



TCS SecureOffice™

Trusted Computer Solutions, Inc.
13873 Park Center Drive, Suite 225
Herndon, VA 20171 USA
+1.703.318.7134 (Phone)
+1.703.318.5041 (Fax)
www.tcs-sec.com

White Paper



TCS SecureOffice™

Overview

TCS SecureOffice™ provides simultaneous secure access to both Microsoft Windows™ applications and traditional Sun Microsystems Solaris™ mission-critical applications running at different sensitivity levels...all from a single desktop. The SecureOffice capability is available in two different architectures...the traditional “workstation” (i.e., “fat client”) architecture and the newer “appliance” (i.e., “ultra thin client”) architecture. Information assurance and a “secure information sharing” capability is provided by the **TCS System Foundation™** and other TCS trusted software applications operating in conjunction with the Sun Microsystems Trusted Solaris™ operating environment. See Figure 1, “**TCS SecureOffice**”, and Figure 2, “**TCS SecureOffice Thin Client**”, for specific sample architecture diagrams.

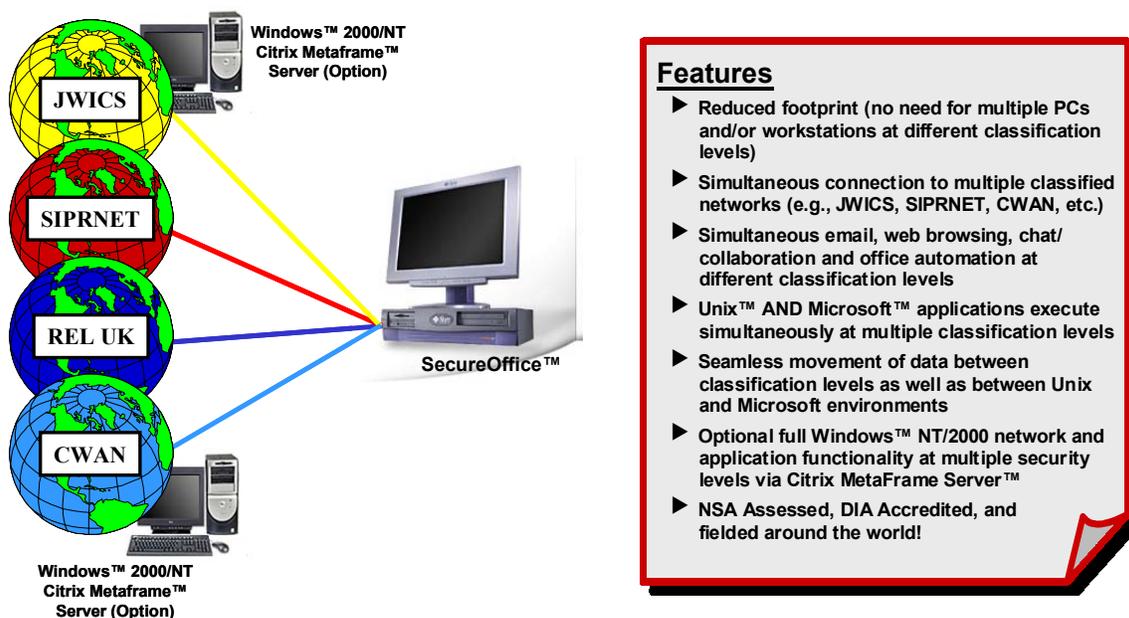


Figure 1 - TCS SecureOffice™

SecureOffice allows users to retrieve, process, and disseminate information across multiple networks operating at different security classifications and sensitivity levels. The SecureOffice solution provides a number of popular office

automation and administrative applications. The system provides a secure Windows 95-like capability as part of the standard configuration and allows for an optional Windows 2000/NT environment that is fully application and network capable via Citrix MetaFrame™ (See Figure 3 “Windows Environment Via Citrix MetaFrame” for a depiction the Windows environment). Information access and dissemination is achieved using Netscape Navigator™ for web browsing and Netscape Messenger™ for e-mail in the Solaris environment and Microsoft Internet Explorer™ for web browsing and Microsoft Outlook™ for e-mail in the Windows environment.

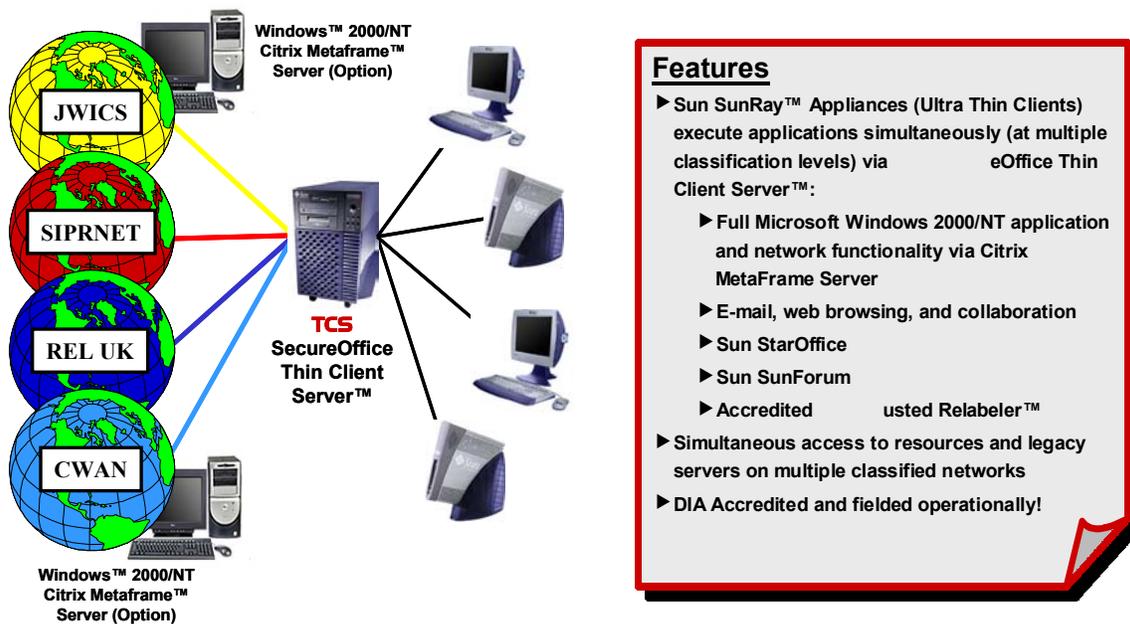


Figure 2 - TCS SecureOffice Thin Client™

The SecureOffice value proposition includes a reduced desktop footprint (e.g., no need for multiple PCs and/or workstations operating at different security classification levels), simultaneous connection to multiple classified networks, simultaneous e-mail, web browsing, chat/collaboration, and office automation at different classification levels, full Microsoft Windows NT/2000 application and network functionality, simultaneous execution of Microsoft and Sun Microsystems applications at multiple classification levels, and seamless movement of data between networks.

Additionally, in the appliance (i.e., thin client) architecture, SecureOffice Thin Client offers hot desk session mobility and increased desktop security, while eliminating desktop maintenance or administration, and desktop software

upgrades, This results in a higher level of desktop information assurance, reduced total cost of ownership, and individual user's increased productivity. *Bottom line: Lower cost...increased security.*

Hot desk session mobility allows users to always have instant access to their active session. Simply pull their access card from the card reader and walk away. The system saves the user's session for the next time they walk up to the device and plug in their access card to that or any other device. Depending upon site security policy, a user password can be required to be used in conjunction with the access card.

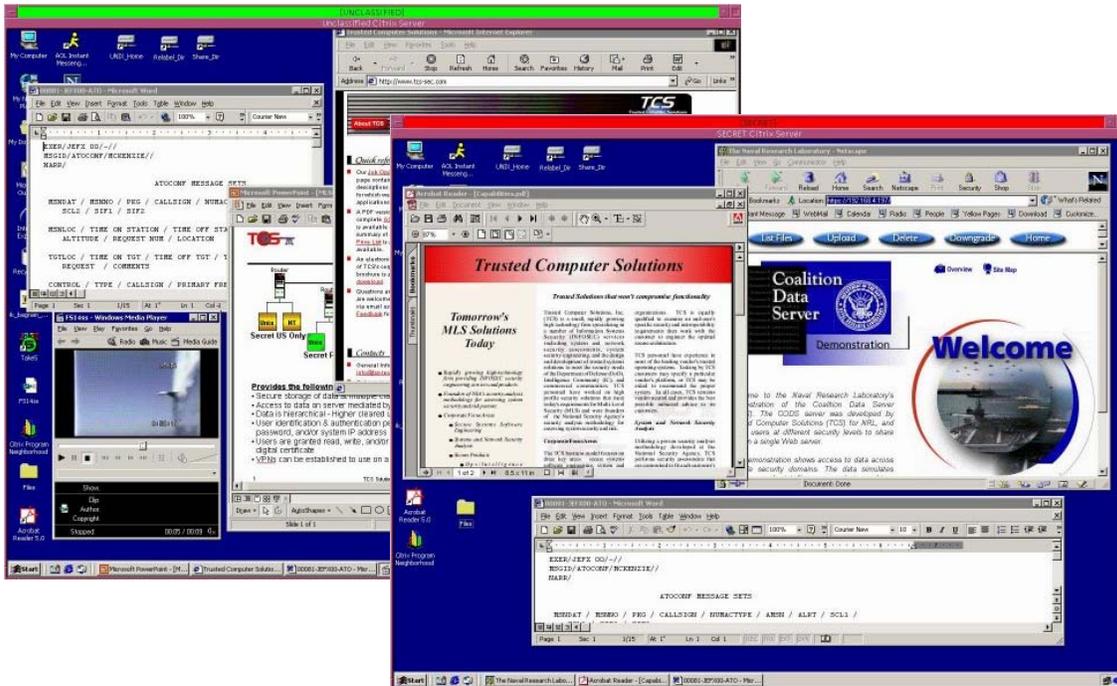


Figure 3 - Windows Environment Via Citrix MetaFrame™

Features

SecureOffice has the ability to operate at and connect to a number of different classified networks or domains simultaneously. For example, the system can connect to the Top Secret Joint Worldwide Intelligence Community System (JWICS), the Secret IP Router Network (SIPRNET), and a Secret Coalition Wide Area Network (CWAN) simultaneously, enabling access to Intelligence Community, Command & Control (i.e., Global Command and Control System

(GCCS)), and Coalition resources from the same desktop. The system could alternatively be connected to SIPRNET and the uNclassified IP Router Network (NIPRNET) simultaneously allowing access to mission-critical resources on SIPRNET while securely accessing information on the Internet. The total number of supported network connections at different security levels is limited only by the hardware (many hardware platforms support up to 13 physical network interfaces). The total number of security levels that can be processed internally (not associated with a physical network) is practically unlimited.

SecureOffice provides a number of security features that help ensure a safe and reliable mechanism for transferring data from one network to another. In conjunction with the Mandatory Access Controls (MAC), role based administration, use of least privilege, and removal of the super-user root account features indigenous to Trusted Solaris, the **TCS** Trusted Relabeler™ is the trusted software application which permits the bi-directional transfer of information from one network to another. After ensuring that the user is authorized to transfer the information, the Trusted Relabeler performs a virus scan, a dirty word check, and requires the user to view the file prior to transfer.

SecureOffice is built upon the **TCS**secure:System Foundation™ software which provides a number of security and functionality capabilities. System Foundation includes **TCS**secure:eFilter™, a sophisticated firewall-like kernel level IP packet filtering capability, which is configured to allow access to SecureOffice by only designated systems on each network. The IP filter will disallow communication with all systems and networks except for those that have been specifically authorized.

System Foundation also includes **TCS**secure:AdminSuite™, which provides a simple-to-use set of tools for administering and configuring the system. With AdminSuite the administrator can easily reconfigure the system, knowing that the GUI tools will automatically and properly modify all affected security tables and databases. This saves the administrator from having to memorize all the security tables and their data formats in order to make simple system configuration adjustments.

Architecture

As shown in Figures 1 and 2, the SecureOffice capability is available in the traditional “workstation” (i.e., “fat client”) architecture and in the newer “appliance” (i.e., “ultra thin client”) architecture. Windows 2000/NT environments are provided by Citrix Metaframe Servers on each network for which the Windows environment is required. The total number of supported network connections at

different security levels is limited only by the availability of the hardware network interfaces. SecureOffice runs on any Trusted Solaris-supported workstation platform. Figure 4, “Real-World SecureOffice™ Architecture Supporting Combatant Commander”, is an accredited and operational sample architecture.

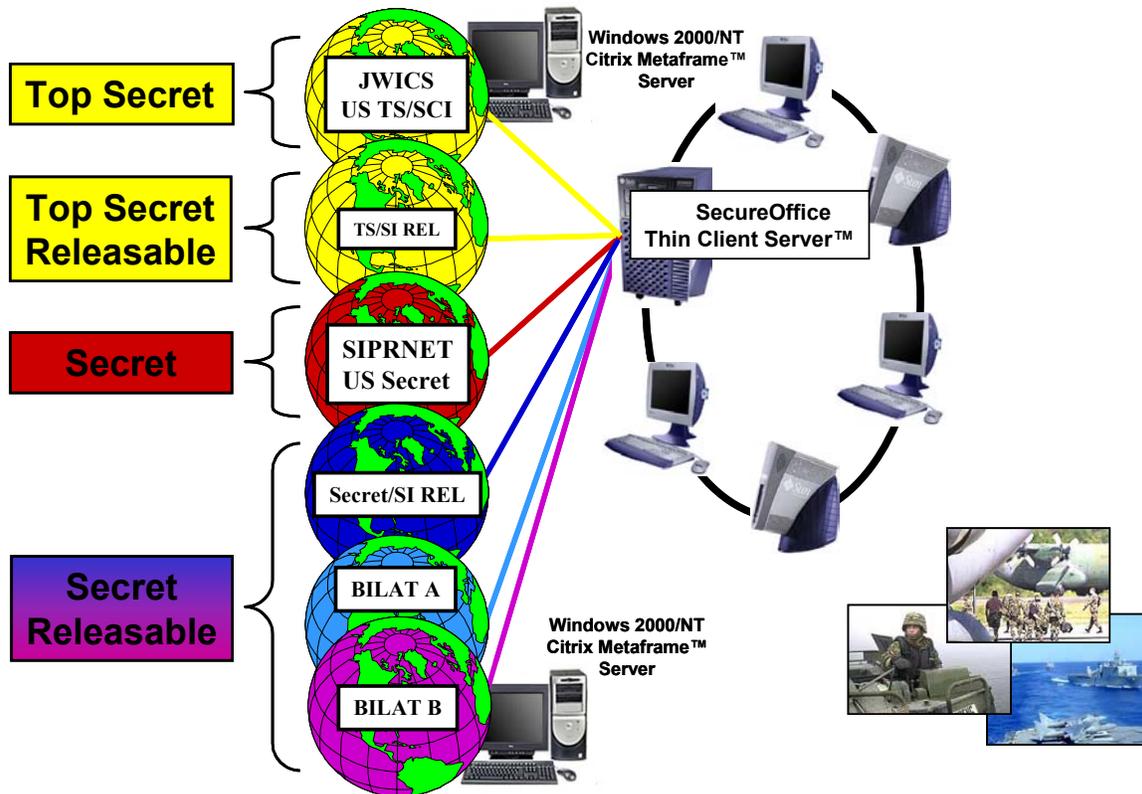


Figure 4 – “Real-World SecureOffice™ Architecture Supporting Combatant Commander”

Security Accreditation

SecureOffice has undergone extensive and rigorous security certification and accreditation testing by the National Security Agency (NSA) and the Defense Intelligence Agency (DIA) and has been accredited by DIA for simultaneous connection to Top Secret SCI (i.e., JWICS), Top Secret SCI Releasable, Secret level networks (i.e., SIPRNET), Secret Releasable networks (i.e., SECRET REL), and Secret Bilateral (SECRET BI-LAT) networks. Other network combinations can be accredited.

Trusted Solaris™ Operating Environment

The Sun Microsystems Trusted Solaris Operating Environment is designed to meet the security needs of users from the desktop to the data center. Trusted Solaris 8 software extends the capabilities of the Solaris Operating Environment to provide superior safeguards against internal and external threats far beyond the protection commonly found in standard operating systems. Trusted Solaris software includes comprehensive firewall protection along with other access control methods. Additionally, to help stop security violations by authorized users, it enables administrators to implement a security policy that controls the access and handling of information, including system administration, operation, and monitoring tools.



SecureOffice is built upon the Trusted Solaris operating environment, which has been evaluated under a number of international evaluation schemes such as the Common Criteria (CC). Trusted Solaris received an Evaluation Assurance Level 4 (EAL4) certification under CC. This certification was measured against the Label Security Protection Profile (LSPP), Controlled Access Protection Profile (CAPP), and the Role-Based Access Control Protection Profile (RBACPP). These certifications are the highest of any commercially available system in its class, ensuring that **TCS** customers have the most advanced secure operating environment available today.

Trusted Solaris supports a wide variety of hardware platforms from Sun Microsystems from low-end workstations and servers to 100+ CPU high-end platforms. In addition, Trusted Solaris, a commercial off-the-shelf product, is based on the Solaris operating system, Common Desktop Environment (CDE), and Solstice™ AdminSuite™. Trusted Solaris and SecureOffice are fully Y2K compliant.

Security features of Trusted Solaris include:

- Labeling Information
- Mandatory (MAC) and Discretionary Access Control (DAC)
- Privileges / Authorizations
- Administrative Roles/Solstice AdminSuite
- Trusted CDE Window System
- Trusted Networking
- Trusted Printing
- Execution Profiles
- Scalable Security

Additional Information

Trusted Computer Solutions, Inc.
13873 Park Center Road, Suite 225
Herndon, VA 20171 USA
+1.703.318.7134 (Phone)
+1.703.318.5041 (Fax)
info@tcs-sec.com

Secure Information Sharing...

...Means Solving These Problems

...With Enabling Technologies

...Delivered in TCS Solutions

