

JSP 602 Instruction	1036	Applicability	Applications, Infrastructure, Security
Configuration Identity	Version: 01.02 Amended: 2009-03-02 Reviewed: 2006-06-28	Epoch Applicability	2005 - 2009

JSP 602: 1036 - Security Architecture

Outline

Description: The Security Architecture defines minimum security requirements for the exchange of information to support MOD operations and its wider Departmental business.

Reasons for Implementation: To meet MOD's security and information sharing objectives, security controls must be strategically placed. If security protection is implemented in a piecemeal fashion by individual projects, it will hinder the efficient and effective information sharing that is essential for achieving NEC. Adherence to the DSA within MOD is essential for achieving NEC. Protection needs for information and services must be met, as they are an integral part of the operational C2I and ISTAR requirements. Multiple projects must support this provision in a consistent fashion across the system of systems. Any deficiency represents a point of weakness that undermines the system as a whole and jeopardises the protection of key assets that are crucial to the success of current operations or future capability. If this deficiency must be made good by more restrictive controls elsewhere, this is likely to impede information sharing and operational effectiveness. Compliance with a security architecture is therefore not just a security issue, it has critical implications for operational effectiveness. Failure to implement the SIA or to comply with defined standards leads to problems with interoperability of defence equipment and lack of flexibility in its use for deployment, impairing operational effectiveness.

Issues: Enforcement of the security of MOD CIS is primarily carried out by accreditation, which must be obtained before any CIS is permitted to store, process or forward any official information.

Three levels of minimum standards are defined as part of the Unified GII Security Architecture:

- DSA defines the set of major security constraints to be applied across all MOD's system of systems to achieve coherent protection for NEC. It is defined by DGINFO/DCBMJ6/J6Pol/CIS Security Architecture using Domain Based Security techniques as defined in DIAN-08.
- SIA provides design descriptions and guidance for the implementation of inter-operating projects and systems in conformance with the DSA.
- Functional and Interface standards defines standards for security functionality to be adhered to by systems implementing specific parts of the DSA and SIA.

Policy on the Unified Architecture is not yet agreed, however agreement on the high level DSA and on a process for its further definition is at an advanced stage and full endorsement within MOD is currently being sought.

Guidance: DIAN-07 details the accreditation process by which security concerns are managed in the project life cycle. Adherence to MOD's security architecture should be achieved through these processes. DIAN-08 details the language used to define the DSA.

Policy

Strategic

1036.01: General Security Architecture Policy

1036.01.01 JSP440 defines mandatory policy for security within MOD. The DSA takes a federated approach to compliance with this policy. It introduces project dependencies for security in order to enable the information sharing required by NEC. Hence compliance with JSP440 is dependent on compliance with the DSA by all MOD's interconnected systems.

1036.02: Defence Security Architecture

1036.02.01 All projects providing CIS capability to MOD shall declare the position of the CIS within the DSA. The project shall specify all:

1036.02.01.01 security domain(s) supported by the CIS

1036.02.01.02 portals either implemented or relied on by the CIS to enable users to work in the domains

1036.02.01.03 connections that are either implemented or relied on by the CIS provided

1036.02.01.04 infrastructure islands implemented by the CIS

1036.02.01.05 causeways implemented or relied on by the CIS

The project shall provide a security argument with supporting evidence to show that all of the security requirements specified by the architecture for these architecture components are met, either by the project or by another identified authority. Compliance with this policy is necessary from all contributing projects in order to remove the necessity for inter-project boundaries which place artificial barriers to effective information sharing.

1036.03: Security Implementation Architecture

1036.03.01 Projects shall identify all other projects and systems with which interoperability is required and demonstrate that security parameters associated with the exchange of information are mutually compatible.

Liaison among projects delivering in comparable timescales is essential to ensure that a consistent approach to the provision of security measures is taken.

1036.04: Functional and Interface Standards

1036.04.01 Functional Interface Standards relating to cryptographic devices are mandated within JSP602: 1032 - Cryptography and Key Management.

1036.04.02 Functional Interface Standards relating to PKI are mandated within JSP602: 1004 – Certificate Services.

These JSP602s cover the current MOD policy relating to interface standards.

Comment: MOD policy is still developing in this area of security architectures. This policy category will be updated as more policy is developed.

Deployed

1036.05: Defence Security Architecture

As for Strategic domain.

Comment: CIS provided in the Deployed domain may contribute to the same security domains as in the Strategic domain and must meet the same minimum levels of protection.

1036.06: Security Implementation Architecture

1036.06.01 Projects shall identify all other projects and systems with which interoperability is likely to be required for any realistic deployment. They shall demonstrate that the security properties and assumptions of the CIS are compatible with participation in each of the declared scenarios.

Liaison among projects delivering in comparable timescales is essential to ensure flexible and efficient use of CIS for deployment.

1036.07: Functional and Interface Standards

As for Strategic domain.

Tactical

1036.08: Defence Security Architecture

As for Strategic domain.

Comment: CIS provided in the Tactical domain may contribute to a more limited range of security domains within the DSA, primarily because of the high threat nature of the environment within which they operate.

1036.09: Security Implementation Architecture

As for Deployed domain.

Interoperability of equipment in the tactical environment is particularly important to minimise the footprint, weight and sustainment burden of the total CIS equipment carried.

1036.10: Functional and Interface Standards

As for Strategic domain.

Remote

1036.11: Defence Security Architecture

As for Strategic domain.

Comment: CIS provided in the Remote domain may contribute to a more limited range of security domains within the DSA, primarily because of the relatively unprotected physical environment within which the equipment is used.

1036.12: Security Implementation Architecture

As for Deployed domain.

1036.13: Functional and Interface Standards

As for Strategic domain.

Responsibility for Implementing the Policy

CMIS is responsible for implementing the policy, supported by DPA, with the Integration Authority playing a key role in promoting awareness and ensuring compliance.

Procedure

All projects are required to conduct an ISA at the start of the project to identify the key security issues faced by the project and agree them with the accreditor. This process includes proposing a likely position of the project within the DSA. It also includes an initial appraisal of related projects and confirmation that the project's proposed position within the DSA is compatible with the positions of these related projects. The ISA also provides an outline plan for the accreditation process agreed with the accreditor.

By defining the accreditation process, a mechanism is put in train to agree with the accreditor:

- the evidence needed by Main Gate to show that the security requirements have been sufficiently defined and reconciled with functional requirements;
- the activities required and the evidence to be presented to achieve accreditation for each stage of the project at which capability (whether experimental, training or operational etc.) is delivered.

As the project requirements become firmly defined, the position within the DSA is finalised and published for the benefit of other projects. All of the derived security requirements are included (by insertion or reference) in the SRD for the project.

All relevant Reference Points within the Security Implementation Architecture are identified and the requirement to implement the interfaces defined at these reference points are included (by insertion or reference) in the SRD for the project.

Where there is a need to interoperate with other systems and there are no defined Reference Points in the Security Implementation Architecture that are applicable, the projects work together with the participation of technical advisors and accreditors to define a suitable Reference Point.

Reference configurations are provided to show the connectivity to other systems which enables the project to deliver the required operational capability. Security properties at the interfaces to other systems are fully described.

Relevant Links

JSP602: 1032 - Cryptography and Key Management

JSP602: 1004 - Certificate Services

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

Information on DIAN07 and DIAN08 is available on the RLI only from D Def Sy.
(<http://defenceintranet.diiweb.r.mil.uk/defenceintranet/teams/browseteamcategories/ddefsyinformationsecurity.htm>)

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	Projects shall provide evidence at Initial Gate that they have conducted an Initial Scoping Appraisal and obtained the agreement of their accreditor that: the need for security and accreditation have been adequately recognised by the project, the expected position of the project in the DSA has been defined and any concerns about potential non-compliance have been highlighted, and the proposed approach to the accreditation process is acceptable in principle. Projects shall specify in the project URD all the domains of the DSA within which the users require to work and the connections they require to use.
Main Gate/DP2	Projects shall provide evidence at Main Gate that they have obtained the agreement of their accreditor that: their declared position within the DSA is fully consistent with the functional requirements of the project as expressed in the project URD and SRD, the project is committed to satisfying all of the relevant security requirements derived from the DSA, any potential incompatibilities in the security relevant properties of interfaces to other systems/projects for all relevant scenarios of use have been resolved, and all relevant functional interfaces and standards have been recognised and requirements for compliance are included in the SRD.
Release Authority/DP5	All the evidence agreed with the accreditor as necessary to show compliance with HMG Policy, the DSA and other security requirements defined for the project shall be presented.