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

Chief Security Office

Date: 25/03/2025

Department for Work & Pensions

This PKI & Key Management Security Standard is part of a suite of standards, designed to promote consistency across the Department for Work and Pensions (DWP), and supplier base with regards to the implementation and management of security controls. For the purposes of this standard, the term DWP and Authority are used interchangeably.

Technical security standards form part of the DWP Digital Blueprint which is a living body of security principles, architectural patterns, code of practice, practices and radars, that aim to support Product Delivery Units (PDUs) and suppliers in delivering the DWP and HMG Digital Strategy. Security standards and policies considered appropriate for public viewing are published here:

Government Publications Security Policies and Standards

Technical security standards cross-refer to each other where needed, so can be confidently used together. They contain both mandatory and advisory elements, described in consistent language (see table below).

(Important note for screen reader users.) Paragraphs that contain a **'must'** statement, and therefore denote a mandatory requirement, will contain the following statement after the heading:

(Important) this paragraph contains 'must' activities.

Table 1 – Terms

Term	Intention
must	denotes a requirement: a mandatory element.
should	should denotes a recommendation: an advisory element.
may	denotes approval.
might	denotes a possibility.
can	denotes both capability and possibility.
is/are	is/are denotes a description.

1. Contents

Contents

2. Revision history

Version	Author	Description	Date
1.0		First published version	18/09/2017
2.0		Full update in line with current best practices and standards; • Updated Intro, purpose, audience, scope; added reference to CIS v8 security controls • Added NIST CSF references • Compliance changed to Security Assurance • 11.1 – Added statements on random number generation, key encryption and storage, certificate lifetimes, cert revocation and use of OCSP • 11.2 – Added statements on random number generation, key encryption and storage • 11.3 – Added requirements for CA usage, storage and encryption, symmetric key sharing • 11.4 – Added requirements for escrowed key encryption and retention, use of trust stores, allow listing • 11.5 – Added key inventory requirements • 11.6 – Added Key revocation requirements	22/03/2023

		• 11.7 – Added monitoring and alerting requirements 11.8 – Added Auditing requirements	
2.1		All NIST references reviewed and updated to reflect NIST 2.0 All security measures reviewed in line with risk and threat assessments Approval history - Review period changed to up to 2 years Intro – Quantum computing 11.1.9 Use of publicly trusted CA, where possible and available 11.1.11 Use of OCSP removed 11.3.1 Must 11.3.12 Validate key access requests 11.3.13 Key management systems patching 11.3.14 Monitoring key management systems 11.4.4 KEK monitoring External References – SS-033 Patching Standard Glossary - KEK	25/03/2025

3. Approval history

Version	Name	Role	Date
1.0		Chief Security Officer	18/09/2017
2.0		Chief Security Officer	22/03/2023
2.1		Chief Security Officer	25/03/2025

This document is continually reviewed to ensure it is updated in line with risk, business requirements, and technology changes, and will be updated at least every 2 years - the current published version remains valid until superseded.

4. Compliance

Compliance with this standard will be verified through various methods, including ut not limited to:

- controls tests performed by 1st line teams and by 2nd line activities (e.g. security testing teams)
- security assurance activities to ensure that Architectural Design and delivery are appropriate and aligned to applicable Authority Security Standards. [See Security Assurance Strategy – Ref. H].
- independent external audit

Results of these will be fed back to the appropriate Authority Risk and System Owners.

5. Exceptions Process

(Important) this paragraph contains ‘must’ activities.

In this document the term **“must”** is used in bold letters to indicate a mandatory security measure. Any exceptions to the application of this standard, or where specific security measures cannot be adhered to, **must** be presented to the Authority. This **must** be carried out prior to deployment and managed through the design caveats or exception process.

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

Exceptions to the standard **must** be maintained on a risk register for accountability, traceability, and security governance reporting to senior management.

6. Audience

This document is intended for, but not necessarily limited to, technical architects, engineers, developers, security teams, project teams, including suppliers engaged in the design, development, implementation and operation of systems, services and applications.

7. Accessibility statement

(Important) this paragraph contains ‘must’ activities.

Users of this standard **must** consider accessibility design requirements as appropriate. Further information on accessibility standards can be found in Appendix F.

8. Introduction

(Important) this paragraph contains ‘must’ activities.

This PKI & Key Management Security Standard defines the minimum technical security measures that **must** be implemented to secure objects such as digital certificates, private keys and symmetric keys for use within the Authority.

One of the biggest challenges that cryptography faces today is the future threat from quantum computing, which leverages the properties of quantum physics to perform operations that are impossible or impractical for classical computers, and thus has the potential to impact public key infrastructure. To address this challenge, post-quantum cryptography (PQC) algorithms are being developed that are resistant to quantum attacks. See ‘NIST Post-Quantum Cryptography’ and ‘NCSC: Post-Quantum Cryptography – what comes next ?’ [External References].

See the DWP Approved Cryptographic Algorithms document [Ref. I] for approved algorithms.

As this standard only provides minimum measures, they **should** be exceeded as appropriate depending on the threats and risks that need to be addressed, the sensitivity of the data, and in keeping with latest security enhancements.

The security measures are derived from industry best practice i.e. guidance published by NIST, CIS, NCSC and OWASP (see Appendix C for full list external references) and support the implementation of appropriate security controls as selected by the Authority or our third party providers, such as the CIS Critical Security Controls set. [see External References]

Every effort has been made to ensure the security measures are vendor and technology agnostic as far as possible; this is to ensure greater applicability of the standard regardless of the technologies used. The security measures **may** be implemented in different ways, depending on the technology choices and business requirements in question.

The aim of this standard is to:

- ensure security controls that are applicable to PKI & key management are implemented consistently across the Authority and by third party providers where applicable.
- mitigate risks from common threats and vulnerabilities associated with PKI & key management, to an acceptable level for operation.
- support the achievement of security outcomes described in Appendix A.

Technical security standards ultimately support the achievement of security outcomes sought by the Authority. They set the expectations for what needs to be done to achieve them and why, and provide an objective, measurable statement of the Authority's existing security posture in a number of important areas. The outcomes are based on the official NIST sub-categories where possible to ensure close alignment with the NIST Cyber Security Framework (CSF) and are enabled by the implementation of controls from the CIS Critical Security Controls set. [see External References]. Those relevant to the subject of each standard can be found in Appendix A of every technical security standard.

9. Purpose

The purpose of this standard is to ensure that Authority systems and services are designed, configured, deployed, and managed consistently to protect against typical threats at the OFFICIAL tier.

This standard also serves to provide a baseline in which assurance and compliance activities can be carried out, so that the Authority can be assured that security obligations are being met or exceeded.

10. Scope

(Important) this paragraph contains ‘must’ activities.

This standard provides security measures that apply to all Authority PKI & key management deployments, (including those deployed in cloud environments) or those owned or managed by an Authority supplier or contracted third party as part of an Authority activity.

All cloud PKI deployments should refer to this standard for the minimum security measures, and any exceptions **must** be logged as per the exceptions process referenced above.

Where FIPS 140 is referenced, the *dash numbers* are not included e.g. FIPS 140-2. The reason for this is that these represent versions of the standard that are valid for a period of time for certification to be issued against. These certificates have a defined lifespan, so that older versions of the FIPS 140 standard expire over time. Hence newer versions of the FIPS standard are automatically covered.

Any queries regarding the security measures laid out in this standard **should** be sent to the Authority.

11. Minimum Technical Security Measures

(Important) this paragraph contains ‘must’ activities.

The following section defines the minimum security measures that **must** be implemented to achieve the security outcomes described in Appendix A. For ease of reference, the official NIST sub-category ID is provided against each security measure e.g. PR.PT-3, to indicate which outcome(s) it contributes towards. Refer to Appendix A for full description of outcomes.

This standard is complementary to SS-007 Use of Cryptography Security Standard [Ref. A]. 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.

11.1. Digital Certificates and Asymmetric Cryptography

(Important) this table contains ‘must’ activities.

Reference	Minimum Technical Security Measures	NIST ID
11.1.1	Asymmetric keys **must** only be generated using random number generators (RNG) in line with FIPS 140-2 Security Requirements for Cryptographic Module Annex C: Approved Random Number Generators [see External References].	PR.DS-02 PR.DS-10
11.1.2	Asymmetric keys **must** be generated on the end entity/subject where they are to be used. If this is not possible and keys need to be generated away from the end entity/subject, then it **must** be encrypted in transit and at rest.	PR.DS-01 PR.DS-02 PR.DS-10
11.1.3	Any access to Asymmetric keys **must** be monitored, authenticated, and authorised.	PR.AA-01 PR.AA-02 PR.AA-03
11.1.4	A CA’s private asymmetric key **must** be generated and stored securely in a cryptographic vault, such as a hardware security module (HSM), or an isolated cryptographic service, in accordance with Section 11.3, both of which **must** be in line with SS-007 Use of Cryptography Security Standard [Ref. A].	PR.DS-01
11.1.5	Private keys for any end entity/subject **must** be stored in an approved and secured storage device (such as a Trusted Platform Module [TPM] using a TPM 2.0 hardware chip for laptop devices for example), in line with SS-007 Use of Cryptography Security Standard [Ref. A].	PR.DS-01

11.1.6	All requests for digital certificates **must** contain a Certificate Signing Request (CSR) in an appropriate format. The CSR **must** not be trusted until it is verified, then forwarded to the CA to issue the certificate. Deployments of self-signed certificates do exist on the Authority estate due to legacy requirements, but do not meet the requirements of this standard. For this reason, 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 Authority's X.509 Certificate Policy [Ref. B].	PR.IR-01
11.1.7	Private certificate-signing keys **must** be protected in accordance with a suitable policy from the Authority's X.509 Certificate Policy [Ref. B] and have an associated approved Certification Practice Statement (CPS). This also includes any third-party provider acting as an Authority Certificate Authority (CA), who **must** also develop a Certification Practice Statement (CPS).	PR.DS-01 GV.OC-03
11.1.8	Certificate generation, issuance and management **must** be conducted in accordance with a suitable policy from the DWP's X.509 Certificate Policy [Ref. B] throughout all stages of its lifetime.	PR.DS-01 PR.DS-02
11.1.9	Digital certificates **must** be generated with a maximum lifetime of: a) Twenty (20) years, for a Root CA key pair; b) Fifteen (15) years for a policy CA key pair;	PR.DS-01 PR.DS-02

	c) Five (5) years, for a Subordinate CA key pair; d) Two (2) years, for an end-entity key pair; e) One (1) year may be necessary depending on the end device type. Some specific use cases will mandate lifetimes lower than the figures stated above which are permitted. Certificate lifetimes **must** be short as they reduce the opportunity for an attacker. End entity certificate lifetimes **must** be proportional to the risk, use-case, and administration overhead required to keep the certificates active. • All certificates are to be provided by the Authority’s Enterprise PKI Service (Signed and Provisioned) wherever possible and available. Where this is not possible, an approved publicly trusted certificate authority **must** be used. • Any subcategorisation, within the certificate, must not be based on a left-sided wildcard (e.g. *.cert) as this has known vulnerabilities. These requirements are additionally subject to the exceptions defined in the Authority’s X.509 Certificate Policy [Ref. B].	
11.1.10	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.).	PR.DS-01 PR.DS-02

11.2. Symmetric Cryptography

(Important) this table contains 'must' activities.

Reference	Minimum Technical Security Measures	NIST ID
11.2.1	Symmetric keys **must** only be generated using random number generators (RNG) in line with FIPS 140-2 Security Requirements for Cryptographic Module Annex C: Approved Random Number Generators [see External References].	PR.DS-01 PR.DS-02
11.2.2	Immediately after generation, the symmetric key **must** be held securely in accordance with Section 11.3 below, and SS-007 Use of Cryptography Security Standard [Ref. A].	PR.DS-01 PR.DS-02
11.2.3	Symmetric keys **must not** be disclosed to any parties that do not have authorised access to the object the key is protecting, as in accordance with Section 11.3 below.	PR.AA-05 PR.DS-01 PR.DS-02
11.2.4	Symmetric key-wrapping keys **must** only be used to encrypt other keys that use symmetric-key algorithms as in accordance with Section 11.3 below and **must not** be used for any other purpose.	PR.DS-01 PR.DS-02
11.2.5	After the originator-usage period has passed, a symmetric key **must not** be utilised for further protection.	PR.DS-02

11.3. Secure Key Management

(Important) this table contains ‘must’ activities.

Reference	Minimum Technical Security Measures	NIST ID
11.3.1	The root CA **must** be kept offline and **must** be unavailable for certificate issues and other use. It **must** only be used when an authorised function must be completed, which **must** be audited and witnessed by the Crypto Custodian.	PR.DS-01 PR.DS-02 PR.AA-05
11.3.2	All domains, applications and endpoints **must** have access to an approved CA.	PR.DS-01 PR.DS-02
11.3.3	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).	PR.DS-01 PR.DS-02
11.3.4	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.	PR.DS-02
11.3.5	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, in line with SS-007 Use of Cryptography Security Standard [Ref. A].	PR.DS-01 PR.DS-02

11.3.6	Asymmetric private keys and symmetric keys **must** be encrypted on persistent memory when not in active use. This process **must** be conducted using approved cryptographic algorithms. See the DWP Approved Cryptographic Algorithms Excel Workbook [Ref. I] for approved algorithms.	PR.DS-10
11.3.7	Asymmetric private keys and symmetric keys **must** be cleansed from volatile memory when not in active use (i.e. overwritten with zeros).	PR.DS-10
11.3.8	Asymmetric private keys and symmetric keys **must** be integrity protected while not in active use. See the DWP Approved Cryptographic Algorithms Excel Workbook [Ref. I] for approved algorithms.	PR.DS-10
11.3.9	Cryptographic operations (e.g. encryption, decryption, signing, etc.) **must** be performed using approved cryptographic algorithms. See the DWP Approved Cryptographic Algorithms Excel Workbook [Ref. I] for approved algorithms.	PR.DS-01 PR.DS-02
11.3.10	Keys and key pairs **must** be unambiguously attributable to an entity (‘entity’ refers to an individual person or machine). Sharing of keys and key pairs is strictly prohibited.	PR.AA-01 PR.AA-04
11.3.11	Administration of the PKI environment **must** be in line with SS-001 (part 2) Privileged User Access Security Standard [Ref. G).	PR.AA-05
11.3.12	Requests to access keys, including automated requests from API calls or operating systems, **must** be validated before being granted.	PR.AA-04

11.3.13	Key management systems **must** be kept up to date in line with SS-033 Security Patching Standard [Ref. J].	PR.PS-02 ID.AM-08
11.3.14	Key management systems **must** be monitored for anomalies such as unusual patterns or activities that may indicate a potential attack. Anomaly detection mechanisms can help identify and respond to suspicious behaviour promptly.	DE.CM-09

11.4. Key Backup & Storage

(Important) this table contains 'must' activities.

Reference	Minimum Technical Security Measures	NIST ID
11.4.1	If a single key is relied upon to provide access to a system or data, that key **must** be backed-up or escrowed, unless the key belongs to a CA. CA keys **must** never be escrowed.	PR.DS-11
11.4.2	Backed-up and escrowed keys **must** be protected to at least the same level as the operational key. Any database that is used to store the keys **must** be encrypted using at least a FIPS 140 certified and validated module. See the DWP Approved Cryptographic Algorithms Excel Workbook [Ref. I] for approved algorithms.	PR.DS-01 PR.DS-11
11.4.3	Backup keying material **must** remain accessible for at least as long as any data dependent on it is required for access or legislative retention requirements. Once the data is no longer required and is due for deletion, the keys **must** be deleted as well.	PR.DS-01 PR.DS-11

11.4.4	Keys that are stored in offline devices **must** be encrypted using Key Encryption Keys (KEKs) or on an approved secure device / trust store. These **must** be equivalent to, or stronger than, the keys being safeguarded. Monitoring **must** be in place to ensure that Key Encryption Keys are not used unless properly authorised.	PR.DS-01
11.4.5	Approved secure devices / trust stores **must** be configured in accordance with the principle of implicit deny (i.e. where all required trust chains are allow listed, with all others denied).	PR.DS-01
11.4.6	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.	PR.AA-01 PR.AA-02

11.5. Key Inventory

(Important) this table contains 'must' activities.

Reference	Minimum Technical Security Measures	NIST ID
11.5.1	A key inventory **must** be implemented and **must** contain details regarding each key. However, the inventory **must not** contain secret or private keys, and **must** only reference these with a key identifier or a pointer to the key's location. Details of what entity/subject owns the key, key type, intended algorithm, length, usage and expiration date **must** all be included in the inventory. Key inventory **must** be managed in accordance with the DWP Cryptographic Key Management policy [Ref. E].	PR.DS-01

11.5.2	A certificate inventory **must** be implemented and **must** contain details regarding each certificate, such as the owners name and contact information. The certificates' public keys' corresponding private keys **must** not be listed in the inventory. Key inventory **must** be managed in accordance with the DWP Cryptographic Key Management policy [Ref. E].	PR.DS-01

11.6. Key Revocation & Compromise

Different environments may have specific requirements regarding key revocation, please refer to the relevant security design patterns for PKI on the Architecture Blueprint for more information.

(Important) this table contains 'must' activities.

Reference	Minimum Technical Security Measures	NIST ID
11.6.1	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.	PR.AA-05 PR.IR-01
11.6.2	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.	GV.PO-02 PR.AA-05 PR.IR-01

11.6.3	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 h) Steps required to install the new key material.	DE.CM-09 RS.MA-01 RC.RP-02
11.6.4	The key revocation method **must** be regularly updated and signed; otherwise, a compromised key may not be advertised in a timely manner.	ID.AM-08
11.6.5	Any revocation of a key **must** be recorded in a centralised logging platform.	PR.PS-04

11.7. Monitoring and Alerting

(Important) this table contains ‘must’ activities.

Reference	Minimum Technical Security Measures	NIST ID
11.7.1	To provide full visibility of PKI operations, CA logs **must** be exported to a central logging facility in line with SS-012 Protective Monitoring Security Standard [Ref. F]. Access to these logs **must** be restricted to authorised users and stakeholders only, in line with SS-001 (part 2) Privileged User Access Security Standard [Ref. G]. Write access **must** be limited and safeguards **must** be in place to detect changes in logs.	PR.AA-05 PR.PS-04

11.8. Auditing

(Important) this table contains ‘must’ activities.

Reference	Minimum Technical Security Measures	NIST ID
11.8.1	An audit capability **must** be in place to identify any vulnerabilities within the PKI environment and key management domain. The three types of audits to be conducted are: • Preliminary and regular compliance audits (preferably automated) **must** be conducted to evaluate if a key management system is ready to operate or to continue to operate in accordance with the DWP Cryptographic Key Management policy [Ref. E]. • Protective mechanisms in place **must** be reviewed on a regular basis to determine if the mechanisms accurately and effectively support the necessary rules, as well as the degree of security they currently offer and are projected to offer in the future. Attacks and new technical advances **must** be considered. The actions of the entities that use, operate, and maintain the system **must** be reviewed to ensure that they are adhering to established security procedures and accessing only those keys and metadata for which they are authorised.	PR.PS-04 DE.CM-09

12. Appendices

Appendix A – Security Outcomes

The minimum security measures defined in this standard contribute to the achievement of security outcomes described in the table below. For consistency, the official NIST Sub-category IDs have been carried through to the standards.

Table 2 – List of Security Outcomes Mapping

Ref	Security Outcome (sub-category)	Related security measures
GV.OC-03	Legal, regulatory, and contractual requirements regarding cybersecurity - including privacy and civil liberties obligations - are understood and managed	11.1.7
GV.PO-02	Policy for managing cybersecurity risks is reviewed, updated, communicated, and enforced to reflect changes in requirements, threats, technology, and organizational mission	11.6.2
ID.AM-08	Systems, hardware, software, services, and data are managed throughout their life cycles	11.3.13, 11.6.4
PR.AA-01	Identities and credentials for authorized users, services, and hardware are managed by the organization	11.1.3, 11.3.10, 11.4.6
PR.AA-02	Identities are proofed and bound to credentials based on the context of interactions	11.1.3, 11.4.6

PR.AA-03	Users, services, and hardware are authenticated	11.1.3
PR.AA-04	Identity assertions are protected, conveyed, and verified	11.3.10, 11.3.12
PR.AA-05	Access permissions, entitlements, and authorizations are defined in a policy, managed, enforced, and reviewed, and incorporate the principles of least privilege and separation of duties	11.2.3, 11.3.1, 11.3.11, 11.6.1, 11.6.2, 11.7.1
PR.DS-01	The confidentiality, integrity, and availability of data-at-rest are protected	11.1.2, 11.1.4, 11.1.5, 11.1.7, 11.1.8, 11.1.9, 11.1.10, 11.1.11, 11.2.1, 11.2.2, 11.2.3, 11.2.4, 11.3.1, 11.3.2, 11.3.3, 11.3.5, 11.3.9, 11.4.2, 11.4.3, 11.4.4, 11.4.5, 11.5.1, 11.5.2
PR.DS-02	The confidentiality, integrity, and availability of data-in-transit are protected	11.1.1, 11.1.2, 11.1.8, 11.1.9, 11.1.10, 11.1.11, 11.2.1, 11.2.2, 11.2.3, 11.2.4, 11.2.5, 11.3.1, 11.3.2, 11.3.3, 11.3.4, 11.3.5, 11.3.9
PR.DS-10	The confidentiality, integrity, and availability of data-in-use are protected	11.1.1, 11.1.2, 11.3.6, 11.3.7, 11.3.8
PR.DS-11	Backups of data are created, protected, maintained, and tested	11.4.1, 11.4.2, 11.4.3,

PR.IR-01	Networks and environments are protected from unauthorized logical access and usage	11.1.6, 11.6.1, 11.6.2
PR.PS-02	Software is maintained, replaced, and removed commensurate with risk	11.3.13
PR.PS-04	Log records are generated and made available for continuous monitoring	11.6.5, 11.7.1, 11.8.1
DE.CM-09	Computing hardware and software, runtime environments, and their data are monitored to find potentially adverse events	11.3.14, 11.6.3, 11.8.1
RS.MA-01	The incident response plan is executed in coordination with relevant third parties once an incident is declared	11.6.3
RC.RP-02	Recovery actions are selected, scoped, prioritized, and performed	11.6.3

Appendix B – Internal References

Below, is a list of internal documents that **should** read in conjunction with this standard.

Table 3 – Internal References

Ref	Document	Publicly Available*
A	SS-007 Use of Cryptography Security Standard	Yes
B	DWP X.509 Certificate Policy	No
C	DWP Strategic PKI HLD V0.17	No
D	PKI Implementation Strategy Version 1.1	No
E	DWP Cryptographic Key Management Policy	Yes
F	SS-012 Protective Monitoring Security Standard	Yes
G	SS-001 (part 2) Privileged User Access Security Standard	Yes
H	Security Assurance Strategy	No
I	DWP Approved Cryptographic Algorithms	No
J	SS-033 Security Patching Standard	Yes

*Request to access to non-publicly available documents **should** be made to the Authority.

Appendix C External references

The following publications and guidance were considered in the development of this standard and **should** be referred to for further guidance.

Table 4 – External References

External Documents List
CIS Critical Security Controls set
NIST 800-57 Rev 5 Recommendation for Key Management
OWASP
NCSC PKI Standards
FIPS 140-2 Security Requirements for Cryptographic Module Annex C: Approved Random Number Generators
What Is Post-Quantum Cryptography? | NIST
NCSC: Post-Quantum Cryptography – what comes next ?

Appendix D Abbreviations

Table 5 – Abbreviations

Abbreviation	Definition
ITHC	IT Health Check
CSR	Certificate Signing Request
CA	Certificate Authority
CP	Certificate Policy
CPS	Certification Practice Statement
HSM	Hardware Security Module
KEK	Key Encryption Key
OCSP	Online Certificate Status Protocol
PQC	Post Quantum Cryptography
TPM	Trusted Platform Module

Appendix E – Definition of Terms

Table 6 – Glossary

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.

Appendix F - Accessibility artefacts

A variety of accessibility guidance is available from the below URL, that includes:

Guidance and tools for digital accessibility

Understanding accessibility requirements for public sector bodies