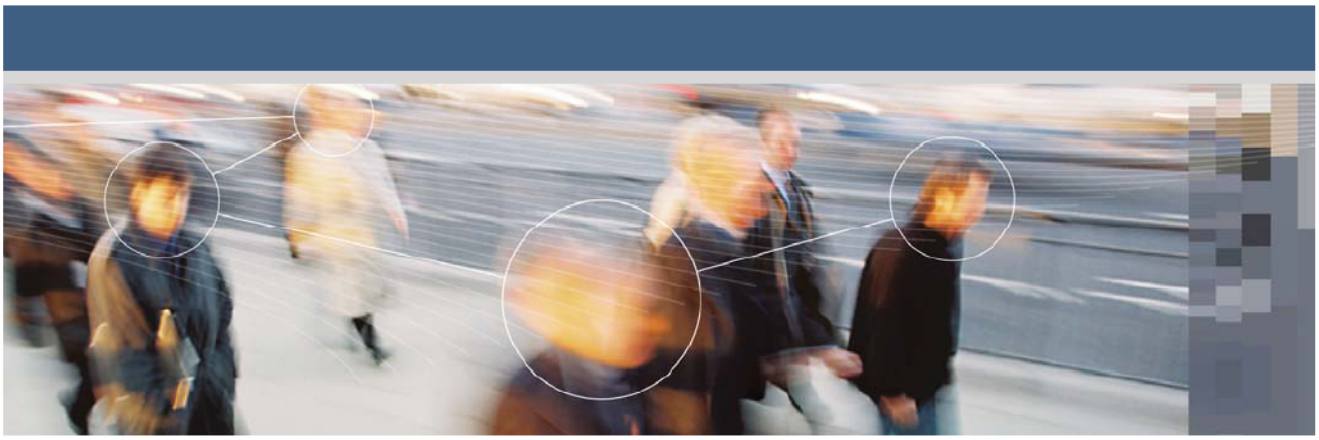
Entrust® Securing Digital Identities & Information



Entrust Managed Services PKI™
Why you need to keep a key history

Document issue: 1.0
September 2009

What is a key history?

When you issue certificates, those certificates have keys associated with them that let users encrypt, decrypt, sign, authenticate and perform other cryptographic operations. As these keys age, the risk of compromise to them increases. Just like a password, a key that's been around for three years will have had many more opportunities to be cracked than a key that's only been around for one. To mitigate this risk, keys are updated periodically, and the older ones placed in storage. (The current key is also placed in storage.) This collection of keys, both old and new, is known as the user's key history.

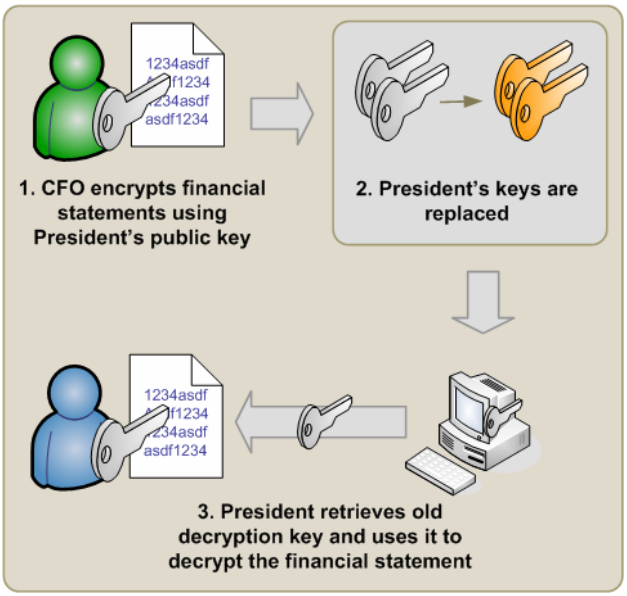
Why keep older keys?

If keys are no longer in use, why bother hanging on to them? Why not simply discard them? The answer is that the older keys *are* still used, albeit less frequently than the new ones. The following examples illustrate this point.

Example 1: Decrypting older documents

1. Your company's CFO encrypts financial statements for the President using the President's public encryption key.
2. The President's encryption key pair expires and is replaced.
3. The President now wants to decrypt the financial statements. His current decryption key won't work, because the statements were encrypted with an older public key. Instead, software on the President's computer retrieves the older decryption key from storage and uses it to decrypt the statements.

If this older key were not available, it would be impossible to decrypt the statements, and the information in them would be lost forever.



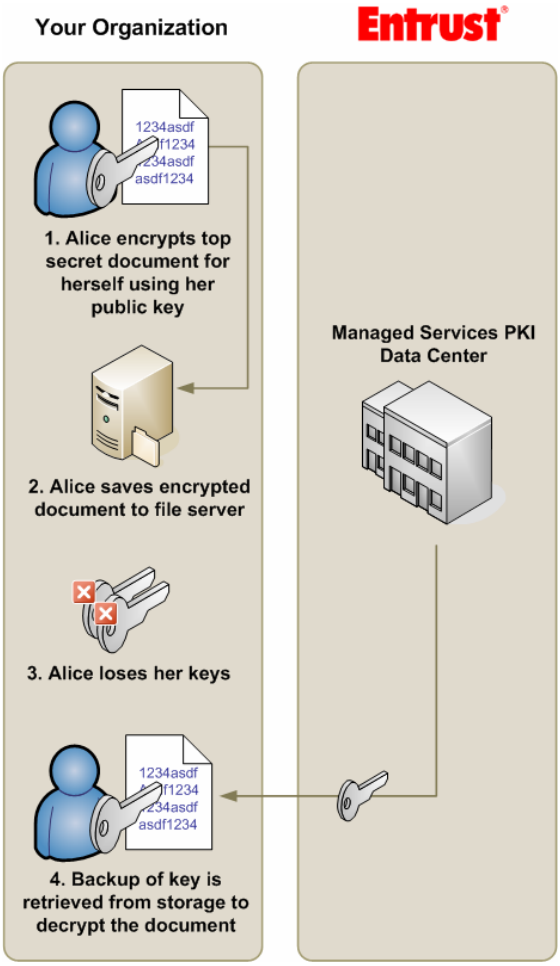
Why keep the current key in the key history?

As mentioned earlier, not only are older keys kept in storage: the current key is also kept in storage in case of theft, loss, or damage. Example 2 illustrates when the current key might be retrieved from the key history.

Example 2: Losing a key

1. Alice encrypts a top secret document for herself using her encryption key.
2. Alice saves the document on a file server, which gets backed up nightly.
3. Alice's computer becomes infected with a virus, causing her to lose all her data, including the key necessary to decrypt the top secret document. The top secret document is itself safe on the file server, but remember, it is encrypted.
4. The only to way to decrypt the document is to retrieve Alice's current decryption key from storage.

If this key had not been placed in storage, it would be impossible to decrypt the file, and the information in it would be lost forever.



Why your organization needs key histories

It is absolutely imperative that a key history be preserved for each user. Without a key history, encrypted data will be lost.

The value of Entrust Managed Services PKI

When you issue certificates through Entrust Managed Services PKI, a full key history is kept for each user on our servers in a state-of-the-art 24x7x365 facility. Entrust's offering delivers these benefits:

No extra charge for key backup

The fee for maintaining a key history is included in the price of the service. Most other vendors charge extra.

No setup at your site

There is no need to run a server at your site to maintain the key histories. All histories are backed up by Entrust, at its facilities.

Secure facilities and service

Entrust's data center offers high-end servers with enterprise-class monitoring, access control, high-availability and disaster recovery mechanisms. Entrust's security practices undergo an annual ISO 21188 audit accepted by the US federal government.

Fully automated key backup

Microsoft offers a key history feature, but it requires that your IT staff periodically export (decrypt) the key histories of all your users and then re-import (re-encrypt) them with a new key after the old one expires. This manual and error-prone overhead is not required with Entrust: key backup and encryption is fully automated, with no chance of human error or data loss.

Information

Contact: 1-888-690-2424, email: entrust@entrust.com

For more information, see http://www.entrust.com/managed_services.