Encryption Policy

Doorway

ISO 27001 Annex A: A.10.1.1, A.10.1.2, A.14.1.2, A.18.1.5

Keywords: Encryption key management

Purpose

This policy defines organizational requirements for the use of cryptographic controls, as well as the requirements for cryptographic keys, in order to protect the confidentiality, integrity, authenticity, and nonrepudiation of information.

Scope

This policy applies to all systems, equipment, facilities and information within the scope of Doorway's information security program. All employees, contractors, part-time, and temporary workers, service providers, 3rd party integrations and those employed by others to perform work on behalf of the organization having to do with cryptographic systems, algorithms, or keying material are subject to this policy and must comply with it.

Background

This policy defines the high level objectives and implementation instructions for Doorway's use of cryptographic algorithms and keys. It is vital that the organization adopt a standard approach to cryptographic controls across all work centers in order to ensure end-to-end security, while also promoting interoperability. This document defines the specific algorithms approved for use, requirements for key management and protection, and requirements for using cryptography in cloud environments.

Roles and Responsibilities

The Security Officer is responsible for updating, reviewing, and maintaining this policy.

Policy

Cryptography Controls

Doorway must protect individual systems or information by means of cryptographic controls as defined in Table 3:

Table 3: Cryptographic Controls

Name of System/Type of Information	Cryptographic Tool	Encryption Algorithm	Key Size
Public Key Infrastructure (PKI) for Authentication	OpenSSL	AES-256	256-bit key
Data Encryption Keys	OpenSSL	AES-256	256-bit key
Virtual Private Network (VPN) keys	OpenSSL and OpenVPN	AES-256	256-bit key
Website SSL Certificate	OpenSSL, CERT	AES-256	256-bit key

Obtaining Information

When required, customers of Doorway's cloud-based software platform offering must be able to obtain information regarding:

- The cryptographic tools used to protect their information.
- Any capabilities that are available to allow cloud service customers to apply their own cryptographic solutions.
- The identity of the countries where the cryptographic tools are used to store or transfer cloud service customers' data.

Governing Law

The use of organisationally-approved encryption must be governed in accordance with the laws of the country, region, or other regulating entity in which users perform their work. Encryption must not be used to violate any laws or regulations including import/export restrictions. The encryption used by Doorway conforms to international standards and U.S. import/export requirements, and thus can be used across international boundaries for business purposes.

Key Management

Except where otherwise stated, keys must be managed by their owners, including the human resources platforms that integrate with Doorway. Cryptographic keys must be protected against loss, change or destruction by applying appropriate access control mechanisms to prevent unauthorised use and backing up keys on a regular basis.

Key Management Service

All key management must be performed using software that automatically manages key generation, access control, secure storage, backup and rotation of keys. Specifically:

- The key management service must provide key access to specifically-designated users, with the ability to encrypt/decrypt information and generate data encryption keys.
- The key management service must provide key administration access to specifically-designated users, with the ability to create, schedule delete, enable/disable rotation, and set usage policies for keys.
- The key management service must store and backup keys for the entirety of their operational lifetime.
- The key management service must rotate keys at least once every 12 months.

Secret Key

Keys used for secret key encryption (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.
- 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 authorised and the each encrypted portion is transmitted using different transmission mechanisms.

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

Public key cryptography (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.

Doorway's Public Key Infrastructure (PKI)

- The public-private key pairs used by the Doorway'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 Doorway policies.
- Access to the private keys stored on a Doorway-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

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 smart-card, the requirements for protecting the private keys are the same as those for private keys associated with Doorway 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 Doorway *Password Policy*.

Commercial/Outside Organization Public Key Infrastructure (PKI)

In working with business partners and 3rd party integrations, 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.

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.

Hardware Token Storage

Hardware tokens storing encryption keys will be treated as sensitive company equipment, as described in Doorway's *Physical Security Policy*, when outside company offices.

- All hardware tokens, smart-cards, 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 Pass-phrases

All PINs, passwords or pass-phrases used to protect encryption keys must meet complexity and length requirements described in Doorway's *Password Policy*.

Loss and Theft

The loss, theft, or potential unauthorised disclosure of any encryption key covered by this policy must be reported immediately.

Revision History

Version	Date	Editor	Description of Changes
1.0	15.03.2022	Henry Sinclair	Initial Creation
2.0	13.10.2022	Hugh Fraser	Inclusion of HR platform integration specifications