



## **TSCP Publicly Releases Secure E-mail Specifications**

### **Roadmap for Safeguarding E-mail Communication Meets A&D's Rigorous Standards**

**HERNDON, Va. (Jan. 8, 2008)** – The Transglobal Secure Collaboration Program (TSCP) today announced a major breakthrough in its effort to make e-mail a viable communication channel in the rigorous environment where global government defense organizations and partners do business: the release of its Secure E-mail specification.

The TSCP's Secure E-mail specification directly addresses the need to eliminate e-mail's inherent identity and data transmission security flaws, allowing users to safely send and receive sensitive information user to user and desktop to desktop. The requirements were defined and endorsed by the members of the TSCP: U.S. Department of Defense (DoD), U.K. Ministry of Defence (MoD), BAE Systems, Boeing, EADS, Lockheed Martin, Northrop Grumman, Raytheon and Rolls-Royce.

The implementation is based on TSCP-defined specifications available publicly on [www.tscp.org](http://www.tscp.org). The specification provides step-by-step instructions organizations must follow to assign vetted identity information to all e-mail senders and recipients. The currently deployed implementation was constructed with commercial-off-the-shelf (COTS) solutions, open source software and a commercial trusted third-party service, CertiPath. The resulting architecture guarantees that information only travels to and from trusted parties.

“The most basic collaboration tool is e-mail, but it was never designed for security,” said Jim Cisneros, Deputy Chief Information Officer (CIO), Future Combat Systems (FCS) at Boeing, and Chair of the TSCP. “Trusting the authenticity and accuracy of e-mails is imperative for government organizations, prime contractors and our suppliers to jointly develop new technologies and respond to emerging threats.”

TSCP is in the process of preparing to assist current DoD programs in implementing Secure E-mail, for information currently classified as “Controlled Unclassified Information” (CUI), which includes “For Official Use Only” (FOUO) and “Sensitive But Unclassified” (SBU) information. The MoD also expects to deploy the capability enterprise-wide in 2008 for classifications up to “U.K. Restricted”. Prime contractors will adopt the specifications on an ongoing basis across equivalent levels of proprietary information – increasing the urgency for suppliers to have compatible e-mail frameworks.

(more)

“Sending ‘Restricted’ e-mails to allies and suppliers is far more complex than it sounds, requiring a proven architecture behind the scenes to ensure maximum safeguards,” said John Cook, Info Advisor of the U.K. MoD. “Secure E-mail will become increasingly essential to do business with the MoD.”

### How It Works

Secure E-mail requires organizations to have three components:

- **A PKI-based identity management program** administered in-house or through a certification service provider, depending on the organization’s size. PKI assures the identities for all employees and links digital certificates for signing and/or encrypting e-mail messages to those identities.
- **Implementation of the Secure E-mail specification.** Any organization can download the do-it-yourself manual on TSCP’s site and implement it with minimal IT resources.
- **End-user encryption certificate lookup**, either via a self-hosted LDAP proxy or a third-party provider, to automate the collection of users’ encryption certificates in Microsoft Outlook® or Lotus Notes® e-mail clients.

Unlike other secure e-mail implementations, TSCP’s Secure E-mail ensures in real time that the sender’s and receiver’s identities are known at a common level of assurance and are both still valid, and the underlying identity management systems can be trusted. That assurance, once vetted, is used to grant access to sensitive information. This prevents, for example, former employees from logging in and receiving “restricted” data.

"The TSCP is transforming e-mail from one of the most extensively used but least trusted collaboration capabilities to one that can be trusted with sensitive information," said Paul Grant, Deputy Information Sharing Executive, Information Sharing Office in the Office of the DoD CIO. "This will serve as foundational for sharing 'Controlled Unclassified Information' with our mission partners, which certainly includes our suppliers."

The Secure E-mail specification will be regularly updated to support export control processes, intellectual property protection and feedback from members and non-members alike. For full background and documentation on Secure E-mail, visit [www.tscp.org](http://www.tscp.org).

# # #

### About TSCP

TSCP is the only government-industry partnership specifically focused on designing solutions to address the most critical issues facing the A&D industry: mitigating the compliance, complexity, cost and IT security risks inherent in large-scale, multi-

### 3-3-3 TSCP Releases Secure E-mail Specification

national collaborative programs. The TSCP was founded in 2002, and has delivered several specifications and guidance documents on securing A&D supply chain data. The group today focuses on identity federation policies and governance. The TSCP is open to government organizations, prime contractors, integrators, suppliers and member trade groups. For more information, please visit [www.tscp.org](http://www.tscp.org).

**TSCP contacts:**

Keith Ward (North America)  
+1 (703) 713-4452  
[k.ward@ngc.com](mailto:k.ward@ngc.com)

Marc Speltens (Europe)  
+32 2-745-05-62  
[marc.speltens@sit.aero](mailto:marc.speltens@sit.aero)

Wayne Grundy  
Director, Transglobal Secure Collaboration Program  
Tel +44 7801 71 6134  
[wayne.grundy@tscp.org](mailto:wayne.grundy@tscp.org)

**Media contact:**

Adam Parken  
Corporate Ink Public Relations  
+1 (617) 969-9192  
[aparken@corporateink.com](mailto:aparken@corporateink.com)