

S/MIME Advanced Encryption Standard (AES)  
Requirement for the Session Initiation Protocol (SIP)

Status of this Memo

This document specifies an Internet standards track protocol for the Internet community, and requests discussion and suggestions for improvements. Please refer to the current edition of the "Internet Official Protocol Standards" (STD 1) for the standardization state and status of this protocol. Distribution of this memo is unlimited.

Copyright Notice

Copyright (C) The Internet Society (2004).

Abstract

RFC 3261 currently specifies 3DES as the mandatory-to-implement ciphersuite for implementations of S/MIME in the Session Initiation Protocol (SIP). This document updates the normative guidance of RFC 3261 to require the Advanced Encryption Standard (AES) for S/MIME.

Table of Contents

|  |   |
|--|---|
| 1. Introduction . . . . .                            | 2 |
| 2. Terminology . . . . .                             | 3 |
| 3. S/MIME Ciphersuite Requirements for SIP . . . . . | 3 |
| 4. Security Considerations . . . . .                 | 3 |
| 5. References . . . . .                              | 4 |
| 5.1. Normative References . . . . .                  | 4 |
| 5.2. Informative References . . . . .                | 4 |
| 6. Acknowledgments . . . . .                         | 4 |
| 7. Author's Address . . . . .                        | 5 |
| 8. Full Copyright Statement . . . . .                | 6 |

## 1. Introduction

The Session Initiation Protocol (SIP) specification ([RFC 3261](#) [1]) currently details optional support (a normative MAY) for the use of secure MIME, or S/MIME ([RFC 2633](#) [8]). Since [RFC 3261](#) was published, the S/MIME specification and the underlying Cryptographic Message Syntax (CMS, [RFC 3369](#) [3]) have undergone some revision. Ongoing work has identified AES as a algorithm that might be used for content encryption in S/MIME.

The Advanced Encryption Standard (AES [6]) is widely believed to be faster than Triple-DES (3DES, which has previously been mandated for usage with S/MIME) and to be comparably secure. AES is also believed to have comparatively low memory requirements, which makes it suitable for use in mobile or embedded devices, an important use-case for SIP.

As an additional consideration, the SIP specification has a recommendation (normative SHOULD) for support of Transport Layer Security (TLS, [RFC 2246](#) [7]). TLS support in SIP requires the usage of AES. That means that currently, implementations that support both TLS and S/MIME must support both 3DES and AES. A similar duplication of effort exists with DSS in S/MIME as a digital signature algorithm (the mandatory TLS ciphersuite used by SIP requires RSA). Unifying the ciphersuite and signature algorithm requirements for TLS and S/MIME would simplify security implementations.

It is therefore desirable to bring the S/MIME requirement for SIP into parity with ongoing work on the S/MIME standard, as well as to unify the algorithm requirements for TLS and S/MIME. To date, S/MIME has not yet seen widespread deployment in SIP user agents, and therefore the minimum ciphersuite for S/MIME could be updated without obsoleting any substantial deployments of S/MIME for SIP (in fact, these changes will probably make support for S/MIME easier). This document therefore updates the normative requirements for S/MIME in [RFC 3261](#).

Note that work on these revisions in the S/MIME working group is still in progress. This document will continue to track that work as it evolves. By initiating this process in the SIP WG now, we provide an early opportunity for input into the proposed changes and give implementers some warning that the S/MIME requirements for SIP are potentially changing.

## 2. Terminology

In this document, the key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "NOT RECOMMENDED", "MAY", and "OPTIONAL" are to be interpreted as described in [BCP 14](#), [RFC 2119](#) [2] and indicate requirement levels for compliant SIP implementations.

## 3. S/MIME Ciphersuite Requirements for SIP

The following updates the text of [RFC 3261 Section 23.3](#), specifically the fifth bullet point. The text currently reads:

- o S/MIME implementations MUST at a minimum support SHA1 as a digital signature algorithm, and 3DES as an encryption algorithm. All other signature and encryption algorithms MAY be supported. Implementations can negotiate support for these algorithms with the "SMIMECapabilities" attribute.

This text is updated with the following:

S/MIME implementations MUST at a minimum support RSA as a digital signature algorithm and SHA1 as a digest algorithm [5], and AES as an encryption algorithm (as specified in [4]. For key transport, S/MIME implementations MUST support RSA key transport as specified in section 4.2.1. of [5]. S/MIME implementations of AES MUST support 128-bit AES keys, and SHOULD support 192 and 256-bit keys. Note that the S/MIME specification [8] mandates support for 3DES as an encryption algorithm, DH for key encryption and DSS as a signature algorithm. In the SIP profile of S/MIME, support for 3DES, DH and DSS is RECOMMENDED but not required. All other signature and encryption algorithms MAY be supported. Implementations can negotiate support for algorithms with the "SMIMECapabilities" attribute.

Since SIP is 8-bit clean, all implementations MUST use 8-bit binary Content-Transfer-Encoding for S/MIME in SIP. Implementations MAY also be able to receive base-64 Content-Transfer-Encoding.

## 4. Security Considerations

The migration of the S/MIME requirement from Triple-DES to AES is not known to introduce any new security considerations.

## 5. References

### 5.1. Normative References

- [1] Rosenberg, J., Schulzrinne, H., Camarillo, G., Johnston, A., Peterson, J., Sparks, R., Handley, M., and E. Schooler, "SIP: Session Initiation Protocol", [RFC 3261](#), June 2002.
- [2] Bradner, S., "Key words for use in RFCs to indicate requirement levels", [BCP 14](#), [RFC 2119](#), March 1997.
- [3] Housley, R., "Cryptographic Message Syntax (CMS)", [RFC 3369](#), August 2002.
- [4] Schaad, J., "Use of the Advanced Encryption Standard (AES) Encryption Algorithm in Cryptographic Message Syntax (CMS)", [RFC 3565](#), July 2003.
- [5] Housley, R., "Cryptographic Message Syntax (CMS) Algorithms", [RFC 3394](#), August 2002.

### 5.2. Informative References

- [6] National Institute of Standards & Technology, "Advanced Encryption Standard (AES).", FIPS 197, November 2001.
- [7] Dierks, T. and C. Allen, "The TLS Protocol Version 1.0", [RFC 2246](#), January 1999.
- [8] Ramsdell, B., Ed., "S/MIME Version 3.1 Message Specification", [RFC 3851](#), July 2004.

## 6. Acknowledgments

Thanks to Rohan Mahy, Gonzalo Camarillo, and Eric Rescorla for review of this document.

## 7. Author's Address

Jon Peterson  
NeuStar, Inc.  
1800 Sutter St  
Suite 570  
Concord, CA 94520  
US

Phone: +1 925/363-8720  
EMail: [jon.peterson@neustar.biz](mailto:jon.peterson@neustar.biz)  
URI: <http://www.neustar.biz/>

## 8. Full Copyright Statement

Copyright (C) The Internet Society (2004). 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 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](mailto:ietf-ipr@ietf.org).

## Acknowledgement

Funding for the RFC Editor function is currently provided by the Internet Society.