Security Standard - Microservices Architecture (SS-028)

Chief Security Office

Date: 25/10/17

Department for Work & Pensions

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

Version Control Table

Version	Date	Major Change

Updating policy

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

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

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

Contents

1. Introduction

1.1. This document describes the best practices and security control requirements for the deployment of Microservices within the DWP estate. As this area of technology, matures so shall the control points in this standard to reflect this developing technology space.

1.2. For further clarity and relevance, this standard is aligned to the DWP Digital Blueprint, which defines the direction for all Departmental technology.

2. Purpose

2.1. The purpose of this standard is to list the security requirements in relation to how to deploy, implement and control the usage of Microservices within the DWP.

2.2. Secondly, this standard provides a reference to conduct compliance based technical security audits against.

2.3. Projects should use this documentation to ensure that the security best practises for their system are being adequately and accurately addressed.

3. Exceptions

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

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

3.3. Exceptions to this standard MUST be maintained on a risk register for accountability, traceability and security governance reporting to senior management.

4. Audience

4.1. This standard is intended for Suppliers, system administrators, security groups, and IT staff involved in securing environments for DWP systems and applications and provided the security requirements on how to manage, implement and configure Microservices Architecture.

5. Scope

5.1. This standard is applicable to systems handling data within the OFFICIAL tier of the Government Security Classification Policy (GSCP). This includes OFFICIAL information that attracts the SENSITIVE handling caveat. All implementations of Microservices MUST meet all the requirements in this standard or gain authorization with DWP security architectural risk review (see exceptions process).

5.2. The security control requirements laid out in this standard are product agnostic and applicable for all implementations of Microservice architecture that are provisioned for departmental use.

5.3. In the In the event of uncertainty on the controls laid out in this standard please contact the Security front door for guidance and support on items which require clarification.

6. Security Controls Assurance

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

7. Technical Security Control Requirements

In this document the term MUST in upper case is used to indicate an absolute requirement. Failure to meet these requirements will require a formal exemption (see section [3. Exceptions] above).

7.1 Microservices Architecture Attack Surface

Reference	Security Control requirement
10.1.1	Microservices MUST run inside an approved application container technology. (As defined within the Containerisation security standard SS-011). The DWP Blueprint documentation describes which specific technology is approved for use within the department. As Microservices scale, the attack surface of the application inevitably increases. A method of reducing the overall attack surface is to use approved containers which expose the minimum attack surface
10.1.2	Systems Administrators MUST ensure the container Runtime environment is maintained in accordance with the current policy on S/W versions.
10.1.3	Containers MUST be configured according to DWP approved Security Best Practices. (see Containerisation Security Standard SS-011).
10.1.4	IP Filtering technologies MUST be applied to the Microservices host environment as a minimum to control connectivity to the Microservices executing on the host.
10.1.5	Communication with a Microservice MUST be done via 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.
10.1.6	Containers hosting Microservices MUST be limited to exposing a single port or the minimal number of ports required to provide the service. All other ports MUST be explicitly blocked.
10.1.7	A tool to monitor and visualise inter-service communication MUST be deployed as part of the management capabilities of the Microservices architecture.
10.1.8	A baseline of normal communication activities MUST be created and thresholds on monitoring and logging tools MUST be configured to trigger when events such as traffic spikes, or unusual traffic flows are detected.
10.1.9	Production, development and QA environments MUST be isolated, running on logically separate networks.
10.1.10	A catalogue of API's and their characteristics MUST be published so that developers of consuming software are clear on the function, URI, and other specific requirements for using the service.
10.1.11	The operation of the Microservice, its resource consumption and performance MUST be monitored and spikes in consumption addressed through capacity management activities.
10.1.12	Microservices MUST be protected by a Defence in Depth approach. This will include – Filtering of communication flows, Authentication and Authorisation of access to a Microservice and the use of encryption technologies.

Reference	Security Control requirement
10.1.13	Except during traffic inspection, the Microservices API gateway, must not retain OFFICIAL/OFFICIAL SENSITIVE information in memory.

7.2 Authentication Requirements

Reference	Security Control requirement
10.2.1	The Authentication model for Microservices MUST be defined early in the software development lifecycle. This includes the use of federated identity where appropriate. The gateway must authenticate to an approved and assured authentication service.
10.2.2	A well-known and secure open standard protocol for centralised authentication using tokens MUST be leveraged.
10.2.3	The Token based authentication mechanism MUST use an algorithm to generate the security token that follows the guidance in the Use of Cryptography Standard (SS07)
10.2.4	Multiple active authentications per user or process MUST be allowed, with a strict upper bound set to mitigate any potential Denial of Service attacks.
10.2.5	Authentication Tokens MUST have an associated TTL to prevent replay attacks.
10.2.6	TTL's for Authentication Tokens MUST be updated with a new expiration time each time a token is re-validated
10.2.7	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.
10.2.8	Expired Tokens MUST be regularly purged from memory.
10.2.9	It MUST NOT be possible to (maliciously) replay a previously delegated request.
10.2.10	Public Key Infrastructure best practices MUST be adhered to for certificate exchange when using JSON web tokens for authentication. (see DWP PKI standard)
10.2.11	Authentication Tokens MUST be encrypted. This is to mitigate the exposure time should a token become compromised.
10.2.12	Every API endpoint MUST authenticate to the gateway.
10.2.13	The gateway Must implement a mechanism to restrict the number and alert on repeated authentication failures.
10.2.14	Where the use of a password is required and has been agreed, through the exceptions process, then the passwords must be created and managed in accordance with the Authentication and Authorisation Access Control standard.

7.3 API keys and Signed Requests

Reference	Security Control requirement
10.3.1	Services MUST have integrity mechanisms in place to handle data that has been transmitted to them to ensure that it has not been altered in transmission.
10.3.2	The function call hierarchy MUST be configured in such a way that a threat actor is not able to intercept API calls across the network and leverage the data in such a way to launch a replay attack against the service.
10.3.3	Each service MUST have a totally unique API key for calling another service. This key MUST comprise of a unique Service ID and a User ID at minimum.
10.3.4	Communication of API keys MUST utilise encryption in transit (TLS)
10.3.5	All API requests MUST be cryptographically signed. Signatures MUST include request parameter data, service ID, API key, and originating time stamp as a minimum.
10.3.6	Functions MUST be created using an approved SDK.
10.3.7	Development of Microservices MUST follow the guidance published in the Software Development standard (SS003)

7.4 Deployments and Best Practices

Reference	Security Control requirement
10.4.1	Policy configuration MUST be applied in an automated manner to enforce segmentation as part of the Orchestration processes.
10.4.2	Underlying software, certificates, services and infrastructure upon which Microservices are reliant MUST be patched in line with DWP patching policy
10.4.3	Deployment and updates MUST be automated using an Orchestration service.
10.4.4	All traffic between endpoints in the microservices architecture including that carrying authentication credentials MUST utilise TLS. The Use Of Cryptography (SS-07) security standard will give further guidance on the use of TLS.

7.5 Data and Messaging Privilege Restriction

Reference	Security Control requirement
10.5.1	API calls made by users and systems MUST be limited to only those necessary for those users or systems to perform their functions
10.5.2	Data available to services MUST be limited to the minimum required for them to function
10.5.3	Database credentials MUST provide access to only the minimum amount of data possible to discharge the function for which those credentials are issued

Reference	Security Control requirement
10.5.4	Database credentials MUST provide access only to functionality and operations required to discharge the function for which those credentials are issued
10.5.5	Services MUST only be able to access messaging channels required for their function.
10.5.6	Access to any given messaging channel MUST be limited to functionality required (such as read only, write, etc)
10.5.7	Messaging credentials MUST be protected appropriately at rest and in Transit.

7.6. Monitoring and Logging

Reference	Security Control requirement
10.6.1	Individual Microservices and the Microservice gateway MUST produce appropriate logs in compliance with the protective monitoring standard
10.6.2	All API requests MUST be logged to a centralised logging and monitoring system, in compliance with the protective monitoring standard.
10.6.3	Microservices MUST log performance and throughput metrics A baseline set of normal metrics MUST be established.
10.6.4	Thresholds MUST be configured on logging and monitoring system(s) such that abnormal metrics trigger alerts for investigation

8. Compliance

Compliance with this standard MUST occur as follows:

Compliance	Due Date
On-going	From the first day of approval
Retrospective	Within 6 months of the approval of the standard.

9. Accessibility

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

10. Security Standards Reference List

Document Name	Location	Version

11. Reference Documents

12. Definition of Terms

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).

13. Glossary

Abbreviation	Definition
AES	Advanced Encryption Standard – defined in FIPS 197. Different modes of operation are covered in different documents.
CA	Certificate Authority
DA	Design Authority (DA)
DWP	Department of Work and Pensions (DWP)
Port	TCP/IP port number
Runtime	Software providing the execution environment for applications within an Application Container.

14. Controls Catalogue Mapping

The table below shows how the controls in this standard map to the DWP Controls Catalogue and thereon to control points in international security standards including but not limited to ISO/IEC 27002:2013, NIST 800-53, and the OWASP ASVS.

SS28 Micro Services Architecture Security standard	**DWP Controls Catalogue - Baseline Control Set**	
10.1.1	DWP_NT05 Isolation of Information System Components	Organizations can isolate information system components performing different missions and/or business functions. Such isolation limits unauthorized information flows among system components and also provides the opportunity to deploy greater levels of protection for selected components. Separating system components with boundary protection mechanisms provides the capability for increased protection of individual components and to more effectively control information flows between those components. This type of enhanced protection limits the potential harm from cyberattacks and errors. The degree of separation provided varies depending upon the mechanisms chosen. Boundary protection mechanisms include, for example, routers, gateways, and firewalls separating system components into

SS28 Micro Services Architecture Security standard	**DWP Controls Catalogue - Baseline Control Set**	
		physically separate networks or subnetworks, cross-domain devices separating subnetworks, virtualization techniques, and encrypting information flows among system components using distinct encryption keys
10.1.12	DWP_AP07 Threat and Vulnerability Management Vulnerability / Patch Management	Policies and procedures shall be established, and supporting processes and technical measures implemented, for timely detection of vulnerabilities within organizationally-owned or managed applications, infrastructure network and system components (e.g., network vulnerability assessment, penetration testing) to ensure the efficiency of implemented security controls. A risk-based model for prioritizing remediation of identified vulnerabilities shall be used. Changes shall be managed through a change management process for all vendor-supplied patches, configuration changes, or changes to the organization's internally developed software. Upon request, the provider informs customer (tenant) of policies and procedures and identified weaknesses especially if customer (tenant) data is used as part the service and/or customer (tenant) has some shared responsibility over implementation of control.
10.1.13	DWP_GV01 Governance and Risk Management Baseline Requirements	Baseline security requirements shall be established for developed or acquired, organizationally-owned or managed, physical or virtual, applications and infrastructure system and network components that comply with applicable legal, statutory, and regulatory compliance obligations. Deviations from standard baseline configurations must be authorized following change management policies and procedures prior to deployment, provisioning, or use. Compliance with security baseline requirements must be reassessed at least annually unless an alternate frequency has been established and authorized based on business need.
10.1.4	DWP_NT05	See 10.1.1
10.1.5	DWP_NT05	See 10.1.1
10.1.6	DWP_NT03 Network Controls	Networks shall be managed and controlled to protect information in systems and applications

SS28 Micro Services Architecture Security standard	**DWP Controls Catalogue - Baseline Control Set**	
10.1.7	DWP_NT02 Infrastructure & Virtualization Security Network Security	Network environments and virtual instances shall be designed and configured to restrict and monitor traffic between trusted and untrusted connections. These configurations shall be reviewed at least annually, and supported by a documented justification for use for all allowed services, protocols, and ports, and by compensating controls.
10.1.8	DWP_NT02 DWP_OP06 Capacity management	See 10.1.7 The use of resources shall be monitored, tuned and projections made of future capacity requirements to ensure the required system performance
10.1.9	DWP_NT01 Separation of development, test and operational environments	Development, testing and operational environments shall be separated to reduce the risks of unauthorised access or changes to the operational environment.
10.1.10	DWP_SD06 Secure development policy DWP_SD15 Interoperability & Portability Policy & Legal	Rules for the development of software and systems shall be established and applied to developments within the organisation. Policies, procedures, and mutually-agreed upon provisions and/or terms shall be established to satisfy customer (tenant) requirements for service-to-service application (API) and information processing interoperability, and portability for application development and information exchange, usage, and integrity persistence.
10.1.11	DWP_OP06	See 10.1.8
10.1.12	DWP_NT05	See 10.1.1
10.1.13		
10.2.1	DWP_SD01 Information security requirements analysis and specification	The information security related requirements shall be included in the requirements for new information systems or enhancements to existing information systems.
10.2.2	DWP_CL02 Application & Interface Security Application Security	Applications and programming interfaces (APIs) shall be designed, developed, deployed, and tested in accordance with leading industry standards (e.g., OWASP for web applications) and adhere to applicable legal, statutory, or regulatory compliance obligations

SS28 Micro Services Architecture Security standard	**DWP Controls Catalogue - Baseline Control Set**	
	DWP_GV01 Governance and Risk Management Baseline Requirements	Baseline security requirements shall be established for developed or acquired, organizationally-owned or managed, physical or virtual, applications and infrastructure system and network components that comply with applicable legal, statutory, and regulatory compliance obligations. Deviations from standard baseline configurations must be authorized following change management policies and procedures prior to deployment, provisioning, or use. Compliance with security baseline requirements must be reassessed at least annually unless an alternate frequency has been established and authorized based on business need.
10.2.3	DWP_GV01	See 10.2.2
10.2.4	DWP_SD01 Information security requirements analysis and specification	The information security related requirements shall be included in the requirements for new information systems or enhancements to existing information systems.
10.2.5	DWP_SD01	See 10.2.4
10.2.6	DWP_SD01	See 10.2.4
10.2.7	DWP_SD01	See 10.2.4
10.2.8	DWP_SD01	See 10.2.4
10.2.9	DWP_SD01	See 10.2.4
10.2.10	DWP_SD01	See 10.2.4
10.2.11	DWP_CY06 Encryption & Key Management Sensitive Data Protection	Policies and procedures shall be established, and supporting business processes and technical measures implemented, for the use of encryption protocols for protection of sensitive data in storage (e.g., file servers, databases, and end-user workstations), data in use (memory), and data in transmission (e.g., system interfaces, over public networks, and electronic messaging) as per applicable legal, statutory, and regulatory compliance obligations.
10.2.12	DWP_SD01	See 10.2.4
10.2.13	DWP_SD01	See 10.2.4
10.2.14	DWP_AC11 Management of secret authentication information for users	The allocation of secret authentication information shall be controlled through a formal management process.

SS28 Micro Services Architecture Security standard	**DWP Controls Catalogue - Baseline Control Set**	
10.3.1	DWP_CL06 Application & Interface Security Data Integrity	Data input and output integrity routines (i.e., reconciliation and edit checks) shall be implemented for application interfaces and databases to prevent manual or systematic processing errors, corruption of data, or misuse.
10.3.2	DWP_SD05 Protecting application services transactions	Information involved in application service transactions shall be protected to prevent incomplete transmission, mis-routing, unauthorised message alteration, unauthorised disclosure, unauthorised message duplication or replay.
10.3.3		
10.3.4	DWP_CY06	See 10.2.11
10.3.5	DWP_CY06	See 10.2.11
10.3.6	DWP_GV01	See 10.2.2
10.3.7	DWP_GV01	See 10.2.2
10.4.1	DWP_NT08 Segregation in networks	Groups of information services, users and information systems shall be segregated on networks.
10.4.2	DWP_AP07	See 10.1.2
10.4.3		
10.4.4	DWP_CY06	See 10.2.11
10.5.1	DWP_AC02 Access to networks and network services	Users should only be provided with access to the network and network services that they have specifically been authorised to use.
10.5.2	DWP_AC02	See 10.5.1
10.5.3	DWP_AC02	See 10.5.1
10.5.4	DWP_AC02	See 10.5.1
10.5.5	DWP_AC02	See 10.5.1
10.5.6	DWP_AC02	See 10.5.1
10.5.7	DWP_CY06	See 10.2.11
10.6.1	DWP_EV01 Event logging	Event logs recording user activities, exceptions, faults and information security events shall be produced, kept and regularly reviewed.
10.6.2	DWP_EV01 DWP_EV04 Protection of log information	See 10.6.1 Logging facilities and log information shall be protected against tampering and unauthorised access.
10.6.3	DWP_EV01	See 10.6.1
10.6.4	DWP_EV01	See 10.6.1