FFI Forsvarets forskningsinstitutt

Experiences from implementing dynamic and secure Web Services

11th ICCRTS

September 26-28, 2006

Cambridge, UK

Raymond Haakseth

Norwegian Defence Research Establishment (FFI)

raymond.haakseth@ffi.no

Outline/ Agenda

- Introduction and Motivation
- SOA and Web Services
- Demonstrator Architecture
- Implementation Experience and Lessons Learned
  - Service Registry
  - Publish/Subscribe
  - Data Exchange Model
  - Security
- Conclusion
- Further Work

Introduction and Motivation

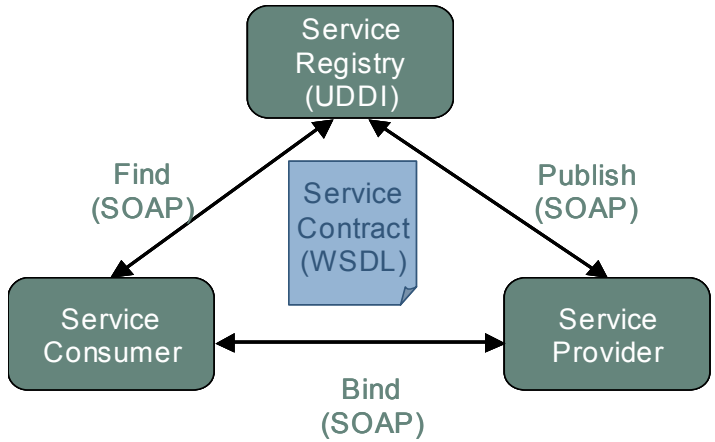
- Transition towards Network Enabled Capabilities (NEC)*
  - dynamic information sharing
  - interoperability
  - security
- SOA and Web Services identified as key architectures and technologies for NEC
- AIM: Develop an architecture for and implement dynamic and secure Web Service
- Experiment/Demonstration conducted at NATO Coalition Warrior Interoperability Demonstration (CWID)
- NATO RTO/IST-061 research group;
  - France, Germany, Netherlands, Norway, Poland and NC3A

* Network Based Defence (NBD) is the Norwegian equivalent to NEC.

SOA and Web Services

- Military resources can be made available as services, that may be accessed over a communication infrastructure
- Information is characterised by metadata and published in the network

- Efficient discovery, downloading and subscription of relevant information
- Faster deployment of new technology and functionality
- Dynamical reconfiguration of functionality in a relatively short time
- Integration of functionality over different networks and heterogeneous technologies

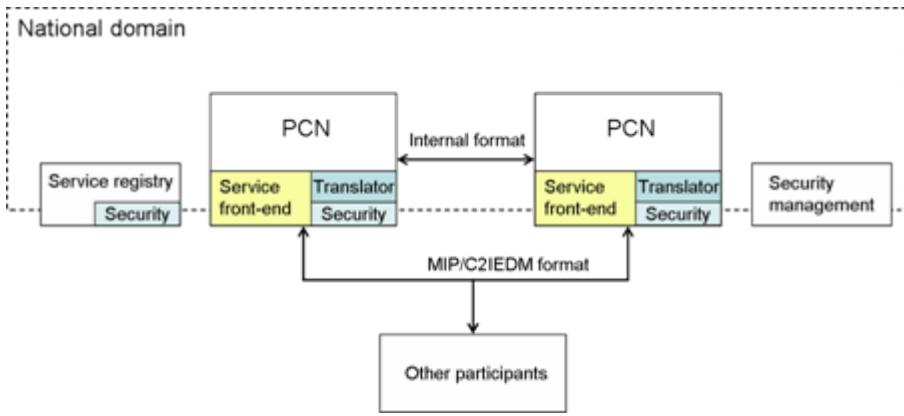


Demonstrator

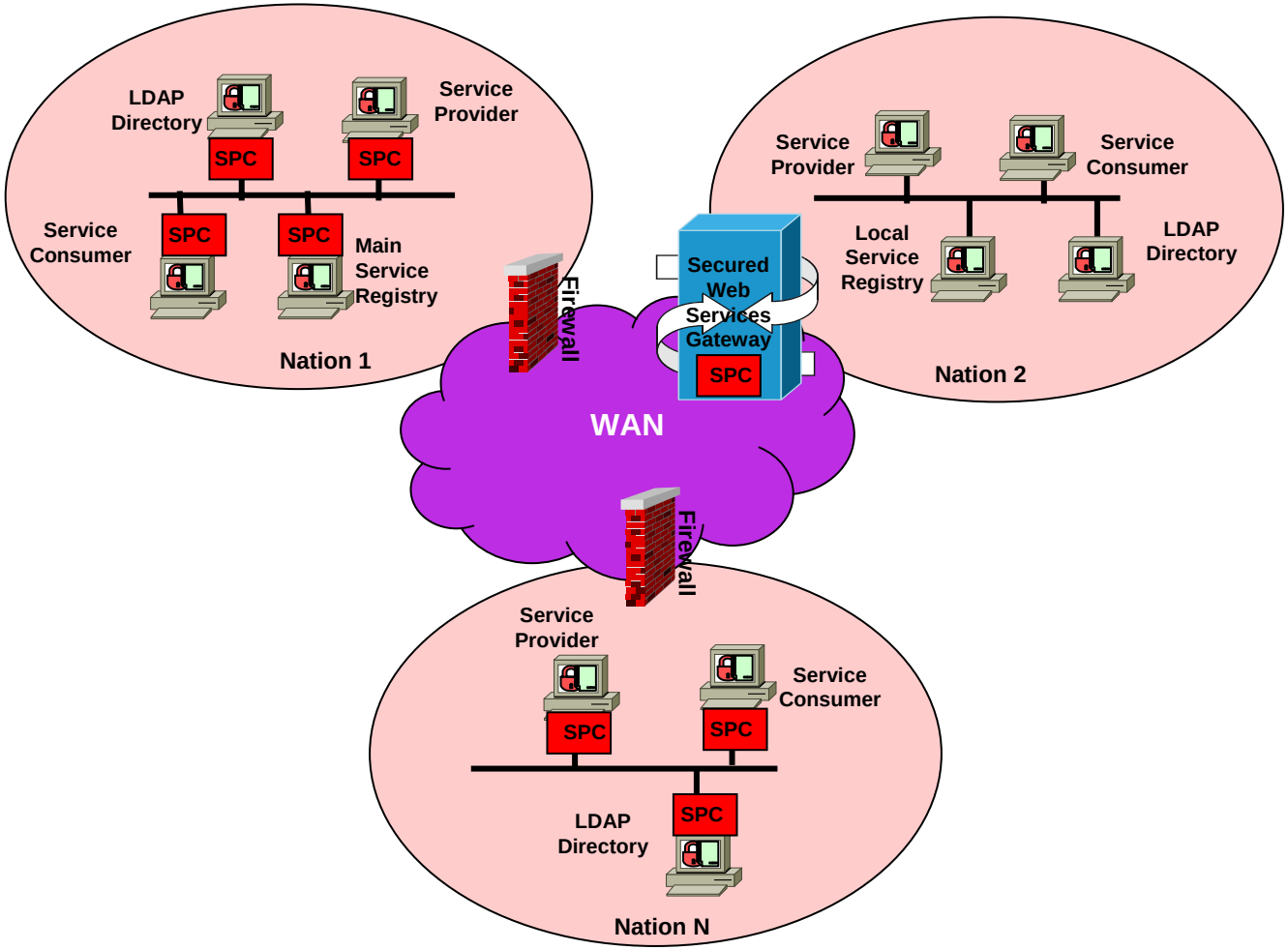
- Main focus of experiments:
  - Dynamic Service Registry
  - Publish/Subscribe information exchange
  - End-to-End Security
  - Data Exchange Model
- Major guideline
  - Use COTS products and standards where possible
- Military Context:
  - Compiling a situational picture, and sharing it
  - Data generated by a synthetic environment

Demonstrator Architecture

- National Domain
  - In-house developed C2 system
  - Distributed and independent Picture Compilation Nodes (PCN)
    - interconnected in a Peer-to-Peer (P2P) manner
  - Cooperatively generate a Common Operational Picture (COP)
  - COP represented and exchanged in an internal format.
- Interoperability with other nations
  - Publish/Subscribe:
    - COP exchanged using the C2 Information Exchange Data Model (C2IEDM)
    - Moving Target Indicator (MTI)
  - Sensor Request
  - Security Management
  - Service Registry



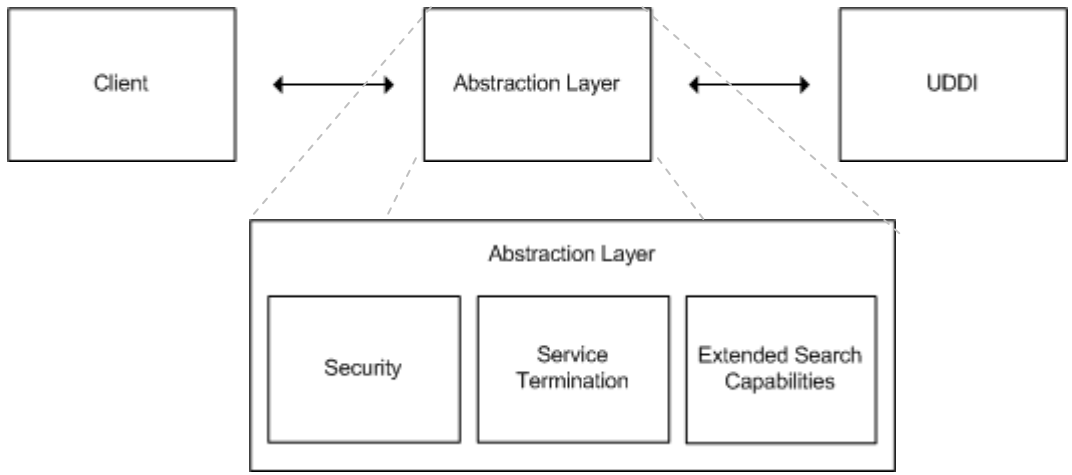
NATO RTO/IST-061 Secure SOA Supporting NEC Demonstrator Architecture (CWID 2006)



SPC: System Protection Component

Service Registry

- Basis for dynamic Web Services
  - Publishing of services
  - Discovery of services
- Based on the Universal Description Discovery & Integration (UDDI) v.3 specification
- Choice made to use an UDDI implementation from Systinet
- Using UDDI Building Blocks:
  - businessEntity
  - businessService
  - bindingTemplate
  - tModels
- Extended functionality
  - Security
  - Termination policy
  - Extended search

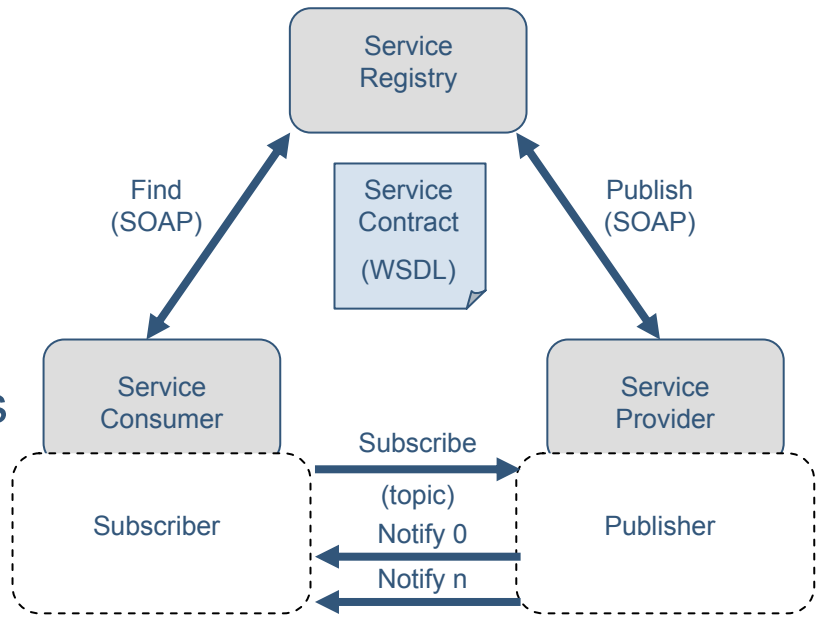


Service Registry - Evaluation

- Filtering (e.g. geographical search and access control)
  - Performed in the *Abstraction Layer*
  - Several interactions with the backend UDDI needed to collect the needed information.
  - Difficult to establish one unambiguous security context.
- Highly dynamic information
  - E.g. geographic position and coverage area
  - Not consistent with the purpose and design of UDDI
  - Frequent updates needed → performance issue
- Complexity
  - UDDI is highly extensible when using the tModel construct
  - Small amount of metadata produces large number of tModels
    - Our small experiment produce 20++ tModels
  - Management and fast discovery may become a challenge

Publish/Subscribe

- Well known pattern for event-driven, asynchronous communication.
  - Combination of “push” and “pull”
  - Fits well into a SOA
- Choice made to use the Web Services Notification (WSN), with the WS-Base Notification and WS-Topics proposed standards from OASIS
- Subscriptions are established on topics
  - Maritime Picture
  - Land Picture
  - MTI Track
- Subtopics can be used to create topic trees
  - Fine-grained filtering of messages
- Used the Globus Toolkit 4.0 (GT4) framework



Publish/Subscribe - Evaluation

- Communication pattern
  - Use point-to-point message distribution at the transport layer
  - May impact sender side efficiency
    - Large number of subscribers, large notifications or both
  - For efficient transport, multicast should be considered used
- Lack of QoS management
  - SubscriptionPolicy defined, but not specified
  - Examples of QoS parameters that a subscriber should be able to request:
    - Message size
    - Message frequency
    - Message content

Data Exchange Model

- Using data model defined by the Multilateral Interoperability Programme (MIP)
- C2 Information Exchange Data Model (C2IEDM) from MIP Baseline 2, object-oriented XML version
  - Best alternative for a common vocabulary
  - Well defined data structures
  - XML is well aligned with Web Services
- miniMIP
  - Adaptation of the model to our needs
  - Reduced set of entities (30 out of 240)
  - No changes to the model, only reduction
- Strategy: Exchanging a series of “Object Items” as self contained XML messages.

Data Exchange Model - Evaluation

- Transformation between data models
  - Not always clear how information should be translated
  - Information Loss
    - Internal COP representation richer than MIP
- Complexity
  - miniMIP is still a very complex XML structure
  - Reaching a common understanding of the model is time consuming
- Data redundancy
  - Trade-off between ease of use and efficiency
- Update policies
  - Exchange all data for each notification
  - Partial or incremental data exchange

End-to-End Security

- Security Challenges in NEC
  - Increased information sharing may lead to increased vulnerability
  - Dynamic and seamless information exchange
  - IP-sec only prevent disclosure of information between systems
  - CNA (Computer Network Attacks) targets systems behind IP-sec and firewall devices
  - ➢ End-to-End security will be required for securing information
- Used available standards such as Web Services Security, XML Signatures, XML Encryption, LDAP and X.509(PKI)
- Developed XML Security Label and mechanisms for deploying it.
  - XML translation of the IETF S/MIME ESS security label

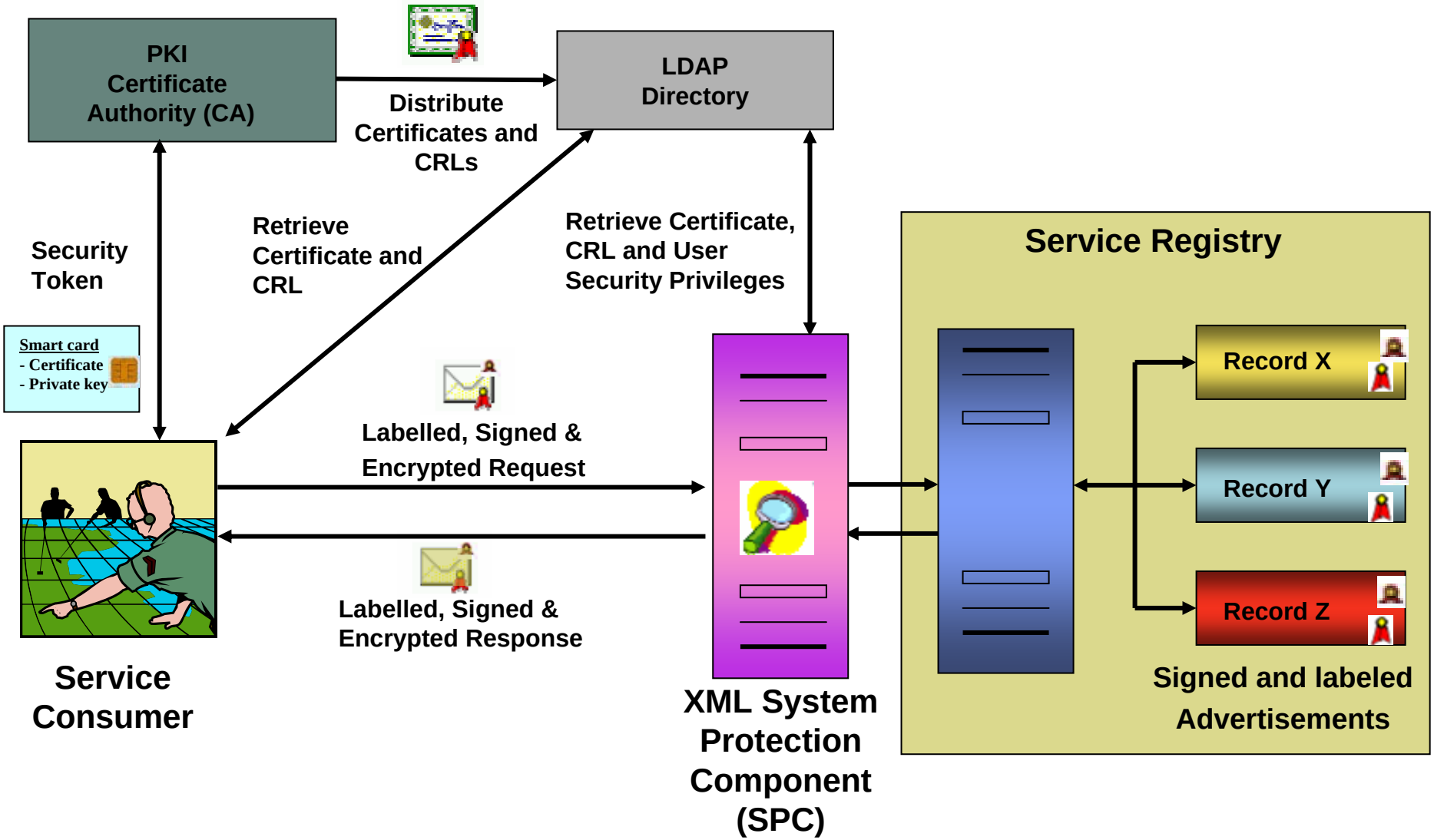
Security Services in the Demonstrator

- 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
  - Using WS-Notification

Example

Security in the Service Registry

(Access Control at the Object Level based on Security Labels and Privileges)



End-to-End Security - Evaluation

- Security Components
  - Security Protection Component (SPC)
  - Label Handling Component (LHC)
  - ➢ Both implemented using available software from Apache and standard Java APIs for certificate and XML handling.
- Integration with COTS software
  - Low level SOAP message manipulation needed
  - Outcome of the serialization of Java objects to actual XML may differ
    - Broken signatures
  - Notifications; access control must be performed at emission time
    - Security level may not be known at subscription time
  - Labeling of UDDI records may be difficult
    - Often comprised of numerous small entities

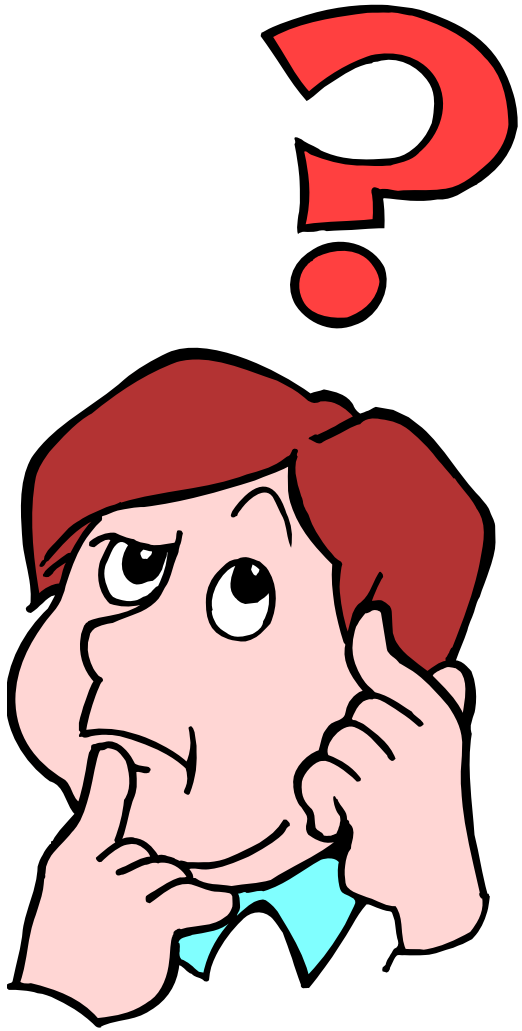
Conclusion

- SOA and the technologies presented here have significant potential in the construction of NEC
  - Flexibility and adaptivity
  - Resources made available as services
  - Efficient discovery
  - Faster deployment of new technology and functionality
  - Dynamic reconfiguration and replacement services within a relatively short timeframe
  - Integration over different networks
- Wrapping of legacy systems is shown to be a viable solution for migration.
- The standards and software used is still immature
  - Need to be very precise when writing specifications
  - Need to check software compatibility carefully
- Security challenges need to be resolved
  - Technical solutions
  - Security policy and management procedures
- **The experimental implementation is promising and we recommend further research**

Further Work

- Security
  - Privilege management
  - Object level security
  - Risk based approaches
  - May require changes in security policies
- Bandwidth consumption
  - Binary XML
  - Compression
  - Partial or incremental data exchange
  - More efficient protocol solution
- Service Registry
  - Semantics
  - Common vocabularies to enable extended use of metadata
- Publish/Subscribe
  - Alternatives to WS-Notification should be investigated
  - Subscription policy and QoS

Questions and Answers

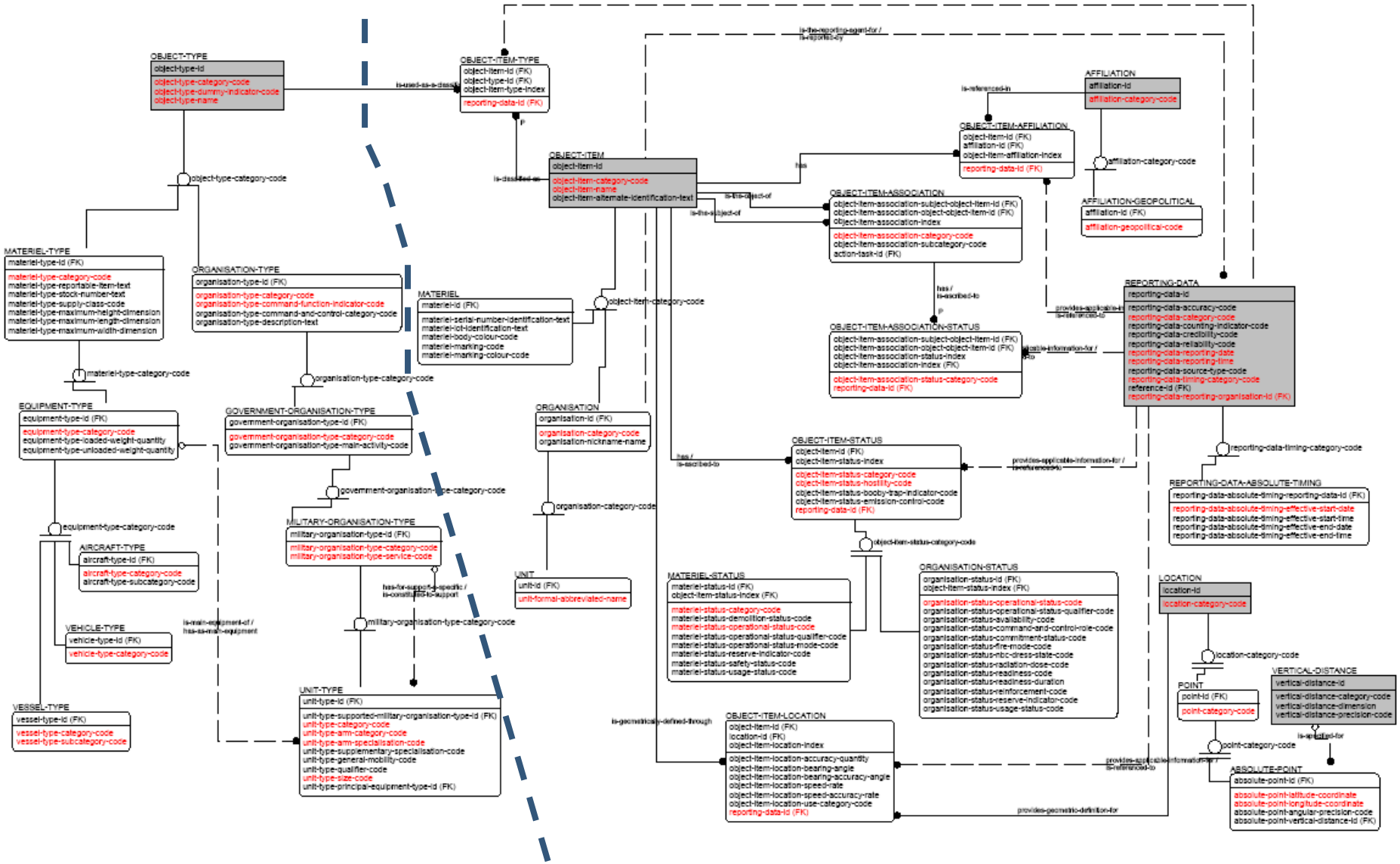


Extra slides

Mini MIP (30/240)

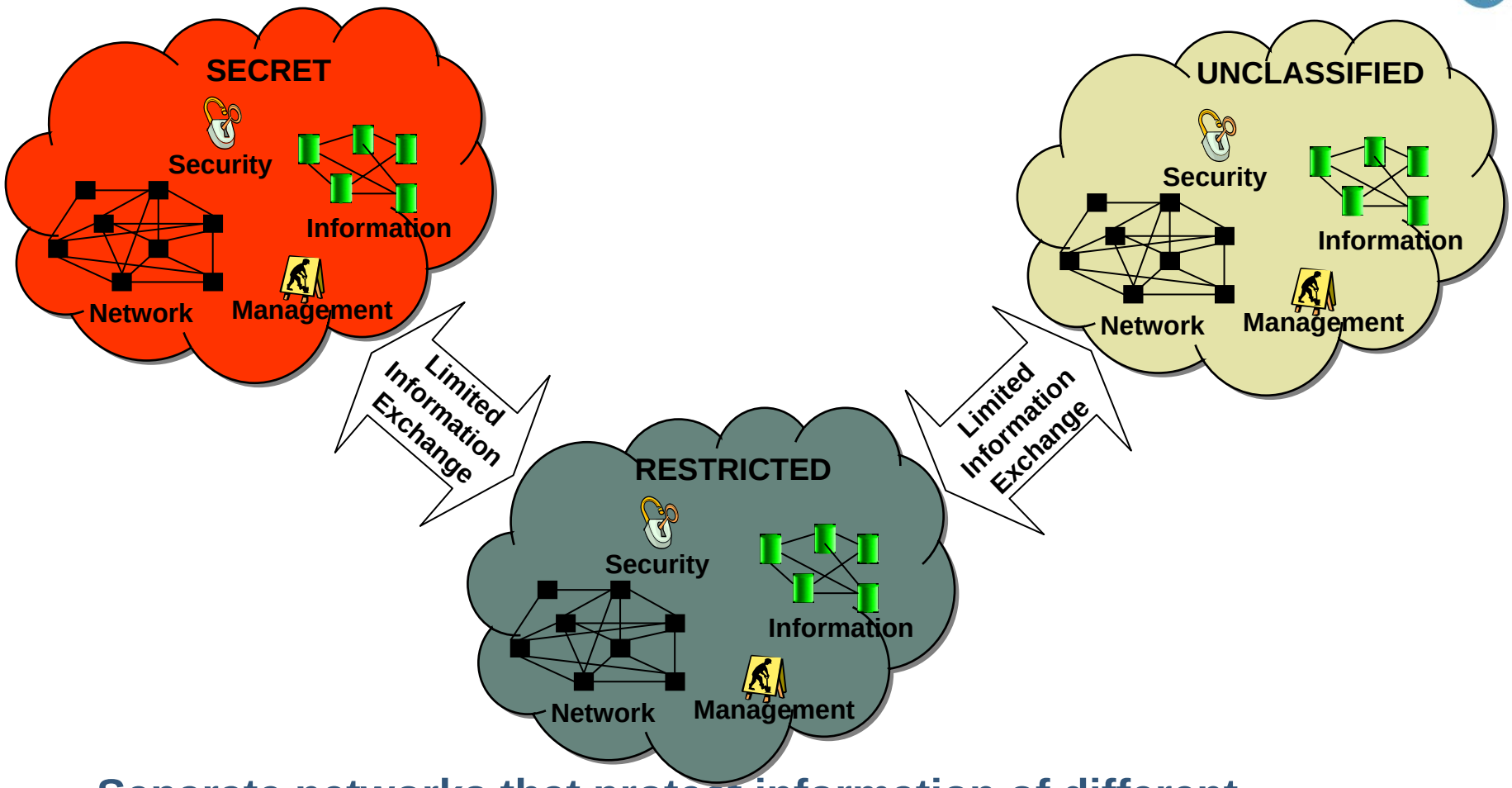
MINI MIP2 -- Annex A Logical / Logical View

MINI MIP 22.02.2006
Based on C2IEDM 6.15e



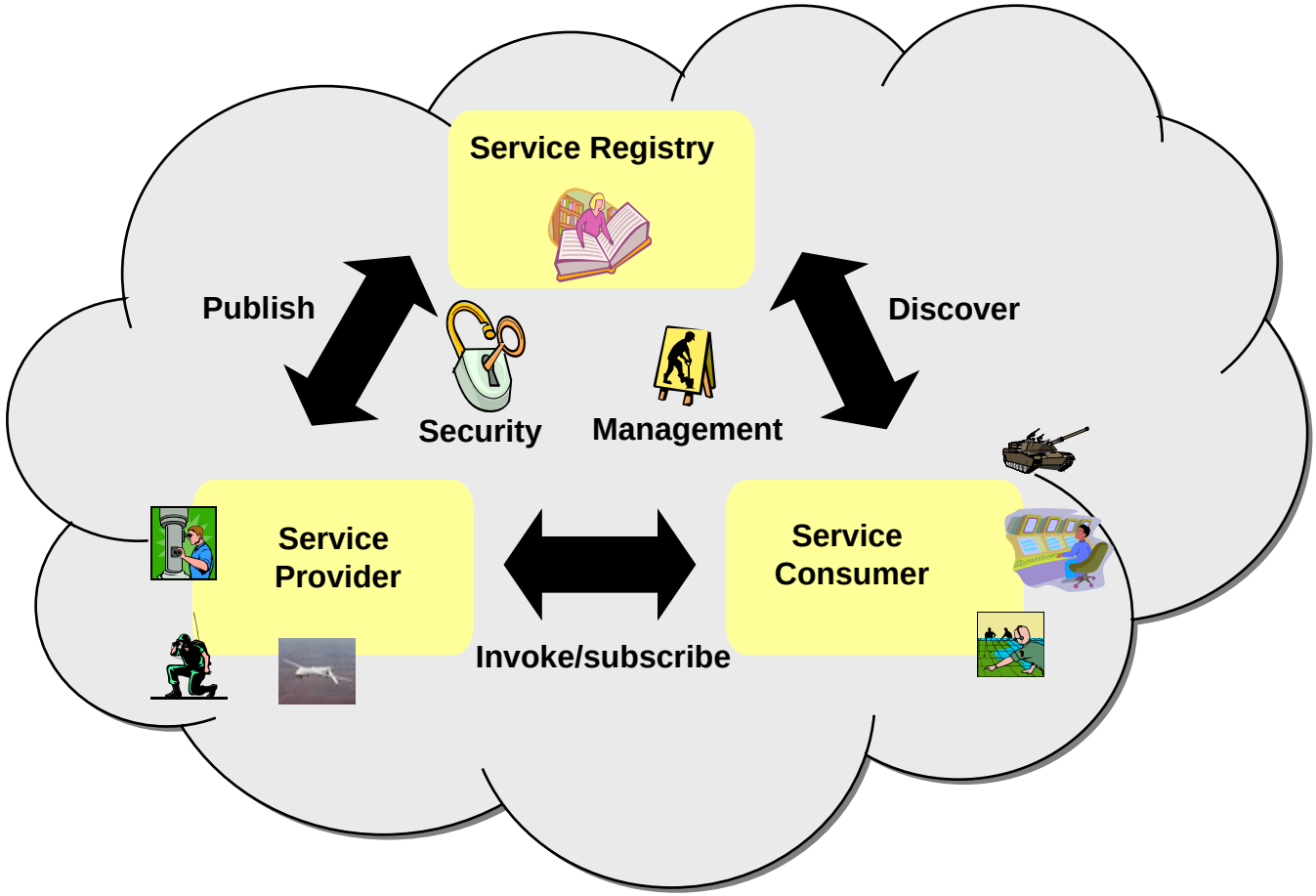
Current Status

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