Security Standard – Public Key Infrastructure & Key Management (SS-002)

Chief Security Office

Date: September 2017

Department for Work & Pensions

IMPORTANT. DWP Security Policies and Standards apply to DWP suppliers and contractors where explicitly stated in the Security Schedule of the contract. DWP Standards are not a cross government requirement.

Version Control Table

Version	Date	Major Change

Updating policy

This Standard will be reviewed for continued completeness, relevancy and accuracy within 1 year of being granted “final” status, and at yearly intervals thereafter.

The version control table will show the published update date and provide a thumbnail of the major change. CAUTION: the thumbnail is not intended to summarise the change and not a substitute for reading the full text.

IMPORTANT. DWP Security Policies and Standards apply to DWP suppliers and contractors where explicitly stated in the Security Schedule of the contract. DWP Standards are not a cross government requirement.

Contents

1. Introduction

1.1. This Public Key Infrastructure & Key Management Security Standard provides the list of controls that are required to secure objects such as digital certificates, private keys and symmetric keys to a Department for Work and Pensions (DWP) approved level of security. It is to minimise the risk from known threats both physical and logical to an acceptable level for operations.

1.2. For further clarity and relevance, this standard is aligned to the Department's internal technical strategy paper, the DWP Digital Blueprint, which defines the direction for all departmental technology.

1.3. Furthermore the security controls presented in this standard are taken from the international best practice for Cryptographic Key Management (e.g. those best practices provided by the Open Web Application Security Project (OWASP)) and have been tailored for Departmental suitability.

2. Purpose

2.1. The purpose of this document is to enable teams to work to a defined set of security requirements which enable solutions to be developed, deployed and managed to Departmental security standards, which are based upon international best practice for deployments of cryptography.

2.2. Secondly, this standard provides a means to conduct compliance based technical security audits and IT Health Checks (ITHCs).

3. Exceptions

3.1. In this document the term "MUST" in upper case is used to indicate an absolute requirement. Failure to meet these requirements will require a formal exemption as detailed below.

3.2. Any exceptions to the application of this standard or where controls cannot be adhered to MUST be presented to an assigned Security Architect and considered for submission to the DWP Design Authority (DA) advisory or governance board, where appropriate. This MUST be carried out prior to deployment and managed through the design caveats or exception process.

3.3. Such exception requests may invoke the Risk Management process in order to clarify the potential impact of any deviation to the configuration detailed in this standard.

3.4. Exceptions to this standard MUST be maintained on the system or project's risk register for accountability, traceability and security governance reporting to senior management.

4. Audience

4.1. This standard is intended for consumption by suppliers, technical architects, database administrators, developers, security groups, and also IT staff such as security compliance teams, involved in securing environments for DWP systems and applications.

5. Scope

5.1. This standard is to cover systems handling data within the OFFICIAL tier of the Government Security Classification Policy (GSCP), which includes the handling caveat OFFICIAL-SENSITIVE. All of the organisation's deployments of asymmetric and symmetric cryptography falling within this category will be subject to the requirements specified within this security standard. The requirements will be applied to new and existing installations.

5.2. The security control requirements laid out in this standard are product agnostic and applicable for all systems that are provisioned for departmental use – including those provisioned in Infrastructure as a Service (IaaS) and Platform as a Service (PaaS) environments.

6. Security Controls Assurance

6.1. Controls presented in this standard or referred to via this standard may be subjected to a formalised IT Health Check to provide evidence of adequacy and effectiveness.

7. Technical Security Control Requirements

This standard is complementary to SS-007 Security Standard – Use of Cryptography. SS-007 will provide requirements for key generation, key lengths, appropriate algorithms, and software/hardware selection. This standard will provide requirements for the ongoing management, storage and use of cryptographic keys.

10.1. Digital Certificates and Asymmetric Cryptography

Reference	Security Control Requirement
10.1.1	Cryptographic keys MUST only be generated for use with approved algorithms and key lengths as specified in SS-007 Security Standard – Use of Cryptography.
10.1.2	All requests for digital certificates MUST contain a Certificate Signing Request (CSR) in an appropriate format. For self-signed certificates, the CSR MUST contain information agreed upon by both the signing entity/entities and the consuming entity/entities. For CA-signed certificates, the CSR MUST conform to the CA's template and the DWP's X.509 Certificate Policy.
10.1.3	Immediately after generation, private asymmetric keys MUST be held securely in accordance with Section 10.3.
10.1.4	Private certificate-signing keys MUST be protected in accordance with a suitable policy from the DWP X.509 Certificate Policy, and have an associated approved Certification Practice Statement (CPS).
10.1.5	Certificate generation, issuance and management MUST be conducted in accordance with a suitable policy from the DWP X.509 Certificate Policy throughout all stages of its lifetime.
10.1.6	Digital certificates MUST be generated with a maximum lifetime of: a) Twenty (20) years, for a Root CA key pair; b) Ten (10) years, for a Subordinate CA key pair; c) Two (2) years, for an end-user key pair. These requirements are additionally subject to the exceptions defined in the DWP X.509 Certificate Policy.
10.1.7	Asymmetric key pairs not found in digital certificates MUST only be used for a maximum of five (5) years before re-key. Keys that are used often may be subject to a more stringent re-key requirement.
10.1.8	Digital certificates MUST be re-keyed (i.e. a new key pair generated and a new certificate requested) whenever a replacement certificate is necessary (e.g. due to expiry, compromise, etc.).
10.1.9	Systems consuming digital certificates MUST have available to them an up-to-date and resilient source of revocation information. This source of revocation information MUST be checked prior to accepting a certificate, and a revoked certificate MUST not be trusted.

10.2. Symmetric Cryptography

Reference	Security Control Requirement
10.2.1	Symmetric keys MUST only be generated for use with approved algorithms, modes of operation and key lengths as specified in SS-007 Security Standard – Use of Cryptography.
10.2.2	Immediately after generation, the symmetric key MUST be held securely in accordance with Section 10.3 below.

IMPORTANT. DWP Security Policies and Standards apply to DWP suppliers and contractors where explicitly stated in the Security Schedule of the contract. DWP Standards are not a cross government requirement.

10.3. Secure Key Management

Reference	Security Control Required
10.3.1	Software and hardware used to generate and protect secret keys MUST be selected in accordance with: a) The DWP X.509 Certificate Policy; and b) SS-007 Security Standard – Use of Cryptography.
10.3.2	A key or key pair MUST only be used for a single purpose (i.e. authentication keys cannot be used for encryption, signing keys cannot be used for key wrapping).
10.3.3	Generated asymmetric private keys and symmetric keys MUST be transported using a secure channel where the level of security is commensurate with the level of security granted by the key(s) themselves.
10.3.4	Asymmetric private keys and symmetric keys MUST be stored in location(s) where the principle of least privilege is used to grant or deny access to those key(s).
10.3.5	The service enforcing the principle of least privilege (e.g. a Hardware Security Module or an isolated cryptographic vault) MUST provide a level of security commensurate with the level of security granted by the asymmetric private keys or symmetric keys to be protected.
10.3.6	Asymmetric private keys and symmetric keys MUST be encrypted on persistent memory when not in active use.
10.3.7	Asymmetric private keys and symmetric keys MUST be integrity protected while not in active use.
10.3.8	Asymmetric private keys and symmetric keys MUST be cleansed from volatile memory when not in active use (i.e. overwritten with zeros).
10.3.9	Cryptographic operations (e.g. encryption, decryption, signing, etc.) MUST be performed within the confines of the cryptographic vault or cryptographic hardware, and never directly on the system where the encrypted or decrypted data will be stored or processed.
10.3.10	If a single key is relied upon to provide access to a system or quantity of data, that key MUST be backed-up or escrowed, unless the key belongs to a CA. CA keys MUST never be escrowed.
10.3.11	Backed-up and escrowed keys MUST be protected to at least the same level as the operational key.
10.3.12	Keys and key pairs MUST be unambiguously attributable to a single entity. Sharing of keys and key pairs is strictly prohibited.
10.3.13	There MUST be a mechanism to immediately revoke all authorisations associated with keys used for authentication and signing. This mechanism MUST be resilient in the face of denial of service attacks, and MUST be resistant against being used in a denial of service attack.
10.3.14	In the event of key compromise or suspected key compromise, all authorisations associated with those affected key(s) MUST be immediately revoked; unless a key compromise recovery plan has identified that availability is more important than confidentiality and integrity, in which case the key compromise recovery plan MUST be followed.
10.3.15	A key compromise recovery plan MUST be documented and easily accessible to all relevant parties. The plan MUST include details of: a) The identity and contact details of person(s) who should be notified; b) The identity and contact details of person(s) who will perform recovery actions; c) The re-key method; d) An inventory of all keys and their uses; e) The monitoring of the re-keying operations; f) Steps to identify all information which may be compromised as a result of the incident, and all signatures that may be invalid as a result of the incident; g) Method of distribution for new key material; and

Reference	Security Control Required
	h) Steps required to install the new key material.
10.3.16	Trust stores MUST be configured in accordance with the principle of implicit deny (i.e. where all required trust chains are whitelisted, with all others denied).
10.3.17	Once configured, import and export operations on trust stores MUST be subject to strict access controls and objects stored in the trust store MUST be integrity protected.

8. Compliance

Compliance with this standard MUST occur as follows:

Compliance	Due Date
On-going	From the first day of approval
Retrospective	12 months after approval

9. Accessibility

No user interfaces are included in this standard and accessibility is not applicable as part of this standard. However it is deemed that projects implementing this standard are obliged to incorporate accessibility functions where necessary.

10. Security Standards Reference List

Document Name	Location	Version
Exceptions Process		XX
DWP X.509 Certificate Policy		V1.0
SS-007 Security Standard – Use of Cryptography		1.0

11. Reference Documents

DWP Digital Blueprint – Blueprint Online

12. Definition of Terms

Term	*Definition*
Secret Key	A parameter passed to a cryptographic algorithm which would cause damage to confidentiality, integrity, authenticity or accountability if it was disclosed to an unauthorised party.
DWP X.509 Certificate Policy	A set of mandatory requirements governing the issuance and on-going management of internal, self-signed digital certificates within the Department.
Certification Practice Statement	A document written by a Certificate Authority (CA) describing its own security controls, processes and procedures; demonstrating how it has met the requirements stated in the corresponding Certificate Policy.
Digital Signature	The result of a cryptographic transformation of data that, when properly implemented with a supporting infrastructure and policy, provides the services of: 1. Origin authentication; 2. Data integrity authentication; 3. Signer non-repudiation.
Key Renewal	The process by which a current key or key pair has its lifetime extended.
Key Re-key	The process by which a current key or key pair is replaced by a new, randomly generated key or key pair.
Digital Certificate	An electronic document used to prove the ownership of a public key.
X.509	A standard that defines the format of public-key certificates.
Principle of Least Privilege	The principle by which an individual or entity has access to only those systems and services that they are absolutely necessary to access as part of their job function.
Key Escrow	A data security measure in which a key is untrusted to a third party (i.e. kept in escrow).
Principle of Implicit Deny	The principle by which all access is denied unless explicitly configured to be accepted for a specific scenario.

13. Glossary

ITHC	IT Health Check
CSR	Certificate Signing Request
CA	Certificate Authority
CP	Certificate Policy
CPS	Certification Practice Statement
HSM	Hardware Security Module

14. Controls Catalogue Mapping

The requirements in this standard are derived from the high-level controls prescribed in the DWP Controls Catalogue.