
Security Standard – Microservices (SS-028)

Chief Security Office

Date: 30/07/2026



Department
for Work &
Pensions

This Microservices 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 Department 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:

<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).

(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	denotes a recommendation: an advisory element.
may	denotes approval.
might	denotes a possibility.
can	denotes both capability and possibility.
is/are	denotes a description.

1. Contents

1. Contents	3
2. Revision History	3
3. Approval History	6
4. Compliance	6
5. Exceptions Process	7
6. Audience	7
7. Accessibility Requirements	7
8. Introduction	8
9. Purpose	9
10. Scope	9
11. Minimum Technical Security Measures	10
11.1 Microservices Attack Surface	10
11.2 Authentication Requirements	13
11.3 Deployments and Best Practice	15
11.4 Microservices Layer and UI/UX	16
11.5 Data and Messaging Privilege Restriction	16
11.6 Runtime Protection	18
11.7 Monitoring and Logging	19
12 Appendices	20
Appendix A Security Outcomes	20
Appendix B Internal References	23
Appendix C External References	24
Appendix D Abbreviations	24
Appendix E Definition of Terms	25
Appendix F Accessibility artefacts	26

2. Revision History

Version	Author	Description	Date
1.0		First published version	25/10/2017
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 11.1.1 Threat model	21/11/2023

		11.1.2 In-support software versions 11.1.4 Microservices cannot run on the host network. 11.1.7 Separation of environments 11.1.10 Application footprint 11.1.11 data in multiple security contexts 11.2.1 Service registry must have validation checks 11.2.2 OAUTH and JSON Web Tokens 11.2.3 Approved algorithms 11.2.4 Removed 11.2.5 Differing TTL values 11.2.10 OAUTH; Shared library tokens; secrets not hardcoded 11.2.11 Hash-based message authentication 11.3.2 Including code-based 11.3.3 Internal services and mutual authentication pattern 11.4.1 UI/UX allowlisted ports 11.4.2 Rate limited procedure invocation 11.5.4 No direct communication 11.6.1 All nodes	
--	--	--	--

		11.6.2 Event types; logging of sensitive data	
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 Introduction - NCSC Cloud Security Principles 11.1.2 Clarified vendor software vs. open source 11.1.5 Communications and monitoring 11.1.7 Baseline activities 11.1.8 Cost 11.1.9 Must 11.1.11 Multi Level Security controls 11.1.12 Workload integrity assurance 11.2 Ref changed to Software Development Standard 11.2.1 RBAC & ABAC and separation of duties; SSO 11.2.4 Timestamp and nonce 11.2.10 Passphrases 11.2.11 OIDC client credentials 11.3.1 Misconfiguration 11.3.2 Vulnerable software blocking 11.3.3 TLS version removed; mTLS	30/07/2026

		11.3.4 Critical system isolation 11.3.5 Artefact signing 11.5.4 Service mesh and zero trust 11.5.5 TLS connections 11.6 Runtime Protection 11.7.1 & 11.7.2 DWP SIEM	
--	--	--	--

3. Approval History

Version	Name	Role	Date
1.0		Chief Security Officer	25/10/2017
2.0		Chief Security Officer	21/11/2023
2.1		Chief Security Officer	30/07/2026

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. I].
- 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 Requirements

(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 Microservices Security Standard defines the minimum technical security measures that **must** be implemented for use within the Authority.

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 NCSC, 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 set [see External References]. NCSC Cloud Security Principles [see External References] should also be referenced for additional guidance on data-in-transit, separation, governance, operational security, secure development, supply chain, identity, external interfaces, service administration, audit, and incident response.

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 microservices are implemented consistently across the Authority and by third party providers where applicable.
- mitigate risks from common threats and vulnerabilities associated with microservices, 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

This standard applies to all microservices deployments within the Authority and supplier base (contracted third party providers), for the purposes of delivering applications and services that handle Authority data.

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.

11.1 Microservices Attack Surface

(Important) this paragraph contains must activities.

Reference	Minimum Technical Security Measures	NIST ID
11.1.1	Microservices must run inside an approved application container technology. (As defined within SS-011 Containerisation Security Standard [Ref. A]). The DWP Architecture Blueprint Technology Radars [Ref. B] describes which specific technologies are approved for use within the Authority.	PR.DS-10
11.1.2	Systems Administrators must ensure the container Runtime environment software is in vendor support; where open source software is utilised, it must be at least 'n-1'.	PR.PS-02
11.1.3	Containers must be configured according to Authority approved Security Best Practices. (see SS-011 Containerisation Security Standard [Ref. A]).	PR.DS-10 PR.PS-01
11.1.4	Microservices must not run on the host network, as they could access other services running on the same host.	PR.IR-01

11.1.5	Communication with a Microservice must be done via a gateway service to provide load balancing and a standard set of security capabilities for the Microservices to consume. As a minimum these services must provide, authentication, authorisation, logging and alerting.	PR.IR-01
11.1.6	Containers hosting Microservices must be limited to exposing a single port or the minimum number of ports required to provide the service. All other ports must be explicitly blocked.	PR.IR-01
11.1.7	A baseline of normal communication activities must be created and thresholds on alerting and logging tools must be configured to trigger when events such as traffic spikes, or unusual traffic flows are detected.	PR.IR-01 DE.CM-01
11.1.8	The operation of the Microservice, its resource consumption and performance must be monitored and spikes in consumption addressed through capacity and cost management activities.	DE.CM-09
11.1.9	Microservices must be protected by a Defence in Depth approach. This must include – Filtering of communication flows, Authentication and Authorisation of access to a Microservice, and the use of encryption technologies.	ID.AM-03 PR.DS-01 PR.AA-03 PR.IR-01
11.1.10	Microservices must have the smallest application footprint possible and designed using a single responsibility principle.	PR.PS-01

11.1.11	Each deployed microservice must implement Multi Level Security (MLS) controls to ensure it operates within a single security context and to prevent unauthorised information leakage. This includes enforcing the MLS principles of 'no read up' (a lower-security service must not access higher-security data) and 'no write down' (a higher-security service must not write data to a lower-security context). In cases where data needs to legitimately pass between different security levels, additional traversal controls such as client re-authentication or re-direction back to an authorisation server or API gateway must be utilised.	PR.AA-05 PR.PS-01 PR.IR-01
11.1.12	As Microservices scale, the threat model must be reviewed.	ID.RA-04

11.2 Authentication Requirements

Please refer to SS-003 Secure Software Development Standard [Ref. F] for more information on API Authentication requirements.

(Important) this paragraph contains must activities.

Reference	Minimum Technical Security Measures	NIST ID
11.2.1	The Authentication model for Microservices must be defined early in the software development lifecycle and must utilise Role Based Access Controls and / or Attribute Based Access Controls as appropriate to enforce separation of duties i.e. to ensure that a single individual does not hold enough privilege to complete a critical or high-risk process alone. This includes the use of single sign-on (i.e. where authorised users access multiple applications and domains using a single set of credentials) where appropriate. The gateway must authenticate to an approved and assured authentication service.	PR.AA-01 PR.AA-03 PR.AA-05
11.2.2	The latest versions of OAuth or JSON Web Token using security best practices must be used.	PR.AA-01 PR.AA-03
11.2.3	The Token based authentication mechanism must use an approved Authority algorithm to generate the security token that is in line with SS-007 Use of Cryptography Security Standard [Ref. C].	PR.AA-01 PR.AA-03 PR.DS-02
11.2.4	Authentication Tokens must have an associated timestamp and nonce (number used once, see Appendix E Definition of Terms) to prevent replay attacks.	PR.AA-01 PR.AA-03

11.2.5	Expired Tokens must not be allowed to be replayed as a legitimate authentication request. Also a suitable HTTP error code (401) should be returned to the user.	PR.AA-01 PR.AA-03
11.2.6	Expired Tokens must be regularly purged from memory.	PR.AA-01 PR.AA-03
11.2.7	It must not be possible to replay a previously delegated request.	PR.AA-04
11.2.8	Public Key Infrastructure best practices must be adhered to for certificate exchange when using OAUTH or JSON web tokens for authentication. (see SS-002 PKI & Key Management Security Standard [Ref. D]). In addition, when shared libraries are used; • Token expiry times must be as short as possible • Token secrets must not be part of the library code • Token secrets must not be hard coded	PR.AA-01 PR.AA-03 PR.DS-02
11.2.9	Authentication tokens must be cryptographically signed, or protected by a hash-based message authentication code (HMAC) scheme, see (see SS-002 PKI & Key Management Security Standard [Ref. D]).	PR.AA-01 PR.AA-03 PR.DS-02
11.2.10	Where the use of passwords or passphrases is required they must be created and managed in accordance with SS-001 pt.1 Access & Authentication Security Standard [Ref. E].	PR.AA-01 PR.AA-03
11.2.11	Where a user utilises 'in-seat' services, service to service OIDC (OpenID Connect) client credentials must not be passed between services.	PR.AA-01 PR.AA-05

11.3 Deployments and Best Practice

(Important) this paragraph contains must statements

Reference	Minimum Technical Security Measures	NIST ID
11.3.1	Policy configuration must be applied in an automated manner to enforce segmentation. Care must be taken when configuring microservices, as misconfiguration is a commonly exploited vulnerability.	PR.PS-01 PR.IR-01
11.3.2	Underlying software, certificates, services and infrastructure upon which Microservices are reliant (including those that are code-based) must be patched (or updated) in line with SS-033 Patching & Exposure Management Standard (ref. G]. Software components with known critical vulnerabilities must be identified and blocked from use through automated Software Bill of Materials (SBOM) analysis.	PR.PS-02
11.3.3	All traffic between endpoints in microservices (including internal services) that carry authentication credentials must utilise TLS / mTLS. SS-007 Use of Cryptography Security Standard [Ref. C] provides further guidance on the use of TLS, as does SP-006 Channel Encryption & Mutual Authentication Security Design Pattern [Ref. J].	PR.DS-02
11.3.4	Critical systems must be isolated, by placing in dedicated clusters or namespaces.	PR.DS-01 PR.PS-06
11.3.5	Artefact signing must be utilised to ensure artefact integrity.	PR.DS-10 PR.PS-06

11.4 Microservices Layer and UI/UX

(Important) this paragraph contains must activities.

Reference	Minimum Technical Security Measures	NIST ID
11.4.1	The security controls between the UX functions and the microservices layer must only permit connections on necessary and allowlisted TCP and UDP ports.	PR.IR-01
11.4.2	Each logic function triggering a stored procedure on the application components must limit the rate of procedure invocation based on user ID.	PR.IR-01

11.5 Data and Messaging Privilege Restriction

(Important) this paragraph contains must activities.

Reference	Minimum Technical Security Measures	NIST ID
11.5.1	Services must only be able to access messaging channels required for their function.	PR.PS-01 PR.IR-01
11.5.2	Access to any given messaging channel must be limited to functionality required (such as read only, write, etc).	PR.AA-05
11.5.3	Messaging credentials must be protected appropriately at rest and in transit.	PR.DS-01 PR.DS-02

11.5.4	Clients must communicate to the target service via a single gateway URL, rather than communicating directly to the service. Service Mesh patterns (e.g. sidecars, policy enforcement, mutual TLS between all services) or mesh-native zero trust constructs must be utilised where available. A service mesh standardises the ‘authenticate and authorise everywhere’ principle, policy-driven routing, fine-grained telemetry, and consistent mTLS that verify each request and avoid implicit trust in internal networks.	PR.DS-02
11.5.5	Keep-alive TLS connections must be in use for frequently interacting services. (See also section 11.1.5)	PR.DS-02

11.6 Runtime Protection

(Important) this paragraph contains must activities.

Reference	Minimum Technical Security Measures	NIST ID
11.6.1	Prevent unsafe or non-compliant deployments into production or other sensitive environments by enforcing policy-based admission controls.	PR.AA-05 PR.PS-01 PR.PS-05
11.6.2	Prevent unauthorised runtime modifications and interactive access by: • Disabling mechanisms that allow direct command execution within running workloads (e.g., shell access or remote exec). • Preventing runtime changes to configuration, environment variables, or file systems that are not part of the deployment artefact. • Ensuring all infrastructure and application changes are made through automated pipelines using approved and tested artefacts. • Monitoring and alerting on any attempts to bypass immutability controls.	PR.PS-01 PR.PS-05 DE.CM-09

11.7 Monitoring and Logging

(Important) this paragraph contains must activities.

Reference	Minimum Technical Security Measures	NIST ID
11.7.1	Individual Microservices and the Microservice gateway must produce appropriate logs to an Authority approved centralised Security Information and Event Management (SIEM) system in compliance with SS-012 Protective Monitoring Security Standard. [Ref. H]. Continuous security monitoring must be implemented that covers all nodes.	PR.PS-04 DE.AE-03
11.7.2	All API requests must be logged to an Authority approved centralised Security Information and Event Management (SIEM) system, in compliance with SS-012 Protective Monitoring Security Standard [Ref. H]. Input validation errors, extra parameters errors, crashes and core dumps must be logged. Care must be taken to prevent sensitive and/or personal data being logged, which can be achieved by; • Field-level redaction. • Personal data tokenisation. • Mandatory log schemas for correlation at scale (e.g., trace IDs propagated via W3C Trace Contexts) as part of observability.	PR.PS-04 DE.CM-09 DE.AE-03

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 1 – List of Security Outcomes Mapping

NIST Ref	Security Outcome (sub-category)	Related Security measure
ID.AM-03	Representations of the organisation's authorised network communication and internal and external network data flows are maintained	11.1.9
ID.RA-04	Potential impacts and likelihoods of threats exploiting vulnerabilities are identified and recorded	11.1.12
PR.AA-01	Identities and credentials for authorised users, services, and hardware are managed by the organisation	11.2.1, 11.2.2, 11.2.3, 11.2.4, 11.2.5, 11.2.6, 11.2.8, 11.2.9, 11.2.10, 11.2.11
PR.AA-03	Users, services, and hardware are authenticated	11.1.9, 11.2.1, 11.2.2, 11.2.3, 11.2.4, 11.2.5, 11.2.6, 11.2.8, 11.2.9, 11.2.10
PR.AA-04	Identity assertions are protected, conveyed, and verified	11.2.7

PR.AA-05	Access permissions, entitlements, and authorisations are defined in a policy, managed, enforced, and reviewed, and incorporate the principles of least privilege and separation of duties	11.1.11, 11.2.1, 11.2.11, 11.5.2, 11.6.1
PR.DS-01	The confidentiality, integrity, and availability of data-at-rest are protected	11.1.9, 11.3.4, 11.5.3
PR.DS-02	The confidentiality, integrity, and availability of data-in-transit are protected	11.2.3, 11.2.8, 11.2.9, 11.3.3, 11.5.3, 11.5.4, 11.5.5
PR.DS-10	The confidentiality, integrity, and availability of data-in-use are protected	11.1.1, 11.1.3, 11.3.5
PR.PS-01	Configuration management practices are established and applied	11.1.3, 11.1.10, 11.1.11, 11.3.1, 11.5.1, 11.6.1, 11.6.2
PR.PS-02	Software is maintained, replaced, and removed commensurate with risk	11.1.2, 11.3.2
PR.PS-04	Log records are generated and made available for continuous monitoring	11.7.1, 11.7.2
PR.PS-05	Installation and execution of unauthorised software are prevented	11.6.1, 11.6.2
PR.PS-06	Secure software development practices are integrated, and their performance is monitored throughout the software development life cycle	11.3.4, 11.3.5

PR.IR-01	Networks and environments are protected from unauthorised logical access and usage	11.1.4, 11.1.5, 11.1.6, 11.1.9, 11.1.7, 11.1.11, 11.3.1, 11.4.1, 11.4.2, 11.5.1
DE.CM-01	Networks and network services are monitored to find potentially adverse events	11.1.7
DE.CM-09	Computing hardware and software, runtime environments, and their data are monitored to find potentially adverse events	11.1.8, 11.6.2, 11.7.2
DE.AE-03	Information is correlated from multiple sources	11.7.1, 11.7.2

Appendix B Internal References

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

Table 2 – Internal References

Ref	Document	Publicly Available*
A	SS-011 Containerisation Security Standard	Yes
B	DWP Architecture Blueprint (Technology Radars)	No
C	SS-007 Use of Cryptography Security Standard	Yes
D	SS-002 PKI & Key Management Security Standard	Yes
E	SS-001 pt.1 Access & Authentication Security Standard	Yes
F	SS-003 Software Development Security Standard	Yes
G	SS-033 Patching & Exposure Management Standard	Yes
H	SS-012 Protective Monitoring Security Standard	Yes
I	Security Assurance Strategy	No
J	SP-006 Channel Encryption & Mutual Authentication Security Design Pattern.	No

Requests to access 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 3 – External References

External Documents List
CIS Critical Security Controls v8 controls set
NIST SP 800-204: Security Strategies for Microservices-based Application Systems
OWASP Top 10 Web Application Security Risks
NCSC Cloud Security Principles

Appendix D Abbreviations

Table 4 – Abbreviations

Abbreviation	Definition
CA	Certificate Authority
DDA	Digital Design Authority
DWP	Department for Work and Pensions (DWP)
Port	TCP/IP port number
Runtime	Software providing the execution environment for applications within an Application Container.

Appendix E Definition of Terms

Table 5 – Glossary

Term	Definition
Cryptographic Items	All logical and physical items used to achieve confidentiality, integrity, non-repudiation and accountability; including, but not limited to: devices, products, systems, key variables and code systems.
Cryptographic Key Material	Any parameter passed to an encryption cipher which influences the output of the algorithm (with the exception of the message itself).
Decoupling	It's an approach in IT development and operations where two or more systems work or are connected without being directly connected. In theory, this means that a change can be made to one service without the developer having to worry about how the change will impact other services.
Nonce	A nonce (a "number used once") is a unique, random string or number generated for a single, specific message. The receiver records the nonces it has already processed; if a message arrives with a previously used nonce, the server rejects it as a duplicate.
Service registry	The service registry service is used by microservices that are coming online to publish their locations in a process called service registration and is also used by microservices seeking to discover registered services.

Appendix F Accessibility artefacts

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

DWP Digital Accessibility Policy | DWP Intranet

<https://accessibility-manual.dwp.gov.uk/>

<https://www.gov.uk/guidance/guidance-and-tools-for-digital-accessibility>

<https://www.gov.uk/guidance/accessibility-requirements-for-public-sector-websites-and-apps>