P.O. Box 6082, Willemstad, Curaçao – Telephone: +1 (631) 480 2118 (USA)

End-user Encryption Key Protection Policy

Document version: 01-2023

1 – Purpose

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's important to encrypt certain documents and electronic communications, they may not be familiar with minimum standards for the protection of encryption keys. This policy 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.

2 – 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 the following.

1. Encryption keys issued by CUN.
2. Encryption keys used for CUN's business.
3. Encryption keys used to protect data owned by CUN, its students, employees and affiliates.

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

3 – 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 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 CUN'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

1. The public-private key pairs used by CUN'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 'escrowing' any private keys associated with identity certificates. The private key associated with any encryption certificates, which are used to encrypt e-mail and documents, must be 'escrowed' in compliance with CUN's policies.
2. Access to the private keys stored on a CUN 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. 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 a smartcard, the requirements for protecting the private keys are the same as those for private keys associated with CUN'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 CUN's ICT Department, for secure storage.
4. CUN 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 CUN's Password Policy. CUN will store and protect the escrowed keys.
5. In working with CUN 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.
6. 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 smartcard. 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, in case of outside 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 and passphrases, used to protect encryption keys, must meet complexity and length requirements described in CUN's Password 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 CUN's ICT Department. ICT staff will direct the end-user in any actions that will be required regarding revocation of certificates or public-private key pairs.

4 – Policy compliance

CUN will verify compliance to this policy through various methods, including but not limited to, business tool reports and internal and external audits.

Any exception to the policy must be approved by CUN's ICT Department in advance.

Any user found to have violated this policy may be subject to disciplinary action

5 – Revision History

Date of Change	Summary of Change
January 1, 2023	