Storage Maintenance (storm)
Internet-Draft
Updates: 3720, 3723, 3821, 3822, 4018, 4172, 4173, 4174, 5040,
Intended status: Standards Track
Expires: December 09, 2013
June 07, 2013

D. Black
EMC
P. Koning
Dell

# IP Storage: IPsec Requirements Update for IPsec v3
## draft-ietf-storm-ipsec-ips-update-01

## Abstract

RFC 3723 includes requirements for IPsec usage with IP Storage protocols (e.g., iSCSI) based on IPsec v2 (RFC 2401 and related RFCs). This document updates those requirements to IPsec v3 (RFC 4301 and related RFCs) and updates implementation requirements to reflect developments in cryptography since RFC 3723 was published.

[RFC Editor: The "Updates:" list above has been truncated by xml2rfc. The complete list is - Updates: 3720, 3723, 3821, 3822, 4018, 4172, 4173, 4174, 5040, 5041, 5042, 5043, 5044, 5045, 5046, 5047, 5048 (if approved) ]

## Status of This Memo

## Copyright Notice

Table of Contents

1. Introduction . . . . . . . . . . . . . . . . . . . . . . . . 2
1.1. Requirements Language . . . . . . . . . . . . . . . . . . . 3
1.2. Updated RFCs . . . . . . . . . . . . . . . . . . . . . . . 3
2. ESP Requirements . . . . . . . . . . . . . . . . . . . . . . . 4
2.1. Data Origin Authentication and Data Integrity Transforms 4
2.2. Confidentiality Transform Requirements . . . . . . . . . 5
3. IKEv1 and IKEv2 Requirements . . . . . . . . . . . . . . . . 6
3.1. Authentication Requirements . . . . . . . . . . . . . . . . 7
3.2. D-H Group and PRF Requirements . . . . . . . . . . . . . . 9
4. IANA Considerations . . . . . . . . . . . . . . . . . . . . . 9
5. Security Considerations . . . . . . . . . . . . . . . . . . . 9
6. References . . . . . . . . . . . . . . . . . . . . . . . . . 9
6.1. Normative References . . . . . . . . . . . . . . . . . . . 9
6.2. Informative References . . . . . . . . . . . . . . . . . . 12
Authors' Addresses . . . . . . . . . . . . . . . . . . . . . . . 13

## 1. Introduction

RFC 3723 [RFC3723] includes requirements for use of IPsec with IP Storage protocols (e.g., iSCSI) based on IPsec v2 (RFC 2401 [RFC2401] and related RFCs). This document updates those requirements to include IPsec v3 (RFC 4301[RFC4301] and related RFCs) to reflect developments since RFC 3723 was published. IP storage protocols can be expected to operate at high data rates (multiple Gigabits/second); the requirements in this document are strongly influenced by that expectation, and hence may not be appropriate for use of IPsec with other protocols that do not operate at high data rates.

In addition to the IPsec v2 requirements in RFC 3723, IPsec v3, as specified in [RFC4301] and related RFCs (e.g., IKEv2 [RFC5996]), SHOULD be implemented for use of IPsec with IP storage protocols. Retention of the mandatory requirement for IPsec v2 provides interoperability with existing implementations, and the strong recommendation for IPsec v3 encourages implementers to move forward to that newer version of IPsec.

Cryptographic developments since the publication of RFC 3723 necessitate changes to the encryption transform requirements for IPsec v2, as explained further in Section 2.2; these updated requirements also apply to IPsec v3.

## 1.1. Requirements Language

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 RFC 2119 [RFC2119].

## 1.2. Updated RFCs

The requirements for IPsec usage with IP storage in RFC 3723 are used by a number of protocols. For that reason, beyond updating RFC 3723, this document also updates the IPsec requirements for each protocol specification that uses RFC 3723, i.e., the following RFCs in addition to RFC 3723:

- [RFC3720] "Internet Small Computer Systems Interface (iSCSI)"
- [RFC3821] "Fibre Channel Over TCP/IP (FCIP)"
- [RFC3822] "Finding Fibre Channel over TCP/IP (FCIP) Entities Using Service Location Protocol version 2 (SLPv2)"
- [RFC4018] "Finding Internet Small Computer Systems Interface (iSCSI) Targets and Name Servers by Using Service Location Protocol version 2 (SLPv2)"
- [RFC4172] "iFCP - A Protocol for Internet Fibre Channel Storage Networking"
- [RFC4173] "Bootstrapping Clients using the Internet Small Computer System Interface (iSCSI) Protocol"
- [RFC4174] "The IPv4 Dynamic Host Configuration Protocol (DHCP) Option for the Internet Storage Name Service"
- [RFC5040] "A Remote Direct Memory Access Protocol Specification"
- [RFC5041] "Direct Data Placement over Reliable Transports"
- [RFC5042] "Direct Data Placement Protocol (DDP) / Remote Direct Memory Access Protocol (RDMAP) Security"
- [RFC5043] "Stream Control Transmission Protocol (SCTP) Direct Data Placement (DDP) Adaptation"

- [RFC5044] "Marker PDU Aligned Framing for TCP Specification"

- [RFC5045] "Applicability of Remote Direct Memory Access Protocol (RDMA) and Direct Data Placement (DDP)"

- [RFC5046] "Internet Small Computer System Interface (iSCSI) Extensions for Remote Direct Memory Access (RDMA)"

- [RFC5047] "DA: Datamover Architecture for the Internet Small Computer System Interface (iSCSI)"

- [RFC5048] "Internet Small Computer System Interface (iSCSI) Corrections and Clarifications"

[RFC3721] and [RFC5387] are not updated by this document, as their usage of RFC 3723 does not encompass its IPsec requirements.

In addition, these updated requirements apply to the new specifications for iSCSI ([I-D.ietf-storm-iscsi-cons]) and iSER ( [I-D.ietf-storm-iser]).

## 2. ESP Requirements

RFC 3723 requires that implementations MUST support IPsec ESPv2 [RFC2406] in tunnel mode as part of IPsec v2 to provide security for both control packets and data packets, and that when ESPv2 is utilized, per-packet data origin authentication, integrity and replay protection MUST be provided.

This document modifies RFC 3723 to require that implementations SHOULD also support IPsec ESPv3 [RFC4303] in tunnel mode as part of IPsec v3 to provide security for both control packets and data packets; per-packet data origin authentication, integrity and replay protection MUST be provided when ESPv3 is utilized.

In addition, at the high speeds at which IP storage protocols are expected to operate, a single IPsec SA could rapidly cycle through the ESP 32-bit sequence number space. In view of this, implementations that are capable of operating at speeds of 1 gigabit/second or higher and that implements both IKEv2 [RFC5996] and ESPv3 [RFC4303] MUST also implement extended (64-bit) sequence numbers for ESPv3 and SHOULD use ESPv3 extended sequence numbers for all security associations that protect IP storage protocol connections.

### 2.1. Data Origin Authentication and Data Integrity Transforms

RFC 3723 requires that:

- o HMAC-SHA1 MUST be implemented [RFC2404], and

- o AES CBC MAC with XCBC extensions SHOULD be implemented [RFC3566].

This document clarifies key sizes for the AES CBC MAC with XCBC extensions; 128-bit AES keys MUST be supported, and other key sizes MAY be supported. This document also adds a requirement for IPsec v3:

- o Implementations that support IKEv2 [RFC5996] SHOULD also implement AES GMAC [RFC4543] with 128-bit AES keys; other AES key sizes MAY be supported.

The rationale for the added requirement is that GMAC is more amenable to hardware implementations that may be preferable for the high data rates at which IP storage protocols can be expected to operate.

### 2.2. Confidentiality Transform Requirements

RFC 3723 requires that:

- o 3DES in CBC mode [RFC2451], [triple-des-spec] MUST be supported, and

- o AES in Counter mode [RFC3686], SHOULD be supported.

The 3DES-CBC requirement matched the basic encryption interoperability requirement for IPsec v2. At the time of RFC 3723's publication, AES Counter mode was the encryption transform that was most amenable to hardware implementation, as hardware implementation may be preferable for the high data rates at which IP storage protocols can be expected to operate.

This document changes both of these requirements based on cryptographic developments since the publication of RFC 3723. The requirement for 3DES CBC has become problematic due to 3DES's 64 bit block size, i.e., the core cipher encrypts or decrypts 64 bits at a time. Security weaknesses in encryption start to appear as the amount of data encrypted under a single key approaches the birthday bound of 32GB (gigabytes) for a cipher with a 64-bit block size [triple-des-birthday]. It is prudent to rekey well before that bound is reached, and 32GB or some significant fraction thereof is less than the amount of data that an IP Storage protocol may transfer in a single session. This may entail rather frequent rekeying, e.g., to obtain an order of magnitude (10x) safety margin by rekeying after 3GB on a multi-gigabit/sec link. In contrast, AES has a 128 bit block size, which results in an astronomical birthdaya bound (2^69 bytes). AES CBC is the primary mandatory-to-implement cryptographic

transform for interoperability, and hence is the appropriate replacement for 3DES CBC.

AES Counter mode is no longer the encryption transform that is most amenable to hardware implementation. That characterization now applies to AES Galois Counter Mode (GCM) [RFC4106], which provides both encryption and integrity protection in a single cryptographic mechanism (in contrast, neither of the RFC 3723 integrity transforms are well suited for hardware implementation, as they do not pipeline well). AES GCM is also capable of providing confidentiality protection for the IKEv2 key exchange protocol, but not the IKEv1 protocol [RFC5282], and therefore the new AES GCM "SHOULD" requirement is based on presence of support for IKEv2.

For the reasons described in the preceding paragraphs, the confidentiality transform requirements in RFC 3723 are replaced by the following:

- 3DES in CBC mode MAY be implemented,

- AES in Counter mode MAY be implemented,

- AES in CBC mode MUST be implemented with 128-bit keys; other key sizes MAY be supported, and

- Implementations that support IKEv2 SHOULD also implement AES GCM with 128-bit keys; other key sizes may be supported.

In addition, NULL encryption [RFC2410] MUST be implemented to enable use of SAs that provide data origin authentication and data integrity, but not confidentiality. Other transforms MAY be implemented in addition to those listed above.

## 3. IKEv1 and IKEv2 Requirements

Note: to avoid ambiguity, the original IKE protocol [RFC2409] is referred to as "IKEv1" in this document.

This document adds requirements for IKEv2 usage with IP Storage protocols and makes the following two changes to the IKEv1 requirements in RFC 3723:

- When DH groups are used, a DH group of at least 2048 bits SHOULD be offered as a part of all proposals to create IPsec Security Associations. Use of 1024 bit DH groups with 3DES CBC and HMAC-SHA1 is no longer recommended.

- The requirement to use UDP port 500 is removed in order to allow NAT traversal [RFC3947].

There are no other changes to RFC 3723's IKEv1 requirements, but many of them are restated in this document in order to provide context for the new IKEv2 requirements.

RFC 3723 requires that IKEv1 [RFC2409] be supported for peer authentication, negotiation of security associations, and key management, using the IPsec DOI [RFC2407], and further requires that manual keying not be used since it does not provide the rekeying support necessary for operation at high data rates. This document adds a requirement that IKEv2 [RFC5996] SHOULD be supported for peer authentication, negotiation of security associations, and key management. The manual keying prohibition in RFC 3723 is extended to IKEv2; manual keying MUST NOT be used with any version of IPsec for use with IP storage protocols.

RFC 3723's requirements for IKEv1 mode implementation and usage are unchanged; this document does not extend those requirements to IKEv2 because IKEv2 does not have modes.

When IPsec is used, the receipt of an IKEv1 Phase 2 delete message or an IKEv2 INFORMATIONAL exchange that deletes the SA SHOULD NOT be interpreted as a reason for tearing down the IP storage connection (e.g., TCP-based). If additional traffic is sent, a new SA will be created to protect that traffic.

The method used to determine whether an IP storage protocol connection should be established using IPsec is regarded as an issue of IPsec policy administration, and thus is not defined in this document. The method used by an implementation that supports both IPsec v2 and v3 to determine which versions of IPsec are supported by the an IP storage peer is also regarded as an issue of IPsec policy administration, and thus is also not defined in this document. If both IPsec v2 and v3 are supported by both endpoints of an IP storage connection, use of IPsec v3 is recommended.

### 3.1. Authentication Requirements

The authentication requirements for IKEv1 are unchanged by this document, but are restated here for context along with the authentication requirements for IKEv2:

a. Peer authentication using a pre-shared cryptographic key MUST be supported. Certificate-based peer authentication using digital signatures MAY be supported. For IKEv1 ([RFC2409]), peer authentication using the public key encryption methods outlined in sections 5.2 and 5.3 of [RFC2409] SHOULD NOT be used.

b. When digital signatures are used for authentication, all IKEv1 and IKEv2 negotiators SHOULD use Certificate Request Payload(s) to specify the certificate authority, and SHOULD check the pertinent Certificate Revocation List (CRL) before accepting a PKI certificate for use in authentication.

c. IKEv1 implementations MUST support Main Mode and SHOULD support Aggressive Mode. Main Mode with pre-shared key authentication method SHOULD NOT be used when either the initiator or the target uses dynamically assigned IP addresses. While in many cases pre-shared keys offer good security, situations in which dynamically assigned addresses are used force the use of a group pre-shared key, which creates vulnerability to a man-in-the-middle attack. These requirements do not apply to IKEv2 because it has no modes.

d. In the IKEv1 Phase 2 Quick Mode, exchanges for creating the Phase 2 SA, the Identification Payload MUST be present. This requirement does not apply to IKEv2 because it has no modes.

e. The following identification type requirements apply to IKEv1. ID_IPV4_ADDR, ID_IPV6_ADDR (if the protocol stack supports IPv6) and ID_FQDN Identification Types MUST be supported; ID_USER_FQDN SHOULD be supported. The IP Subnet, IP Address Range, ID_DER_ASN1_DN, and ID_DER_ASN1_GN Identification Types SHOULD NOT be used. The ID_KEY_ID Identification Type MUST NOT be used.

f. If IKEv2 is supported, the following identification requirements apply. ID_IPV4_ADDR, ID_IPV6_ADDR (if the protocol stack supports IPv6) and ID_FQDN Identification Types MUST be supported; ID_RFC822_ADDR SHOULD be supported. The ID_DER_ASN1_DN, and ID_DER_ASN1_GN Identification Types SHOULD NOT be used. The ID_KEY_ID Identification Type MUST NOT be used.

The reasons for the identification requirements in items e and f above are:

- IP Subnet and IP Address Range are too broad to usefully identify an iSCSI endpoint.

- The _DN and _GN types are X.500 identities; it is usually better to use an identity from subjectAltName in a PKI certificate.

- ID_KEY_ID is an opaque identifier that is not interoperable among different IPsec implementations as specified. Heterogeneity in some IP storage implementations can be expected (e.g., iSCSI initiator vs. iSCSI target implementations), and hence heterogeneity among IPsec implementations for IP storage is important.

### 3.2. D-H Group and PRF Requirements

This document does not change the support requirements for Diffe-Hellman (D-H) groups and Pseudo-Random Functions (PRFs). See [RFC4109] for IKEv1 requirements and [RFC4307] for IKEv2 requirements. Implementors are advised to check for subsequent RFCs that update either of these RFCs, as such updates may change these requirements.

When DH groups are used, a DH group of at least 2048 bits SHOULD be offered as a part of all proposals to create IPsec Security Associations for both IKEv1 and IKEv2.

RFC 3723 requires that that the IKEv1 Quick Mode key exchange that provides perfect forward secrecy MUST be implemented. This document extends that requirement to IKEv2; the CREATE_CHILD_SA key exchange that provides perfect forward secrecy MUST be implemented for use of IPsec with IP Storage protocols.

## 4. IANA Considerations

This document includes no request to IANA.

## 5. Security Considerations

This entire document is about security.

## 6. References

### 6.1. Normative References

[I-D.ietf-storm-iscsi-cons]
Chadalapaka, M., Satran, J., Meth, K., and D. Black, "iSCSI Protocol (Consolidated)", draft-ietf-storm-iscsi-cons-08 (work in progress), January 2013.

[I-D.ietf-storm-iser]
Ko, M. and A. Nezhinsky, "iSCSI Extensions for RDMA Specification", draft-ietf-storm-iser-14 (work in progress), June 2013.

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

[RFC2401] Kent, S. and R. Atkinson, "Security Architecture for the Internet Protocol", RFC 2401, November 1998.

[RFC2404] Madson, C. and R. Glenn, "The Use of HMAC-SHA-1-96 within ESP and AH", RFC 2404, November 1998.

[RFC2406] Kent, S. and R. Atkinson, "IP Encapsulating Security Payload (ESP)", RFC 2406, November 1998.

[RFC2407] Piper, D., "The Internet IP Security Domain of Interpretation for ISAKMP", RFC 2407, November 1998.

[RFC2409] Harkins, D. and D. Carrel, "The Internet Key Exchange (IKE)", RFC 2409, November 1998.

[RFC2410] Glenn, R. and S. Kent, "The NULL Encryption Algorithm and Its Use With IPsec", RFC 2410, November 1998.

[RFC2451] Pereira, R. and R. Adams, "The ESP CBC-Mode Cipher Algorithms", RFC 2451, November 1998.

[RFC3566] Frankel, S. and H. Herbert, "The AES-XCBC-MAC-96 Algorithm and Its Use With IPsec", RFC 3566, September 2003.

[RFC3686] Housley, R., "Using Advanced Encryption Standard (AES) Counter Mode With IPsec Encapsulating Security Payload (ESP)", RFC 3686, January 2004.

[RFC3720] Satran, J., Meth, K., Sapuntzakis, C., Chadalapaka, M., and E. Zeidner, "Internet Small Computer Systems Interface (iSCSI)", RFC 3720, April 2004.

[RFC3723] Aboba, B., Tseng, J., Walker, J., Rangan, V., and F. Travostino, "Securing Block Storage Protocols over IP", RFC 3723, April 2004.

[RFC3821] Rajagopal, M., Rodriguez, E., and R. Weber, "Fibre Channel Over TCP/IP (FCIP)", RFC 3821, July 2004.

[RFC3822] Peterson, D., "Finding Fibre Channel over TCP/IP (FCIP) Entities Using Service Location Protocol version 2 (SLPv2)", RFC 3822, July 2004.

[RFC3947] Kivinen, T., Swander, B., Huttunen, A., and V. Volpe, "Negotiation of NAT-Traversal in the IKE", RFC 3947, January 2005.

[RFC4018] Bakke, M., Hufferd, J., Voruganti, K., Krueger, M., and T. Sperry, "Finding Internet Small Computer Systems Interface (iSCSI) Targets and Name Servers by Using Service Location Protocol version 2 (SLPv2)", RFC 4018, April 2005.

[RFC4106] Viega, J. and D. McGrew, "The Use of Galois/Counter Mode (GCM) in IPsec Encapsulating Security Payload (ESP)", RFC 4106, June 2005.

[RFC4109] Hoffman, P., "Algorithms for Internet Key Exchange version 1 (IKEv1)", RFC 4109, May 2005.

[RFC4172] Monia, C., Mullendore, R., Travostino, F., Jeong, W., and M. Edwards, "iFCP - A Protocol for Internet Fibre Channel Storage Networking", RFC 4172, September 2005.

[RFC4173] Sarkar, P., Missimer, D., and C. Sapuntzakis, "Bootstrapping Clients using the Internet Small Computer System Interface (iSCSI) Protocol", RFC 4173, September 2005.

[RFC4174] Monia, C., Tseng, J., and K. Gibbons, "The IPv4 Dynamic Host Configuration Protocol (DHCP) Option for the Internet Storage Name Service", RFC 4174, September 2005.

[RFC4301] Kent, S. and K. Seo, "Security Architecture for the Internet Protocol", RFC 4301, December 2005.

[RFC4303] Kent, S., "IP Encapsulating Security Payload (ESP)", RFC 4303, December 2005.

[RFC4307] Schiller, J., "Cryptographic Algorithms for Use in the Internet Key Exchange Version 2 (IKEv2)", RFC 4307, December 2005.

[RFC4543] McGrew, D. and J. Viega, "The Use of Galois Message Authentication Code (GMAC) in IPsec ESP and AH", RFC 4543, May 2006.

[RFC5040] Recio, R., Metzler, B., Culley, P., Hilland, J., and D. Garcia, "A Remote Direct Memory Access Protocol Specification", RFC 5040, October 2007.

[RFC5041] Shah, H., Pinkerton, J., Recio, R., and P. Culley, "Direct Data Placement over Reliable Transports", RFC 5041, October 2007.

[RFC5042] Pinkerton, J. and E. Deleganes, "Direct Data Placement Protocol (DDP) / Remote Direct Memory Access Protocol (RDMAP) Security", RFC 5042, October 2007.

[RFC5043] Bestler, C. and R. Stewart, "Stream Control Transmission Protocol (SCTP) Direct Data Placement (DDP) Adaptation", RFC 5043, October 2007.

[RFC5044] Culley, P., Elzur, U., Recio, R., Bailey, S., and J. Carrier, "Marker PDU Aligned Framing for TCP Specification", RFC 5044, October 2007.

[RFC5048] Chadalapaka, M., "Internet Small Computer System Interface (iSCSI) Corrections and Clarifications", RFC 5048, October 2007.

[RFC5282] Black, D. and D. McGrew, "Using Authenticated Encryption Algorithms with the Encrypted Payload of the Internet Key Exchange version 2 (IKEv2) Protocol", RFC 5282, August 2008.

[RFC5996] Kaufman, C., Hoffman, P., Nir, Y., and P. Eronen, "Internet Key Exchange Protocol Version 2 (IKEv2)", RFC 5996, September 2010.

[triple-des-birthday]
McGrew, D., "Impossible plaintext cryptanalysis and probable-plaintext collision attacks of 64-bit block cipher modes (Cryptology ePrint Archive: Report 2012/623)", November 2012, <http://eprint.iacr.org/2012/623>.

[triple-des-spec]
American Bankers Association, ., "American National Standard for Financial Services X9.52-1998 - Triple Data Encryption Algorithm Modes of Operation", July 1998.

### 6.2. Informative References

[RFC3721] Bakke, M., Hafner, J., Hufferd, J., Voruganti, K., and M. Krueger, "Internet Small Computer Systems Interface (iSCSI) Naming and Discovery", RFC 3721, April 2004.

[RFC5045] Bestler, C. and L. Coene, "Applicability of Remote Direct Memory Access Protocol (RDMA) and Direct Data Placement (DDP)", RFC 5045, October 2007.

[RFC5046] Ko, M., Chadalapaka, M., Hufferd, J., Elzur, U., Shah, H., and P. Thaler, "Internet Small Computer System Interface (iSCSI) Extensions for Remote Direct Memory Access (RDMA)", RFC 5046, October 2007.

[RFC5047] Chadalapaka, M., Hufferd, J., Satran, J., and H. Shah, "DA: Datamover Architecture for the Internet Small Computer System Interface (iSCSI)", RFC 5047, October 2007.

[RFC5387] Touch, J., Black, D., and Y. Wang, "Problem and Applicability Statement for Better-Than-Nothing Security (BTNS)", RFC 5387, November 2008.

## Appendix A. Contributors

The original authors of RFC 3723 were: Bernard Aboba, Joshua Tseng, Jesse Walker, Venkat Rangan and Franco Travostino. Comments from Yaron Sheffer have improved this document and are gratefully acknowledged.

## Appendix B. Change Log

This section should be removed before this document is published as an RFC

Changes from -00 to -01:

- Make it clearer that RFC 3723's encryption transform implementation requirements are being changed.

- State that D-H group and PRF implementation requirements are unchanged and provide references to RFCs where they can be found (new section 3.2).

- Add requirements for perfect forward secrecy implementation (also in 3.2).

- Use the correct GMAC reference.

- Many other editorial changes.

## Authors' Addresses

David Black
EMC
176 South Street
Hopkinton, MA  01748
US

Phone: +1 508 293-7953
Email: david.black@emc.com

Paul Koning
Dell
300 Innovative Way
Nashua, NH  03062
US

Phone: +1 603 249-7703
Email: paul_koning@Dell.com