SafeKeyper® Signer

September 1998

The information in this document is provided in compliance with requirements for FIPS 140-1 certification.

GTE Internetworking SafeKeyper® Signer

Description

The GTE Internetworking Safekeyper® Signer security device supports high-assurance Digital Signature applications that require verification of the author's signature and data integrity. The SafeKeyper Signer unit conveniently generates and stores cryptographic keys, protecting them from disclosure, misuse, or loss. Such keys, particularly the private component of a Public Key cryptography pair, can be used to sign digital documents, thereby guaranteeing to another party both the source of material and its integrity. The receiving party is assured that the document cannot later be repudiated by the originator -- the receiver can prove to a third party that the document must have been signed by the apparent originator and that the contents could not have been altered.

The SafeKeyper Signer is an integral component of the SafeKeyper Enterprise CMS. As the Certificate signing unit, the SafeKeyper Signer protects the Private Keys of the Certificate Authority. The SafeKeyper Signer provides the following Certificate signing and managing functionality:

- Secure Email, such as S/MIME, by issuing certificates and revocation lists
- Authentication and operation of web servers and browsers
- Certificate support for IP Security protocols such as SKIP and IKE

In addition, the SafeKeyper Signer can be combined with the appropriate application software to use with digital signature and authentication applications, such as:

- Software license distribution and usage control
- Electronic funds transfer
- Network and host sign-on authorization
- Detection of tampering with, or forgery of, computer-based information

Sample application

One organization is currently using the GTE Internetworking SafeKeyper Signer to sign certificates and revocation lists for use in Secure MIME (S/MIME) electronic mail and in secure Web servers and browsers that support SSL. Since the SafeKeyper Signer protects the private keys of organizations that issue certificates, the organization's customers have a high level of trust in the entire system. The certificates, which are compatible with the CCITT X.509 standard, bind users' names and their public cryptographic keys, thereby assuring the identity of the signer of an electronic document. Every certificate issuer also has a certificate signed by a higher issuing authority, creating a hierarchy of certificates to a known root authority. Any user can obtain a chain of certificates to validate the identity of any other user in the system. GTE Internetworking SafeKeyper Signer, acting as the Certificate Signing Unit, protects the private keys of the certificate signing authorities.

High-assurance cryptographic operations

The SafeKeyper Signer generates key pairs for the issuing authorities to use. The system employs a high-quality, hardware number generator to create keys with a low probability of duplication. The private component of the key pair never leaves the unit in cleartext form -- it is encrypted and stored within the unit and is only decrypted when the authority is activated. When activated, the cleartext form is stored within a portion of memory that is erased if anyone tampers with or opens the unit.

Robust access control and protection from key misuse

Use of an authority's signature is controlled by inserting one or more Cryptographic Ignition Keys (CIKs) which are small data storage devices that activate an authority. Physical control of the CIK provides multi-user access control for the signing capability.

Each authority can be individually configured to require all or a subset of the N CIKs for that authority. A SafeKeyper Signer can store more than one Authority's cryptographic material. Each Authority may have its own CIK or set of CIKs, or two or more Authorities can share a CIK or set of CIKs. In addition, an Authority's activation can require one CIK, or could require a sequence of CIKs to be inserted to initiate activation. The CIK process is configured separately for each Authority. Examples include: two from a set

of two, any two from a set of four, or any k out of a set of N. Safeguarding of the CIK is paramount to maintaining access control over the Authority.

High availablity and protection from key loss

If a SafeKeyper Signer is lost, damaged or otherwise fails, the private keys of the authorities created in it and stored within can be recovered by another SafeKeyper Signer. Recovery preserves the secrecy and protects the private keys, while retaining multi-user control.

Security Policy

The principal security objective for the SafeKeyper unit is that it shall provide secure storage for the private asymmetric components of Signing Authorities (principally CAs) and shall prevent misuse of such keys. This requirement implies the following policies:

a) The critical security components of the unit are:

   1) The symmetric key of the unit.

   2) The private component of the unit's asymmetric key pair.

   3) The symmetric keys for all Signing Authorities in the unit.

   4) The private components of all Signing Authority's asymmetric key pairs.

b) None of the critical security components shall ever leave the module in the clear.

c) Critical security components in cleartext form shall only be stored in tamper-protected memory.

d) At least three separate pieces of information shall be required to activate a Signing Authority. The three elements are the CA's encrypted symmetric key, the CA's encrypted asymmetric keying material, and a module with it's symmetric key.

e) All asymmetric key pairs and symmetric keys shall be generated using a high-quality random number generator. It shall not be possible, from outside the unit, to "seed" or otherwise influence the choice of random numbers.

f) The unit shall be tamper-resistant and tamper-evident.

g). FIPS 140-1 level 3 compliant units have a Crypto Officer role, and the following services can only be performed when that role is active:

1) Reconfiguring the unit with a signed control message.

2) Creating a new Signing Authority in the unit.

3) Transferring a Signing Authority to the unit.

4) Obtaining an encrypted copy of a Signing Authority's asymmetric private key.

5) Changing a Signing Authority's symmetric key.

6) Reconfiguring any Signing Authority with a signed control message.

7) Canceling (removing) a Signing Authority.

For any of the last five services, the Signing Authority shall be activated as part of the transaction.

The Crypto Officer has control over the choice of public key algorithm to be created as well as control over whether CIK shares will be created.

h) All signing operations shall require that the relevant Signing Authority be activated first.

i) Any Signing Authority which is created as a control message signing authority (Control Authority) shall be allowed to sign control messages but shall not be allowed to sign certificates or certificate revocation lists.

j) Any Signing Authority which is created as other than a control authority shall be allowed to sign certificates and certificate revocation lists, but shall not be allowed to sign control messages.

k) In a unit configured to allow signing a hash or signing any ASN.1-encoded request, any Signing Authority may sign such requests. These services shall only be configurable by the factory. (i.e. unit

configuration applies to all Signing Authorities independent of any per authority configuration assigned by a control authority.)

Specifications

Key Features:	RSA key pair creation and signature, to 2048 bits		
	DSA key pair creation and signature, to 1024 bits		
	MD2, MD5, SHA1 Hashing		
	Sign any externally generated hash		
	Supports X.509 Versions 1,2 and 3 Certificates, Versions 1 and 2 CRLs		
	Hardware random generator		
Size:	Height: 2.6 in.	Width:	7.2 in.
	Length: 10.3 in.	Weight:	11 lbs.
Power:	Floor mount transformer:		
	90-270 VAC, 47-63 hz. • DC input: 24v		
	10 w. typical • 18 w. maximum		
Interfaces:	RS-232 25-pin 'D' DTE port		
	Datakey DK1000 (CIK)• Datakey PK-64KS		
LEDs:	Power, alarm, 2 status		
Operating Environment:	Temperature 0-40° C • Humidity 5 - 80% (noncondensing)		
Safety:	Integral UL-listed lithium dioxide battery		
	Power supply: UL1950, CSA 22, EN60950		
	Chassis: FCC Class B, EN55022 Class A, designed to meet Tempest requirements and NACSIM 5100A		
	Designed to meet FIPS 140-1 level 3, and US DOD tamper-resistance requirements for high grade cryptographic devices		

Signing Performance: 512 bit key <3 seconds • 1024 bit key <5 seconds

Key Generation: 512 bit averages 26 seconds

1024 bit averages 97 seconds

Pricing:

5396-5	SafeKeyper (110V-220V) with RS-232 straight-through cable	$9,900
5396-6	SafeKeyper (100V-220V) with RS-232 NULL modem cable	$9,900

- Both models include:SafeKeyper peripheral device with appropriate cable
- Floor-mount power supply
- Power cable (country power kit)
- Two DataKey KSD64 parallel EEPROM key
- Five DataKey DK1000 serial EEPROM key
- Nomaar protective pad to place beneath the SafeKeyper

For more information contact:
GTE Internetworking
150 CambridgePark Drive
Cambridge, MA 02140
Email: netsec@bbn.com

Tel: (800) 295-7897
Fax: (617) 873-4086
Web: http://www.bbn.com

SafeKeyper® is a registered trademark.