JSP 602 Instruction	1032	**Applicability**	Applications, Infrastructure, Network/Communications, Security
Configuration Identity	Version: 02.01 Amended: 2009-03-02 Reviewed: 2009-01-14	**Epoch Applicability**	2005 -2011

JSP 602: 1032 -Cryptography and Key Management

Outline

Description: This policy leaflet covers Cryptography services and the services used to manage crypto keys. Cryptographic services are protocols and practices that enable secure communication and storage of information. Key Management services are protocols and practices that enable the assured use of cryptographic key variables.

*Reason*s *fo*r *Implementation*: To ensure that information is appropriately protected when it is communicated or stored. Without standardisation of cryptographic services, interoperability within and between UK forces, and between UK forces and Allies, will be complicated by the use of different approaches to cryptography. Standardisation of key management services will help ensure that a common best practice is uniformly applied across Government.

Issues: None identified

Guidance: IPTs/Users having a secure information exchange requirement, a need to protect sensitive data, or an envisaged need to connect to a protectively marked network or system will need some form of cryptographic device. As such they must discuss their requirements with the Defence Cryptosecurity Authority (DCA) Projects Section in order to ensure that any requirement is properly processed and complies with current and future MOD and UK Information Assurance policy.

IPT/User Cryptographic requirements must be captured using the Project Cryptographic Plan (PCP) document which must be used to ensure continued cryptographic support.

A PCP is an IPTs/user owned document produced to a DCA template. The DCA Projects Section will assist and advise IPTs/users throughout the drafting process. Once completed and approved by the DCA PCP Management Review Board, the document will be passed, for approval, to the CESG as the National Technical Authority (NTA) for Information Assurance.

Cryptography and Key Management is outside the scope of both the e-GIF and the NC3TA.

Policy

Strategic

1032.01: Cryptographic Equipment

1032.01.01 All cryptographic equipment shall:

> **1032.01.01.01** Use algorithms for encryption and key management approved by CESG as the NTA for Information Assurance. For RESTRICTED see Cabinet Office S(E)N 02/3;
>
> **1032.01.01.02** Be accredited for use at the appropriate protective marking by the NTA;

1032.02: Narrow Band Voice and Data

1032.02.01 All cryptographic devices providing a narrowband (under 64 kbps) on demand data or voice service shall use:

> **1032.02.01.01** Transfer within UK forces -NGVDC MER profile shall be used (see comment)
>
> **1032.02.01.02** Transfer with Close Allies -FNBDT MIR profile shall be used (see comment)
>
> **1032.02.01.03** Transfer with Allies and non-Government Organisation -there are no mandated standards (see comment).

The aim is to provide an inherently interoperable capability to UK forces, with assured separation between communities achieved cryptographically.

Comment: NGVDC / FNBDT provides secure voice (using MELP) in channels of at least 2.4 kbps. There is no inherent size to the data channel the NGVDC / FNBDT may support, they do however become inefficient at high rates and a LEF encryptor should be considered. Transfers with allies and NGOs is recognised as a something that is desirable and needs to be addressed. However, no work has been undertaken thus far.

1032.03: IPv4 and IPv6 Traffic

1032.03.01 All cryptographic devices providing an IP service shall use:

> **1032.03.01.01** Transfer within UK forces -HAIPIS MER profile shall be used
>
> **1032.03.01.02** Transfer with Close Allies -HAIPIS MIR profile shall be used
>
> **1032.03.01.03** Transfer with Allies and non-Government Organisation -there are no mandated standards (see comment).
>
> *Comment*: The application of traffic flow security to IP cryptos is limited by the need for efficient network usage. Transfers with allies and NGOs is recognised as a something that is desirable and needs to be addressed. However, no work has been undertaken thus far.

The aim is to provide an inherently interoperable capability to UK forces, with assured separation between communities achieved cryptographically.

1032.04: Link Layer Traffic

1032.04.01 All cryptographic devices providing a link layer service shall

use:

> **1032.04.01.01** Transfer within UK forces -LEF MER profile shall be used
>
> **1032.04.01.02** Transfer with Close Allies -LEF MIR profile shall be used

Strategic (continued)

1032.04.01.03 Transfer with Allies and non-Government Organisation -there are no mandated standards (see comment).

The aim is to provide an inherently interoperable capability to UK forces, with assured separation between communities achieved cryptographically.

Comment: Link-layer traffic should be considered to be using ”nailed up” (i.e. permanently allocated) high speed links (>100kpbs). Slower links may be better serviced by NGVDC / FNBDT. Transfers with allies and NGOs is recognised as something that is desirable and needs to be addressed. However, no work has been undertaken thus far.

1032.05: Key Management Services

1032.05.01 Key management shall be in accordance with Infosec standard No. 4. The following standards shall be used for key management services:

1032.05.01.01 Network transfer from UK Key Management System to crypto-there are no mandated standards (see comment).

1032.05.01.02 Crypto Fill Gun Interface -EKMS 308

1032.05.01.03 Transfer from UK Key Management System to Local Key Management System -EKMS 319, 320.

IS.4 is the UK national standard for key management in UK Government.

Comment: Crypto’s and systems that receive key material via a UK NDA distribution route must conform to common standards for transfer of material between the UK key management system and individual cryptos or local key management systems. Transfers within system are advised to follow the above standards. Standards for Network transfer from UK Key Management System to cryptos are currently being developed by CESG. Appropriate standards will be published when available.

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 cryptography and key management services across the GII.

Procedure

All cryptographic equipment will be subject to evaluation by CESG.

Relevant Links

JSP602: 1013 -Internetworking

JSP602: 1020 -MOD LAN to MOD WAN

JSP602: 1021 -MOD LAN/WAN to External WAN

JSP602: 1022 -MOD WAN to MOD WAN

JSP602: 1004 -Certificate Services

JSP602: 1036 -Security Architecture

JSP602: 1029 -Voice Interchange

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) as required.
Main Gate/DP2	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. A Project Cryptographic Plan (PCP) and Key Management Plan (Part 2) agreed with DCA and CESG shall be submitted. Where cryptographic capability is to be included in equipment being developed an agreed (with CESG) evaluation plan shall be submitted.
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 the test house, an evaluation certificate from CESG for equipment covered by the evaluation plans or a Key Management Plan agreed with UK KPA.