

Internet Security Association and Key Management Protocol (ISAKMP)

Status of this Memo

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

Copyright Notice

Copyright (C) The Internet Society (1998). All Rights Reserved.

Abstract

This memo describes a protocol utilizing security concepts necessary for establishing Security Associations (SA) and cryptographic keys in an Internet environment. A Security Association protocol that negotiates, establishes, modifies and deletes Security Associations and their attributes is required for an evolving Internet, where there will be numerous security mechanisms and several options for each security mechanism. The key management protocol must be robust in order to handle public key generation for the Internet community at large and private key requirements for those private networks with that requirement. The Internet Security Association and Key Management Protocol (ISAKMP) defines the procedures for authenticating a communicating peer, creation and management of Security Associations, key generation techniques, and threat mitigation (e.g. denial of service and replay attacks). All of these are necessary to establish and maintain secure communications (via IP Security Service or any other security protocol) in an Internet environment.

## Table of Contents

1	Introduction	4
1.1	Requirements Terminology	5
1.2	The Need for Negotiation	5
1.3	What can be Negotiated?	6
1.4	Security Associations and Management	7
1.4.1	Security Associations and Registration	7
1.4.2	ISAKMP Requirements	8
1.5	Authentication	8
1.5.1	Certificate Authorities	9
1.5.2	Entity Naming	9
1.5.3	ISAKMP Requirements	10
1.6	Public Key Cryptography	10
1.6.1	Key Exchange Properties	11
1.6.2	ISAKMP Requirements	12
1.7	ISAKMP Protection	12
1.7.1	Anti-Clogging (Denial of Service)	12
1.7.2	Connection Hijacking	13
1.7.3	Man-in-the-Middle Attacks	13
1.8	Multicast Communications	13
2	Terminology and Concepts	14
2.1	ISAKMP Terminology	14
2.2	ISAKMP Placement	16
2.3	Negotiation Phases	16
2.4	Identifying Security Associations	17
2.5	Miscellaneous	20
2.5.1	Transport Protocol	20
2.5.2	RESERVED Fields	20
2.5.3	Anti-Clogging Token ("Cookie") Creation	20
3	ISAKMP Payloads	21
3.1	ISAKMP Header Format	21
3.2	Generic Payload Header	25
3.3	Data Attributes	25
3.4	Security Association Payload	27
3.5	Proposal Payload	28
3.6	Transform Payload	29
3.7	Key Exchange Payload	31
3.8	Identification Payload	32
3.9	Certificate Payload	33
3.10	Certificate Request Payload	34
3.11	Hash Payload	36
3.12	Signature Payload	37
3.13	Nonce Payload	37
3.14	Notification Payload	38
3.14.1	Notify Message Types	40
3.15	Delete Payload	41
3.16	Vendor ID Payload	43

4	ISAKMP Exchanges	44
4.1	ISAKMP Exchange Types	45
4.1.1	Notation	46
4.2	Security Association Establishment	46
4.2.1	Security Association Establishment Examples	48
4.3	Security Association Modification	50
4.4	Base Exchange	51
4.5	Identity Protection Exchange	52
4.6	Authentication Only Exchange	54
4.7	Aggressive Exchange	55
4.8	Informational Exchange	57
5	ISAKMP Payload Processing	58
5.1	General Message Processing	58
5.2	ISAKMP Header Processing	59
5.3	Generic Payload Header Processing	61
5.4	Security Association Payload Processing	62
5.5	Proposal Payload Processing	63
5.6	Transform Payload Processing	64
5.7	Key Exchange Payload Processing	65
5.8	Identification Payload Processing	66
5.9	Certificate Payload Processing	66
5.10	Certificate Request Payload Processing	67
5.11	Hash Payload Processing	69
5.12	Signature Payload Processing	69
5.13	Nonce Payload Processing	70
5.14	Notification Payload Processing	71
5.15	Delete Payload Processing	73
6	Conclusions	75
A	ISAKMP Security Association Attributes	77
A.1	Background/Rationale	77
A.2	Internet IP Security DOI Assigned Value	77
A.3	Supported Security Protocols	77
A.4	ISAKMP Identification Type Values	78
A.4.1	ID_IPV4_ADDR	78
A.4.2	ID_IPV4_ADDR_SUBNET	78
A.4.3	ID_IPV6_ADDR	78
A.4.4	ID_IPV6_ADDR_SUBNET	78
B	Defining a new Domain of Interpretation	79
B.1	Situation	79
B.2	Security Policies	80
B.3	Naming Schemes	80
B.4	Syntax for Specifying Security Services	80
B.5	Payload Specification	80
B.6	Defining new Exchange Types	80
	Security Considerations	81
	IANA Considerations	81
	Domain of Interpretation	81
	Supported Security Protocols	82

Acknowledgements	82
References	82
Authors' Addresses	85
Full Copyright Statement	86

## List of Figures

1	ISAKMP Relationships . . . . .	16
2	ISAKMP Header Format . . . . .	22
3	Generic Payload Header . . . . .	25
4	Data Attributes . . . . .	26
5	Security Association Payload . . . . .	27
6	Proposal Payload Format . . . . .	28
7	Transform Payload Format . . . . .	30
8	Key Exchange Payload Format . . . . .	31
9	Identification Payload Format . . . . .	32
10	Certificate Payload Format . . . . .	33
11	Certificate Request Payload Format . . . . .	34
12	Hash Payload Format . . . . .	36
13	Signature Payload Format . . . . .	37
14	Nonce Payload Format . . . . .	38
15	Notification Payload Format . . . . .	39
16	Delete Payload Format . . . . .	42
17	Vendor ID Payload Format . . . . .	44

## 1 Introduction

This document describes an Internet Security Association and Key Management Protocol (ISAKMP). ISAKMP combines the security concepts of authentication, key management, and security associations to establish the required security for government, commercial, and private communications on the Internet.

The Internet Security Association and Key Management Protocol (ISAKMP) defines procedures and packet formats to establish, negotiate, modify and delete Security Associations (SA). SAs contain all the information required for execution of various network security services, such as the IP layer services (such as header authentication and payload encapsulation), transport or application layer services, or self-protection of negotiation traffic. ISAKMP defines payloads for exchanging key generation and authentication data. These formats provide a consistent framework for transferring key and authentication data which is independent of the key generation technique, encryption algorithm and authentication mechanism.

ISAKMP is distinct from key exchange protocols in order to cleanly separate the details of security association management (and key management) from the details of key exchange. There may be many different key exchange protocols, each with different security properties. However, a common framework is required for agreeing to the format of SA attributes, and for negotiating, modifying, and deleting SAs. ISAKMP serves as this common framework.

Separating the functionality into three parts adds complexity to the security analysis of a complete ISAKMP implementation. However, the separation is critical for interoperability between systems with differing security requirements, and should also simplify the analysis of further evolution of a ISAKMP server.

ISAKMP is intended to support the negotiation of SAs for security protocols at all layers of the network stack (e.g., IPSEC, TLS, TLSP, OSPF, etc.). By centralizing the management of the security associations, ISAKMP reduces the amount of duplicated functionality within each security protocol. ISAKMP can also reduce connection setup time, by negotiating a whole stack of services at once.

The remainder of [section 1](#) establishes the motivation for security negotiation and outlines the major components of ISAKMP, i.e. Security Associations and Management, Authentication, Public Key Cryptography, and Miscellaneous items. [Section 2](#) presents the terminology and concepts associated with ISAKMP. [Section 3](#) describes the different ISAKMP payload formats. [Section 4](#) describes how the payloads of ISAKMP are composed together as exchange types to establish security associations and perform key exchanges in an authenticated manner. Additionally, security association modification, deletion, and error notification are discussed. [Section 5](#) describes the processing of each payload within the context of ISAKMP exchanges, including error handling and associated actions. The appendices provide the attribute values necessary for ISAKMP and requirement for defining a new Domain of Interpretation (DOI) within ISAKMP.

## 1.1 Requirements Terminology

The keywords MUST, MUST NOT, REQUIRED, SHALL, SHALL NOT, SHOULD, SHOULD NOT, RECOMMENDED, MAY, and OPTIONAL, when they appear in this document, are to be interpreted as described in [[RFC-2119](#)].

## 1.2 The Need for Negotiation

ISAKMP extends the assertion in [[DOW92](#)] that authentication and key exchanges must be combined for better security to include security association exchanges. The security services required for

# Explore Litigation Insights

Docket Alarm provides insights to develop a more informed litigation strategy and the peace of mind of knowing you're on top of things.

## Real-Time Litigation Alerts



Keep your litigation team up-to-date with **real-time alerts** and advanced team management tools built for the enterprise, all while greatly reducing PACER spend.

Our comprehensive service means we can handle Federal, State, and Administrative courts across the country.

## Advanced Docket Research



With over 230 million records, Docket Alarm's cloud-native docket research platform finds what other services can't. Coverage includes Federal, State, plus PTAB, TTAB, ITC and NLRB decisions, all in one place.

Identify arguments that have been successful in the past with full text, pinpoint searching. Link to case law cited within any court document via Fastcase.

## Analytics At Your Fingertips



Learn what happened the last time a particular judge, opposing counsel or company faced cases similar to yours.

Advanced out-of-the-box PTAB and TTAB analytics are always at your fingertips.

## API

Docket Alarm offers a powerful API (application programming interface) to developers that want to integrate case filings into their apps.

## LAW FIRMS

Build custom dashboards for your attorneys and clients with live data direct from the court.

Automate many repetitive legal tasks like conflict checks, document management, and marketing.

## FINANCIAL INSTITUTIONS

Litigation and bankruptcy checks for companies and debtors.

## E-DISCOVERY AND LEGAL VENDORS

Sync your system to PACER to automate legal marketing.