

<b>JSP 602 Instruction</b>	1003	<b>Applicability</b>	Applications, Infrastructure, Security Configuration Identity
<b>Configuration Identity</b>	Version: 01.02 Amended: 2009-03-02 Reviewed: 2006-06-21	<b>Epoch Applicability</b>	2005 - 2009

## **JSP 602: 1003 - Authentication Services**

### **Outline**

*Description:* Authentication Services describe the methods and services that support the authentication of users to Defence systems and services.

*Reasons for Implementation:* The reliable identification of MOD entities is crucial to the secure operation of Defence systems and a key supporting technology for NEC.

*Issues:* MOD policy on smart tokens primarily deals with smart cards rather than other technology.

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

## Policy

### **Strategic**

#### **1003.01: Smart Cards**

**1003.01.01** All implementations of smart cards shall be in accordance with the following policy:

**1003.01.01.01** JSP 457 Volume 6: Smart Cards

*This policy is intended to provide the overarching guidance for Defence smart card interoperability.*

*Comment:* JSP457 Volume 6 is concerned only with smart tokens that conform to ISO7816. This means that tokens other than smart cards (USB tokens, for example) are not addressed by the policy, and their use should be approved by the Defence Smart Token Authority. Passwords and biometrics are also out of scope.

**1003.01.02** The authentication services shall also adhere to the physical and IT security policy set out in:

**1003.01.02.01** JSP440 - the Defence Manual of Security (in particular Volume 3 paragraphs 2320 - 2322)

**1003.01.02.02** MPS 2000 (section 10.3, in particular)

#### **1003.02: Authentication Services**

**1003.02.01** All implementations of authentication services shall follow the government guidance as defined in Infosec Memoranda 24, 26, 27, and 28:

**1003.02.01.01** Infosec Memorandum 24: Passwords, Tokens and Biometrics Used in Combination for Identification and Authentication of Users in Government IT Systems

**1003.02.01.02** Infosec Memorandum 26: Passwords for Identification and Authentication

**1003.02.01.03** Infosec Memorandum 27: Assessment of the Contribution of Tokens to Multi-Factor Identification and Authentication Systems

**1003.02.01.04** Infosec Memorandum 28: Use of Biometrics for Identification and Authentication

*These documents are designed to be used in conjunction to assess how authentication technologies may be combined to achieve a required strength of authentication.*

*Comment:* The guidance given relates only to passwords, tokens and biometrics used for identification and authentication purposes. Separate advice must be sought if cryptographic protection of information (eg, on a smart card) is required.

**1003.02.02** All implementations of authentication services shall conform to:

**1003.02.02.01** E-Government Strategy Framework Policy and Guidelines version 2.0

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

<b>Deployed</b>
As for Strategic domain.

<b>Tactical</b>
As for Strategic domain.

<b>Remote</b>
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 authentication services or supply and use smart cards in an authentication role.

## **Procedure**

Not Applicable

## **Relevant Links**

JSP602: 1004 - Certificate Services

AMS guidance on JSP 457 Volume 6 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>)

CESG Infosec Memoranda can be found here. (<http://www.cesg.gov.uk/>)

E-Government Strategy Framework Policy and Guidelines version 2.0 can be found here.  
([http://www.govtalk.gov.uk/policydocs/policydocs\\_document.asp?docnum=650\&topic=56\&topicitle=Security+Framework\&subjectitle=Security](http://www.govtalk.gov.uk/policydocs/policydocs_document.asp?docnum=650\&topic=56\&topicitle=Security+Framework\&subjectitle=Security))

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
<b>Initial Gate/DP1</b>	MOD Projects shall submit a formal declaration that they have read and understood the policy and sought guidance from the SME(s).
<b>Main Gate/DP2</b>	MOD Projects shall reference in their SRD (and MODAF technical views) the specific policy elements contained within this leaflet that are applicable to the system, equipment or application they are procuring or updating.
<b>Release Authority/DP5</b>	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.