

File Edit View Insert Format Tools Message Help

Send

Cut

Copy

Paste

Undo

Check

Spelling

Attach

Priority

From:

Signed, sealed and delivered: making email secure

The UK Council for Electronic Business (UKCeB) prides itself as being 'both a catalyst and a facilitator', in promoting joint industry/MOD secure collaboration activity. In this special feature, Carl Billson, UKCeB Task Force Business Consultant, writes exclusively for MOD DCB, explaining a new secure approach to sharing confidential information.

How do you make email – the most basic and prevalent form of information exchange in business – sufficiently secure for its confident use across 'Team Defence', and implement it in a way that is inclusive of the needs of the small and medium-sized enterprises (SMEs) that play a vital role in the supply chain and support network? This challenge has been successfully addressed by Signed and Encrypted Email Over The Internet (SEEOTI), an approach that has been evaluated by members of the UK Council for Electronic Business (UKCeB).

Ltd undertook to organise and project manage the SEEOTI Project on behalf of MOD CIO and UKCeB. Widespread participation involving over 20 organisations reflected awareness of shared issues of incoherent and incomplete communication capabilities that, in turn, limit the ability to work efficiently and effectively across Team Defence.

Users in the evaluation enacted a scenario based on the need to exchange selected documents that had commercial, IPR and defence sensitivities in a controlled and audited manner via email. SEEOTI

How does SEEOTI work?

SEEOTI implements the Secure Email specifications derived by the Transglobal Secure Collaboration Program (TSCP) – a spin-off from a previous UKCeB initiative that involves multinational A&D companies as well as specialist IT organisations. It integrates Commercial Off The Shelf (COTS) products from TSCP members Deep-Secure, TITUS and Boldon James. Learning gained from the SEEOTI evaluation and dialogue with SMEs is helping these suppliers develop commercial packages that will provide SEEOTI as a bundled 'plug-in' service designed for SMEs who often have limited or no dedicated IT resources. So, let's examine the use of SEEOTI in a typical scenario that requires secure exchange of documents between various parties.

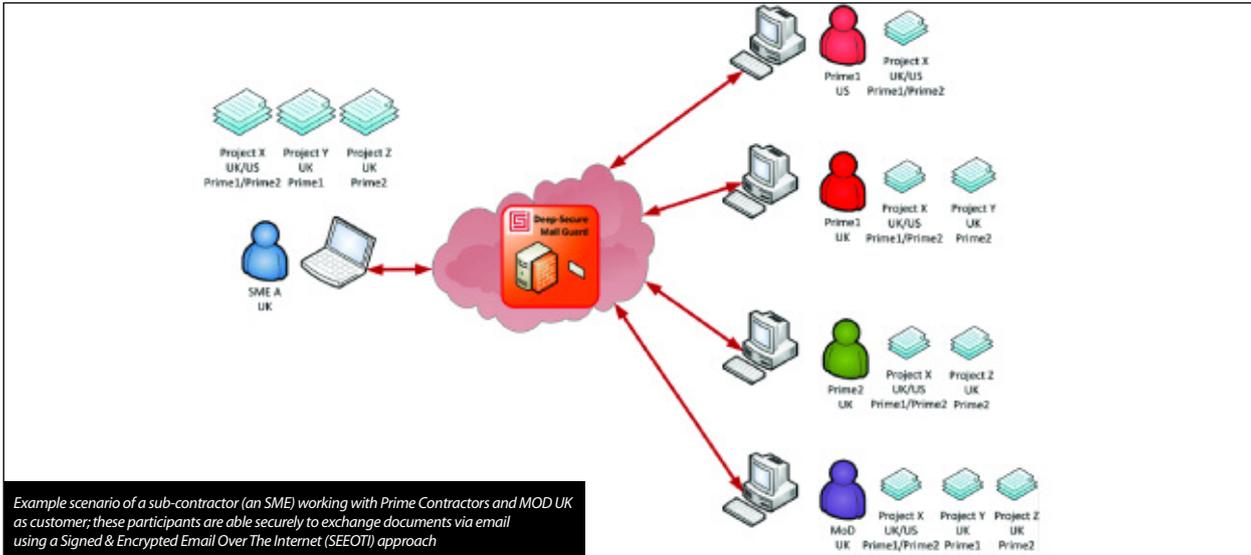
The schematic illustrates the SEEOTI principles in a scenario involving a small UK-based SME that is working with Prime Contractors on three different UK projects (X, Y and Z) for the UK Ministry of Defence (MOD): a UK-based project with Prime 1; a UK-based project with Prime 2; and a joint UK/US project with both Prime 1 and Prime 2. Hence, SME A will be authorised and cleared to exchange documents relating to all three Projects X, Y and Z. Between SME A and the other four participants in this project is the cloud-based Deep-Secure Mail Guard which has a SEEOTI 'policy' configured in line with the requirements of SME A working with the four participants shown. This means that the rules governing email document exchanges using SEEOTI are configured, maintained and audited

"SEEOTI is one of a number of secure collaboration activities for Team Defence supported by the UKCeB Secure Information Sharing (SIS) Programme"

It is widely acknowledged that there is a need for a simple-to-use, standards-based enabling technology for email, one that allows SMEs to communicate securely with one another, with the MOD and with the major aerospace and defence (A&D) contractors: a common approach to secure email connectivity to underpin trusted collaboration within Team Defence.

A project to enable companies to have hands-on evaluation of SEEOTI was sponsored by the MOD's Chief Information Officer (MOD CIO) and UKCeB. Deep-Secure

configuration enables set-up of the business 'rules' that provide system control and governance over the exchange of encrypted emails. Using a SEEOTI approach, each business and individual is well supported by the solution to carry out the 'right' or permitted actions in terms of issuing emails; and, recipients also have assurance that the encrypted contents are securely delivered and from an accredited source. This is 'Signed and Encrypted Email Over The Internet', a generic capability but discussed here in terms of defence.



using the Deep-Secure Mail Guard. It is assumed, but not shown, that each of the partner organisations has a similar Mail Guard function to protect its networks.

This scenario-as-schematic shows the Mail Guard policy or rules are set up to determine the individuals in each organisation that are authorised and cleared to exchange documents on specific projects only. Here, for example, the US-based element of Prime 1 can exchange documents for Project X; the UK-based Prime 1 for Projects X and Y; the UK-based Prime 2 for Projects X and Z; and, the MOD person can exchange documents on all three projects. This straightforward and easily replicable SEEOTI approach means that participants do not require multiple, costly to maintain and bespoke solutions for secure email exchanges; the SEEOTI approach provides interoperability benefits for all.

SEEOTI is one of a number of secure collaboration activities for Team Defence supported by the UKCeB Secure Information Sharing (SIS) Programme, with sponsorship from the Joint Information Group (JIG) comprising industry and MOD and in collaboration with the TSCP whose members include prominent players in Team Defence.

In late 2011, the UK MOD established a senior-level Secure Information Sharing Steering Group (MOD SIS SG) with UKCeB participation. Its Terms of Reference are to "provide the governance and direction in order to deliver... coherent Secure Information Sharing across the extended Defence enterprise". It will "develop a strategy and roadmap for the delivery of Secure Information Sharing in order to promote interoperability with NATO, OGD and Industry. This will require the definition of a clear target architecture that assures coherent, incremental, scalable implementation that exploits delivery opportunities available in current funded projects."

What's next?

The next stage of SEEOTI development is a small-scale production capability to be implemented by a joint MOD/industry project team such that representatives from various business functions such as engineering, contracts, legal and project management have

opportunities to use SEEOTI capability, evaluating its business benefits in a real project context.

On behalf of Team Defence, UKCeB is committed to this next phase of 'hands-on' implementation and evaluation that will help shape the adoption of SEEOTI capability, and acknowledges the continuing

commitment of Deep-Secure Ltd and other participants. The intention is that the SEEOTI approach will be extended for 'Restricted Over The Internet' (ROTI) which requires prior accreditation of end points, provision of Digital Certificates for users and the specification of appropriate technology and where it is to be deployed.

MOD and industry endorsements for the SEEOTI approach on Secure Information Sharing

"Secure information sharing is a critical capability necessary to enable effective Contractorised Logistic Support for equipment and platforms. The Deep-Secure SEEOTI Evaluation was an extremely valuable exercise and indicates that secure information sharing is achievable with clear and demonstrable benefits for Team Defence."

Brigadier Alan Clacher, Joint Chair of MOD/Industry Joint Information Group Portfolio Management Board

"The SEEOTI work is a great example of how UKCeB can help industry and MOD to understand how technology can be exploited to improve collaborative working to help address the challenges of the current business environment."

Nigel Whitehead, Chairman of UKCeB Council and Group MD, Programmes & Support, BAE Systems

"This is a remarkable example of public/private achievement between the TSCP membership, the UK MOD and the UKCeB partners. With the growing need for secure collaboration throughout all business sectors and the ever-increasing threat on asserted digital identities used on the web, the success of SEEOTI is an encouraging step towards better trusted exchanges within the supply chain."

Philippe Lafandre, Chairman, Transglobal Secure Collaboration Program (TSCP) Systems

The MOD Information Strategy 2011 [MOD IS 2011, p8] highlights the need for collaboration between partners:

"Collaboration is key to enabling Information Superiority and the ability to make better decisions. By collaborating across organisational and national boundaries we will achieve improved shared awareness, which in turn will contribute to more effective and agile outcomes. Collaboration means creating, sharing and exploiting information with our allies, industry partners and OGDs, which is appropriately protected and secured. This can only happen if our information is assured, including the application of the right cyber practices and skills. Only then will users have the confidence that the information can be trusted, while being safe from malicious acts or misuse."

About UKCeB – www.ukceb.org

The UKCeB mission is "to transform secure information sharing for through life collaboration in defence acquisition and support". A not-for-profit organisation, UKCeB provides a 'Team Defence' perspective and drives forward activities prioritised by its joint MOD/industry membership.