FFI Forsvarets forskningsinstitutt

An Architecture for Experimenting with Secure and Dynamic Web Services

11th CCRTS
June 20-22, 2006
San Diego

rolf.rasmussen@ffi.no
Norwegian Defence
Research Establishment

Outline

- Background
- Technology presentation
  - Dynamic Service Discovery
  - End-to-End Web Services Security
  - Publish/subscribe
  - Data Exchange Formats
- Considerations and limitations
- Evaluation
- Conclusion

Background

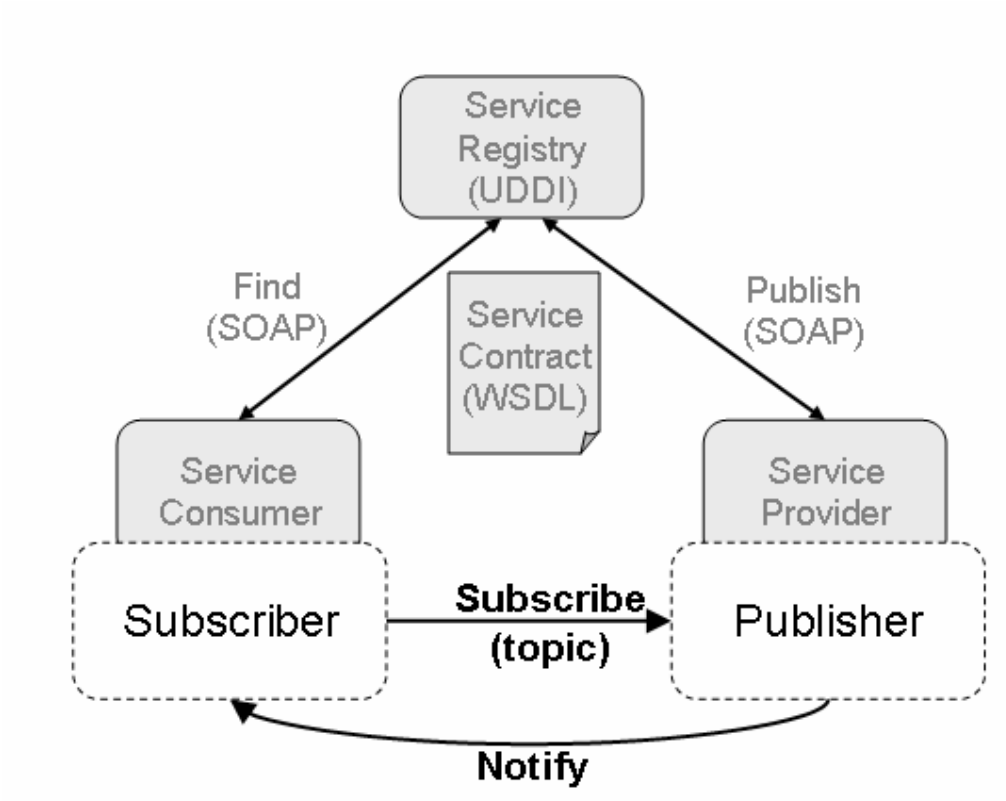
- About...
  - Norwegian Defence and FFI
  - Network Based Defence
  - NATO Network Enabled Capabilities
  - Service Oriented Architecture
  - Web Services
- Experiment goal
  - Implement a Technology Demonstration
  - Demonstrate End-to-End WS-Security
  - Evaluate Publish/subscribe using Web Services

NATO RTO/IST 061:

”Secure Service Oriented Architectures (SOA) supporting Network Enabled Capability (NEC)”

- NATO research group
- Focus on Service Oriented Architecture (SOA) and Web Services technologies
  - in an international (NATO-NEC) context
  - including security aspects
  - including disadvantaged grids aspects
- Distributed demonstrator for research of limitations and possibilities for interconnection and security of Web Services based systems using today’s standards, specifications and COTS technology
- Demonstration at Combined Warrior Interoperability Demonstration (CWID) 2006
- Evaluation of results and solutions

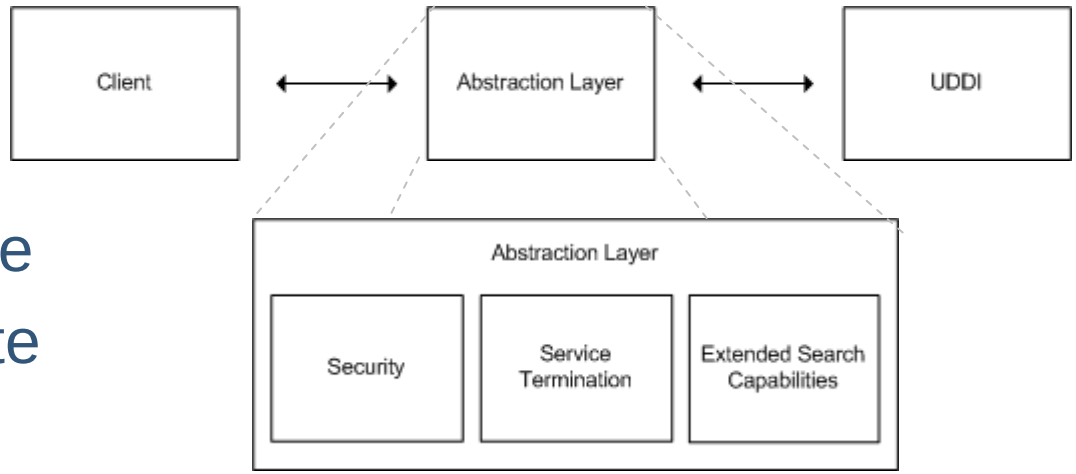
Technology presentation - SOA using Web Services



- Dynamic Service Discovery
- End-to-End Security
- Publish/ Subscribe
- Data Exchange using MIP

Dynamic Service Discovery

- UDDI based
  - businessEntity
  - businessService
  - bindingTemplate
  - tModel
- Abstraction layer
  - security
  - termination policy
  - extended search

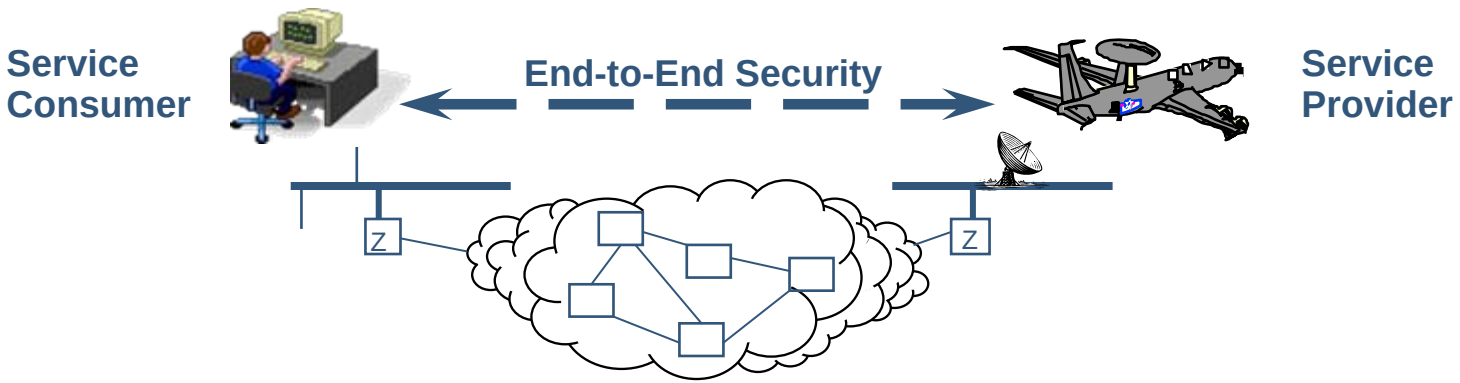


Challenges
•Representing metadata that in itself is dynamic (e.g. mobile sensor positions)
•Advanced service discovery will involve semantics (a common vocabulary is required)

UDDI: Universal Description, Discovery and Integration

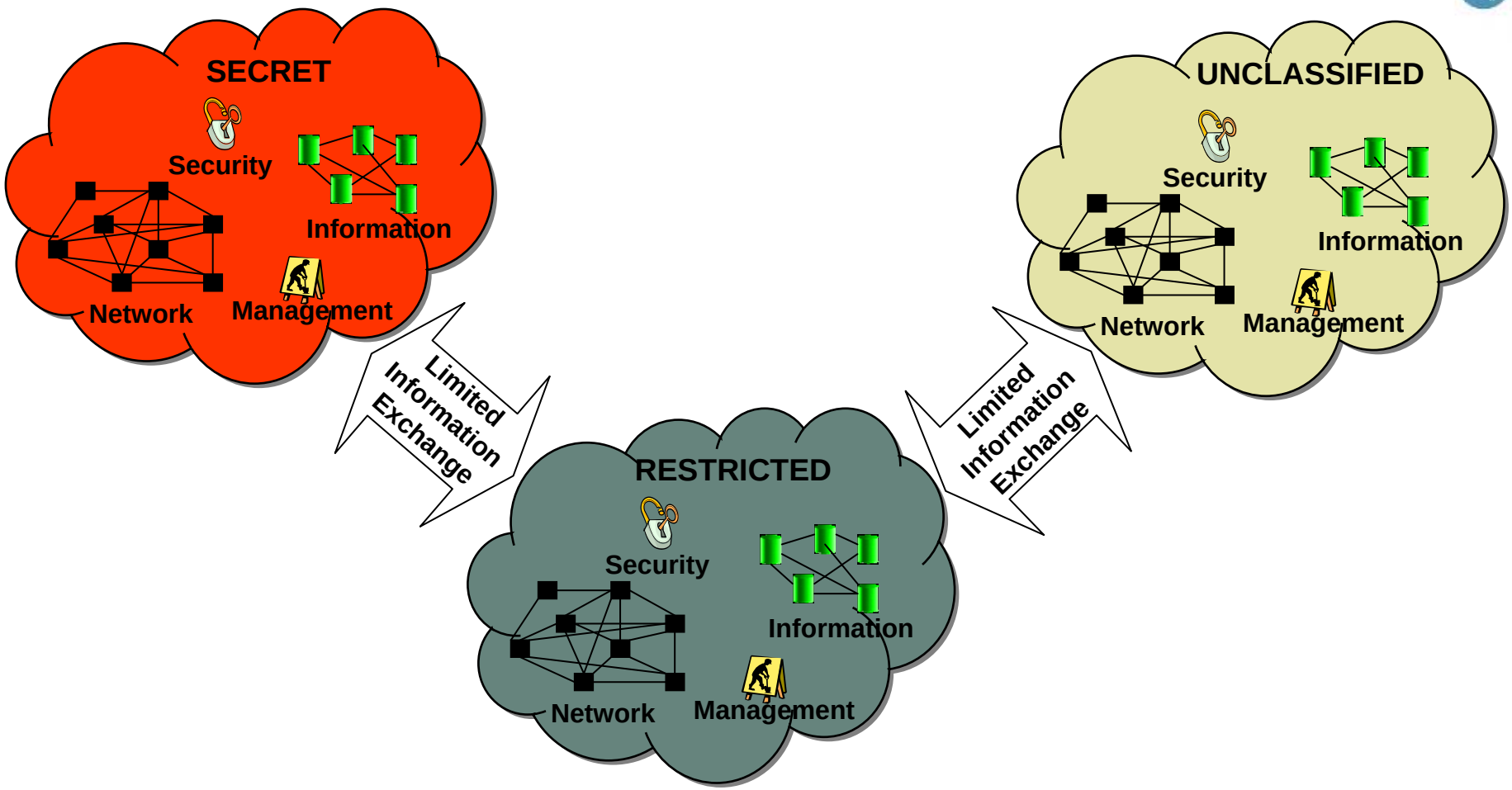
Security Challenges in SOA

- The increased Information sharing in SOA may lead to increased vulnerability if security is not properly integrated
- Introduction of security mechanisms, which allows for dynamic and seamless exchange of information between units will be a challenge
- IP-sec will give confidentiality between systems, but will not prevent unauthorised access within the systems or LANs.
- Computer Network Attacks (CNA) will focus on attacks behind the firewalls (crypto devices) within the LANs/Systems
- End-to-end security services will be required for securing the information in the NEC systems/LANs



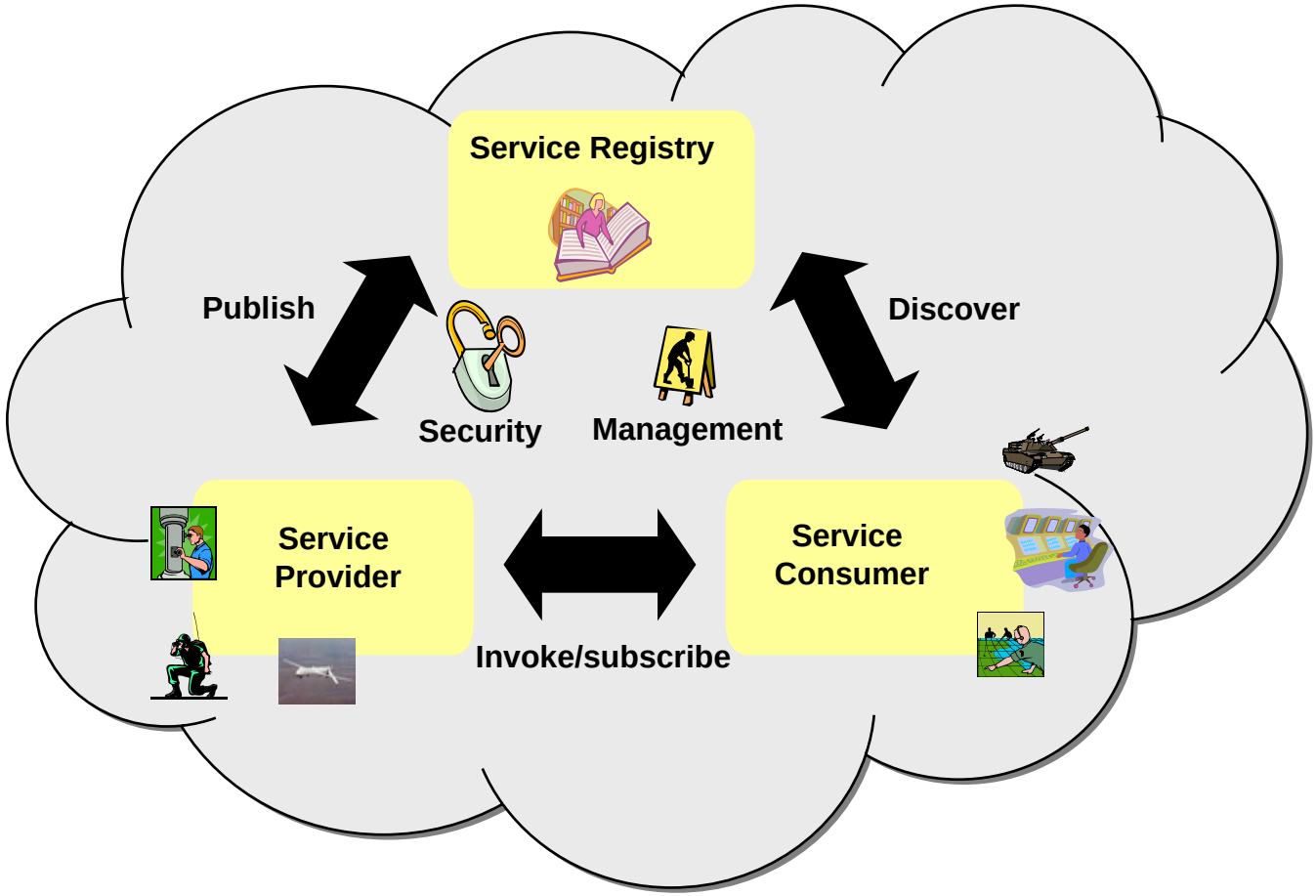
Current Status

Stove Piped Networks for Secure Communications



Separate networks that protect information of different classification using physical, cryptographic and administrative separation.

Future NEC Solution (Long term vision)



The Information is made available for those who have privileges to access it and the system protects the information at the object level.

Access Control at object level based on security labels and user privileges

NEC Requires a More Flexible Security Policy

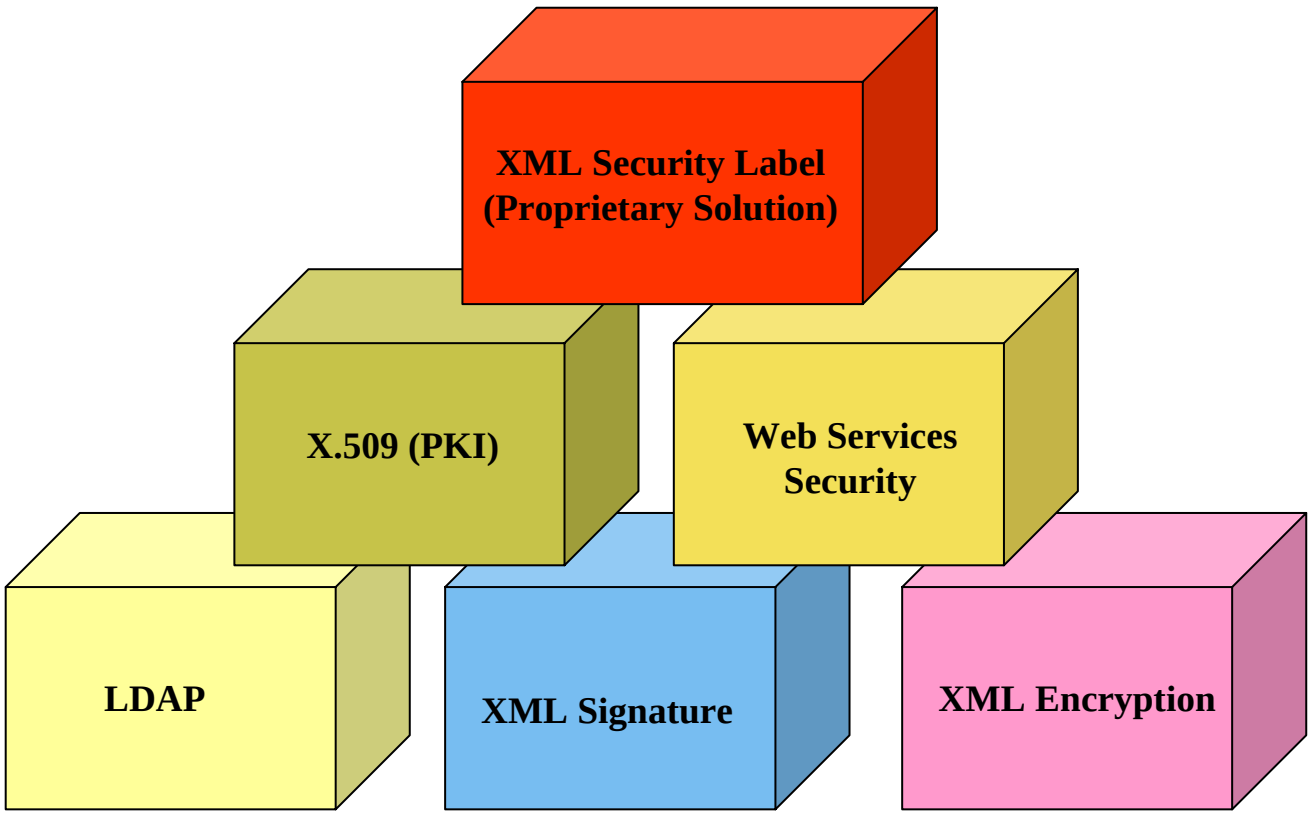
The protection of the information should dynamically be adapted to the threat based on risk evaluation:

- how important is the access to the information for completing the mission
- what is the threat: location, environment, surroundings, etc.
- how sensitive is the information
- what is the trust and privileges of the users requiring access to the information
- what types of information systems/networks are used
- how long will the information be classified vs probability of the information being compromised during that time

Security Services in the Demonstrator

- All Web Services information is exchanged using SOAP messages
- All SOAP messages are attached a security label, encrypted and signed
- A “Domain XML Guard” filters all information leaving the domain based on the security label
- All advertisements in the Service Registry are attached security labels and signed before storage
- Before information is sent to a requestor, her security privileges are checked against the security label of the information
- The LDAP Legacy system is wrapped in SOAP and the SOAP security services are provided to the LDAP replication process

Use of Civil Standards and Specifications as Far as Possible (W3C, IETF and OASIS)



Publish/Subscribe Web Services - Experimental implementation

- The Publish/Subscribe pattern offers an excellent combination of ”push” and ”pull”
- Architecture based on WS-Notification specifications
- Implementation makes use of the Globus Toolkit 4.0 Framework
- Data exchange is performed using two generic notification services
  - Common Operational Picture (COP) for operational purposes on C2 level
  - Moving Target Indicator (MTI) Tracks for tactical purposes

Data Exchange Format: MIP

- Using MIP XML Object-oriented Data Model
  - Better than reusing existing formatted message definitions (e.g. ADatP-3)
  - MIP Data Model – the best alternative for a common vocabulary
  - The object-oriented MIP model provides well-defined data structures
  - XML is well aligned with Web Services
- Strategy: Exchanging a series of “Object Items” as self-contained XML messages
- Reduced set of entities involved (30 out of 240)
- Still very complex XML structures

MIP: Multilateral Interoperability Programme

CWID Test Cases

1. **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
2. **Information delivery using Publish/Subcribe**
   - 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
3. **New services made ready for use**
   - Show that a new instance of a well-known service interface, or a new service with a not previously defined data format, can be published and used
4. **COI Cooperation**
   - Show Net Centric cooperation between the C2 and ISR COIs using the object oriented MIP data model
5. **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 are allowed to access/receive them
6. **Distributed Security Management**
   - Show that Certificates/user privileges can be issued or revoked, and evaluate the time needed till full effect among all nations involved
7. **Dynamic Service Replacement**
   - Show that a broken service may be automatically replaced

Evaluation (1)

- As opposed to the typically pre-planned and pre-configured data exchange patterns in military systems, the proposed technologies offer flexibility and adaptivity
  - Military resources are made available as services, accessible over a communication infrastructure
  - Information is characterized by metadata and published in the network
  - Efficient discovery, downloading and subscription to relevant information
  - Faster deployment of new technology and functionality
  - Dynamic reconfiguration of functionality within a relatively short timeframe
  - Integration of functionality over different networks and heterogeneous technologies

Evaluation (2)

- No major showstoppers identified
- Potential problems:
  - Performance issues
  - Scalability
  - Bandwidth consumption
  - Use of COTS and open source
  - Incompatibilities between the technologies involved
  - Military conditions may expose unexpected challenges
- Flexibility may lead to increased vulnerability if security is not properly integrated
- Success depends on adequate security policy and management procedures

Conclusion

Secure and Dynamic Web Services

- Interesting technologies that contribute to the “flexible but secure” nature of Network Based Defence
- The combination of these technologies is powerful
- UDDI is not well suited as a dynamic service registry
- Web Services and XML are large consumers of bandwidth and processing power
- Need to revise and re-work security policies
- Important challenges in the area of future security management

The experimental implementations look very promising, and we recommend this work to be pursued