Chapter 1 – INTRODUCTION AND BACKGROUND

1.1 INTRODUCTION

The IST-061/RTG-027 Task Group was established in December 2004 with a planned duration of two years, until the end of 2006. The following companies and organizations participated in the Group's work:

- Thales (France, Norway): http://www.thales.com/;
- Norwegian Defence Research Establishment (Norway): http://www.ffi.no/;
- European Aeronautic Defence and Space Company (France): http://www.eads.com/;
- TNO (Netherlands): http://www.tno.nl/;
- Research Establishment for Applied Science (Germany): http://www.fgan.de; and
- Military Communication Institute (Poland): http://www.wil.waw.pl/.

The lead nations were France and Norway. During the Task Group work, the original topic, "Information Infrastructure Supporting Net-Centric Warfare Communications", was changed to "Secure Service Oriented Architectures (SOA) Supporting Network Enabled Capabilities". The rest of this chapter describes the background, the scope of work, and the achieved results.

1.2 SCOPE OF WORK

The actual scope of work is defined in the "Terms of Reference", published in Annex B of this report.

The original scope of work considered the functional and technical architecture of an "information communication infrastructure" integrating all the communication services necessary for systems conforming to the principles of Network Enabled Capabilities (NEC). The design was to be performed through identifying services at the **Network level and the Middleware level.**

Issues related with the network level considered, among other things, connectivity services (e.g., route selection), Quality of Service (QoS), network-level security (Virtual Private Networks (VPNs), firewalls), application communication services, etc.

The middleware level required the analysis of message oriented services, data distribution and object management services, data management services, Directory and Naming services and, finally, Security services.

However, it soon became obvious that handling both levels within a single Task Group was too ambitious. In fact, each of the levels would require a single, focused activity, and the interactions between middleware and network could likely require yet more effort. The Task Group decided to focus on the middleware level and skip the rest. Thus, the final project was a compromise but the results were still satisfying. The revised "Terms of Reference" resulting from this change of focus have been included in this report.

1.3 BACKGROUND OF SERVICE ORIENTED ARCHITECTURES

Current military C2, ISR, Combat Management systems are based on a federation of dedicated and heterogeneous systems, and because of that their operational integration deals with the following difficulties:

- Lack of operational interoperability;
- Weak integration of Information Systems services for Situation Awareness (from the strategic level to the tactical level); and
- Lack of global system management, prohibiting dynamic (re-)configuration of systems.

In the NATO NEC Feasibility Study (from NC3A), Service Oriented Architecture (SOA) was identified as a possible solution to the above-mentioned problems. Moving towards a Service Oriented Architecture (SOA) is a way to achieve the seamless information and service sharing required in a future NATO NEC.

SOA is a paradigm for organizing and utilizing distributed capabilities that enables the creation of applications that are built by combining loosely coupled and interoperable services to support the requirements of the business processes. In a SOA environment resources are made available as independent services that can be accessed without knowledge of their underlying platform implementation [19]. The key is independent services with defined interfaces that can be called to perform their tasks in a standard way, without the service having pre-knowledge of the calling application, and without the application having or needing knowledge of how the service actually performs its tasks. In this way, SOA supports the integration and consolidation activities within complex enterprise systems.

A SOA consist of Service Providers who offer their service(s) to Service Consumers by making a description of their services available for discovery, thereby making it possible to match the needs of service consumers with capabilities provided by service providers. Service Consumers can then find (discover) these services. After discovering suitable services, Service Consumers can start using the service in accordance to the specified service contract. A service provides access to one or more capabilities using a prescribed interface. The access is exercised consistent with constraints and policies as specified by the service description. The policies are described in a contract. Policies potentially apply to many aspects of SOA: security, privacy, manageability, Quality of Service and so on. Beyond such infrastructure-oriented policies, participants may also express business-oriented policies – such as hours of business, return policies and so on.

Services can be combined to form the desired application or system: A service consumer can use different services from different service providers and aggregate them into a new service offered to potential service consumers. SOA allows for services to be shared, but still to be under the control of a specific owner.

The Organisation for the Advancement of Structured Information Standards (OASIS) [3] is a not-for-profit, global consortium that drives the development, convergence and adoption of e-business standards. OASIS is developing the SOA reference model, which is currently the most practical alternative to be used as basis for deployments of SOA and the closest thing to a standard available.

A service-oriented architecture may be implemented using a wide range of interoperability standards, including Remote Procedure Calls, DCOM, ORB or Web Services (which were chosen in this project, see Section 3.1). Web Services are promising technologies for implementing SOA allowing for dynamic information sharing between military units. Among the many interesting features of Web Services are dynamic discovery of services and information exchange using event driven models like publish/subscribe. These services inter-operate based on a formal definition (or contract, e.g., WSDL, see 3.x) that is independent of the underlying platform and programming language. SOA is applied to implement (parts of) the middleware level as discussed in Section 1.2. COTS solutions to implement SOA currently exist. This implies the acceptance of SOA, making it a viable path to implement military solutions.

Some problems are not solved by SOA. Dynamic security solutions and bandwidth constraints in tactical networks are some great challenges that have to be solved in order to fully deploy a Service Oriented Architecture supporting NATO NEC.

1.4 TECHNICAL SPECIFICATION AND DEMONSTRATION

The Task Group cooperated to develop a technical specification of a secure SOA (Service Oriented Architecture) using Web Services, with dynamic discovery and replacement of services, effective information exchange through request/response and publish/subscribe communication patterns, and end-to-end security. The specification defines interfaces, protocols and functionality, which must be implemented to achieve interoperability between national systems that wish to share tactical pictures. A shortened version of the specification is contained in Annex A. The demonstration consisted of the application of before mentioned technologies to make these tactical pictures available and to access and share them. Additionally, to verify whether the specification is complete and "just works", the Task Group agreed to implement an experimental system and demonstrate it during the Coalition Warrior Interoperability Demonstration 2006 (CWID'2006) in Lillehammer, Norway.

1.5 SCOPE OF THE REPORT

This report contains the following chapters:

- Chapter 2, "Application of SOA to Support NEC", describes high-level ideas of how tactical communication in coalition environments using SOA, SOAP and XMLSEC can be achieved;
- Chapter 3, "Service Oriented Architectures Technologies Used", provides an overview of the technologies that are the building blocks for the project;
- Chapter 4, "The Demonstrator Scenario", describes the demonstrator scenario including the relevant communication events and processes;
- Chapter 5, "CWID'2006 Demonstrator and Realization", summarizes the specification, describes the actual setup at CWID'2006 and lists experiments that were conducted;
- Chapter 6, "Results and Lessons Learned", describes the results from the experiments and the lessons learned; and
- Finally, Annex A, "Demonstrator Specification", contains a shortened version of the demonstrator's specification.