Network Working Group
Internet-Draft
Intended status: Experimental
Expires: December 22, 2007

A. Friedman
Technion IIT
Y. Sheffer
Check Point
A. Shaqed
Correlix, Inc.
June 20, 2007

Short-Term Certificates
draft-friedman-ike-short-term-certs-02

Status of this Memo

This Internet-Draft will expire on December 22, 2007.

Copyright Notice

Abstract

This document describes an extension to IKEv2 that allows an endpoint which has authenticated to a gateway to request a short-term credential, possession of which proves the authentication. This allows it to prove to a security gateway that it was already authenticated by another trusted security gateway, thereby allowing

the authentication of the endpoint without user intervention. This credential is a certificate issued by the authenticating gateway for a short period of time, which can be used to authenticate the user with IKE signature based authentication.

Requirements Language

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].

Table of Contents

1. Introduction

Many organizations manage one or more security gateways that provide IPsec [RFC4301] services, to allow secured connectivity between roaming endpoints and the organizational site, as well as between the organizational sites themselves. In most cases, an endpoint needs to connect to only one security gateway to gain access to internal resources. However, several situations may require an endpoint to connect to additional security gateways of the same organization. For example, this may happen when the organization manages multiple entry points to the internal network for failover, or when the endpoint needs to connect to hosts lying behind multiple security gateways.

Connection to each of the security gateways requires mutual authentication between the endpoint and the security gateway. The IKEv2 Protocol [RFC4306] allows the use of legacy authentication systems along with authentications that use public key signatures and shared secrets. Legacy strong authentication systems typically require active participation of the user operating the endpoint. For example, methods using a token may require the user to enter a passcode appearing on the token. IKE authentication methods may require such an intervention as well, e.g., entering a password to get access to a certificate file. Even if the endpoint was previously authenticated by one security gateway, any connection to an additional security gateway will require additional authentication.

This document describes an extension to IKEv2 that allows an endpoint to perform an IKE exchange to request a "short term certificate". This short term certificate can be used in subsequent IKE authentications to prove to a security gateway that the endpoint was already authenticated by another trusted security gateway, thereby allowing the authentication of the endpoint without user intervention. The basic idea is to allow a security gateway to vouch for the authenticity of an endpoint, thereby saving the need for user

involvement in the recurring authentication.

The protocol presented here is similar in concept to the one suggested in the now expired draft of the Pre-IKE Credential Provisioning Protocol [PIC]. PIC was proposed as a form of using legacy authentication methods to enable certificate enrollment for use in IKE. While PIC is performed outside of IKE, the protocol we propose is an extension to IKEv2 used by an entity already authenticated in a former IKEV2 exchange.

A work in progress [I-D.ohba-preauth-ps] focuses on pre-authentication in the context of EAP [RFC3748], and is mainly driven

by the need to provide seamless and fast inter-technology handovers for mobile devices. In contrast, short-term certificates do not assume a common EAP server behind the gateways, and do not require gateways to communicate with each other.

2. Preliminaries

The methods described in this document depend on trust between security gateways. A security gateway should be able to verify that a certificate presented by an endpoint was indeed issued by another trusted security gateway, and to establish the integrity of the presented certificate. The way this trust is established and maintained (e.g., PKI [RFC3280]) lies outside the scope of this document.

3. Short-Term Certificate Usage

The use of Short-Term Certificates takes the following form:

1. At any time following a successful mutual authentication and the establishment of an IKE SA, an endpoint MAY send a request for a Short Term Certificate.

2. Subject to security gateway configuration and policy, the gateway issues a Short Term Certificate and sends it back to the endpoint. The lifetime of the Short Term Certificate will typically be the timeout until re-authentication is required.

According to the IKEv2 specification, a gateway that does not support this type of request will send an empty CFG_REPLY or a response with no CFG_REPLY at all.

3. During the validity period of the certificate, the endpoint MAY use the certificate for signature-based authentication with any security gateway that trusts the issuer of the certificate, instead of using any default authentication method. Note that any security gateway that conforms to IKEv2 specification can authenticate this certificate, whether or not it conforms to the Short Term Credentials specification.

The following sections describe the message exchange required for issuing a Short-Term Certificate, how the certificate is used and how expiration of a certificate should be handled.

4. Short-Term Certificates Issue Exchange

At any point after the security gateway authenticated the endpoint and the IKE SA was established, the endpoint MAY initiate a Short Term Certificate request and send it to the security gateway. A Short Term Certificate may also be requested from a security gateway which did not authenticate the endpoint directly, but authenticated it based on another Short Term Certificate (i.e., authentication with Short Term Certificates is transitive).

A Short Term Certificate Request is sent as a Configuration Payload of type CFG_REQUEST in an INFORMATIONAL exchange. The reply is sent as a Configuration Payload of type CFG_REPLY in an INFORMATIONAL exchange. The following attribute types have been defined for the Short Term Certificate issue exchange:

Attribute Type	Value	Request Length	Response Length
STC_CERTIFICATE_TYPE	TBD+0	1 octet	1 octet
STC_ROOT_CA	TBD+1	0 or more	--
STC_CERTREQ	TBD+2	0 or more	--

STC_CHAIN	TBD+3	1 octet	--
STC_CERTIFICATE	TBD+4	--	0 or more
STC_LIFETIME	TBD+5	--	4 octets

- STC_CERTIFICATE_TYPE - An encoding of a certificate type which indicates the type of certificate provided in the STC_CERTIFICATE attribute, according to the Certificate Encoding values provided for the Certificate Payload in Sec. 3.6 of IKEv2 [RFC4306] . In a request message, this field defines the encodings of all requested attributes. In a reply message, this value MUST be identical to the one appearing in the request, and MUST determine the encodings of all included attributes. For interoperability, all implementations MUST support type 1, "PKCS #7 wrapped X.509 certificate" [RFC2315].

- STC_ROOT_CA - MUST NOT be sent in a reply. An encoding identifying the Certificate Authority on whose trust chain a signature is requested. If STC_CERTIFICATE_TYPE is type 1, this field MUST contain the Binary Distinguished Encoding Rules (DER) encoding of an ASN.1 X.500 Distinguished Name [ITU.X501.1993] that identifies a Certificate Authority. In a request message, one trusted Certificate Authority MAY be provided.

- STC_CERTREQ - MUST NOT be sent in a reply. An encoding of a certification request, including the requesting endpoint identity,

a public key to be associated with this identity, and a proof of possession of the matching private key. If STC_CERTIFICATE_TYPE is type 1, this field MUST contain a PKCS #10 [RFC2986] encoded certification request.

- STC_CHAIN - MUST NOT be sent in a reply. A flag used to denote whether a single certificate is required (NO_CHAIN=0) or a full certificate chain (FULL_CHAIN=1). If the client already possesses the certificates required to construct a certificate chain, it may set this variable to NO_CHAIN (0) in the request message to save bandwidth. This flag is a hint: the responder MAY reply with a full chain even if no chain was requested, and vice versa.

- STC_CERTIFICATE - MUST NOT be sent in a request. Whenever the request is accepted and a short term certificate is issued, the

responder MUST set this attribute with an encoding of the issued certificate according to the type that appeared in the request message, and set the STC_LIFETIME attribute in accordance with the certificate contents. If STC_CERTIFICATE_TYPE is type 1, this field MUST contain a PKCS #7 encoding of the issued certificate.

- STC_LIFETIME - MUST NOT be sent in a request. In the reply message, this attribute contains the remaining lifetime of the Short Term Certificate, in seconds. This value can be used by the endpoint to keep track of the Short Term Certificate expiration time, so a new certificate can be requested and the old certificate deleted by expiration. This attribute is required since the client cannot rely on the notBefore and notAfter fields supplied in the certificate: there is no guarantee that the endpoint's clock is synchronized with the security gateway's clock. In addition, the notBefore field may be set several minutes prior to certificate creation time (to compensate for minor clock deviation between security gateways).

The endpoint MAY use a fixed private/public key pair for all Short Term Credential exchanges, or create a different key pair for each Short Term Certificate in use. Security considerations (see the Security Considerations section (Section 8)) may apply in case a fixed private/public key pair is used for more than one Short Term Credential exchange.

In case a security gateway receives a malformed Short Term Certificate request, it MUST send a notification payload of type INVALID_SYNTAX in the response message. If the Short Term Certificate request is rejected for any other reason (e.g., gateway configuration or security policy), the gateway MUST send a notification payload of type STC_UNSUPPORTED in the response message to inform that the request was rejected. In both cases, the

CFG_REPLY payload MUST either be sent empty or dropped altogether from the response.

When a security gateway issues a Short Term Certificate, the following restrictions apply:

- The Short Term Certificate MUST be a legal IKEv2 certificate, per IKEv2 [RFC4306] and PKI4IPsec

[I-D.ietf-pki4ipsec-ikecert-profile].

- It is RECOMMENDED that the private/public keys used by the security gateway to issue Short Term Certificates will be different from those used for authenticating the security gateway.

- The gateway MUST check that the identity appearing in the received certification request matches the identity of the endpoint associated with the IKE SA used to perform the exchange (similarly to the specification in PKI4IPsec [I-D.ietf-pki4ipsec-ikecert-profile]). In case of a mismatch, the gateway MUST reject the request. In other words, a gateway MUST NOT issue a certificate which identifies a different entity than the one associated with the IKE SA.

- The gateway MUST verify the signature in the certification request, to assert that the client possesses the private key corresponding to the public key being certified. In case of an invalid signature, the gateway MUST reject the request.

- The Short Term Certificate expiration time MUST NOT exceed the remaining time for repeated authentication [RFC4478], if such time is defined. If there is no defined time for repeated authentication, the gateway MUST limit the expiration time to no more than 24 hours. Note that IKE SA lifetime is irrelevant for determining Short Term Certificates expiration time, since rekeying IKE SAs does not require re-authentication.

- If the security gateway has a signing key that was certified by the root CA described in the Short Term Certificate request, then it MUST use this key to sign the Short Term Certificate. If no signing key matches a requested root CA, then the gateway MUST reject the request. If no STC_ROOT_CA was specified in the request, the security gateway MAY choose the root CA to use. Alternatively, it MAY reject the request.

- The issued certificate MUST be of the type requested in a STC_CERTIFICATE_TYPE attribute of the request message. In other words, the STC_CERTIFICATE_TYPE attribute has the same value in the request and the response.

- The key associated with the subject of the certificate MUST be the

public key sent in the Short Term Certificate request.

- When a full certificate chain should be sent to the endpoint, it is RECOMMENDED to make use of "Hash and URL" formats for the certificate chain to keep message size below the maximum UDP message size supported.

5. Using Short-Term Certificates

Once an endpoint acquired a Short Term Certificate from a security gateway, this certificate can be used for signature based authentication with any other security gateway that trusts the issuing gateway.

Note that certificate specifications are flexible enough to allow for transferring proprietary authentication-related information from the issuing security gateway to any other security gateway which will validate the Short Term Certificate. Such proprietary extensions and their implications on security are out of the scope of this document.

6. Expiration of Short-Term Certificates

An endpoint SHOULD NOT keep a Short Term Certificate after its expiration time was reached, since trying to use this certificate would result in a failed authentication. It is RECOMMENDED to refrain from using a Short Term Certificate for authentication if its expiration time is very close (e.g., less than ten minutes), since a repeated authentication [RFC4478] may take place once the newly created IKE SA is expired.

When the user terminates communications with a site ("logs off"), the Short Term Credentials associated with the site MUST be destroyed. Typically this will occur in conjunction with deletion of IKE_SAs with the site. However IKE_SAs may also be deleted without explicit user action.

7. IANA Considerations

The proposed extension requires IANA allocations for the "TBD" attribute types and the STC_UNSUPPORTED notify message type described in Section 4.

8. Security Considerations

Since certificates are widely used as long term credentials, special care should be taken to prevent abuse of Short Term Certificates which would lead to security risks.

The expiration time of the Short Term Certificate can never be later than a time limit defined for repeated authentication. This restriction prevents the use of Short Term Credentials for artificial extension of the IKE SA validity time, bypassing actual authentication of the user.

The Short Term Certificate issue exchange is protected with the established IKE SA. This maintains the confidentiality and the integrity of the exchange. Impersonating a security gateway would not allow a malicious user to abuse a Short Term Certificate and impersonate a valid user. Even if a malicious user was able to acquire a Short Term Certificate of another user, knowledge of the private key is still required to be able to use the Short Term Certificate successfully.

Lifetime of private/public key pairs needs to be considered if the same key pair is used for more than a single Short Term Certificate exchange. The client SHOULD generate new private/public key pairs at regular intervals, in accordance with security policy. This is the same situation as applies in all certificate request protocols: The same private/public key pair can be used in multiple requests, but its lifetime should nonetheless be considered limited.

9. Operational Considerations

Because of the granularity of Short Term Certificates expiration time, the administrator MUST prevent clock rollback on gateways and synchronize the clocks of mutually trusting security gateways. For example, the NTPv3 [RFC1305] or SNTPv4 [RFC4330] protocols can be implemented to provide this functionality. When such protocols are implemented to provide gateway synchronization, they SHOULD be properly secured to prevent attacks based on desynchronizing security gateway clocks.

10. Acknowledgements

11. References

11.1. Normative References

[I-D.ietf-pki4ipsec-ikecert-profile]
Korver, B., "The Internet IP Security PKI Profile of IKEv1/ISAKMP, IKEv2, and PKIX", draft-ietf-pki4ipsec-ikecert-profile-12 (work in progress), February 2007.

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

[RFC4306] Kaufman, C., "Internet Key Exchange (IKEv2) Protocol", RFC 4306, December 2005.

11.2. Informative References

[I-D.ohba-preauth-ps]
Ohba, Y., "EAP Pre-authentication Problem Statement", draft-ohba-preauth-ps-01 (work in progress), March 2007.

[ITU.X501.1993]
International Telecommunications Union, "Information Technology - Open Systems Interconnection - The Directory: Models", ITU-T Recommendation X.501, ISO Standard 9594-2, 1993.

[PIC] Sheffer, Y., Krawczyk , H., and B. Aboba , "PIC, A Pre-IKE Credential Provisioning Protocol, Internet-draft (expired), draft-ietf-ipsra-pic-06.txt", October 2002.

[RFC1305] Mills, D., "Network Time Protocol (Version 3) Specification, Implementation", RFC 1305, March 1992.

[RFC2315] Kaliski, B., "PKCS #7: Cryptographic Message Syntax Version 1.5", RFC 2315, March 1998.

[RFC2986] Nystrom, M. and B. Kaliski, "PKCS #10: Certification Request Syntax Specification Version 1.7", RFC 2986, November 2000.

[RFC3280] Housley, R., Polk, W., Ford, W., and D. Solo, "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile", RFC 3280, April 2002.

[RFC3748] Aboba, B., Blunk, L., Vollbrecht, J., Carlson, J., and H. Levkowetz, "Extensible Authentication Protocol (EAP)", RFC 3748, June 2004.

[RFC4301] Kent, S. and K. Seo, "Security Architecture for the Internet Protocol", RFC 4301, December 2005.

[RFC4330] Mills, D., "Simple Network Time Protocol (SNTP) Version 4 for IPv4, IPv6 and OSI", RFC 4330, January 2006.

[RFC4478] Nir, Y., "Repeated Authentication in Internet Key Exchange (IKEv2) Protocol", RFC 4478, April 2006.

Authors' Addresses

Arik Friedman
Technion IIT
Haifa 32000
Israel

Email: arikf@cs.technion.ac.il

Yaron Sheffer
Check Point Software Technologies Ltd.
5 Hasolelim st.
Tel Aviv 67897
Israel

Email: yaronf at checkpoint dot com

Ariel Shaqed (Scolnicov)
Correlix, Inc.
Herzelia Pituah

Israel

Email: ariel.shaqed+ietf@gmail.com

Full Copyright Statement

Intellectual Property

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).