



# Rock message signing and signature verification API

---

## Table of Contents

|   |   |
|---|---|
| 1. API OVERVIEW.....                        | 3 |
| 1.1. Rock VPN overview.....                 | 3 |
| 1.2. Where the Signature API fits in .....  | 4 |
| 1.3. API Development Kit Deliverables ..... | 5 |
| 1.4. Architecture .....                     | 5 |
| 1.5. Signature standards used .....         | 7 |
| 1.6. Licensing requirements .....           | 7 |
| 1.7. Communications protocols used.....     | 7 |
| 2. DEFINITIONS AND ABBREVIATIONS.....       | 8 |
| 3. CONTACT DETAILS.....                     | 8 |

---

## 1. API OVERVIEW

The Rock VPN signer API provides a mechanism for programmers to make use of the message signing and signature verification functionality provided by Rock VPN.

The API provides remote procedure calls to the Rock VPN system that allows programmers to request signatures and signature verification of messages.

Signatures are used to verify the source and integrity of the message being transmitted.

Example implementations are also provided.

### 1.1. Rock VPN overview

The purpose of this section is not to give a complete overview of Rock VPN, but to highlight the components that will interact with the API.

The Rock VPN products implement the IPsec protocol suite, an IETF standard for securing traffic on the Internet. The IPsec protocol suite consists of traffic security protocols, cryptographic key management procedures and protocols that are used together to provide security at the network level.

The Rock VPN product suite consists of Workstation, Server and Gateway Software modules. A VPN Appliance is also available.

Rock VPN can make use of Electronic Signatures, using Public Key Cryptography based on the RSA encryption standard. In normal use, Rock VPN will use digital signatures as part of a network-level protocol exchange to authenticate the communicating partner.

These certificates are distributed using the Rock VPN Central Manager. The Central Manager acts as a Certificate Authority, and is capable of signing user or device certificates based on certain rules defined by the operator of the Central Manager.

Certificates can either be attached to a device (for instance a Server or VPN Appliance) or to a person (for example a user with a smart card).

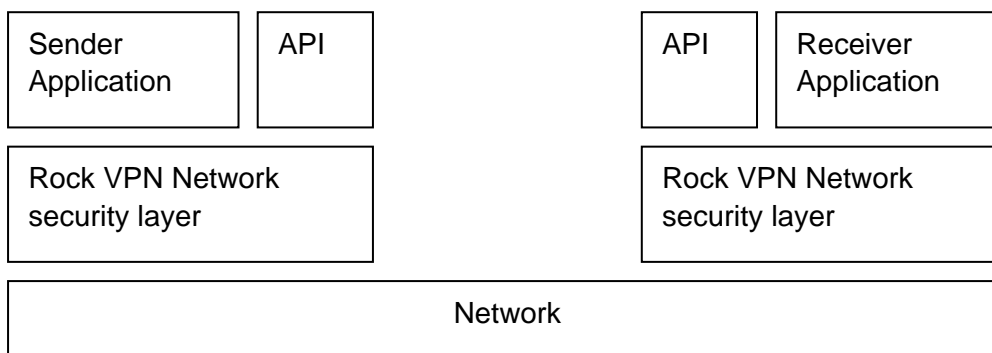
---

## 1.2. Where the Signature API fits in

Whilst the standard Rock VPN products make provision for authenticating devices or users at the network level, this facility does not allow an application to verify the origin or integrity of an entire message.

The Message API provides the application programmer with the facility to make use of the Rock VPN certificate management functions to generate and distribute certificates at a system level, whilst making simple calls to the Rock VPN service on the local host to digitally sign and verify messages.

Typical usage of the API



**Figure 1-1**

In Figure 1-1, the Sender Application will generate a message that needs protection. This message will then be passed to the API in the Sender Domain, and signed using the Sender Private Key. The Identity of the sender is embedded into the message itself. This identity must be present in the Certificate of the Sender.

The identity of the sender is typically embedded into the Distinguished Name of the certificate. For instance **CN=JNB, O=FirstBank** could be used to identify a specific branch of a bank. As a parameter to the API, the Issuer name is also passed. *It is very important that the Issuer name be installed and supplied locally, since modifications of both signature and verifier information could take place, allowing a bogus message to be accepted by the system.*

The message and signature is then sent to the other side, and the Receiver Application will verify the message by passing the Sender identity (obtained from the message), the message itself and the signature to the API. The API verifies that

- The message is intact (has not been modified)
- That the certificate identified by the sender identity was in fact used to sign the message
- That the certificate is valid (signed by the certificate authority that the API trusts)

---

The advantage to application developers and system integrators of using the API in this way are:

- Applications can use a simple interface to achieve strong cryptographic protection of their messages, without making complex code changes.
- Certificates are distributed and managed by the Rock VPN certification infrastructure, and addressed by using names. Applications do not have to manipulate or manage them.

### **1.3. API Development Kit Deliverables**

Printed matter:

- Application Program Interface User Manual

Software:

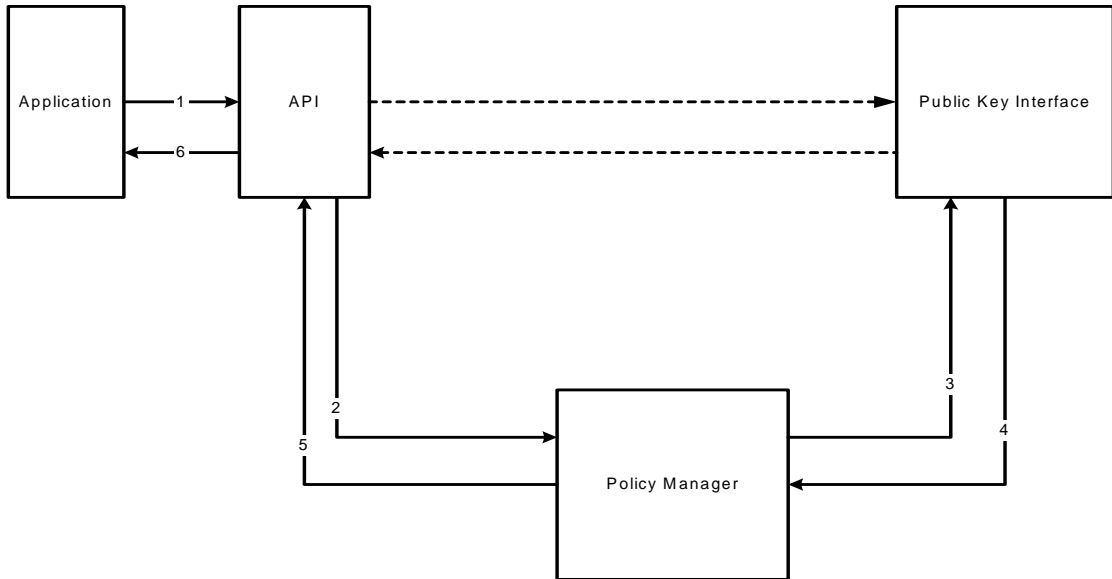
- Microsoft windows style DLL
- 'C' header file
- Source code of the library to be compiled on a Unix system (in this case HP-UX)

### **1.4. Architecture**

As discussed above, the API provides remote procedure calls that access services on the Rock VPN system. Figure 1.1 shows a block diagram of the components in Rock VPN and where the API fits in.

The application will use function calls through a dynamic library in a windows based system where the application was written in VB and a static library in other systems.

These calls are translated into RP calls to the public key interface system via the policy manager. Note that the policy manager and PKI must be on the same machine and that both must be active before calls are made.



**Figure 1-2: Block diagram showing the various components of an Rock VPN system with the calls through the API.**

---

## 1.5. Signature standards used

The signature is built using the PKCS#1 version 2 standard. The signatures generated are detached from the message content. This standard is also described in RFC 2437.

## 1.6. Licensing requirements

The signature API is a separately licensed product from NSS. In order to enable the API, NSS must provide a license file that activates the API functionality.

The following information is required to issue the license:

|  |
|--|
| In the case where connections will be made from localhost only |
| Customer information   |

|  |
|--|
| In the case where connections will be made from another host (eg where the Rock VPN Appliance signs on behalf of another host) |
| Customer information   |
| Host IP address or range of addresses  |

## 1.7. Communications protocols used

TCP/IP is used between the client library and the Rock VPN service performing the actual signature.

The client library will connect to well known port number ... on the host running the service.

In the case where the API client and the Rock VPN service is running on two platforms, no confidentiality protection is provided for between a host running the API client and the Rock VPN.

The controls involved in this case are:

- Pass-phase required to activate the private key
- Filter rules implemented by Rock VPN
- IP address restriction in the license file.

---

## 2. DEFINITIONS AND ABBREVIATIONS

|                 |   |
|-----------------|---|
| <i>AES</i>      | Advanced Encryption Standard, the successor to DES. See Rijndael.   |
| <i>CBC</i>      | Cipher Block Chaining, a feedback mode used on a block cipher.  |
| <i>DES</i>      | Data Encryption Standard, a 64-bit block cipher.  |
| <i>ESP</i>      | Encapsulating Security Payload (described in RFC 2406).   |
| <i>FTP</i>      | File Transfer Protocol.   |
| <i>IKE</i>      | Internet Key Exchange (described in RFC 2409).  |
| <i>IP</i>       | Internet Protocol   |
| <i>IV</i>       | Initialisation Vector. This is an initialisation variable used in block cipher modes such as CBC.   |
| <i>KLD</i>      | A FreeBSD loadable kernel module.   |
| <i>Rijndael</i> | The algorithm chosen for AES.   |
| <i>SA</i>       | Security Association. A unidirectional connection created for security purposes. All traffic traversing an SA is provided the same security processing. Both AH and ESP make use of SAs. A major function of IKE is the establishment and maintenance of SAs. |
| <i>TCP</i>      | Transmission Control Protocol   |

## 3. CONTACT DETAILS

Tel: +603-6203 5303  
Fax: +603-6203 5302  
URL: [www.rockvpn.com](http://www.rockvpn.com)

For more information or support requests, please visit [www.rockvpn.com](http://www.rockvpn.com) or [www.mynetsec.com](http://www.mynetsec.com).