Network Working Group	L. Hornquist Astrand
Internet-Draft	Apple, Inc
Updates: 1964, 1510, 3961, 4120,	July 11, 2010
4121 (if approved)	
Intended status: Standards Track	
Expires: January 12, 2011	

Deprecate DES support for Kerberos
draft-lha-des-die-die-die-05

Abstract

A long long time ago Data Encryption Standard (DES) was standardized. Some 30 years later (2003) is was withdrawn as a standard by National Institute of Standards and Technology (NIST), today 6 years later, its time for DES to finally die. By 2008 it was possible to brute force DES keys in 6.4 days using less than USD 10k worth of hardware. So by 2008 DES had passed its sell-by date. This document updates RFC1964, RFC4120, and RFC4121 to deprecate the use of DES in Kerberos. Because the version of Kerberos specified in RFC1510 only supports DES and has been replaced by RFC4120, RFC1510 is reclassified as historic.

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 January 12, 2011.

Copyright Notice

1. 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] (Bradner, S., “Key words for use in RFCs to Indicate Requirement Levels,” March 1997.).

---

2. Background

Kerberos 5 was defined in [RFC1510] (Kohl, J. and B. Neuman, “The Kerberos Network Authentication Service (V5),” September 1993.) and updated in [RFC4120] (Neuman, C., Yu, T., Hartman, S., and K. Raeburn, “The Kerberos Network Authentication Service (V5),” July 2005.), the Kerberos crypto system is defined by [RFC3961] (Raeburn, K., “Encryption and Checksum Specifications for Kerberos 5,” February 2005.) and includes support for DES encryption types. This document updates [RFC1964] (Linn, J., “The Kerberos Version 5 GSS-API Mechanism,” June 1996.), [RFC4120] (Neuman, C., Yu, T., Hartman, S., and K. Raeburn, “The Kerberos Network Authentication Service (V5),” July 2005.), and [RFC4121] (Zhu, L., Jaganathan, K., and S. Hartman, “The Kerberos Version 5 Generic Security Service Application Program Interface (GSS-API) Mechanism: Version 2,” July 2005.) to deprecate the use of DES in Kerberos.

Because the version of Kerberos specified in [RFC1510] (Kohl, J. and B. Neuman, “The Kerberos Network Authentication Service (V5),” September 1993.) only supports DES and has been replaced by [RFC4120] (Neuman, C., Yu, T., Hartman, S., and K. Raeburn, “The Kerberos Network Authentication Service (V5),” July 2005.), [RFC1510] (Kohl, J. and B. Neuman, “The Kerberos Network Authentication Service (V5),” September 1993.) is reclassified as historic.

DES was withdrawn in [DES-Transition-Plan] (National Institute of Standards and Technology, “DES Transition Plan - Federal Register / Vol. 70, No. 96,” May 2006.) by National Institute of Standards and Technology (NIST). IETF have also published its the position in [RFC4772] (Kelly, S., “Security Implications of Using the Data Encryption Standard (DES),” December 2006.), which in the recommendation summery is made very clear: "don't use DES".

In Kerberos Generic Security Services Application Programming Interface (GSS-API) mechanism [RFC1964] (Linn, J., “The Kerberos Version 5 GSS-API Mechanism,” June 1996.) and the updated version [RFC4121] (Zhu, L., Jaganathan, K., and S. Hartman, “The Kerberos Version 5 Generic Security Service Application Program Interface (GSS-API) Mechanism: Version 2,” July 2005.) the following checksum and encryption mechanism is defined: three SGN ALG: 0000 - DES MAC MD5, 0100 - MD2.5 0200 - DES MAC and one SEAL ALG 0000 - DES. With newer encryption types for Kerberos defined in [RFC4121] (Zhu, L., Jaganathan, K., and S. Hartman, “The Kerberos Version 5 Generic Security Service Application Program Interface (GSS-API) Mechanism: Version 2,” July 2005.), Microsofts ARCFOUR4-HMAC based GSS-API mech, and MITs DES3 , there is no need to support the old DES based SGN/SEAL types.

---

3. Recommendations

This document removes the RECOMMENDED types from [RFC4120] (Neuman, C., Yu, T., Hartman, S., and K. Raeburn, "The Kerberos Network Authentication Service (V5)," July 2005.):

> Encryption: DES-CBC-MD5(3)
>
> Checksums: DES-MD5 (8, RSA-MD5-DES from [RFC3961] (Raeburn, K., "Encryption and Checksum Specifications for Kerberos 5," February 2005.)).

Kerberos implementation and deployments SHOULD NOT implement the single DES encryption types: DES-CBC-CRC(1), DES-CBC-MD4(2), DES-CBC-MD5(3).
Kerberos implementation and deployments SHOULD NOT implement the checksum type: CRC32(1), RSA-MD4(2), RSA-MD4-DES(3), DES-MAC(4), DES-MAC-K(5), RSA-MD4-MAC-K(6), DES-MD5(7), RSA-MD5-DES(8).
Note that RSA-MD5 might be with non-DES encryption types, for example, when doing a TGS-REQ with a ARCFOUR-HMAC-MD5 some client uses RSA-MD5 for the checksum that is stored inside the encrypted part of the authenticator. This use of RSA-MD5 should probably be considered safe, so the Kerberos implementation should make sure this usage is not disabled when used with legacy system that can't handle newer checksum types.
Kerberos GSS mechanism implementation and deployments SHOULD NOT implement the SGN ALG: DES MAC MD5(0000), MD2.5(0100), DES MAC(0200) (updates [RFC1964] (Linn, J., "The Kerberos Version 5 GSS-API Mechanism," June 1996.)).
Kerberos GSS mechanism implementation and deployments SHOULD NOT implement the SEAL ALG: DES(0000) (updates [RFC1964] (Linn, J., "The Kerberos Version 5 GSS-API Mechanism," June 1996.)).
The effect of the two last sentences is that this document deprecates section 1.2 in [RFC1964] (Linn, J., "The Kerberos Version 5 GSS-API Mechanism," June 1996.).

---

4. Acknowledgements

Jeffrey Hutzelman, Simon Josefsson, Mattias Amnefelt and Leif Johansson have read the document and provided suggestions for improvements. Sam hartman proposed moving [RFC1510] (Kohl, J. and B. Neuman, "The Kerberos Network Authentication Service (V5)," September 1993.) to historic.

---

5. Security Considerations

Removing support for single DES improves security since DES is considered to be insecure.

---

6. IANA Considerations

There are no IANA Considerations for this document

---

7. References

7.1. Normative References

[RFC1964]	Linn, J., “The Kerberos Version 5 GSS-API Mechanism,” RFC 1964, June 1996 (TXT).
[RFC2119]	Bradner, S., “Key words for use in RFCs to Indicate Requirement Levels,” BCP 14, RFC 2119, March 1997 (TXT, HTML, XML).
[RFC3961]	Raeburn, K., “Encryption and Checksum Specifications for Kerberos 5,” RFC 3961, February 2005 (TXT).
[RFC4120]	Neuman, C., Yu, T., Hartman, S., and K. Raeburn, “The Kerberos Network Authentication Service (V5),” RFC 4120, July 2005 (TXT).
[RFC4121]	Zhu, L., Jaganathan, K., and S. Hartman, “The Kerberos Version 5 Generic Security Service Application Program Interface (GSS-API) Mechanism: Version 2,” RFC 4121, July 2005 (TXT).

7.2. Informative References

[DES-Transition-Plan]	National Institute of Standards and Technology, “DES Transition Plan - Federal Register / Vol. 70, No. 96,” May 2006.
[RFC1510]	Kohl, J. and B. Neuman, “The Kerberos Network Authentication Service (V5),” RFC 1510, September 1993 (TXT).
[RFC4772]	Kelly, S., “Security Implications of Using the Data Encryption Standard (DES),” RFC 4772, December 2006 (TXT).

Author's Address

	Love Hornquist Astrand
	Apple, Inc
	Cupertino
	USA
Email:	lha@apple.com