

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

By submitting this Internet-Draft, each author represents that any applicable patent or other IPR claims of which he or she is aware have been or will be disclosed, and any of which he or she becomes aware will be disclosed, in accordance with [Section 6 of BCP 79](#).

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF), its areas, and its working groups. Note that other groups may also distribute working documents as Internet-Drafts.

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."

The list of current Internet-Drafts can be accessed at <http://www.ietf.org/ietf/1id-abstracts.txt>.

The list of Internet-Draft Shadow Directories can be accessed at <http://www.ietf.org/shadow.html>.

This Internet-Draft will expire on July 24, 2008.

Copyright Notice

Copyright (C) The IETF Trust (2008).

Abstract

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

Table of Contents

1.	Introduction	3
2.	Requirements notation	3
3.	Camellia	3
4.	Security Considerations	3
5.	IANA Considerations	4
6.	Normative References	4
	Author's Address	4
	Intellectual Property and Copyright Statements	5

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., Donnerhake, 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

Copyright (C) The IETF Trust (2008).

This document is subject to the rights, licenses and restrictions contained in [BCP 78](#), and except as set forth therein, the authors retain all their rights.

This document and the information contained herein are provided on an "AS IS" basis and THE CONTRIBUTOR, THE ORGANIZATION HE/SHE REPRESENTS OR IS SPONSORED BY (IF ANY), THE INTERNET SOCIETY, THE IETF TRUST AND THE INTERNET ENGINEERING TASK FORCE DISCLAIM ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO ANY WARRANTY THAT THE USE OF THE INFORMATION HEREIN WILL NOT INFRINGE ANY RIGHTS OR ANY IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

Intellectual Property

The IETF takes no position regarding the validity or scope of any Intellectual Property Rights or other rights that might be claimed to pertain to the implementation or use of the technology described in this document or the extent to which any license under such rights might or might not be available; nor does it represent that it has made any independent effort to identify any such rights. Information on the procedures with respect to rights in RFC documents can be found in [BCP 78](#) and [BCP 79](#).

Copies of IPR disclosures made to the IETF Secretariat and any assurances of licenses to be made available, or the result of an attempt made to obtain a general license or permission for the use of such proprietary rights by implementers or users of this specification can be obtained from the IETF on-line IPR repository at <http://www.ietf.org/ipr>.

The IETF invites any interested party to bring to its attention any copyrights, patents or patent applications, or other proprietary rights that may cover technology that may be required to implement this standard. Please address the information to the IETF at ietf-ipr@ietf.org.

Acknowledgment

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

