Network Working Group	R.J.Y. Yount
Internet-Draft	Carnegie Mellon University
Intended status: Standards Track	August 15, 2011
Expires: February 16, 2012	

The Unencrypted Form Of Kerberos 5 KRB-CRED Message
draft-ietf-krb-wg-clear-text-cred-02

Abstract

The Kerberos 5 KRB-CRED message is used to transfer Kerberos credentials between applications. When used with a secure transport the unencrypted form of the KRB-CRED message may be desirable. This document describes the unencrypted form of the KRB-CRED message.

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 February 16, 2012.

1. Introduction

There are applications which need to transfer Kerberos credentials between them without having a prior relationship with established Kerberos keys. When transferred over a transport that provides confidentiality and integrity, the unencrypted form of the KRB-CRED message MAY be used. One application employing this method is the

Kerberos attribute transport mechanism described in section 2.8 of the SAML V2.0 Kerberos Attribute Profile *[sstc-saml-attribute-kerberos]*. In the SAML application, the Identity Provider (IdP) somehow obtains a Kerberos service ticket from the Kerberos Key Distribution Center (KDC) when required by the SAML system and transfers the credential to a Service Provider (SP) within an attribute statement. The SP can then use the credential to access a Kerberos protected service.
The Kerberos 5 specification as described in [RFC4120] mentions the non-standard legacy use of unencrypted KRB-CRED with Generic Security Services Application Programming Interface (GSS-API) [RFC1964] by the MIT, Heimdal, and Microsoft Kerberos implementations. This document provides a formal specification of the unencrypted form of the KRB-CRED message to enable its continued use in new applications.

2. Requirements notation

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. The Unencrypted Form Of The KRB-CRED

The unencrypted form of the KRB-CRED contains EncryptedData as defined in Section 5.2.9 [RFC4120]. The encryption type (etype) MUST be specified as 0. The optional key version number (kvno) SHOULD NOT be present and MUST be ignored by the recipient if present. The cipher text (cipher) is a copy of the EncKrbCredPart as defined in Section 5.8.1 [RFC4120] which is in clear text.

4. Kerberos Encryption Type 0 Is Not An Encryption System

The Kerberos Encryption Type 0 is an invalid value [RFC3961]. Layers above the encryption layer are left to interpret its use in their own context specific manner. The use of encryption type 0 in the unencrypted form of the KRB-CRED is not to specify an encryption type. In the context of the KRB-CRED it is a message specific indicator to be interpreted as the message is not encrypted. This approach was chosen due to existing Kerberos implementations which conform to this specification.

5. Security Considerations

The KRB-CRED message contains sensitive information related to Kerberos credentials being transferred, such as their secret session keys, client and server principal names, and validity period. Possession of this information, along with the ticket itself, would allow an attacker to impersonate the client named in the ticket. The possibility of modification of the KRB-CRED enables the attacker to substitute the credentials. This can result in the recipient using the credentials of

a client which was not intended. As a result, the KRB-CRED message must be carefully safeguarded.
The use of an unencrypted form of the KRB-CRED message MUST only be used with a transport where sender and recipient identities can been established to be known to each other. The transport MUST also provide confidentiality, integrity, and end to end security. Examples of transports which MAY be securely used to transport an unencrypted KRB-CRED message would include Transport Layer Security (TLS) [RFC5246] where mutual authentication has been established and those encoded within encrypted and signed SAML Security Assertion Markup Language (SAML) 2.0 *[OASIS.saml-core-2.0-os]* statement.

6. Acknowledgements

The following individuals have contributed to the development of this specification.
Thomas Hardjono, Massachusetts Institute of Technology
Josh Howlett, Individual
Jeffrey Hutzelman, Carnegie Mellon University

7. IANA Considerations

The reference for Kerberos encryption type 0 should be updated to point to this document.

8. References

8.1. Normative References

[RFC1964]	Linn, J., "The Kerberos Version 5 GSS-API Mechanism", RFC 1964, June 1996.
[RFC2119]	Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.
[RFC4120]	Neuman, C., Yu, T., Hartman, S. and K. Raeburn, "The Kerberos Network Authentication Service (V5)", RFC 4120, July 2005.
[RFC5246]	Dierks, T. and E. Rescorla, "The Transport Layer Security (TLS) Protocol Version 1.2", RFC 5246, August 2008.
[OASIS.saml-core-2.0-os]	Cantor, S., Kemp, J., Philpott, R. and E. Maler, "Assertions and Protocol for the OASIS Security Assertion Markup Language (SAML) V2.0", OASIS Standard saml-core-2.0-os, March 2005.

8.2. Informative References

	Howlett, J and T Hardjono, "SAML V2.0 Kerberos Attribute Profile Version 1.0, OASIS Security

[sstc-saml-attribute-kerberos]	Services Draft, sstc-saml-attribute-kerberos.odt (work in progress)", December 2010.
[RFC3961]	Raeburn, K., "Encryption and Checksum Specifications for Kerberos 5", RFC 3961, February 2005.

Author's Address

Russell J. Yount Yount Carnegie Mellon University
5000 Forbes Avenue Pittsburgh, Pennsylvania 15213 US Phone: +1 412 268 8391 EMail: rjy@cmu.edu

Table of Contents