NETWORK WORKING GROUP   L. Zhu
Internet-Draft   K. Jaganathan
Expires: June 3, 2005   Microsoft Corporation
                                                          N. Williams
                                                      Sun Microsystems
                                                     December 3, 2004

                         OCSP Support for PKINIT
                    draft-ietf-krb-wg-ocsp-for-pkinit-03

Status of this Memo

   This document is an Internet-Draft and is subject to all provisions
   of section 3 of RFC 3667. 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 become aware will be disclosed, in accordance with
   RFC 3668.

   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 June 3, 2005.

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 PKINIT - 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 [[CLARIFICATIONS](#)],
   where the client and the KDC MAY piggyback OCSP responses for
   certificates used in authentication exchanges, as defined in
   [[PKINIT](#)].

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

2. Conventions Used in This Document

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 [RFC2119].

3. Message Definition

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

              PA-PK-OCSP-RESPONSE   16

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

        PKOcspData ::= SEQUENCE OF OcspResponse

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

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

The KDC that receives a PA-PK-OCSP-RESPONSE then 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 [PKINIT].

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 their own revocation status verification independently.

[4](). Security Considerations

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

   There is a downgrade attack against clients which want OCSP responses
   from the KDC for the KDC's certificates. The clients, however, can
   treat the absence of valid OCSP responses as an error, based on their
   local configuration.

[5](#). IANA Considerations

No IANA actions are required for this document.

6. Acknowledgements

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

7. References

7.1 Normative References

[CLARIFICATIONS]
            Neuman, B., Yu, Y., Hartman, S. and K. Raeburn, "The
            Kerberos Network Authentication Service (V5)",
            draft-ietf-krb-wg-kerberos-clarifications, work in
            progress.

[PKINIT]   Tung, B., Neuman, B. and S. Medvinsky, "Public Key
            Cryptography for Initial Authentication in Kerberos",
            draft-ietf-cat-kerberos-pk-init, work in progress.

[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.

[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.

7.2 Informative References

[OCSP-PROFILE]
            Deacon, A. and R. Hurst, "Lightweight OCSP Profile for
            High Volume Environments", August 2004.

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

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.