Australian Government
Department of Defence
Defence Science and
Technology Organisation

Coalition Theatre Logistics (CTL) Advanced Concept Technology Demonstration (ACTD) Architecture Overview

Egon Kuster

Command and Control Division
Information Science Laboratory

DSTO-TN-0607

Abstract

This paper gives a basic background to the Coalition Theatre Logistics (CTL) Advanced Concept Technology Demonstration (ACTD) program and details the proposed information sharing architecture to be used therein. Outlined are the main components of the CTL architecture and how each component interacts with the others. Although the architecture outlined in this document has been developed specifically for the logistics space, it could also be adapted for use within other distributed information sharing projects. The architecture addresses issues with releasing data into coalition environments, transferring and transforming data between national environments and providing coalition planning and information services.

Published by

DSTO Information Sciences Laboratory
PO Box 1500
Edinburgh South Australia 5111 Australia

Telephone: (08) 8259 5555
Fax: (08) 8259 6567

AR-013-302
December 2004

APPROVED FOR PUBLIC RELEASE

Coalition Theatre Logistics (CTL) Advanced Concept Technology Demonstration (ACTD) Architecture Overview

Executive Summary

Many issues arise when transferring data within coalition environments containing multiple nations. These include:

- Data formats
- Data release
- Legacy applications
- Coalition applications
- Coalition data requirements
- Application and data ownership

CTL ACTD aims to develop a prototype system that solves these issues. First a coalition environment needs to be created by using coalition networks. This creates two environments, the national space and the Coalition Information Environment (CIE). Between these two environments a security gateway and release mechanism stops unsolicited data moving from the national system into the coalition environment without being released by a foreign disclosure officer. The security gateway also stops any malicious entities on the coalition network from accessing the national network. Once the data is within the coalition space it must be managed and transferred to the required user. To facilitate data management and application access within the coalition space a number of components have been identified:

- National Release Point (NRP) (including national application server)
- Information Manager
- Coalition Application Server
- Coalition Data Schema
- Coalition Information Database (CID)
- File System
- Coalition Portal Server

Each NRP is owned and maintained by its deploying nation and provides a gateway between the national and coalition environments. Here data being imported to or exported from the national domain is transformed between the national and coalition data formats. The NRP also contains an application server allowing nations to provide applications and services that can be used in the coalition environment but that have not yet become an agreed coalition tool. Agreed coalition tools are stored and run from within the coalition application

server. Data within the CIE can be stored either within the national NRPs or within the CID. The Information Manager controls the distributed data within the CIE. All communication within the CIE is handled with platform-neutral Web Services. Applications within the CIE are accessed via the Coalition Portal Server using Internet-based technologies.

The architecture outlined in this document can support applications developed in either Microsoft's .NET or Java J2EE (Java 2 Enterprise Edition). As it uses open standards for communicating and developing applications the end solution is not tied to any particular vendor implementation, allowing for flexibility for the implementing nation.

Outlined in the latter part of this document are five case studies discussing how the architecture operates within different scenarios. These define the accepted scenarios to use this architecture for sharing and accessing of coalition data.

The architecture is very flexible in its application. It is postulated that it could be used for multiple purposes where coalitions require sharing of information, albeit that it was initially designed for logistics operations. CTL ACTD is implementing this architecture gradually over the next couple of years, producing a number of demonstrations of varying capability and completeness.

Acknowledgments

I would like to acknowledge Mr Richard Creps (Lockheed Martin Mission Systems, USA) for providing valuable input to the development of this report and concepts within.

Contents

Acronyms

.NET	Microsoft's "dot" NET platform
ACTD	Advanced Concept Technology Demonstrator
Air gap	A physical break in the network where information is transferred by physical transfer on removable media
AO	Area of Operations
C2	Command and Control
CIE	Coalition Information Environment
CID	Coalition Information Database
CTL	Coalition Theatre Logistics
DSTO	Defence Science and Technology Organisation
J2EE	Java 2 Enterprise Edition
JWID	Joint Warrior Interoperability Demonstration
LM	Lockheed Martin
MHE	Mechanised Handling Equipment
NRP	National Release Point
WebDAV	Web-based Distributed Authoring and Versioning

1. CTL Background

The CTL-ACTD (Coalition Theatre Logistics – Advanced Concept Technology Demonstration) initiative is designed to enhance combat service support to coalition forces by providing operational and logistic staff with access to timely, integrated and accurate logistic information – in short, to provide logistics situation awareness. This will facilitate the following:

- Enhanced theatre engagement opportunities.
- Multi-national collaborative logistics analysis capability.
- Improved deployment capability of coalition forces.
- Efficient force sustainment, exploiting cross-coalition synergies.
- Detailed monitoring for execution of logistics operations against plans, allowing "management by exception".
- Rapid logistics re-planning (reacting to significant variations in demand, deviations from projected support and interruptions to supply chains).
- Improved logistics C2 (Command and Control) interoperability and coalition-wide logistics situation awareness.

The CTL ACTD Requirements Study (Jan–Apr 2001) identified gaps in Australia's coalition logistics information and decision-making capabilities whose rectification was of highest priority (balancing urgency against achievability). This study complemented a parallel study carried out by US PACOM J41. The US/AS agreed requirements (as subsequently amplified) are:

CTL Requirement 1: Determine the total lift requirement for the coalition forces. Develop multinational movement plans that use assigned strategic lift assets to deploy coalition forces into theatre, phased such that personnel are operational on entry to theatre (necessary equipment and services available on arrival). Track in-transit strategic lift assets from the National Support Area to the AO (Area of Operations) and identify the primary characteristics and destinations of the on-board personnel, forces and cargo.

CTL Requirement 2: Provide visibility (location and status) of materiel and personnel while in transit, via military transport and/or commercial carriers, from the National Support Area to the AO and within the AO to the coalition logistics release point. Include tracking of progress of orders and ability to search greater amounts of detail.

CTL Requirement 3: Provide the best available infrastructure information on ports, airfields, rail yards, staging and assembly areas and ground lines of transportation to deploy and sustain forces and equipment. Infrastructure data is to include details of MHE (Mechanised Handling Equipment) and refuelling abilities. A method of achieving this being pursued by DSTO (Defence Science and Technology Organisation) is the bringing of relevant data from disparate sources to a suitable common view using web-portal technologies.

2. Architecture Background

In 2001 the CTL ACTD project started with the aim to integrate Australian logistics systems with the US logistics systems. The first trial of this was to be demonstrated in September 2001 although the demonstration was postponed due to uncontrollable circumstances associated with September 11. The trial was eventually conducted during JWID 2002 (Joint Warrior Interoperability Demonstration). The tool suite used in JWID was comprised mainly of US tools with minor alterations to support integration into the JWID environment and scenario. Although the JWID demonstration went well, it featured only a limited capability for transferring coalition data due in part to limited Australian participation. JWID did however provide a good forum to expose the concepts and ideas of CTL to a wider audience and provided valuable experience. Before the JWID demonstration even started, work had begun on the new CTL architecture. The new architecture has been developed to solve the issues of differing data formats, provide processes and interfaces for transmission of data, and create an overall environment into which tools and services could be plugged. Work on this architecture was conducted jointly between DSTO (Defence Science and Technology Organisation) Australia and Lockheed Martin (LM) in the US. The CTL Technical workshop held in Canberra, Australia in June 2002 was the pivotal meeting where both the US and Australian technical teams agreed on the new CTL architecture that is outlined in this document.

3. Architecture Overview

From work conducted by DSTO and LM the architecture depicted in Figure 1 below was developed.

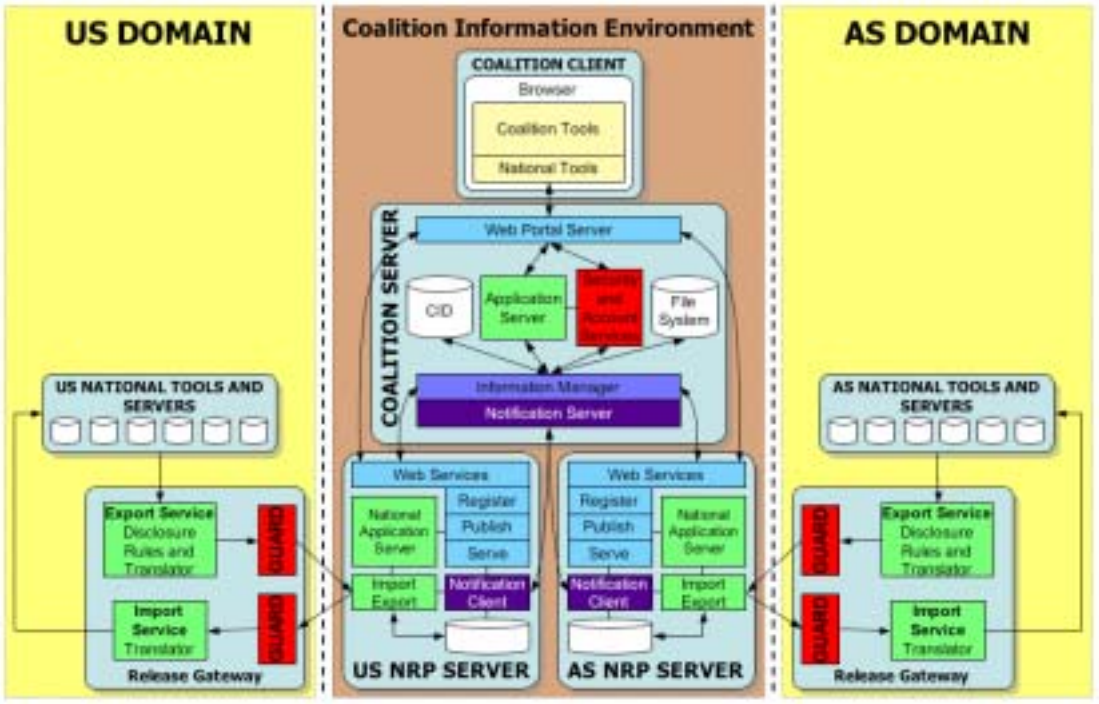

Figure 1 – CTL Architecture

The primary difference between the architecture depicted above and previous architectures used within CTL is that it was developed from the ground up to support legacy applications and sharing of data over coalition networks. The basic principle behind its design is to support any nation no matter what type of national systems they use to exchange logistics information with other coalition nations. The main driver behind the architecture is development of a common ontology[1] for logistics data, to be used as the standard data structure for moving data within the Coalition Information Environment (CIE) over coalition networks.

The main components illustrated in the diagram above are the application servers, Information Manager, National Release Point (NRP) servers, File System and the Coalition Information Database (CID).

[1] An ontology is a description (like a formal specification of a program) of concepts and relationships. For CTL ACTD the common ontology is based on development of XML Schemas that define a common language understood by all CTL members.

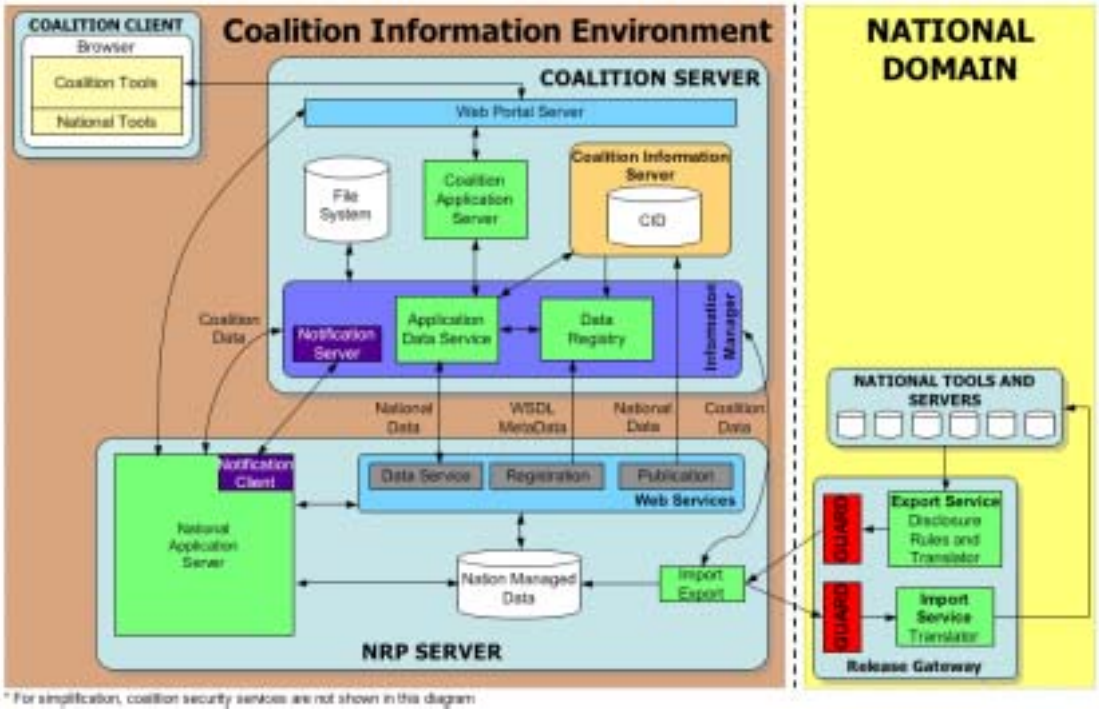

Figure 2 – CTL Architecture Detail

More detail about the architecture is depicted in Figure 2 above. This second diagram shows the Information Manager and NRP in more detail. As shown the Information Manager contains two components, the Data Registry and the Application Data Service. The Information Manager is described in more detail later. Figure 2 also clearly depicts two coalition databases, the CID and the NRP database; both are discussed in the following sections.

3.1 National and Coalition Domains

The CTL architecture has been split into two areas, the national domain (potentially one for each nation in the coalition) and the coalition domain (also known as the CIE). The national domain contains the national logistics systems and data sources. The data contained within this domain will most likely be stored in national formats. Data to be pushed into the coalition domain will have to be cleared for release (following national security release policies and procedures) and then moved into the coalition domain via the data guards that are depicted in red within the release gateway on Figure 2. These guards stop or limit any malicious entities within the coalition domain from accessing data stored in the national domain. After moving through the guard the data is then stored within the NRP or pushed through the NRP and stored in the CID.

The policies and procedures for releasing data from the national domain into the coalition domain are each nation's responsibility, as they will need to be accredited by their individual national security authority. For the current version of CTL, data that is released into the coalition domain is assumed to be released to all coalition nations, although the releasing nation may place restrictions on access capabilities to the data. The purpose of the release gateway is to stop items from being released into the coalition domain that are not deemed releasable. For example a document that can only be handled by Australians would not be released to other coalition nations and therefore would not be released into the coalition domain. Near-term versions of

the release gateway will most likely be very labour-intensive and involve an individual manually checking data to determine if it's allowed to be released into the coalition. In the future it is planned to automate this process (at least partly) by providing contracts for types of data that are allowed for release and then automatically pushing this type of data through the release gateway without human interaction.

When data is transferred from the national domain into the coalition domain the data must be converted from its original national data format into the coalition data format. This can be done on either the national domain side of the guards as shown in the diagrams above or after the data has been pushed through the guards and is within the coalition domain but before it has been released or exposed to other coalition nations (or both as appropriate). It is up to the nation releasing data into the coalition to determine at what point the data is converted, as long as it is converted before being transferred from the NRP to the coalition server or another nation's NRP. This process must be performed in reverse when moving data out of the coalition domain back into the national domain, as the data will need to be in the national data formats to work correctly with the national tools and services.

It is expected that the systems contained within the national domain and within the NRP will be owned and maintained by each nation. The coalition server will be deployed and maintained by the coalition's lead nation. Therefore a nation does not have to worry about the specific implementation details of other nations' NRPs as long as they all adhere to the coalition standards for exposing data, applications and services contained within the NRP.

3.2 National Release Point (NRP)

Within the CIE there could be multiple NRPs, potentially one for every nation that is involved in the coalition. The purpose of the NRP is to contain all the nation's data and tools so that they are still under national control. Within the NRP is the NRP database that contains the nation's data that has been released to the coalition. It is expected information that is updated regularly could also be contained within this database; some examples of data to be stored within the NRP are:

- Infrastructure Information
- GIS Information
- In-Transit Visibility Information
- Force Contribution Details
- Local files

The information within the NRP database is then exposed to the coalition via the NRP web services that communicate with the application servers and Information Manager. The NRP serves as a gateway for all data coming out of the national systems. The NRP provides the capability to export data out of the CIE back into the national systems via the security guards. The exact configuration of the NRP is up to each nation; it is foreseen that some nations may configure their NRP considerably differently from others. This should not matter, as interoperability and access to the data will be available through the CIE, provided that the data definitions as agreed in the ontology and web services have been adhered to.

A key benefit of having the NRP is it allows each nation to have added control over releasing data to other nations within the coalition domain. The NRP also allows the nation to add its own applications and non-standard data into the coalition without affecting the overall coalition architecture. Although CTL ACTD is not providing rigorous access control, the use of NRPs could allow for the implementation of tighter security. It is possible that in the future some information could be released to the coalition and additional information only selectively released to other nations from the NRP. For example, information could be contained within the NRP that was only releasable to Australia and US but not UK. Although this is a potential for the future it is not being considered for the current version of CTL. The aim of this architecture is to support the current documented requirements and provide a framework for future concepts and ideas to be explored at a later stage with a minimum of redesign and re-engineering.

3.2.1 NRP Database

Each NRP database will contain national information for use by the NRP's applications or to store national data that is being exposed to the coalition by the NRP's web services or is in transit between the coalition domain and the national domain. The NRP database is under the control of the nation that owns the NRP server. The structure of the NRP database is not controlled by the coalition and will not affect the rest of the CIE as long as the NRP's web services meet the coalition standards.

3.3 Coalition Server

Within the coalition domain is the coalition server, which contains all the standard applications and services that are available to all nations. It contains the required infrastructure to facilitate data transfer, notification and coalition storage within the CIE. The main components of the Coalition Server are the Web Portal Server, Information Manager, CID, Security Services and File System. Without these core services the CTL architecture will not function correctly.

3.3.1 Web Portal Server

The Web Portal Server's purpose is to provide the presentation layer for coalition applications. Users access the portal server by using a web browser that displays each portal page. A portal page is comprised of multiple portlets, which are the presentation components of the applications contained within the application servers both on the NRPs and Coalition Server. The portal server enables the user to choose the layout and selection of portlets to be displayed in a portal page. This customisation allows a user to combine portlets from multiple applications and compare the outputs from the different applications. The portal server also has other personalisation features that allow applications to customise their data to users' requirements.

When developing applications to exploit the full capabilities of the portal server, the application must be reduced into components that output HTML (and associated technologies). Each of these components is wrapped to create the portlets that are displayed within the portal page. It is possible to create multiple portlets for a particular application so that each portlet provides a different view on the data the application uses. The portal server provides a superior method for displaying web

based applications to users and is strongly recommended for use as the presentation medium for both NRP and Coalition server resident applications within the CIE.

3.3.2 Information Manager

The Information Manager is used to register data contained within either the NRP or the CID and services contained in the application servers. This registry allows coalition and national applications to find the location of data and services within the CIE. The registry is wrapped with an outer layer of functionality that incorporates CTL-specific business logic. For example the registry wrapper will send out notifications when new data is registered. Also contained within the Information Manager are a number of services and components to help maintain and move information around the CIE. One of these services is the Data Access Service that provides a logical layer above the data contained within the coalition.

There are two methods of using the Information Manager, either by using the registry and then accessing the data sources directly or by using the Data Access Service, which abstracts the finding and collating of data from the client. Using the Data Access Service may present performance issues within the architecture and therefore experiments will be conducted using both data access methods to compare the differences in speed and usability.

Accessing data via the Data Access Service allows for storage of complex queries within the Information Manager so that each application does not have to duplicate the same capability. Applications may additionally require execution of complex operations that are not available within the Data Access Service; these applications can query and access the data directly and execute their own operations on the data. Providing both data access methods allows for greater flexibility.

3.3.3 Application Servers

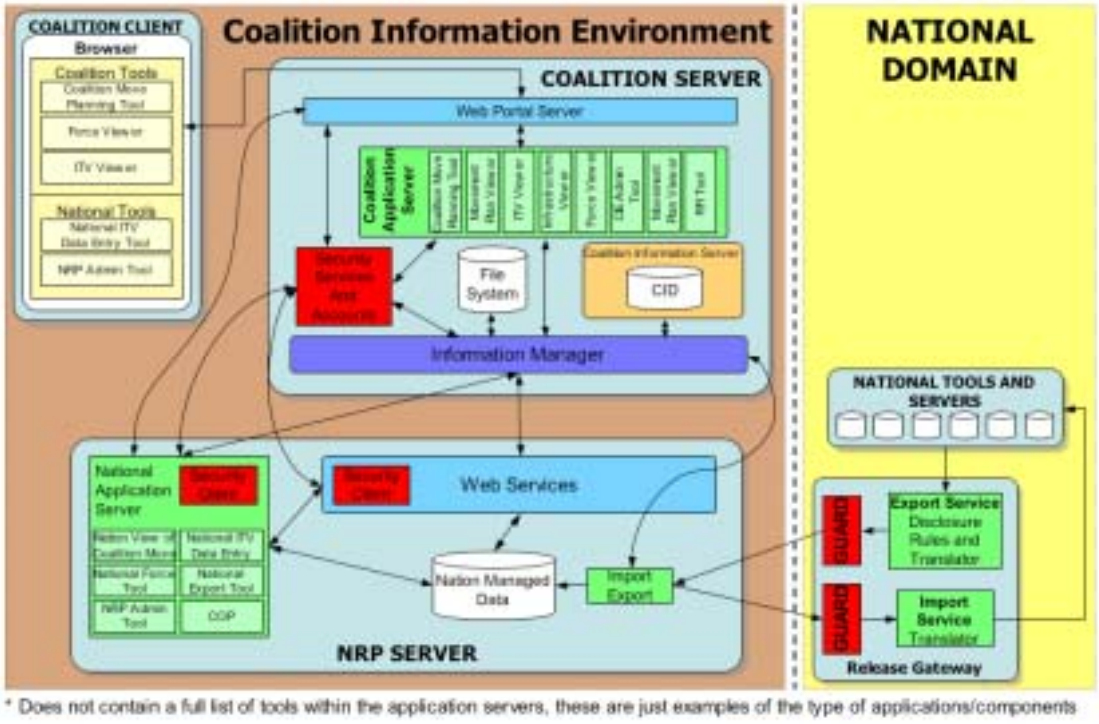

Figure 3 – CTL Application Servers

There are two types of application servers, one found within the coalition server and the other found in the NRPs (see Figure 3). The main purpose of the application servers is to contain the business logic needed to run the tools and services used within the CIE. For example a coalition tool for developing, modifying and viewing coalition movement plans would be stored and run from within the coalition server's application server. The reason for the two types of application servers is that the coalition application server is used to store the accredited and agreed coalition applications, whereas the national application server stores applications, tools and services that a nation has created and wishes to use within the CIE but which have not been accepted as agreed coalition tools or services. Tools that reside within both application servers and may be accessed by the coalition portal and communicate with the coalition data sources must support the standards and requirements for communicating with the portal server and coalition data sources. For more information about the core coalition application tool suite see Section 5.

For the initial implementation of CTL the coalition application server will be completed using BEA WebLogic, which is a J2EE (Java 2 Enterprise Edition) based application server. In addition, a secondary Microsoft .NET server is likely to be stood up to support applications that run within the .NET environment. The J2EE and .NET applications will communicate via the use of standard SOAP/Web Service messages. It is also expected that the coalition security services will need to interoperate with the .NET server and therefore hooks between J2EE and .NET to the security services will be provided.

The purpose of having distinct coalition and NRP application servers is so that a nation can provide its own capabilities to the coalition without having to go through the process of accrediting applications to become part of the core coalition tool suite.

3.3.4 Coalition Information Database (CID)

The Coalition Information Database (CID) is used to store data within the coalition that is not handled by the nation's NRP. The CID can also be used to store national data for nations that do not have their own NRP, for example nations who do not have suitable national logistics systems. The CID also stores data that has been created within the coalition. Some example types of data to be stored within the CID are:

- National Movement Requests
- Coalition Movement Plans
- Coalition Application Data
- Coalition Sustainment Plans

The data structures used within the CID and to be used for data transmission are standard throughout the CIE and all coalition applications will understand this common data format. For example, a standard structure is being designed to store or transmit movement requests within the CIE. The CIE relies on the use of these standard data structures.

The first implementation of the CID will use an Oracle database, although it will be designed so that any of the usual relational databases could be used.

3.3.5 File System

Along with the CID the coalition server also contains a file server. The file server allows file-based information to be contained within the coalition and shared with other coalition users. For example Word documents and Excel spreadsheets could be stored and accessed on the coalition's file server. It is planned for the file system to be accessed via WebDAV (Web-based Distributed Authoring and Versioning) interfaces so that all clients have a common access method. It is expected that all files stored within the file server will be linked with metadata that describes the files' contents, authors' details, and expected uses. Currently, details about the file system's access method and how to associate the files with metadata have not been fully explored or developed.

3.4 Data Schemas and Communication Services

Throughout this document a set of data standards and communication methods is discussed but never defined. This is because the CTL architecture has been developed independent of the data representation and communication technologies. The initial implementation of CTL uses XML Data Schemas and Web Services to define and move information in the coalition information environment. Although these two technologies have been chosen, the CTL architecture allows for other concepts and technologies to be used. For instance, agent-based technology could be used to share information within the CIE.

As XML and Web Services are open standards developed by a worldwide user group and implemented by multiple vendors, they allow for greater interoperability within CTL. Definitions for CTL XML data schemas are outside the scope of this document. When the specifications are completed they will be delivered as supplements to this architecture overview as separate documentation.

4. Case Studies

To explain how the described architecture would function, five example case studies are explored:

1. Importing data from national logistics systems into the CIE.
2. Accessing infrastructure data from within the CIE.
3. Exporting data out of the coalition to be used in the national logistics systems.
4. Accessing coalition tools that adhere completely to the coalition tool requirements.
5. Accessing coalition tools that do not adhere to full coalition tool requirements.

4.1 Case Study 1

Importing data from national logistics systems into the CIE using the NRP

While using the CTL system there will be many cases when information that is stored within national systems will need to be released into the coalition domain to be transmitted to other coalition members or used as an information source for developing coalition plans or gaining logistical situational awareness. There are two methods of exporting data from a national system into the CIE. This first method is to push the data through the NRP straight into the CID and store the data within the coalition server (shown in Figure 4). The second method is to push the data into the CIE and store it within the NRP database to be accessed later via the NRP's web services (shown in Figure 5).

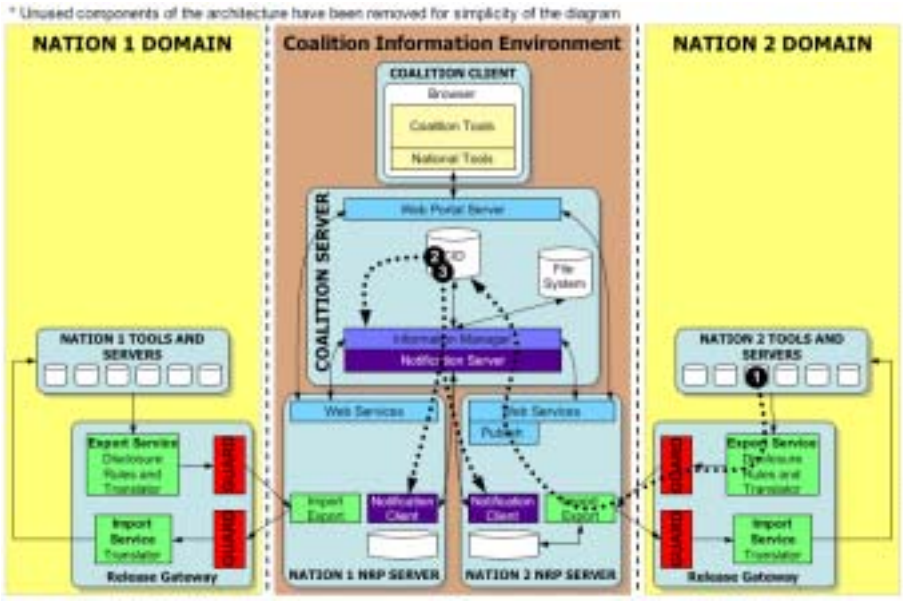

Figure 4 – Case Study 1 (Version 1)

Process Flow (Version 1 – see Figure 4):

1. First the data is exported from the national system and transformed into the coalition data format. The data is then transferred through the security guard into the CIE where it is stored within the CIE database. (The transformation of the data can be conducted before or after going through the guard. It is up

to the implementing nation to make this decision based on security or policy issues.) After the data has been translated, the coalition-formatted data is published using the web services to the CID.

2. The CID registers the new data that has been published with the data registry contained in the Information Manager so that other applications or services know where to find the information if required.
3. After registering the data, the Information Manager's registry then informs all notification clients subscribed to this data type via the notification server.

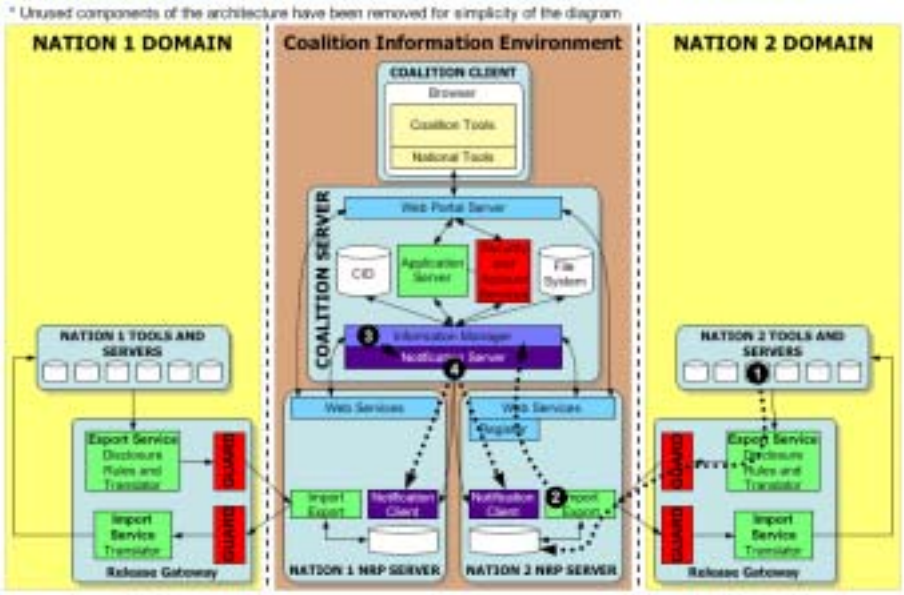

Figure 5 – Case Study 1 (Version 2)

Process Flow (Version 2 – see Figure 5):

1. The data is exported from the national system, transformed into the coalition data format, and transferred through the guard into the NRP within the CIE. (As above, the translation could also occur after passing through the guard.)
2. The import/export component within the NRP must then register the data contained within the NRP database with the Information Manager.
3. After registering the new data, the Information Manager's registry sends out a notification message to all subscribed clients via the notification server.

4.2 Case Study 2

Accessing infrastructure data from within the CIE

This second case study identifies how data is accessed from a browser client situated within the CIE. This is the typical method to access the coalition and national (NRP-resident) tools and the data that these applications rely upon.

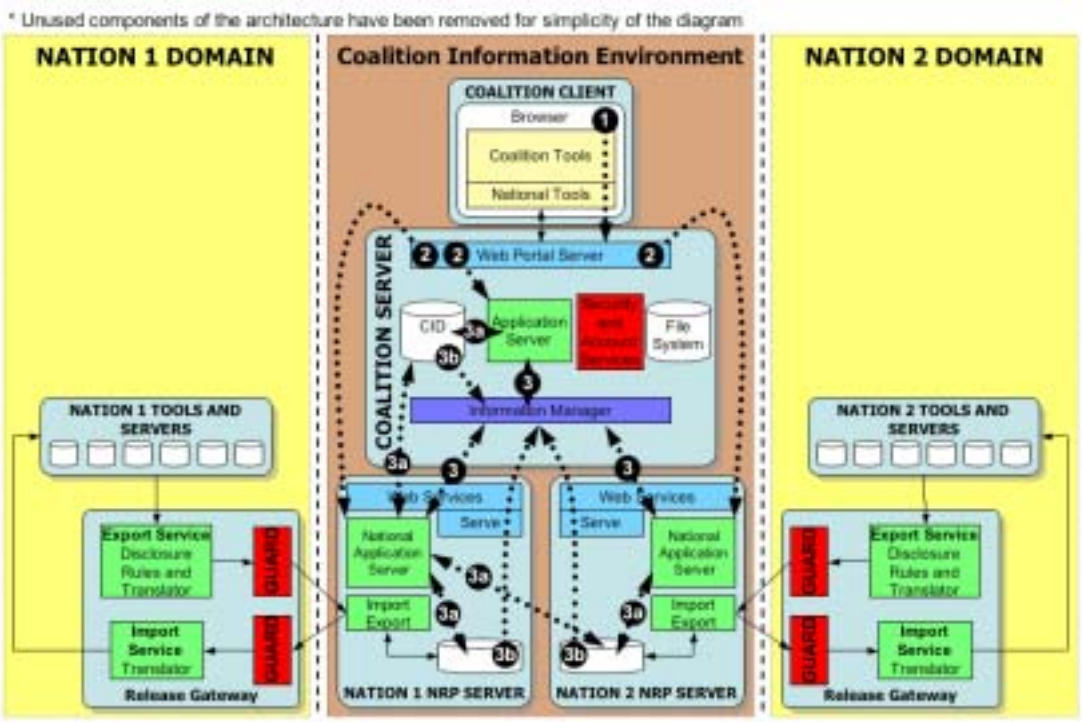

Figure 6 – Case Study 2

Process Flow (see Figure 6):

1. The user requests the portal page by using their Internet browser (eg. Netscape or Internet Explorer). The portal page will contain a number of different tools/service portlets that may be contained on both the coalition and national application servers.
2. The portal then sends off requests for the portlets contained on the application servers (both coalition and national servers).
3. The application servers may then need access to data; there are two methods of retrieving this data.
    a. The application servers query the Information Manager's Data Registry as to the location of required data. After the location of the data has been acquired then the data is accessed directly via web services.
    b. The application servers send a request for data to the Information Manager. The Information Manager then queries its own Data Registry to locate the data. After locating the data the Information Manager then requests the data on behalf of the application from its source, collates the data and sends the result back to the requesting application server.
4. This step is not shown on the diagram, but the application servers send their portlet (display) information with the included data back to the portal server and then back to the user's browser.

4.3 Case Study 3

Exporting data out of the coalition to be used in national logistics systems

This case study describes how data is moved back out of the CIE into national logistics systems to be further processed and integrated. This type of scenario will support coalitions where one nation has a strong national system and can export coalition data to their national system to process and value-add. The resultant data could then be pushed back into the CIE for other nations to access or not as appropriate.

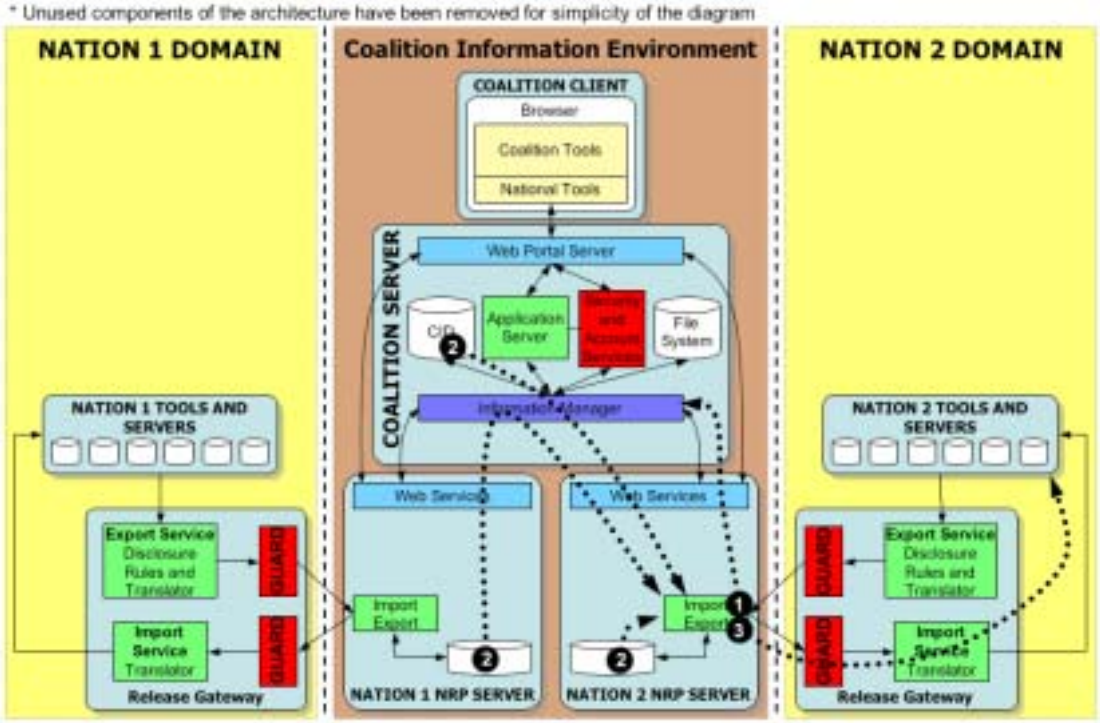

Figure 7 – Case Study 3

Process Flow (see Figure 7):

1. The import/export adapter within the National Release Point communicates with the Information Manager (either via the data registry or the Data Application Service) for the data required.
2. The adapter gets the data back either from the Information Manager or directly from the web services. Data can come from either the CID or NRP databases (including the requesting NRP's database).
3. The data is then sent back out of the CIE through the guard into the national domain to be converted to national data formats and used within the national applications and services.

4.4 Case Study 4

Accessing coalition tools that adhere completely to coalition tool requirements

This case study gives an indication of what the user would see if they accessed tools within the coalition environment via the web portal interface. This particular example only shows tools that comply with the full coalition requirements for both presentation and coalition data manipulation. This does not mean that the tools being accessed within this case study must all be located on the coalition server, the tools could also be located on multiple NRPs. All tools within this case study will have to meet the full requirements imposed by the core coalition tool requirements. This will include requirements on how data is accessed and stored, the formats used for the data, and the method of presentation of its components.

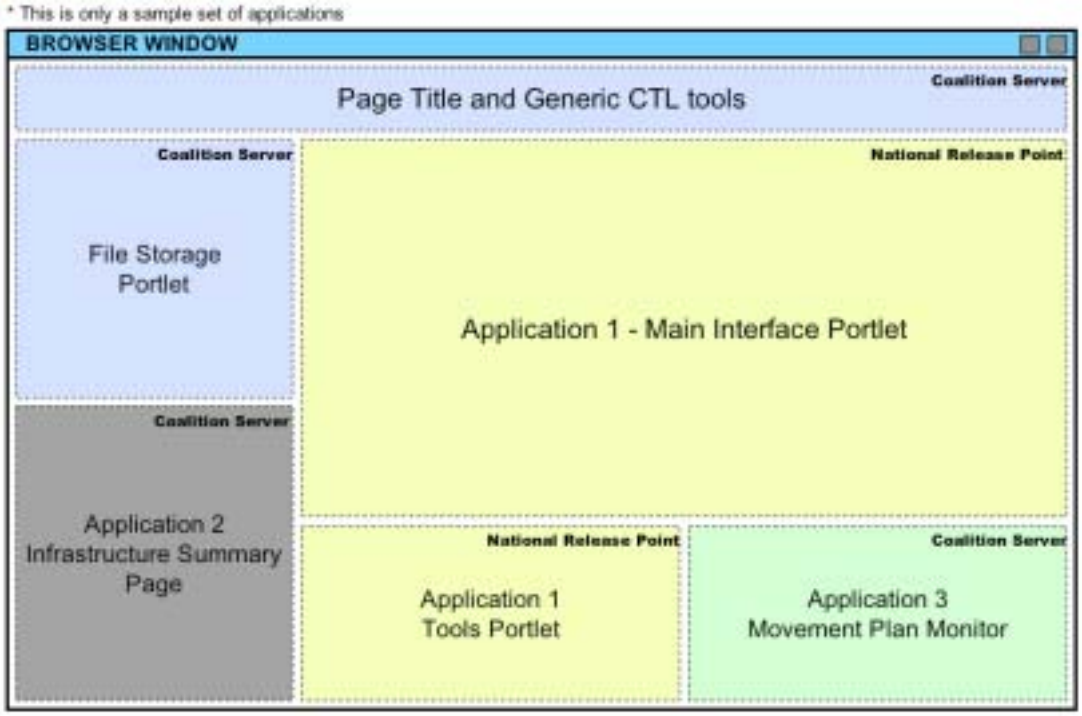

Figure 8 – Portal window containing 3 conforming applications (from both the NRP and Coalition Servers)

In Figure 8 a mock-up example of a portal page is shown where the tools are displayed to the user in a web browser. On the page are a number of portlets that together create the whole portal page. Each of these portlets has been generated from the applications contained within the application servers, on both the NRPs and the coalition server. Each portlet is a component of the application's interface. It is possible to combine multiple portlets from various applications onto the same portal page to create custom views. It is also possible for more than one portlet to be used by one application. By allowing the user to configure the portal pages, applications can be selected that are relevant to the user and the data that they show is filtered or customised to the user's request. Summary pages from different applications on the same portal page can allow users to compare the outputs. As the coalition applications all operate from the same coalition data, if one application alters the underlying data all the applications will also be updated to create a common data view.

This scenario is the preferred method for developing and presenting applications. In so doing, applications must adhere to the presentation requirements to use the coalition portal server to render the application interfaces. If this does not occur then the situation as explained below in Case Study 5 occurs.

4.5 Case Study 5

Accessing coalition tools that do not adhere to full coalition tool requirements

This example is similar to Case Study 4 except that some of the applications being accessed do not fully meet coalition requirements for either data access or interface design. These types of non-conforming applications will most likely reside within the NRPs. Even though the application is operating from within the NRP this does not mean that the application is constrained in its ability to expose its full capability. The purpose of placing these non-conforming applications within the NRP is to allow them to still be accessible by the coalition without corrupting coalition databases or infrastructure with nation-specific data requirements or capabilities. NRP-resident applications can use and store data within the coalition databases. The data within the tool's own NRP database can be in any format, therefore this storage method will support applications that do not meet the full coalition data requirements.

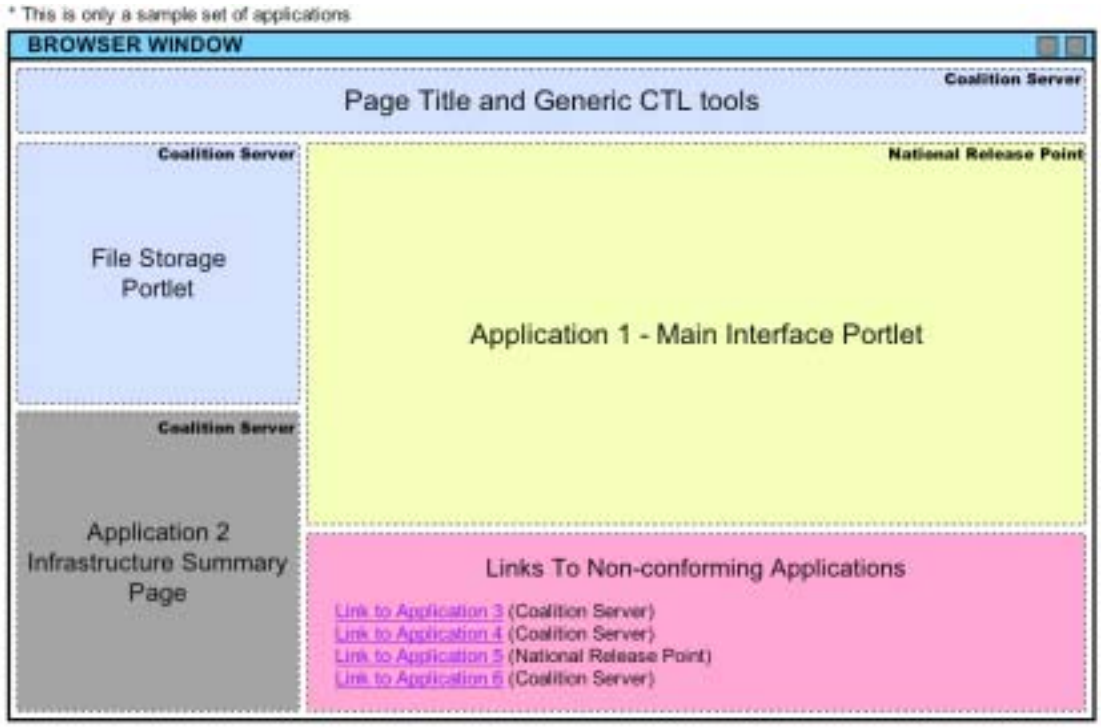

Figure 9 – Portal window containing 6 conforming and non-conforming applications (from both the NRP and Coalition Servers)

Figure 9 is very similar to the figure in Case Study 4 where the user accesses the coalition tools using a web browser and the coalition portal server. The difference is that this page also contains a number of applications that do not adhere to the coalition presentation requirements and therefore can only be shown as links. When the user clicks on these links the application will then load up in a separate window and operate as normal. These types of applications do not integrate well with other

coalition applications and can detract from the overall user experience. This method of access is provided for compatibility with applications that cannot or will not be adapted to conform to coalition application/service requirements. Non-conforming applications may still access coalition data as long as they adhere to coalition data service requirements while doing so. In this example, the coalition portal is used solely as a common place to find the applications; none of its additional capabilities are used.

As the aim of CTL is to integrate applications and tools, this method is discouraged; it does not provide the user with a seamless view of the applications. Having applications running in separate windows and using multiple user interface designs can be confusing, and increases learning times and detracts from usability. Therefore application developers are strongly encouraged to utilise the full capabilities of the portal server.

5. Coalition Applications (Policies and Procedures)

Within the CIE there are two types of application servers, one that resides within the coalition server and the other that resides within the NRP. NRP applications do not need to meet the full CIE requirements, but when accessing coalition data they must adhere to coalition data format and access standards. The applications contained in the coalition server are termed the core coalition applications. Proposed core coalition applications will have to go through an approval procedure. The types of checks an application must pass are:

- Work seamlessly with communication and data services
- Adhere to the coalition data formats and standards
- Integrate into the coalition portal framework
- Integrate with the coalition security services
- Must be available for all coalition nations

The full processes, procedures and criteria for approving an application as a member of the core coalition tool suite have not yet been completed. The concept though is that the developer of the application will put forward their product for scrutiny by the CTL Approval Board that will then judge if the application meets the requirements to become part of the core coalition tool suite. Members of the Board will include a member from the CTL project management and technical teams from each nation involved in the CTL program. Applications are also chosen based on the coalition's needs, so it is therefore possible for an application to meet all the requirements to become a coalition application but if there is no need for the application it could still be rejected for inclusion to the coalition tool suite.

Applications that have already been accepted into the core coalition tool suite are not outside this approval process. As new applications are developed that supersede already accepted applications, the older core coalition application must be compared to the new application to determine which provides better capability to the coalition. Updates to existing core coalition applications must also be reviewed as the new functionality provided may supersede other tools. It is still possible though to have two tools providing similar capabilities.

The next few sections describe examples of the types of qualities and requirements that prospective applications must meet to become part of the core coalition tool suite.

5.1 Work seamlessly with communication and data services

Any application proposed to become part of the core coalition application tool suite must adhere to the communication standards used within the Coalition Information Environment. For example, the application must communicate with the Information Manager to retrieve data, either directly by finding the location from the registry and communicating directly to the data services via web services, or by using the Information Manager's Data Access Service. The application must use the standard interfaces for these communications with coalition services.

5.2 Adhere to the coalition data formats and standards

The format of the data that the application creates and stores within the coalition data stores (CID or NRP databases and registered with the Information Manager) must adhere to the CTL coalition data formats. The application must also adhere to the standards for communicating with other services within the CIE so that all core coalition applications can interoperate with each other.

5.3 Integrate with the coalition portal framework

It is planned that most core coalition applications will be accessed via the coalition portal. Therefore the coalition applications must be able to provide their interface in a format that is digestible by the portal server. This normally entails the application providing a modular web-based interface to the client so that each module can be displayed within its own portlet. It is also possible for the application to contain a java applet type interface or to be a standalone application that runs within the coalition environment (for offline data input). It is preferred that all core coalition applications be accessed by using the coalition portal.

5.4 Integrate with the coalition security services

The proposed coalition application must integrate with the coalition security services to authenticate users and determine the allowed access levels to requested data. If an application does not conform to the full coalition security service requirements then it cannot be considered for integration as part of the core coalition tool suite. The application must adhere to the security rules when a client is accessing the application and when the application is requesting data.

5.5 Available to all coalition nations

The last major hurdle that the proposed application must pass is that access to the application must be available to all nations. This means that all nations must have access to the executable code so that they can create their own coalition server and implement their own instance of core coalition applications. The reasoning behind this requirement is that the coalition server will be the responsibility of the lead nation. Therefore all nations who have the potential of becoming a lead nation must be able to instantiate their own copy of the coalition server and the applications and services that it provides. This means that any applications that become core coalition applications must be available to all potential lead nations at reasonable cost and effort. It is not just a matter of all nations having access to the application for use, but they must also be capable of gaining licenses for the software. The actual policies and procedures for the handling of the core coalition applications still need to be developed by CTL policy staff.

6. Architecture Benefits

There are many benefits with this new version of the CTL architecture. The main points are its flexibility, extensibility and adaptability. As most communication within the Coalition environment is conducted using web services, it does not rely on a particular hardware platform to be used thus allowing each nation to implement their components of the architecture with whatever hardware platform they are familiar with, reducing the learning time and the need for retraining staff.

As the architecture is based around the use of open standards it is also possible for each nation to choose the type of software that they wish to use to implement core coalition applications. It is even possible to reduce costs by using open-source and free versions of software provided they adhere to the CTL standards.

The new architecture is adaptable to support future requirements, for example the use of stronger security within the NRPs so that nations can control what other nations are viewing. The use of standard data formats allows for each nation to convert their national data into the coalition formats, which helps other nations to convert from the coalition format back into their national format quickly and easily. The creation of standardised data formats also helps to organise and clarify the types of information that are required to be shared within coalition environments.

The new architecture provides a means to separate national coalition applications from core coalition applications. In addition it is recommended that an approval process is developed for adding core coalition applications. This allows nations to provide their own tools and place them within the coalition domain and to access coalition data without forcing all other nations to also use these tools or potentially corrupting coalition data.

Creating the new architecture has also forced the CTL team to take a step back and take a broad look at where CTL is heading and what is needed within the project. It has also allowed us to develop the data requirements so that they clearly reflect the needs of the coalition rather than of any one nation.

7. Architecture Disadvantages

The main disadvantage of the architecture is the need to develop a large amount of new infrastructure and messaging systems to support the extensible and adaptable nature of the architecture. There is also the need to alter applications to make them compatible with the coalition domain's data and presentation requirements. These alterations may be considerable for applications on the coalition server but could be relatively minor for NRP-resident applications.

Another disadvantage is that web services security standards are still being developed and are in constant flux, but this is changing quickly as many large commercial companies are feeding resources into this area.

Additionally, when using the new architecture and its web-based infrastructure there are potential performance issues. Currently the performance of web services versus other technologies has not been fully explored. This is one driver behind development of the Data Application Service within the Information Manager (so applications have the choice of accessing the data directly themselves or using the Data Application Service). The Data Application Service itself could also be a potential bottleneck within the architecture if all data requests use this capability.

At this time, the above issues are only viewed as potential problems; much experimentation and testing is planned to fully explore the issues and optimise the system appropriately.

8. Conclusion

The new CTL architecture as outlined within this document provides some key features not present in the past CTL architecture or any other coalition architecture available to date. These include:

- Ability to have core coalition applications supported by additional national applications within the coalition environment.
- Standard use of data formats for exchange of coalition logistics data.
- Support for nations who do not have suitable C2 (Command and Control) infrastructure and applications.
- Provision of greater control for each nation as to how their data is handled and accessed from within the coalition environment.
- Support for both J2EE and .NET applications and services.
- A modular infrastructure that allows additional functionality to be plugged into the architecture.
- Design based around standards allowing each nation to implement their solution with their choice of software (eg. BEA WebLogic, IBM WebSphere, JBoss, etc).

The overall benefits of the new architecture are its flexibility and extensibility. It will allow CTL developers to provide a platform enabling new applications and services to be dropped into the architecture and to access coalition data available on the system. Without such an architectural framework, it would have become increasingly difficult to work with and manage the overall CTL system.

References

1. Kuster, E. (2002) Proposed Coalition Theatre Logistics Advanced Concept Technology Demonstration Architecture, DSTO, Command and Control Division
2. Directorate of Military Strategy and Strategic Doctrine (October 2001) *ADP 00.03 Coalition Operations – Draft 04*, Australian Defence Doctrine Publication
3. C4ISR Architectures Working Group (1997) *C4ISR Architecture Framework Version 2.0,* United States of America Department of Defence
4. Joint Test Publication 4-08 (2001) *Joint Doctrine for Logistics Support of Multinational Operations,* United States of America Department of Defence
5. Joint Publication 3-16 (2000) *Joint Doctrine for Multinational Operations*, United States of America Department of Defence
6. Ryan, A. (2000) *Primary Responsibilities and Primary Risks – Australian Defence Force Participation in the International Force East Timor*, Study Paper No. 304, Australian Land Warfare Studies Centre
7. MacMillan, K. (2002) *Policy Management – Coalition Theatre Logistics – Task Report*, Booz Allen Hamilton
8. Finkelstein, C. (2002) XML Web Services, *XML Data Interchange for eBusiness Conference*, Sydney, Australia, 5-6 March 2002, BTELL
9. Ryan, A. (1999) Command and Control in Multinational Military Operations: Historical Lessons For Future Regional Peacekeeping, *TTCP Workshop on Global Resource Management: Exploiting Command and Control Information Systems in Coalition Peacekeeping Operations*, DSTO Salisbury, Australia, 9 November 1999

Distribution List

Coalition Theatre Logistics (CTL) Advanced Concept Technology Demonstration (ACTD) Architecture Overview

Egon Kuster

AUSTRALIA

DEFENCE ORGANISATION

	No. of copies
Task Sponsor	
Director General Strategic Logistics Branch (CDRE Clinton Thomas)	1
Deputy Director Logistics Information Environments (Mr Selby Dyer, (R1-3-A163))	1
S&T Program	
Chief Defence Scientist FAS Science Policy AS Science Corporate Management Director General Science Policy Development	shared copy
Counsellor Defence Science, London	Doc Data Sheet
Counsellor Defence Science, Washington	Doc Data Sheet
Scientific Adviser to MRDC, Thailand	Doc Data Sheet
Scientific Adviser Joint	1
Navy Scientific Adviser	Doc Data Sheet & Dist List
Scientific Adviser - Army	Doc Data Sheet & Dist List
Air Force Scientific Adviser	Doc Data Sheet & Dist List
Scientific Adviser to the DMO M&A	Doc Data Sheet & Dist List
Scientific Adviser to the DMO ELL	Doc Data Sheet & Dist List
Information Sciences Laboratory	
Chief Command & Control Division	Doc Data Sheet
Research Leader Command Decision Environments Branch	1
Research Leader Information Enterprises Branch	1
Research Leader Joint Command Analysis Branch	Doc Data Sheet
Research Leader Intelligence Information Branch	Doc Data Sheet
Head Human Systems Integration	Doc Data Sheet
Head Information Exploitation	Doc Data Sheet
Head Effects-Based Modelling and Analysis	Doc Data Sheet
Head Information Systems	1
Head Distributed Enterprises	Doc Data Sheet
Head Joint Operations Analysis and Support	Doc Data Sheet
Head Command Concepts and Architectures	Doc Data Sheet
Head Command Process Integration and Analysis	Doc Data Sheet
Head Intelligence Analysis	Doc Data Sheet
Task Manager: Dr Andrew Au (CC&A/C2D Fern Hill)	1
Author: Dr Egon Kuster	1
Publications and Publicity Officer, C2D/EOC2D	1 shared copy

DSTO Library and Archives

Library Edinburgh	1
Defence Archives	1
Library Canberra	Doc Data Sheet

Capability Development Group

Director General Maritime Development	Doc Data Sheet
Director General Land Development	1
Director General Capability and Plans	Doc Data Sheet
Assistant Secretary Investment Analysis	Doc Data Sheet
Director Capability Plans and Programming	Doc Data Sheet
Director Trials	Doc Data Sheet
(Australian CTL Project Manager – Mr Selby Dyer	1

Chief Information Officer Group

Deputy CIO	Doc Data Sheet
Director General Information Policy and Plans	Doc Data Sheet
AS Information Strategy and Futures	Doc Data Sheet
AS Information Architecture and Management	Doc Data Sheet
Director General Australian Defence Simulation Office	Doc Data Sheet
Director General Information Services	Doc Data Sheet

Strategy Group

Director General Military Strategy	Doc Data Sheet
Director General Preparedness	Doc Data Sheet
Assistant Secretary Governance and Counter-Proliferation	Doc Data Sheet

Navy

Maritime Operational Analysis Centre, Building 89/90 Garden Island Sydney

Deputy Director (Operations))	Doc Data Sht & Dist List
Deputy director (Analysis))	Shared
Director General Navy Capability, Performance and Plans, Navy Headquarters	Doc Data Sheet
Director General Navy Strategic Policy and Futures, Navy Headquarters	Doc Data Sheet

Air Force

SO (Science) - Headquarters Air Combat Group, RAAF Base, Williamtown NSW 2314	Doc Data Sht & Exec Summ

Army

SO (Science) - Land Headquarters (LHQ), Victoria Barracks NSW	Doc Data & Exec Summ
SO (Science), Deployable Joint Force Headquarters (DJFHQ) (L), Enoggera QLD	Doc Data Sheet

Joint Operations Command

Director General Joint Operations	Doc Data Sheet
Chief of Staff Headquarters Joint Operations Command	Doc Data Sheet
Commandant ADF Warfare Centre	Doc Data Sheet
Director General Strategic Logistics	Doc Data Sheet

Intelligence and Security Group

DGSTA Defence Intelligence Organisation	1
Manager, Information Centre, Defence Intelligence Organisation	1 (PDF)
Assistant Secretary Capability Provisioning	Doc Data Sheet
Assistant Secretary Capability and Systems	Doc Data Sheet
Assistant Secretary Corporate, Defence Imagery and Geospatial Organisation	Doc Data Sheet

Defence Materiel Organisation

Deputy CEO	Doc Data Sheet
Head Aerospace Systems Division	Doc Data Sheet
Head Maritime Systems Division	Doc Data Sheet
Chief Joint Logistics Command	Doc Data Sheet

Defence Libraries

Library Manager, DLS-Canberra	1
Library Manager, DLS - Sydney West	Doc Data Sheet

OTHER ORGANISATIONS

National Library of Australia	1
NASA (Canberra)	1

UNIVERSITIES AND COLLEGES

Australian Defence Force Academy

Library	1
Head of Aerospace and Mechanical Engineering	1
Hargrave Library, Monash University	Doc Data Sheet
Librarian, Flinders University	1

OUTSIDE AUSTRALIA

INTERNATIONAL DEFENCE INFORMATION CENTRES

US Defense Technical Information Center	2
UK Dstl Knowledge Services	2
Canada Defence Research Directorate R&D Knowledge & Information Management (DRDKIM)	1
NZ Defence Information Centre	1

ABSTRACTING AND INFORMATION ORGANISATIONS

Library, Chemical Abstracts Reference Service	1
Engineering Societies Library, US	1
Materials Information, Cambridge Scientific Abstracts, US	1
Documents Librarian, The Center for Research Libraries, US	1

SPARES	5

Total number of copies: Printed 36 + PDF 1 = 37

DEFENCE SCIENCE AND TECHNOLOGY ORGANISATION
DOCUMENT CONTROL DATA

1. PRIVACY MARKING/CAVEAT (OF DOCUMENT)

2. TITLE

Coalition Theatre Logistics (CTL) Advanced Concept Technology Demonstration (ACTD) Architecture Overview

3. SECURITY CLASSIFICATION (FOR UNCLASSIFIED REPORTS THAT ARE LIMITED RELEASE USE (L) NEXT TO DOCUMENT CLASSIFICATION)

Document	(U)
Title	(U)
Abstract	(U)

4. AUTHOR(S)

Egon Kuster

5. CORPORATE AUTHOR

Information Sciences Laboratory
PO Box 1500
Edinburgh South Australia 5111 Australia

6a. DSTO NUMBER	6b. AR NUMBER	6c. TYPE OF REPORT	7. DOCUMENT DATE
DSTO-TN-0607	AR-013-302	Technical Note	December 2004

8. FILE NUMBER	9. TASK NUMBER	10. TASK SPONSOR	11. NO. OF PAGES	12. NO. OF REFERENCES
9505-25-13	JTW 01/307	DGSL	30	9

13. DOWNGRADING/DELIMITING INSTRUCTIONS

http://www.dsto.defence.gov.au/corporate/reports/DSTO-TN-0607.pdf

14. RELEASE AUTHORITY

Chief, Command and Control Division

15. SECONDARY RELEASE STATEMENT OF THIS DOCUMENT

Approved for public release

OVERSEAS ENQUIRIES OUTSIDE STATED LIMITATIONS SHOULD BE REFERRED THROUGH DOCUMENT EXCHANGE, PO BOX 1500, EDINBURGH, SA 5111

16. DELIBERATE ANNOUNCEMENT

No Limitations

17. CITATION IN OTHER DOCUMENTS Yes

18. DEFTEST DESCRIPTORS

Joint Military Activities, Joint Operations, Logistics Information Systems, Computer Network Architecture

19. ABSTRACT

This paper gives a basic background to the Coalition Theatre Logistics (CTL) Advanced Concept Technology Demonstration (ACTD) program and the details of the proposed information sharing architecture to be used therein. Outlined are the main components of the CTL architecture and how each component interacts with the others. Although the architecture outlined in this document has been developed specifically for the logistics space, it could also be adapted for use within other distributed information sharing projects. The architecture addresses issues with releasing data into coalition environments, transferring and transforming data between national environments and providing coalition planning and information services.