POL00362910



# Cyber Security Standard

## Encryption Standard

## Version – V3.2

POL00362910

POL00362910



# 1 Overview

## 1.1 Introduction by the Standard Owner

Post Office is committed to protecting its employees, customers, Third Party Supply Chain and information assets from damaging or illegal actions by individuals, either knowingly or unknowingly. Post Office enables this through the development and deployment of policies, standards and guidelines which are aligned to international best practices. Effective cyber and information security is a team effort involving everyone in Post Office.

## 1.2 Purpose

The purpose of this document is to state a minimum security baseline to ensure encryption controls are applied, where appropriate. This must incorporate effective key management controls and practices to ensure strong key lifecycle management controls vital to guarding against key compromise.

The objective of this standard is to ensure:

- Technical and procedural standards are defined for the safe, efficient and effective deployment of cryptographic services in support of business objectives.
- The use of encryption keys does not expose Post Office to crypto-analysis or brute force key cracking to compromise the data.
- Stored encrypted data can be retrieved and decrypted even if the ordinary method of decrypting data is not possible.
- The distribution of keys to known entities that are authorised to access the encrypted data is controlled and managed.

To ensure compliance to the business requirements, and items which are subject to legal and regulatory related encryption requirements, specific control requirements for the handling of Payment Card Industry – Data Security Standard (PCI-DSS), Data Protection Act 2018 and Government data must be included.

The following requirements will be implemented, where appropriate:

- Encryption for transmission, (data-in-motion).
- Encryption for storage, (data-at-rest).

Encryption solutions will be subject to approval by IT Security and must be fully documented when applied to any Post Office managed service.

## 1.3 Core Principles

To ensure appropriate use and management of encryption controls, (e.g. preserve the integrity of sensitive information and confirm the identity of the originator of transactions or communications).

To work towards meeting this objective it is essential that the following actions are performed:

- A set of business requirements must be gathered and documented.
- A security assessment by IT Security must be performed and documented.

POL00362910



- A Data Privacy Impact Assessment must be performed and documented.
- Based on a review of the above outputs, determine if cryptographic controls are required.

## 1.4 Application

This standard applies to any service provided to the Post office where Post Office data or data processed by the Post Office on behalf of third parties is in transit or at rest.

POL00362910



# 2 Policy Framework

## 2.1 Policy Framework

This standard forms part of the Cyber and Information Security Policy Set. This contains controls that form part of the Information Technology Control Framework (ITCF) governed by the overarching Post Office wide framework.

## 2.2 Who must comply?

Compliance with this standard is mandatory for all Post Office employees and applies wherever in the world Post Offices business is undertaken. All third parties who do business with Post Office, including consultants, suppliers and business and franchise partners, will be required to agree contractually to this standard or have their own equivalent standard/policy.

POL00362910



# 3 Minimum Controls

The table below sets out the minimum control standards.

| Control Ref | Control | Attestation Guidance |
|---|---|---|
| PHT0575 | Manage the use of encryption controls and cryptographic controls. | Employ only secure versions of cryptographic controls.<br>Establish, implement, and maintain an encryption management and cryptographic controls policy.<br>Establish, implement, and maintain cryptographic key management procedures.<br>Disseminate and communicate cryptographic key management procedures to interested personnel and affected parties. |
| PHT0580 | Recover encrypted data for lost cryptographic keys, compromised cryptographic keys, or damaged cryptographic keys. | The organization shall establish procedures for recovering damaged or lost cryptographic keys<br>Cryptographic key management policy, standards and procedures covering key generation, distribution, installation, renewal, revocation, recovery and expiry should be established<br>Maintain availability of information in the event of the loss of cryptographic keys by users. |
| PHT0581 | Generate strong cryptographic keys. | Use approved random number generators for creating cryptographic keys. |
| PHT0583 | Implement decryption keys so that they are not linked to user accounts. | Decryption keys must not be tied to user accounts |
| PHT0584 | Include the establishment of cryptographic keys in the cryptographic key management procedures. | Policies and procedures shall be established, and supporting business processes and technical measures implemented, for the management of cryptographic keys in the service's cryptosystem (e.g., lifecycle management from key generation to revocation and replacement, public key infrastructure) |
| PHT0585 | Disseminate and communicate cryptographic keys securely. | The Key Management Plan should include how cryptographic keys are received<br>The Key Management Plan should include how the cryptographic keys are delivered |

POL00362910



| | | |
|---|---|---|
| | | The Key Management Plan should include local, remote, and central cryptographic key distribution. |
| PHT0586 | Store cryptographic keys securely. | Restrict access to cryptographic keys.<br>Store cryptographic keys in encrypted format.<br>Store key-encrypting keys and data-encrypting keys in different locations. |
| PHT0590 | Change cryptographic keys, as necessary. | Procedures should include the process for changing cryptographic keys at the end of a defined cryptoperiod.<br>The organization must ensure the cryptographic key procedures include the periodic changing of cryptographic keys. The keys should be changed at least annually or whenever a key is suspected of or known to be compromised |
| PHT0591 | Destroy cryptographic keys promptly after the retention period. | Procedures should include processes for archiving, destroying keys |
| PHT0592 | Control cryptographic keys with split knowledge and dual control. | The organization should implement segregation of duties, so one individual does not have knowledge of the entire cryptographic key or access to the all parts that make up the cryptographic key |
| PHT0593 | Prevent the unauthorized substitution of cryptographic keys. | The organization should implement techniques to detect when cryptographic keys are substituted<br>The organization must ensure the cryptographic key procedures include the procedures to prevent unauthorized cryptographic keys from being substituted for the original key |
| PHT0594 | Manage outdated cryptographic keys, compromised cryptographic keys, or revoked cryptographic keys. | Revoke old cryptographic keys or invalid cryptographic keys immediately.<br>Replace known or suspected compromised cryptographic keys immediately. |
| PHT0597 | Require key custodians to sign the key custodian's roles and responsibilities. | Key-management procedures should be implemented to require key custodians to sign a form specifying that they understand and accept their key-custodian responsibilities. |
| PHT0598 | Establish, implement, and maintain Public Key certificate application procedures. | Establish, implement, and maintain Public Key renewal or rekeying request procedures. |
| PHT0600 | Use strong data encryption to transmit restricted data or | See Classification Standard |

POL00362910



| | | |
|---|---|---|
| | restricted information, as necessary. | Configure the encryption strength to be appropriate for the encryption methodology of the cryptographic controls. This applies to both data in transit and data at rest. |
| PHT0602 | Encrypt traffic over public networks with trusted cryptographic keys. | Information communicated between database servers and web applications is encrypted.<br>The control system shall provide the capability to protect the confidentiality of information traversing any zone boundary |
| PHT0603<br>CTRL0020609 | Establish trusted paths to transmit restricted data or restricted information over public networks or wireless networks. | Protect application services information transmitted over a public network from unauthorized modification.<br>Protect application services information transmitted over a public network from unauthorized disclosure.<br>Protect application services information transmitted over a public network from contract disputes.<br>Protect application services information transmitted over a public network from fraudulent activity.<br><br>An assessment is performed to define:<br>- All network communication methods that require protection; and<br>- required encryption depending on types of content being transferred.<br><br>The assessment is aligned with POL's Encryption Standard<br><br>All exceptions are appropriately managed e.g. remediation or included as part of a residual risk assessment. |
| PHT0615 | Disseminate and communicate any changes in the cryptosystem to interested personnel and affected parties. | Establish a standard change management procedure, to accommodate changes from internal and external sources, for review, approval, implementation and communication of cryptographic, encryption and key management technology changes |

POL00362910



# 4 Cryptographic Provision Guidance

Where cryptographic services are required, only approved cryptographic solutions (i.e. tools, processes, algorithms, and key lengths) are to be used.

The approved algorithms can be found in section 5 Minimum Requirements.

There will be a documented cryptography security and key lifecycle management solution that will consist of, at a minimum, the following:

- Effective security governance arrangements of cryptographic controls, when used to reduce information risk and securing of data.
- Operation of the service with a view to good industry standard security practices, ensuring operational management processes and procedures (i.e. cryptographic keys and digital certificates) used by the technologies.
- Safeguard encryption keys with at least one, if not all, of the following options:
    - Encryption key files within an encryption key management system.
    - Encryption key files with a trusted third party through an agreed escrow service.
- Roles and responsibilities are clearly defined and individuals with the required expertise fulfil each role.
- Policies, processes, procedures and implementation mechanisms must be in place for encrypting sensitive information when required for:
    - Data-at-rest (e.g. information systems, application, databases and endpoints).
    - Data-in-motion (e.g. system interfaces, electronic messaging, and untrusted networks).
    - Integrity.
    - Non-repudiation.
- Digital certificates deployed comply with the X.509 standard.
- Strong cryptographic and security protocols are regularly reviewed to identify any risks or vulnerabilities.

## 4.1 Public Key Infrastructure

A documented process for managing cryptographic keys must be established which includes the following:

- Generation of cryptographic keys using industry recommended key lengths (see section 4 'Minimum Requirements' for further details).
- Secure distribution, activation, storage, recovery and replacement/update of cryptographic keys.
- Immediate revocation (deactivation) of cryptographic keys (e.g. if a key is compromised, or a key owner changes job or leaves the Post Office). Management of cryptographic keys that may have been compromised, such as by disclosure to an external party.
- Recovery of cryptographic keys that are lost, corrupted or have expired. Backup/archive of cryptographic keys and the maintenance of cryptographic key history (e.g. to allow access to backed up or archived information).
- Allocation of defined activation/de-activation dates.
- Restriction of access to cryptographic keys to authorised individuals.

POL00362910



- The encryption solution should not allow for or accept substitution of keys coming from unauthorized sources or unexpected processes
- Sharing of cryptographic keys (e.g. using split key generation) required for protecting sensitive information and critical systems.
- Actions to be taken in the event of loss or compromise of the public key infrastructure.
- Establishment of a root Certification Authority (CA) and one or more subsidiary CAs (sub-CAs). Use of Post Office root CA to sign sub-CA's, which will be used to produce operational cryptographic material.
- Methods of protecting important internal CAs (and related sub-CAs).
- Integration of the public key infrastructure with business applications and technical infrastructure that will use it.
- Establishment of one or more Registration Authorities (RAs).

## 4.2 Risk-based Assessments

The selection and implementation of a cryptographic solution must take into account the following:

- Assessing the risks (including legal risks) associated with using cryptographic solutions (including encryption algorithms).
- Identifying legal obligations (for relevant jurisdictions).
- Identify the data types (e.g. PCI-DSS, client, customer, business, HR data etc.).
- Identify data that is hosted and communicated (e.g. at-rest and/or in-motion).

IT Security are responsible for:

- Approving the use of cryptographic solutions.
- Approving the assignment of responsibilities for cryptographic solutions.
- Providing advice regarding conflicting laws and regulations (including dealing with license issues) relating to the use of encryption (cryptographic solutions) in different jurisdictions.
- Reviewing compliance and providing input into the requirements to ensure the technology supports future capabilities.

## 4.3 Key Management

Ensure that the security of the encrypted data by the cryptographic scheme cannot be undermined by malicious intent directed at the key management process, protecting access to the keys in storage that could be used to compromise trust in the cryptographic scheme.

- Key management should address the following stages of the lifecycle:
- Key generation
- Key registration
- Key storage
- Key distribution and installation
- Key use
- Key rotation
- Key backup
- Key recovery
- Key revocation

POL00362910



- Key suspension
- Key destruction

## 4.4 Compromise of Cryptographic Material

The Post Office must be informed of any known breach or compromise of a cryptographic key or certificate as this is classed as a potential Security Incident. All Security Incidents must to be reported using the agreed Incident Management Process, which will be managed in accordance with contractual obligations.

In order to contain any potential impact to the integrity and confidentiality of Post Office data, all compromised cryptographic keys or certificates may need to be revoked and replaced, subject to completion of evidence gathering as part of any forensic investigation.

## 4.5 PCI-DSS

All payment cardholder data in scope for PCI-DSS must be encrypted in accordance with the current PCI-DSS standards

POL00362910



# 5 Minimum Requirements

Not all combinations of algorithms and key sizes are appropriate. To enhance interoperability obtain authentication, signature, and key establishment certificates with complementary algorithms for all public keys.

The following table shows the **minimum requirements** for various cryptographic uses:

Hash function summary

| Primitive | Output Length | Recommendation | |
|---|---|---|---|
| | | Legacy | Future |
| SHA-2<br>SHA-3<br>Whirlpool | 256, 384, 512<br>256, 384, 512<br>512 | ✓<br>✓<br>✓ | ✓<br>✓<br>✓ |
| SHA-2<br>RIPEMD-160<br>SHA-1 | 224<br>160<br>160 | ✓<br>✓<br>✓ | ×<br>×<br>× |
| MD-5<br>RIPEMD-128 | 128<br>128 | ×<br>× | ×<br>× |

Recommended Algorithms and Key Sizes

| | Legacy | Recommendation | |
|---|---|---|---|
| | | Legacy | Future |
| AES Symmetric Key Size | 80 | 128 | 256 |

**Please note - Symmetric key encryption is subject to key search attacks, (e.g. brute force attacks). To minimize the risk of key search attacks, longer key lengths decrease the possibility of successful attacks.**

| Key Type | Algorithms and Key Sizes |
|---|---|
| Digital Signature keys used for authentication (for User or Devices) | RSA (2048 bits)<br>ECDSA (Curve P-256) |
| Digital Signature keys used for non-repudiation (for User or Devices) | RSA (2048 bits)<br>ECDSA (Curve P-256 or P-384) |
| CA and OCSP Responder Signing Keys | RSA (2048 bits or 3072 bits)<br>ECDSA (Curve P-256 or P-384) |
| Key Establishment Keys (for Users or Devices) | RSA (2048 bits)<br>Diffie-Hellman (2048 bits)<br>ECDSA (Curve P-256 or P-384) |

POL00362910



The private keys of important internal CAs and related sub-CAs must be reviewed by IT Security and should be protected by:

Storing them on approved hardware (e.g. a hardware storage module (HSM)), which is subject to strong logical and physical controls.

Sharing them across two or more authorised individuals (often referred to as secret splitting or key sharing) to avoid misuse of the CA (and related sub-CAs).

The following table shows the recommendations for CAs:

Digital Signature Recommendations for CAs and OCSP Responders.

| Public Key Algorithms and Key Sizes | Hash Algorithms | Padding Scheme |
|---|---|---|
| RSA (2048 or 3072 bits) | SHA-256 | PKCS #1 v1.5 |
| ECDSA (Curve P-256) | SHA-256 | N/A |
| ECDSA (Curve P-384) | SHA-256 | N/A |

Recommendations Combinations for the Recommended Algorithms and Key.

| Authentication Key Type | Signature key | Key Establishment |
|---|---|---|
| RSA 2048 | RSA 2048 | RSA 2048 |
| RSA 2048 | RSA 2048 | Diffie-Hellman 2048 |
| ECDSA P-256 | ECDSA P-256 | ECDH P-256 |
| ECDSA P-256 | ECDSA P-384 | ECDH P-384 |
| ECDSA P-384 | ECDSA P-384 | ECDH P-384 |

POL00362910



# 6 Where to go for help

## 6.1 Additional Policies

This standard is part of the Cyber Security Policy framework. The full set can be found at:

https://poluk.sharepoint.com/sites/cybersecurity2/SitePages/Cyber-and-Information-Security-Policy-Set.aspx

## 6.2 How to raise a concern

Any Post Office employee who suspects something is wrong has a duty to:

- Discuss the matter fully with their Line Manager; or,
- Report their suspicions by contacting the Service Desk.

## 6.3 Who to contact for more information

If you need further information about this standard or wish to report an issue in relation to this standard, please contact Cyber Security Team via cyber GRO

POL00362910



# 7 Version Control & Approval

## 7.1 Version Control

| Date | Version | Updated by | Change Details |
|---|---|---|---|
| 30/12/2016 | 1.0 | IT Security | Final version |
| 15/03/2018 | 1.1 | IT Security | Changed to the new template for policies<br>Changed to reflect the new Post Office structure<br>Minor editorial changes at annual review |
| 23/05/2018 | 1.2 | IT Security | Updated post peer review |
| 08/06/2018 | 2.0 | IT Security | Final Version |
| 13/01/2020 | 2.1 | IT Security | Updated to include minimum controls |
| 12/06/2020 | 2.1 | Cyber Security | Approved by ISC |
| 28/07/2021 | 2.2 | Cyber Compliance | Final version submitted for approval |
| 02/08/2021 | 3.0 | Cyber Compliance | Approved by ISC |
| 23/11/2022 | 3.1 | Cyber Compliance | Updated to align with control framework |
| 25/04/2023 | 3.2 | Cyber Compliance | CSF Approval for publication |

## 7.2 Standard Approval

**Standard Owner:** Chief Information Security Officer
**Standard Author:** Ehtsham Ali
**Approved by Owner:** 25/04/2023
**Next review:** 25/04/2024