Guidance for backup of Encryption Keys

1. Need for Backup Policy for the Organisation

1.1. Encryption

Encryption is the process of transforming information (referred to as plaintext) using an algorithm (called cipher) to make it unreadable to anyone except those possessing special knowledge, usually referred to as a key; the reverse is called decryption. In case of Public Key Cryptography where a key pair is generated for encryption, the clear text is encrypted using one key and complementary key is used for decryption.

1.2. Necessity to backup

Following are some situations when it is necessary to recover encryption keys:

- An employee loses the private encryption key and cannot read encrypted mail/documents (tender etc.).
- An employee is on an extended leave, and someone needs to access an encrypted document.
- An employee leaves the company, and company officials need to perform an audit that requires gaining access to the employee's encrypted data.

Therefore, if data is being encrypted, somebody must manage the keys and there must be a key backup/recovery procedure in place.

2. Backup Procedure

2.1. Encryption key pair given by NICCA

NICCA has a dual key pair policy, i.e. two key pairs are given – one for Digital Signature and one for Encryption. After the request for certificate issuance of Encryption key pair is processed, the user is asked to download the certificate. The certificate is downloaded as a password protected file.

2.2. Taking backup

The file which is downloaded from the NICCA website needs to be backed up securely in case of contingencies mentioned at 1.2 above.

2.2.1. Different media to take backup

Backup of the file can be taken in different media like CD, pen drive, smart card etc. A comprehensive list of all the storage media and their pros and cons are given in Annexure I.

2.2.2. Backup procedure

Choose the appropriate media from the above-mentioned in Annexure I.

a. In case the media chosen is from Sr no. 1 to 4. then copy the file downloaded from NICCA website into the media and store it securely.

b. In case the media chosen is Sr. no. 5 or 6 then the file downloaded from NICCA website has to be imported into the media as per the manual given along with the media.

After ensuring that the file has been created in the media chosen, the downloaded file has to be destroyed from the computer (in this case deleted). The password pertaining to should be written and kept in a tamper proof sealed envelope.

3. Safekeeping of the Backups

3.1. Backups have to be kept in a fire proof safe, preferably with split control. This means that the key should not be accessible by a single individual.

4. Key Recovery Procedures

4.1. Procedures must be in place to ensure that the keys can be recovered only after the requisite permission from the competent authority has been obtained. The key recovery must be done in the presence of witnesses.

The key may be needed to be recovered in the following cases:

a. Loss of the key
b. Unable to use the key stored in the Crypto device because of loss of pin to access the device.

Once the key has been taken out and the encrypted data is recovered (decrypted), a new encryption key pair must generated and the data must be encrypted using the new key pair. This must be stored as per the procedure.

In case of loss of key, the CA must be informed for initiating the revocation procedure.

In case the pin is lost, the recovery procedure remains the same. After the data is decrypted the encryption key pair can be imported into the user device.

ANNEXURE I

The table below is from the guidelines advised by Controller of Certifying Authorities (CCA), giving the pros and cons of different storage media.
Ref: http://cca.gov.in/rw/pages/storageofprivatekey.en.do

Sr. No	Storage media	Advantages	Disadvantages
1.	Computer Hard Disk	Easiest	1. Computer must be maintained in a secure fashion (access should be restricted etc.) 2. Any backups taken must also be protected is a similar way as they will contain a copy of the private key.
2.	Floppy	1. Easy to use 2. Can be carried on person	1. Private key can be taken out of the floppy. 2. Floppy may get corrupted. 3. The device does not contain any cryptographic module built into it to enable the creation of secure digital signature. 4. In case of Floppy the private key can be overwritten.

3.	CD-R/RW	1. Easy to use 2. Can be carried on person	1. Private key can be taken out of the CD-R/RW. 2. CD-R/RW may get corrupted. 3. The device does not contain any cryptographic module built into it to enable the creation of secure digital signature. 4. In case of CD-RW the private key can be overwritten.
4.	Pen Drives/USB Drives/Flash Drives	1. Easy to use 2. Can be carried on person	1. Private key can be taken out of the USB drive. 2. The device does not contain any cryptographic module built into it to enable the creation of secure digital signature. 3. In case of USB Drive the private key can be overwritten.
5.	Smart Cards	1. Once generated on the smart card **the private key does not come out of the device in its original form**. 2. The smart card has **a chip built into it, which has crypto modules** to enable the signing/encryption/decryption operation to happen in the card itself.	1. Requires a smart card reader to be attached to the computer. 2. Cost is more.
6.	USB Crypto Tokens	1. Once generated on the USB crypto token **the private key does not come out of the device in its original form**. 2. The USB crypto token **has crypto modules** to enable the signing/encryption/decryption operation to happen in the token itself. 3. Does not require any special reader, can be used on any machine since USB ports are available on almost all PCs.	1. Cost is more.