Internet Engineering Task Force
Internet-Draft
Intended status: Standards Track
Expires: August 12, 2012

S. Sorce, Ed.
Red Hat
T. Yu, Ed.
T. Hardjono, Ed.
MIT Kerberos Consortium

Feb 9, 2012

Container Authenticated by Multiple MACs
draft-ietf-krb-wg-cammac-01

Abstract

Abstract: This document proposes a Kerberos Authorization Data container similar to AD-KDC-ISSUED, but that allows for multiple MACs or signatures on the contained Authorization Data elements.

Status of this Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at http://datatracker.ietf.org/drafts/current/.

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."

This Internet-Draft will expire on August 12, 2012.

Copyright Notice

Table of Contents

1. Introduction

This draft proposes a Authorization Data container for Kerberos that identifies a base set of MAC and other elements necessary to authenticate the authorization data being carried in such a way that not only the KDC but also services can independently verify that the data has been authenticated by the KDC and has not been tampered with.

2. 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].

3. Validation

Authorization data is highly sensitive and must be validated to insure no tampering has occured.

In order to validate any information the receiving client need to be able to cryptographically verify the data. This is done by introducing a new AuthorizationData element called AD-CAMMAC that contains enough information to bind the contents to a principal in a way that a receiving client can verify autonomously without further contact with the KDC.

The following information is needed:

- The KDC signature.
- The Service Signature.
- Optional Trusted Service Key Signature.

o Optional PUBKEY KDC Signature.

The KDC signature is required to allow the KDC to validate the data withouth requiring to recompute the contents at every TGS request.

The SVC signature is required so that the Service can verify that the authorization data has been validated by the KDC.

Both the Trusted Service Checksum and the asymmetric KDC Signature are useful to verify the authenticity of the contents on the same host, when the data is received by a less trusted service and passed

to a more trusted service on the same host without the need for additional roundtrips to the KDC.

The ad-type for AD-CAMMAC is (TBD).

4. Encoding

The Kerberos protocol is defined in [RFC4120] using Abstract Syntax Notation One (ASN.1) [X680]. As such, this specification also uses the ASN.1 syntax for specifying both the abstract layout of the AD-CAMMAC attributes, as well as its encoding.

4.1. AD-CAMMAC

```
AD-CAMMAC                   ::= SEQUENCE {
      kdc-signature         [0] Checksum,
      svc-signature         [1] Checksum,
      trusted-svc-signature [2] OPT-Checksum OPTIONAL,
      pubkey-signature      [3] TBD OPTIONAL,
      elements              [4] AuthorizationData
}

OPT-Checksum          ::= SEQUENCE {
      identifier      [0] PrincipalName,
      signature       [1] Checksum
}
```

kdc-signature
   A cryptographic checksum computed over the encoding of the elements field, keyed with the krbtgt key.
   Checksum type TBD.

svc-signature
   A cryptographic checksum computed over the encoding of the elements field, keyed with the service long term key.
   Checksum type TBD.

trusted-svc-signature
A principal name and a cryptographic checksum computed over the encoding of the elements field, keyed with the long term key of the principal name specified in the Name field. Unless otherwise explicitly administratively configured, the key SHOULD be found by substituting the service name component of the principal name of the service with 'host'.
If the service is 'host' this checksum is redundant and can be omitted.
If the resulting host/<name>@REALM or the administratively configured service is not found in the KDC database this cheksum can be omitted.
Checksum type TBD.

pubkey-signature
A name identifying the asymmetric key-pair used.
A checksum computed over the encoding of the elements field using the Private Key identified in the Name field.
If an asymmetric key is not available this checksum MUST be omitted.
Signature type TBD.

elements
A sequence of authorization data elements issued by the KDC.

5. Assigned numbers

TBD

6. IANA Considerations

TBD.

7. Security Considerations

Although generally authorization data are conveyed within a ticket and are thereby protected using the existing encryption methods on the ticket, some authorization data requires the additional

protection provided by the CAMMAC.

8. Acknowledgements

TBD.

9. References

9.1. Normative References

[RFC3961] Raeburn, K., "Encryption and Checksum Specifications for Kerberos 5", RFC 3961, February 2005.

[RFC3962] Raeburn, K., "Advanced Encryption Standard (AES) Encryption for Kerberos 5", RFC 3962, February 2005.

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

9.2. Informative References

[MIT-Athena] Steiner, J., Neuman, B., and J. Schiller, "Kerberos: An Authentication Service for Open Network Systems. In Proceedings of the Winter 1988 Usenix Conference. February.", 1988.

[RFC1510] Kohl, J. and B. Neuman, "The Kerberos Network Authentication Service (V5)", RFC 1510, September 1993.

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

[RFC3552] Rescorla, E. and B. Korver, "Guidelines for Writing RFC Text on Security Considerations", BCP 72, RFC 3552, July 2003.

[X.690] ISO, "ASN.1 encoding rules: Specification of Basic

Encoding Rules (BER), Canonical Encoding Rules (CER) and
Distinguished Encoding Rules (DER) - ITU-T Recommendation
X.690 (ISO/IEC International Standard 8825-1:1998)", 1997.

Appendix A. Additional Stuff

This becomes an Appendix.

Authors' Addresses

Simo Sorce (editor)
Red Hat

Email: ssorce@redhat.com

Tom Yu (editor)
MIT Kerberos Consortium

Email: tlyu@mit.edu

Thomas Hardjono (editor)
MIT Kerberos Consortium

Email: hardjono@mit.edu