Network Working Group
Internet-Draft
Updates: 4880 (if approved)
Intended status: Standards Track
Expires: July 24, 2008

D. Shaw
January 21, 2008

The Camellia Cipher in OpenPGP
draft-ietf-openpgp-camellia-01

Status of this Memo

Copyright Notice

Abstract

This document presents the necessary information to use the Camellia symmetric block cipher in the OpenPGP protocol.

Table of Contents

1. Introduction

The OpenPGP protocol [RFC4880] can support many different symmetric ciphers. This document presents the necessary information to use the Camellia [RFC3713] cipher in the OpenPGP protocol.

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. Camellia

Camellia is specified in [RFC3713]. It is a 128-bit block cipher (as is AES and Twofish in OpenPGP), that supports 128-bit, 192-bit, and 256-bit keys. This document defines the use of the 128-bit and 256-bit Camellia key lengths in OpenPGP.

The OpenPGP symmetric key algorithm number for Camellia with a 128-bit key is XXXX and the algorithm number for a 256-bit key is YYYY. [[To be allocated by IANA. Please fill this in: presumably XXXX == 11 and YYYY == 12]]

OpenPGP applications MAY implement Camellia. If implemented, Camellia may be used in any place in OpenPGP where a symmetric cipher is usable, and is subject to the same usage requirements (such as its presence in the Preferred Symmetric Algorithms signature subpacket) as the other symmetric ciphers in OpenPGP.

While the OpenPGP algorithm preferences system prevents interoperability problems with public key encrypted messages, if Camellia (or any other optional cipher) is used for encrypting private keys, there could be interoperability problems when migrating a private key from one system to another. A similar issue can arise when using an optional cipher for symmetric-only encrypted messages, as this OpenPGP message type does not perform cipher negotiation. Those using optional ciphers in this manner should take care they are using a cipher that their intended recipient can decrypt.

4. Security Considerations

At publication time, there are no known weak keys for Camellia, and the Camellia algorithm is believed to be strong. However, as with any technology involving cryptography, implementers should check the

current literature, as well as the Camellia home page at <http://info.isl.ntt.co.jp/camellia/>, to determine if Camellia has been found to be vulnerable to attack.

5. IANA Considerations

This document requires IANA to assign two algorithm numbers from the registry of OpenPGP Symmetric-Key Algorithms that was created by [RFC4880].

6. Normative References

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

[RFC3713] Matsui, M., Nakajima, J., and S. Moriai, "A Description of the Camellia Encryption Algorithm", RFC 3713, April 2004.

[RFC4880] Callas, J., Donnerhacke, L., Finney, H., Shaw, D., and R. Thayer, "OpenPGP Message Format", RFC 4880, November 2007.

Author's Address

David Shaw

Email: dshaw@jabberwocky.com

Full Copyright Statement

Intellectual Property

Acknowledgment

Funding for the RFC Editor function is provided by the IETF Administrative Support Activity (IASA).