Defence PKI Disclosure Statement

Version 1.1 (Issue) - Oct 2011

The Defence Public Key Infrastructure (DPKI) is governed by the DPKI Policy Management Authority (DPMA) under the authority of the United Kingdom of Great Britain and Northern Ireland Ministry of Defence (MoD).

The Defence PKI Disclosure Statement (PDS) document is a supplement to the Defence PKI (DPKI) Certificate Policy (DCP) Version 3 and does not substitute or replace it. Its purpose is to summarise some of the key aspects of the DCP for the benefit of subscribers and relying parties.

For comprehensive information about the items disclosed in this document, please refer to the DCP available at http://www.mod.uk/pki. The DCP must be read before potential subscribers apply for, or rely on a certificate issued by the MOD.

1) Contact Information

All queries relating to this document or the DPKI should be directed to:

DPKI Policy Management Authority
Chief Information Officer (02.N.29)
Ministry of Defence
Main Building
London
SW1A 2HB

Email: dpki-dpma@mod.uk

2) Certificate Type, Validation Procedures and Usages

The DPKI provides the capability for the creation and management of X.509 Version 3 public key certificates (referred to as just Certificates in this document) for use in applications requiring communication between networked (and possibly stand-alone) computer-based systems operating at SECRET and below for the Defence environment.

Such uses may include, but are not limited to, the following:

i. Authentication of users to applications and infrastructure

ii. Message signing and/or encryption

iii. Signing and/or encryption of electronic forms/files/contracts

iv. Authentication of infrastructure devices and services such as Routers, Web Servers, Firewalls, VPNs and Directories

v. Support for auditing and accountability

Ultimately, the DPKI support the primary security services: access control, confidentiality, integrity, authentication and non-repudiation.

To check the validity of DPKI certificates, the DPKI offers the On-line Certificate Status Protocol (OCSP) as defined in RFC 2560 to provide on-line access to the current revocation status of all certificates. This is the primary means of checking the revocation status of a certificate for End Entities and Relying Parties, the use of Certificate Revocation Lists (CRL) are acceptable but unfavoured. All Relying Parties are expected to use systems and software compatible with OCSP to ensure access to up-to-date status information.

3) Reliance Limits

The DPKI has not set any reliance limits for certificates issued under the DCP. However, other authorities may set reliance limits for specific application usage. See Limitation of Liability below.

4) Obligations of Subscribers

The DPKI supports multiple Registration Authorities (RA) that cater for distinct elements of Defence. In terms of DPKI human subscribers, individuals will maintain a ‘person’ identity where their name is used and a ‘role’ identity where their job role\title is used. However, the following high level obligations are pertinent for all subscribers who shall:

- Make only true and accurate representation to the Registration Authority as to the information required to determine eligibility for a certificate and for information contained within the certificate.
- Confirm the accuracy of the information contained within the certificate before using it.
- Only use their certificate and associated keys for legitimate MoD business transactions.
- Take reasonable measures to protect their private keys, hardware tokens or activation PIN against loss, disclosure, modification or unauthorised use.
- Immediately notify the issuing RA in accordance with policy covered in the DCP and supplemented by local operating procedures of a suspected or known compromise of the private key or its associated activation PIN.
- Keep private keys confidential.
- Keep confidential, any passwords, pass-phrases, PINs or other personal secrets used in obtaining authenticated access to PKI facilities.

5) Certificate Status checking obligations of Relying Parties

It is the responsibility of the Relying Party to verify the status of any DPKI issued certificate using the DPKI Validation Authority (VA) Service. If it is not possible to determine the current revocation status of a certificate, because the VA service is unavailable or the current CRL is not accessible, then the Relying Party may choose to accept the certificate if it is in all other respects valid. However, the MOD accepts no liability if such an action is taken.

6) Limited Warranty & Disclaimer / Limitation of Liability

This subject has not been summarised for the PDS because the DPMA consider that the "Limited Warrant & Disclaimer" and "Limitation of Liability" information should be read and understood in its entirety.

Section 9 of the DCP refers, specifically paragraphs 9.7 and 9.8

7) Applicable Agreements, Certification Practice Statement, Certificate Policy

The Subscriber Agreement
The Subscriber Agreement is now complete and has been approved.

Certification Practice Statement
CPS's for DPKI CA servers are Protectively Marked (PM) and are therefore not published.

Certificate Policy
http://www.mod.uk/pki

8) Privacy Policy

The DPKI Authorities and repositories within the DPKI shall implement and maintain a privacy policy, in accordance with the Data Protection Act 1998, the Human Rights Act 1998 and the Freedom of Information Act 2000.

9) Refund Policy

Not Applicable.

10) Applicable Law and Dispute Resolution

The construction, interpretation and validity of the DCP shall be governed by English Law.

Any dispute arising out of or relating to the DPKI Certificate Policies as described in the DCP shall be resolved using the appropriate dispute resolution procedure in accordance with the DCP under section 9.

11) CA and Repository Licences, Trust Marks and Audit.

The DPKI Authorities have achieved tScheme Grant of Approval.