

Recent security incidents have highlighted the risks associated with data handling. This article examines an existing solution, designed for high assurance secure networks, to respond to some of the key government priorities



Assuring data handling procedures

Organisations depend on information to operate efficiently, and effective modern organisations rely on information technology to access, process and transport that information. Information technology is also used to automate manual processes, provide new ways of working and/or to facilitate remote client access to services. However, this technology also introduces new or amplifies existing security threats and vulnerabilities which, if realised, would impact severely the organisation's efficiency and effectiveness and which could, in turn, undermine the client's confidence in an organisation.

An example of these risks being realised was the HMRC loss of Child Benefit data, which became one of the catalysts

for a series of official reviews of information security and data handling procedures within government departments. These comprehensive reviews made a number of recommendations for immediate actions and for implementation in the future. EADS Defence & Security believe that the elimination of current weaknesses could be accelerated by government departments working in partnership with private sector companies, familiar with meeting the complex and diverse security needs of government.

The need for action

Three government reports have highlighted the need for action – the Cabinet Office report on Data Handling Procedures in

Government, the Data Sharing Review and the HMRC Information Security Report.

The Cabinet Office report on Data Handling Procedures in Government acknowledges the complex and diverse delivery chains. It focuses on management and cultural issues – identifying a need to ensure staff understand and comply with security policies and practices. The need for privacy impact assessments to consider both individual records and data aggregation is also identified. Other key findings include measuring the effectiveness of security through audit and monitoring and for new systems to be accredited and subjected to penetration testing.

The Data Sharing Review focused on regulatory aspects, codes of practice and

“Effective use of information is absolutely central to the challenges facing government today – whether in improving health, tackling child poverty or protecting the public from crime and terrorism”

Sir Gus O'Donnell Data Handling Procedures in Government, Final Report, June 2008

cultural changes, but also identified the need for decisions to be taken in the context of strong governance, transparency and accountability. It identified that technology had a role to play in achieving these goals.

The HMRC review following the loss of the Child Benefit data identified that operational concerns had taken precedence over security risks with authorisation not being sought to release data, and data being transported using insecure methods. It also identified that HMRC continued to operate paper based processes in a digital world and that technical and process measures needed to be taken to minimise the scope for error or malicious action.

The way forward

IT systems enforce end point security, controlling access to system assets and data held with that system. However, in the modern organisation there are multiple islands of data, both physical and electronic, with complex data flows between these islands. These data flows introduce a significant risk of losing or compromising data. Moreover, modern government needs to exchange data across an extended enterprise including other government departments, partners, mobile systems and home users. This increases the risk to data significantly. In consequence, a system is required that can control, manage and track the exchange of data across the extended enterprise.

The system must also be flexible enough to embrace changes in working practices, to prevent technology impeding government transformation initiatives. Designed by EADS to meet the stringent requirements of the MoD, Receptor is a system that meets these challenges having much of the required functionality already with a capability to include additional functionality while guaranteeing not to compromise extant functions.

Receptor is designed using techniques for software development within the nuclear

industry and to meet the rigour required of high grade cryptographic key management systems. Receptor is a web browser based application providing control, governance and accountability of the movement of both physical and electronic material between organisations, individual users and/or information systems. Based on proven government processes, Receptor has a flexible core capability which enforces central security policies while allowing localisation to accommodate departmental working practices. Where functionality can be managed and processed by the system without user intervention, system managers can configure their system to determine the level of automation and mandate the level of control and auditing to be applied between automated and manual processes.

Receptor operates a Central Office of Records for the whole life accounting of all material and is based around a Central Master Account (CMA). Subordinate accounts operate either as deployed databases located on a separate server or as logical accounts on the parent account server. This allows the system to be configured to compartmentalise the data when restricting access to authorised users.

Through its network management capability, Receptor can operate as either a hierarchical or flat/central distribution system. Receptor manages distribution through the use of vouchers to record the request and movement of material through the system, and can support either a “push” mechanism against a predefined delivery schedule or a “pull” mechanism, where the end accounts/users receive their material on demand. The network management capability also specifies the required transport links and levels of cryptographic protection between accounts.

Receptor also provides a comprehensive monitoring capability using audit and accounting facilities to determine the accuracy of the system and of the electronically

controlled assets. System data also provides the baseline data for musters and stock checks to confirm the holdings of physical assets. When assets with an expiry date reach their end of life, the system alerts the asset owners and identifies the assets as requiring destruction.

Had Receptor been in place at the HMRC, it would have significantly reduced the possibility of data loss and also have expedited the search for the missing data. Introducing Receptor into departments such as HMRC would strengthen data security, reduce data handling costs through process automation and demonstrate the commitment of management to meet their data handling responsibilities.

Introducing Receptor pan-government would enforce a common standard across departments, improve confidence in government's ability to protect data and to deliver a cost effective solution to the data handling problem.

Receptor could be used in conjunction with existing IT systems, thereby removing the need for a ‘big bang’ replacement of current technology.

Receptor, combined with a cryptography solution such as ECTOCRYPT™, would provide a multi-level secure data transfer capability across the extended enterprise, a development which would help make a reality of concepts like the Public Sector Network (PSN). ●

Steve Scott

Business Architect

EADS Defence & Security Systems

www.eadsdsuk.com

For further details on Receptor please contact ukinfo@eads.com

