Security Standard – Use of Cryptography (SS-007)

Chief Security Office

Date: 25/03/2025

This Use of Cryptography 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

2. Revision history

Version	Author	Description	Date
1.0		First published version	04/2017
2.0		Full update in line with current best practices and standards, recorded NIST references and made changes to grammar. Introduction and Scope updated for Mandatory ‘**must**’ statements and introduced Crypto manual. FIPS 140 and CPA assurance requirements updated throughout. 11.1 Reworded 11.1.4 - refined requirement to implement in accordance with Crypto manual that supports assurance TOE 11.2.1 and 11.4.1 - grammar refresh 11.5.1 - PKCS minimum version updated 11.6.3 subsumed into 11.6.2 11.7.2 Introduced TPM 11.8.1 updated Salt value	07/12/2022

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 – Mitigating factors & compensating controls; Quantum resistant cryptography; defence in depth References to NCSC CPA removed as it no longer supports encryption products 11.1.2 Patching cryptographic systems 11.1.7 Monitoring cryptographic systems 11.2.8 Quantum resistant algorithms 11.3.1 Elliptic Curve Cryptography 11.3.2 Must 11.6.4 Logon and privileged functions 11.8.1 Cryptographic salting Internal Refs – version number removed from DWP Approved Crypto Algorithms document External refs & Glossary - Quantum resistant cryptography	25/03/2025

3. Approval history

Version	Name	Role	Date
1.0		Chief Security Officer	02/04/2017
2.0		Chief Security Officer	07/12/2022
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 but 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. D].
- 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. It **must** be applied in the design, assurance, and audit of cryptographic controls deployed across the Authority and supplier base where applicable.

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 standard defines a set of minimum-security measures that **must** be met when implementing cryptographic controls for the purposes of mitigating risks, or to comply with legal and regulatory requirements or both. When considering risk, an assessment **must** include consideration of mitigating factors and compensating controls.

Cryptographic controls **must** be implemented whenever it is necessary to protect the confidentiality and integrity of electronic information in transit or at rest from threats facing the Authority. Threats can be physical or logical in nature such as media containing sensitive data being stolen, or hackers sniffing data packets across the network. Cryptographic controls can also be used to authenticate the identities of both the sender and recipient to one another and protect against repudiation.

Below are some examples of when cryptographic controls **must** be used:

- Sending sensitive data over an untrusted network e.g., between two endpoints over the internet.
- Storing sensitive data in a multi-tenanted cloud hosted environment e.g., passwords, personal citizen information.
- Connecting remote workers from home to access the Authority’s network.
- Protecting citizen data at rest e.g., in databases or object stores.
- To comply with legal or regulatory requirements.

One of the biggest challenges that cryptography faces today is the future threat from substantially more powerful quantum computers. Quantum computing leverages the properties of quantum physics to perform operations that are impossible or impractical for classical computers, and thus has the potential to impact asymmetric, and to a lesser extent symmetric cryptographic operations. 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. B] for approved algorithms.

It should also be noted that weak passwords, social engineering attacks, and accidental data exposure are common pitfalls in maintaining secure encrypted systems, so a ‘defence-in-depth’ approach **must** be followed to protect Authority data.

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 and OWASP (see Appendix C for full list external references) and support the implementation of appropriate security controls as selected by DWP 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:

- enable technical teams to work towards a set of minimum-security measures which are based on industry best practice.
- ensure cryptographic controls are designed, developed, and deployed consistently respecting the cryptographic manual on which validation was awarded.
- ensure cryptographic controls are configured to only use Authority approved cryptographic algorithms as defined in DWP Approved Cryptographic Algorithm document [Ref. B].
- enforce the use of independently assured cryptographic products where needed.

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 systems and services utilising cryptography to encrypt Authority data 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 **must** be applied whenever it is determined that cryptographic controls are required following a security risk assessment process or to satisfy legal and regulatory requirements. Therefore, all the Authority’s ICT systems, networks, and end user devices including portable storage devices are in scope of this standard.

There are however certain measures regarding the use of cryptography in the cloud deliberately excluded from this standard, as this is covered in SS-023 – Cloud Computing Security Standard [Ref. C]. As such, this standard **must** be read in conjunction with SS-023.

It should also be noted that while key management is a fundamental aspect of ensuring the security of information protected by cryptography, this area is outside of the scope of this standard and is covered elsewhere in SS-002 PKI and Key Management Security Standard [Ref. D].

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.

The security measures **must** be applied to new and existing installations, and adherence to these measures **must** be included in all contracts for outsourced services where applicable.

Any queries regarding the security measures laid out in this standard **must** be sent to an assigned DWP Security Architect or Project Team Lead.

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.

11.1. Software and Hardware Requirements

(Important) this table contains 'must' activities.

Reference	Minimum Technical Security Measures	NIST ID
11.1.1	The Cryptographic software deployed **must** be selected having an active validation to FIPS 140 and FIPS 197.	PR.DS-01 PR.DS-02
11.1.2	Systems supporting cryptographic operations **must** be kept up to date in line with SS-033 Security Patching Standard [Ref. E].	PR.PS-02
11.1.3	Cryptographic hardware deployed **must** have an active validation against a recognised scheme. FIPS 140 and FIPS 197 meet this standard.	PR.DS-01 PR.DS-02
11.1.4	Cryptographic software / hardware **must** be deployed, configured, and operated in accordance with the security procedures and cryptographic manual supporting the products' validation.	PR.DS-01 PR.DS-02 PR.PS-01 PR.PS-02 PR.PS-03

11.1.5	Cryptographic software / hardware **must** only be used when still under active vendor support or still inside its validation period.	PR.PS-02 PR.PS-03
11.1.6	Where applicable cryptographic operations **must** be performed on hardware, this requires appropriate validations to be in place; For HSMs, FIPS 140 at level 3 or higher For TPMs, v2.0 or higher Where applicable, cryptographic operations **must** be used in software, this requires appropriate validations to be in place; For software packages, FIPS 140 at level 2 or higher; For software libraries, FIPS 140 at level 1 or higher	PR.DS-01 PR.DS-02
11.1.7	Cryptographic 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

11.2. Cryptographic Algorithm Requirements

(Important) this table contains 'must' activities.

Reference	Minimum Technical Security Measures	NIST ID
11.2.1	Cryptographic algorithms and modes of operation **must** be selected from the DWP Approved Cryptographic Algorithms document [Ref. B]. **Note.** Approval by the Authority is indicated by inclusion in the above document. Where multiple algorithms are deployed, the order of preference given by this document **must** also be technically enforced.	PR.DS-01 PR.DS-02
11.2.2	Approved asymmetric cryptography **must** be used where the use of symmetric cryptography is inappropriate e.g. weaknesses in implementation, unable to handle certificate exchange or physical key exchange, or for authentication purposes.	PR.DS-01 PR.DS-02
11.2.3	The list of approved cryptographic algorithms **must** be reviewed at least annually.	PR.PS-02
11.2.4	Approved hashing algorithms **must** be used as the basis for: • Creating message digests; • Generating digital signatures; • Message Authentication Codes (MACs / HMACs); • Pseudorandom Functions (PRFs); • Key Derivation Functions (KDFs). • See the DWP Approved Cryptographic Algorithms document [Ref. B] for approved algorithms.	PR.DS-01 PR.DS-02

11.2.5	Where information is to be encrypted and authenticated, the Message Authentication Code (MAC) **must** be computed after encryption (i.e. encrypt-then-MAC).	PR.DS-01 PR.DS-02
11.2.6	Use of Elliptic Curve Cryptography (ECC) curves and key parameters **must** be selected from those recommended in the latest version of FIPS 186.	PR.DS-01
11.2.7	Use of Diffie Hellman key exchange algorithm **must** be used in conjunction with the following parameters as appropriate: DH Group 19 DH Group 20 DH Group 21	PR.DS-01
11.2.8	Wherever possible, quantum-resistant algorithms **must** be used. Even though quantum computing capabilities may not currently be mature enough to break many forms of encryption in use today, it is known that threat actors are collecting vast quantities of encrypted data to potentially decrypt once quantum computing capabilities become more generally available. See the DWP Approved Cryptographic Algorithms document [Ref. B] for approved algorithms.	PR.DS-01

11.3. Generation of Cryptographic Key Material

(Important) this table contains ‘must’ activities.

Reference	Minimum Technical Security Measures	NIST ID
11.3.1	Where pseudorandom number generation is required, but not provided as part of vendor software, (including initialisation vectors), this **must** use cryptographically secure sources of entropy (using Elliptic Curve Cryptography). Acceptable sources are: • External modules which have received FIPS 140 certification. • Operating system certified sources (e.g. Microsoft CryptoAPI:NG, /dev/random).	PR.DS-01
11.3.2	Virtual Machines (VMs) and operating systems running on Solid State Drives (SSDs) **must** utilise an assured feed of pseudorandom data from an external entropy feed (as per the section above), as they cannot be relied upon to produce their own, except in the case where an external module described in section 11.3.1 above is deployed.	PR.DS-01

11.4. Compression

(Important) this table contains ‘must’ activities.

Reference	Minimum Technical Security Measures	NIST ID
11.4.1	Compression of data **must** be a separate process to the encryption and decryption operations themselves. Compression routines that execute alongside encryption and decryption functions (e.g. TLS compression) **must** not be used.	PR.DS-01

11.5. Message Padding

(Important) this table contains ‘must’ activities.

Reference	Minimum Technical Security Measures	NIST ID
11.5.1	Messages to be encrypted by an approved asymmetric algorithm **must** use PKCS#1 v2.2 minimum. Fallback to earlier version is not allowed.	PR.DS-01 PR.DS-02

11.6. Encryption in Transit

(Important) this table contains ‘must’ activities.

Reference	Minimum Technical Security Measures	NIST ID
11.6.1	Encrypted communication transiting Authority owned and / or supplier managed infrastructure **must** be designed to support content inspection capabilities as per SS-006 Security Boundaries Security Standard [Ref. A].	PR.DS-02

11.6.2	Encrypted communications channels **must** be protected using protocols, protocol suites and techniques in accordance with the relevant cryptographic manual, the DWP Approved Cryptographic Algorithms document [Ref. B] and require Digital Design Authority approval of the solution.	PR.DS-02
11.6.3	Encrypted sessions **must** re-negotiate new symmetric keys after one of the following criteria is met: The data volume specified in the validation has exceeded its maximum limit The time limit specific in the validation has exceeded its maximum limit.	PR.DS-02
11.6.4	Logon and privileged functions **must** be cryptographically protected to prevent credential leaks.	PR.DS-02

11.7. Encryption at Rest

(Important) this table contains ‘must’ activities.

Reference	Minimum Technical Security Measures	NIST ID
11.7.1	All user-writeable partitions on Authority devices (including laptops, mobile phones, portable storage devices etc.) **must** be encrypted at the media-level (i.e. Full Disk Encryption (FDE)).	PR.DS-01
11.7.2	Where applicable, the master encryption key **must** reside within assured cryptographic hardware and **must** not leave the assured cryptographic hardware for the master keys’ service life.	PR.DS-01

11.7.3	Information held encrypted at rest **must** also be integrity protected.	PR.DS-01
11.7.4	Where multiple layers of encryption are available (e.g. media-level and database field-level), each layer **must** be applied proportionally to mitigate risks identified during a risk assessment process.	PR.DS-01
11.7.5	The encryption software deployed on devices as described in 11.7.1 **must** require sufficient entropy as part of the authentication mechanism. In a scheme that uses a password as the authentication mechanism, this equates to a password that is of sufficient length and complexity to match the requirements in the password policy defined for the system.	PR.DS-01
11.7.6	Encryption software deployed on devices (i.e. laptops, portable storage devices etc.) **must** restrict the number of authentication attempts within any given time interval. Where the number of attempts and time interval are not specified as part of the product’s certification, these values **must** be configured in line with the password policy for the system/device in question.	PR.AA-03 PR.DS-01

11.8. Passwords

(Important) this table contains 'must' activities.

Reference	Minimum Technical Security Measures	NIST ID
11.8.1	For password-based cryptography, incorporating cryptographic salts (i.e. adding random data to passwords before encryption) adds an extra layer of security. Authentication information which grants authorised access to asset(s) **must**: • not be stored in plain text or in any reversible format; • be salted with at least 128 bits of pseudorandom data; • be hashed using a method described in the DWP Approved Cryptographic Algorithms Document [Ref. B].	PR.DS-01 PR.AA-03

11.9. Cryptographic Key Management

(Important) this table contains 'must' activities.

Reference	Minimum Technical Security Measures	NIST ID
11.9.1	Cryptographic keys **must** be managed and protected in accordance with the controls present in SS-002 PKI & Key Management Security Standard [Ref. D].	PR.DS-01

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
PR.AA-03	Users, services, and hardware are authenticated	11.7.6, 11.8.1
PR.DS-01	The confidentiality, integrity, and availability of data-at-rest are protected	11.1.1, 11.1.3, 11.1.4, 11.1.6, 11.2.1, 11.2.2, 11.2.4, 11.2.5, 11.2.6, 11.2.7, 11.2.8, 11.3.1, 11.3.2, 11.4.1, 11.5.1, 11.7.1, 11.7.2, 11.7.3, 11.7.5, 11.7.6, 11.8.1, 11.9.1
PR.DS-02	The confidentiality, integrity, and availability of data-in-transit are protected	11.1.1, 11.1.3, 11.1.4, 11.1.6, 11.2.1, 11.2.2, 11.2.4, 11.2.5, 11.5.1, 11.6.1, 11.6.2, 11.6.3, 11.6.4
PR.PS-01	Configuration management practices are established and applied	11.1.4

PR.PS-02	Software is maintained, replaced, and removed commensurate with risk	11.1.2, 11.1.3, 11.1.4, 11.1.5, 11.2.3
PR.PS-03	Hardware is maintained, replaced, and removed commensurate with risk	11.1.4, 11.1.5
DE.CM-09	Computing hardware and software, runtime environments, and their data are monitored to find potentially adverse events	11.1.7

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-006 Security Boundaries security standard	Yes
B	DWP Approved Cryptographic Algorithms	No
C	SS-023 Cloud Computing Security Standard	Yes
D	SS-002 PKI and Key Management Security Standard	Yes
E	SS-033 Security Patching Standard	Yes
F	DWP Security Assurance Strategy	No

*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

Document
NIST SP 800-57 Part 1 Revision 5 – Recommendation for Key Management: Part 1 - General
NIST Special Publication 800-107 Revision 1, Recommendation for Applications Using Approved Hash Algorithms
Transitioning the Use of Cryptographic Algorithms and Key Lengths (nist.gov)
NIST SP 800-132, Recommendation for Password-Based Key Derivation Part 1: Storage Applications
What Is Post-Quantum Cryptography? | NIST
NCSC: Post-Quantum Cryptography – what comes next ?

Appendix D Abbreviations

Table 5 – Abbreviations

Abbreviation	Definition	Owner
CPA	Commercial Product Assurance	NCSC
CTR	Counter	Industry
DDA	DWP Design Authority	DWP
DH	Diffie Hellman	Public
FDE	Full Disk Encryption	Industry
FIPS	Federal Information Processing Standard	NIST
HMAC	Keyed-hash Message Authentication Code	Industry
ISO	International Organisation for Standardization	ISO
KDF	Key Derivation Functions	Industry
MAC	Message Authentication Code	Industry
NCSC	National Cyber Security Centre	NCSC
NIST	National Institute of Standards and Technology	NIST
NIST CSF	NIST Cyber Security Framework	NIST

Abbreviation	Definition	Owner
PDU	Produce Delivery Units	DWP
PRF	Pseudorandom Functions	Industry
PKCS	Public Key Cryptography Standard	RSA Security
PKI	Public Key infrastructure	Industry
RBG	Random Bit Generator	Industry
RDP	Remote Desktop Protocol	Microsoft
SHA	Secure Hash Algorithm	Industry
SSD	Solid State Drives	Industry
SSH	Secure Shell	IETF
TLS	Transport Layer Security	IETF
TPM	Trusted Platform Module	Industry
USB	Universal Serial Bus	Industry
VM	Virtual Machine	Industry

Appendix E Glossary

Table 6 – Glossary

Term	Definition
Initialisation Vector (IV)	A binary vector used as the input to initialize the algorithm for the encryption of a plaintext block sequence to increase security by introducing additional cryptographic variance and to synchronize cryptographic equipment.
Public Key Infrastructure (PKI)	The architecture, organization, techniques, practices, and procedures that collectively support the implementation and operation of a certificate-based public key cryptographic system. Framework established to issue, maintain, and revoke public key certificates.
Message Authentication Code (MAC)	A cryptographic checksum on data that uses a symmetric key to detect both accidental and intentional modifications of the data.
PQC	Post-Quantum Cryptography, also known as Quantum Resistant Cryptography, refers to cryptographic algorithms that are resistance to quantum computing attacks.
Quantum Computing	Quantum computing leverages the properties of quantum physics to perform operations that are impossible or impractical for classical computers.
Trusted Platform Module (TPM)	A tamper-resistant integrated circuit built into some computer motherboards that can perform cryptographic operations (including key generation) and protect small amounts of sensitive information, such as passwords and cryptographic keys.

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