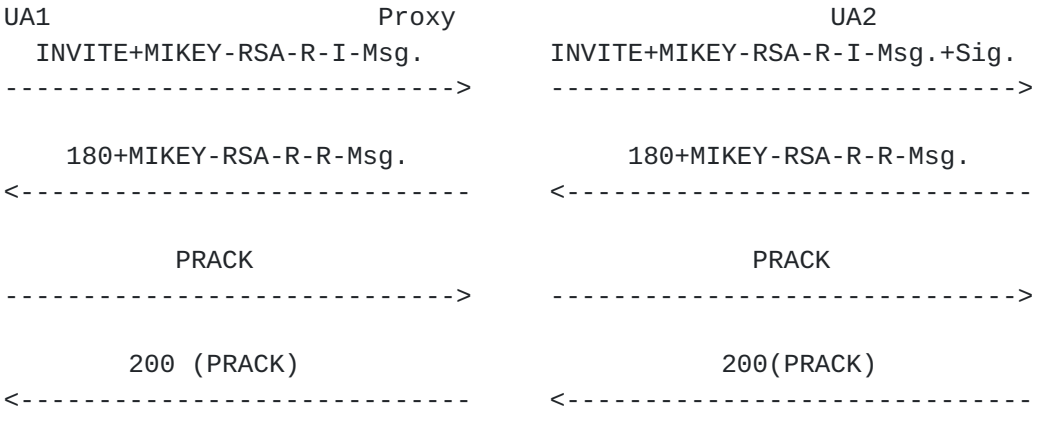
Section 4.1.

4.3. Usage Example

In the following an example is given to depict the usage of this BCP in a common scenario. Let's assume we have the standard SIP trapezoid as scenario were SIP UA Alice is connected to the SIP Proxy located in domain example.com. Alice want's to call Bob residing in the (different administrative) domain biloxli.com as shown below.



Alice and Bob both support the MIKEY-RSA-R approach (ref. [I-D.ietf-msec-mikey-rsa-r]) for setting up keys for securing the media exchange. Here, the sender and receiver do not need to know the certificate of the other peer in advance as it can be sent in the MIKEY initiator message. Thus, the receiver of this message can utilize the received key material to encrypt the session parameter and send them back as part of the MIKEY response message. The certificate check of the embedded certificate may be done depending on the signing authority. The call flow can be described as following:



For the sake of simplicity only the successful forward case is shown here. Upon receiving the INVITE message, UA2 checks the Identity Info header and verifies the signature according to [RFC4474]. After successful verification UA2 stores the certificate, which is part of the MIKEY _RSA_R Initiator message with the identity stated in the FROM header field. This certificate is used in the response to the request to secure the MIKEY-RSA-R answer. UA2 stores the certificate for the duration of the session. Besides use for securing the inital MIKEY exchange, the certificate may be used to secure further

security messages, like re-keying or similar. Note, that the usage of MIKEY is stated here only as an example. The BCP is not bound to MIKEY but is applicable to any kind of certificate transmission.

5. Conclusion

In this document we present a procedure for in-band certificate exchange and association with an identity in the FROM header field as a best current practice use case for [RFC4474]. It would require a callee UA 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 callee side. Similarly a request may be sent in the reverse direction via an authentication service containing the certificate of the callee, creating a temporary binding at the caller 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. Here it is assumed that the device does not provide an appropriate interface for the credential provisioning. 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-sip-certs] a notification with an empty body may be sent to indicate that the certificate is no longer valid. Alternatively out-of-band mechanisms can be used. If certificate revocation is necessary may depend on the lifetime of the certificates.

If signaling security in terms of TLS is not provided on the path to the authentication proxy, an adversary may copy and paste the credential material included in the original request message into another request, which may lead to wrong bindings at the receiver side. Note, that the adversary does not have the corresponding private key, thus is not able to establish a security association with the receiver.

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 Francois Audet for the discussions in context of SIP identity. Especially the authors would also like to thank John Elwell for the discussion in the context of connected identity. Additionally, we would like to thank Andreas Pashalidis for his comments.

9. References

9.1. 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.

[RFC4474] Peterson, J. and C. Jennings, "Enhancements for Authenticated Identity Management in the Session Initiation Protocol (SIP)", RFC 4474, August 2006.

9.2. Informative References

[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-07 (work in progress), August 2006.

[I-D.ietf-sip-certs] Jennings, C., "Certificate Management Service for The Session Initiation Protocol (SIP)", draft-ietf-sip-certs-02 (work in progress), October 2006.

[I-D.ietf-sip-connected-identity] Elwell, J., "Connected Identity in the Session Initiation Protocol (SIP)", draft-ietf-sip-connected-identity-02 (work in progress), October 2006.

[I-D.ietf-sip-saml] Tschofenig, H., "SIP SAML Profile and Binding", draft-ietf-sip-saml-01 (work in progress), October 2006.

[RFC3830] Arkko, J., Carrara, E., Lindholm, F., Naslund, M., and K. Norrman, "MIKEY: Multimedia Internet KEYing", RFC 3830, August 2004.

[RFC4567] Arkko, J., Lindholm, F., Naslund, M., Norrman, K., and E. Carrara, "Key Management Extensions for Session Description Protocol (SDP) and Real Time Streaming Protocol (RTSP)", RFC 4567, July 2006.

Appendix A. Alternative Approaches

A.1. Associating user identity and credentials upfront

SIP-CERTS [I-D.ietf-sip-certs] and SIP Identity [RFC4474] 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-sip-certs] is suitable 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 in 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 users 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 SIP-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-sip-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-sip-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 [RFC4474], 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 [RFC4474] and would require further specification.

A document supporting this approach is provided in SIP-SAML [I-D.ietf-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 towards a registrar .

Authors' Addresses

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

Email: steffen.fries@siemens.com

Hannes Tschofenig
Siemens Networks GmbH & Co KG
Otto-Hahn-Ring 6
Munich, Bavaria 81739
Germany

Email: Hannes.Tschofenig@siemens.com

Kai Fischer
Siemens Enterprise Communications GmbH & Co KG
Otto-Hahn-Ring 6
Munich, Bavaria 81739
Germany

Email: Kai.Fischer@siemens.com

Full Copyright Statement

Intellectual Property

Acknowledgment

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