Internet Engineering Task Force (IETF)
Request for Comments: 6071
Obsoletes: 2411
Category: Informational
ISSN: 2070-1721

S. Frankel
NIST
S. Krishnan
Ericsson

February 2011

IP Security (IPsec) and Internet Key Exchange (IKE) Document Roadmap

Abstract

Over the past few years, the number of RFCs that define and use IPsec and Internet Key Exchange (IKE) has greatly proliferated. This is complicated by the fact that these RFCs originate from numerous IETF working groups: the original IPsec WG, its various spin-offs, and other WGs that use IPsec and/or IKE to protect their protocols' traffic.

This document is a snapshot of IPsec- and IKE-related RFCs. It includes a brief description of each RFC, along with background information explaining the motivation and context of IPsec's outgrowths and extensions. It obsoletes RFC 2411, the previous "IP Security Document Roadmap."

The obsoleted IPsec roadmap (RFC 2411) briefly described the interrelationship of the various classes of base IPsec documents. The major focus of RFC 2411 was to specify the recommended contents of documents specifying additional encryption and authentication algorithms.

Status of This Memo

This document is not an Internet Standards Track specification; it is published for informational purposes.

This document is a product of the Internet Engineering Task Force (IETF). It represents the consensus of the IETF community. It has received public review and has been approved for publication by the Internet Engineering Steering Group (IESG). Not all documents approved by the IESG are a candidate for any level of Internet Standard; see Section 2 of RFC 5741.

Information about the current status of this document, any errata, and how to provide feedback on it may be obtained at http://www.rfc-editor.org/info/rfc6071.

Table of Contents

1. Introduction

IPsec (Internet Protocol Security) is a suite of protocols that provides security to Internet communications at the IP layer. The most common current use of IPsec is to provide a Virtual Private Network (VPN), either between two locations (gateway-to-gateway) or between a remote user and an enterprise network (host-to-gateway); it can also provide end-to-end, or host-to-host, security. IPsec is also used by other Internet protocols (e.g., Mobile IP version 6 (MIPv6)) to protect some or all of their traffic. IKE (Internet Key Exchange) is the key negotiation and management protocol that is most commonly used to provide dynamically negotiated and updated keying material for IPsec. IPsec and IKE can be used in conjunction with both IPv4 and IPv6.

In addition to the base documents for IPsec and IKE, there are numerous RFCs that reference, extend, and in some cases alter the core specifications. This document obsoletes [RFC2411]. It attempts to list and briefly describe those RFCs, providing context and rationale where indicated. The title of each RFC is followed by a letter that indicates its category in the RFC series [RFC2026], as follows:

- S: Standards Track (Proposed Standard, Draft Standard, or Standard)
- E: Experimental
- B: Best Current Practice
- I: Informational

For each RFC, the publication date is also given.

This document also categorizes the requirements level of each cryptographic algorithm for use with IKEv1, IKEv2, IPsec-v2, and IPsec-v3. These requirements are summarized in Appendix A. These levels are current as of February 2011; subsequent RFCs may result in altered requirement levels.

This document does not define requirement levels; it simply restates those found in the IKE and IPsec RFCs. If there is a conflict between this document and any other RFC, then the other RFC takes precedence.

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. IPsec/IKE Background Information

2.1. Interrelationship of IPsec/IKE Documents

The main documents describing the set of IPsec protocols are divided into seven groups. This is illustrated in Figure 1. There is a main Architecture document that broadly covers the general concepts, security requirements, definitions, and mechanisms defining IPsec technology.

There are an Encapsulating Security Payload (ESP) Protocol document and an Authentication Header (AH) Protocol document that cover the packet format and general issues regarding the respective protocols. The "Encryption Algorithm" document set, shown on the left, is the set of documents describing how various encryption algorithms are used for ESP. The "Combined Algorithm" document set, shown in the middle, is the set of documents describing how various combined mode algorithms are used to provide both encryption and integrity protection for ESP. The "Integ-Protection Algorithm" document set, shown on the right, is the set of documents describing how various integrity-protection algorithms are used for both ESP and AH.

The "IKE" documents, shown at the bottom, are the documents describing the IETF Standards-Track key management schemes.

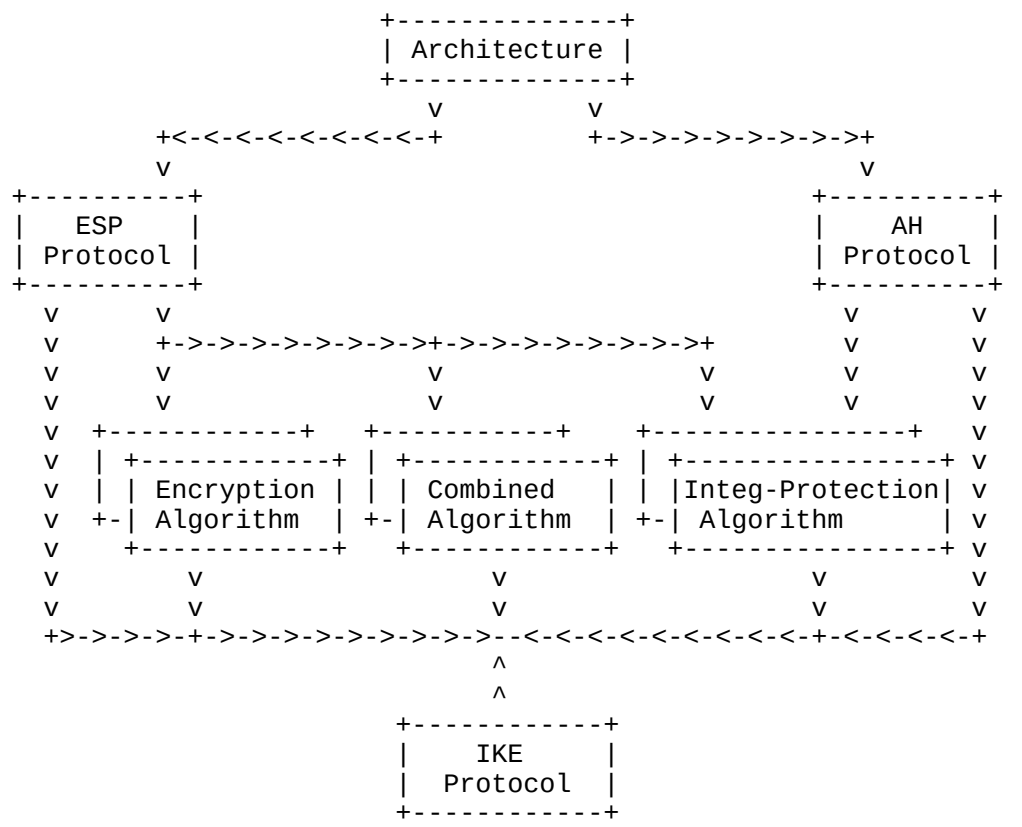

Figure 1. IPsec/IKE Document Interrelationships

2.2. Versions of IPsec

Two versions of IPsec can currently be found in implementations. The "new" IPsec (referred to as IPsec-v3 in this document; see Section 3.1.1 for the RFC descriptions) obsoleted the "old" IPsec (referred to as IPsec-v2 in this document; see Section 3.1.2 for the RFC descriptions); however, IPsec-v2 is still commonly found in operational use. In this document, when the unqualified term IPsec is used, it pertains to both versions of IPsec. An earlier version of IPsec (defined in RFCs 1825-1829), obsoleted by IPsec-v2, is not covered in this document.

2.2.1. Differences between "Old" IPsec (IPsec-v2) and "New" IPsec (IPsec-v3)

IPsec-v3 incorporates "lessons learned" from implementation and operational experience with IPsec-v2 and its predecessor, IPsec-v1.

Knowledge was gained about the barriers to IPsec deployment, the scenarios in which IPsec is most effective, and the requirements that needed to be added to IPsec to facilitate its use with other protocols. In addition, the documentation for IPsec-v3 clarifies and expands details that were underspecified or ambiguous in IPsec-v2.

Changes to the architecture document [RFC4301] include:

- More detailed descriptions of IPsec processing, both unicast and multicast, and the interactions among the various IPsec databases
- In IPsec-v2, an SA (Security Association) is uniquely identified by a combination of the SPI (Security Parameters Index), protocol (ESP or AH) and the destination address. In IPsec-v3, a unicast SA is uniquely identified by the SPI and, optionally, by the protocol; a multicast SA is identified by a combination of the SPI and the destination address and, optionally, the source address.
- More flexible SPD (Security Policy Database) selectors, including ranges of values and ICMP message types as selectors
- Decorrelated (order-independent) SAD (Security Association Database) replaced the former ordered SAD
- Extended sequence numbers (ESNs) were added
- Mandatory algorithms defined in standalone document
- AH [RFC4302] is mandatory to implement (MUST) in IPsec-v2, optional (MAY) in IPsec-v3

Changes to ESP [RFC4303] include:

- Combined mode algorithms were added, necessitating changes to packet format and processing
- NULL authentication, mandatory (MUST) in ESP-v2, is optional (MAY) in ESP-v3

2.3. Versions of IKE

Two versions of IKE can currently be found in implementations. The "new" IKE (generally referred to as IKEv2) obsoleted the "old" IKE (generally referred to as IKEv1); however, IKEv1 is still commonly found in operational use. In this document, when the unqualified term IKE is used, it pertains to both versions of IKE.

2.3.1. Differences between IKEv1 and IKEv2

As with IPsec-v3, IKEv2 incorporates "lessons learned" from implementation and operational experience with IKEv1. Knowledge was gained about the barriers to IKE deployment, the scenarios in which IKE is most effective, and the requirements that needed to be added to IKE to facilitate its use with other protocols as well as in general-purpose use. The documentation for IKEv2 replaces multiple, at times contradictory, documents with a single document; it also clarifies and expands details that were underspecified or ambiguous in IKEv1.

Once an IKE negotiation is successfully completed, the peers have established two pairs of one-way (inbound and outbound) SAs. Since IKE always negotiates pairs of SAs, the term "SA" is generally used to refer to a pair of SAs (e.g., an "IKE SA" or an "IPsec SA" is in reality a pair of one-way SAs). The first SA, the IKE SA, is used to protect IKE traffic. The second SA provides IPsec protection to data traffic between the peers and/or other devices for which the peers are authorized to negotiate. It is called the IPsec SA in IKEv1 and, in the IKEv2 RFCs, it is referred to variously as a CHILD_SA, a child SA, and an IPsec SA. This document uses the term "IPsec SA". To further complicate the terminology, since IKEv1 consists of two sequential negotiations, called phases, the IKE SA is also referred to as a Phase 1 SA and the IPsec SA is referred to as a Phase 2 SA.

Changes to IKE include:

- Replaced multiple alternate exchange types with a single, shorter exchange
- Streamlined negotiation format to avoid combinatorial bloat for multiple proposals
- Protect responder from committing significant resources to the exchange until the initiator’s existence and identity are confirmed
- Reliable exchanges: every request expects a response
- Protection of IKE messages based on ESP, rather than a method unique to IKE
- Add traffic selectors: distinct from peer IDs and more flexible
- Support of EAP-based authentication methods and asymmetric authentication (i.e., initiator and responder can use different authentication methods)

2.4. IPsec and IKE IANA Registries

Numerous IANA registries contain values that are used in IPsec, IKE, and related protocols. They include:

- IKE Attributes (http://www.iana.org/assignments/ipsec-registry): values used during IKEv1 Phase 1 exchanges, defined in [RFC2409].
- "Magic Numbers" for Internet Security Association and Key Management Protocol (ISAKMP) (http://www.iana.org/assignments/isakmp-registry): values used during IKEv1 Phase 2 exchanges, defined in [RFC2407], [RFC2408], and numerous other cryptographic algorithm RFCs.
- IKEv2 Parameters (http://www.iana.org/assignments/ikev2-parameters): values used in IKEv2 exchanges, defined in [RFC5996] and numerous other cryptographic algorithm RFCs.
- Cryptographic Suites for IKEv1, IKEv2, and IPsec (http://www.iana.org/assignments/crypto-suites): names of cryptographic suites in [RFC4308] and [RFC4869].

3. IPsec Documents

3.1. Base Documents

IPsec protections are provided by two special headers: the Encapsulating Security Payload (ESP) Header and the Authentication Header (AH). In IPv4, these headers take the form of protocol headers; in IPv6, they are classified as extension headers. There are three base IPsec documents: one that describes the IP security architecture, and one for each of the IPsec headers.

3.1.1. "Old" IPsec (IPsec-v2)

3.1.1.1. RFC 2401, Security Architecture for the Internet Protocol (S, November 1998)

[RFC2401] specifies the mechanisms, procedures, and components required to provide security services at the IP layer. It also describes their interrelationship and the general processing required to inject IPsec protections into the network architecture.

The components include:

- SA (Security Association): a one-way (inbound or outbound) agreement between two communicating peers that specifies the IPsec protections to be provided to their communications. This includes the specific security protections, cryptographic algorithms, and secret keys to be applied, as well as the specific types of traffic to be protected.

- SPI (Security Parameters Index): a value that, together with the destination address and security protocol (AH or ESP), uniquely identifies a single SA.

- SAD (Security Association Database): each peer's SA repository. The RFC describes how this database functions (SA lookup, etc.) and the types of information it must contain to facilitate SA processing; it does not dictate the format or layout of the database. SAs can be established in either transport mode or tunnel mode (see below).

- SPD (Security Policy Database): an ordered database that expresses the security protections to be afforded to different types and classes of traffic. The three general classes of traffic are traffic to be discarded, traffic that is allowed without IPsec protection, and traffic that requires IPsec protection.

RFC 2401 describes general inbound and outbound IPsec processing; it also includes details on several special cases: packet fragments, ICMP messages, and multicast traffic.

3.1.1.2. RFC 2402, IP Authentication Header (S, November 1998)

[RFC2402] defines the Authentication Header (AH), which provides integrity protection; it also provides data-origin authentication, access control, and, optionally, replay protection. A transport mode AH SA, used to protect peer-to-peer communications, protects upper-layer data, as well as those portions of the IP header that do not vary unpredictably during packet delivery. A tunnel mode AH SA can be used to protect gateway-to-gateway or host-to-gateway traffic; it can optionally be used for host-to-host traffic. This class of AH SA protects the inner (original) header and upper-layer data, as well as those portions of the outer (tunnel) header that do not vary unpredictably during packet delivery. Because portions of the IP header are not included in the AH calculations, AH processing is more complex than ESP processing. AH also does not work in the presence of Network Address Translation (NAT). Unlike IPsec-v3, IPsec-v2 classifies AH as mandatory to implement.

3.1.1.3. RFC 2406, IP Encapsulating Security Payload (ESP) (S, November 1998)

[RFC2406] defines the IP Encapsulating Security Payload (ESP), which provides confidentiality (encryption) and/or integrity protection; it also provides data-origin authentication, access control, and, optionally, replay and/or traffic analysis protection. A transport mode ESP SA protects the upper-layer data, but not the IP header. A tunnel mode ESP SA protects the upper-layer data and the inner header, but not the outer header.

3.1.2. "New" IPsec (IPsec-v3)

3.1.2.1. RFC 4301, Security Architecture for the Internet Protocol (S, December 2005)

[RFC4301] obsoletes [RFC2401], and it includes a more complete and detailed processing model. The most notable changes are detailed above in Section 2.2.1. IPsec-v3 processing incorporates an additional database:

- PAD (Peer Authorization Database): contains information necessary to conduct peer authentication, providing a link between IPsec and the key management protocol (e.g., IKE)

3.1.2.2. RFC 4302, IP Authentication Header (S, December 2005)

[RFC4302] obsoletes [RFC2402]. Unlike IPsec-v2, IPsec-v3 classifies AH as optional.

3.1.2.3. RFC 4303, IP Encapsulating Security Payload (ESP) (S, December 2005)

[RFC4303] obsoletes [RFC2406]. The most notable changes are detailed above in Section 2.2.1.

3.2. Additions to IPsec

Once the IKEv1 and IPsec-v2 RFCs were finalized, several additions were defined in separate documents: negotiation of NAT traversal, extended sequence numbers, UDP encapsulation of ESP packets, opportunistic encryption, and IPsec-related ICMP messages. Additional uses of IPsec transport mode were also described: protection of manually configured IPv6-in-IPv4 tunnels and protection of IP-in-IP tunnels. These documents describe atypical uses of IPsec transport mode, but do not define any new IPsec features.

Once the original IPsec Working Group concluded, additional IPsec-related issues were handled by the IPsecME (IPsec Maintenance and Extensions) Working Group. One such problem is the capability of middleboxes to distinguish unencrypted ESP packets (ESP-NULL) from encrypted ones in a fast and accurate manner. Two solutions are described: a new protocol that requires changes to IKEv2 and IPsec-v3 and a heuristic method that imposes no new requirements. Another issue that was addressed is the problem of using IKE and IPsec in a high-availability environment.

3.2.1. RFC 3947, Negotiation of NAT-Traversal in the IKE (S, January 2005)

[RFC3947] defines an optional extension to IKEv1. It enables IKEv1 to detect whether there are any NATs between the negotiating peers and whether both peers support NAT traversal. It also describes how IKEv1 can be used to negotiate the use of UDP encapsulation of ESP packets for the IPsec SA. For IKEv2, this capability is described in [RFC5996].

3.2.2. RFC 3948, UDP Encapsulation of IPsec ESP Packets (S, January 2005)

[RFC3948] is an optional extension for IPsec-v2 and IPsec-v3. It defines how to encapsulate ESP packets in UDP packets to enable the traversal of NATs that discard packets with protocols other than UDP or TCP. This makes it possible for ESP packets to pass through the NAT device without requiring any change to the NAT device itself. The use of this solution is negotiated by IKE, as described in [RFC3947] for IKEv1 and [RFC5996] for IKEv2.

3.2.3. RFC 4304, Extended Sequence Number (ESN) Addendum to IPsec Domain of Interpretation (DOI) for Internet Security Association and Key Management Protocol (ISAKMP) (S, December 2005)

The use of ESNs allows IPsec to use 64-bit sequence numbers for replay protection, but to send only 32 bits of the sequence number in the packet, enabling shorter packets and avoiding a redesign of the packet format. The larger sequence numbers allow an existing IPsec SA to be used for larger volumes of data. [RFC4304] describes an optional extension to IKEv1 that enables IKEv1 to negotiate the use of ESNs for IPsec SAs. For IKEv2, this capability is described in [RFC5996].

3.2.4. RFC 4322, Opportunistic Encryption using the Internet Key Exchange (IKE) (I, December 2005)

Opportunistic encryption allows a pair of end systems to use encryption without any specific pre-arrangements. [RFC4322] specifies a mechanism that uses DNS to distribute the public keys of each system involved and uses DNS Security (DNSSEC) to secure the mechanism against active attackers. It specifies the changes that are needed in existing IPsec and IKE implementations. The majority of the changes are needed in the IKE implementation and these changes relate to the handling of key acquisition requests, the lookup of public keys and TXT records, and the interactions with firewalls and other security facilities that may be co-resident on the same gateway.

3.2.5. RFC 4891, Using IPsec to Secure IPv6-in-IPv4 Tunnels (I, May 2007)

[RFC4891] describes how to use IKE and transport-mode IPsec to provide security protection to manually configured IPv6-in-IPv4 tunnels. This document uses standard IKE and IPsec, without any new extensions. It does not apply to tunnels that are initiated in an automated manner (e.g., 6to4 tunnels [RFC3056]).

3.2.6. RFC 3884, Use of IPsec Transport Mode for Dynamic Routing (I, September 2004)

[RFC3884] describes the use of transport-mode IPsec to secure IP-in-IP tunnels, which constitute the links of a multi-hop, distributed virtual network (VN). This allows the traffic to be dynamically routed via the VN's trusted routers, rather than routing all traffic through a statically routed IPsec tunnel. This RFC has not been widely adopted.

3.2.7. RFC 5840, Wrapped Encapsulating Security Payload (ESP) for Traffic Visibility (S, April 2010)

ESP, as defined in [RFC4303], does not allow a network device to easily determine whether protected traffic that is passing through the device is encrypted or only integrity protected (referred to as ESP-NULL packets). [RFC5840] extends ESPv3 to provide explicit notification of integrity-protected packets, and extends IKEv2 to negotiate this capability between the IPsec peers.

3.2.8. RFC 5879, Heuristics for Detecting ESP-NULL packets (I, May 2010)

[RFC5879] offers an alternative approach to differentiating between ESP-encrypted and ESP-NULL packets through packet inspection. This method does not require any change to IKE or ESP; it can be used with ESP-v2 or ESP-v3.

3.3. General Considerations

3.3.1. RFC 3715, IPsec-Network Address Translation (NAT) Compatibility Requirements (I, March 2004)

[RFC3715] "describes known incompatibilities between NAT and IPsec, and describes the requirements for addressing them". This is a critical issue, since IPsec is frequently used to provide VPN access to the corporate network for telecommuters, and NATs are widely deployed in home gateways, hotels, and other access networks typically used for remote access.

3.3.2. RFC 5406, Guidelines for Specifying the Use of IPsec Version 2 (B, February 2009)

[RFC5406] offers guidance to protocol designers on how to ascertain whether IPsec is the appropriate security mechanism to provide an interoperable security solution for the protocol. If this is not the case, it advises against attempting to define a new security protocol; rather, it suggests using another standards-based security protocol. The details in this document apply only to IPsec-v2.

3.3.3. RFC 2521, ICMP Security Failures Messages (E, March 1999)

[RFC2521] specifies an ICMP message for indicating failures related to the use of IPsec protocols (AH and ESP). The specified ICMP message defines several codes for handling common failure modes for IPsec. The failures that are signaled by this message include invalid or expired SPIs, failure of authenticity or integrity checks on datagrams, decryption and decompression errors, etc. These messages can be used to trigger automated session-key management or to signal to an operator the need to manually reconfigure the SAs. This RFC has not been widely adopted. Furthermore, [RFC4301] discusses the pros and cons of relying on unprotected ICMP messages.

3.3.4. RFC 6027, IPsec Cluster Problem Statement (I, October 2010)

[RFC6027] describes the problems of using IKE and IPsec in a high availability environment, in which one or both of the peers are clusters of gateways. It details the numerous types of stateful

information shared by IKE and IPsec peers that would have to be available to other members of the cluster in order to provide high-availability, load sharing, and/or failover capabilities.

4. IKE Documents

4.1. Base Documents

4.1.1. IKEv1

IKE is the preferred key management protocol for IPsec. It is used for peer authentication; to negotiate, modify, and delete SAs; and to negotiate authenticated keying material for use within those SAs. The standard peer authentication methods used by IKEv1 (pre-shared secret keys and digital certificates) had several shortcomings related to use of IKEv1 to enable remote user authentication to a corporate VPN: it could not leverage the use of legacy authentication systems (e.g. RADIUS databases) to authenticate a remote user to a security gateway; and it could not be used to configure remote users with network addresses or other information needed in order to access the internal network. Automatic key distribution is required for IPsec-v2, but alternatives to IKE may be used to satisfy that requirement.

Several Internet Drafts were written to address these problems: two such documents include "Extended Authentication within IKE (XAUTH)" [IKE-XAUTH] (and its predecessor, "Extended Authentication within ISAKMP/Oakley (XAUTH)" [ISAKMP-XAUTH]) and "The ISAKMP Configuration Method" [IKE-MODE-CFG] (and its predecessor [ISAKMP-MODE-CFG]). These Internet Drafts did not progress to RFC status due to security flaws and other problems related to these solutions. However, many current IKEv1 implementations incorporate aspects of these solutions to facilitate remote user access to corporate VPNs. These solutions were not standardized, and different implementations implemented different versions. Thus, there is no assurance that the implementations adhere fully to the suggested solutions or that one implementation can interoperate with others that claim to incorporate the same features. Furthermore, these solutions have known security issues. All of those problems and security issues have been solved in IKEv2; thus, use of these non-standardized IKEv1 solutions is not recommended.

4.1.1.1. RFC 2409, The Internet Key Exchange (IKE) (S, November 1998)

This document defines a key exchange protocol that can be used to negotiate authenticated keying material for SAs. This document implements a subset of the Oakley protocol in conjunction with ISAKMP to obtain authenticated keying material for use with ISAKMP, and for

other security associations such as AH and ESP for the IETF IPsec DOI. While, historically, IKEv1 was created by combining two security protocols, ISAKMP and Oakley, in practice, the combination (along with the IPsec DOI) has commonly been viewed as one protocol, IKEv1. The protocol's origins can be seen in the organization of the documents that define it.

4.1.1.2. RFC 2408, Internet Security Association and Key Management Protocol (ISAKMP) (S, November 1998)

This document defines procedures and packet formats to establish, negotiate, modify, and delete Security Associations (SAs). It is intended to support the negotiation of SAs for security protocols at all layers of the network stack. ISAKMP can work with many different key exchange protocols, each with different security properties.

4.1.1.3. RFC 2407, The Internet IP Security Domain of Interpretation for ISAKMP (S, November 1998)

Within ISAKMP, a Domain of Interpretation is used to group related protocols using ISAKMP to negotiate security associations. Security protocols sharing a DOI choose security protocol and cryptographic transforms from a common namespace and share key exchange protocol identifiers. This document defines the Internet IP Security DOI (IPSEC DOI), which instantiates ISAKMP for use with IP when IP uses ISAKMP to negotiate security associations.

4.1.1.4. RFC 2412, The OAKLEY Key Determination Protocol (I, November 1998)

[RFC2412] describes a key establishment protocol that two authenticated parties can use to agree on secure and secret keying material. The Oakley protocol describes a series of key exchanges -- called "modes" -- and details the services provided by each (e.g., perfect forward secrecy for keys, identity protection, and authentication). This document provides additional theory and background to explain some of the design decisions and security features of IKE and ISAKMP; it does not include details necessary for the implementation of IKEv1.

4.1.2. IKEv2

4.1.2.1. RFC 4306, Internet Key Exchange (IKEv2) Protocol (S, December 2005)

This document contains the original description of version 2 of the Internet Key Exchange (IKE) protocol. It covers what was previously covered by separate documents: ISAKMP, IKE, and DOI. It also

addresses NAT traversal, legacy authentication, and remote address acquisition. IKEv2 is not interoperable with IKEv1. Automatic key distribution is required for IPsec-v3, but alternatives to IKE may be used to satisfy that requirement. This document has been superseded by [RFC5996].

4.1.2.2. RFC 4718, IKEv2 Clarifications and Implementation Guidelines (I, October 2006)

[RFC4718] clarifies many areas of the original IKEv2 specification [RFC4306] that were seen as potentially difficult to understand for developers who were not intimately familiar with the specification and its history. It does not introduce any changes to the protocol, but rather provides descriptions that are less prone to ambiguous interpretations. The goal of this document was to encourage the development of interoperable implementations. The clarifications in this document have been included in the new version of the IKEv2 specification [RFC5996].

4.1.2.3. RFC 5996, Internet Key Exchange Protocol Version 2 (IKEv2) (S, September 2010)

[RFC5996] combines the original IKEv2 RFC [RFC4306] with the Clarifications RFC [RFC4718], and resolves many implementation issues discovered by the community since the publication of these two documents. This document was developed by the IPsecME (IPsec Maintenance and Extensions) Working Group, after the conclusion of the original IPsec Working Group. Automatic key distribution is required for IPsec-v3, but alternatives to IKE may be used to satisfy that requirement.

4.2. Additions and Extensions

4.2.1. Peer Authentication Methods

4.2.1.1. RFC 4478, Repeated Authentication in Internet Key Exchange (IKEv2) Protocol (E, April 2006)

[RFC4478] addresses a problem unique to remote access scenarios. How can the gateway (the IKE responder) force the remote user (the IKE initiator) to periodically reauthenticate, limiting the damage in the case where an unauthorized user gains physical access to the remote host? This document defines a new status notification, that a responder can send to an initiator, which notifies the initiator that the IPsec SA will be revoked unless the initiator reauthenticates within a specified period of time. This optional extension applies only to IKEv2, not to IKEv1.

4.2.1.2. RFC 4739, Multiple Authentication Exchanges in the Internet Key Exchange (IKEv2) Protocol (E, November 2006)

IKEv2 supports several mechanisms for authenticating the parties but each endpoint uses only one of these mechanisms to authenticate itself. [RFC4739] specifies an extension to IKEv2 that allows the use of multiple authentication exchanges, using either different mechanisms or the same mechanism. This extension allows, for instance, performing certificate-based authentication of the client host followed by an EAP authentication of the user. This also allows for authentication by multiple administrative domains, if needed. This optional extension applies only to IKEv2, not to IKEv1.

4.2.1.3. RFC 4754, IKE and IKEv2 Authentication Using the Elliptic Curve Digital Signature Algorithm (ECDSA) (S, January 2007)

[RFC4754] describes how the Elliptic Curve Digital Signature Algorithm (ECDSA) may be used as the authentication method within the IKEv1 and IKEv2 protocols. ECDSA provides many benefits including computational efficiency, small signature sizes, and minimal bandwidth compared to other available digital signature methods like RSA and DSA. This optional extension applies to both IKEv1 and IKEv2.

4.2.1.4. RFC 5998, An Extension for EAP-Only Authentication in IKEv2 (S, September 2010)

IKEv2 allows an initiator to use EAP for peer authentication, but requires the responder to authenticate through the use of a digital signature. [RFC5998] extends IKEv2 so that EAP methods that provide mutual authentication and key agreement can also be used to provide peer authentication for the responder. This optional extension applies only to IKEv2, not to IKEv1.

4.2.2. Certificate Contents and Management (PKI4IPsec)

The format, contents, and interpretation of Public Key Certificates (PKCs) proved to be a source of interoperability problems within IKE and IPsec. PKI4IPsec was an attempt to set in place some common procedures and interpretations to mitigate those problems.

4.2.2.1. RFC 4809, Requirements for an IPsec Certificate Management Profile (I, February 2007)

[RFC4809] enumerates requirements for Public Key Certificate (PKC) lifecycle transactions between different VPN System and PKI System products in order to better enable large scale, PKI-enabled IPsec

deployments with a common set of transactions. This document discusses requirements for both the IPsec and the PKI products. These optional requirements apply to both IKEv1 and IKEv2.

4.2.2.2. RFC 4945, The Internet IP Security PKI Profile of IKEv1/ISAKMP, IKEv2, and PKIX (S, August 2007)

[RFC4945] defines a profile of the IKE and Public Key Infrastructure using X.509 (PKIX) frameworks in order to provide an agreed-upon standard for using PKI technology in the context of IPsec. It also documents the contents of the relevant IKE payloads and further specifies their semantics. In addition, it summarizes the current state of implementations and deployment and provides advice to avoid common interoperability issues. This optional extension applies to both IKEv1 and IKEv2.

4.2.2.3. RFC 4806, Online Certificate Status Protocol (OCSP) Extensions to IKEv2 (S, February 2007)

When certificates are used with IKEv2, the communicating peers need a mechanism to determine the revocation status of the peer's certificate. OCSP is one such mechanism. [RFC4806] defines the "OCSP Content" extension to IKEv2. This document is applicable when OCSP is desired and security policy (e.g., firewall policy) prevents one of the IKEv2 peers from accessing the relevant OCSP responder directly. This optional extension applies only to IKEv2, not to IKEv1.

4.2.3. Dead Peer Detection

4.2.3.1. RFC 3706, A Traffic-Based Method of Detecting Dead Internet Key Exchange (IKE) Peers (I, February 2004)

When two peers communicate using IKE and IPsec, it is possible for the connectivity between the two peers to drop unexpectedly. But the SAs can still remain until their lifetimes expire, resulting in the packets getting tunneled into a "black hole". [RFC3706] describes an approach to detect peer liveliness without needing to send messages at regular intervals. This RFC defines an optional extension to IKEv1; dead peer detection (DPD) is an integral part of IKEv2, which refers to this feature as a "liveness check" or "liveness test".

4.2.4. Remote Access

The IKEv2 Mobility and Multihoming (MOBIKE) protocol enables two additional capabilities for IPsec VPN users: 1) moving from one address to another without re-establishing existing SAs and 2) using

multiple interfaces simultaneously. These solutions are limited to IPsec VPNs; they are not intended to provide more general mobility or multihoming capabilities.

The IPsecME Working Group identified some missing components needed for more extensive IKEv2 and IPsec-v3 support for remote access clients. These include efficient client resumption of a previously established session with a VPN gateway, efficient client redirection to an alternate VPN gateway, and support for IPv6 client configuration using IPsec configuration payloads.

4.2.4.1. RFC 4555, IKEv2 Mobility and Multihoming Protocol (MOBIKE) (S, June 2006)

IKEv2 assumes that an IKE SA is created implicitly between the IP address pair that is used during the protocol execution when establishing the IKEv2 SA. IPsec-related documents had no provision to change this pair after an IKE SA was created. [RFC4555] defines extensions to IKEv2 that enable an efficient management of IKE and IPsec Security Associations when a host possesses multiple IP addresses and/or where IP addresses of an IPsec host change over time.

4.2.4.2. RFC 4621, Design of the IKEv2 Mobility and Multihoming (MOBIKE) Protocol (I, August 2006)

[RFC4621] discusses the involved network entities and the relationship between IKEv2 signaling and information provided by other protocols. It also records design decisions for the MOBIKE protocol, background information, and records discussions within the working group.

4.2.4.3. RFC 5266, Secure Connectivity and Mobility Using Mobile IPv4 and IKEv2 Mobility and Multihoming (MOBIKE) (B, June 2008)

[RFC5266] describes a solution using Mobile IPv4 (MIPv4) and mobility extensions to IKEv2 (MOBIKE) to provide secure connectivity and mobility to enterprise users when they roam into untrusted networks.

4.2.4.4. RFC 5723, Internet Key Exchange Protocol Version 2 (IKEv2) Session Resumption (S, January 2010)

[RFC5723] enables a remote client that has been disconnected from a gateway to re-establish SAs with the gateway in an expedited manner, without repeating the complete IKEv2 negotiation. This capability requires changes to IKEv2. This optional extension applies only to IKEv2, not to IKEv1.

4.2.4.5. RFC 5685, Re-direct Mechanism for the Internet Key Exchange Protocol Version 2 (IKEv2) (S, November 2009)

[RFC5685] enables a gateway to securely redirect VPN clients to another VPN gateway, either during or after the IKEv2 negotiation. Possible reasons include, but are not limited to, an overloaded gateway or a gateway that needs to shut down. This requires changes to IKEv2. This optional extension applies only to IKEv2, not to IKEv1.

4.2.4.6. RFC 5739, IPv6 Configuration in Internet Key Exchange Protocol Version 2 (IKEv2) (E, February 2010)

In IKEv2, a VPN gateway can assign an internal network address to a remote VPN client. This is accomplished through the use of configuration payloads. For an IPv6 client, the assignment of a single address is not sufficient to enable full-fledged IPv6 communications. [RFC5739] proposes several solutions that might remove this limitation. This optional extension applies only to IKEv2, not to IKEv1.

5. Cryptographic Algorithms and Suites

Two basic requirements must be met for an algorithm to be used within IKE and/or IPsec: assignment of one or more IANA values and an RFC that describes how to use the algorithm within the relevant protocol, packet formats, special considerations, etc. For each RFC that describes a cryptographic algorithm, this roadmap will classify its requirement level for each protocol, as either MUST, SHOULD, or MAY [RFC2119]; SHOULD+, SHOULD-, or MUST- [RFC4835]; optional; undefined; or N/A (not applicable). A designation of "optional" means that the algorithm meets the two basic requirements, but its use is not specifically recommended for that protocol. "Undefined" means that one of the basic requirements is not met: either there is no relevant IANA number for the algorithm or there is no RFC specifying how it should be used within that specific protocol. "N/A" means that use of the algorithm is inappropriate in the context (e.g., NULL encryption for IKE, which always requires encryption; or combined mode algorithms, a new feature in IPsec-v3, for use with IPsec-v2).

This document categorizes the requirement level of each algorithm for IKEv1, IKEv2, IPsec-v2, and IPsec-v3. If an algorithm is recommended for use within IKEv1 or IKEv2, it is used either to protect the IKE SA’s traffic (encryption and integrity-protection algorithms) or to generate keying material (Diffie-Hellman or DH groups, Pseudorandom Functions or PRFs). If an algorithm is recommended for use within IPsec, it is used to protect the IPsec/child SA’s traffic, and IKE is capable of negotiating its use for that purpose. These requirements

are summarized in Table 1 (Appendix A). These levels are current as of February 2011; subsequent RFCs may result in altered requirement levels. For algorithms, this could mean the introduction of new algorithms or upgrading or downgrading the requirement levels of current algorithms.

The IANA registries for IKEv1 and IKEv2 include IANA values for various cryptographic algorithms. IKE uses these values to negotiate IPsec SAs that will provide protection using those algorithms. If a specific algorithm lacks a value for IKEv1 and/or IKEv2, that algorithm's use is classified as "undefined" (no IANA #) within IPsec-v2 and/or IPsec-v3.

5.1. Algorithm Requirements

Specifying a core set of mandatory algorithms for each protocol facilitates interoperability. Defining those algorithms in an RFC separate from the base protocol RFC enhances algorithm agility. IPsec-v3 and IKEv2 each have an RFC that specifies their mandatory-to-implement (MUST), recommended (SHOULD), optional (MAY), and deprecated (SHOULD NOT) algorithms. For IPsec-v2, this is included in the base protocol RFC. That was originally the case for IKEv1, but IKEv1's algorithm requirements were updated in [RFC4109].

5.1.1. RFC 4835, Cryptographic Algorithm Implementation Requirements for Encapsulating Security Payload (ESP) and Authentication Header (AH) (S, April 2007)

[RFC4835] specifies the encryption and integrity-protection algorithms for IPsec (both versions). Algorithms for IPsec-v2 were originally defined in [RFC2402] and [RFC2406]. [RFC4305] obsoleted those requirements, and was in turn obsoleted by [RFC4835]. Therefore, [RFC4835] applies to IPsec-v2 as well as IPsec-v3. Combined mode algorithms are mentioned, but not assigned a requirement level.

5.1.2. RFC 4307, Cryptographic Algorithms for Use in the Internet Key Exchange Version 2 (IKEv2) (S, December 2005)

[RFC4307] specifies the encryption and integrity-protection algorithms used by IKEv2 to protect its own traffic, the Diffie-Hellman (DH) groups used within IKEv2, and the pseudorandom functions used by IKEv2 to generate keys, nonces, and other random values. [RFC4307] contains conflicting requirements for IKEv2 encryption and integrity-protection algorithms. Where there are contradictory requirements, this document takes its requirement levels from Section

3.1.1, "Encrypted Payload Algorithms", rather than from Section 3.1.3, "IKEv2 Transform Type 1 Algorithms", or Section 3.1.4, "IKEv2 Transform Type 2 Algorithms".

5.1.3. RFC 4109, Algorithms for Internet Key Exchange version 1 (IKEv1) (S, May 2005)

[RFC4109] updates IKEv1's algorithm specifications, which were originally defined in [RFC2409]. It specifies the encryption and integrity-protection algorithms used by IKEv1 to protect its own traffic; the Diffie-Hellman (DH) groups used within IKEv1; the hash and pseudorandom functions used by IKEv1 to generate keys, nonces and other random values; and the authentication methods and algorithms used by IKEv1 for peer authentication.

5.2. Encryption Algorithms

The encryption-algorithm RFCs describe how to use these algorithms to encrypt IKE and/or ESP traffic, providing confidentiality protection to the traffic. They describe any special constraints, requirements, or changes to packet format appropriate for the specific algorithm. In general, they do not describe the detailed algorithmic computations; the reference section of each RFC includes pointers to documents that define the inner workings of the algorithm. Some of the RFCs include sample test data, to enable implementors to compare their results with standardized output.

When any encryption algorithm is used to provide confidentiality, the use of integrity protection is strongly recommended. If the encryption algorithm is a stream cipher, omitting integrity protection seriously compromises the security properties of the algorithm.

DES, as described in [RFC2405], was originally a required algorithm for IKEv1 and ESP-v2. Since the use of DES is now deprecated, this roadmap does not include [RFC2405].

5.2.1. RFC 2410, The NULL Encryption Algorithm and Its Use With IPsec (S, November 1998)

[RFC2410] is a tongue-in-cheek description of the no-op encryption algorithm (i.e., using ESP without encryption). In order for IKE to negotiate the selection of the NULL encryption algorithm for use in an ESP SA, an identifying IANA number is needed. This number (the value 11 for ESP_NULL) is found on the IANA registries for both IKEv1 and IKEv2, but it is not mentioned in [RFC2410].

Requirement levels for ESP-NULL:

IKEv1 - N/A
IKEv2 - N/A
ESP-v2 - MUST [RFC4835]
ESP-v3 - MUST [RFC4835]

NOTE: RFC 4307 erroneously classifies ESP-NULL as MAY for IKEv2; this has been corrected in an errata submission for RFC 4307.

5.2.2. RFC 2451, The ESP CBC-Mode Cipher Algorithms (S, November 1998)

[RFC2451] describes how to use encryption algorithms in cipher-block-chaining (CBC) mode to encrypt IKE and ESP traffic. It specifically mentions Blowfish, CAST-128, Triple DES (3DES), International Data Encryption Algorithm (IDEA), and RC5, but it is applicable to any block-cipher algorithm used in CBC mode. The algorithms mentioned in the RFC all have a 64-bit blocksize and a 64-bit random Initialization Vector (IV) that is sent in the packet along with the encrypted data.

Requirement levels for 3DES-CBC:

IKEv1 - MUST [RFC4109]
IKEv2 - MUST- [RFC4307]
ESP-v2 - MUST [RFC4835]
ESP-v3 - MUST- [RFC4835]

Requirement levels for other CBC algorithms (Blowfish, CAST, IDEA, RC5):

IKEv1 - optional
IKEv2 - optional
ESP-v2 - optional
ESP-v3 - optional

5.2.3. RFC 3602, The AES-CBC Cipher Algorithm and Its Use with IPsec (S, September. 2003)

[RFC3602] describes how to use AES in cipher block chaining (CBC) mode to encrypt IKE and ESP traffic. AES is the successor to DES. AES-CBC is a block-mode cipher with a 128-bit blocksize, a random IV that is sent in the packet along with the encrypted data, and keysizes of 128, 192 and 256 bits. If AES-CBC is implemented, 128-bit keys are MUST; the other sizes are MAY. [RFC3602] includes IANA values for use in IKEv1 and ESP-v2. A single IANA value is defined for AES-CBC, so IKE negotiations need to specify the keysize.

Requirement levels for AES-CBC with 128-bit keys:

IKEv1 - SHOULD [RFC4109]
IKEv2 - SHOULD+ [RFC4307]
ESP-v2 - MUST [RFC4835]
ESP-v3 - MUST [RFC4835]

Requirement levels for AES-CBC with 192- or 256-bit keys:

IKEv1 - optional
IKEv2 - optional
ESP-v2 - optional
ESP-v3 - optional

5.2.4. RFC 3686, Using Advanced Encryption Standard (AES) Counter Mode With IPsec Encapsulating Security Payload (ESP) (S, January 2004)

[RFC3686] describes how to use AES in counter (CTR) mode to encrypt ESP traffic. AES-CTR is a stream cipher with a 32-bit random nonce (1/SA) and a 64-bit IV. If AES-CTR is implemented, 128-bit keys are MUST; 192- and 256-byte keys are MAY. Reuse of the IV with the same key and nonce compromises the data's security; thus, AES-CTR should not be used with manual keying. AES-CTR can be pipelined and parallelized; it uses only the AES encryption operations for both encryption and decryption.

Requirement levels for AES-CTR:

IKEv1 - undefined (no IANA #)
IKEv2 - optional [RFC5930]
ESP-v2 - SHOULD [RFC4835]
ESP-v3 - SHOULD [RFC4835]

5.2.5. RFC 5930, Using Advanced Encryption Standard Counter Mode (AES-CTR) with the Internet Key Exchange version 02 (IKEv2) Protocol (I, July 210).

[RFC5930] extends [RFC3686] to enable the use of AES-CTR to provide encryption and integrity protection for IKEv2 messages.

5.2.6. RFC 4312, The Camellia Cipher Algorithm and Its Use with IPsec (S, December 2005)

[RFC4312] describes how to use Camellia in cipher block chaining (CBC) mode to encrypt IKE and ESP traffic. Camellia-CBC is a block-mode cipher with a 128-bit blocksize, a random IV that is sent in the packet along with the encrypted data, and keysizes of 128, 192, and

256 bits. If Camellia-CBC is implemented, 128-bit keys are MUST; the other sizes are MAY. [RFC4312] includes IANA values for use in IKEv1 and IPsec-v2. A single IANA value is defined for Camellia-CBC, so IKEv1 negotiations need to specify the keysize.

5.2.7. RFC 5529, Modes of Operation for Camellia for Use with IPsec (S, April 2009)

[RFC5529] describes the use of the Camellia block-cipher algorithm in conjunction with several different modes of operation. It describes the use of Camellia in cipher block chaining (CBC) mode and counter (CTR) mode as an encryption algorithm within ESP. It also describes the use of Camellia in Counter with CBC-MAC (CCM) mode as a combined mode algorithm in ESP. This document defines how to use IKEv2 to generate keying material for a Camellia ESP SA; it does not define how to use Camellia within IKEv2 to protect an IKEv2 SA's traffic. However, this RFC, in conjunction with IKEv2's generalized description of block-mode encryption, provide enough detail to allow the use of Camellia-CBC algorithms within IKEv2. All three modes can use keys of length 128 bits, 192 bits, or 256 bits. [RFC5529] includes IANA values for use in IKEv2 and IPsec-v3. A single IANA value is defined for each Camellia mode, so IKEv2 negotiations need to specify the keysize.

Requirement levels for Camellia-CBC:

- IKEv1 - optional
- IKEv2 - optional
- ESP-v2 - optional
- ESP-v3 - optional

Requirement levels for Camellia-CTR:

- IKEv1 - undefined (no IANA #)
- IKEv2 - undefined (no RFC)
- ESP-v2 - optional (but no IANA #, so cannot be negotiated by IKE)
- ESP-v3 - optional

Requirement levels for Camellia-CCM:

- IKEv1 - N/A
- IKEv2 - undefined (no RFC)
- ESP-v2 - N/A
- ESP-v3 - optional

5.2.8. RFC 4196, The SEED Cipher Algorithm and Its Use with IPsec (S, October 2005)

[RFC4196] describes how to use SEED in cipher block chaining (CBC) mode to encrypt ESP traffic. It describes how to use IKEv1 to negotiate a SEED-ESP SA, but does not define the use of SEED to protect IKEv1 traffic. SEED-CBC is a block-mode cipher with a 128-bit blocksize, a random IV that is sent in the packet along with the encrypted data, and a keysize of 128 bits. [RFC4196] includes IANA values for use in IKEv1 and IPsec-v2. [RFC4196] includes test data.

Requirement levels for SEED-CBC:

IKEv1 - undefined (no IANA #)
IKEv2 - undefined (no IANA #)
ESP-v2 - optional
ESP-v3 - optional (but no IANA #, so cannot be negotiated by IKE)

5.3. Integrity-Protection (Authentication) Algorithms

The integrity-protection algorithm RFCs describe how to use these algorithms to authenticate IKE and/or IPsec traffic, providing integrity protection to the traffic. This protection is provided by computing an Integrity Check Value (ICV), which is sent in the packet. The RFCs describe any special constraints, requirements, or changes to packet format appropriate for the specific algorithm. In general, they do not describe the detailed algorithmic computations; the reference section of each RFC includes pointers to documents that define the inner workings of the algorithm. Some of the RFCs include sample test data, to enable implementors to compare their results with standardized output.

Some of these algorithms generate a fixed-length ICV, which is truncated when it is included in an IPsec-protected packet. For example, standard HMAC-SHA-1 (Hashed Message Authentication Code) generates a 160-bit ICV, which is truncated to 96 bits when it is used to provide integrity protection to an ESP or AH packet. The individual RFC descriptions mention those algorithms that are truncated. When these algorithms are used to protect IKEv2 SAs, they are also truncated. For IKEv1, HMAC-SHA-1 and HMAC-MD5 are negotiated by requesting the hash algorithms SHA-1 and MD5, respectively; these algorithms are not truncated when used to protect an IKEv1 SA. For HMAC-SHA-1 and HMAC-MD5, the IKEv2 IANA registry contains values for both the truncated version and the standard non-truncated version; thus, IKEv2 has the capability to negotiate either version of the algorithm. However, only the truncated version is used for IKEv2 SAs and for IPsec SAs. The non-truncated version is

reserved for use by the Fibre Channel protocol [RFC4595]. For the other algorithms (AES-XCBC, HMAC-SHA-256/384/512, AES-CMAC, and HMAC-RIPEMD), only the truncated version can be used for both IKEv2 and IPsec-v3 SAs.

One other algorithm, AES-GMAC [RFC4543], can also provide integrity protection. It has two versions: an integrity-protection algorithm for use within AH-v3, and a combined mode algorithm with null encryption for use within ESP-v3. [RFC4543] is described in Section 5.4, "Combined Mode Algorithms".

5.3.1. RFC 2404, The Use of HMAC-SHA-1-96 within ESP and AH (S, November 1998)

[RFC2404] describes HMAC-SHA-1, an integrity-protection algorithm with a 512-bit blocksize, and a 160-bit key and Integrity Check Value (ICV). For use within IPsec, the ICV is truncated to 96 bits. This is currently the most commonly used integrity-protection algorithm.

Requirement levels for HMAC-SHA-1:

IKEv1 - MUST [RFC4109]
IKEv2 - MUST [RFC4307]
IPsec-v2 - MUST [RFC4835]
IPsec-v3 - MUST [RFC4835]

5.3.2. RFC 3566, The AES-XCBC-MAC-96 Algorithm and Its Use With IPsec (S, September 2003)

[RFC3566] describes AES-XCBC-MAC, a variant of CBC-MAC, which is secure for messages of varying lengths (unlike classic CBC-MAC). It is an integrity-protection algorithm with a 128-bit blocksize and a 128-bit key and ICV. For use within IPsec, the ICV is truncated to 96 bits. [RFC3566] includes test data.

Requirement levels for AES-XCBC-MAC:

IKEv1 - undefined (no RFC)
IKEv2 - optional
IPsec-v2 - SHOULD+ [RFC4835]
IPsec-v3 - SHOULD+ [RFC4835]

5.3.3. RFC 4868, Using HMAC-SHA-256, HMAC-SHA-384, and HMAC-SHA-512 with IPsec (S, May 2007)

[RFC4868] describes a family of algorithms, successors to HMAC-SHA-1. HMAC-SHA-256 has a 512-bit blocksize and a 256-bit key and ICV. HMAC-SHA-384 has a 1024-bit blocksize and a 384-bit key and ICV.

HMAC-SHA-512 has a 1024-bit blocksize and a 512-bit key and ICV. For use within IKE and IPsec, the ICV is truncated to half its original size (128 bits, 192 bits, or 256 bits). Each of the three algorithms has its own IANA value, so IKE does not have to negotiate the keysize.

Requirement levels for HMAC-SHA-256, HMAC-SHA-384, HMAC-SHA-512:

IKEv1 - optional
IKEv2 - optional
IPsec-v2 - optional
IPsec-v3 - optional

5.3.4. RFC 2403, The Use of HMAC-MD5-96 within ESP and AH (S, November 1998)

[RFC2403] describes HMAC-MD5, an integrity-protection algorithm with a 512-bit blocksize and a 128-bit key and Integrity Check Value (ICV). For use within IPsec, the ICV is truncated to 96 bits. It was a required algorithm for IKEv1 and IPsec-v2. The use of plain MD5 is now deprecated, but [RFC4835] states: "Weaknesses have become apparent in MD5; however, these should not affect the use of MD5 with HMAC".

Requirement levels for HMAC-MD5:

IKEv1 - MAY [RFC4109]
IKEv2 - optional [RFC4307]
IPsec-v2 - MAY [RFC4835]
IPsec-v3 - MAY [RFC4835]

5.3.5. RFC 4494, The AES-CMAC-96 Algorithm and Its Use with IPsec (S, June 2006)

[RFC4494] describes AES-CMAC, another variant of CBC-MAC, which is secure for messages of varying lengths. It is an integrity-protection algorithm with a 128-bit blocksize and 128-bit key and ICV. For use within IPsec, the ICV is truncated to 96 bits. [RFC4494] includes test data.

Requirement levels for AES-CMAC:

IKEv1 - undefined (no IANA #)
IKEv2 - optional
IPsec-v2 - optional (but no IANA #, so cannot be negotiated by IKE)
IPsec-v3 - optional

5.3.6. RFC 2857, The Use of HMAC-RIPEMD-160-96 within ESP and AH (S, June 2000)

[RFC2857] describes HMAC-RIPEMD, an integrity-protection algorithm with a 512-bit blocksize and a 160-bit key and ICV. For use within IPsec, the ICV is truncated to 96 bits.

Requirement levels for HMAC-RIPEMD:

IKEv1 - undefined (no IANA #)
IKEv2 - undefined (no IANA #)
IPsec-v2 - optional
IPsec-v3 - optional (but no IANA #, so cannot be negotiated by IKE)

5.3.7. RFC 4894, Use of Hash Algorithms in Internet Key Exchange (IKE) and IPsec (I, May 2007)

In light of recent attacks on MD5 and SHA-1, [RFC4894] examines whether it is necessary to replace the hash functions currently used by IKE and IPsec for key generation, integrity protection, digital signatures, or PKIX certificates. It concludes that the algorithms recommended for IKEv2 [RFC4307] and IPsec-v3 [RFC4305] are not currently susceptible to any known attacks. Nonetheless, it suggests that implementors add support for AES-XCBC-MAC-96 [RFC3566], AES-XCBC-PRF-128 [RFC4434], and HMAC-SHA-256, -384, and -512 [RFC4868] for future use. It also suggests that IKEv2 implementors add support for PKIX certificates signed with SHA-256, -384, and -512.

5.4. Combined Mode Algorithms

IKEv1 and ESP-v2 use separate algorithms to provide encryption and integrity protection, and IKEv1 can negotiate different combinations of algorithms for different SAs. In ESP-v3, a new class of algorithms was introduced, in which a single algorithm can provide both encryption and integrity protection. [RFC5996] describes how IKEv2 can negotiate combined mode algorithms to be used in ESP-v3 SAs. [RFC5282] adds that capability to IKEv2, enabling IKEv2 to negotiate and use combined mode algorithms for its own traffic. When properly designed, these algorithms can provide increased efficiency in both implementation and execution.

Although ESP-v2 did not originally include combined mode algorithms, some IKEv1 implementations have added the capability to negotiate combined mode algorithms for use in IPsec SAs; these implementations do not include the capability to use combined mode algorithms to protect IKE SAs. IANA numbers for combined mode algorithms have been added to the IKEv1 registry.

5.4.1. RFC 4309, Using Advanced Encryption Standard (AES) CCM Mode with IPsec Encapsulating Security Payload (ESP) (S, December 2005)

[RFC4309] describes how to use AES in counter with CBC-MAC (CCM) mode, a combined algorithm, to encrypt and integrity protect ESP traffic. AES-CCM is a block-mode cipher with a 128-bit blocksize; a random IV that is sent in the packet along with the encrypted data; a 24-bit salt value (1/SA); keysizes of 128, 192, and 256 bits and ICV sizes of 64, 96 and 128 bits. If AES-CCM is implemented, 128-bit keys are MUST; the other sizes are MAY. ICV sizes of 64 and 128 bits are MUST; 96 bits is MAY. The salt value is generated by IKE during the key-generation process. Reuse of the IV with the same key compromises the data's security; thus, AES-CCM should not be used with manual keying. [RFC4309] includes IANA values that IKE can use to negotiate ESP-v3 SAs. Each of the three ICV lengths has its own IANA value, but IKE negotiations need to specify the keysize. [RFC4309] includes test data. [RFC4309] describes how IKE can negotiate the use of AES-CCM to use in an ESP SA. [RFC5282] extends this to the use of AES-CCM to protect an IKEv2 SA.

Requirement levels for AES-CCM:

IKEv1 - N/A
IKEv2 - optional
ESP-v2 - N/A
ESP-v3 - optional [RFC4835]

NOTE: The IPsec-v2 IANA registry includes values for AES-CCM, but combined mode algorithms are not a feature of IPsec-v2. Although some IKEv1/IPsec-v2 implementations include this capability (see Section 5.4), it is not part of the protocol.

5.4.2. RFC 4106, The Use of Galois/Counter Mode (GCM) in IPsec Encapsulating Security Payload (ESP) (S, June 2005)

[RFC4106] describes how to use AES in Galois/Counter (GCM) mode, a combined algorithm, to encrypt and integrity protect ESP traffic. AES-GCM is a block-mode cipher with a 128-bit blocksize; a random IV that is sent in the packet along with the encrypted data; a 32-bit salt value (1/SA); keysizes of 128, 192, and 256 bits; and ICV sizes of 64, 96, and 128 bits. If AES-GCM is implemented, 128-bit keys are MUST; the other sizes are MAY. An ICV size of 128 bits is a MUST; 64 and 96 bits are MAY. The salt value is generated by IKE during the key-generation process. Reuse of the IV with the same key compromises the data's security; thus, AES-GCM should not be used with manual keying. [RFC4106] includes IANA values that IKE can use to negotiate ESP-v3 SAs. Each of the three ICV lengths has its own IANA value, but IKE negotiations need to specify the keysize.

[RFC4106] includes test data. [RFC4106] describes how IKE can negotiate the use of AES-GCM to use in an ESP SA. [RFC5282] extends this to the use of AES-GCM to protect an IKEv2 SA.

Requirement levels for AES-GCM:

IKEv1 - N/A
IKEv2 - optional
ESP-v2 - N/A
ESP-v3 - optional [RFC4835]

NOTE: The IPsec-v2 IANA registry includes values for AES-GCM, but combined mode algorithms are not a feature of IPsec-v2. Although some IKEv1/IPsec-v2 implementations include this capability (see Section 5.4), it is not part of the protocol.

5.4.3. RFC 4543, The Use of Galois Message Authentication Code (GMAC) in IPsec ESP and AH (S, May 2006)

[RFC4543] is the variant of AES-GCM [RFC4106] that provides integrity protection without encryption. It has two versions: an integrity-protection algorithm for use within AH, and a combined mode algorithm with null encryption for use within ESP. It can use a key of 128-, 192-, or 256-bits; the ICV is always 128 bits, and is not truncated. AES-GMAC uses a nonce, consisting of a 64-bit IV and a 32-bit salt (1/SA). The salt value is generated by IKE during the key generation process. Reuse of the salt value with the same key compromises the data's security; thus, AES-GMAC should not be used with manual keying. For use within AH, each keysize has its own IANA value, so IKE does not have to negotiate the keysize. For use within ESP, there is only one IANA value, so IKE negotiations must specify the keysize. AES-GMAC cannot be used by IKE to protect its own SAs, since IKE traffic requires encryption.

Requirement levels for AES-GMAC:

IKEv1 - N/A
IKEv2 - N/A
IPsec-v2 - N/A
IPsec-v3 - optional

NOTE: The IPsec-v2 IANA registry includes values for AES-GMAC, but combined mode algorithms are not a feature of IPsec-v2. Although some IKEv1/IPsec-v2 implementations include this capability (see Section 5.4), it is not part of the protocol.

5.4.4. RFC 5282, Using Authenticated Encryption Algorithms with the Encrypted Payload of the Internet Key Exchange version 2 (IKEv2) Protocol (S, August 2008)

[RFC5282] extends [RFC4309] and [RFC4106] to enable the use of AES-CCM and AES-GCM to provide encryption and integrity protection for IKEv2 messages.

5.5. Pseudo-Random Functions (PRFs)

IKE uses pseudorandom functions (PRFs) to generate the secret keys that are used in IKE SAs and IPsec SAs. These PRFs are generally the same algorithms used for integrity protection, but their output is not truncated, since all of the generated bits are generally needed for the keys. If the PRF's output is not long enough to supply the required number of bits of keying material, the PRF is applied iteratively until the requisite amount of keying material is generated.

For each IKEv2 SA, the peers negotiate both a PRF algorithm and an integrity-protection algorithm; the former is used to generate keying material and other values, and the latter is used to provide protection to the IKE SA's traffic.

IKEv1's approach is more complicated. IKEv1 [RFC2409] does not specify any PRF algorithms. For each IKEv1 SA, the peers agree on an unkeyed hash function (e.g., SHA-1). IKEv1 uses the HMAC version of this function to generate keying material and to provide integrity protection for the IKE SA. Therefore, PRFs that are not HMACs cannot currently be used in IKEv1.

Requirement levels for PRF-HMAC-SHA1:

IKEv1 - MUST [RFC4109]
IKEv2 - MUST [RFC4307]

Requirement levels for PRF-HMAC-SHA-256, PRF-HMAC-SHA-384, and PRF-HMAC-SHA-512:

IKEv1 - optional [RFC4868]
IKEv2 - optional [RFC4868]

5.5.1. RFC 4434, The AES-XCBC-PRF-128 Algorithm for the Internet Key Exchange Protocol (IKE) (S, February 2006)

[RFC3566] defines AES-XCBC-MAC-96, which is used for integrity protection within IKE and IPsec. [RFC4434] enables the use of AES-XCBC-MAC as a PRF within IKE. The PRF differs from the integrity-

protection algorithm in two ways: its 128-bit output is not truncated to 96 bits, and it accepts a variable-length key, which is modified (lengthened via padding or shortened through application of AES-XCBC) to a 128-bit key. [RFC4434] includes test data.

Requirement levels for AES-XCBC-PRF:

IKEv1 - undefined (no RFC)
IKEv2 - SHOULD+ [RFC4307]

NOTE: RFC 4109 erroneously classifies AES-XCBC-PRF as SHOULD for IKEv1; this has been corrected in an errata submission for RFC 4109.

5.5.2. RFC 4615, The Advanced Encryption Standard-Cipher-based Message Authentication Code-Pseudorandom Function-128 (AES-CMAC-PRF-128) Algorithm for the Internet Key Exchange Protocol (IKE) (S, August 2006)

[RFC4615] extends [RFC4494] to enable the use of AES-CMAC as a PRF within IKEv2, in a manner analogous to that used by [RFC4434] for AES-XCBC.

Requirement levels for AES-CMAC-PRF:

IKEv1 - undefined (no IANA #)
IKEv2 - optional

5.6. Cryptographic Suites

5.6.1. RFC 4308, Cryptographic Suites for IPsec (S, December 2005)

An IKE negotiation consists of multiple cryptographic attributes, both for the IKE SA and for the IPsec SA. The number of possible combinations can pose a challenge to peers trying to find a common policy. To enhance interoperability, [RFC4308] defines two pre-defined suites, consisting of combinations of algorithms that comprise typical security policies. IKE/ESP suite "VPN-A" includes use of 3DES, HMAC-SHA-1, and 1024-bit modular exponentiation group (MODP) Diffie-Hellman (DH); IKE/ESP suite "VPN-B" includes AES-CBC, AES-XCBC-MAC, and 2048-bit MODP DH. These suites are intended to be named "single-button" choices in the administrative interface, but do not prevent the use of alternative combinations.

5.6.2. RFC 4869, Suite B Cryptographic Suites for IPsec (I, May 2007)

[RFC4869] adds four pre-defined suites, based upon the United States National Security Agency’s "Suite B" specifications, to those specified in [RFC4308]. IKE/ESP suites "Suite-B-GCM-128" and "Suite-

B-GCM-256" include use of AES-CBC, AES-GCM, HMAC-SHA-256, or HMAC-SHA-384, and 256-bit or 384-bit elliptic-curve (EC) DH groups. IKE/AH suites "Suite-B-GMAC-128" and "Suite-B-GMAC-256" include use of AES-CBC, AES-GMAC, HMAC-SHA-256, or HMAC-SHA-384, and 256-bit or 384-bit EC DH groups. While [RFC4308] does not specify a peer-authentication method, [RFC4869] mandates pre-shared key authentication for IKEv1; public key authentication using ECDSA is recommended for IKEv1 and required for IKEv2.

5.7. Diffie-Hellman Algorithms

IKE negotiations include a Diffie-Hellman exchange, which establishes a shared secret to which both parties contributed. This value is used to generate keying material to protect both the IKE SA and the IPsec SA.

IKEv1 [RFC2409] contains definitions of two DH MODP groups and two elliptic curve (EC) groups; IKEv2 [RFC5996] only references the MODP groups. The requirements levels of these groups are:

Requirement levels for DH MODP group 1:

IKEv1 - MAY [RFC4109]
IKEv2 - optional

Requirement levels for DH MODP group 2:

IKEv1 - MUST [RFC4109]
IKEv2 - MUST- [RFC4307]

Requirement levels for EC groups 3-4:

IKEv1 - MAY [RFC4109]
IKEv2 - undefined (no IANA #)

5.7.1. RFC 3526, More Modular Exponential (MODP) Diffie-Hellman groups for Internet Key Exchange (IKE) (S, May 2003)

[RFC2409] and [RFC5996] define two MODP DH groups (groups 1 and 2) for use within IKE. [RFC3526] adds six more groups (groups 5 and 14-18). Group 14 is a 2048-bit group that is strongly recommended for use in IKE.

Requirement levels for DH MODP group 14:

IKEv1 - SHOULD [RFC4109]
IKEv2 - SHOULD+ [RFC4307]

Requirement levels for DH MODP groups 5, 15-18:

IKEv1 - optional [RFC4109]
IKEv2 - optional

5.7.2. RFC 4753, ECP Groups For IKE and IKEv2 (I, January 2007)

[RFC4753] defines three EC DH groups (groups 19-21) for use within IKE.

The document includes test data.

Requirement levels for DH EC groups 19-21:

IKEv1 - optional [RFC4109]
IKEv2 - optional

5.7.3. RFC 5903, Elliptic Curve Groups modulo a Prime (ECP Groups) for IKE and IKEv2 (I, June 2010)

[RFC5903] obsoletes [RFC4753], fixing an inconsistency in the DH shared secret value.

5.7.4. RFC 5114, Additional Diffie-Hellman Groups for Use with IETF Standards (I, January 2008)

[RFC5114] defines five additional DH groups (MODP groups 22-24 and EC groups 25-26) for use in IKE. It also includes three EC DH groups (groups 19-21) that were originally defined in [RFC4753]; however, the current specification for these groups is [RFC5903]. The IANA group numbers are specific to IKE, but the DH groups are intended for use in multiple IETF protocols, including Transport Layer Security/Secure Socket Layer (TLS/SSL), Secure/Multipurpose Internet Mail Extensions (S/MIME), and X.509 Certificates.

Requirement levels for DH MODP groups 22-24, EC groups 25-26:

IKEv1 - optional
IKEv2 - optional

6. IPsec/IKE for Multicast

[RFC4301] describes IPsec processing for unicast and multicast traffic. However, classical IPsec SAs provide point-to-point protection; the security afforded by IPsec’s cryptographic algorithms is not applicable when the SA is one-to-many or many-to-many, the case for multicast. The Multicast Security (msec) Working Group has defined alternatives to IKE and extensions to IPsec for use with

multicast traffic. Different multicast groups have differing characteristics and requirements: number of senders (one-to-many or many-to-many), number of members (few, moderate, very large), volatility of membership, real-time delivery, etc. Their security requirements vary as well. Each solution defined by msec applies to a subset of the large variety of possible multicast groups.

6.1. RFC 3740, The Multicast Group Security Architecture (I, March 2004)

[RFC3740] defines the multicast security architecture, which is used to provide security for packets exchanged by large multicast groups. It defines the components of the architectural framework; discusses Group Security Associations (GSAs), key management, data handling, and security policies. Several existing protocols, including Group DOI (GDOI) [RFC3547], Group Secure Association Key Management Protocol (GSAKMP) [RFC4535], and Multimedia Internet KEYing (MIKEY) [RFC3830], satisfy the group key management requirements defined in this document. Both the architecture and the components for Multicast Group Security differ from IPsec.

6.2. RFC 5374, Multicast Extensions to the Security Architecture for the Internet Protocol (S, November 2008)

[RFC5374] extends the security architecture defined in [RFC4301] to apply to multicast traffic. It defines a new class of SAs (GSAs - Group Security Associations) and additional databases used to apply IPsec protection to multicast traffic. It also describes revisions and additions to the processing algorithms in [RFC4301].

6.3. RFC 3547, The Group Domain of Interpretation (S, July 2003)

GDOI [RFC3547] extends IKEv1 so that it can be used to establish SAs to protect multicast traffic. This document defines additional exchanges and payloads to be used for that purpose.

6.4. RFC 4046, Multicast Security (MSEC) Group Key Management Architecture (I, April 2005)

[RFC4046] sets out the general requirements and design principles for protocols that are used for multicast key management. It does not go into the specifics of an individual protocol that can be used for that purpose.

6.5. RFC 4359, The Use of RSA/SHA-1 Signatures within Encapsulating Security Payload (ESP) and Authentication Header (AH) (S, January 2006)

[RFC4359] describes the use of the RSA digital signature algorithm to provide integrity protection for multicast traffic within ESP and AH. The algorithms used for integrity protection for unicast traffic (e.g., HMAC) are not suitable for this purpose when used with multicast traffic.

7. Outgrowths of IPsec/IKE

Operational experience with IPsec revealed additional capabilities that could make IPsec more useful in real-world scenarios. These include support for IPsec policy mechanisms, IPsec MIBs, payload compression (IPComp), extensions to facilitate additional peer authentication methods (Better-Than-Nothing Security (BTNS), Kerberized Internet Negotiation of Keys (KINK), and IPSECKEY), and additional capabilities for VPN clients (IPSRA).

7.1. IPsec Policy

The IPsec Policy (ipsp) Working Group originally planned an RFC that would allow entities with no common Trust Anchor and no prior knowledge of each other's security policies to establish an IPsec-protected connection. The solutions that were proposed for gateway discovery and security policy negotiation proved to be overly complex and fragile, in the absence of prior knowledge or compatible configuration policies.

7.1.1. RFC 3586, IP Security Policy (IPSP) Requirements (S, August 2003)

[RFC3586] describes the functional requirements of a generalized IPsec policy framework, that could be used to discover, negotiate, and manage IPsec policies.

7.1.2. RFC 3585, IPsec Configuration Policy Information Model (S, August 2003)

As stated in [RFC3585]:

> This document presents an object-oriented information model of IP Security (IPsec) policy designed to facilitate agreement about the content and semantics of IPsec policy, and enable derivations of task-specific representations of IPsec policy such as storage schema, distribution representations, and policy specification languages used to configure IPsec-enabled endpoints.

This RFC has not been widely adopted.

7.2. IPsec MIBs

Over the years, several MIB-related Internet Drafts were proposed for IPsec and IKE, but only one progressed to RFC status.

7.2.1. RFC 4807, IPsec Security Policy Database Configuration MIB (S, March 2007)

[RFC4807] defines a MIB module that can be used to configure the SPD of an IPsec device. This RFC has not been widely adopted.

7.3. IPComp (Compression)

The IP Payload Compression Protocol (IPComp) is a protocol that provides lossless compression for IP datagrams. Although IKE can be used to negotiate the use of IPComp in conjunction with IPsec, IPComp can also be used when IPsec is not applied.

The IPComp protocol allows the compression of IP datagrams by supporting different compression algorithms. Three of these algorithms are: DEFLATE [RFC2394], LZS [RFC2395], and the ITU-T V.44 Packet Method [RFC3051], which is based on the LZJH algorithm.

7.3.1. RFC 3173, IP Payload Compression Protocol (IPComp) (S, September 2001)

IP payload compression is especially useful when IPsec-based encryption is applied to IP datagrams. Encrypting the IP datagram causes the data to be random in nature, rendering compression at lower protocol layers ineffective. If IKE is used to negotiate compression in conjunction with IPsec, compression can be performed prior to encryption. [RFC3173] defines the payload compression protocol, the IPComp packet structure, the IPComp Association (IPCA), and several methods to negotiate the IPCA.

7.4. Better-Than-Nothing Security (BTNS)

One of the major obstacles to widespread implementation of IPsec is the lack of pre-existing credentials that can be used for peer authentication. Better-Than-Nothing Security (BTNS) is an attempt to sidestep this problem by allowing IKE to negotiate unauthenticated (anonymous) IPsec SAs, using credentials such as self-signed certificates or "bare" public keys (public keys that are not connected to a public key certificate) for peer authentication. This ensures that subsequent traffic protected by the SA is conducted with

the same peer, and protects the communications from passive attack. These SAs can then be cryptographically bound to a higher-level application protocol, which performs its own peer authentication.

7.4.1. RFC 5660, IPsec Channels: Connection Latching (S, October 2009)

[RFC5660] specifies, abstractly, how to interface applications and transport protocols with IPsec so as to create channels by latching connections (packet flows) to certain IPsec Security Association (SA) parameters for the lifetime of the connections. Connection latching is layered on top of IPsec and does not modify the underlying IPsec architecture.

7.4.2. RFC 5386, Better-Than-Nothing-Security: An Unauthenticated Mode of IPsec (S, November 2008)

[RFC5386] specifies how to use IKEv2 to set up unauthenticated security associations (SAs) for use with the IPsec Encapsulating Security Payload (ESP) and the IPsec Authentication Header (AH). This document does not require any changes to the bits on the wire, but specifies extensions to the Peer Authorization Database (PAD) and Security Policy Database (SPD).

7.4.3. RFC 5387, Problem and Applicability Statement for Better-Than-Nothing Security (BTNS) (I, November 2008)

[RFC5387] considers that the need to deploy authentication information and its associated identities is a significant obstacle to the use of IPsec. This document explains the rationale for extending the Internet network security protocol suite to enable use of IPsec security services without authentication.

7.5. Kerberized Internet Negotiation of Keys (KINK)

Kerberized Internet Negotiation of Keys (KINK) is an attempt to provide an alternative to IKE for IPsec peer authentication. It uses Kerberos, instead of IKE, to establish IPsec SAs. For enterprises that already deploy the Kerberos centralized key management system, IPsec can then be implemented without the need for additional peer credentials. Some vendors have implemented proprietary extensions for using Kerberos in IKEv1, as an alternative to the use of KINK. These extensions, as well as the KINK protocol, apply only to IKEv1, and not to IKEv2.

7.5.1. RFC 3129, Requirements for Kerberized Internet Negotiation of Keys (I, June 2001)

[RFC3129] considers that peer-to-peer authentication and keying mechanisms have inherent drawbacks such as computational complexity and difficulty in enforcing security policies. This document specifies the requirements for using basic features of Kerberos and uses them to its advantage to create a protocol that can establish and maintain IPsec security associations ([RFC2401]).

7.5.2. RFC 4430, Kerberized Internet Negotiation of Keys (KINK) (S, March 2006)

[RFC4430] defines a low-latency, computationally inexpensive, easily managed, and cryptographically sound protocol to establish and maintain security associations using the Kerberos authentication system. This document reuses the Quick Mode payloads of IKEv1 in order to foster substantial reuse of IKEv1 implementations. This RFC has not been widely adopted.

7.6. IPsec Secure Remote Access (IPSRA)

IPsec Secure Remote Access (IPSRA) was an attempt to extend IPsec protection to "road warriors", allowing IKE to authenticate not only the user's device but also the user, without changing IKEv1. The working group defined generic requirements of different IPsec remote access scenarios. An attempt was made to define an IKE-like protocol that would use legacy authentication mechanisms to create a temporary or short-lived user credential that could be used for peer authentication within IKE. This protocol proved to be more cumbersome than standard Public Key protocols, and was abandoned. This led to the development of IKEv2, which incorporates the use of EAP for user authentication.

7.6.1. RFC 3457, Requirements for IPsec Remote Access Scenarios (I, January 2003)

[RFC3457] explores and enumerates the requirements of various IPsec remote access scenarios, without suggesting particular solutions for them.

7.6.2. RFC 3456, Dynamic Host Configuration Protocol (DHCPv4) Configuration of IPsec Tunnel Mode (S, January 2003)

[RFC3456] explores the requirements for host configuration in IPsec tunnel mode, and describes how the Dynamic Host Configuration Protocol (DHCPv4) may be used for providing such configuration information. This RFC has not been widely adopted.

7.7. IPsec Keying Information Resource Record (IPSECKEY)

The IPsec Keying Information Resource Record (IPSECKEY) enables the storage of public keys and other information that can be used to facilitate opportunistic IPsec in a new type of DNS resource record.

7.7.1. RFC 4025, A method for storing IPsec keying material in DNS (S, February 2005)

[RFC4025] describes a method of storing IPsec keying material in the DNS using a new type of resource record. This document describes how to store the public key of the target node in this resource record. This RFC has not been widely adopted.

8. Other Protocols That Use IPsec/IKE

IPsec and IKE were designed to provide IP-layer security protection to other Internet protocols' traffic as well as generic communications. Since IPsec is a general-purpose protocol, in some cases, its features do not provide the granularity or distinctive features required by another protocol; in some cases, its overhead or prerequisites do not match another protocol's requirements. However, a number of other protocols do use IKE and/or IPsec to protect some or all of their communications.

8.1. Mobile IP (MIPv4 and MIPv6)

8.1.1. RFC 4093, Problem Statement: Mobile IPv4 Traversal of Virtual Private Network (VPN) Gateways (I, August 2005)

[RFC4093] describes the issues with deploying Mobile IPv4 across virtual private networks (VPNs). IPsec is one of the VPN technologies covered by this document. It identifies and describes practical deployment scenarios for Mobile IPv4 running alongside IPsec in enterprise and operator environments. It also specifies a set of framework guidelines to evaluate proposed solutions for supporting multi-vendor seamless IPv4 mobility across IPsec-based VPN gateways.

8.1.2. RFC 5265, Mobile IPv4 Traversal across IPsec-Based VPN Gateways (S, June 2008)

[RFC5265] describes a basic solution that uses Mobile IPv4 and IPsec to provide session mobility between enterprise intranets and external networks. The proposed solution minimizes changes to existing firewall/VPN/DMZ deployments and does not require any changes to IPsec or key exchange protocols. It also proposes a mechanism to minimize IPsec renegotiation when the mobile node moves.

8.1.3. RFC 3776, Using IPsec to Protect Mobile IPv6 Signaling Between Mobile Nodes and Home Agents (S, June 2004)

This document specifies the use of IPsec in securing Mobile IPv6 traffic between mobile nodes and home agents. It specifies the required wire formats for the protected packets and illustrates examples of Security Policy Database and Security Association Database entries that can be used to protect Mobile IPv6 signaling messages. It also describes how to configure either manually keyed IPsec security associations or IKEv1 to establish the SAs automatically. Mobile IPv6 requires considering the home address destination option and Routing Header in IPsec processing. Also, IPsec and IKE security association addresses can be updated by Mobile IPv6 signaling messages.

8.1.4. RFC 4877, Mobile IPv6 Operation with IKEv2 and the Revised IPsec Architecture (S, April 2007)

This document updates [RFC3776] in order to work with the revised IPsec architecture [RFC4301]. Since the revised IPsec architecture expands the list of selectors to include the Mobility Header message type, it becomes much easier to differentiate between different mobility header messages. Since the ICMP message type and code are also newly added as selectors, this document uses them to protect Mobile Prefix Discovery messages. This document also specifies the use of IKEv2 configuration payloads for dynamic home address configuration. Finally, this document describes the use of IKEv2 in order to set up the SAs for Mobile IPv6.

8.1.5. RFC 5026, Mobile IPv6 Bootstrapping in Split Scenario (S, October 2007)

[RFC5026] extends [RFC4877] to support dynamic discovery of home agents and the home network prefix; for the latter purpose, it specifies a new IKEv2 configuration attribute and notification. It describes how a Mobile IPv6 node can obtain the address of its home agent, its home address, and create IPsec security associations with its home agent using DNS lookups and security credentials preconfigured on the Mobile Node. It defines how a mobile node (MN) can request its home address and home prefixes through the Configuration Payload in the IKE_AUTH exchange and what attributes need to be present in the CFG_REQUEST messages in order to do this. It also specifies how the home agent can authorize the credentials used for IKEv2 exchange.

8.1.6. RFC 5213, Proxy Mobile IPv6 (S, August 2008)

[RFC5213] describes a network-based mobility management protocol that is used to provide mobility services to hosts without requiring their participation in any mobility-related signaling. It uses IPsec to protect the mobility signaling messages between the two network entities called the mobile access gateway (MAG) and the local mobility anchor (LMA). It also uses IKEv2 in order to set up the security associations between the MAG and the LMA.

8.1.7. RFC 5568, Mobile IPv6 Fast Handovers (S, July 2009)

When Mobile IPv6 is used for a handover, there is a period during which the Mobile Node is unable to send or receive packets because of link switching delay and IP protocol operations. [RFC5568] specifies a protocol between the Previous Access Router (PAR) and the New Access Router (NAR) to improve handover latency due to Mobile IPv6 procedures. It uses IPsec ESP in transport mode with integrity protection for protecting the signaling messages between the PAR and the NAR. It also describes the SPD entries and the PAD entries when IKEv2 is used for setting up the required SAs.

8.1.8. RFC 5380, Hierarchical Mobile IPv6 (HMIPv6) Mobility Management (S, October 2008)

[RFC5380] describes extensions to Mobile IPv6 and IPv6 Neighbor Discovery to allow for local mobility handling in order to reduce the amount of signaling between the mobile node, its correspondent nodes, and its home agent. It also improves handover speed of Mobile IPv6. It uses IPsec for protecting the signaling between the mobile node and a local mobility management entity called the Mobility Anchor Point (MAP). The MAP also uses IPsec Peer Authorization Database (PAD) entries and configuration payloads described in [RFC4877] in order to allocate a Regional Care-of Address (RCoA) for mobile nodes.

8.2. Open Shortest Path First (OSPF)

8.2.1. RFC 4552, Authentication/Confidentiality for OSPFv3 (S, June 2006)

OSPF is a link-state routing protocol that is designed to be run inside a single Autonomous System. OSPFv2 provided its own authentication mechanisms using the AuType and Authentication protocol header fields but OSPFv3 removed these fields and uses IPsec instead. [RFC4552] describes how to use IPsec ESP and AH in order to protect OSPFv3 signaling between two routers. It also enumerates the IPsec capabilities the routers require in order to support this specification. Finally, it also describes the operation of OSPFv3

with IPsec over virtual links where the other endpoint is not known at configuration time. Since OSPFv3 exchanges multicast packets as well as unicast ones, the use of IKE within OSPFv3 is not appropriate. Therefore, this document mandates the use of manual keys.

8.3. Host Identity Protocol (HIP)

8.3.1. RFC 5201, Host Identity Protocol (E, April 2008)

IP addresses perform two distinct functions: host identifier and locator. This document specifies a protocol that allows consenting hosts to securely establish and maintain shared IP-layer state, allowing separation of the identifier and locator roles of IP addresses. This enables continuity of communications across IP address (locator) changes. It uses public key identifiers from a new Host Identity (HI) namespace for peer authentication. It uses the HMAC-SHA-1-96 and the AES-CBC algorithms with IPsec ESP and AH for protecting its signaling messages.

8.3.2. RFC 5202, Using the Encapsulating Security Payload (ESP) Transport Format with the Host Identity Protocol (HIP) (E, April 2008)

The HIP base exchange specification [RFC5201] does not describe any transport formats or methods for describing how ESP is used to protect user data to be used during the actual communication. [RFC5202] specifies a set of HIP extensions for creating a pair of ESP Security Associations (SAs) between the hosts during the base exchange. After the HIP association and required ESP SAs have been established between the hosts, the user data communication is protected using ESP. In addition, this document specifies how the ESP Security Parameter Index (SPI) is used to indicate the right host context (host identity) and methods to update an existing ESP Security Association.

8.3.3. RFC 5206, End-Host Mobility and Multihoming with the Host Identity (E, April 2008)

When a host uses HIP, the overlying protocol sublayers (e.g., transport layer sockets) and Encapsulating Security Payload (ESP) Security Associations (SAs) are bound to representations of these host identities, and the IP addresses are only used for packet forwarding. [RFC5206] defines a generalized LOCATOR parameter for use in HIP messages that allows a HIP host to notify a peer about alternate addresses at which it is reachable. It also specifies how a host can change its IP address and continue to send packets to its peers without necessarily rekeying.

8.3.4. RFC 5207, NAT and Firewall Traversal Issues of Host Identity Protocol (HIP) (I, April 2008)

[RFC5207] discusses the problems associated with HIP communication across network paths that include network address translators and firewalls. It analyzes the impact of NATs and firewalls on the HIP base exchange and the ESP data exchange. It discusses possible changes to HIP that attempt to improve NAT and firewall traversal and proposes a rendezvous point for letting HIP nodes behind a NAT be reachable. It also suggests mechanisms for NATs to be more aware of the HIP messages.

8.4. Stream Control Transmission Protocol (SCTP)

8.4.1. RFC 3554, On the Use of Stream Control Transmission Protocol (SCTP) with IPsec (S, July 2003)

The Stream Control Transmission Protocol (SCTP) is a reliable transport protocol operating on top of a connection-less packet network such as IP. [RFC3554] describes functional requirements for IPsec and IKE to be used in securing SCTP traffic. It adds support for SCTP in the form of a new ID type in IKE [RFC2409] and implementation choices in the IPsec processing to account for the multiple source and destination addresses associated with a single SCTP association. This document applies only to IKEv1 and IPsec-v2; it does not apply to IKEv2 AND IPsec-v3.

8.5. Robust Header Compression (ROHC)

8.5.1. RFC 3095, RObust Header Compression (ROHC): Framework and four profiles: RTP, UDP, ESP, and uncompressed (S, July 2001)

ROHC is a framework for header compression, intended to be used in resource-constrained environments. [RFC3095] applies this framework to four protocols, including ESP.

8.5.2. RFC 5225, RObust Header Compression Version 2 (ROHCv2): Profiles for RTP, UDP, IP, ESP, and UDP-Lite (S, April 2008)

[RFC5225] defines an updated ESP/IP profile for use with ROHC version 2. It analyzes the ESP header and classifies the fields into several classes like static, well-known, irregular, etc., in order to efficiently compress the headers.

8.5.3. RFC 5856, Integration of Robust Header Compression over IPsec Security Associations (I, May 2010)

[RFC5856] describes a mechanism to compress inner IP headers at the ingress point of IPsec tunnels and to decompress them at the egress point. Since the Robust Header Compression (ROHC) specifications only describe operations on a per-hop basis, this document also specifies extensions to enable ROHC over multiple hops. This document applies only to tunnel mode SAs and does not support transport mode SAs.

8.5.4. RFC 5857, IKEv2 Extensions to Support Robust Header Compression over IPsec (S, May 2010)

ROHC requires initial configuration at the compressor and decompressor ends. Since ROHC usually operates on a per-hop basis, this configuration information is carried over link-layer protocols such as PPP. Since [RFC5856] operates over multiple hops, a different signaling mechanism is required. [RFC5857] describes how to use IKEv2 in order to dynamically communicate the configuration parameters between the compressor and decompressor.

8.5.5. RFC 5858, IPsec Extensions to Support Robust Header Compression over IPsec (S, May 2010)

[RFC5856] describes how to use ROHC with IPsec. This is not possible without extensions to IPsec. [RFC5858] describes the extensions needed to IPsec in order to support ROHC. Specifically, it describes extensions needed to the IPsec SPD, SAD, and IPsec processing including ICV computation and integrity verification.

8.6. Border Gateway Protocol (BGP)

8.6.1. RFC 5566, BGP IPsec Tunnel Encapsulation Attribute (S, June 2009)

[RFC5566] adds an additional BGP Encapsulation Subsequent Address Family Identifier (SAFI), allowing the use of IPsec and, optionally, IKE to protect BGP tunnels. It defines the use of AH and ESP in tunnel mode and the use of AH and ESP in transport mode to protect IP in IP and MPLS-in-IP tunnels. It also defines how public key fingerprints (hashes) are distributed via BGP and used later to authenticate IKEv2 exchange between the tunnel endpoints.

8.7. IPsec Benchmarking

The Benchmarking Methodology WG in the IETF is working on documents that relate to benchmarking IPsec [BMWG-1] [BMWG-2].

8.7.1. Methodology for Benchmarking IPsec Devices (Work in Progress)

[BMWG-1] defines a set of tests that can be used to measure and report the performance characteristics of IPsec devices. It extends the methodology defined for benchmarking network interconnecting devices to include IPsec gateways and adds further tests that can be used to measure IPsec performance of end-hosts. The document focuses on establishing a performance testing methodology for IPsec devices that support manual keying and IKEv1, but does not cover IKEv2.

8.7.2. Terminology for Benchmarking IPsec Devices (Work in Progress)

[BMWG-2] defines the standardized performance testing terminology for IPsec devices that support manual keying and IKEv1. It also describes the benchmark tests that would be used to test the performance of the IPsec devices.

8.8. Network Address Translators (NAT)

8.8.1. RFC 2709, Security Model with Tunnel-mode IPsec for NAT domains (I, October 1999)

NAT devices provide transparent routing to end-hosts trying to communicate from disparate address realms, by modifying IP and transport headers en route. This makes it difficult for applications to pursue end-to-end application-level security. [RFC2709] describes a security model by which tunnel mode IPsec security can be architected on NAT devices. It defines how NATs administer security policies and SA attributes based on private realm addressing. It also specifies how to operate IKE in such scenarios by specifying an IKE-ALG (Application Level Gateway) that translates policies from private realm addressing into public addressing. Although the model presented here uses terminology from IKEv1, it can be deployed within IKEv1, IKEv2, IPsec-v2, and IPsec-v3. This security model has not been widely adopted

8.9. Session Initiation Protocol (SIP)

8.9.1. RFC 3329, Security Mechanism Agreement for the Session Initiation Protocol (SIP) (S, January 2003)

[RFC3329] describes how a SIP client can select one of the various available SIP security mechanisms. In particular, the method allows secure negotiation to prevent bidding down attacks. It also describes a security mechanism called ipsec-3gpp and its associated parameters (algorithms, protocols, mode, SPIs and ports) as they are used in the 3GPP IP Multimedia Subsystem.

8.10. Explicit Packet Sensitivity Labels

8.10.1. RFC 5570, Common Architecture Label IPv6 Security Option (CALIPSO) (I, July 2009)

[RFC5570] describes a mechanism used to encode explicit packet Sensitivity Labels on IPv6 packets in Multi-Level Secure (MLS) networks. The method is implemented using an IPv6 hop-by-hop option. This document uses the IPsec Authentication Header (AH) in order to detect any malicious modification of the Sensitivity Label in a packet.

9. Other Protocols That Adapt IKE for Non-IPsec Functionality

Some protocols protect their traffic through mechanisms other than IPsec, but use IKEv2 as a basis for their key negotiation and key management functionality.

9.1. Extensible Authentication Protocol (EAP)

9.1.1. RFC 5106, The Extensible Authentication Protocol-Internet Key Exchange Protocol version 2 (EAP-IKEv2) Method (E, February 2008)

[RFC5106] specifies an Extensible Authentication Protocol (EAP) method that is based on the Internet Key Exchange version 2 (IKEv2) protocol. EAP-IKEv2 provides mutual authentication and session-key establishment between an EAP peer and an EAP server. It describes the full EAP-IKEv2 message exchange and the composition of the protocol messages.

9.2. Fibre Channel

9.2.1. RFC 4595, Use of IKEv2 in the Fibre Channel Security Association Management Protocol (I, July 2006)

Fibre Channel (FC) is a gigabit-speed network technology used for Storage Area Networking. The Fibre Channel Security Protocols (FC-SP) standard has adapted the IKEv2 protocol [RFC4306] to provide authentication of Fibre Channel entities and setup of security associations. Since IP is transported over Fibre Channel and Fibre Channel is transported over IP, there is the potential for confusion when IKEv2 is used for both IP and FC traffic. [RFC4595] specifies identifiers for IKEv2 over FC in a fashion that ensures that any mistaken usage of IKEv2/FC over IP or IKEv2/IP over FC will result in a negotiation failure due to the absence of an acceptable proposal.

9.3. Wireless Security

9.3.1. RFC 4705, GigaBeam High-Speed Radio Link Encryption (I, October 2006)

[RFC4705] describes the encryption and key management used by GigaBeam as part of the WiFiber(tm) family of radio-link products and is intended to serve as a guideline for similar wireless product development efforts to include comparable capabilities. It specifies the algorithms that are used to provide confidentiality and integrity protection of both subscriber and management traffic. It also specifies a custom security protocol that runs between two Gigabeam Radio Control Modules (RCMs).

10. Acknowledgements

The authors would like to thank Yaron Sheffer, Paul Hoffman, Yoav Nir, Rajeshwar Singh Jenwar, Alfred Hoenes, Al Morton, Gabriel Montenegro, Sean Turner, Julien Laganier, Grey Daley, Scott Moonen, Richard Graveman, Tero Kivinen, Pasi Eronen, Ran Atkinson, David Black, and Tim Polk for reviewing this document and suggesting changes.

11. Security Considerations

This RFC serves as a review of other documents and introduces no new security considerations itself; however, please see each of the individual documents described herein for security considerations related to each protocol.

12. References

12.1. Informative References

[BMWG-1] Kaeo, M. and T. Van Herck, "Methodology for Benchmarking IPsec Devices", Work in Progress, July 2009.

[BMWG-2] Kaeo, M., Van Herck T., and M. Bustos, "Terminology for Benchmarking IPsec Devices", Work in Progress, July 2009.

[IKE-MODE-CFG] Dukes, D. and R. Pereira, "The ISAKMP Configuration Method", Work in Progress, September 2001.

[IKE-XAUTH] Beaulieu, S. and R. Pereira, "Extended Authentication within IKE (XAUTH)", Work in Progress, October 2001.

[ISAKMP-MODE-CFG]
Pereira, R., Anand, S., and B. Patel, "The ISAKKMP Configuration Method", Work in Progress, August 1999.

[ISAKMP-XAUTH]
Pereira, R. and S. Beaulieu, "Extended Authentication within ISAKMP/Oakley (XAUTH)", Work in Progress, December 1999.

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

[RFC2026] Bradner, S., "The Internet Standards Process -- Revision 3", BCP 9, RFC 2026, October 1996.

[RFC2394] Pereira, R., "IP Payload Compression Using DEFLATE", RFC 2394, December 1998.

[RFC2395] Friend, R. and R. Monsour, "IP Payload Compression Using LZS", RFC 2395, December 1998.

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

[RFC2402] Kent, S. and R. Atkinson, "IP Authentication Header", RFC 2402, November 1998.

[RFC2403] Madson, C. and R. Glenn, "The Use of HMAC-MD5-96 within ESP and AH", RFC 2403, November 1998.

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

[RFC2405] Madson, C. and N. Doraswamy, "The ESP DES-CBC Cipher Algorithm With Explicit IV", RFC 2405, 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.

[RFC2408] Maughan, D., Schertler, M., Schneider, M., and J. Turner, "Internet Security Association and Key Management Protocol (ISAKMP)", RFC 2408, 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.

[RFC2411] Thayer, R., Doraswamy, N., and R. Glenn, "IP Security Document Roadmap", RFC 2411, November 1998.

[RFC2412] Orman, H., "The OAKLEY Key Determination Protocol", RFC 2412, November 1998.

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

[RFC2521] Karn, P. and W. Simpson, "ICMP Security Failures Messages", RFC 2521, March 1999.

[RFC2709] Srisuresh, P., "Security Model with Tunnel-mode IPsec for NAT Domains", RFC 2709, October 1999.

[RFC2857] Keromytis, A. and N. Provos, "The Use of HMAC-RIPEMD-160-96 within ESP and AH", RFC 2857, June 2000.

[RFC3051] Heath, J. and J. Border, "IP Payload Compression Using ITU-T V.44 Packet Method", RFC 3051, January 2001.

[RFC3056] Carpenter, B. and K. Moore, "Connection of IPv6 Domains via IPv4 Clouds", RFC 3056, February 2001.

[RFC3095] Bormann, C., Burmeister, C., Degermark, M., Fukushima, H., Hannu, H., Jonsson, L-E., Hakenberg, R., Koren, T., Le, K., Liu, Z., Martensson, A., Miyazaki, A., Svanbro, K., Wiebke, T., Yoshimura, T., and H. Zheng, "RObust Header Compression (ROHC): Framework and four profiles: RTP, UDP, ESP, and uncompressed", RFC 3095, July 2001.

[RFC3129] Thomas, M., "Requirements for Kerberized Internet Negotiation of Keys", RFC 3129, June 2001.

[RFC3173] Shacham, A., Monsour, B., Pereira, R., and M. Thomas, "IP Payload Compression Protocol (IPComp)", RFC 3173, September 2001.

[RFC3329] Arkko, J., Torvinen, V., Camarillo, G., Niemi, A., and T. Haukka, "Security Mechanism Agreement for the Session Initiation Protocol (SIP)", RFC 3329, January 2003.

[RFC3456] Patel, B., Aboba, B., Kelly, S., and V. Gupta, "Dynamic Host Configuration Protocol (DHCPv4) Configuration of IPsec Tunnel Mode", RFC 3456, January 2003.

[RFC3457] Kelly, S. and S. Ramamoorthi, "Requirements for IPsec Remote Access Scenarios", RFC 3457, January 2003.

[RFC3526] Kivinen, T. and M. Kojo, "More Modular Exponential (MODP) Diffie-Hellman groups for Internet Key Exchange (IKE)", RFC 3526, May 2003.

[RFC3547] Baugher, M., Weis, B., Hardjono, T., and H. Harney, "The Group Domain of Interpretation", RFC 3547, July 2003.

[RFC3554] Bellovin, S., Ioannidis, J., Keromytis, A., and R. Stewart, "On the Use of Stream Control Transmission Protocol (SCTP) with IPsec", RFC 3554, July 2003.

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

[RFC3585] Jason, J., Rafalow, L., and E. Vyncke, "IPsec Configuration Policy Information Model", RFC 3585, August 2003.

[RFC3586] Blaze, M., Keromytis, A., Richardson, M., and L. Sanchez, "IP Security Policy (IPSP) Requirements", RFC 3586, August 2003.

[RFC3602] Frankel, S., Glenn, R., and S. Kelly, "The AES-CBC Cipher Algorithm and Its Use with IPsec", RFC 3602, September 2003.

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

[RFC3706] Huang, G., Beaulieu, S., and D. Rochefort, "A Traffic-Based Method of Detecting Dead Internet Key Exchange (IKE) Peers", RFC 3706, February 2004.

[RFC3715] Aboba, B. and W. Dixon, "IPsec-Network Address Translation (NAT) Compatibility Requirements", RFC 3715, March 2004.

[RFC3740] Hardjono, T. and B. Weis, "The Multicast Group Security Architecture", RFC 3740, March 2004.

[RFC3776] Arkko, J., Devarapalli, V., and F. Dupont, "Using IPsec to Protect Mobile IPv6 Signaling Between Mobile Nodes and Home Agents", RFC 3776, June 2004.

[RFC3830] Arkko, J., Carrara, E., Lindholm, F., Naslund, M., and K. Norrman, "MIKEY: Multimedia Internet KEYing", RFC 3830, August 2004.

[RFC3884] Touch, J., Eggert, L., and Y. Wang, "Use of IPsec Transport Mode for Dynamic Routing", RFC 3884, September 2004.

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

[RFC3948] Huttunen, A., Swander, B., Volpe, V., DiBurro, L., and M. Stenberg, "UDP Encapsulation of IPsec ESP Packets", RFC 3948, January 2005.

[RFC4025] Richardson, M., "A Method for Storing IPsec Keying Material in DNS", RFC 4025, March 2005.

[RFC4046] Baugher, M., Canetti, R., Dondeti, L., and F. Lindholm, "Multicast Security (MSEC) Group Key Management Architecture", RFC 4046, April 2005.

[RFC4093] Adrangi, F., Ed., and H. Levkowetz, Ed., "Problem Statement: Mobile IPv4 Traversal of Virtual Private Network (VPN) Gateways", RFC 4093, August 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.

[RFC4196] Lee, H., Yoon, J., Lee, S., and J. Lee, "The SEED Cipher Algorithm and Its Use with IPsec", RFC 4196, October 2005.

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

[RFC4302] Kent, S., "IP Authentication Header", RFC 4302, December 2005.

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

[RFC4304] Kent, S., "Extended Sequence Number (ESN) Addendum to IPsec Domain of Interpretation (DOI) for Internet Security Association and Key Management Protocol (ISAKMP)", RFC 4304, December 2005.

[RFC4305] Eastlake 3rd, D., "Cryptographic Algorithm Implementation Requirements for Encapsulating Security Payload (ESP) and Authentication Header (AH)", RFC 4305, December 2005.

[RFC4306] Kaufman, C., Ed., "Internet Key Exchange (IKEv2) Protocol", RFC 4306, December 2005.

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

[RFC4308] Hoffman, P., "Cryptographic Suites for IPsec", RFC 4308, December 2005.

[RFC4309] Housley, R., "Using Advanced Encryption Standard (AES) CCM Mode with IPsec Encapsulating Security Payload (ESP)", RFC 4309, December 2005.

[RFC4312] Kato, A., Moriai, S., and M. Kanda, "The Camellia Cipher Algorithm and Its Use With IPsec", RFC 4312, December 2005.

[RFC4322] Richardson, M. and D. Redelmeier, "Opportunistic Encryption using the Internet Key Exchange (IKE)", RFC 4322, December 2005.

[RFC4359] Weis, B., "The Use of RSA/SHA-1 Signatures within Encapsulating Security Payload (ESP) and Authentication Header (AH)", RFC 4359, January 2006.

[RFC4430] Sakane, S., Kamada, K., Thomas, M., and J. Vilhuber, "Kerberized Internet Negotiation of Keys (KINK)", RFC 4430, March 2006.

[RFC4434] Hoffman, P., "The AES-XCBC-PRF-128 Algorithm for the Internet Key Exchange Protocol (IKE)", RFC 4434, February 2006.

[RFC4478] Nir, Y., "Repeated Authentication in Internet Key Exchange (IKEv2) Protocol", RFC 4478, April 2006.

[RFC4494] Song, JH., Poovendran, R., and J. Lee, "The AES-CMAC-96 Algorithm and Its Use with IPsec", RFC 4494, June 2006.

[RFC4535] Harney, H., Meth, U., Colegrove, A., and G. Gross, "GSAKMP: Group Secure Association Key Management Protocol", RFC 4535, June 2006.

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

[RFC4552] Gupta, M. and N. Melam, "Authentication/Confidentiality for OSPFv3", RFC 4552, June 2006.

[RFC4555] Eronen, P., "IKEv2 Mobility and Multihoming Protocol (MOBIKE)", RFC 4555, June 2006.

[RFC4595] Maino, F. and D. Black, "Use of IKEv2 in the Fibre Channel Security Association Management Protocol", RFC 4595, July 2006.

[RFC4615] Song, J., Poovendran, R., Lee, J., and T. Iwata, "The Advanced Encryption Standard-Cipher-based Message Authentication Code-Pseudo-Random Function-128 (AES-CMAC-PRF-128) Algorithm for the Internet Key Exchange Protocol (IKE)", RFC 4615, August 2006.

[RFC4621] Kivinen, T. and H. Tschofenig, "Design of the IKEv2 Mobility and Multihoming (MOBIKE) Protocol", RFC 4621, August 2006.

[RFC4705] Housley, R. and A. Corry, "GigaBeam High-Speed Radio Link Encryption", RFC 4705, October 2006.

[RFC4718] Eronen, P. and P. Hoffman, "IKEv2 Clarifications and Implementation Guidelines", RFC 4718, October 2006.

[RFC4739] Eronen, P. and J. Korhonen, "Multiple Authentication Exchanges in the Internet Key Exchange (IKEv2) Protocol", RFC 4739, November 2006.

[RFC4753] Fu, D. and J. Solinas, "ECP Groups For IKE and IKEv2", RFC 4753, January 2007.

[RFC4754] Fu, D. and J. Solinas, "IKE and IKEv2 Authentication Using the Elliptic Curve Digital Signature Algorithm (ECDSA)", RFC 4754, January 2007.

[RFC4806] Myers, M. and H. Tschofenig, "Online Certificate Status Protocol (OCSP) Extensions to IKEv2", RFC 4806, February 2007.

[RFC4807] Baer, M., Charlet, R., Hardaker, W., Story, R., and C. Wang, "IPsec Security Policy Database Configuration MIB", RFC 4807, March 2007.

[RFC4809] Bonatti, C., Ed., Turner, S., Ed., and G. Lebovitz, Ed., "Requirements for an IPsec Certificate Management Profile", RFC 4809, February 2007.

[RFC4835] Manral, V., "Cryptographic Algorithm Implementation Requirements for Encapsulating Security Payload (ESP) and Authentication Header (AH)", RFC 4835, April 2007.

[RFC4868] Kelly, S. and S. Frankel, "Using HMAC-SHA-256, HMAC-SHA-384, and HMAC-SHA-512 with IPsec", RFC 4868, May 2007.

[RFC4869] Law, L. and J. Solinas, "Suite B Cryptographic Suites for IPsec", RFC 4869, May 2007.

[RFC4877] Devarapalli, V. and F. Dupont, "Mobile IPv6 Operation with IKEv2 and the Revised IPsec Architecture", RFC 4877, April 2007.

[RFC4891] Graveman, R., Parthasarathy, M., Savola, P., and H. Tschofenig, "Using IPsec to Secure IPv6-in-IPv4 Tunnels", RFC 4891, May 2007.

[RFC4894] Hoffman, P., "Use of Hash Algorithms in Internet Key Exchange (IKE) and IPsec", RFC 4894, May 2007.

[RFC4945] Korver, B., "The Internet IP Security PKI Profile of IKEv1/ISAKMP, IKEv2, and PKIX", RFC 4945, August 2007.

[RFC5026] Giaretta, G., Ed., Kempf, J., and V. Devarapalli, Ed., "Mobile IPv6 Bootstrapping in Split Scenario", RFC 5026, October 2007.

[RFC5106] Tschofenig, H., Kroeselberg, D., Pashalidis, A., Ohba, Y., and F. Bersani, "The Extensible Authentication Protocol-Internet Key Exchange Protocol version 2 (EAP-IKEv2) Method", RFC 5106, February 2008.

[RFC5114] Lepinski, M. and S. Kent, "Additional Diffie-Hellman Groups for Use with IETF Standards", RFC 5114, January 2008.

[RFC5201] Moskowitz, R., Nikander, P., Jokela, P., Ed., and T. Henderson, "Host Identity Protocol", RFC 5201, April 2008.

[RFC5202] Jokela, P., Moskowitz, R., and P. Nikander, "Using the Encapsulating Security Payload (ESP) Transport Format with the Host Identity Protocol (HIP)", RFC 5202, April 2008.

[RFC5206] Nikander, P., Henderson, T., Ed., Vogt, C., and J. Arkko, "End-Host Mobility and Multihoming with the Host Identity Protocol", RFC 5206, April 2008.

[RFC5207] Stiemerling, M., Quittek, J., and L. Eggert, "NAT and Firewall Traversal Issues of Host Identity Protocol (HIP) Communication", RFC 5207, April 2008.

[RFC5213] Gundavelli, S., Ed., Leung, K., Devarapalli, V., Chowdhury, K., and B. Patil, "Proxy Mobile IPv6", RFC 5213, August 2008.

[RFC5225] Pelletier, G. and K. Sandlund, "RObust Header Compression Version 2 (ROHCv2): Profiles for RTP, UDP, IP, ESP and UDP-Lite", RFC 5225, April 2008.

[RFC5265] Vaarala, S. and E. Klovning, "Mobile IPv4 Traversal across IPsec-Based VPN Gateways", RFC 5265, June 2008.

[RFC5266] Devarapalli, V. and P. Eronen, "Secure Connectivity and Mobility Using Mobile IPv4 and IKEv2 Mobility and Multihoming (MOBIKE)", BCP 136, RFC 5266, June 2008.

[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.

[RFC5380] Soliman, H., Castelluccia, C., ElMalki, K., and L. Bellier, "Hierarchical Mobile IPv6 (HMIPv6) Mobility Management", RFC 5380, October 2008.

[RFC5386] Williams, N. and M. Richardson, "Better-Than-Nothing Security: An Unauthenticated Mode of IPsec", RFC 5386, November 2008.

[RFC5374] Weis, B., Gross, G., and D. Ignjatic, "Multicast Extensions to the Security Architecture for the Internet Protocol", RFC 5374, November 2008.

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

[RFC5406] Bellovin, S., "Guidelines for Specifying the Use of IPsec Version 2", BCP 146, RFC 5406, February 2009.

[RFC5529] Kato, A., Kanda, M., and S. Kanno, "Modes of Operation for Camellia for Use with IPsec", RFC 5529, April 2009.

[RFC5566] Berger, L., White, R., and E. Rosen, "BGP IPsec Tunnel Encapsulation Attribute", RFC 5566, June 2009.

[RFC5568] Koodli, R., Ed., "Mobile IPv6 Fast Handovers", RFC 5568, July 2009.

[RFC5570] StJohns, M., Atkinson, R., and G. Thomas, "Common Architecture Label IPv6 Security Option (CALIPSO)", RFC 5570, July 2009.

[RFC5660] Williams, N., "IPsec Channels: Connection Latching", RFC 5660, October 2009.

[RFC5685] Devarapalli, V. and K. Weniger, "Redirect Mechanism for the Internet Key Exchange Protocol Version 2 (IKEv2)", RFC 5685, November 2009.

[RFC5723] Sheffer, Y. and H. Tschofenig, "Internet Key Exchange Protocol Version 2 (IKEv2) Session Resumption", RFC 5723, January 2010.

[RFC5739] Eronen, P., Laganier, J., and C. Madson, "IPv6 Configuration in Internet Key Exchange Protocol Version 2 (IKEv2)", RFC 5739, February 2010.

[RFC5840] Grewal, K., Montenegro, G., and M. Bhatia, "Wrapped Encapsulating Security Payload (ESP) for Traffic Visibility", RFC 5840, April 2010.

[RFC5856] Ertekin, E., Jasani, R., Christou, C., and C. Bormann, "Integration of Robust Header Compression over IPsec Security Associations", RFC 5856, May 2010.

[RFC5857] Ertekin, E., Christou, C., Jasani, R., Kivinen, T., and C. Bormann, "IKEv2 Extensions to Support Robust Header Compression over IPsec", RFC 5857, May 2010.

[RFC5858] Ertekin, E., Christou, C., and C. Bormann, "IPsec Extensions to Support Robust Header Compression over IPsec", RFC 5858, May 2010.

[RFC5879] Kivinen, T. and D. McDonald, "Heuristics for Detecting ESP-NULL Packets", RFC 5879, May 2010.

[RFC5903] Fu, D. and J. Solinas, "Elliptic Curve Groups modulo a Prime (ECP Groups) for IKE and IKEv2", RFC 5903, June 2010.

[RFC5930] Shen, S., Mao, Y., and NSS. Murthy, "Using Advanced Encryption Standard Counter Mode (AES-CTR) with the Internet Key Exchange version 02 (IKEv2) Protocol", RFC 5930, July 2010.

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

[RFC5998] Eronen, P., Tschofenig, H., and Y. Sheffer, "An Extension for EAP-Only Authentication in IKEv2", RFC 5998, September 2010.

[RFC6027] Nir, Y., "IPsec Cluster Problem Statement", RFC 6027, October 2010.

Appendix A. Summary of Algorithm Requirement Levels

Table 1: Algorithm Requirement Levels

ALGORITHM	REQUIREMENT LEVEL			
	IKEv1	IKEv2	IPsec-v2	IPsec-v3
Encryption Algorithms:				
ESP-NULL	N/A	N/A	MUST	MUST
3DES-CBC	MUST	MUST-	MUST	MUST-
Blowfish/CAST/IDEA/RC5	optional	optional	optional	optional
AES-CBC 128-bit key	SHOULD	SHOULD+	MUST	MUST
AES-CBC 192/256-bit key	optional	optional	optional	optional
AES-CTR	undefined	optional	SHOULD	SHOULD
Camellia-CBC	optional	optional	optional	optional
Camellia-CTR	undefined	undefined	undefined	optional
SEED-CBC	undefined	undefined	optional	undefined
Integrity-Protection Algorithms:				
HMAC-SHA-1	MUST	MUST	MUST	MUST
AES-XCBC-MAC	undefined	optional	SHOULD+	SHOULD+
HMAC-SHA-256/384/512	optional	optional	optional	optional
AES-GMAC	N/A	N/A	undefined	optional
HMAC-MD5	MAY	optional	MAY	MAY
AES-CMAC	undefined	optional	undefined	optional
HMAC-RIPEMD	undefined	undefined	optional	undefined

Table 1: Algorithm Requirement Levels (continued)

ALGORITHM	REQUIREMENT LEVEL			
	IKEv1	IKEv2	IPsec-v2	IPsec-v3
Combined Mode Algorithms:				
AES-CCM	N/A	optional	N/A	optional
AES-GCM	N/A	optional	N/A	optional
AES-GMAC	N/A	N/A	undefined	optional
Camellia-CCM	N/A	undefined	N/A	optional
Pseudorandom Functions:				
PRF-HMAC-SHA1	MUST	MUST		
PRF-HMAC-SHA-256/384/512	optional	optional		
AES-XCBC-PRF	undefined	SHOULD+		
AES-CMAC-PRF	undefined	optional		
Diffie-Hellman Algorithms:				
DH MODP grp 1	MAY	optional		
DH MODP grp 2	MUST	MUST-		
DH MODP grp 5	optional	optional		
DH MODP grp 14	SHOULD	SHOULD+		
DH MODP grp 15-18	optional	optional		
DH MODP grp 22-24	optional	optional		
DH EC grp 3-4	MAY	undefined		
DH EC grp 19-21	optional	optional		
DH EC grp 25-26	optional	optional		

Authors' Addresses

Sheila Frankel
NIST
Bldg. 223 Rm. B366
Gaithersburg, MD 20899

Phone: 1-301-975-3297
EMail: sheila.frankel@nist.gov

Suresh Krishnan
Ericsson
8400 Decarie Blvd.
Town of Mount Royal, QC
Canada

Phone: 1-514-345-7900 x42871
EMail: suresh.krishnan@ericsson.com