



WHITE PAPER

Enterprise Key Management

Understanding the Core Issues of Key Management—Including Key Recovery—and the Unique, State-of-the-Art Solution Offered by VeriSign.®



Where it all comes together.™



CONTENTS

+ Enterprise Key Management	3
Key-Pair Generation—	
Central vs. Distributed	3
Encryption Private-Key Backup	3
+ Key-Backup Requirements and the Need for Dual Key Pairs	4
+ Key-Backup Risks	5
+ VeriSign Key Management Solution	6
+ How VeriSign Compares	7



Enterprise Key Management

In this White Paper, we address issues of public key infrastructure (PKI) user-key management, including key-pair generation, key backup and recovery, and requirements for dual key pairs. We assume the reader already has a basic appreciation of the general nature of public key technology and PKI.

+ Key-Pair Generation: Central vs. Distributed

A client key pair is generated in one of two locations. Key generation may be distributed—that is, built into the client product. In this case, the client generates the key pair, locally stores the private key securely, formats a certificate-signing request sent to a certification authority (CA), receives a certificate from the CA, and stores the certificate locally. The alternative is central key-pair generation, in which a system at the enterprise's administration center generates the key pair, executes a transaction with the enterprise CA to have a certificate issued, and ships the private key and certificate, packaged together, to the client for importation into its local store. Modern PKI client products, such as Microsoft® and Netscape® Web and mail clients, support both alternatives.

Central key generation is sometimes favored, especially if the private key needs to be backed up centrally (see later discussion). Also, this method allows for batch-oriented credentials establishment and distribution in large user communities and is amenable to use with smart cards.

VeriSign recognizes the legitimate need for both alternatives, and VeriSign® Managed PKI supports them, configurable by the enterprise customer.

+ Encryption Private-Key Backup

When a public-key/private-key pair is used to protect stored encrypted data, the private key may need to be recovered if its primary copy is lost or becomes otherwise inaccessible. Without such a capability, loss of a private key may mean loss of valuable data. For example, if an employee forgets a password needed to unlock encrypted files or stored email messages, or if a disgruntled worker is terminated and leaves without divulging a key needed for decryption, the enterprise may lose important data.

Key backup is complicated by the fact that a user will use different key pairs through time—for example, when a new key pair is generated every year. Sometimes, an old private key may need to be recovered to decrypt an old encrypted file. A key-backup system therefore needs to keep track of a key history for each user (i.e., copies of all old-encryption private keys), with the ability to recover any key from that history if needed.

What about the public-policy agenda whereby governments want to be able to decrypt intercepted encrypted data for law-enforcement or national-security reasons? If deployment of a private-key backup capability were to facilitate legal use of strong cryptography by an international organization, this policy might constitute a big plus for an enterprise. But, generally, should a PKI solution bow to such requirements?

The VeriSign position is that key backup is an enterprise's choice, and issues of government-mandated key recovery are entirely between the enterprise and the government. Any role the company might play in government-mandated release of private keys will be limited to that reflected in customer agreements and required by law.

Key-Backup Requirements and the Need for Dual Key Pairs

Key pairs are used for one or more of three basic purposes: encryption, authentication, and nonrepudiation. The following table shows the requirements for private key backup for each case.

Key-Pair Usage	Backup Requirement
Encryption	Sometimes need to back up
Authentication (based on digital signature or encryption)	Do not care
Nonrepudiation	Backup might be harmful (based on digital signature)

Encryption private keys need to be backed up if the key pair is used to protect stored data or in some other situations—for example, when an organization wants to be able to decrypt all data entering or leaving the corporation for audit or regulatory purposes. In the case of private keys used for authentication purposes, for example, for a Web client to authenticate to a Web server, or for a software developer to sign its code releases, there is no need to back up the private key (because a lost key means no loss of data), nor is there any particular objection to backing up such a private key.

In the case of a digital signature with nonrepudiation properties—for example, a digital signature on a document intended to be legally binding but with a risk the signer might subsequently deny signing it—it may be detrimental to have a backed-up private key: the signer might successfully repudiate the signature by claiming that another copy of the private key exists that might have been used by an imposter to forge a signature.

You can see from the examples above that if a private-key pair used for encryption purposes needs to be backed up, that key should not be used for nonrepudiation purposes, because doing so could weaken the nonrepudiation characteristic. If you have an application that faces both these requirements simultaneously, you should generate and maintain two key pairs—one to be used for each purpose, and only one of which has its private key backed up.

VeriSign Managed PKI supports dual key pairs when this approach is a requirement. However, VeriSign wants its customers to understand the requirement's true nature. Dual key pairs are rarely required in PKI-based technology.

Secure Sockets Layer (SSL) Web server needs no backup private key, because a lost key can be replaced, and the same is true of an SSL Web client and software signing. For Internet applications, it is sometimes necessary for an enterprise to back up its employees' private keys, but the nonrepudiation issue does not generally arise in the same application. For example, is it realistic that an employee, facing accusation of fraudulently submitting a padded expense claim, might mount the defense that his or her employer had forged the expense claim by signing it with a backed-up private key? Digital signature-based nonrepudiation is unlikely to be applicable in such a case.

When multiple organizations transact business over an extranet, signed transactions may

need to be nonrepudiatable; therefore, the legitimate owners of private keys should hold them closely. But why would there be a backup requirement, except for a possible local one, when the key is backed up under the full control of its legitimate owner? Can one organization be expected to give its private keys for backup purposes to an organization it does business with?

Dual key pairs are necessary in a situation in which, on one hand, an enterprise trusts an entity to hold the private key that can unlock its private data but, on the other hand, distrusts that same entity because it might forge the enterprise's digital signature. However, this scenario is not realistic in the context of making decisions about procuring application products.

Key-Backup Risks

Backup of user private keys is problematic to enterprises because of the enormous risks it presents. Consider, for example, the following simplistic key-backup approach employed by the typical vendor of PKI software products: All user private keys are backed up in the local database of the PKI manager system on the enterprise's premises. The database is encrypted, and the encryption key is made available on the basis of one or two administrators logging on and presenting passwords. In other words, all the private keys of the corporation are stored in one place, dependent on the security of one workstation, with one mechanism for unlocking the database.

In the event an intruder penetrates that workstation and plants a virus, or someone learns an enterprise administrator's password, or one of the administrators is bribed or otherwise decides to turn against the organization, every corporate secret is exposed. The only way to counter these risks is to place the system in a highly physically secured facility, isolate the system from all network access, and install the most stringent of procedures for screening, supervision, and training of operational and maintenance personnel—but at what cost, and with what residual risk?

Fortunately, there is a better way: use state-of-the-art key-recovery technology and a distributed-architecture approach. VeriSign is unique in offering such an approach to enterprise customers.

Few applications require dual key pairs, but VeriSign supports them for those that do. Stand-alone vendors of PKI software vendors that have built their architectures around universal dual key pairs unnecessarily lock the enterprise into proprietary client software.

VeriSign Key-Management Solution

VeriSign offers an enterprise key-recovery solution that involves the VeriSign® Key Management Service, an optional software system installed on an enterprise's premises that operates in conjunction with a VeriSign Managed PKI service. This combination allows an enterprise manager to control backup and recovery of user private keys and digital certificates with minimal risks and minimal security costs.

Private keys are stored on the enterprise's premises in a nonvulnerable, enveloped form. Each user's private key is individually encrypted with its own Triple Data Encryption Standard (Triple DES) symmetric key generated in Federal Information Processing Standard (FIPS) 140-1 level-2 registered hardware. A key-escrow record (KER) is generated using state-of-the-art key-recovery technology, and the Triple DES key is combined with a random-session key mask also generated in hardware and destroyed. Only the resulting masked-session key (MSK) is securely sent and stored at VeriSign. The KER (containing the end user's private key) and the random-session key mask are stored in the Key Manager database on the enterprise's premises.

Recovery of a private key and a digital certificate requires the VeriSign Managed PKI administrator to securely log on and authenticate to the VeriSign Managed PKI Control Center, select the appropriate key pair to recover, and click a hyperlink. Only after an approved administrator takes the final step is the MSK for that key pair returned from the Managed PKI database, operated out of VeriSign's secure data center.

The administrator automatically submits a link to the appropriate key pair and the MSK to the Key Manager database on the enterprise's premises. The Key Manager database combines the MSK with the random-session key mask and regenerates the Triple DES key used to originally encrypt the private key, allowing recovery of the end user's private key. As a final step, an encrypted Public Key Cryptography Standards #12 (PKCS#12) file is returned to the administrator and ultimately distributed to the end user.

This design has significant security advantages over the single-point-of-failure key-backup databases offered by competing PKI-software vendors. Note the following features:

- The user private keys never leave enterprise premises, and VeriSign has no access to them.
- The security requirements surrounding the Key Manager database are modest. Should an intruder obtain copies of the encrypted private keys and KERs, that intruder still cannot gain access to the VeriSign Managed PKI recovery functionality within the Managed PKI Control Center. This precaution obviates the need for a high-grade secure facility to house the Key Manager at the enterprise.
- In a worst-case scenario, in which an intruder obtains all the enterprise's encrypted private keys and KERs, as well as administrator access to the VeriSign Managed PKI service, private keys can still be recovered only one by one. VeriSign will maintain records of the unusual recovery activity, thereby greatly limiting the damage that can be done.

When an enterprise needs to back up private keys, the paramount requirements are enterprise control and high security. With the state-of-the-art key-management solution offered by VeriSign, private keys are held by the enterprise but can be exposed only after a confirming transaction with a highly secure center. PKI built on PKI-component software leaves all the costs of security, and all the risk, with the enterprise.

Most significantly, the VeriSign key-management solution works with native Microsoft, Netscape, and IBM® Lotus® Web and mail clients, in addition to products that have been enabled by VeriSign through one of the supported toolkits. This feature contrasts with competitive PKI solutions that work only with proprietary clients from the PKI vendor.

How VeriSign Compares

The VeriSign key-recovery solution compares favorably with those of PKI product vendors. For example, the table below compares the VeriSign key-management solution with that of Entrust.®

Table 2

Feature	VeriSign Managed PKI	Entrust
Dual-key support	YES	YES
Encryption private keys are backed up	YES	YES
Private keys never leave enterprise	YES	YES
Support for full key histories	YES	YES
Key database is invulnerable to single-point attack	YES	NO
Disaster recovery	YES	NO
Works with out-of-the box clients	YES (Including IBM Lotus, Microsoft, and Netscape Web clients only)	NO (Entrust proprietary and mail clients)

+ For More Information

For more information about VeriSign Managed PKI, please call 650-426-5310, or visit www.verisign.com/products/pki.

Visit us at www.Verisign.com for more information.

©2005 VeriSign, Inc. All rights reserved. VeriSign, the VeriSign logo, "Where it all comes together," and other trademarks, service marks, and designs are registered or unregistered trademarks of VeriSign and its subsidiaries in the United States and in foreign countries. Microsoft is a trademark of Microsoft Corporation. IBM and Lotus are trademarks of IBM Corporation. Netscape is a trademark of Netscape Communications. All other trademarks are the property of their respective owners.