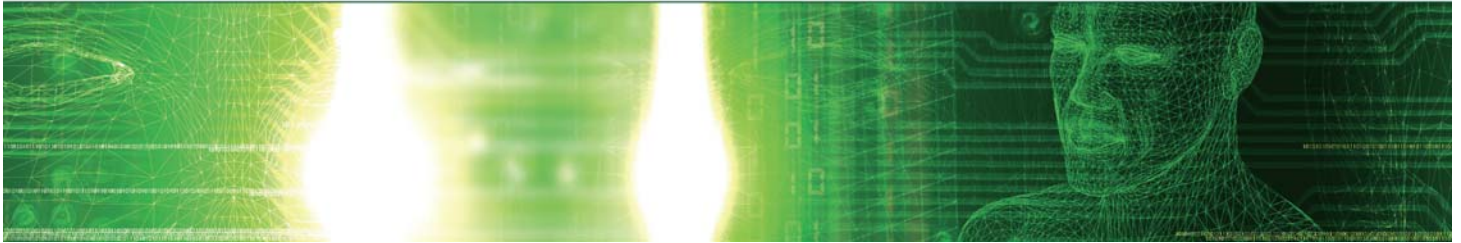


July 2010  
Issue No: 1.0

# Busy Reader Guide Requirements for Secure Delivery of Online Public Services



NATIONAL TECHNICAL AUTHORITY  
FOR INFORMATION ASSURANCE



## Introduction

The volume of public services being made available online to the citizen is increasing. Current and future HMG ICT projects must consider how end-to-end security of these services is achieved.

Whilst the Requirements for Secure Delivery of Online Public Services (RSDOPS) are working documents and do not currently constitute formal policy, these documents are published to increase awareness, understanding and encourage debate in this area.

The CTO Council are in the process of endorsing the RSDOPS documents to ensure a broader engagement with stakeholders. Feedback is now sought to ensure that stakeholders' views are captured as part of the ongoing development process and, where appropriate, are used to refine the content.

It is intended that the RSDOPS will replace the 2002 e-Government Security Framework (e-GSF).

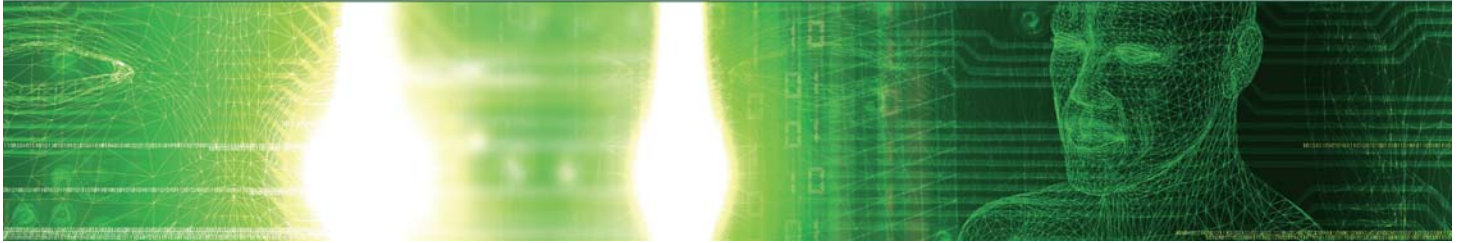
This Busy Reader Guide is aimed at senior management and other stakeholders responsible for service and system security with an interest in the procurement and provisioning, accreditation and security management, to assist in understanding, describing and managing potential risks posed by increased online transactions and interaction with the citizen over the Internet.

## Background

The RSDOPS is a response to shared services challenge 6 (Information Assurance) identified in the 2005 Transformational Government strategy and sets out an approach to deriving, discussing and agreeing security requirements for systems delivering public services electronically.

In response to the changed technical and political environment for delivery of public services, the following design aims were set for the RSDOPS work:

- Informed by the 2007 National IA Strategy (NIAS) – NIAS objective 1 requires the information owner to comprehend, manage, and accept the information risk of doing business.
  - Wider Audience – RSDOPS is not protectively marked and publically available with the objective of demonstrating to all stakeholders (including the public) that government attention to information risk is fair, reasoned, and proportionate.
  - Stakeholder Neutral – RSDOPS is explicitly stakeholder neutral and addresses the reasonable expectations of all involved parties.
-



- Discourage Blame Transfer Behaviour – RSDOPS actively discourages the transfer of ill understood risk as a mechanism for potential blame dispersal.
- Evident Roots in the 2002 e-GSF – The 2002 e-GSF is widely used as a language to describe security challenges and responses and investment in this should be preserved as far as is practicable.

Requirements for Secure Delivery of Online Public Services consists of two parts.

### **Part 1 – Principles**

Provides an introduction giving details of the status and scope of the publication and contextual material (such as background, policy, legislation and external standards).

The technical approach provided builds on the NIAS to provide a conceptual model supported by a recommended methodology for deriving security requirements.

The document outlines how security analysis of citizen facing services should focus initially on preservation of the business value of the transaction to all stakeholders rather than seeking to cast the analysis as a data security problem. The security problem now has to be described in terms of less familiar security properties such as accountability, provenance, and business value rather than the more traditional security properties of data confidentiality, integrity and availability.

The document recommends deriving the security requirements from a statement of stakeholder expectations that will be meaningful to the stakeholders themselves. This can be used as a basis of agreement between the parties with an interest in service security. An outline methodology for developing a security case is presented.

A candidate set of stakeholders is identified with examples of expectations that should be answered. Concerns and risks are assessed against each expectation from various viewpoints and are documented in table form for reference. Example expectations for the end user include privacy, authenticity, confidentiality, integrity availability, transparency, identity, reliance, payment safety, accountability and fairness, inclusivity and non-discoverability.

### **Part 2 – Security components**

Detailed information on each security components set is provided. An End User section covers the security components relevant to the people and businesses accessing the service. A Server section covers the security components relevant to the ICT hosting a particular service. A Network section covers the components relevant to the network infrastructure that is used to access the services and an Assurance section covers the components relevant to gain confidence in the end-to-end security of the public sector services. Greater detail of the requirements, examples and provisioning to attain each level is provided.

---



The copyright of this document is reserved and vested in the Crown.

IA  
CESG  
B2h  
Hubble Road  
Cheltenham  
Gloucestershire  
GL51 0EX

Tel: +44 (0)1242 709141  
Fax: +44 (0)1242 709193  
Email: [enquiries@cesg.gsi.gov.uk](mailto:enquiries@cesg.gsi.gov.uk)

© Crown Copyright 2010. Communications on CESG telecommunications systems may be monitored or recorded to secure the effective operation of the system and for other lawful purposes.

---