Network Working Group
Internet-Draft
Updates: 1510, 1964, 4120, 4121, 4757
(if approved)
Intended status: BCP
Expires: August 30, 2012

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

February 27, 2012

# Deprecate DES, RC4-HMAC-EXP, and other weak cryptographic algorithms in Kerberos

draft-ietf-krb-wg-des-die-die-die-04

## 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, RFC4121, and RFC4757 to deprecate the use of DES, RC4-HMAC-EXP, and other weak cryptographic algorithms in Kerberos. Because RFC1510 (obsoleted by RFC4120) supports only DES, this document 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 30, 2012.

## 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].

## 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, mostly because of its small key size. 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 and other weak cryptographic algorithms in Kerberos, including some unkeyed checksums and hashes, along with the weak 56-bit "export strength" RC4 variant enctype of [RFC4757].

## 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. [RFC3961] describes the Kerberos cryptographic system and includes support for DES encryption types, but it does not specify requirement levels for them.

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 RC4-HMAC based GSS-API mechanism, and MIT's DES3 (which is not published as an

RFC), there is no need to support the old DES based integrity (SGN) and confidentiality (SEAL) types.

[RFC4757] describes the RC4-HMAC encryption types used by Microsoft Windows, and allows for a 56-bit "export strength" variant. (The character constant "fortybits" used in the definition is a historical reference and does not refer to the actual key size of the enctype.)

## 4. DES insecurity

The insecurity of DES has been evident for many years. Even around the time of its first publication, cryptographers raised the possibility that 56 bits was too small a key size for DES. 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 or deploy the following single DES encryption types: DES-CBC-CRC(1), DES-CBC-MD4(2), DES-CBC-MD5(3) (updates [RFC4120]).

Kerberos implementations and deployments SHOULD NOT implement or deploy the following "export strength" RC4 variant encryption type: RC4-HMAC-EXP(24) (updates [RFC4757]). This document does not add any sort of requirement for conforming implementations to implement RC4-HMAC(23).

Kerberos implementations and deployments SHOULD NOT implement or deploy the following checksum types: CRC32(1), RSA-MD4(2), RSA-MD4-DES(3), DES-MAC(4), DES-MAC-K(5), RSA-MD4-DES-K(6), RSA-MD5-DES(8) (updates [RFC4120]).

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 (updates [RFC4120]). One example is that some legacy systems only support RC4-HMAC(23) [RFC4757] for encryption when DES is not available; these systems use RSA-MD5 checksums inside Authenticators encrypted with RC4-HMAC.

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

Kerberos GSS mechanism implementations and deployments SHOULD NOT implement or deploy the following 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

Mattias Amnefelt, Ran Atkinson, Henry Hotz, Jeffrey Hutzelman, Leif Johansson, Simon Josefsson, and Martin Rex have read the document and provided suggestions for improvements. Sam Hartman proposed moving [RFC1510] to Historic. Michiko Short provided information about the dates of end of support for Windows releases.

## 7. Security Considerations

Removing support for single DES improves security, because DES is considered to be insecure. RC4-HMAC-EXP has a similarly inadequate key size, so removing support for it also improves security.

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.

The security considerations of [RFC4757] continue to apply to RC4-HMAC, including the known weaknesses of RC4 and MD4, and this document does not change the Informational status of [RFC4757] for now. The main reason to not actively discourage the use of RC4-HMAC is that it is the only encryption type that interoperates with older versions of Microsoft Windows once DES and RC4-HMAC-EXP are removed. These older versions of Microsoft Windows will likely be in use until at least 2015.

## 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.

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

[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.

[RFC4757] Jaganathan, K., Zhu, L., and J. Brezak, "The RC4-HMAC Kerberos Encryption Types Used by Microsoft Windows", RFC 4757, December 2006.

### 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.

[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