

JSP 602 Instruction	1004	Applicability	Applicability Applications, Infrastructure, Integration, Security
Configuration Identity	Version: 01.02 Amended: 2009-03-02 Reviewed: 2006-06-21	Epoch Applicability	2005 - 2009

JSP 602: 1004 - Certificate Services

Outline

Description: Certificate Services describe the methods and services that support the management of public and private keys and public key certificates for use in PKI based schemes.

Reasons for Implementation: Certificate services are used to protect the confidentiality and integrity of information. They can also be used to support authentication and identity management across Defence.

Issues: Current UK Defence PKI Policy does not cover the use of PKI above the level of Restricted. This will be ratified in the near future and will be detailed within a future version of JSP457 Volume 5: Public Key Infrastructure.

Guidance: All PKIs implemented within UK Defence must follow the policy and guidance set out in JSP 457 Volume 5: Public Key Infrastructure.

For guidance on DCP and CPS projects should contact the DPMA.

This policy is outside the scope of the e-GIF. This policy is consistent with the NC3TA.

Policy

Strategic

1004.01: Defence PKI Policy

1004.01.01 All implementations of certificate services shall implement the following policies:

1004.01.01.01 JSP 457 Volume 5: Public Key Infrastructure Technologies and X.509 Public-key Certificates.

Comment: This policy stipulates a number of standards to which components of a Defence PKI must conform. These include the implementation of PKIX standards for X.509 interoperability, support for PKCS certificate requests, and the provision of a HSM with FIPS140 Level 3 or equivalent to protect CA signing keys.

1004.01.01.02 MOD Defence PKI X.509 Certificate Policy and associated DKPI document set.

This policy is intended to provide the overarching direction for Defence PKI implementations.

1004.01.02 All implementations of certificate services shall also adhere to the physical and IT security policy set out in:

1004.01.02.01 JSP440 - the Defence Manual of Security (in particular Volume 3 paragraphs 2320 - 2322)

1004.01.02.02 MPS 2000 (section 10.3, in particular)

Comment: Adherence to a common set of standards across Defence will ensure that implementations of certificate services are able to interoperate within MOD and with external partners.

1004.02: HMG Policy

1004.02.01 All implementations of certificate services shall conform to:

1004.02.01.01 e-Government Strategy Framework and Policy Guidelines

This framework is aimed at those seeking to establish, procure or provide e-Government services.

1004.02.02 If certificates are to be used for secure IPSec connections, the implementation shall follow:

1004.02.02.01 Manual V - Use of IPSec in Government Systems - Implementation Standards

1004.02.02.02 S(E)N 03/1 - the Use of IPSec in Government Systems

1004.02.03 If certificates are to be used for authentication in the TLS protocol, the implementation shall follow the guidance given in:

1004.02.03.01 S(E)N 00/3 - Using Transport Layer Security Protocol in Information Age Government Applications

1004.03: Other Policy

1004.03.01 Certificate service providers wishing to show that they operate according to 'best practice' shall demonstrate compliance with:

Strategic (Continued)
1004.03.01.01 tScheme (www.tscheme.org)

Deployed
As for Strategic domain.

Tactical
As for Strategic domain.

Remote
As for Strategic domain.

Responsibility for Implementing the Policy

Implementation of this policy shall be the responsibility of all IPTs (and their suppliers) that provide Certificate services and/or Public Key Infrastructures.

Procedure

Not Applicable.

Relevant Links

JSP 602: 1003 Authentication Services

AMS guidance on JSP 457 Volume 5 can be found here (not yet available).
<http://www.ams.mod.uk/ams/default.htm>

AMS guidance on JSP 440 can be found here (restricted site only).
<http://www.ams.mod.uk/ams/default.htm>

Information on 'Manual V - Use of IPsec in Government Systems - Implementation Standards' can be found from the CESG Bookstore. The Bookstore is only available over the RLI, and information on CESG can be found here. (<http://www.cesg.gov.uk/>)

Information on 'S(E)N 03/1 - the Use of IPsec in Government Systems' can be found from the CESG Bookstore. The Bookstore is only available over the RLI, and information on CESG can be found here. (<http://www.cesg.gov.uk/>)

Information on 'S(E)N 00/3 - Using Transport Layer Security Protocol in Information Age Government Applications' can be found from the CESG Bookstore. The Bookstore is only available over the RLI, and information on CESG can be found here. (<http://www.cesg.gov.uk/>)

A glossary of terms and abbreviations used within this document is available [here](#).

Instructions on how to read a JSP602 leaflet are available [here](#).

Compliance

Stage	Compliance Requirements
Initial Gate/DP1	MOD Projects shall submit a formal declaration that they have read and understood the policy and sought guidance from the SME(s).
Main Gate/DP2	Projects shall submit a formal declaration that they have read and understood the policy and sought guidance from the SME(s). The use of PKI must be endorsed by both the Defence ComSec Operating Authority and the Accreditor(s) before procurement action is initiated (JSP 440 Volume 3)
Release Authority/DP5	MOD Projects (supported by their equipment suppliers) shall provide evidence of their compliance with the elements of this policy defined within the SRD (and MODAF technical views). Evidence of conformance shall be presented from Factory Acceptance Tests and tests carried out at appropriate Defence Test and Reference Facilities.