

An update for Government from the Intelligent Customer Mechanism

The Intelligent Customer Mechanism (ICM), developed by the IA Technical Programme, promotes collaboration across Government and Industry to enable a joined-up approach to acquiring trusted ICT.



Green light for the ICM as the way forward for 'Common Good' IA capability

The IA Delivery Group (IADG)* adopted the ICM approach for delivering 'Common Good' IA capability at their meeting in mid September. At the same meeting it was agreed that Secure Data Transfer (SDT) would be the first topic to be addressed through the ICM formally.

At the November meeting the IADG commended the progress made by the SDT Collaboration Group, initiated by the CESG ICM team, which has been investigating the business needs and options for achieving a pan-Government SDT capability. The IADG endorsed the specific SDT recommendations put forward and requested development of a more detailed proposal in time for the next meeting in January 09.

* *Background to IADG*

The Data Handling Review (DHR) led to changes in IA governance. These changes included the establishment of ministerial responsibility for IA and supporting committees to oversee IA delivery across Government. The changes included decisions affecting the IA Technical Programme (IATP) and the ICM. It was decided that GCHQ would deliver the IATP (hence IATP is no longer a Cabinet Office-led programme) and would also 'own' the ICM.

The IADG is one of the oversight committees, chaired by John Suffolk, the Government CIO. The IADG reports to the IA Oversight Board, chaired by Sir Gus O'Donnell, Head of the Civil Service, which reports to ministers on the performance of Government Departments in delivering the DHR recommendations and National IA Strategy.

The IADG articulates wider IA business needs, establishes the 'Common Good' requirement for funding IA capabilities, and determines the need for new IA policies and standards.

Progress on the Secure Data Transfer collaborative initiative

An SDT collaboration group has been formed with representatives from across Government (CTO Council, HMRC, DWP, MoD, GCB, IPS, Home Office, NHS, ONS, FCO, DCLG). Other departments also provided initial input (DCSF, Met Office, BERR, NPIA, MoJ).

Agreement was reached in principle among key stakeholders to work towards convergence on a reduced set of interoperable SDT capabilities, including a single preferred service for exchange of data with external organisations.

Although still at an early stage of developing plans and requirements, the collaboration group has identified some areas with potential for seeking new assured shared services or capabilities from Industry, including:

- Seamless interconnection and exchange between the existing secure data transfer systems serving various communities over networks in central government and the wider public sector, including local authorities, health, criminal justice and the police forces
- Packaged solutions for all organisations within or outside the secure government networks, to enable integration and connection with the proposed pan-Government SDT capability for external transfers, which is likely to build out from the current Government Gateway services including authentication
- Provision of services to support secure document and message exchange between individuals both within and beyond secure government networks, who need measures to protect sensitive, personal or 'need to know' content where standard email or automated data transfer remains inappropriate
- Provision of capability to support collaborative working and more effective sharing of information between government departments and with external partners (e.g. Industry)
- While HMG should, in time, minimise the use of removable media, requirements for the exchange of data using assured and appropriately secured removable media solutions remain, for the time being, at various levels of protective marking.

Additional 'Common Good' topics for consideration

The ICM - led collaborative approach has also identified further topics which have been endorsed by the IADG for consideration. Treatment of these topics through the ICM will be funded jointly by IATP sponsors and OGDs. The CESG Systems Engineering team will now convert these topics into a coherent delivery portfolio, which is holistically linked to the IATP 09/10 portfolio.

The list below has been determined from OGDs', and specifically CTO Council's, input as the highest priority topics for required 'Common Good' capability.

The first two topics to follow the Secure Data Transfer initiative for collaborative ICM treatment are **Remote Access** and **Identity Management**.

New topics for collaborative ICM treatment

Remote access

Identity Management

Sharing beyond boundaries

Virtualisation and Data Separation

Multi Level Security

Convergence, VOIP & Unified Messaging

Collaborative Working

IA audit standards & tools

NGN

GSI/xGSI

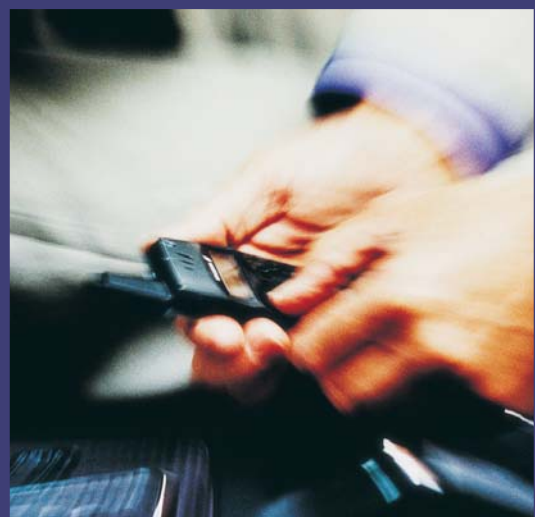
Access control & access rights management

Service Orientated Architecture

Secure Mobile Communications

Trusted Computing

Off Shoring



IATP PROJECT NEWS

SMI (Security Management Infrastructure)

The SMI project is working collaboratively with the MoD CIPHER programme to deliver:

- an SMI which will allow future IA components, such as firewalls, cryptographic functions and authentication servers, to be initialised, configured, updated and managed in a trusted, secure way - **essential for all government ICT systems in the future.**

MoD has the 'lead department' role to develop an SMI solution which will address both MoD and wider government needs.

The assessment phase contracts were signed in early November with the two preferred consortia leads for the CIPHER assessment phase, Thales and Logica. The consortia are now beginning work to assess and demonstrate SMI solutions, leading to a recommended solution being proposed for full development. Both consortia have held initial CIPHER events to engage with wider Industry.

NGN (Next Generation Networks)

To meet the demands for flexible voice and data services, the telecommunications industry is migrating to new technologies. Government and Industry are working together to understand and respond to the new challenges and risks presented by this complex environment.

The development of Good Practice Guidance for use by the telecommunications industry to support them achieving the 'Standard Security Level' required for PROTECT government use, or that equivalent to traditional PSTN service, is nearing completion.

A draft copy can be obtained by email request at ngn_assurance@cesg.gsi.gov.uk

Work is currently underway to define, agree and implement a scheme for the independent validation of the 'Standard Security Level', it is envisaged this scheme will be operated by industry but governed by CESG. The scheme is expected to be up and running by Spring 2010.

In the meantime, for anyone wanting to obtain interim assurance for a NGN telecommunications system or service to the 'Standard Security Level' or to meet impact levels 3,3,4, interim guidance is expected to be available later this month and available via www.cesg.gov.uk/policy_technologies/ngn/index.shtml

Secure Mobile Communications

Progress on SME-PED*

- The US State Department has agreed a Technical Assistance Agreement which will allow the transfer of SME-PED US technology from the US to the UK
- CESG is working on a Proof of Concept Network Operations Centre (POC-NOC), which is the pilot infrastructure required to test SME-PED in the UK. The pilot is expected to go live in Spring 2009
- CESG is progressing discussions with HMG customers, including MoD, regarding the lead department role for the UK SME-PED pilot.

**SME-PED stands for Secure Mobile Environment Personal Electronic Device which is a PDA-type device for secure voice and data communications developed in the US.*

IATP Trials Team - Industry and Government working together to deliver

Collaborative workshops and trials have been proving their worth for some time now - getting away from the traditional 'stovepipe', insular mentality and, instead, encouraging a 'Common Good' mindset.

This intelligent, collaborative way of working has already resulted in savings in excess of £6 million for Government.

The IATP trials team was originally formed to organise collaborative trials of cryptographic devices as they come to market. The membership includes active representation from the High Threat Club (MoD, Intelligence Agencies, FCO, CO) and now the Police. Lead departments are identified for each product trial and form the test plan and contractual agreements on behalf of the rest of the team.

Industry views the trials team as a key source of HMG customer feedback and is making more use of the team's meetings to review product requirements and marketing plans.

Following the ICM approach, the trials team is helping to create a marketplace for new IA products, as well as for the new UK specifications of HAPE and SCIP. Here, the team is working with HMG to ensure demand for strategic products is made tangibly clear to Industry players by acting as a facilitator in early commercial discussions.

The team is ensuring Industry has the information it needs to fulfill contracts with HMG, such as the BRENT specification work advertised through the Crypto Developers' Forum.

The catalogue - one stop shop for non-high grade IA goods and services

The IATP has been working collaboratively with OGC buying solutions, MoD and CESG on the development of an IA section of the MoD DE&S Information Systems & Services ICS Catalogue which can be accessed at: <http://www.icscat.mod.uk>

It is intended to be a 'one stop shop' for the purchase of non-high-grade IA goods, services and consultancy. Having registered on line, customers in public sector organisations can use the online ordering facility via the website above.

All the products and services included in the IA section are government approved. This means that they have gone through evaluation and certification under a scheme recognised by CESG, as the National Technical Authority for IA.

FOCUS FOR THE ICM AND IATP GOING FORWARD

As we move forward the ICM focus remains very firmly on 'Common Good' pan-government initiatives and reports to, and seeks funding through, the IADG.

IATP will be focussing on work which addresses the more 'high-grade' needs of its sponsoring departments. John Taylor (MoD CIO), as the most significant funder of IATP, has taken on the role of Senior Sponsor for the programme and John Cook (DGInfo) is IATP Director.

Both IATP and ICM work will be enabling capability delivery through Industry.

Further information about the portfolio of work to be taken forward in 2009/10 will be in the next issue of IA matters.

Accessing information on the ICM and IATP

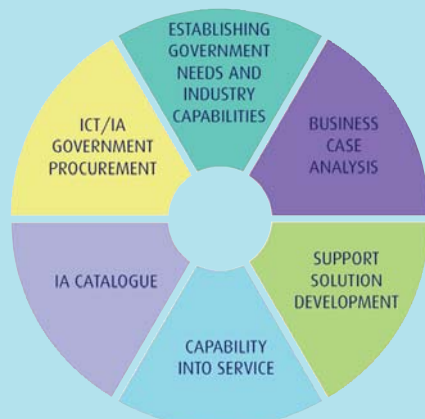
This issue (and previous issues published in October and November, which were aimed at Industry) can be accessed from the IA UK website at: <http://www.iauk.org.uk>

The IATP external web pages are currently being updated and will be transferred to their new home on the CESG external web site within the next few weeks.

The ICM is a collaborative way of working which enables the UK Government to manage its information in an assured way.

GOVERNMENT DEPARTMENTS HAVE A VITAL ROLE TO PLAY IN THIS COLLABORATION

SAVE THROUGH COLLABORATION



Get involved and be kept up to date

Regular updates will be published. For more information and to find out how you can play a part please contact: icm@gchq.gsi.gov.uk

Send your feedback to icm@gchq.gsi.gov.uk with suggestions you may have for improvements or for future topics for inclusion.