



Design and Implementation of a File Transfer and Web Services Guard Employing Cryptographically Secured XML Security Labels

Andreas Thümmel, Knut Eckstein

**CIS Division, NATO C3 Agency
The Hague, The Netherlands**





Agenda

- NATO IA / Secure information sharing challenges
 - Guards / cross domain solutions (CDS)
 - Labeling
- Use cases: File transfer and web services
- NC3A XML Security Label Standardization Proposal
- Guard Prototype Architecture
- XML cross domain IA challenges
- Demo



NATO IA Challenges

- NATO S – Nat S solutions to be accredited by Nations and NATO
- Solutions should be usable for Nat S to Nat S as well
- Cost effective, affordable solutions sought
- Support cutting edge as well as legacy technologies
- Digitally signed, “reliable” labels
- Should transcend individual application environments
- Support labeling of non-XML and (complex) XML data



CDS Use Case I

- High -> low transfer of releasable document (parts)
- Human (creator) to human (consumer) transaction
- “Real time” information sharing
 - No replication via “swivel chair”
 - Automated document redaction (no manual generation of releasable version)
- Pre-approved list of document types and formats
- Low -> high browsing – *NOT* Internet browsing



CDS Use Case II

- Bi-directional web services across domains
- NATO/national core enterprise services federation
- Machine (WS requestor) to machine (WS provider)
- Pre-approved list of message types
- Automated message redaction (no additional implementation of “NATO releasable” web service message types)



Use Cases Common Characteristics

- XML security labels
- Processing XML infosets
- Release “granularity” at XML information item level
- HTTP as transport mechanism
- Adaptable to multiple guard platforms

**Application
Layer**

**HTTP Middleware
Layer**

OS Layer

NC3A Security Label Proposal

- Employs XML DSIG references to entire documents (URIs) or XML document parts (XPointer, XPath)
- Groups references of same classification and caveat into LabeledObjectGroups



