Provo City School District Technology Security Policy

Encryption Procedure

Last Update Status: *Updated January 2015*

1. Overview

The purpose of this procedure is to provide guidance that limits the use of encryption to those algorithms that have received substantial public review and have been proven to work effectively. Additionally, this procedure provides direction to ensure that Federal regulations are followed, and legal authority is granted for the dissemination and use of encryption technologies outside of the United States.

Encryption Key Management, if not done properly, can lead to compromise and disclosure of private keys used to secure sensitive data and hence, compromise of the data. While users may understand it is important to encrypt certain documents and electronic communications, they may not be familiar with minimum standards for protection encryption keys.

2. Purpose

This procedure outlines the requirements for protecting encryption keys that are under the control of end users. These requirements are designed to prevent unauthorized disclosure and subsequent fraudulent use. The protection methods outlined will include operational and technical controls, such as key backup procedures, encryption under a separate key and use of tamper-resistant hardware.

3. Scope

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

- Encryption keys issued by PCSD
- Encryption keys used for PCSD business
- Encryption keys used to protect data owned by PCSD

Public keys contained in digital certificates are specifically exempted from this procedure.

4. Procedure

All encryption keys covered by this procedure must be protected to prevent unauthorized disclosure and subsequent fraudulent use.

- Secret Key Encryption Keys

  Keys used for secret key encryption, also called symmetric cryptography, 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 PCSD's *Acceptable Encryption Procedure.* 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.

- 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.

- PCSD's Public Key Infrastructure (PKI) Keys
  The public-private key pairs used by the PCSD'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 the InfoSec Team 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, must be escrowed in compliance with
  PCSD policies.

  Access to the private keys stored on a PCSD 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.

- Other Public Key Encryption Keys
  Other types of keys may be 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 PCSD'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.

  The InfoSec Team shall not escrow any private keys associated with identity certificates. All backups, including escrow copies, shall be protected with a password or passphrase that is compliant with PCSD *Password Procedure*. InfoSec representatives will store and protect the escrowed keys as described in the PCSD *Certificate Practice Statement Procedure*.

- 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.

- 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 key-ring, 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.

- Hardware Token Storage

  Hardware tokens storing encryption keys will be treated as sensitive company equipment, as described in PCSD's *Physical Security procedure*, 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.

- 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 PCSD's *Password Procedure.*

- Loss and Theft

  The loss, theft, or potential unauthorized disclosure of any encryption key covered by this procedure must be reported immediately to The InfoSec Team. InfoSec personnel will direct the end user in any actions that will be required regarding revocation of certificates or public-private key pairs.

- Key Agreement and Authentication

- Key exchanges must use one of the following cryptographic protocols: Diffie-Hellman, IKE, or Elliptic curve Diffie-Hellman (ECDH).

- End points must be authenticated prior to the exchange or derivation of session keys.

- Public keys used to establish trust must be authenticated prior to use. Examples of authentication include transmission via cryptographically signed message or manual verification of the public key hash.
- All servers used for authentication (for example, RADIUS or TACACS) must have installed a valid certificate signed by a known, trusted provider.
- All servers and applications using SSL or TLS must have the certificates signed by a known, trusted provider.

5. Definitions and Terms

The following definition and terms can be found in the SANS Glossary located at: https://www.sans.org/security-resources/glossary-of-terms/

- Certificate authority (CA)
- Digital certificate
- Digital signature
- Key escrow
- Plaintext
- Public key cryptography
- Public key pairs
- Symmetric cryptography