An interface between applications and keying systems
draft-ietf-btns-c-api-02.txt

Status of this Memo

By submitting this Internet-Draft, each author represents that any applicable patent or other IPR claims of which he or she is aware have been or will be disclosed, and any of which he or she becomes aware will be disclosed, in accordance with Section 6 of BCP 79.

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.

This Internet-Draft will expire on August 20, 2008.

Copyright Notice

Copyright (C) The IETF Trust (2008).
Abstract

Table of Contents

1. Overview .................................................. 3
2. Introduction .............................................. 4
3. Objects involved ........................................... 5
3.1. Scope of Protection Token .............................. 5
3.2. Scope of Identity Token ................................. 5
3.3. Validity period of Protection Token .................... 5
3.4. Validity period of Identity Token ...................... 6
4. Namespace .................................................... 7
5. pToken discovery ............................................ 8
6. Accessor Functions ......................................... 9
7. Security Considerations .................................... 10
8. IANA Considerations ....................................... 11
9. Acknowledgments .......................................... 12
10. References ................................................ 13
10.1. Normative references .................................. 13
10.2. Non-normative references ............................. 13
      Author’s Address ........................................ 14
      Intellectual Property and Copyright Statements ....... 15
1. Overview

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 [RFC2119].
2. Introduction

Purpose of this API.
3. Objects involved

There are two major kinds of objects that are defined by this document. These are the Protection Token (pToken) and the Identity Token (iToken). Both objects are abstracted into unique opaque tokens which may be manipulated only indirectly by applications.

Each object has a series of attributes associated with it. The API provides a mechanism to query the value of attributes of the token. The attributes are where all of the content of the objects are.

Each token has a scope - the place and time in which it can be considered valid. There are many conflicting qualities that one would wish for the token, and the result is a different compromise among these qualities for each token type. The tokens should be:

- small
- easy to allocate and deallocate
- automatically cleaned up when an application terminates (both properly and improperly)
- easily compared
- easily passed back in a recvmsg(2) call as auxiliary data (for pToken)

3.1. Scope of Protection Token

The protection token has a per-process (i.e. per-address space) scope. The scope of the token is not related to the underlying protection provided by IPsec. The token is a handle.

3.2. Scope of Identity Token

The identity token has a per-system scope, although two applications running on the same system may not be able to compare it literally.

3.3. Validity period of Protection Token

The pToken is valid only within the scope of a single process. The token may not be saved in any long term storage.

It is permitted for one protection token to be replaced with another (equivalent) protection token due to a node moving, suspending and resuming, or due to extended network outages, however the underlying identity token would be guaranteed to be the same. This would most
likely occur with unconnected sockets, where due to the outage/downtime, the keying system was unable to maintain a keying channel, and had to re-create the keys from scratch.

3.4. Validity period of Identity Token

The iToken may be valid across the entire system, although it may need to be turned into an external representation. Some forms of identity token may be valid across systems, but in general an identity token is only valid in reference to a local set of trust anchors. (See [RFC2692]).
4. Namespace

All functions and macros defined by this API are prefixed with "ipsec_" for functions and variables, and with "IPSEC_" if they are macros or enumerated types. (cf. to appropriate POSIX section?)

Whenever sensible, the enumerated values defined in [RFC2367] are used if appropriate.
5. pToken discovery

An application that receives a connection using accept(2), or with recvmsg(2) needs to get a protection token that is associated with the socket.

For connected sockets (such as TCP and some SCTP modes), the protection token should not change during the lifetime of the socket, so a simple process is appropriate.

For unconnected sockets (such as UDP and some SCTP modes), each datagram received may be received may arrive from a different source, and therefore may have different protections applied. A protection token needs to be returned with each datagram, so it must be returned as ancilliary data with recvmsg(2).

For connected sockets, the pToken will not change during the connection. (see notes about rekeying). A simple function is provided to return a pToken from a file descriptor. Many implementations are likely to implement this using getsockopt(2), but an interface in those terms is not specified in order to keep it somewhat abstract.
6. Accessor Functions
7. Security Considerations

stuff
8. IANA Considerations

stuff
9. Acknowledgments

stuff
10. References

10.1. Normative references


10.2. Non-normative references

Author’s Address

Michael C. Richardson
Sandelman Software Works
470 Dawson Avenue
Ottawa, ON  K1Z 5V7
CA

Email: mcr@sandelman.ottawa.on.ca
URI:  http://www.sandelman.ottawa.on.ca/
Full Copyright Statement

Copyright (C) The IETF Trust (2008).

This document is subject to the rights, licenses and restrictions contained in BCP 78, and except as set forth therein, the authors retain all their rights.

This document and the information contained herein are provided on an "AS IS" basis and THE CONTRIBUTOR, THE ORGANIZATION HE/SHE REPRESENTS OR IS SPONSORED BY (IF ANY), THE INTERNET SOCIETY, THE IETF TRUST AND THE INTERNET ENGINEERING TASK FORCE DISCLAIM ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO ANY WARRANTY THAT THE USE OF THE INFORMATION HEREIN WILL NOT INFRINGE ANY RIGHTS OR ANY IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

Intellectual Property

The IETF takes no position regarding the validity or scope of any Intellectual Property Rights or other rights that might be claimed to pertain to the implementation or use of the technology described in this document or the extent to which any license under such rights might not be available; nor does it represent that it has made any independent effort to identify any such rights. Information on the procedures with respect to rights in RFC documents can be found in BCP 78 and BCP 79.

Copies of IPR disclosures made to the IETF Secretariat and any assurances of licenses to be made available, or the result of an attempt made to obtain a general license or permission for the use of such proprietary rights by implementers or users of this specification can be obtained from the IETF on-line IPR repository at http://www.ietf.org/ipr.

The IETF invites any interested party to bring to its attention any copyrights, patents or patent applications, or other proprietary rights that may cover technology that may be required to implement this standard. Please address the information to the IETF at ietf-ipr@ietf.org.

Acknowledgment

Funding for the RFC Editor function is provided by the IETF Administrative Support Activity (IASA).