

## **Annex B – TERMS OF REFERENCE**

### **I. ORIGIN**

#### **A. Background**

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

- Lack of operational interoperability due to the differences between information models used within the different (national) military Information Systems;
- Weak integration of Information Systems services for sharing of Situation Awareness from the strategic level to the tactical level; and
- Lack of global system management allowing the dynamic configuration of systems. This would enable these systems to deal with the diversity of operational scenarios going from intensive combat to peace keeping operations.

The military system evolution towards Network Enabled Capabilities (NEC) has to overcome these difficulties with the objective to achieve “Information Superiority”, “Situation Awareness” and the capability to manage OODA (Observation, Orientation, Decision, Action) loops associated with the network integration of a “sensor-to-shooter” concept.

NEC will allow for seamless information exchange between all involved entities to achieve better and faster coordination of sensors, effectors and decision makers. The successful implementation of NEC systems requires the consistent integration of all the communication and information services implemented by the involved multi-platform Combat, Surveillance, Intelligence or Command systems.

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 will allow for available services and information to be published, discovered and shared in a flexible and dynamic manner over a communications network.

Security will be one of the greatest challenges in the development of a flexible and dynamic SOA. The need for a seamless information exchange requires changes in security policy as well as the introduction of end-to-end security solutions.

#### **B. Justification (Relevance for NATO)**

The realization of NATO NEC requires improved interoperability not only for C2 systems but also for ISR and Combat systems. According to the NATO NEC Feasibility Study (from NC3A), improvements in information exchange may be achieved by developing a Service Oriented Architecture (SOA). The development of a SOA in NATO will require interoperability between national systems at several levels from the data models describing the syntax and semantics of the information to the protocols for exchanging the information. The use of open standards will be essential in achieving this interoperability. Standards and specifications exist today that may be used to implement a SOA. The most common of these are the W3C/OASIS Web Services specifications, which are based on XML. An evaluation of the standards and specifications developed for XML, Web Services and XML Security, needs to be done in order to see whether they meet the military requirements defined for a future NATO NEC.

### **II. OBJECTIVES**

This activity will include the following objectives:

## **ANNEX B – TERMS OF REFERENCE**

---

- A. The design, specification and development of a multi-national distributed demonstrator to be used to evaluate some of today's most common standards, specifications and technologies for implementing a Service Oriented Architecture. This involves:
- a) Development of a simple scenario describing interoperability of a joint and combined task force.
  - b) Development of an XML data model for describing the syntax and semantics for the information to be exchanged between nations.
  - c) Explore available COTS technology, especially the use of Web Services for service discovery, service subscription and service invocation.
  - d) Use of end-to-end XML security solutions (including XML labeling and privileges). This involves the use of available XML security standards and specifications (as far as possible) for protecting the XML information exchanged using the Web Services technology.
- B. The work on the demonstrator will be followed up by an evaluation phase, which will include:
- a) Evaluation of the solutions chosen and the technologies used in the SOA demonstrator.
  - b) Evaluation of the civil specifications, standards and technology for use in military systems.
  - c) Recommendations for changes and/or amendments to the specifications if required.
  - d) Proposals for further work required for NATO and the nations in order to move towards a secure Service Oriented Architecture.

The team is expected to provide technical reports on the particular issues identified above.

The duration of the task group is two years.

### **III. RESOURCES**

#### **A. Membership**

Members should preferably have been personally involved in the application of XML and related middleware technology to military CIS problems in recent years.

Lead nation: France and Norway will Co-Chair the group

#### **B. National and/or NATO Resources Needed**

At least 0.2 man years per scientist including travel funding for at least four meetings per year. Scientists should have access to national prototypes relevant to the specific goals above.

#### **C. RTA Resources Needed**

No NATO resources are identified.

### **IV. SECURITY CLASSIFICATION LEVEL**

The initial, recommended security classification level for this activity is NATO UNCLASSIFIED. In the CWID 06 participation, all equipment will be classified NATO secret. All personnel involved must be at least cleared to NATO SECRET.

## **V. PARTICIPATION BY PARTNER NATIONS**

Partner nations should not be invited to avoid complicating the discussion of national research results, prototypes, etc.

## **VI. LIAISON**

Contact and collaboration with NC3A and related NATO working groups will be required.

