IPSEC Working Group
INTERNET-DRAFT
draft-ietf-ipsec-openpgp-01.txt

Will Price
PGP Security
23 March 2001

OpenPGP Key Usage in IKE

Status of this Memo

This document is a submission to the IETF IP Security Protocol (IPSEC) Working Group. Comments are solicited and should be addressed to the working group mailing list (ipsec@lists.tislab.com) or to the editor.

This document is an Internet-Draft and is in full conformance with all provisions of Section 10 of RFC2026.

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

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet- Drafts as reference material or to cite them other than as "work in progress."

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

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

Copyright Notice

Abstract

This document defines a profile for the usage of OpenPGP keys within the IKE [IKE] protocol. The ISAKMP [ISAKMP] protocol on which IKE is based defines an identifier for the use of OpenPGP [OPENPGP] keys, but does not define how they should be used.

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in RFC 2119.

Certificate Payload Key Format

Whenever an OpenPGP key is sent as part of a Certificate payload, the format MUST be that of the raw binary OpenPGP key. OpenPGP wrappings such as ASCII Armor MUST NOT be used.

For RSA Signature authentication, the RSA master key is used for signing. For DSS Signature authentication, the DSS master key is used for signing. For Public Key Encryption modes, the current valid subkey is used for encryption. If the key has no subkeys, but the master key is usable for encryption such as an RSA master key, the master key is used for encryption.

Use of Multiple Certificate Formats

The Certificate Request payload SHOULD be used to aid in distinguishing between the types of certificate expected by the remote system. Each side MAY request any type of certificate. There is no requirement that both sides must request the same type of certificate. It is RECOMMENDED that implementations use the Certificate Request payload regularly when performing certificate-based authentication in order to aid in interoperability between implementations that may use multiple certificates in multiple formats.

If a specific OpenPGP certificate authority is requested, the Certificate Authority field of the Certificate Request payload should contain the full OpenPGP fingerprint of the certificate authority. Note that the use of the Certificate Request payload remains important regardless of whether a specific certificate authority is requested. This allows the remote IKE implementation to know the preferred type of certificate.

Phase 1 Identification

Identification payloads in IKE Phase 1 when using certificate authentication are required by the IPsec DOI [DOI] to use IDs which represent the certificate.

Phase 1 identities when authenticating with an OpenPGP key MUST be of type ID_KEY_ID and contain the full OpenPGP fingerprint of the authenticating key represented as raw binary bytes of the size of the key's hash algorithm output.

Other Payloads

Other payloads such as Signature, and the format of public key encryption remain identical to the formats defined in IKE.

Infrastructure

Methods for retrieving up to date key revocation information, establishing designated revokers, and otherwise establishing key validity through the PGP web of trust or through an OpenPGP meta-introducer hierarchy are already well-established. Implementations of this specification MUST NOT accept revoked or expired keys for authentication.

References

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

[ISAKMP] D. Maughan, M. Schertler, M. Schneider, J. Turner, "Internet Security Association and Key Management Protocol (ISAKMP)", RFC 2408, November 1998

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

[OpenPGP] J. Callas, L. Donnerhacke, H. Finney, R. Thayer, "OpenPGP Message Format", RFC 2440, November 1998.

Author

Will Price <wprice@pgp.com>
PGP Security, Inc.