

SONIC is a cost-effective WAN-based Top Secret (TS) shared working environment.

System Features

- Top Secret secure data repository
- Access to data repository across secure WAN
- Remote access terminals unclassified when not in use
- Site to site data transfer at any level from unclassified to TS

SONIC consists of two unique and accredited applications: StoS and PIEV.

StoS (Site to Site) is an application allowing the entire contents of media, either a floppy disk or a CD, to be transferred between identified sites using a dedicated communications path. The path is established and then broken as part of a session-based transaction. All events within the session are auditable with added verification of the destination user being identified and logged. CRC (Cyclic Redundancy Check) methodology is employed to ensure data integrity. Any interruption to the session either physical (i.e. network failure) or user-initiated (i.e. media ejection) causes the session to be 'torn down' without the data being physically written out ensuring complete control of the transfer.

StoS transfer provides an auditable mechanism for transferring files at different classifications ranging from RESTRICTED to TOP SECRET.

PIEV is a highly secure data repository, which provides users with the ability to **Print, Import, Export** or **View MS Office** files, and many other file formats, whilst maintaining a very high level of auditable security. The implementation allows sharing of highly classified documents over a geographically separated network and is fully scalable. The remote systems, being implemented utilising diskless workstations, are unclassified when not in use.

The ability to disseminate Top Secret information efficiently, whilst retaining document control greatly improves the cost and time factors of handling such information.

The system allows import and export of documents using removable media. A backup, restore and archive function is provided. Printing is audited to single page granularity.

Users can export a document to another system, add comments, review or amend and then re-import the document as a separate instance of the original file under tight configuration control. Additions or amendments to the original file are stored using a time-stamp to allow historical actions to be viewed, similar to a version control application.

Security on this system is extremely high, using role-based group access and tightly locked down facilities.

Both PIEV and StoS are configured to allow the generation of reports based on complete inter-site and user interaction from authentication to session termination.

MASS is an independent UK Systems House providing a full Information Systems portfolio with specialist skills in:

- **Secure Systems**
- **Information Systems Deployment**
- **Database Technologies**
- **Managed Services**

MASS (Head Office)
Grove House
Rampley Lane
Little Paxton St Neots
Cambridgeshire PE19 6EL
United Kingdom

Tel: +44 (0)1480 222600
Fax: +44 (0)1480 407366

MASS (Lincoln Office)
1 Alumina Court
Tritton Road
Lincoln
Lincolnshire LN6 7QY
United Kingdom

Tel: +44 (0)1522 502050
Fax: +44 (0)1522 690250

E-mail: systems@mass.co.uk
Web Site: www.mass.co.uk

A Cohort plc Company



HARDWARE

SONIC is a thin client implementation, using a desktop terminal, running Windows XP embedded. Each client is configured with a floppy disk drive, a CD writer and a printer. Access to any provided device is constrained by the role-based security definitions. The client PC is 'hardened' to ensure that user functionality and any interaction with the operating system is completely restricted and controlled.

A secure terminal server running Windows Terminal Services and Citrix Metaframe XPs provides the published software to the client desktop.

An authentication server running Windows and employing Active Directory provides secure authentication using role-based group access. Mirrored drives are used for increased reliability.

SOFTWARE

The PIEV & StoS-software is hosted on the terminal server, along with its database. All the information (including the documents) is stored within the database and all access is logged and controlled.

HP DataProtector is used to provide the enhanced backup and restore functionality, and Sophos anti-virus software is used to sweep file imports. The Windows implementation provides CESG approved password and authentication security and a single version of MS Office allows viewing of MS Office documents.

SECURITY

The enhanced security of the system is achieved by:

- Use of a stateless thin client. The operating system is stored using "disk on chip" technology. All data is stored server side.
- Client memory is implemented in RAM disk ensuring no permanent storage in the system other than the database. The RAM disk is flushed on completion of a transaction or if interrupted.
- USB ports are locked down on an individual basis. Any device not recognised (or allowed) will be automatically locked out and all transactions terminated on the current client session. A security event is also written to the audit logs.
- Standard group policies are used to secure client and server desktops, preventing any interaction with the operating system.
- Security event reports can be tailored to suit individual requirements or environments.
- Unused ports on routers will be disabled and IP, MAC address and port location is used to verify hardware.
- Each page of a print job is treated as a separate job. Any interruption to the print facility will result in the job being stopped and a security event logged. The audit function will provide details of printed pages, file size, user, etc.
- The ability to generate reports based on Site/User interaction that can be reconciled against document registers or user activity.
- The physical system is subject to periodic CESG Health Checks to ensure security conformity and compliance.

