End User Encryption Key Protection Policy

Created by or for the SANS Institute. Feel free to modify or use for your organization. If you have a policy to contribute, please send e-mail to stephen@sans.edu.

1.0 Purpose
This document describes Information Security's required protections for encryption keys that are under the control of end users. These protections are designed to prevent unauthorized disclosure and subsequent fraudulent use. The protection methods will include operational and technical controls, such as key backup procedures, encryption under a separate key and use of tamper-resistant hardware.

2.0 Scope
This policy applies to any encryption keys listed below and to the person responsible for any encryption key listed below. The encryption keys covered by this policy are:

encryption keys issued by <Company Name>;
encryption keys used for <Company Name> business; or
encryption keys used to protect data owned by <Company Name>.

The public keys contained in digital certificates are specifically exempted from this policy.

3.0 Policy
All encryption keys covered by this policy must be protected to prevent their unauthorized disclosure and subsequent fraudulent use.

3.1 Secret Key Encryption Keys
Keys used for secret key encryption, also called symmetric key encryption, must be protected as they are distributed to all parties that will use them. During distribution, the symmetric encryption keys must be encrypted using a stronger algorithm with a key of the longest key length for that algorithm authorized in <Company Name>'s Acceptable Encryption Policy. If the keys are for the strongest algorithm, then the key must be split, each portion of the key encrypted with a different key that is the longest key length authorized and the each encrypted portion is transmitted using different transmission mechanisms. The goal is to provide more stringent protection to the key than the data that is encrypted with that encryption key.

Symmetric encryption keys, when at rest, must be protected with security measures at least as stringent as the measures used for distribution of that key.

3.2 Public Key Encryption Keys
Public key cryptography, or asymmetric cryptography, uses public-private key pairs. The public key is passed to the certificate authority to be included in the digital certificate issued to the end user. The digital certificate is available to everyone once it issued. The private key should only be available to the end user to whom the corresponding digital certificate is issued.

3.2.1 <Company Name>'s Public Key Infrastructure (PKI) Keys
The public-private key pairs used by the <Company Name>'s public key infrastructure (PKI) are generated on the tamper-resistant smart card issued to an individual end user. The private key associated with an end user's identity certificate, which are only used for digital signatures, will never leave the smart card. This prevents Information Security from escrowing any private keys associated with identity certificates. The private key associated with any encryption certificates, which are used to encrypt email and other documents, will be escrowed as covered in the <Company Name> Certificate Practice Statement Policy. Access to the private keys stored on a <Company Name> issued smart card will be protected by a personal identification number (PIN) known only to the individual to whom

the smart card is issued. The smart card software will be configured to require entering the PIN prior to any private key contained on the smart card being accessed.

3.2.2 Other Public Key Encryption Keys
These types of keys are generated in software on the end user's computer and can be stored as files on the hard drive or on a hardware token. If the public-private key pair is generated on smartcard, the requirements for protecting the private keys are the same as those for private keys associated with <Company Name's> PKI. If the keys are generated in software, the end user is required to create at least one backup of these keys and store any backup copies securely. The user is also required to create an escrow copy of any private keys used for encrypting data and deliver the escrow copy to the local Information Security representative for secure storage. Information Security shall not escrow any private keys associated with identity certificates. All backups, including escrow copies, shall be protected with a password or passphrase. Information Security representatives will store and protect the escrowed keys as described in the <Company Name> Certificate Practice Statement Policy.

3.2.2.1 Commercial or Outside Organization Public Key Infrastructure (PKI) Keys
In working with business partners, the relationship may require the end users to use public-private key pairs that are generated in software on the end user's computer. In these cases, the public-private key pairs are stored in files on the hard drive of the end user. The private keys are only protected by the strength of the password or passphrase chosen by the end user. For example, when an end user requests a digital certificate from a commercial PKI, such as VeriSign or Thawte, the end user's web browser will generate the key pair and submit the public key as part of the certificate request to the CA. The private key remains in the browser's certificate store where the only protection is the password on the browser's certificate store. A web browser storing private keys will be configured to require the user to enter the certificate store password anytime a private key is accessed.

3.2.2.2 PGP Key Pairs
If the business partner requires the use of PGP, the public-private key pairs can be stored in the user's key ring files on the computer hard drive or on a hardware token, for example, a USB drive or a smart card. Since the protection of the private keys is the passphrase on the secret keying, it is preferable that the public-private keys are stored on a hardware token. PGP will be configured to require entering the passphrase for every use of the private keys in the secret key ring.

3.3 Hardware Token Storage
Hardware tokens storing encryption keys will be treated as sensitive company equipment, as described in <Company Name>'s Physical Security policy, when outside company offices. In addition, all hardware tokens, smartcards, USB tokens, etc., will not be stored or left connected to any end user's computer when not in use. For end users traveling with hardware tokens, they will not be stored or carried in the same container or bag as any computer.

3.4 Personal Identification Numbers (PINs), Passwords and Passphrases
All PINs, passwords or passphrases used to protect encryption keys must meet complexity and length requirements described in <Company Name>'s Password Protection Policy.

3.5 Loss and Theft
The loss, theft, or potential unauthorized disclosure of any encryption key covered by this policy must be reported immediately to Information Security. Information Security personnel will direct the end user in any actions that will be required regarding revocation of certificates or public-private key pairs.

4.0 Enforcement
Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

5.0 Definitions

Term	Definition
Asymmetric key encryption	See public key encryption.
Certificate authority (CA)	An entity that issues digital certificates for use by other parties. It is an example of a trusted third party.
Digital certificate	An electronic document that uses a digital signature from a certificate authority (CA) to bind together a public key with an identity—the individual's name, email address, etc.

Digital signature	A mathematical scheme for demonstrating the authenticity of a digital message or document. If valid, a digital signature gives the recipients assurance that the signer sent the message and that it was not altered in transit.
Plaintext	Data that is not encrypted
Cipher text	Data that has been encrypted.
Key	A piece of information that determines the functional output of a cryptographic algorithm.
Key escrow	An arrangement in which the private keys needed to decrypt encrypted data are held by the issuing organization so that, under certain circumstances, an authorized third party may gain access to those keys.
Secret key cryptography	Secret key cryptography uses the same key at both ends of the communications channel to encrypt the plaintext message or decrypt the cipher text.
Symmetric key encryption	See secret key encryption.
Public key cryptography	A cryptographic approach that uses public key-private key pairs. This type of cryptography uses asymmetric key algorithms because the key used to encrypt a message is not the same as the key used to decrypt it.
Public-private key pairs	Two encryption keys that are generated together and have the characteristic that data encrypted by one can be decrypted by the other. The keys are related mathematically, but the private key cannot be feasibly (i.e., in actual or projected practice) derived from the public key. Used in public key cryptography.

6.0 Revision History
08/12/2009 - 1.0 initial policy version, Rick Smith