Network Working Group
Internet-Draft
Updates: 1510, 1964, 4120, 4121
(if approved)
Intended status: Standards Track
Expires: August 11, 2012

L. Hornquist Astrand
Apple, Inc
T. Yu
MIT Kerberos Consortium

February 8, 2012

# Deprecate DES support for Kerberos
# draft-ietf-krb-wg-des-die-die-die-01

## Abstract

The Kerberos 5 network authentication protocol, originally specified in RFC1510, can use the Data Encryption Standard (DES) for encryption. Almost 30 years after first publishing DES, the National Institute of Standards and Technology (NIST) finally withdrew the standard in 2005, reflecting a long-established consensus that DES is insufficiently secure. By 2008, commercial hardware costing less than USD 15,000 could break DES keys in less than a day on average. DES is long past its sell-by date. Accordingly, this document updates RFC1964, RFC4120, and RFC4121 to deprecate the use of DES in Kerberos. Because RFC1510 (obsoleted by RFC4120) supports only DES, this document also reclassifies RFC1510 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 August 11, 2012.

## Copyright Notice

Copyright (c) 2012 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to BCP 78 and the IETF Trust's Legal

Provisions Relating to IETF Documents
(http://trustee.ietf.org/license-info) in effect on the date of
publication of this document. Please review these documents
carefully, as they describe your rights and restrictions with respect
to this document. Code Components extracted from this document must
include Simplified BSD License text as described in Section 4.e of
the Trust Legal Provisions and are provided without warranty as
described in the Simplified BSD License.

## 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].

## 2. Introduction

The original specification of the Kerberos 5 network authentication protocol [RFC1510] supports only the Data Encryption Standard (DES) for encryption. For many years, the cryptographic community has regarded DES as providing inadequate security. Accordingly, this document reclassifies [RFC1510] (obsoleted by [RFC4120]) as Historic, and updates current Kerberos-related specifications [RFC1964], [RFC4120], and [RFC4121] to deprecate the use of DES in Kerberos.

## 3. Affected specifications

The original IETF specification of Kerberos 5 [RFC1510] only supports DES for encryption. [RFC4120] obsoletes [RFC1510] and updates the Kerberos specification to include additional cryptographic algorithms, but still permits the use of DES.

The specification of the Kerberos Generic Security Services Application Programming Interface (GSS-API) mechanism [RFC1964] and its updated version [RFC4121] define checksum and encryption mechanisms based on DES. With the existence of newer encryption types for Kerberos GSS-API defined in [RFC4121], Microsoft's ARCFOUR-HMAC based GSS-API mechanism, and MIT's DES3, there is no need to support the old DES based integrity (SGN) and confidentiality (SEAL) types.

## 4. DES insecurity

The insecurity of DES has been evident for many years. The National

Institute of Standards and Technology (NIST) officially withdrew DES in 2005 [DES-Withdrawal], and also announced a transition period that ended on May 19, 2007 [DES-Transition-Plan]. The IETF has also published its position in [RFC4772], in which the recommendation summary is very clear: "don't use DES".

In 2006, researchers demonstrated the ability to brute force a DES key in an average of less than 9 days using less than EUR 10,000 worth of hardware [Break-DES]. By 2008, a company was offering hardware capable of breaking a DES key in less than a day on average [DES-1day] that cost less than USD 15,000 [DES-crack]. Brute force key searches of DES will only get faster and cheaper. (The aforementioned company markets its device for one-click recovery of lost DES keys.) It is clear that it is well past time to retire the use of DES in Kerberos.

## 5. Recommendations

This document hereby removes the following RECOMMENDED types from [RFC4120]:

Encryption: DES-CBC-MD5(3)
Checksums: DES-MD5 (8, named RSA-MD5-DES in [RFC3961]).

Kerberos implementations and deployments SHOULD NOT implement the single DES encryption types: DES-CBC-CRC(1), DES-CBC-MD4(2), DES-CBC-MD5(3).

Kerberos implementations and deployments SHOULD NOT implement the checksum types: CRC32(1), RSA-MD4(2), RSA-MD4-DES(3), DES-MAC(4), DES-MAC-K(5), RSA-MD4-MAC-K(6), RSA-MD5-DES(8).

It is possible to safely use the RSA-MD5(7) checksum type, but only with additional protection, such as the protection that an encrypted Authenticator provides. Implementations MAY use RSA-MD5 inside an encrypted Authenticator for backward compatibility with systems that do not support newer checksum types. One example is that some legacy systems only support ARCFOUR-HMAC-MD5 for encryption when DES is not available; these systems use RSA-MD5 checksums inside Authenticators encrypted with ARCFOUR-HMAC-MD5.

Kerberos GSS mechanism implementations and deployments SHOULD NOT implement the SGN ALG: DES MAC MD5(0000), MD2.5(0100), DES MAC(0200) (updates [RFC1964]).

Kerberos GSS mechanism implementations and deployments SHOULD NOT implement the SEAL ALG: DES(0000) (updates [RFC1964]).

The effect of the two last sentences is that this document deprecates section 1.2 in [RFC1964].

This document hereby reclassifies [RFC1510] as Historic.

## 6. Acknowledgements

Jeffrey Hutzelman, Simon Josefsson, Mattias Amnefelt, Leif Johansson, and Ran Atkinson have read the document and provided suggestions for improvements. Sam Hartman proposed moving [RFC1510] to Historic.

## 7. Security Considerations

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

Kerberos defines some encryption types that are either underspecified or that only have number assignments but no specifications. Implementations should make sure that they only implement and enable secure encryption types.

RC4, used in ARCFOUR-HMAC, is considered weak; however, the use in Kerberos is vetted and considered secure for now. The main reason to not actively discourage the use of ARCFOUR-HMAC is that it is the only encryption type that interoperates with older versions of Microsoft Windows once DES is removed.

## 8. IANA Considerations

There are no IANA Considerations for this document.

## 9. References

### 9.1. 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.

[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.

## 9.2. Informative References

[Break-DES]
Kumar, S., Paar, C., Pelzl, J., Pfeiffer, G., Rupp, A., and M. Schimmler, "How to break DES for EUR 8,980 - SHARCS'06 - Special-purpose Hardware for Attacking Cryptographic Systems", April 2006, <http://www.copacobana.org/paper/copacobana_SHARCS2006.pdf>.

[DES-1day]
SciEngines GmbH, "Break DES in less than a single day", <http://www.sciengines.com/company/news-a-events/74-des-in-1-day.html>.

[DES-Transition-Plan]
National Institute of Standards and Technology, "DES Transition Plan", May 2005, <http://csrc.nist.gov/groups/STM/common_documents/DESTranPlan.pdf>.

[DES-Withdrawal]
National Institute of Standards and Technology, "Announcing Approval of the Withdrawal of Federal Information Processing Standard (FIPS) 46-3, Data Encryption Standard (DES); FIPS 74, Guidelines for Implementing and Using the NBS Data Encryption Standard; and FIPS 81, DES Modes of Operation - Federal Register Document 05-9945", 70 FR 28907-28908, May 2005, <http://www.gpo.gov/fdsys/pkg/FR-2005-05-19/pdf/05-9945.pdf>.

[DES-crack]
Scott, T., "DES Brute Force Cracking Efforts 1977 to 2010", 2010, <http://www.tjscott.net/security.extras/des.crack.efforts.pdf>.

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

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

[RFC4772] Kelly, S., "Security Implications of Using the Data Encryption Standard (DES)", RFC 4772, December 2006.

Authors' Addresses

Love Hornquist Astrand
Apple, Inc
Cupertino
USA

Email: lha@apple.com

Tom Yu
MIT Kerberos Consortium
77 Massachusetts Ave
Cambridge, Massachusetts
USA

Email: tlyu@mit.edu