Chapter 6 – RESULTS AND LESSONS LEARNED

This chapter describes the results achieved by IST-061. This is done by first describing the view of each participating nation on the national outcome of the testing done at NATO CWID 2006. References to CWID Test Case definitions and results are given for each nation, as well as results of interactions with participating non-members of IST-061.

Second, the results are described on an IST-061 group level. Besides the very important Specification document, resulting from an integration of national contributions and technical discussions in the group to arrive on proposed solutions for "Secure SOA supporting NEC", the perceived group-level results are summed up. As has been mentioned above, a shortened version of this specification document is presented in Annex A of this report. Some of the material contributed to the specification is strictly limited in distribution to the members of the group and had therefore to be removed before the specification could be included.

Finally there are comments on what may be considered "lessons learned" form this work.

6.1 RESULTS FROM PARTICIPANTS

This section highlights the results from the perspectives of the individual participating organizations and companies in no particular order.

6.1.1 Results from Thales (France)

The transformation of the armed forces is leading to a redefinition of both, the operational requirements and the way in which the armed forces are organised. This impacts on how system architecture should be organised as well. A Thales department, the Battlespace Transformation Centre (BTC) is working on assessing how the transformation impacts System Architecture and Operational Concepts each other. This is why it was interesting in experimenting and getting proof of the relevance of SOA principles and their implementation on Web Services in that context.

The targeted operational capabilities were defined according to drivers such as an enhancement of dynamic connectivity, the security issues within a coalition, and two tenets of NCW that are the information sharing and the shared situational awareness. The results from an operational point of view were the achievement of the following capabilities:

- Dynamic creation of ad hoc COI on the battlefield: Services were in topics regarding two Communities of Interest (COI) (.i.e. C2 COI and ISR COI). COI Members on different platforms may publish/subscribe to their topics. Hence, they send/receive relevant information to/from appropriate members.
- Sharing of services providing situation pictures: Platforms disseminated information over the WAN through services providing Land and Maritime Pictures.
- Sharing of Sensor resource: The platform requested information from a Sensor on a remote platform and a change of its tasking.
- Dynamic Management of Security: The Security Certificates given at planning time allowed managing the initial connection between Platforms. When connected, directories of security certificates were synchronised and updates of security parameters were processed with an immediate effect. Then platforms managed access authorisation to information "on the fly" by revoking security certificates.
- End-to-end secure exchange with different level of security.

The system is composed of two main sub-systems: An IEG and an Application Infrastructure (For more details, please refer to Section 5.3.2). The IEG contains the information assurance and discovery services. The Application Infrastructure features systems offering information delivery services from situation pictures of C2IS to data sensors. The system was built according to assumptions that were verified during the experiment:

- In that architecture all security functions are located in the IEG on the edge of the platform. A central location allows facilitating security management such as the configuration management of security certificates as well as giving a unique access point to the remote platforms. The experiment showed this choice brought an easier buildability of the system and therefore a better maintainability.
- As the discovery services are in the gateway, the platform can only expose those services to the coalition that the platform operators are willing to provide. There is a strict segregation between the internal registry containing all platforms services and those that are exposed to the coalition.
- The application Infrastructure relies on a Data Dissemination Layer, which allows plugging in systems supporting services in an easy way. It allows an easy adding/removing of systems as well.

The benefit of such a system architecture is to get the capability to present an SOA interface to the coalition side of the system while internally we can insert legacy architectures or legacy systems. Additionally it gets a great flexibility because the number and the type of systems can be modified in an easy and affordable way thanks to the plug in on the data dissemination layer.

The technical services such as discovery and information assurance services were enablers in the interoperability of platforms. Despite their different implementation, the participants had the same services providing the same functionality and sharing common standards.

The implementation of the demonstrator was based on Open Standards and used COTS implementations whenever feasible. There was no showstopper although some COTS take some liberties with respect to the standards they implement. The demonstrator implementation used some of the standards recommended in the NNEC Feasibility Study. However, some discrepancies about the used versions have to be noted.

The result is a set of technical components abiding by WS Standards, UDDI and LDAP. It would not have been possible to develop this demonstrator within a so short period of time without the availability of products from the commercial market and the open source community (For more details, please refer to Section 5.3.2.5).

However, the development showed weaknesses of some of these standards in terms of their maturity and the scanty number of implementation. For instance, WS-Notification has few implementations. Moreover, when it is implemented, the COTS did not fully abide by this standard. An example of such an incomplete implementation is the Globus Toolkit version 4 (GT4). Nevertheless, when many of these problems were occurring, often they were fixed thanks to information and source code solution available on the Web.

The issue is not the difficulty or the cost to get the mastery of Web Services. The price is not so high. It is rather the relevance of the choice of standards. The standards are not mature enough, and they may evolve. Hence some of them may become obsolete.

Despite these considerations, the result of the implementation was satisfactory from a technical point of view. The major point is the capability to make legacy systems and infrastructures available as Web Services with reasonable effort. In that way we get a smooth and affordable transition from legacy to NEC.

There was a significant effort to achieve this implementation. It encompasses a large scope of capabilities when comparing with other CWID06 demonstrations. Of course these capabilities do not cover all the

operational needs for a NEC context, but the work done is a good achievement and can mitigate some future risks, as it has been the opportunity to validate many assumptions and to reject some others.

6.1.2 Results from FFI (Norway) and Thales (France)

For the Norwegian participants in IST-061 and NATO CWID 2006, the work on "Secure SOA supporting NEC" has taken a lot of effort, especially if you include all preparation and specification work. The results of those efforts can be summed up in an extremely valuable learning experience for the participants.

The Norwegian focus of the NATO CWID experiment may be described as the combination of four technical areas:

- Dynamic Service Discovery;
- Publish/Subscribe style information exchange;
- End-to-end security; and
- Use of Object-oriented C2IEDM.

The goal of the experiment was to prove that the combination of the four areas could be implemented, and demonstrate information exchange between nations based on the implementations. Underlying is the strong assumption that technology like this is essential to support Network Enabled Capability.

The Norwegian testing at CWID was formally based on seven Test Cases defined up front. The NATO CWID 2006 Report concludes on the Norwegian SecSOA at an overall level: "The information was retrieved successfully by partners." A closer look into the Norwegian Test Cases is given in Table 6.1 below. The numbering (TC#) refers to the NATO CWID Test Case Tool.

Table 6.1: Results of Norwegian Demonstration

TC#	Heading	Description	Result
615	Information delivery using Publish/Subscribe	Show that services are made available to others by publishing, and that efficient delivery of updates is achieved by subscribing to an information delivery service	Success
616	New services made ready for use	Show that a new instance of a known service interface, or a new service with a not previously defined data format, can be published and used	Partial success (50%) – did not test new data formats
617	COI Cooperation	Show Net Centric cooperation between the C2 and ISR COIs using the object oriented MIP (C2IEDM) data model	Success
618	Enhanced end-to-end WS-Security	Show that all SOAP messages exchanged between nations are secured using PKI-based end-to-end object level security mechanisms	Success
619	Access control at the object level	Show that the information objects (WS-notifications or UDDI records) may be securely marked and that only users with the right security privileges can access/receive them	Partial success (90%) – UDDI records were not secured
620	Distributed Security Management	Show that Certificates/user privileges can be issued or revoked, and evaluate the time that is needed until the change has been propagated to all nations involved	Success
621	Dynamic Service Replacement	Show that a broken service may be automatically replaced	Not tested

As stated in the table, there are some areas where our initial expectations were not met. First, the Test Case on "Dynamic service replacement" was cancelled. Second, "New services made ready for use" was not tested "with a not previously defined data format". And finally, the implementation of security on the Service Registry turned out not to be compatible with the respective implementation on Publish/Subscribe. As a result, we could not fully test object level security in the Service Registry.

These are to a large extent implementation shortcomings, and not limitations of the technical concept given in the specifications. But some of them clearly point in the direction of limited "dynamicity", especially when it comes to the Service Discovery and the use of metadata.

On the national level, working together on-site at CWID 2006 has reinforced relations between the participants of the Norwegian CWID delegation, creating a good foundation upon which an even better CWID participation for the coming years can be built. Also, the SecSOA experience helps FFI and the Norwegian Defence in the evaluation of leading technology and how to use it in upcoming work to implement a national Information Infrastructure.

For FFI, the results can be summed up into experience for the scientists and documentation aimed at internal and external use. Being clearly visible as a CWID 2006 participant is also assumed to be a positive result for FFI.

6.1.3 Results from Safelayer (Spain)

The demonstrator proved that Nations can exchange information in a common and secure way. Using the new Web services technologies and the security PKI services they provided information to authorized Nation-consumers.

The SP-ATI2 scenario proved:

- Nation-consumers were able to find the topics that Nation-producers provided and exchange data.
- The parties were able to secure and authenticate the exchanged data as well as ensured the its integrity and the confidentiality of the exchanged data.
- Data exchange was possible among Nations with different PKI domains, offering the same security guaranties to inter-domain communications.

The CWID Web-based Test Case Tool was used for the planning, execution and documentation of NATO CWID Test Cases. The Test Case Tool is an online, interactive database used to coordinate and document interoperability testing and experimentation in NATO CWID.

Scenario test cases were developed based on Interoperability Test Requirements within the context of the SP-ATI2 demonstrator. Interoperability test cases were created based on trials intentions to test specific system capabilities against the following partners:

- France (IT/ID Name: FR-SAIS);
- Norway (IT/ID Name: NO-SecSOA);
- Poland (IT/ID Name: PL-SOA WS); and
- NC3A (IT/ID Name: NATO-CSSI-IVAS).

Trials used the Test Case Tool to record test plans and results in cooperation with their partners (information providers and consumers). Following the execution of a test case, trial partners agreed on a result (Success, Limited Success or Interoperability Issues), then submitted their recommendations to the Interoperability Assessment Team for review.

SP-ATI2 demonstrator focused only on the security aspects, considering the following tests:

- **End-to-End Message level security**: Show that SOAP messages are encrypted and digitally signed using user digital user certificates. Intended recipients must be able to verify the authenticity and the integrity of the data and then to decrypt the information.
- **Digital certificate/user privilege management**: Show that certificates/user privileges can be revoked. Digital signatures using revoked certificates must not be accepted. No information must be provided to users presenting revoked certificates.
- **Access control at the object level**: Show that the information objects (WS-notifications) may be securely marked and that only users with the right security privileges are allowed to access/receive them.

6.1.3.1 Conclusions

CWID 2005 revealed a growing interest on Web services and XML Technologies. Future CWID editions will offer the opportunity to analyze new fields of application, demonstrate the benefits of these technologies, while maintaining the Web services security and PKI technologies in the mainstream. The NATO RTO/IST-061 Secure SOA demonstrators provided real application-cases testing the best state-of-the-art of the technology and its application to the military field.

On the other hand, new technologies usually mean new security protocols in the arena. XML flexibility may reveal interoperability problems on Web service security protocols which must be specially tested: SP-ATI2 makes focus on security interoperability aspects. Preformed tests showed that despite of using different technologies; demonstrators were able to *interoperate and to securely exchange information* (strongly authenticated, digitally signed and encrypted). Norway-Spain and Poland-Spain demonstrator tests where all successful while partially successful in NC3A-Spain.

Finally, we had the opportunity to analyze different architectural approaches of the demonstrators. While most of the demonstrators used PKI toolkits to incorporate security to application, SP-ATI2 used a completely different approach, based on the concept of the PKI-Based Trust Service Provider. *This approach showed that thanks to SOA and Web services, security services can be independent from the applications*. It also simplifies the integration and allows the audit, changes and security upgrades to be transparent to the applications.

6.1.4 Results from EADS (France)

Challenges and objectives for this demonstration were multiple and at different level. The main challenge was to do real experimentation of all the topics that were discussed in this working group. The realization in a CWID context with real multinational systems was a great experience. EADS' objective in this demonstration was to bring legacy systems to interoperate with other nations in this particular context.

Another good challenge during realization was to always keep in mind that SOA is made for flexibility and all architecture used should always be simple (simple to implement, simple to deploy, simple to use). A lot of effort had been spent in this item even if it is not demonstrative.

The modularity of infrastructure solutions is also a big issue. As web service provider, we were able, theoretically, during the CWID demonstration to use any of the web service infrastructures.

During CWID, one of the big challenges was to being able to interoperate with multiple countries and organization at the same time. This CWID gave us the opportunity to make tests with Norway, Poland, NC3A and Spain. It gave us the feedback of the effort we should spend to realize loose coupled interoperability. This effort should be compared to MIP trials that interoperate with messaging or

database. During tests, we also observed that each team was able to work independently. Only one distant service is sufficient for tests. And when different service providers are connected at the same time, we had a global vision of situations without reconfiguring. In the battlefield, having this possibility to be connected to a secured network and to get the common operational picture fitted to our needs (without browsing a registry, without configuring service providers …) is a first step for network centric warfare.

6.2 GROUP-LEVEL RESULTS FOR IST-061

The primary result from the work in IST-061 is the Specification document. Version 1.0 was agreed on and distributed to the group March 17, 2006. An updated version is to be found as an annex to this report.

A secondary result is the proof-of-concept that was performed as a contribution to NATO CWID in May and June 2006. The viability of the experimental implementations of the specification reinforces the value of the specification document.

The NATO CWID results are good examples of how SOA using Web Services may be a suitable technology for systems that are to support NEC. Military resources are made available as services, accessible from the network. Services are described by metadata that is published on the network.

The aim of the specified solutions is to provide more flexibility and adaptivity. The benefits of using this secure and dynamic SOA solution in a military environment are as follows:

- Military resources can be made available as services that may be accessed over a communication infrastructure;
- Information is characterized by metadata and published in the network;
- Efficient discovery and downloading of and subscription to relevant information;
- Faster deployment of new technology and functionality;
- Dynamic reconfiguration of functionality within a relatively short timeframe; and
- Integration of functionality over different networks and heterogeneous technologies.

In the security area, IST-061 has initiated important work. End-to-end security at the object level is an important contribution to existing security regimes. It is an interesting future solution with a great potential, given adequate security policy and management procedures.

IST-061 has developed an experimental solution for the future that has been federated in a European environment. The work has demonstrated how a UDDI Service Registry can be extended to meet future requirements. A practical way of using XML-based MIP/C2IEDM for multinational information exchange has been shown.

The results achieved clearly indicate that SOA is a good foundation for the NATO Network and Information Infrastructure. SOA has the potential of overcoming the limitations of current “stove-piped” solutions.

It is hard to determine the level of success for an effort like IST-061. Many important goals have been achieved, but in hindsight it is easy to spot parts that could have been improved. Overall, and especially when speaking to the world outside the IST-061 group itself, the many positive achievements certainly qualify for the label “Success”. This group can be proud of its results.

A more detailed discussion within the group will reveal substantial goals at the nation and participant level that were not met. “*Limited dynamics*” and “*Specifications were not detailed enough*” are examples of

limiting factors. This may indicate that the correct label on behalf of the participants should be "Partial success". The lessons learned will indicate some shortcomings that can be read as reductions to the success level. On the other hand, it may be argued that those lessons learned are very valuable results in themselves, and should count positively instead of limiting the success.

6.3 LESSONS LEARNED

The experimental implementations relied heavily on Commercial Off The Shelf (COTS) technologies. COTS does not work reliably yet, and is not always compliant with the standards. Standards are not even stable yet. There are bugs in COTS and open source software.

To ease implementation, there was widespread sharing of software components within the group. This makes it easy for smaller participants to join, which is positive, but you get less independent implementations and less validation accordingly. There were only two fundamentally different implementations of IST-061 during CWID.

The group learned numerous lessons about complexity. To sum it up:

- The volume and complexity of MIP/C2IEDM was a problem;
- XML technology is not mature enough; and
- Compatibility problems create needs for agreements on more than schemas and interface descriptions.

Communicating the results of the work is a challenge. Technical elements like SOA and security are hard to visualise in a demo. Although we had agreed on a Scenario framework with a high degree of independency for each nation, we did not make it to a common "live demo" at CWID. There are different views within the group upon publication of the written results.

At CWID, the group members had to participate from their respective national delegations. It is hard to become visual as a group that way. A wish for future events like CWID is to facilitate presence as a NATO RTO group.

The IST-061 group recommends to other NATO RTO groups to conduct implementations and/or demonstrations – e.g. at NATO CWID – in order to create more results than "just paper". Nevertheless, it should be realized that implementation work is generally much more resource consuming than writing reports. But it is valuable to get detailed knowledge on the subject and to validate or reject the assumptions.