Security Standard –

Use of Cryptography

(SS-007)

Chief Security Office

Date: 07/12/2022

Department for Work & Pensions

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 terms 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. The suit of security standards and policies considered appropriate for public viewing are published here:

https://www.gov.uk/government/publications/dwp-procurement-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).

Table 1 - List of 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. Table of 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

3. Approval history

Version	Approver	Role	Date
1.0		Chief Security Officer	04/2017
2.0		Chief Security Officer	07/12/2022

This document will be reviewed for continued completeness, relevancy, and accuracy within 1 year of being granted "final" status, and at year intervals thereafter.

4. Compliance

Security assurance teams will verify compliance with this standard through various methods, including but not limited to, internal and external audits, and feed back to the appropriate Authority Risk and System Owner.

5. Exceptions Process

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 measure's details 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

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

8. Introduction

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.

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 and its suppliers. 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.

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 the Authority or our third-party providers, such as the CIS Critical Security Controls v8 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 the Authority's 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 v8 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

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 should be sent to the Authority.

11. Minimum Technical Security Measures

The following section defines the minimum-security measures that **must** be met when deploying cryptographic controls, so that the outcomes described in Appendix A can be achieved. For ease of reference, the relevant NIST sub-category ID is provided against each security measure e.g., PR.DS-5 to indicate which outcome(s) it contributes towards. Refer to Appendix A for full descriptions of security outcomes.

11.1 Software and Hardware Requirements

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. Encryption products certified via NCSC certification e.g., Commercial Product Assurance (CPA) meets the standard. [See External References].	PR.DS-5 PR.DS-1 PR.DS-2 ID.BE-4
11.1.2	Cryptographic software **must** be maintained in accordance with SS-033 Security Patching Standard [Ref. E].	PR.IP-12
11.1.3	Cryptographic hardware deployed **must** have an active validation against a recognised scheme. FIPS 140 and FIPS 197 meet this standard as do products certified by the NCSC Commercial Product Assurance (CPA) scheme. [See External References].	PR.DS-5 PR.AC-5

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.IP-1 PR.IP-3 PR.DS-1 PR.DS-2 PR.AC-5
11.1.5	Cryptographic software / hardware **must** only be used when still under active vendor support or still inside its validation period.	PR.MA-1 PR.IP-3
11.1.6	Where applicable cryptographic operations **must** be performed on hardware, this requires appropriate validations to be in place; a) For HSMs, FIPS 140 at level 3 or higher b) For TPMs, v2.0 or higher Where applicable, cryptographic operations **must** be used in software, this requires appropriate validations to be in place; a) For software packages, FIPS 140 at level 2 or higher; b) For software libraries, FIPS 140 at level 1 or higher	PR.DS-5

11.2 Cryptographic Algorithm Requirements

Reference	Minimum Technical Security Measures	NIST ID
11.2.1	Cryptographic algorithms and modes of operation **must** be selected from the Authority's 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.IP-1
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-1, PR.DS-2
11.2.3	The list of approved cryptographic algorithms **must** be reviewed at least annually.	PR.IP-1 PR.IP-3
11.2.4	Approved hashing algorithms **must** be used as the basis for: a) Creating message digests; b) Generating digital signatures; c) Message Authentication Codes (MACs / HMACs); d) Pseudorandom Functions (PRFs); e) Key Derivation Functions (KDFs).	PR.AC-1, PR.AC-6

	See the Authority's Approved Cryptographic Algorithms document [Ref. B] for approved algorithms.	
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-6
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-6
11.2.7	Use of Diffie Hellman key exchange algorithm **must** be used in conjunction with the following parameters as appropriate: 1) DH Group 19 2) DH Group 20 3) DH Group 21	PR.DS-2, PR.PT-4

11.3 Generation of Cryptographic Key Material

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. Acceptable sources are: a) External modules which have received NCSC CPA or FIPS 140 certification. b) Operating system certified sources (e.g. Microsoft CryptoAPI:NG, /dev/random).	PR.DS-5 PR.IP-1 PR.IP-3
11.3.2	Virtual Machines (VMs) and operating systems running on Solid State Drives (SSDs) will require 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-1 PR.DS-2 ID.BE-4

11.4 Compression

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.IP-1 PR.DS-6

10.5 Message Padding

Reference	Minimum Technical Security Measures	NIST ID
10.5.1	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-1, PR.DS-2, PR.IP - 1

11.6 Encryption in Transit

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.PT-4 PR.PT-1
11.6.2	Encrypted communications channels **must** be protected using protocols, protocol suites and techniques in accordance with the relevant cryptographic manual, the Authority's Approved Cryptographic Algorithms document [Ref. B] and require Authority approval of the solution.	PR.DS-2, PR.DS-5, PR.PT-4
11.6.3	Encrypted sessions **must** re-negotiate new symmetric keys after one of the following criteria is met:	PR.DS-1, PR.DS-2

	a) The data volume specified in the validation has exceeded its maximum limit b) The time limit specific in the validation has exceeded its maximum limit.	

11.7 Encryption at Rest

Reference	Minimum Technical Security Measures	NIST ID
11.7.1	All user-writeable partitions on portable devices (laptops, mobile phones, portable storage devices etc.) **must** be encrypted at the media-level (i.e. Full Disk Encryption (FDE)).	PR.DS-1
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-5 PR.DS-1 PR.AC-1
11.7.3	Information held encrypted at rest **must** also be integrity protected.	PR.DS-6 PR.DS-8
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-1 PR.DS-5

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.AC-1 PR.AC-7 PR.DS-1 PR.DS-2
11.7.6	Encryption software deployed on devices (i.e. laptops, portable storage devices) **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.AC-1 PR.AC-7 PR.DS-1 PR.DS-2

11.8 Passwords

Reference	Minimum Technical Security Measures	NIST ID
11.8.1	Authentication information which grants authorised access to asset(s) **must**: a) not be stored in plain text or in any reversible format; b) be salted with at least 128 bits of pseudorandom data; c) be hashed using a method described in the Authority's Approved Cryptographic Algorithms Document [Ref. B].	PR.DS-1 PR.AC-1 PR.AC-4

11.9 Cryptographic Key Management

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 and Key Management Security Standard [Ref. D].	PR.DS-1, PR.DS-2 ID.RA-1 ID.RA-3 ID.RA-5

12 Appendixes

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
ID.BE-4	Dependencies and critical functions for delivery of critical services are established	11.1.1 11.3.2
PR.AC-1	Identities and credentials are issued, managed, verified, revoked, and audited for authorized devices, users and processes	11.2.4 11.7.5 11.7.6
PR.AC-5	Network integrity is protected (e.g. network segregation, network segmentation	11.1.3
PR.AC-6	Identities are proofed and bound to credentials and asserted in interactions	11.2.4
PR.DS-1	Data-at-rest is protected	11.1.1, 11.2.2, 11.3.2, 11.5.1, 11.6.3, 11.7.1, 11.7.4, 11.8.1, 11.9.1
PR.DS-2	Data-in-transit is protected	11.1.1, 11.2.1, 11.2.7, 11.3.2, 11.5.1, 11.6.2, 11.6.3, 11.9.1
PR.DS-5	Protections against data leaks are implemented	11.1.1, 11.1.4, 11.1.6, 11.3.1, 11.6.2, 11.7.2
PR.DS-6	Integrity checking mechanisms are used to verify software, firmware, and information integrity	11.2.5 11.2.6 11.7.3

PR.IP-1	A baseline configuration of information technology/industrial control systems is created and maintained incorporating security principles (e.g. concept of least functionality)	11.1.4 11.2.1 11.2.3 11.3.1
PR.IP-3	Configuration change control processes are in place	11.1.4, 11.1.5, 11.2.1, 11.3.1
PR.IP-12	A vulnerability management plan is developed and implemented	11.1.2 11.4.1
PR.MA-1	Maintenance and repair of organizational assets are performed and logged, with approved and controlled tools	11.1.5
PR.PT-1	Audit/log records are determined, documented, implemented and reviewed in accordance with policy	11.6.1
PR.PT-4	Communications and control networks are protected	11.2.7, 11.6.1, 11.6.2

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 v0.9.6	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

Request to access to non-publicly available documents **should be made to the assigned Authority Contracts/Supplier Manager.*

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
Commercial Product Assurance (CPA)
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

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
GCM	Galois/Counter Mode	Industry
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
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
Initialization 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.
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 - GOV.UK (www.gov.uk)

Understanding accessibility requirements for public sector bodies - GOV.UK (www.gov.uk)