Online Certificate Status Protocol (OCSP) Support for
Public Key Cryptography for
Initial Authentication in Kerberos (PKINIT)

Status of This Memo

This document specifies an Internet standards track protocol for the
Internet community, and requests discussion and suggestions for
improvements. Please refer to the current edition of the "Internet
Official Protocol Standards" (STD 1) for the standardization state
and status of this protocol. Distribution of this memo is unlimited.

Copyright Notice

Abstract

This document defines a mechanism to enable in-band transmission of
Online Certificate Status Protocol (OCSP) responses in the Kerberos
network authentication protocol. These responses are used to verify
the validity of the certificates used in Public Key Cryptography for
Initial Authentication in Kerberos (PKINIT), which is the Kerberos
Version 5 extension that provides for the use of public key
cryptography.

Table of Contents

1. Introduction

   Online Certificate Status Protocol (OCSP) [RFC2560] enables
   applications to obtain timely information regarding the revocation
   status of a certificate. Because OCSP responses are well bounded and
   small in size, constrained clients may wish to use OCSP to check the
   validity of the certificates for Kerberos Key Distribution Center
   (KDC) in order to avoid transmission of large Certificate Revocation
   Lists (CRLs) and therefore save bandwidth on constrained networks
   [OCSP-PROFILE].

   This document defines a pre-authentication type [RFC4120], where the
   client and the KDC MAY piggyback OCSP responses for certificates used
   in authentication exchanges, as defined in [RFC4556].

   By using this OPTIONAL extension, PKINIT clients and the KDC can
   maximize the reuse of cached OCSP responses.

2. Conventions Used in This Document

   In this document, the key words "MUST", "MUST NOT", "REQUIRED",
   "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY",
   and "OPTIONAL" are to be interpreted as described in [RFC2119].

3. Message Definition

   A pre-authentication type identifier is defined for this mechanism:

           PA-PK-OCSP-RESPONSE   18

   The corresponding padata-value field [RFC4120] contains the DER [X60]
   encoding of the following ASN.1 type:

           PKOcspData ::= SEQUENCE OF OcspResponse
                           -- If more than one OcspResponse is
                           -- included, the first OcspResponse
                           -- MUST contain the OCSP response
                           -- for the signer's certificate.
                           -- The signer refers to the client for
                           -- AS-REQ, and the KDC for the AS-REP,
                           -- respectively.

           OcspResponse ::= OCTET STRING
                           -- Contains a complete OCSP response,
                           -- as defined in [RFC2560].

   The client MAY send OCSP responses for certificates used in PA-PK-
   AS-REQ [RFC4556] via a PA-PK-OCSP-RESPONSE.

The KDC that receives a PA-PK-OCSP-RESPONSE SHOULD send a PA-PK-
OCSP-RESPONSE containing OCSP responses for certificates used in the
KDC's PA-PK-AS-REP. The client can request a PA-PK-OCSP-RESPONSE by
using a PKOcspData containing an empty sequence.

The KDC MAY send a PA-PK-OCSP-RESPONSE when it does not receive a
PA-PK-OCSP-RESPONSE from the client.

The PA-PK-OCSP-RESPONSE sent by the KDC contains OCSP responses for
certificates used in PA-PK-AS-REP [RFC4556].

Note the lack of integrity protection for the empty or missing OCSP
response; lack of an expected OCSP response from the KDC for the
KDC's certificates SHOULD be treated as an error by the client,
unless it is configured otherwise.

When using OCSP, the response is signed by the OCSP server, which is
trusted by the receiver. Depending on local policy, further
verification of the validity of the OCSP servers may be needed

The client and the KDC SHOULD ignore invalid OCSP responses received
via this mechanism, and they MAY implement CRL processing logic as a
fall-back position, if the OCSP responses received via this mechanism
alone are not sufficient for the verification of certificate
validity. The client and/or the KDC MAY ignore a valid OCSP response
and perform its own revocation status verification independently.

4. Security Considerations

The pre-authentication data in this document do not actually
authenticate any principals, but are designed to be used in
conjunction with PKINIT.

There is no binding between PA-PK-OCSP-RESPONSE pre-authentication
data and PKINIT pre-authentication data other than a given OCSP
response corresponding to a certificate used in a PKINIT pre-
authentication data element. Attacks involving removal or
replacement of PA-PK-OCSP-RESPONSE pre-authentication data elements
are, at worst, downgrade attacks, where a PKINIT client or KDC would
proceed without use of CRLs or OCSP for certificate validation, or
denial-of-service attacks, where a PKINIT client or KDC that cannot
validate the other's certificate without an accompanying OCSP
response might reject the AS exchange or might have to download very
large CRLs in order to continue. Kerberos V does not protect against
denial-of-service attacks; therefore, the denial-of-service aspect of
these attacks is acceptable.

If a PKINIT client or KDC cannot validate certificates without the
aid of a valid PA-PK-OCSP-RESPONSE, then it SHOULD fail the AS
exchange, possibly according to local configuration.

5. Acknowledgements

This document was based on conversations among the authors, Jeffrey
Altman, Sam Hartman, Martin Rex, and other members of the Kerberos
working group.

6. References

6.1. Normative References

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

[RFC2560]   Myers, M., Ankney, R., Malpani, A., Galperin, S., and
                C. Adams, "X.509 Internet Public Key Infrastructure
                Online Certificate Status Protocol - OCSP", RFC 2560,
                June 1999.

[RFC4120]   Neuman, C., Yu, T., Hartman, S., and K. Raeburn, "The
                Kerberos Network Authentication Service (V5)", RFC
                4120, July 2005.

[RFC4556]   Zhu, L. and B. Tung, "Public Key Cryptography for
                Initial Authentication in Kerberos (PKINIT)", RFC
                4556, June 2006.

[X690]   ASN.1 encoding rules: Specification of Basic Encoding
                Rules (BER), Canonical Encoding Rules (CER) and
                Distinguished Encoding Rules (DER), ITU-T
                Recommendation X.690 (1997) | ISO/IEC International
                Standard 8825-1:1998.

6.2. Informative References

[OCSP-PROFILE] Deacon, A. and R. Hurst, "Lightweight OCSP Profile for
                High Volume Environments", Work in Progress, May 2006.

Authors' Addresses

    Larry Zhu
    Microsoft Corporation
    One Microsoft Way
    Redmond, WA 98052
    US

    EMail: lzhu@microsoft.com

    Karthik Jaganathan
    Microsoft Corporation
    One Microsoft Way
    Redmond, WA 98052
    US

    EMail: karthikj@microsoft.com

    Nicolas Williams
    Sun Microsystems
    5300 Riata Trace Ct
    Austin, TX 78727
    US

    EMail: Nicolas.Williams@sun.com

Full Copyright Statement

Intellectual Property

Acknowledgement