IT03.09

Document Access Servelet
(DAS)

TECHNICAL INTEROPERABILITY RESULTS

TECHNICAL ASSESSMENT SUMMARY | INTEROPERABILITY | INPUT/OUTPUT | System CONFIGURATION REQUIREMENTS | DATAFLOW | RECOMMENDATIONS | HOME

IT03.09 ASSESSMENT COMPONENTS

WARFIGHTER | TECHNICAL INTEROPERABILITY | INFORMATION ASSURANCE | SEIWG
(If a text entry is not linked, there is no assessment in that category for this trial)

TECHNICAL ASSESSMENT SUMMARY

The Joint Interoperability Test Command (JITC) technical assessment focused on the ability of each selected trial to satisfy their interoperability objectives by providing data to and receiving data from external interfaces, as well as using standard communications ports, protocols, and data formats. The JITC assessed the Document Access Servelet (DAS), IT03.09, during the two-week CWID 2006 execution at the following locations:

U.S. SITES

- ESC, Hanscom AFB, MA
- USEUCOM, Stuttgart, Germany
- USNORTHCOM, Colorado Springs, CO
- NSWC, Dahlgren, VA
- SPAWAR, San Diego, CA

COALITION SITES

- Canada CFEC, Ontario
- New Zealand JFHQ, Wellington

BACK TO TOP

INTEROPERABILITY

During CWID 2006, the DAS demonstrated secure document and file access control provided by a web-based administrative interface for system configuration, key management, and Community of Interest (COI) maintenance tasks. The DAS administrators granted and denied users access using centralized COI membership rosters. Collaboration and dissemination of file-based information was secured and controlled by the addition and

subtraction of COI and COI members. When documents were encrypted for more than one COI, a user only needed to be a member of one of those COI to decrypt that document. The strength of this system is that encrypted data does not need to be re-encrypted when COI membership changes.

When users attempted to decrypt an encrypted document for a particular COI, their SecretAgent client automatically established a Transport Layer Security (TLS)-secured session (machine to machine) with the DAS server. The DAS then accepted or rejected the decryption request from the client. When the DAS determined that a user was a current COI member, it processed the request and returned a document decryption key to the client; otherwise, the DAS denied the user request.

SecretAgent encrypts by using a random symmetric key wrapped in one or more COI certificates. During decryption, a symmetric key wrapped in a COI certificate is sent to the DAS server where it is unwrapped (for a current COI member) using the COI's private key, rewrapped with the member certificate and returned to client. Decryption then proceeds with the member's private key that unwraps the symmetric key.

All sites reported that the DAS worked successfully.

BACK TO TOP

INPUT DATA

Data Product Type	Data Product Format	Data Transfer Method	Protocols and Ports Used	How the data will be used	Data Source	Simulated	Observed
Text	Text	N/A	N/A	Trial uses LDAP and COI to disseminate data with X.509 certificates.	local/Warfighters	No	Yes
Text	SecretAgent Encrypted Microsoft Office Word	TCP/IP	HTTPS Port 443	Cypher text (.sa5) retrieved from the file server by the Warfighters	portal/ Warfighters	No	Yes
Text	SecretAgent Encrypted Microsoft Office Word	N/A	N/A	The Warfighters attempt to decrypt the cypher text, now held locally	local/Warfighters	No	Yes
Text	Text	TCP/IP	HTTPS Port 443	The local machine communicates the decryption request to the DAS server	local/das server	No	Yes
Text	Microsoft Office Word	N/A	N/A	The Warfighters encrypt this plain text using SA	local/Warfighters	No	Yes

OUTPUT DATA

Data Product Type	Data Product Format	Data Transfer Method	Protocols and Ports Used	How the data will be used	Data Recipient	Simulated	Observed
Text	Text	TCP/IP	HTTPS Port 443	DAS will (or will not in some cases) grant access to the document to be decrypted	das server/local	No	Yes
Text	Microsoft Office Word	N/A	N/A	SA decrypts the cypher text file (.sa5) resulting in this plain text file	local/Warfighters	No	Yes
Alert	Text	N/A	N/A	In the event the user is not authorized to decrypt the file an error message is received	das server/local	No	Yes
Text	SecretAgent Encrypted Microsoft Office Word	N/A	N/A	SA encrypts the plain text file resulting in this cypher text file (.sa5)	local/Warfighters	No	Yes
Text	SecretAgent Encrypted Microsoft Office Word	TCP/IP	HTTPS Port 443	This cypher text file (. sa5) loaded to the file server	local/portal	No	Yes

BACK TO TOP

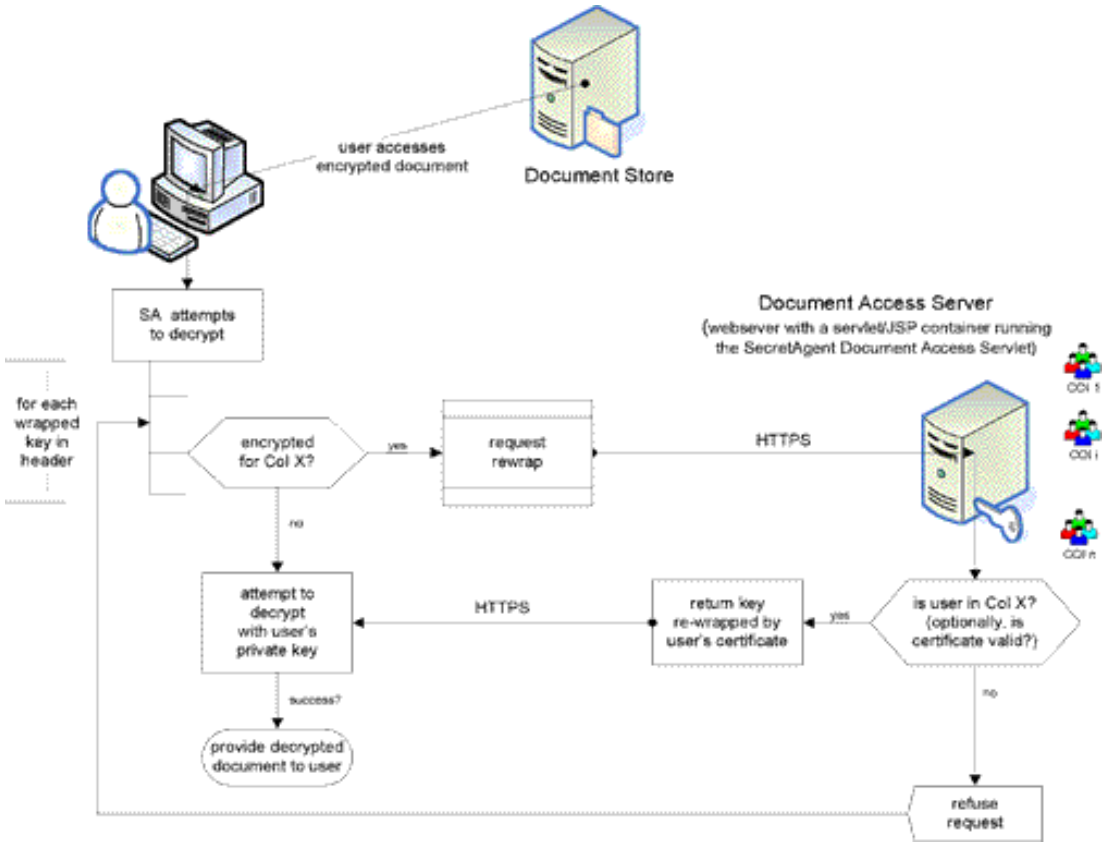
System CONFIGURATION REQUIREMENTS

Component Name	DAS Server 1 UnClass Network and 1 CTF Network					
Hardware Build:						
Platform Make and Model	**Operating System**	**Processor**	**RAM**	**Disk Storage**	**Network Interface**	**Peripheral Devices**
Sun Sunfire T1000	Sun Solaris 10	UltraSPARC T1	1 GB	80 GB	10/100/1000	N/A
Software Build:						
Software Application	**Is Web Client?**	**Require ActiveX?**	**Disk Space**	**RAM Required**	**Data Standards and Version**	
Secret Agent DAS	No	No	2 GB	512 MB	Version 1.4	
Secret Agent	No	No	20 MB	64 MB	Version 5.9.3	
Java Run-time Environment	No	No	371 MB	48 MB	Version 1.4	

Database Authenticator Manager	No	No	10 MB	64 MB	Version 1.0	
Individual X.509 Certificate and Private Key for each Warfighters/operator	No	No	2KB	2KB		
Component Name	PC provided by site					
Hardware Build:						
Platform Make and Model	**Operating System**	**Processor**	**RAM**	**Disk Storage**	**Network Interface**	**Peripheral Devices**
PC	Windows 2000 or higher	As provided by site	As provided by site	As provided by site	As provided by site	N/A
Software Build:						
Software Application	**Is Web Client?**	**Require ActiveX?**	**Disk Space**	**RAM Required**	**Data Standards and Version**	
Individual X.509 Certificate and Private Key for each	No	No	2 KB	2 KB	N/A	
Secret Agent 5.9.3	No	No	20 MB	64 MB	Secret Agent 5.9.3	
Database Authenticator Manager	No	No	10 MB	64 MB	1.0	
Java Run-time Environment	No	No	371 MB	48 MB	1.4	

BACK TO TOP

DATA FLOW



BACK TO TOP

CONCLUSIONS AND RECOMMENDATIONS

The DAS successfully secured and shared documents and files among established COI. Recommend the government sponsor and/or vendor of the DAS pursue Interoperability Certification/Assessment in accordance with Chairman, Joint Chiefs of Staff Instruction 6212.01D, “Interoperability and Supportability of Information Technology and National Security Systems,” 8 March 2006.

BACK TO TOP

INTEROPERABILITY RESULTS ON THIS PAGE

TECHNICAL ASSESSMENT SUMMARY | INTEROPERABILITY | INPUT/OUTPUT | System CONFIGURATION REQUIREMENTS | DATAFLOW | RECOMMENDATIONS

IT03.09 ASSESSMENT COMPONENTS

WARFIGHTER | TECHNICAL INTEROPERABILITY | INFORMATION ASSURANCE | SEIWG

(If a text entry is not linked, there is no assessment in that category for this trial)

GENERAL DIRECTORIES

FINAL REPORT DIRECTORY | ASSESSMENT BRIEFS BOOKLET | HOME

COALITION WARRIOR INTEROPERABILITY DEMONSTRATION 2006 FINAL REPORT