A Trident Systems White Paper

10201 Fairfax Boulevard
Fairfax, VA 22030
703.273.1012
www.tridsys.com

# Collaboration without Boundaries: Cross-Domain Solutions for Network-Centric Operations

*Scott Thomas*
*scott@tridsys.com*

Version 1.1
July 2009

## Contents

**Collaboration,**
***\kə-ˌla-bə-ˈrā-shən***

*The act of working together with others to achieve a common goal.*

## Introduction

In the era of “network centric” operations, the tension between protecting and sharing information has never been greater. Military operations rely on multinational coalitions, while effective disaster response depends on coordination among a dynamic agency roster which can include DoD, as well as many other Federal, state & local agencies. In particular, software tools which allow people in ad hoc groups to collaborate have proven immensely valuable.

Yet despite the need to share information quickly and completely, all these organizations have different security policies; all have network domains whose integrity depends on well-protected boundaries; and no single agency is able to ignore either its own, or others’, security policies in the name of mission accomplishment.

This white paper discusses how to take advantage of collaboration technologies to provide mission-critical, person-to-person communications while enforcing these security policies. When implemented correctly, such cross-domain collaboration takes advantage of new developments in both network-based collaboration and cross-domain security technologies, and provides an environment which accomplishes two previously conflicting goals: empowering time-critical cooperation and enforcing security.

## Cross Domain Solutions

### *A Brief History*

According to the Committee on National Security Systems – the US Government’s policy-making group for information assurance – a Cross-Domain Solution is “any information assurance solution that provides the ability to access or transfer information between two or more security domains.”[1] (A security domain is defined as a system or group of systems operating under a common security policy.) Cross-Domain Solutions (or CDS) fall into two main categories: access solutions, which allow users to see information resources in multiple domains via a single workstation, and transfer solutions, which enable the movement of information from one domain to

[1] United States. Committee on National Security Systems.*CNSS Instruction No. 4009, National Information Assurance (IA) Glossary*. Ft Meade, MD: CNSS Secretariat, 2006.

another.[3] While access solutions provide useful services (such as the use of a software application which exists in another domain), cross-domain collaboration depends on the ability to transfer information between people on different domains.

| UCDMO Baseline List of<br>Available Transfer Solutions |
|---|
| Data Sync Guard (DSG) Ver. 2.1 |
| Defense Information Infrastructure Guard (DII DMS) v3.1.1 |
| eXMeritus HardwareWall (HWW) v2.9.2 |
| Information Support Server Environment (ISSE) 3.6.x |
| Radiant Mercury 4.0.5 P3 and 4.5.2 |
| Secure Messaging and Routing Terminal Next Generation (SMART.neXt) 3.0 |
| Trusted Gateway System (TGS) 2.1 P1 |

**Table 1 The UCDMO Baseline lists all officially-approved transfer solutions**[2]

### *CDS 1.0: Connecting Machines*

The first generation of cross-domain transfer solutions (here named "CDS 1.0") has been fielded for more than ten years. CDS 1.0 systems are focused on transferring either files or heavily-formatted messages between software applications; examples include the highly-successful Radiant Mercury and ISSE Guard, and are often called "Guard solutions" since they automatically enforce policies on information crossing between domains.

The more structured the message, the better these CDS 1.0 solutions enforce transfer policies. Highly-structured messages, due to their limited range of allowable data, are much easier to automatically approve or deny; for instance, if a contact-report message includes a field for "target heading", any value outside the range of [0 – 360°] is clearly wrong, and indicates a problem with that message.

While CDS 1.0 solutions clearly play an important role in allowing software applications (such as Common Operating Picture tools, or intelligence databases) to exchange data while respecting security policies, they have—until recently—been of extremely limited utility in allowing humans to interact across domains. The reason is simple: more loosely-formatted data, so common in interpersonal collaboration, has been difficult to prove "secure" using automated rule sets.

### *The Rise of Collaboration Tools*

Collaboration tools—that is, tools which allow people to interact on digital networks—have been in use since the

[2] United States. Unified Cross Domain Management Office. "Re-Use Baseline List V3.0 (Sanitized)". Adelphi, MD: http://www.ucdmo.gov. Retrieved June 2009.

[3] The Unified Cross Domain Management Office (UCDMO) defines a third type called a Multiple Level Solution, a CDS which stores data in multiple domains, and allows users access at an appropriate security level.

Figure 1 International Security Assistance Force (ISAF) Command Center, June 2009. Coalition operations are depending more and more on collaboration tools as essential elements of mission support.

1960s.[4] However, these capabilities (such as text chat, whiteboarding, and instant messaging) have proven themselves valuable in military and disaster-relief contexts which go well beyond the "social" dimension typically associated with online collaboration tools.

During recent military operations – including Operation Iraqi Freedom (OIF), Operation Enduring Freedom (OEF), and others – text chat has become a default mechanism for military, intelligence, and support personnel to interact on US Government networks.

In one example, the US Navy's Fifth Fleet began OEF with one chat server averaging 300 concurrent chat users at any given time. Due to rapidly increasing load, Fifth Fleet brought a second server online; this second server supported an additional 500 concurrent users. With the commencement of OIF, chat use increased even further, resulting in the installation of two more chat servers, bringing the total to four servers supporting over 2,500 concurrent users.[5]

While such collaboration solutions offer the capability to communicate "synchronously" (that is, in real time) with other users, they carry several risks which make their rapid proliferation problematic, even on single-domain networks. First, most online collaboration by US forces is based on US-only classified networks, such as the Secure Internet Protocol Routed Network (SIPRNet). Coalition users thus find it impossible to coordinate with US forces using chat.

Even in situations where a dedicated Coalition chat solution is established, US personnel often view such "extra" collaboration tools as distracting or inefficient, due to the need to collaborate twice: once on the US-only network, and a second time on the Coalition network. This problem is compounded when involved personnel are spread across multiple networks (such as SIPRNet, the Joint Worldwide Intelligence Communications System or JWICS, and Coalition networks).

[4] Van Vleck, Tom. " The History of Electronic Mail." Multics (Multiplexed Information and Computing Service). 2001. http://www.multicians.org/thvv/mail-history.html. Retrieved June 2009.

[5] Eovito, Capt Bryan A, USMC. "The Impact of Synchronous Text-Based Chat on Military Command and Control." Defense Technical Information Center. 2005. http://www.dtic.mil. Retrieved June 2009.

**Figure 2 US Marines introduce communications software to members of the 7th Iraqi Army Division, November 2008. Collaboration tools are becoming the norm in Coalition scenarios, despite persistent concerns about security.**

Also, the explosion in use of chat tools on Defense and Coalition networks has introduced a substantial risk of security breaches, even in single-domain solutions. For instance, the mIRC chat tool, which is widely deployed on several DoD networks, includes several well-documented security issues which result from its dependence on the Internet Relay Chat (IRC) architecture. Weak user authentication is one example, which can result in a malicious user logging into with false credentials.

Another mIRC security issue is its user-editable chat logs – this could lead to "creative editing" of what was actually said during the chat session. Combining these two security holes could result in a malicious user, with a false identity, having access to protected information—and then covering his tracks by deleting the chat log. In a physically-secure environment (such as inside a locked Tactical Operations Center, or within a badge-only security area), these mIRC security issues are less threatening. However, in a Coalition or disaster-relief context, even single-domain use introduces very real security risks; and the risk increases even more in a cross-domain situation.

## *CDS 2.0: Connecting People*

To take advantage of the very real benefits of collaboration technology, these security issues must be resolved with a level of confidence consistent with existing information assurance rules. Thus, the dramatic breakthrough in military and disaster-relief mission support is the advent of real-time collaboration across security domains (here named "CDS 2.0"). CDS 2.0 offers to humans what CDS 1.0 offered to software applications: a secure and timely way to interact with people on different security domains.

However, to be relevant, any CDS 2.0 solution must answer three critical questions:

1. Is it <u>useful</u>?
2. Is it <u>secure</u>?
3. Is it <u>supportable</u>?

To be <u>useful</u>, CDS 2.0 must provide a way for a person on any network to find and interact with whoever has the information or expertise necessary to help accomplish the mission. Information sharing must be quick, flexible and ad hoc – multiple simultaneous users, on several different networks, possibly speaking several different languages. The collaboration may need to include not just text, but also images and files of supporting information.

To be secure, CDS 2.0 must provide the mechanisms necessary to ensure that the solution reliably enforces DoD, Intelligence Community, and other Federal (and Coalition) information assurance policies. While the details of these policies are not publicly releasable, they include the areas at left.

- ✓ **Confidentiality**: Assurance that information is not disclosed to unauthorized individuals, processes, or devices.
- ✓ **Integrity**: Assured protection against unauthorized modification or destruction of information.
- ✓ **Availability**: Timely, reliable access to data and information services for authorized users.[6]

The ability to support cross-domain collaboration carries additional security concerns related to the fact that the users are responsible, during the chat session, for marking each message. This means that a secure CDS 2.0 solution must provide the ability to control who can receive messages at every combination of classification and dissemination control, while ensuring that incorrectly-marked messages can be identified as soon as possible. The client chat tool must be aware of these security restrictions, providing all relevant classification markings in the user interface, as well as embedded in the chat message itself. Any cross-domain collaboration solution must also involve robust, user-proof logging of every collaboration; this enables later review for evidence of unauthorized disclosure (e.g., inappropriately-classified information).

To be supportable, CDS 2.0 must be interoperable with the significant investments made in CDS 1.0 transfer solutions such as ISSE Guard, Radiant Mercury, Data Sync Guard, and others. These existing, approved transfer solutions represent a robust foundation for new cross-domain capabilities; any cross-domain collaboration solution which cannot interoperate with them would require its own testing & certification, an expensive and unnecessary duplication of proven capabilities.

In addition, any CDS 2.0 solution must be compatible with emerging Federal collaboration standards. Any non-standards-based "solution" would represent a significant user learning curve, the duplication of existing NCES-compatible tools in use, as well as a much more limited user base to support it. A plethora of Instant Messaging (IM) clients exist in the marketplace today - including AIM, Yahoo, MSN, Sametime, IWS, Trillian, and a handful of lesser known tools - but none of these support the necessary security requirements.

[6] *CNSS Instruction No. 4009, National Information Assurance (IA) Glossary.*

Moreover, most of these IM systems are proprietary in nature and are not interoperable.

As one example, the Defense Information Systems Agency (DISA) Net-Centric Enterprise Services (NCES) program, which is charged with defining Defense-wide standards for network-centric systems, has selected the eXtensible Messaging and Presence Protocol (XMPP)—also known as "Jabber"—as its standard for text-based chat. This selection was made over its primary competitor, SIMPLE, due to several factors. First, XMPP requires much less bandwidth–95% less for the same rate of chat.[7] Second, XMPP is based on the eXtensible Markup Language (XML), resulting in an extremely flexible implementation scheme which easily supports extensions necessary to accommodate security markings.

Figure 3 San Diego Police officer uses collaboration tools during CWID 2009. While interagency "cross-domain" information sharing was a major CWID emphasis, only one trial (the CDCIE system) actually had a cross-domain certification pedigree.

## CDS 2.0 in Action

To illustrate the benefits of CDS 2.0, consider some unclassified examples from the 2009 Coalition Warfighter Interoperability Demonstration (CWID). This Joint Staff-directed series of operational scenarios involved more than 30 agencies from eight countries, and was conducted at over a dozen sites worldwide. Cross-Domain collaboration formed a key part of the exercise, as there were multiple security domains including:

1. HS/HD: Unclassified network for Homeland Defense and Homeland Security,
2. CTF-Low: Coalition-releasable classified network, and
3. CTF-High: US-only classified network.

Throughout these scenarios, the United States Joint Forces Command (JFCOM) deployed the Cross-Domain Collaborative Information Environment (CDCIE), an NSA-certified cross-domain collaboration solution based on DoD NCES standards.

CDCIE enables collaboration in the form of text chat and whiteboarding (both with language translation), and standards-based web services among DoD and non-DoD networks (including coalition partners, other government

[7] Scherer, William F. "Collaboration in Bandwidth Constrained Environments." Proceedings of the Systems & Software Technology Conference, Salt Lake City, UT: May 2008.

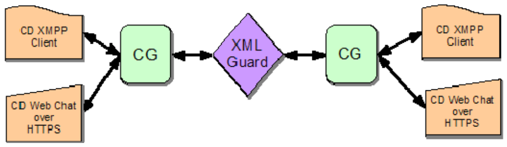


**Figure 4 CDCIE high-level architecture. Ensuring standards adherence results in complete flexibility; Several XML guards are supported by CG, including DSG, ISSE Guard, Radiant Mercury, and commercial XML firewalls. Clients could be one of many XMPP-compliant chat applications which support cross-domain extensions for classification labeling and user certificates.**

> *"Without [CDCIE], there's no way we could have fought the simulated wildfires as quickly as we did. At one point, I had ten different agencies represented in one chat room. If we'd had this [for the wildfires] in 2003, I bet coordination would've been a lot smoother."*
> *- CWID 2009 San Diego first responder*

agencies, and non-governmental organizations) operating at different classification levels.

The CDCIE system architecture, shown at left, consists of three parts:

1. A cross domain XML guard;
2. An XMPP-enabled collaboration server known as Collaboration Gateway (CG);
3. A collaboration client – this can be either a software application on the users' machines, or a web-based client provided by CG.

The CDCIE configuration for CWID included the Data Sync Guard as its XML guard, and three instances of the CG server, one for each security domain.

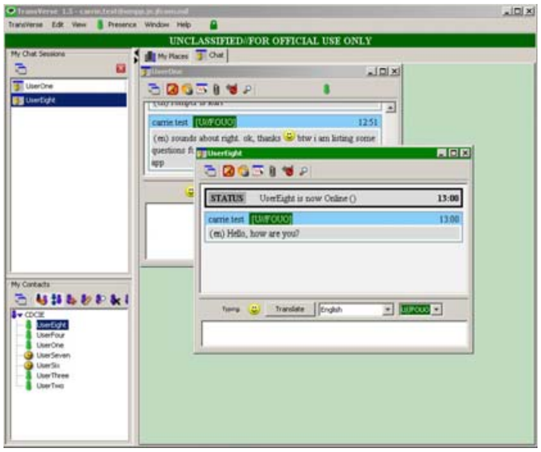
Users at multiple sites worldwide used CDCIE to collaborate on over 300 scenario events, in scenarios which ranged from coordinating multiple agencies' counterterrorism operations to disaster response. Using text chat and whiteboards, personnel from US and Coalition military forces were able to successfully communicate between classified and unclassified networks, enabling close, real-time coordination with law enforcement, emergency management, and other non-military organizations.

### *Collaboration Gateway Overview*

At the heart of CDCIE is Trident's Collaboration Gateway system, or CG. CG provides the mechanisms necessary to enable collaboration through any cross-domain guard capable of transferring XML traffic.

Collaboration requires more than just the transfer of text and whiteboarding messages. CG ensures that information such as user identity and presence, as well as important metadata regarding what information each user is allowed to see. To enforce the security policies necessary for cross-domain transfer, CG also verifies the integrity of all data passed to the cross-domain guard. When coupled with an XMPP-capable chat client, CG provides all the functionality necessary to make the cross-domain transfer both reliable and secure. Specific functions include:

1. Enforce User Security Policy:
    a. User authentication & authorization;



carrie test [U//FOUO] 12:51
(en) sounds about right. ok, thanks btw i am listing some questions f... app

STATUS UserEight is now Online () 13:00

carrie test [U//FOUO] 13:00
(en) Hello, how are you?

Figure 5  TransVerse cross-domain chat client.  With the ability to support both classification markings and multiple-language automated translation, TransVerse is an excellent example of standards-based cross-domain collaboration.

b. Which users are allowed to chat cross-domain;
c. Which users are allowed in which rooms;

2. Enforce Message Security Policy
   a. Checks classification labels in message – forwards or blocks accordingly;
   b. Checks message integrity;
   c. Checks digital signature for non-repudiation of message;
   d. Identity transformation of messages;
   e. Virus scan of messages.
3. Logging & Archive/ Search/Retrieval Service;
   a. All cross-domain messages logged & archived to local database;
   b. All administrative actions are logged to controlled log files
   c. New log files are created each day
   d. Log files cannot be accessed by collaboration users.

To help provide these security features, CG incorporates the XML Digital Signature and XML Encryption algorithms to provide strong authentication and authorization, as well as confidentiality and data integrity. Additionally, both CG and the DSG support the US Intelligence Community (IC) metadata standard for classification labeling of chat messages.

CG features a modular, plug-in architecture that supports any XMPP collaboration tools with the cross-domain extensions necessary to enforce security policies. These extensions include support for the Intelligence Community's metadata standard for classification labeling, and PKI user certificates.  Several cross-domain-aware XMPP clients are available today, including TransVerse, InfoWorkSpace (IWS), JChat, and WebTAS.  Transverse, developed by JFCOM, is freely available on the Internet.  IWS is the collaboration tool from Ezenia which has gained widespread acceptance in the Intelligence Community.  JChat is a Java-based client developed by NATO for use on their networks.  WebTAS is an analytical tool widely used in the DoD, and includes an embedded XMPP client.

CG enables cross-domain security for many collaboration functions which have become ubiquitous in the single-domain world.  As the CDS 2.0 world catches up, users can expect to see cross-domain versions of such functions, including Wikis and blogs, as well as other synchronous functions such as Voice over IP (VoIP) and streaming video. Based on the cross-domain awareness built into CG, these well-accepted collaboration functions will be available without the security boundaries which limit their full potential.

## Implementing Cross Domain Collaboration

Implementation of a cross-domain collaboration solution may sound daunting for the first-timer. However, the process is actually relatively straightforward, as it follows the path established by CDS 1.0 transfer solutions. In general, the following steps apply:[8]

### *Identify collaboration requirements*

A cross-domain collaboration solution begins with the people who need to collaborate. What are their needs? If a synchronous collaboration capability (such as text chat & whiteboarding) is required, are they looking for general-purpose use, or is there a real-time operational support requirement which may demand higher availability? Do your users need language translation? Are there existing tools (such as chat clients) which your users would like to continue to use? For asynchronous collaboration, do your users need the ability to build a wiki with multiple concurrent domains?

### *Identify which and how many domains need to be supported*

In order to provide the right level of information assurance, which domains must be cross-connected? For instance, many US military personnel use SIPRNet terminals for their day-to-day work, while Intelligence Community personnel may use JWICS. Various Coalition networks may also be involved, as may unclassified networks. Collaboration Gateway provides the means to cross-connect several domains at once; in addition, CG offers a means to connect multiple National domains (e.g., a US-only domain, a UK-only domain, etc.) through a "demilitarized zone" (DMZ) which allows each National domain to specify its own security policy.

***Feedback on cross-domain collaboration from exercise TRIDENT WARRIOR 2009:***

> *"There was good MOC to MOC coordination, mostly because of good use of [CDCIE] chat."*
>
> *-Portuguese Maritime Operations Center*

> *"[CDCIE] enabled seamless high side chat collaboration that simply does not exist in real world applications today. We hope that this capability will be available in a program of record down the road."*
>
> *- US Coast Guard Maritime Intelligence Fusion Center*

> *"CDCIE was better than real world because it allowed us to directly communicate and collaborate with partner nations in a real-time, non scheduled format (not VTC, etc.)."*
>
> *- US Fourth Fleet Maritime Operations Center*

[8] Note: this discussion is intended as a general overview, not as detailed, site-specific guidance. For further information which will help you determine how to implement a cross-domain solution for your organization, please consult with your relevant Cross Domain Solutions office, or contact Trident Systems.

Figure 6 French army personnel install network servers at a US base in Germany, 2008. Implementing cross-domain collaboration in even the most complex Coalition environments is straightforward, once functional and security needs are identified.

Additionally, the protection of higher-level classifications (such as Sensitive Compartmented Information) requires a different accreditation approach than Secret and below accreditation.

### *What other cross-domain requirements (and infrastructure) already exist?*

If an existing cross-domain transfer solution exists, then the addition of cross-domain collaboration could be as simple as a modification to the approval paperwork already in place. If there is no existing, approved CDS 1.0 transfer solution, then all cross-domain transfer requirements should be evaluated, as each existing transfer solution on the UCDMO baseline list offers different benefits based on the specific message types (other than collaboration) which need to be passed.

### *Develop installation, integration and training plan*

Whether a completely new installation, or an addition to an existing cross-domain transfer solution, a CDS 2.0 implementation plan must include the specifics of installation, integration with existing infrastructure, and training of all concerned users and administrators. For Collaboration Gateway, this plan can be based on previously-developed examples. In any case, early involvement of local security and information systems support personnel is critical to ensure a smooth transition to operations. Depending on the type & complexity of the cross-domain collaboration solution, a typical installation timeline can involve several months of waiting for the requisite approvals, so leave plenty of time for administrative reviews prior to your go-live date.

### *Install, integrate & train*

Working closely with onsite personnel, the next step (upon approval to connect to live networks) is to execute the plan. CDS 2.0 solutions, particularly those implemented without prior cross-domain transfer solutions in place, will likely require working closely with the solution vendor.

## Summary

Cross-domain solutions have been a part of National information assurance infrastructure for over a decade. Now that such CDS 1.0 solutions have become widely available, the next stage – connections between people, not software – is here.

Recent adopters of Collaboration Gateway include the following:[9]

- US Central Command
- International Security Assistance Force, Afghanistan
- Defense Information Systems Agency
- US Pacific Command
- National Reconnaissance Office
- UK Ministry of Defence
- Joint Interagency Task Force – South

Next steps in cross-domain collaboration include the ability to share information asynchronously, such as the Multi-Level Wiki environment currently under development, and the ability to communicate voice and video data across security domains.

Trident Systems, as the developer of CG and provider of the CDCIE, continues to work on breaking down barriers to multinational and multiagency collaboration. As military, homeland defense, and emergency response missions include an increasingly broad range of participants, cross-domain collaboration offers a simple but powerful way to break the tension between protecting and sharing information.

*About the author:*
Scott Thomas is the Cross-Domain Collaboration Solutions Product Line Manager for Trident Systems Incorporated. A 1984 graduate of Virginia Tech, Scott has led cross-domain solutions development at Trident Systems since 1997. Scott's previous accomplishments include development of Collaboration Gateway, the first true CDS 2.0 product, and the development and deployment of CDCIE. Scott lives and works in Raleigh, North Carolina.

[9] This list is current as of July 2009. To learn about updates to this list, please contact Trident Systems.