DWP Cryptographic Key Management Policy

Contents

1. Background and Purpose

The DWP Cryptographic Key Management Policy and supporting standards are government and industry best practice to meet requirements for the secure delivery of online public services (i.e. to support the Digital Agenda). The overall objective is to protect the confidentiality of sensitive information, preserve the integrity of critical information and confirm the identity of the originator of transactions or communications.

1.1. The purpose of this policy is to provide the top-level framework of governance and direction to ensure secure cryptography management, i.e. the provision or issue, storage, use and recovery or revocation and decommissioning, of cryptographic products and key material (Keymat) for the Department.

1.2. The policy also aims to provide a level of assurance to the Department in the deployment of online digital services and to enable the Department to form effective trust relationships with other UK Government departments and partner agencies.

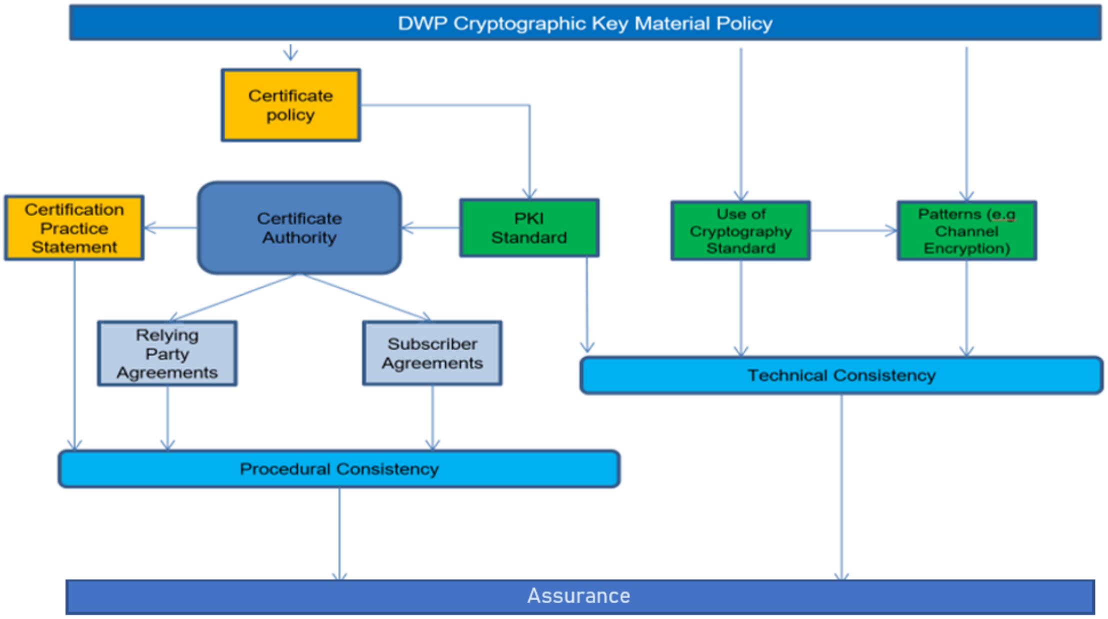

Figure 1 – Cryptography governance framework and established assurance

2. Scope

This policy does not replace any legal or regulatory requirements.

2.1 This policy applies to:

a) DWP Certificate Authorities and Service Providers acting as DWP Certificate Authorities, who must embed the policy requirements into all technical, procedural and administrative processes.

b) DWP staff engaged in designing and implementing new technology solutions, who must reflect the policy requirements into design and build.

c) DWP suppliers that handle/access/process digital certificates and other key material. Suppliers must provide the security measures and safeguards appropriate to the nature and use of the DWP information, where applicable.

d) All DWP personnel who are involved in advising on, authorising or using cryptographic key material, for use in protecting information at the OFFICIAL classification or above, including those with responsibility for the application of cryptographic methods or for the storage, management and distribution of cryptographic items.

2.2 This policy applies equally to the management of all cryptographic devices and materials including commercial encryption products procured from Non-HMG third party suppliers. For consistency the policy sets out requirements in accordance with the widely employed international industry standard set by the Internet Engineering Task Force (IETF) but it also makes reference to Her Majesty's Government (HMG) policy contained in Information Assurance Standard (IAS) No 4, which can be obtained from the Authority.

2.3 For directions on the use of asymmetric cryptographic solutions, (e.g. Public Key Infrastructure (PKI)), all parties must consult the DWP Security Standard – Public Key Infrastructure & Key Management (SS-002) to obtain further instruction on how certificates must be created and handled, and additionally refer to DWP Security Standard – Use of Cryptography (SS-007).

2.4 For symmetric cryptographic assets (e.g. HMG key material, Advanced Encryption Standard (AES) or similar), all parties must consult DWP Security Standard – Use of Cryptography (SS-007), the relevant sections of SS-002 pertaining to key management, and where appropriate Her Majesty's Government (HMG) policy contained in Information Assurance Standard (IAS) No 4.

2.5 For directions on the implementation of the requirements that a DWP Certificate Authority must adhere to, parties must consult the DWP X.509 Certificate Policy. Suppliers can obtain this from the Authority and for others, the certificate policy requirements contained therein are consistent with the Internet Engineering Task Force (IETF) Request for Comments (RFC) 3647 – Public Key Infrastructure X.509 (PKIX) Certificate Policy and Certification Practices Framework .

3. Accountabilities

3.1 The DWP Chief Security Officer is the accountable owner of the DWP Cryptographic Key Management Policy, which incorporates symmetric and asymmetric (public / private key) cryptography requirements, and is responsible for its maintenance and review as delegated through the DWP Deputy Director for Security Policy and Compliance.

3.2. Digital Product Owners/Digital Product Development and Cryptographic Leads will be accountable and responsible for managing services within this governance framework of security policies and standards. This framework will provide the necessary assurance that all key material used within or on behalf of the Department is sufficiently secure according to known risk, industry best practice and HMG policy.

4. Policy Statements

4.1. Cryptography MUST be used in accordance with the DWP Security Classification Policy and the DWP Information Security Policy, and comply as appropriate with DWP X.509 Certificate Policy, (consistent with the Internet Engineering Task Force (IETF) Request for Comments (RFC) 3647 – Public Key Infrastructure X.509 (PKIX) Certificate Policy and Certification Practices Framework) and DWP Security Standard – Public Key Infrastructure & Key Management (SS-002), and DWP Security Standard – Use of Cryptography (SS-007). The DWP mandates the use of cryptography in order to:

a) protect the confidentiality of sensitive information or information that is subject to legal and regulatory-related encryption requirements (e.g. PCI DSS, and the EU General Data Protection Regulation 2016/679 (GDPR));

b) determine if critical information has been altered (e.g. by performing hash functions or digitally signing);

c) provide strong authentication for users of applications and information systems (e.g. by using digital certificates and smartcards);

d) enable the identity of the originator of critical transactions or communications to be proven (e.g. by using digital signatures for non-repudiation).

4.2. The selection and implementation of a cryptographic solution MUST take into account the legal aspects of using encryption, and include:

a) identifying legal obligations (for relevant jurisdictions);

b) assessing the risks (including legal risks) associated with using cryptographic solutions (including encryption algorithms);

c) selecting a suitable cryptographic solution (e.g. that meets legal, regulatory and industry standards).

4.3. Accountable and responsible parties in Digital are required to have in place resources and processes to manage cryptographic solutions that include:

a) approving the use of cryptographic solutions (e.g. by executive management);

b) assigning responsibilities for cryptographic solutions;

c) handling conflicting laws and regulations (e.g. dealing with licence issues) relating to the use of cryptographic solutions in different jurisdictions (e.g. by obtaining advice from the legal function);

d) keeping cryptographic solutions up to date.

4.4. Relevant business managers and IT specialists MUST have access to:

a) expert technical and legal advice on the use of cryptography;

b) a list of approved cryptographic solutions;

c) an up-to-date register of cryptographic solutions.

4.5. All DWP Crypto Authorised personnel, (those in posts established in compliance with HMG IAS No 4), MUST be provided with training appropriate to their role, defined by HMG IAS No 4 and provided by National Cyber Security Centre (NCSC), and they must complete the required authorisation certificate before undertaking their role.

This training should encompass and engender a detailed understanding of the requirements set out in HMG IAS No 4 and its supplements.

4.6. Specific Crypto Training and appropriate certification records MUST be maintained for all such personnel and must be made available for, and be subject to, regular audit.

4.7. Any Crypto Authorised person on the DWP account who contravenes or attempts to contravene this policy or any of its associated standards or procedures may be subject to removal from the DWP account and/or other appropriate disciplinary procedures may apply.

4.8. Where National Cyber Security Centre Commercial Product Assurance (CPA) certificated products are utilised, cryptographic material, including keys MUST only be obtained from defined and Departmentally approved bodies, such as the UK Key Production Authority, through or with the documented approval of the DWP Crypto Custodian or Cluster Custodian team, where appropriate via the Authority.

4.9. Where National Cyber Security Centre Commercial Product Assurance (CPA) certificated products are utilised, implementation procedures MUST be documented and followed in compliance with the requirements of the HMG IAS No 4 and, where appropriate, a Key Management Plan must be created and maintained as defined by HMG IAS No 4.

4.10. A register of approved cryptographic solutions MUST be maintained, which:

a) specifies the intended use of encryption within the organisation;

b) details the locations where cryptographic solutions are applied;

c) contains information relating to the licensing requirements for using cryptographic solutions;

d) is made available to relevant business managers, IT and data specialists and authorised external parties (e.g. regulatory authorities and law enforcement).

4.11. For public / private cryptography such as SSL and TLS, a robust, well-managed and governed Public Key and Trust Infrastructure (PKI) MUST be deployed.

The PKI MUST be supported by:

a) a Certificate Policy (CP) - the DWP X.509 Certificate Policy (consistent with the Internet Engineering Task Force (IETF) Request for Comments (RFC) 3647 – Public Key Infrastructure X.509 (PKIX) Certificate Policy and Certification Practices Framework) states the rules for how a certificate is to be issued, used and when it may be relied upon.

All DWP certificate deployment (or certificate deployment on behalf of the DWP) MUST comply with the DWP X.509 Certificate Policy.

b) Certification Practice Statements (CPS) covering each type of digital certificate issued by a Certification Authority (CA). The CPS is a summary of the detailed processes and procedures which a Certification Authority (CA) employs, stating how the rules specified in the DWP X.509 Certificate Policy and the subsequent technical, procedural and administrative controls are implemented.

4.12. Any DWP Certificate Authority or Service Provider acting as a DWP Certificate Authority MUST develop a Certification Practice Statement (CPS) as a requirement of the DWP X.509 Certificate Policy (consistent with the Internet Engineering Task Force (IETF) Request for Comments (RFC) 3647 – Public Key Infrastructure X.509 (PKIX) Certificate Policy and Certification Practices Framework).

4.13. Any DWP PKI certificate deployment (or certificate deployment on behalf of the DWP) MUST comply with the DWP X.509 Certificate Policy (consistent with the Internet Engineering Task Force (IETF) Request for Comments (RFC) 3647 – Public Key Infrastructure X.509 (PKIX) Certificate Policy and Certification Practices Framework) and / or the DWP Security Standard – Public Key Infrastructure & Key Management (SS-002) as applicable.

4.14. A DWP certificate deployment in compliance with the DWP X.509 Certificate Policy MUST provide security management services including:

- Key / certificate generation, storage, and inventory maintenance;
- Certificate modification and distribution;
- Certificate Revocation List (CRL) generation and distribution;
- Directory management of certificate related items; and
- System management functions such as configuration management and archival.

5. Policy Compliance

5.1. Where the use of cryptography or cryptographic key management is not in compliance with this policy, an exception to the policy must be sought from the DWP risk management function – Enterprise Security Risk Management (ESRM), where appropriate via the Authority.

5.2. If, following a risk assessment, the potential consequence of non-adherence to this policy is estimated to exceed the DWP's risk tolerance, a report must be made (where appropriate via the Authority) to ESRM and the appropriate Security Risk governance bodies, which will agree and oversee with the Accountable Owner(s) and where applicable a supplier, a plan to manage and / or mitigate the system / service risks.

5.3. Compliance to this policy will be declared through annual attestation to the policy by Accountable Owner(s). Accountable parties must be prepared and able to evidence compliance to this policy. Policy Compliance and System RAG reporting will be required by Digital Product Owners/Digital Product Development and Cryptographic Leads in order to meet their part of compliance. Digital Product Owners/Digital Product Development and Cryptographic Leads are also responsible for ensuring an annual review (ITHC) or similar compliance audit, so that they are satisfied that the requirements of the policy are being fulfilled.