CEN

WORKSHOP

AGREEMENT

CWA 15537

April 2006

ICS 13.200

English version

Network Enabled Abilities - Service-Oriented Architecture for civilian and military crisis management

This CEN Workshop Agreement has been drafted and approved by a Workshop of representatives of interested parties, the constitution of which is indicated in the foreword of this Workshop Agreement.

The formal process followed by the Workshop in the development of this Workshop Agreement has been endorsed by the National Members of CEN but neither the National Members of CEN nor the CEN Management Centre can be held accountable for the technical content of this CEN Workshop Agreement or possible conflicts with standards or legislation.

This CEN Workshop Agreement can in no way be held as being an official standard developed by CEN and its Members.

This CEN Workshop Agreement is publicly available as a reference document from the CEN Members National Standard Bodies.

CEN members are the national standards bodies of Austria, Belgium, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Norway, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden, Switzerland and United Kingdom.

EUROPEAN COMMITTEE FOR STANDARDIZATION
COMITÉ EUROPÉEN DE NORMALISATION
EUROPÄISCHES KOMITEE FÜR NORMUNG

Management Centre: rue de Stassart, 36 B-1050 Brussels

© 2006 CEN All rights of exploitation in any form and by any means reserved worldwide for CEN national Members.

Ref. No.:CWA 15537:2006 E

Contents

Contents 2
Foreword 5
Introduction 6
1 Scope 7
2 References 7
3 Definitions, symbols and abbreviations 7
3.1 Definitions 7
3.2 Symbols 8
3.3 Abbreviations 8
4 Service-Oriented Architecture 13
4.1 Motivation 13
4.2 Architecture requirements 13
4.2.1 Location transparency 13
4.2.2 Formal service descriptions 14
4.2.3 Security principles 14
4.2.4 Reuse of infrastructure components and code 14
4.2.5 Dynamic configuration 15
4.2.6 Logical architecture 15
4.2.7 Physical Architecture 16
4.2.8 Other service architectures 16
4.3 Lifecycle processes 16
4.3.1 The NEA environment 16
4.3.2 Establishing the NEA environment 17
4.3.3 Specification of service types 17
4.3.4 Development of services 17
4.3.5 Deployment of services 18
4.3.6 Development of applications 18
4.3.7 Deployment and execution of application instances 18
5 Items of a network enabled abilities environment 18
5.1 General summary 18
5.1.1 Items 18
5.1.2 Non-service based applications 19
5.1.3 Communities of interest 19
5.1.4 Relevant standards 20
5.2 Policies 20
5.2.1 General 20
5.2.2 Policy: Directories 21
5.2.3 Policy: Security 21
5.2.4 Policy: Metadata 22
5.2.5 Policy: Ontology 23
5.2.6 Policy: Service definition 23
5.2.7 Policy: Quality of services 23
5.2.8 Policy: Modelling language 24
5.2.9 Policy: Commercial conditions 24
5.2.10 Policy: System chaining 24
5.3 Service area: Infrastructure and enablers 24
5.3.1 General 24
5.3.2 Service: Service repository 25
5.3.3 Service: Service registry 25
5.3.4 Service: Application repository 25
5.3.5 Security concept: Authentication 25
5.3.6 Security concept: Identification 26

5.3.7 Security concept: Roles, definition 26
5.3.8 Security concept: Authorization 26
5.3.9 Security concept: Certificate 26
5.3.10 Security concept: Letter of credit 27
5.3.11 Security concept: Access control 27
5.3.12 Security concept: Keys and key distribution 27
5.3.13 Security concept: Trusted credential 28
5.3.14 Security concept: Digital signing 28
5.3.15 Security concept: Non repudiation 28
5.3.16 Security concept: Data integrity 28
5.3.17 Security concept: Confidentiality 28
5.3.18 Security concept: Auditing 28
5.3.19 Security concept: Flow control 28
5.3.20 Security concept: Security policy monitoring 29
5.3.21 Security concept: Security information sharing 29
5.3.22 Service area: Contract and payment 29
5.3.23 Concept: Help desk 31
5.3.24 Concept: Computer-based training 31
5.3.25 Concept: Tutorials 31
5.3.26 Concept: Testing 31
5.3.27 Concept: Software Engineering (Development) 31
5.3.28 Service: Time 32
5.3.29 Concept: Quality of Services supervision 32
5.3.30 Service: Catalogue 32
5.3.31 Concept: Publish/subscribe 32
5.3.32 Concept: Broadcasting 32
5.3.33 Service: Events 33
5.3.34 Service: Telephone and video conference 33
5.3.35 Concept: Systems and resources management 34
5.3.36 Concept: Security Management 34
5.3.37 Concept: Service management 35
5.3.38 Concept: Instant messaging 35
5.3.39 Service: Messaging Services 35
5.4 Service area: Geographic information services 36
5.4.1 General 36
5.4.2 Service: Geographic feature service 36
5.4.3 Service: Map service 37
5.4.4 Service: Positioning service 37
5.4.5 Service: Coordinate transformation services 38
5.4.6 Other identified geographic services 38
5.5 Service area: Information management and information sharing 38
5.5.1 General 38
5.5.2 Service: Data management and publishing 39
5.5.3 Service: Data storage 39
5.5.4 Service: Data visibility services 40
5.5.5 Service: Shared space and accessibility 40
5.5.6 Service: Metadata registry and discovery 40
5.5.7 Service: Publish and subscribe 41
5.5.8 Service: Data replication and synchronizing 42
5.5.9 Service: Time synchronisation 43
5.5.10 Service: Data warehousing 43
5.5.11 Service: Information fusion 43
5.5.12 Service: Data mediating 43
5.5.13 Concept: Ontology 44
5.5.14 Service: Sensor data access 44
5.5.15 Service: Sensor coverage information 45
5.6 Service area: Legislation 45
5.6.1 Service: Lawful interception 45
5.6.2 Other identified legislation items 45
5.7 Service area: Traffic monitoring and control 45
5.7.1 General 45

5.7.2 Standards 45
5.7.3 Traffic management services 46
5.7.4 Route planning services 46
5.7.5 Navigation services 46
5.7.6 Vehicle tracking services 46
5.8 Service area: Situation picture 46
5.8.1 General 46
5.8.2 Service: Subject based picture 47
5.8.3 Service: Role based picture 47
5.8.4 Service: Picture of interest 47
5.8.5 Service: Scaleable level of detail 48
5.8.6 Service: Overlay service 48
5.8.7 Service: Information capturing 48
5.8.8 Service: Information filtering 48
5.8.9 Service: Information analysis 48
5.8.10 Service: History tracking 48
5.8.11 Service: Alert & info service 48
5.8.12 Service: Export service 49
5.8.13 Service: Content management 49
5.8.14 Service: Source management 49
5.8.15 Service: Role management 49
5.8.16 Service: Visualization management 49
5.9 Service area: Decision support services 49
5.10 Other items specific for a community of interest 49

Annex A - Inventory of ongoing projects (informative) 50

Foreword

This CEN Workshop Agreement has been developed by the CEN/ISSS Workshop on Network Enabled Abilities (WS/NEA), launched on 22 September 2004.

Workshop meetings took place on 24-25 November 2004 (Brussels), 2-3 February 2005 (Brussels), 2-4 May 2005 (Stockholm), 28-29 September (Brussels) and 7-8 February 2006 (Brussels).

An electronic endorsement process of the CWA, resulting from the last meeting, was organized, which started on 22 February 2006 and ended on 9 March 2006. This endorsement process demonstrated the consensus reached within the Workshop.

The final document was sent on 21 March 2006 to the CEN Management Centre for publication.

The document has been developed through the collaboration of a number of contributing partners, representing a wide mix of interests. The list of participants supporting this CEN Workshop Agreement is:

Bundesamt für Wehrtechnik und Beschaffung (Germany)
Bundeswehr IT-Office (Germany)
DGA, French Defence Standardisation Center
EADS Defence and Security Systems SA
EADS Deutschland GmbH
EADS Telecom
Eberhardt Consulting
Ericsson Microwave Systems AB
ESG Elektroniksystem- und Logistik- GmbH
German delegation to NATO
IT-Consulting Hase
National Land Survey of Sweden
PKN, Polish Committee for Standardization
Polish Ministry of Home Affairs
Rheinmetall Defence Electronics GmbH
Ruag Electronics
Saab Aerotech
Saab Systems
SIST, Slovenian Institute for Standardization
Swedish Armed Forces
Swedish Defence Materiel Administration
Swedish Emergency Management Agency

This CEN Workshop Agreement is publicly available as a reference document from the National Members of CEN: AENOR, AFNOR, ASRO, BSI, CSNI, CYS, DIN, DS, ELOT, EVS, IBN, IPQ, IST, LVS, LST, MSA, MSZT, NEN, NSAI, ON, PKN, SEE, SIS, SIST, SFS, SN, SNV, SUTN and UNI.

This CEN Workshop Agreement is publicly available as a reference document from the National Members of CEN. Comments or suggestions from the users of the CEN Workshop Agreement are welcome and should be addressed to the CEN Management Centre.

Introduction

The overall strategic objective of this CEN Workshop Agreement (CWA) is to make more efficient use of multi-national resources in command and control of future European network centric operations (i.e. military as well as civilian operations), e.g. search and rescue operations and environmental protection operations. Such combined military and civil operations include armed forces, police, coast guard, and emergency agencies, etc. Network Enabled Abilities, NEA, address information system abilities for such network centric operations.

This CWA promotes a Service-Oriented Architecture to be used for Network Enabled Abilities, including the aspects to be considered during development and implementation. The Service-Oriented Architecture makes it possible to utilize resources anywhere in a network; they do not have to be channelled to a specific centre or command post.

This CWA promotes an open environment with utilization of common standards. Required functionality, such as maps, radar pictures, live video pictures, weather information, and use of various types of forces, is described as services. For each service, relevant standards, or the need for standards, are listed.

The name "Network Enabled Abilities" and the acronym NEA was chosen in 2001 to also include homeland security and civil emergency operations and, at that time, the discussion on network centric operations was mainly military driven. Today, NEA seems to be equivalent to network centric operations (NCO) or Network Enabled Capabilities (NEC).

1 Scope

This CWA specifies services and other items mandatory or optional for a Network Enabled Abilities environment. It also includes an inventory of standards and standard-like specifications applicable to each such item. These items include recommended general principles and framework for system design, overall architectures, generic functionality to be considered, concepts, conventions and terminology in order to ensure an optimum multi-purpose interoperability, in particular of national and multi-national military and civil operations.

This CWA is applicable to the full life cycle of information system abilities for network centric operations, including specification, development, deployment, registration, and execution.

The main audience of this document is individuals and organisations participating in the further development of information system abilities for network centric operations.

The identification of services and other items of a NEA environment is non-exhaustive. The items were originally identified as a result of the examination of a number of scenarios.

There might also be other standards and standardisation initiatives than those identified in this CWA. The listed standards are to be regarded as relevant standards known by the workshop participants. However, where there are no standards listed, this might indicate that NEA-specific standards have to be developed.

The evaluation and selection of standards for NEA is identified as a very important task. Yet this is beyond the scope of this CWA and regarded as the subject of a future CWA or standard.

Specifications for design of products and commercial services, decisions on technologies or development of specific applications are issues not in the scope of this CWA.

2 References

This document is an inventory of standards and other specifications relevant for NEA. Due to this, references of these standards and specifications are made at the location where they are mentioned in the document (Chapter 5 - **Items of a network enabled abilities environment**).

3 Definitions, symbols and abbreviations

3.1 Definitions

network centric operations
operations combining military and civil resources

Network Enabled Abilities
information system abilities for network centric operations

NEA environment
environment for managing the full life cycle of network enabled abilities

service area
an abstraction of a set of service types

service
functionality provided through communication and information systems described by an interface
NOTE ISO/IEC TR 14252 defines a service as "distinct part of the functionality that is provided by an entity through interfaces"

service consumer
actor that initiates an execution of a service by making a request

service description
formal specification of a service instance

service implementation
software application implementing the interface of a service

service instance
service implementation deployed by a service provider

Service-Oriented Architecture
software technology for building systems using loosely coupled functions

service provider
actor that executes a service on reception of a request

service registry
directory of available deployed services

service repository
directory for managing services through their full lifecycles, including development and deployment

service type
abstraction of service instances with the same interface

Web Services
specific Software Oriented Architecture specified by W3C

3.2 Symbols

N/A

3.3 Abbreviations

AAA	Authentication, Authorization and Accounting
ACM	Association for Computing Machinery
AFS	Andrew File System
AGLS	Australian Government Locator Service
AIFF	Audio Interchange File Format
B2B	Business to Business
BPEL	Business Process Execution Language
BSM	Base Service Model
CAP	Common Alerting Protocol
CBT	Computer Based Training
CEN	Comité Européen de Normalisation (European Committee for Standardization)
CIFS	Common Internet File System
COM	Common Object Model
CORBA	Common Request Broker Architecture???
CRISP-DM	CRoss Industry Standard Process for Data Mining

CROP	Common Relevant Operational Picture
CWA	CEN Workshop Agreement
CWM	Common Warehouse Metadata
DAP	Digital Audio Broadcasting
DCMI	Dublin Core Metadata Initiative
DDF	Disk Data Format
DDMS	Department of Defense Discovery Metadata Specification
DDS	Data Distribution Service
DGI	Digital Geospatial Information
DGIWG	Digital Geospatial Information Working Group
DISA	Defence Information Systems Agency
DoD	Department of Defense
EAP	Extensible Authentication Protocol
ebXML	Electronic Business using eXtensible Markup Language
EDXL	Emergency Data Exchange Language
ETSI	European Telecommunications Standards Institute
FCIP	Fibre Channel over IP
FTP	File Transfer Protocol
GIF	Graphics Interchange Format
GML	Geography Markup Language
GPS	Global Positioning System
HMAC	Hash Message Authentication Code
HTTP	Hypertext Transfer Protocol
ICT	Information and Communication Technology
IEC	International Electrotechnical Commission
IETF	Internet Engineering Task Force
INSPIRE	Infrastructure for Spatial Information in Europe
IP	Internet Protocol
IPIWG	Intelligence Projects Integrated Working Group
IRC	Internet Relay Chat Protocol
IRIS	Infrastructure for Resilient Internet Systems
iSCSI	Internet SCSI
ISDN	Integrated Services Digital Network
ISO	International Standards Organization

IT	Information Technology
ITCM	Information Technology and Crisis Management
ITIL	Information Technology Infrastructure Library
JC3IEDM	Joint Command, Control, Computer Interoperability Exchange Data Model
JDM	Java Data Mining
JEP	Java Mathematical Expression Parser
JMS	Java Messaging Service
JPEG	Joint Photographic Experts Group
JSR	Java Specification Request
LDAP	Lightweight Directory Access Protocol
LI	Lawful Interception
MAC	Message Authentication Code
MDR	Metadata Registry
MIP	Multilateral Interoperability Programme
MOF	Meta-Object Facility
NAS	Network-attached storage
NASA	National Aeronautics and Space Administration
NATO	North Atlantic Treaty Organisation
NCES	National Center for Education Statistics
NCO	Network Centric Operations
NCOIC	Network Centric Operations Industrial Consortium
NCW	Network Centric Warfare
NDAG	NATO Data Administration Group
NDDS	Network Data Distribution Service
NEA	Network Enabled Abilities
NEC	Network Enabled Capabilities
NNTP	Network News Transport Protocol
NTP	Network Time Protocol
NTP	Network Time Protocol
OASIS	Organization for the Advancement of Structured Information Standards (http://www.oasis-open.org)
OASIS	Organization for the Advancement of Structured Information Standards
OGC	Open Geospatial Consortium
OGSI	Open Grid Service Infrastructure
OLAP	Online Analytical Processing

OLE	Object Linking and Embedding
OLE DB	Object Linking and Embedding Data Base
OMA	Open Mobile Alliance
OMG	Object Management Group
OWL	Ontology Web Language
P2P	Peer to Peer
PHP	Personal Home Page
PHP	PHP Hypertext Preprocessor
PMML	Predictive Model Markup Language
QoS	Quality of Service
RADIUS	Remote Authentication Dial In User Service
RAID	Redundant Array of Independent Disks
RDF	Resource Description Framework
RFC	Remote Function Call
RMI	Remote Method Invocation
RSS	Really Simple Syndication
RTPS	Real-Time Publish-Subscribe
SAML	Security Assertion Markup Language
SAN	Storage Area Network
SCSI	Small Computer System Interface
SDK	Software Development Kit
SensorML	Sensor Modelling Language
SFTP	Simple File Transfer Protocol
SLD	Styled Layer Description
SMI-S	Storage Management Initiative Specification
SOA	Service Oriented Architecture
SOAP	Simple Object Access Protocol
SQL	Structured Query Language
SSL	Secure Sockets Layer
SUMO	Suggested Upper Merged Ontology
SyncML	Synchronization Markup Language
TACACS	Terminal Access Controller Access Control System
TADIL	Tactical Digital Information Links
TC	Technical Committee

TCP	Transmission Control Protocol
TFTP	Trivial File Transfer Protocol
TIBCO	
TLS	Transport Layer Security
TSCP	Transatlantic Secure Collaboration Program
UDDI	Universal Description, Discovery and Integration
UML	Unified Modelling Language
US	United States
W3C	World Wide Web Consortium
WCS	Web Coverage Server
WebNFS	Web Network File System
WFS	Web Feature Server
WG	Working Group
WMS	Web Map Server
WS	Web Service
WSDL	Web Services Description Language
WSRF	Web Service Resource Framework
XACML	eXtensible Access Control Markup Language
XKMS	XML Key Management Specification
XMI	XML Metadata Interchange
XML	eXtensible Markup Language
XML ENC	XML Encryption
XML-DSIG	XML Digital Signature

4 Service-Oriented Architecture

4.1 Motivation

Today, Service-Oriented Architecture (SOA) is seen as the enabler for distributed systems, in particular for systems supporting network centric operations. Advantage of enhanced flexibility and robustness due to the concept of loosely coupling makes it possible to implement highly complex, distributed systems while also incorporating legacy systems and applications.

The Service-Oriented Architecture reflects the way organisations work in a way that makes the architecture easy to comprehend and feasible to provide powerful solutions for complex real life problems throughout all organisational levels. Functionality which is implemented once by the best developers in the field can be used by many applications all across the network. Improvements can affect the whole network immediately.

Through a directory mechanism, services can be registered together with documentation about their interface and their functionality. This makes them available to be used by other services or applications. Several services with similar or the same functionality can compete ensuring the best quality service to be used. Systems can be easily plugged in to the network and immediately offer their services to others in the network providing true plug-and-play on systems level.

This CWA has thus chosen to promote the Service-Oriented Approach to be used for NEA. This document specifies the concept of services and the main aspects to consider when developing and implementing services.

4.2 Architecture requirements

4.2.1 Location transparency

Location transparency is the ability to manage references to service providers outside the implementation of the service consumers. The most common way to do this is to use a service registry that acts as a directory for network locations and characteristics of available service instances. Figure 1 illustrates the relationship between the service consumer, the service provider (Producer in the figure) and the service registry (Location registry in the figure). The service provider publishes its services to the service registry. The service consumer looks up and finds the appropriate service instance and binds to the service provider in order to use the service.

1. It must be possible to manage references to service providers outside the implementation of the service consumers.

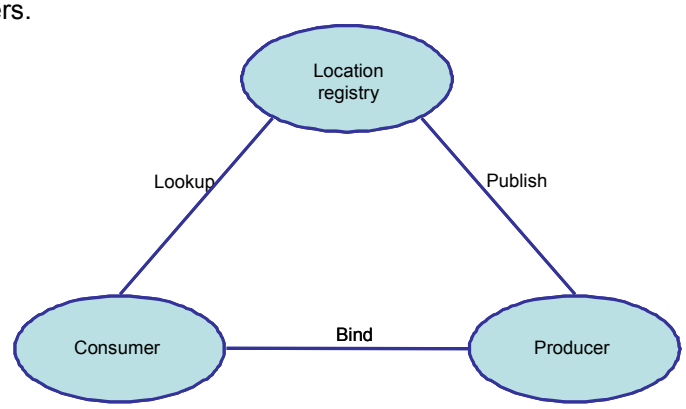

Figure 1 - The relationship between the service consumer, the service provider and the service registry.

4.2.2 Formal service descriptions

a) The service description should, as far as possible, be explicitly expressed in a formal language.

b) All information exchange between service providers and service consumers should be through the protocol and the formally defined interfaces in the service description.

c) The service description shall contain:

1) The achievement of a service

2) The allowed protocols to be used for information exchange

3) The interfaces that are used to exchange information between a service consumer and a service provider

4) The definition of the data types that are used in the interfaces

5) The properties that service consumers can use to distinguish between different implementations of a service

d) It shall be possible to extend service descriptions into new versions in such a way that service consumers and service providers implemented according to the old version can still function.

4.2.3 Security principles

a) Service consumers and service providers must be able to identify themselves using a common method for **authentication** of users and services.

b) There must be a common method and implementation of **authorization** of using services and data. Service providers must check that service consumers are authorized to use the service and obtain the required data before a service request is granted. The information about which users and services that are allowed to use other services must be possible to change dynamically. These changes are themselves subject to authorization.

c) There must be a universal method to obtain **integrity**. A service consumer must be able to check that the data sent from another part is not changed by a third part.

d) There must be a universal method to guarantee the **confidentiality** of the information exchanged. This means that it should not be possible for any outsider to get access to the information that is exchanged.

4.2.4 Reuse of infrastructure components and code

a) The information exchange description should be on a business information exchange abstraction level.

b) There should be an explicit interface between the business logic code and the information exchange code in order to be able to have separated lifecycles.

c) The implementations of the information exchange should, for cost effective reasons, be reused as much as possible.

4.2.5 Dynamic configuration

a) Service implementations must have the ability to be dynamically configured at run time.

b) In a service implementation there should be a separation of the business logic from the implementation of the communication protocols.

c) A service implementation should be able to select among many different communication protocols at the same time.

4.2.6 Logical architecture

Each layer at a service consumer communicates logically horizontally with the corresponding layer at a service provider. Messages are exchanged using a specific protocol for each layer. The services are delivered as messages at the highest level. The protocol is implemented by a protocol at the next lower layer, down to the lowest layer there physical transport is taking place.

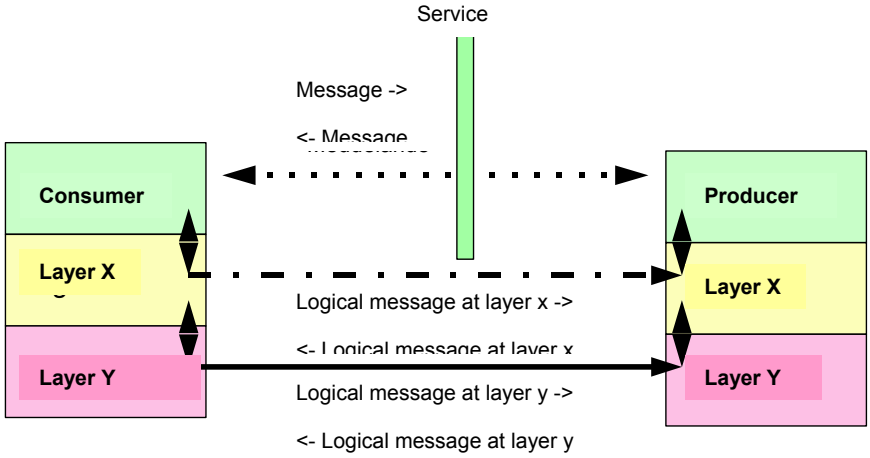

Figure 2 - Layered service architecture

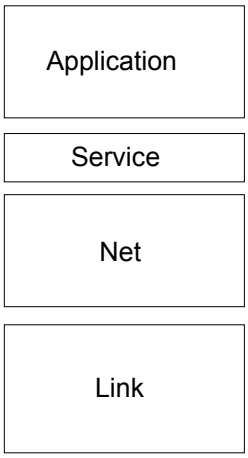

Figure 3 - Position of the service layer

Applications taking the roles as service consumers and service providers interface with the service layer.

Enabling services such as directories, authorisation, etc. are implemented by service provider applications presenting services at the service layer for service consumer applications to use.

4.2.7 Physical Architecture

Figure 4 provides an example of a “physical” architecture implementing the service infrastructure.

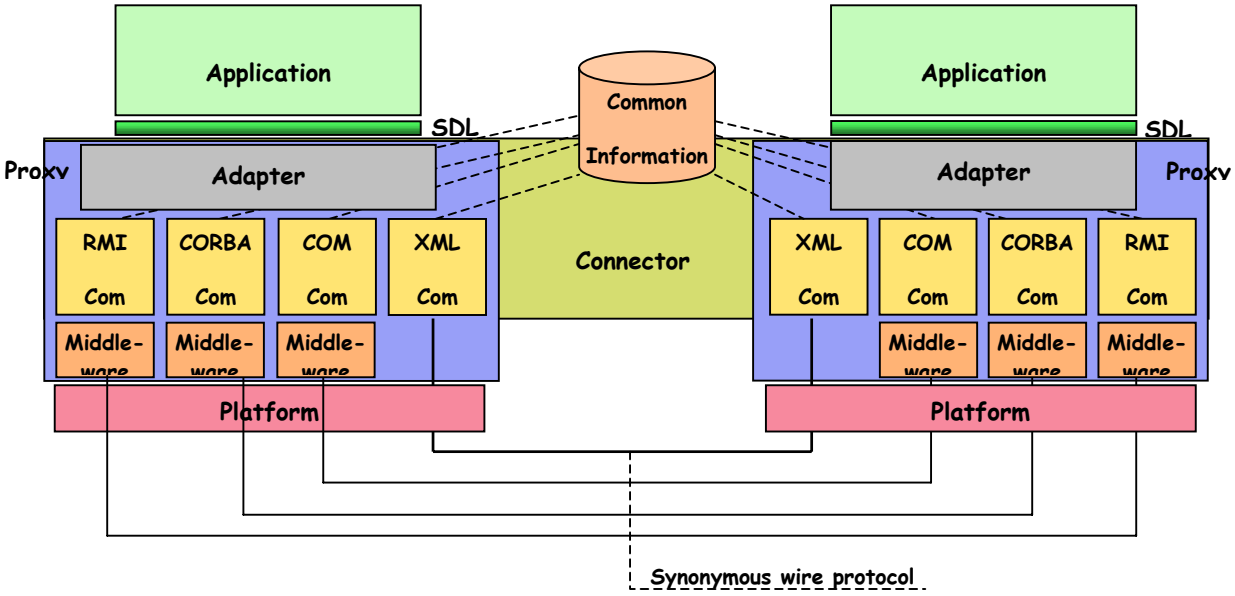

Figure 4 - Example of a physical architecture for services

4.2.8 Other service architectures

Other architectures for the implementation of specific parts of a service will exist, for example the logical architecture for the implementation of Web Service Security (5.2.3), or the conceptual architecture of e-business (5.3.22).

Other architectures, built on top of the service infrastructure and based on services, will have to be defined.

4.3 Lifecycle processes

4.3.1 The NEA environment

In a Service-Oriented Architecture, several aspects of the services have to be considered: specification, development, deployment, registration, look-up, evaluation, invocation, etc. The Network Enabled Abilities environment is required to provide functionality for these aspects.

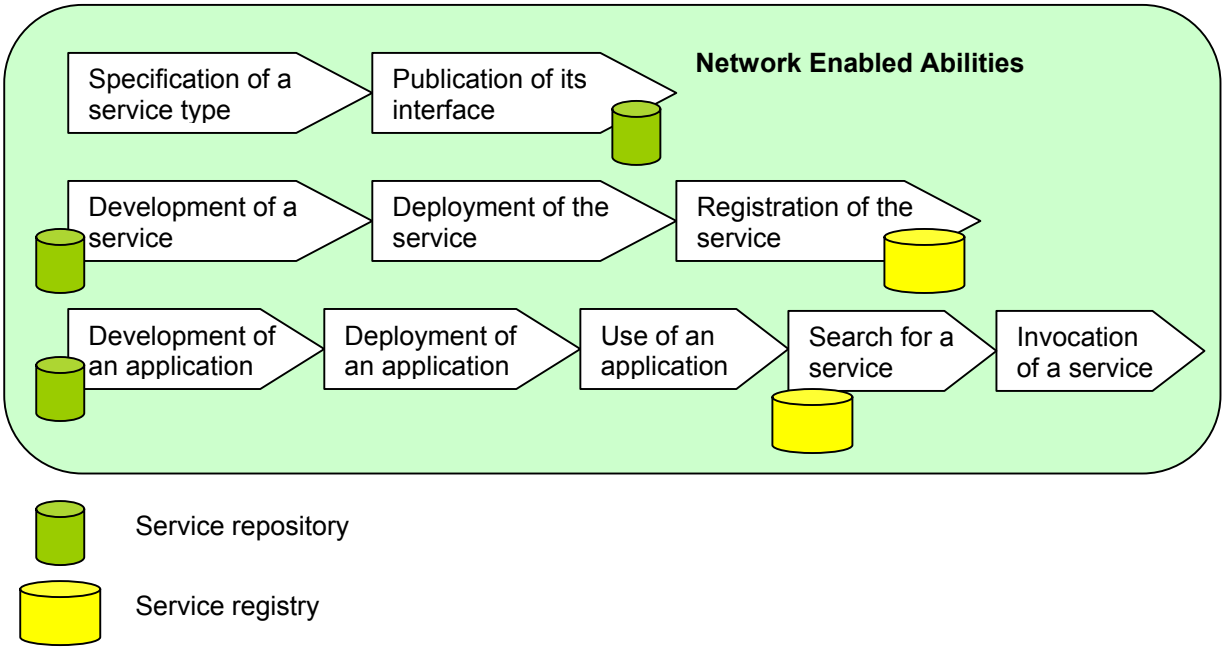

Figure 5 - The role of service repositories and service registries

4.3.2 Establishing the NEA environment

Services need an environment where they can be developed and used. This environment has to exist prior to the services. The process of establishing this environment contains several steps. Publishing this CWA is one of the first. Defining rules and setting up the required repository and registry servers are others.

4.3.3 Specification of service types

One of the greatest advantages of using services compared to using more traditional methods is that there may be multiple compatible services to choose from. Preferences on cost, data quality, availability, etc. may affect selection of the most appropriate one for each occasion. In order to achieve compatibility, service types have to be defined and knowledge about them has to be published.

Input to this process is:

- Description languages and methods
- General, established standards
- Established standards appropriate for the service type
- Location, description and schema for service type repository

Output from this process is published in a service repository:

- Description of the service type
- Schema for service interface
- Schema for service metadata

4.3.4 Development of services

A service implementation is the software that implements the service type. There may be multiple implementations of the same service type.

Input to this process is:

- Location, description and schema for service repository

- Description of the service
- Schema for service interface
- Schema for service metadata

Output is the software that can be deployed as a service. The software is not registered.

4.3.5 Deployment of services

A service instance is a specific execution of software that implements a service type. Deployment includes starting the execution and registering the service in a service registry.

Input to this process is

- The software
- Location, description and schema for service registry

4.3.6 Development of applications

An application is implemented based on one or several service types.

Input to this process is:

- Description of the service types to be used
- Schemas for service interfaces
- Schema for the service metadata
- Schema for registry information common for all services

Output is the application software.

4.3.7 Deployment and execution of application instances

Except for how to find the service registry service, no specific knowledge on services should be required when starting the application. The application may be able to find required services once during deployment or on demand during execution.

5 Items of a network enabled abilities environment

5.1 General summary

5.1.1 Items

The NEA environment contains various items required to specify, implement and utilise functionality in a large domain of interest:

- Policies - rules for organisations, individuals, services and applications on how to describe, publish, find and utilise services
- Infrastructure and enablers - functionality intended to support specification, implementation and execution of services and service based applications. Infrastructural services typically carry no direct business value for network centric operations.
- General services - services that are intended to be used across several communities of interest. Such services typically carry direct business values for network centric operations.
- Community of interest services - services with a direct business value for a specific community.

Services and other items are described as branches of a tree. The top-level structure is described in Figure 6.

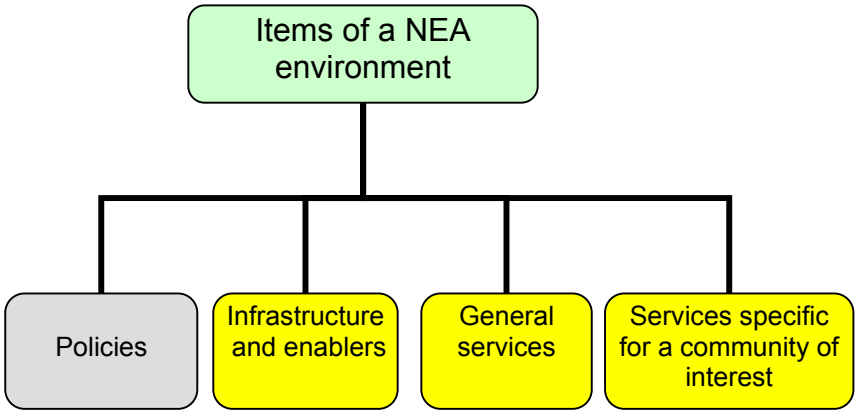

Figure 6 - Items of a NEA environment

Note that the identification of services and other items of a NEA environment is to be regarded as non-exhaustive.

5.1.2 Non-service based applications

For various reasons, all functionality in a NEA environment is not service based:

- a service is not a practical solution
- there are well-established solutions available and wide-spread
- it is important to be compatible with non-NEA environments

In this document, non-service based standards are listed with service-based ones.

5.1.3 Communities of interest

A community of interest is a group of actors (individuals or organisations) collaborating in a joint activity. The actors may come from different disciplines.

The “symmetry of ignorance” or “asymmetry of knowledge” among the different actors within a community of interest serves as a challenge to create new knowledge and shared understanding.

Some services have a direct business value for such a community but not for others (Figure 9) while other services - general services - have a value for almost any community of interest (Figure 7).

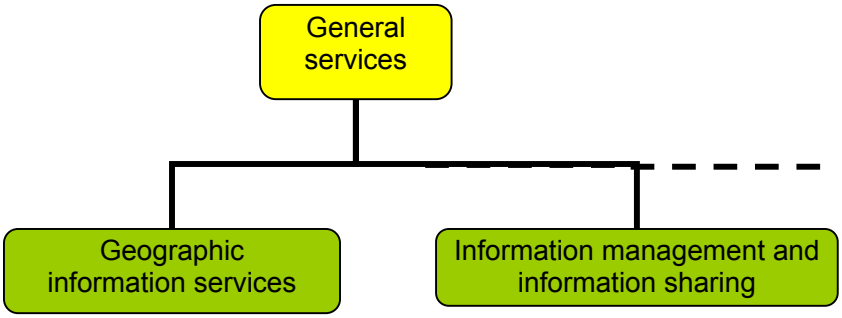

Figure 7 - General services are intended for several communities of interest

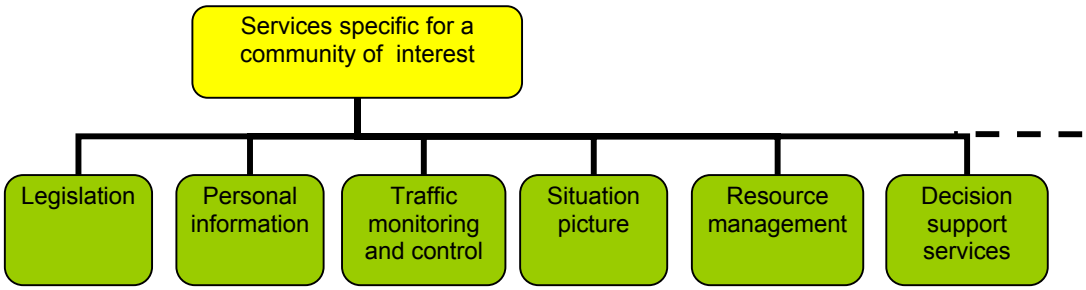

Figure 8 - Services specific for certain communities of interest

5.1.4 Relevant standards

The list of standards, standardisation initiatives and standards bodies provided for each item in this document should be regarded as non-exhaustive, that is, there might be other standards than those identified here. For each item, standards, standardisation initiatives and standards bodies are listed in bold face.

As standards are regarded all type of open specifications. Criteria for an open specification are:

- there must not be a licence cost for implementing the specification
- there must not be a cost for running systems built on the specification
- the specification must be developed and/or maintained in an open process

5.2 Policies

5.2.1 General

Policies for NEA are required for how to describe, publish, find and utilise services. They are rules intended for organisations, individuals, services and applications.

Web Services Policy Framework (WS-Policy) v 1.1 September 2004

This proposed standard, developed by W3, has to be tailored and complemented to meet the needs of NEA. This work is best done in cooperation with organisations such as W3C, Globus Alliance and OASIS.

Web Services Policy Assertions Language (WS-PolicyAssertions) Version 1.0 December 18, 2002

Web Services Policy Attachment (WS-PolicyAttachment) September 2004

5.2.2 Policy: Directories

Directories for advanced discovery, mediation and brokering of services is a relevant issue for NEA.

Through a directory mechanism, services can register together with the documentation about their interface and their functionality. This makes them available to be used by other services or applications.

A policy for directories should include issues such as:

- who is responsible for the directory
- who is allowed to register
- what is to be registered in the directory
- when to register and update
- who is allowed to read the directory

UDDI version 2.1

UDDI (Universal Description, Discovery and Integration) from W3C/OASIS is the native directory for Web Services. It is intended for service registries, that is, it can only be used to publish service instances. UDDI is under development and may in the future also work for service repositories that can store information for development and deployment of services.

W3C RFC2247 LDAP

LDAP/DAP is beside UDDI the most accepted standard for directories on Internet. It has however no service based API. No ongoing work has been identified on how to set up a service based API for LDAP.

Department of Defense Discovery Metadata Specification (DDMS) VERSION 1.3

OASIS ebXML E-business registry

5.2.3 Policy: Security

It is of outmost importance that sufficient and compatible security mechanisms are provided in NEA. This includes mechanisms that:

- clearly establish the identity and authority of the parties
- ensure integrity and security of information sent
- ensure that activities can be proved

The level of security required, as well as the mechanisms used, depends on the situation.

Security policies should include issues such as:

- how to define the required security mechanisms
- how to define the acceptable security mechanisms
- how to describe levels of different security aspects

Web Service Policy includes many basic security policies that should be complemented and further detailed to meet the needs of NEA: The work done in the military domain by e.g. the NCOIC consortium will in addition to the work within the W3C most likely provide input to this work.

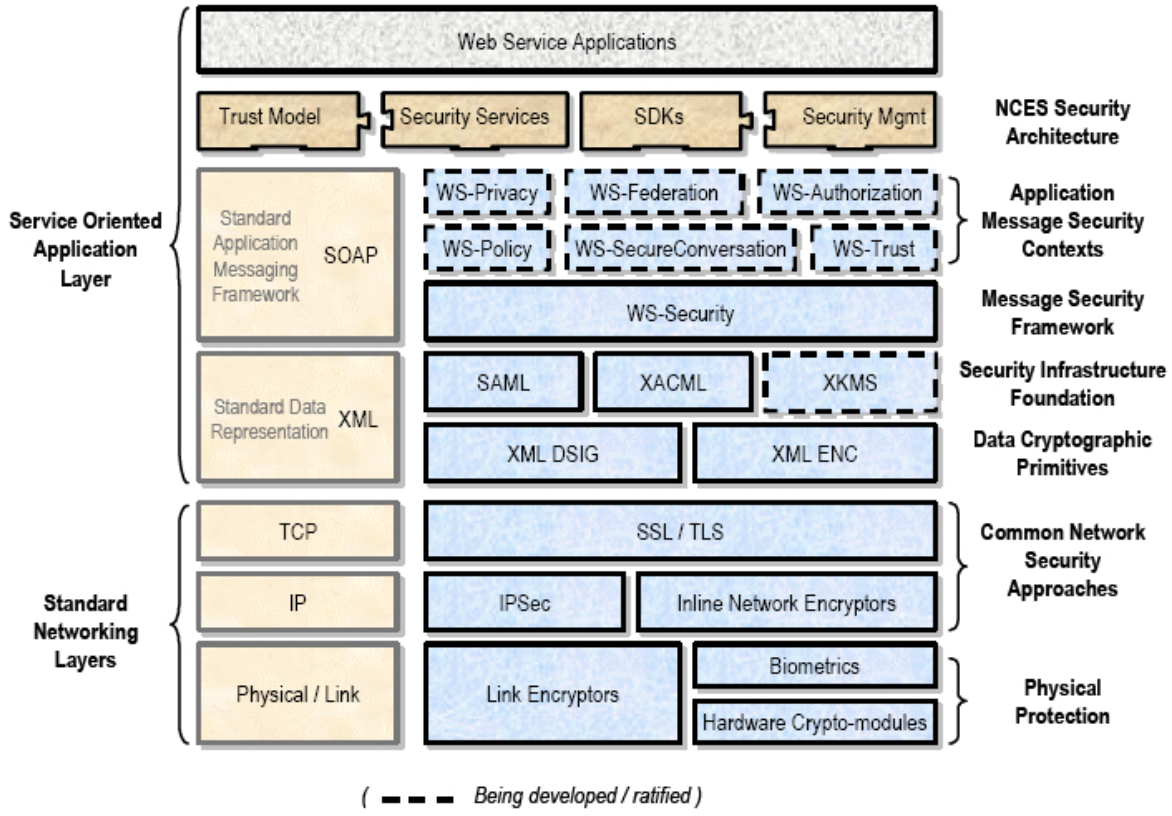

Figure 9 - Security stack standards

Web Services Security (WS-Security, OASIS WSS)

A standard jointly proposed by an industry consortium (IBM, Microsoft and Verisign) and currently being ratified by OASIS (named OASIS WSS). It serves as the foundation to address SOAP-level security issues, with three major propositions: (1) use of security tokens in SOAP headers for user identity and authentication, (2) use of XML-Signature standard for message integrity and authenticity, and (3) use of XML-Encryption for message confidentiality.

Security Assertion Mark-up Language (SAML)

This standard from Organization for the Advancement of Structured Information Standards (OASIS) defines a framework for exchanging security information in XML format. Security information such as authentication artefacts, authorization decisions, and subject attributes are represented in XML constructs called “assertions”, which are issued by SAML Authorities. SAML also defines the protocol, transport bindings, and usage profiles for exchanging the assertions. SAML maps seamlessly to the SOAP transport, and complements the WS-Security specification (see above).

5.2.4 Policy: Metadata

Metadata serve several purposes. First of all a meta-model defining the relations between the components of the service concept and the service definition items shall be established.

Second it shall be used to register information about services, such as who is responsible, version number, status etc in addition to other information in a catalogue.

Third, metadata defining the items as used for e.g. representing information used within a service shall be established. This will e.g. allow for the exchange of information that has not been previously defined, allowing for the relevant information to be dynamically discovered at runtime by evaluation of the associated metadata.

XML and XML Schema

Natural starting point for defining metadata for information related to services.

ISO 11179 Metadata Registries

ISO 15489 Records Management

US DOD Discovery Metadata Specification

XML Schema

IPIWG Metadata Standard

Metadata for images

Format related metadata includes JPEG, GIF, AIFF etc.

Policies for Namespaces (exist e.g. in Nato)

This is clearly an area relevant for further work within NEA.

Department of Defence Discovery Metadata Specification (DDMS) VERSION 1.3

5.2.5 Policy: Ontology

In order to enable more advanced service discovery mechanisms, there must be ways of expressing semantic properties of services.

OWL Web Ontology Language W3C Recommendation 10 February 2004

W3C OWL-S

This standard for service ontologies is still in its infancy. It is a good starting point for further work.

OWL-S is a core set of mark-up language constructs for describing the properties and capabilities of Web Services in unambiguous, computer-interpretable form.

5.2.6 Policy: Service definition

Web Services Description Language (WSDL 1.1)

This W3C standard is the established standard for service definition. It is only applicable for simple functional type of information services and has to be complemented to fully define a service. This is an issue that is explored within the SOA community, but no ready solutions exist at this point in time. Further development should be done in co-operation with organisations such as OASIS and NCOIC.

ISO 19119 Geographic Information – Services

LT1K P04-0278 Framework Service Description

5.2.7 Policy: Quality of services

Among the attributes defined for a service, QoS is one of the most important.
This is a clearly relevant area for NEA.

OMG QoS metamodel

This can be used as a base.

OMG UML Profile for Modelling Quality of Services and Fault Tolerance Characteristics & Mechanisms (ptc/04-09-01)

UML Profile for Schedulability, Performance, and Time Specification

IETF RFC 2460 RFC 2460 Internet Protocol, Version 6 (IPv6)

Point 6 Flow Labels and Appendix A describe the Flow labels.

5.2.8 Policy: Modeling language

The OMG Model-Driven Architecture effort is an excellent technology enabling a separation by the logical model of a service and the possible instantiations in various platforms or solution architectures. This will enable service definitions that can be shared between different technical implementations, including a possibility to survive into future technological solutions.

OMG UML 2.0

OMG UML is the industry standard modelling language. The ongoing work within OMG related to SOA is very relevant for NEA.

OMG XMI 2.1

MOF 2.0

5.2.9 Policy: Commercial conditions

Some services will include costs that have to be paid by the users. As part of the service policy, the relevant applicable ways of regulating payment has to be defined.

OASIS

The OASIS standards organisation can most likely provide some input. See text later on in the document.

5.2.10 Policy: System chaining

In order to achieve larger tasks it must be possible to combine services in ways that are not pre-defined by the service providers.

ISO 19119 - Geographic information - Services

This standard specifies a mechanism called *service chaining* based on the Open Distributed Platform standard [ISO/IEC 10746-2].

5.3 Service area: Infrastructure and enablers

5.3.1 General

The NEA environment is an infrastructure that requires a limited set of basic services supporting the full life cycle of services: building, registering, publishing, finding, managing, etc.

Using services in network centric operations require security. Security solutions for granting identity and for data integrity will handle certain security aspects - they have to implement certain security concepts. It is important that two systems that needs to interoperate are compatible with regards to the implemented security concepts

Functionality needed for support of NEA is not always available as service-oriented solutions but may still very important.

Standards within the area of infrastructure and enablers are mainly technology dependent. There are many standards that fall within this area. The attempt is to create a list with the standards that will affect NEA the most.

5.3.2 Service: Service repository

The idea behind service repositories is to enable sharing of service type definitions amongst different parties.

Web Services

In Web Services, the distinction between *service type* and *service instance* is weak. Therefore the Web Services way is to store references to the instances intermixed with the service type definitions see “5.3.3 Service: Service registry”.

5.3.3 Service: Service registry

Registries containing service instances enable service consumers to find services of a specific service type.

UDDI - Universal Description, Discovery, and Integration

A standard for a platform-independent, open framework for describing services on the Internet, suggested in September 6, 2000. UDDI is intended mainly for B2B enhancement and is based on the W3C's XML standard and, especially on SOAP.

More information can be found at http://www.uddi.org/

UDDI is the Web Services standard for storing service Web Service references.

WSDL

The public interface to the web service is described by Web Services Description Language. This is an XML-based service description on how to communicate using the web service.

5.3.4 Service: Application repository

With the advent of many efficient (enough) platform independent runtime environments, the idea of downloading applications over the net (when needed) has really taken off.

There are two principal repositories for applications:

- Client side applications
- Server side applications

The goal with application repositories is to distribute applications with ease and enable automatic update. The application repositories are technology dependent and no true standard exists.

WebStart

This is a technology for storing java applications on a web server making it possible to download them when needed.

PEAR - PHP Extension and Application Repository

http://pear.php.net/

5.3.5 Security concept: Authentication

Authentication is the process by which a computer, computer program, or another user attempts to confirm that the computer, computer program, or user from whom the second party has received some communication is, or is not, the claimed first party.

WS-Security

The Web Services Security protocol has been accepted as an OASIS standard. The standard allows authentication of actors and confidentiality of the messages sent. The standard is defined in:
http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-soap-message-security-1.0.pdf

Kerberos

This is a computer network authentication protocol which allows individuals communicating over an insecure network to prove their identity to one another in a secure manner. Kerberos is defined in:
http://www.ietf.org/rfc/rfc4120.txt

RADIUS - Remote Authentication Dial In User Service

This is an AAA (authentication, authorization and accounting) protocol for applications such as network access or IP mobility.
http://www.ietf.org/rfc/rfc2865.txt

TACACS+

This protocol provides access control for routers, network access servers and other networked computing devices via one or more centralized servers. TACACS+ provides separate authentication, authorization and accounting services.

EAP - Extensible Authentication Protocol

This is a universal authentication mechanism, frequently used in wireless networks and Point-to-Point connections. (EAP is pronounced "eep"),

HMAC

This is a keyed-hash message authentication code. It is a type of message authentication code (MAC) calculated using a cryptographic hash function in combination with a secret key. As with any MAC it may be used to simultaneously verify both the data integrity and the authenticity of a message.

5.3.6 Security concept: Identification

Identification is the act of identifying something without ambiguity.

5.3.7 Security concept: Roles, definition

The concept of Role is a logical grouping of users. One user can act as zero or more roles. This enables authorization management to be handled more efficient.

5.3.8 Security concept: Authorization

The authorization process is used to decide if person, program or device X is allowed to have access to data, functionality or service Y.

For standards see “5.3.5 Security concept: Authentication” since many of those standards handles authorization as well as authentication.

5.3.9 Security concept: Certificate

A digital certificate is an electronic document which links a public key to a person or a company in a public key infrastructure enabling the user(s) to send encrypted and digitally signed electronic messages. The certificate identifies the user and is required to verify his digital signature. The certificate contains information about the identity and public key of the person/company as well as the certificate's expiration date. Furthermore, the certificate may contain information about the usage of the certificate. Each certificate is signed with the private key of the CA. It vouches for an individual or organisational identity. A digital

certificate can be compared to a driver's license or an ID card in that it authorises the bearer to conduct certain operations, hence making it possible to secure e-business activities.

X.509

This is a widely used standard for defining digital certificates. X.509 is actually an ITU Recommendation, which means that it has not yet been officially defined or approved for standardized usage. As a result, companies have implemented the standard in different ways. For example, both Netscape and Microsoft use X.509 certificates to implement SSL in their Web servers and browsers. But an X.509 Certificate generated by Netscape may not be readable by Microsoft products, and vice versa.

5.3.10 Security concept: Letter of credit

A letter of credit, also referred to as an LOC or LC, is a document issued by a financial institution that essentially acts as an irrevocable guarantee of payment to a beneficiary.

5.3.11 Security concept: Access control

Access control refers first to the practice of restricting entrance to a facility or property to authorized persons, and secondly to the mechanisms which keep track of entries and exits (i.e. visitor's logs, security cameras) or prevent access by unauthorized persons (i.e. gates, electronic locks, biometrics).

Computer security access control includes Authentication, Authorization and Audit.

XML Access Control Markup Language (XACML).

This standard defines a generic authorization architecture and the constructs for expressing and exchanging access control policy information using XML. Policy constructs include policies, rules, combining algorithms, etc. XACML complements SAML so that not only policy decisions can be exchanged in a standard fashion, but policies themselves as well. Version 1.0 was ratified as an OASIS standard in February 2003.

5.3.12 Security concept: Keys and key distribution

A key is a piece of information that controls the operation of a cryptography algorithm. In encryption, a key specifies the particular transformation of plaintext into cipher text, or vice versa during decryption. Keys are also used in other cryptographic algorithms, such as digital signature schemes and keyed-hash functions (also known as MACs), often used for authentication.

There are two types of key algorithms:

- Asymmetric-key algorithms generally allow users to communicate securely without having prior access to a shared secret key, by using a pair of cryptographic keys, designated as public key and private key, which are related mathematically. The term asymmetric-key algorithms is a synonym for public key algorithms.
  Key distribution, this is done through public key servers. When a person creates a key-pair, he keeps one key private and the other, public-key, is uploaded to a server where it can be accessed by anyone to send the user a private, encrypted, message.

- Symmetric-key algorithms is where the encryption key is trivially related to the decryption key, in that they may be identical or there is a simple transform to go between the two keys. The keys, in practice, represent a shared secret between two or more parties that can be used to maintain a private information link.
  For symmetric key algorithms keys need to be changed often and kept secure during distribution and in service. The consequent requirement to choose, distribute and store keys without error and without loss is difficult. Distribution can be done physically and even embed the keys and the algorithms in hardware to assure secrecy.

XML Key Management Specification (XKMS)

This specification is a submission to W3C. It defines a set of abstract interfaces for the underlying private key infrastructure (PKI). The specification consists of two parts: X-KRSS and X-KISS (see below).

XML Key Registration Service Specification (X-KRSS)

This specification covers public key registration and revocation.

XML Key Information Service Specification (X-KISS)

This specification covers mechanisms for locating and validating keys.

5.3.13 Security concept: Trusted credential

Trust Negotiation is an approach to gradually establishing trust between strangers online through the iterative exchange of digital credentials. In contrast to a closed system, where the interacting entities have a pre-existing relationship (often proved by typing a username and password), trust negotiation is an open system, and complete strangers can build trust in one another. This is done by disclosing digital credentials.

5.3.14 Security concept: Digital signing

Digital signature (or public key digital signature) is a type of method for authenticating digital information analogous to ordinary physical signatures on paper, but implemented using techniques from the field of public key cryptography. A digital signature method generally defines two complementary algorithms, one for signing and the other for verification, and the output of the signing process is also called a digital signature.

XML-Signature (XMLDSIG)

This formal W3C recommendation covers the syntax and processing of digitally signing of selected elements in an XML document using either symmetric (secret) key or asymmetric (public/private) key cryptography.

5.3.15 Security concept: Non repudiation

With regards to digital security, non-repudiation means that it can be verified that the sender and the recipient were, in fact, the parties who claimed to send or receive the message, respectively. In other words, non-repudiation of origin proves that data has been sent, and non-repudiation of delivery proves it has been received.

5.3.16 Security concept: Data integrity

Data integrity has the following meaning that data is unchanged from its source and has not been accidentally or maliciously modified, altered, or destroyed.

5.3.17 Security concept: Confidentiality

The International Standards Organization (ISO) has defined Confidentiality as "ensuring that information is accessible only to those authorized to have access"

XML-Encryption (XMLENC)

This W3C recommendation for data confidentiality specifies the syntax and processing rules for encryption and decryption of selected elements in an XML document.

5.3.18 Security concept: Auditing

A computer security audit is a process that can verify that certain standards have been met, and identify areas in need of remediation or improvement.

5.3.19 Security concept: Flow control

The flow control mechanism is used for controlling the flow of data in a network under well-defined conditions, while congestion control is used for controlling the flow of data when congestion has actually occurred. Flow control mechanisms are classified by whether or not they have feedback.

5.3.20 Security concept: Security policy monitoring

Security policy monitoring is continuous monitoring of the security measures in order to achieve information security situation awareness. The concept includes the detection, analysis and prevention of policy violations and intrusion attempts.

ISO/IEC TR 18044 Information technology - Security techniques - Information security incident management

5.3.21 Security concept: Security information sharing

Security information sharing includes collection, reporting and distribution of security-relevant information such as advisories and incident reports.

Common Vulnerabilities and Exposures (CVE)

http://cve.mitre.org/

Common Announcement Interchange Format (CAIF)

http://cert.uni-stuttgart.de/projects/caif/

http://www.caif.info/

Incident Object Description and Exchange Format

http://www.ietf.org/internet-drafts/draft-ietf-inch-iodef-04.txt

http://www.terena.nl/tech/task-forces/tf-csirt/iodef/

Intrusion Detection Message Exchange Format

http://www.ietf.org/internet-drafts/draft-ietf-idwg-idmef-xml-14.txt

Intrusion Detection Exchange Protocol (IDXP)

http://www.ietf.org/internet-drafts/draft-ietf-idwg-beep-idxp-07.txt

ISO/IEC TR 18044 Information technology - Security techniques - Information security incident management

5.3.22 Service area: Contract and payment

This service area contains services and policies for granting fulfilment of promises and agreements for billing and payment.

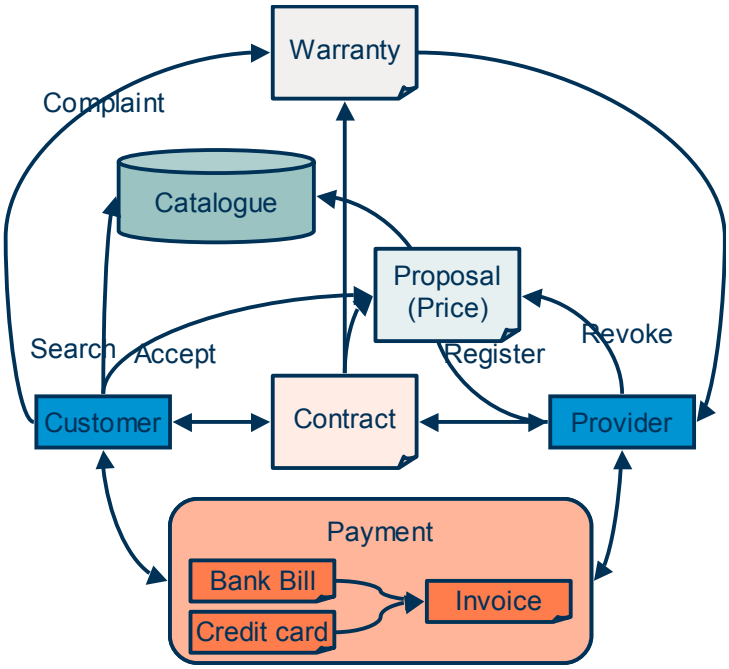

Figure 9 - Workflow for contract and payment

The list below describes the OASIS standardisation work in the e-commerce area.

This area will be addressed after the 10th October.%

OASIS Business Transactions

This technical committee handles issues on managing complex, B2B transactions over the Internet.
http://www.oasis-open.org/committees/download.php/9836/business_transaction-btp-1.1-spec-wd-04.pdf

OASIS Content Assembly Mechanism (CAM)

This technical committee handles issues on describing machine-processable information content flows into and out of XML structures.

OASIS ebXML Business Process

This technical committee handles issues on providing a standards-based business process foundation that promotes the automation and predictable exchange of business collaboration definitions using XML.
http://www.oasis-open.org/committees/download.php/14201/ebxmlbp-v2.0.1-Spec-cd-en-pdf1.zip

OASIS ebXML Collaboration Protocol Profile and Agreement (CPPA)

This technical committee handles issues on describing how trading partners engage in electronic business collaborations through the exchange of electronic messages.
http://www.oasis-open.org/committees/download.php/12208/ebcpp-2.1-april-5-2005-draft.doc

OASIS ebXML Messaging Services

This technical committee handles issues on defining the transport, routing and packaging of e-business transactions.
http://www.oasis-open.org/committees/download.php/6748/wd-ebms-3_0-01.pdf

OASIS ebXML Registry

This technical committee handles issues on defining and managing interoperable registries and repositories.
http://www.oasis-open.org/committees/download.php/13010/ebXMLRegistryOverview.pdf

OASIS Electronic Business Service Oriented Architecture (ebSOA)

This technical committee handles issues on advancing architectural patterns for using Service Oriented Architecture in electronic business.
http://www.oasis-open.org/committees/download.php/13827/TA_Outline_v2.0_29_july_2005.pdf
http://www.oasis-open.org/committees/download.php/14407/SOA_IM_V0.1.doc
http://www.oasis-open.org/committees/download.php/14406/Run-time_SOA_V0.1.doc

OASIS Electronic Procurement Standardization (EPS)

This technical committee handles issues on researching and developing global e-procurement standards and processes.

OASIS Universal Business Language (UBL)

This technical committee handles issues on defining a common XML library of business documents (purchase orders, invoices, etc.).
http://docs.oasis-open.org/ubl/cd-UBL-1.0.zip

5.3.23 Concept: Help desk

A help desk is an information and assistance resource that troubleshoots problems with computers and similar products. Corporations often provide help desk support to their customers via a toll-free number and/or website. There are also in-house help desks geared toward providing the same kind of help for employees only.

5.3.24 Concept: Computer-based training

In Computer-Based Training (CBT) computers are used for training and instruction. CBT programs are called "courseware" and provide interactive training sessions for all disciplines. Using graphics extensively, CBT was originally introduced on LaserDiscs, then CD-ROMs and, later, online. CBT courseware is typically developed with authoring languages that are designed to create interactive question/answer sessions.

Electronic-LEARNING is an umbrella term for providing computer instruction (courseware) online over the public Internet, private distance learning networks or in-house via an intranet.

5.3.25 Concept: Tutorials

A tutorial is a computer program whose purpose it is to assist users in learning how to use (parts of) a software product such as an office suite or any other application, operating system interface, programming tool, or game.

There are two kinds of software tutorials: movie tutorials that you watch, and interactive tutorials where you follow on-screen instructions (and in some cases watch short instruction movies), whereupon you do the tutorial exercises and get feedback depending on your actions.

5.3.26 Concept: Testing

Software testing is a process used to help identify the correctness, completeness and quality of developed computer software. With that in mind, testing can never completely establish the correctness of computer software. Only the process of formal verification can prove that there are no defects.

The quality of the application can and normally does vary widely from system to system but some of the common quality attributes include reliability, stability, portability, maintainability and usability. Refer to the ISO standard ISO 9126 for a more complete list of attributes and criteria.

5.3.27 Concept: Software Engineering (Development)

Software engineering is the profession that creates and maintains software applications by applying technologies and practices from computer science, project management, engineering, application domains, and other fields.

Software is the set of directions that enables computer hardware to perform useful work. In the last decades of the twentieth century, cost reductions in computer hardware led to software becoming a ubiquitous component of the devices used by industrialized societies.

Software engineering, like traditional engineering disciplines, deals with issues of cost and reliability. Some software applications contain millions of lines of code that are expected to perform properly in the face of changing conditions.

This area is of course valid for systems participating in NEA but NEA does not cover this. NEA covers what is needed to insure *interoperability* between systems not *how* systems should be developed.

5.3.28 Service: Time

Network Time Protocol (NTP)

This is a protocol for synchronising the clocks of computer systems over packet-switched, variable-latency data networks. NTP uses UDP port 123 as its transport layer. It is designed particularly to resist the effects of variable latency.

NTP is described in http://www.ietf.org/rfc/rfc1305.txt

5.3.29 Concept: Quality of Services supervision

This is an area that has not been “solved” yet. No standard for Service Quality of Services has been found but some attempts for standards exist.

QoS for Web Services - Requirements and Possible Approaches

(http://www.w3c.or.kr/kr-office/TR/2003/ws-qos/)

5.3.30 Service: Catalogue

Catalogue is a list of materials in a particular collection, arranged in a systematic order. A standard for catalogues is LDAP:

LDAP - Lightweight Directory Access Protocol.

LDAP began as a low-cost, PC-based front-end for accessing X.500 directories. The IETF (Internet Engineering Task Force) spec rapidly became the solution of choice for all types of directory services applications on IP nets. LDAP is a popular base for catalogues.

5.3.31 Concept: Publish/subscribe

The observer pattern (sometimes known as publish/subscribe) is a design pattern used in computer programming to observe the state of an object in a program.

The essence of this pattern is that one or more objects (called listeners) are registered (or register themselves) to hear an event which may be raised by the observed object. (The object which may raise an event generally holds a list of the listeners).

When the event is raised each listener receives a callback (which may be either a virtual function of the listener class or a function pointer (more generally a function object or "functor") passed as an argument to the listener registration method).

5.3.32 Concept: Broadcasting

Multicast is the delivery of information to a group of destinations simultaneously using the most efficient strategy to deliver the messages over each link of the network only once and only create copies when the links to the destinations split. By comparison with multicast, conventional point-to-single-point delivery is called unicast, whereas delivery to every node of the network is broadcast.

Audio-broadcasting MPEG-4 ISO/IEC-14496

Multimedia-Broadcasting MPEG-4 ISO/IEC-14496

5.3.33 Service: Events

WS-Event

This specification provides an XML syntax and a set of processing rules for advertising, subscribing, producing and consuming Web Services Events using a push and pull mode. In the push mode (as in "5.3.31 Concept: Publish/subscribe"), the event notification producer calls a method (callback) on the event consumer passing one or more notifications as parameter. In effect the producer pushes asynchronously notifications to the consumer. In the pull mode, the consumer invokes methods on the producer to retrieve the buffered notifications.
http://devresource.hp.com/drc/specifications/wsmf/WS-Events.jsp

5.3.34 Service: Telephone and video conference

A videoconference (also known as a video teleconference) is a meeting among persons where both telephony and closed circuit television technologies are utilized simultaneously. Video teleconference communication is multi-way and synchronous, as it would be if all parties were in the same room.

Following are the primary standards used with videoconferencing:

Videophone Directory - H.350

This is the ITU standard for a videophone directory.

Session Initiation for Dial-Up Networks and T1 - H.320

This is the ITU standard for dial-up ISDN, fractional T1 and Switched 56 services. H.324 is used with regular phone lines and analogue modems.

Session Initiation for IP Networks - IETF

This is the ITU standard for voice and video over packet networks, which today means IP LANs and the public Internet. SIP is the IETF standard for voice and video over IP. MCUs may handle H.323 clients only or both H.323 and SIP clients. Most traditional IP video clients are H.323, but SIP is gaining ground.

Compression - H.263 and H.264

This is the primary ITU. Codecs for compressing video are H.263 and H.264, the latter halving the bandwidth requirement of the former.

Data Conferencing - T.120

T.120 is the ITU standard for whiteboards, application sharing and application viewing, all of which can be used with or without videoconferencing. Earlier systems mixed data conferencing and video streams together, but newer ones keep T.120 tools separate in order not to sacrifice video quality. Using standard PCs and the Internet for data collaboration is more than adequate. Some vendors support proprietary IP-based data collaboration, such as VCON does with its IPNexus system.

5.3.35 Concept: Systems and resources management

Web Services Resource Framework (WSRF)

The purpose of this technical committee is to define a generic and open framework for modelling and accessing stateful resources using Web Services. Refactoring part of the Open Grid Services Infrastructure (OGSI) has led to this framework.

WSRF includes mechanisms to describe views on the state, to support management of the state through properties associated with the Web service, and to describe how these mechanisms are extensible to groups of Web services.
http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=wsrf

Application notes describing how applications might use the WS-RF family of specifications:
http://docs.oasis-open.org/wsrf/wsrf-application_notes-1.2-notes-pr-01.pdf

WS-Resource

http://docs.oasis-open.org/wsrf/wsrf-ws_resource-1.2-spec-pr-01.pdf

WS-ResourceProperties (WSRF-RP)

http://docs.oasis-open.org/wsrf/wsrf-ws_resource_properties-1.2-spec-pr-01.pdf)

WS-ResourceLifetime (WSRF-RL)

http://docs.oasis-open.org/wsrf/wsrf-ws_resource_lifetime-1.2-spec-pr-01.pdf

WS-ServiceGroup (WSRF-SG)

http://docs.oasis-open.org/wsrf/wsrf-ws_service_group-1.2-spec-pr-01.pdf

WS-BaseFaults (WSRF-BF)

http://docs.oasis-open.org/wsrf/wsrf-ws_base_faults-1.2-spec-pr-01.pdf

ISO 7894-4 Management Framework

IETF RFC3164 BSD Syslog Protocol

IETF RFC3195 Reliable Delivery for syslog

ISO 20000-1 - Information technology - Service management - Specification

ISO 20000-2 - Information technology - Service management - Code of practice

5.3.36 Concept: Security Management

Security management comprises functions that:

- Protects networks and systems from unauthorized access by persons, acts, or influences
- Includes many subfunctions, such as creating, deleting, and controlling security services and mechanisms; distributing security-relevant information; reporting security-relevant events; controlling the distribution of cryptographic keying material; and authorizing subscriber access, rights, and privileges.

ISO/IEC 17799:2000

This standard is essentially the set of security controls: the measures and safeguards for potential implementation. In volume it is the main body of the overall 'standard set' itself.

BS7799-2:1999

This is the 'specification' for an Information Security Management System (ISMS). It is the means to measure, monitor and control security management from a top down perspective. It essentially explains how to apply ISO 17799 and it is this part that can currently be certified against.

ISO/IEC TR 18044 Information technology -- Security techniques -- Information security incident management

ISO 7894-4 Management Framework

ISO/IEC 27001 Information technology - Security techniques - Information security management systems - Requirements

5.3.37 Concept: Service management

Service Management is a method for handling services, especially in the Information- and Communication Technology (ICT) area.

BS 15000 - IT service management

This standard describes an integrated set of management processes for the effective delivery of services to the business and its customers.

BS 15000 is aligned with and complementary to the process approach defined within the IT Infrastructure Library (ITIL) ITIL is a best-practice recommendation from The (British) Office of Government Commerce (OGC).

BS 15000 is currently being fast tracked through ISO and will eventually become ISO 20000.

BS15000-1

This standard consists of 10 sections: Scope, Terms and Definitions, Requirements for a Management System, Planning and Implementing Service Management, Planning and Implementing New or Changed Services, Service Delivery Process, Relationship Processes, Resolution Processes, Control Processes, and Release Process

BS15000-2

This standard provides assistance to organizations that are to be audited against BS15000-1 or are planning service improvements.

5.3.38 Concept: Instant messaging

Instant messaging is for instant communication of text messages and files between users.

RFC 3920: Extensible Messaging and Presence Protocol (XMPP): Core

http://www.rfc-editor.org/rfc/rfc3920.txt

RFC 3921: Extensible Messaging and Presence Protocol (XMPP): Instant Messaging and Presence

http://www.rfc-editor.org/rfc/rfc3921.txt

5.3.39 Service: Messaging Services

Web Service Message Queue WSMQ 1.0 Beta 2

ebXML Messaging Services v3.0 Committee Draft

WS Eventing Specification

Java Messaging Service JMS

5.4 Service area: Geographic information services

5.4.1 General

Geographic information services are services managing information on various aspects on real-world objects with a reference to earth surface.

There are several standardisation initiatives addressing geographic information:

ISO 19100 standards series by ISO/TC211

These standards are all in the process of becoming European standards through CEN/TC 287.
www.isotc211.org.

OGC (Open Geospatial Consortium)

Many of the OGC specification are adopted also by ISO/TC 211.
www.opengeospatial.org

DGIWG (Digital Geospatial Information Working Group)

The group develops and maintains a suite of digital geospatial information (DGI) standards that foster the interchange, access and use of geographic information between the defence organizations of member nations.
www.dgiwg.org .

CEN TC287 WG5

A group of experts working with defining basic functionality required for a spatial data infrastructure for Europe and related standards.

INSPIRE (Infrastructure for spatial information in Europe)

This initiative has made a proposal for an EU directive regarding spatial data in Europe. The work may have a great future impact on standardisation.
http://inspire.jrc.it.

General standards for geographical data are:

ISO 19113 - Geographic information - Quality principles

ISO 19114 - Geographic information - Quality evaluation

ISO 19118 - Geographic information - Encoding

ISO 19124 - Geographic information - Imagery and gridded data components

ISO 19130 - Geographic information - Sensor and data models for imagery

ISO 19131 - Geographic information - Data product specification

ISO 19139 - Geographic information - Metadata XML implementation

OGC Catalogue service interface specification

This standard addresses discovery of geographical data.

ISO 19119 - Geographic information - Services

OGC Basic Services Model (BSM)

OGC Stateless catalogue specification (Cat S)

5.4.2 Service: Geographic feature service

A feature is an abstraction of real-world phenomena, such as rivers, roads, borders or land coverage.

Services for geographic features are managing:

- definitions of geographic features
- topologic, geometric and temporal attributes of geographic features
- other attributes of geographic features
- relations between geographic features
- relations between geographic features and non-geographic features
- coding of datasets containing geographic features
- query and retrieval of geographic features

In the Web Feature Server (WFS) concept, a client application queries a WFS server. The query is coded according to the filter encoding (FE) specification. The WFS server may propagate the query to other WFS servers in order to compile the result. The WFS server returns the result as GML coded data. This means that the WFS server and client have to be designed for a specific application. The established WFS technology is not conformant with the Web Services concept.

A feature catalogue service handles definitions of feature types, attributes and value domains.

ISO 19109 - Rules for application schema

ISO 19110 - Methodology for feature cataloguing

ISO 19107 - Spatial schema

ISO 19108 - Temporal schema

ISO 19123 - Schema for coverage geometry and functions

ISO 19126 - Feature data dictionaries, feature catalogues and their registers

ISO 19136 - GML (OGC GML 3.1)

ISO 19142 - Web Feature Server interface (OGC WFS)

ISO 19143 - Filter Encoding (OGC FE)

5.4.3 Service: Map service

Map services may be provided by a Web Map Server which, on request from a web browser, compiles geographic information from several sources and presents the result as a map image. The server can also tell the client what maps it can produce (capabilities) and answer basic queries about the content of the map (map image interaction).

ISO 19117 - Portrayal

ISO 19128 - Web Map Server interface (OGC WMS)

OGC Web Map Server (WMS) interface

OGC Styled Layer Descriptions (SLD)

Styled Layer Descriptions describes what symbols to use when generating a WMS map image.

OGC Web Coverage Server (WCS) specification

5.4.4 Service: Positioning service

A positioning service provides coordinates for the position relative to the earth surface of an object. Such services may be used for surveying, navigation, tracking, etc.

ISO 19116 - Positioning services

This standard specifies an interface protocol for positioning systems.

5.4.5 Service: Coordinate transformation services

A position contains the coordinates as well as information on the reference system used. There are many reference systems for positioning geographic objects. The purpose of coordinate transformation services is to transform between these reference systems.

ISO 19111 - Spatial referencing by co-ordinates

This standard specifies a schema for describing reference systems.

ISO 19112 - Spatial referencing by geographical identifiers

ISO 19127 - Geodetic codes and parameters

OGC Coordinate transformation services specification

OGC Web Registry Service Specification

This specification describes services for management of translation parameters.

OGC Gazetteer Service Interface Specification (GAZ)

5.4.6 Other identified geographic services

- Spatial analysis service
- Object and position exchange service

5.5 Service area: Information management and information sharing

5.5.1 General

The area covered by information management and information sharing is huge and is not easily divided, e.g different sub areas are divided into three different levels:

- Business and process level which is closely related to the user.
- The system and technological level which should mainly be transparent to the user.
- The intermediate level which partly covers both of the other levels.

The areas are classified from the online usage of systems perspective not the building of systems.

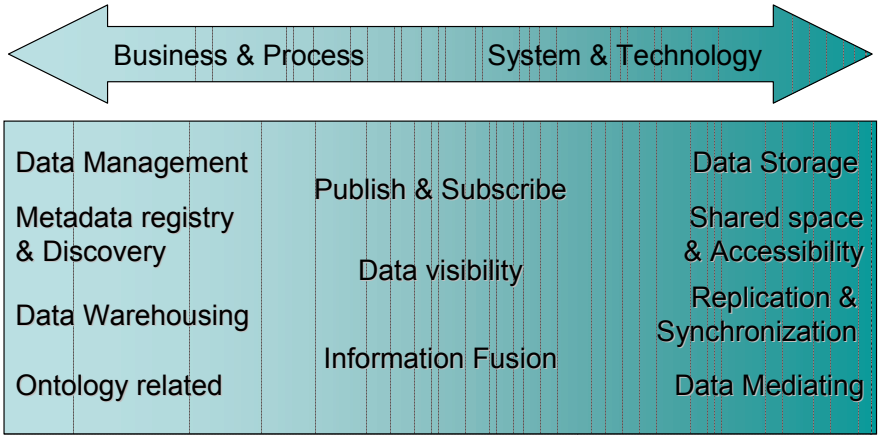

Figure 10 – Different levels of information management and sharing services

5.5.2 Service: Data management and publishing

Data management is considered to be the business and process side of data management. This area also includes data publishing done by the user. Data management is related to other areas like data storage, shared space and data visibility.

Policies and processes are the main tools of data management. Areas which are covered are Registration, Standardization, Certification, Life-Cycle Management, Quality Assurance, and Configuration Management.

Data management is widely used and there are many good examples to follow. For example NATO data management is worked on by the NATO Data Administration Group (NDAG)

ISO/IEC 152 88 - System life cycle processes

5.5.3 Service: Data storage

Data storage is a broad term if applied to data and information storage in general. It could be anything from a general service for data storage and retrieval to the low level data storage of bits and bytes on different media. The latter could also be broken down into data representation schemas, data organisation, data compression etc.

A service could be accessible by a single entity, a group of entities or by the public. Storage could be done temporarily or for a longer period of time. A general data storage service must therefore be very flexible or broken down in more specialised data storage services. Several specialised services could be combined to form more powerful or general services.

There will probably be dependencies to information security services to handle access control to the storage [5.3.8], metadata registry and discovery [5.5.6] and data warehousing services [5.5.10] etc. (to enable efficient management of data etc.).

File transfer protocols:

File Transfer Protocol (FTP)

Trivial File Transfer Protocol (TFTP)

Simple File Transfer Protocol (SFTP)

Hypertext Transfer Protocol (HTTP)

Distributed file systems:

Common Internet File System (CIFS)

Andrew File System (AFS)

Web Network File System (WebNFS)

Data storage:

Storage Area Network (SAN)

Network-attached storage (NAS)

Internet SCSI (iSCSI)

Fibre Channel over IP (FCIP)

Storage Management Initiative Specification (SMI-S)

The Common Redundant Array of Independent Disks (RAID) Disk Data Format (DDF)

5.5.4 Service: Data visibility services

Today's networks, systems, applications, and businesses processes are becoming larger and more distributed. This distributed nature guarantees scalability, fast response, redundancy in case of failure, and many other features far exceeding the capabilities of the classical central-server design. At the same time, it becomes increasingly important to have end-to-end visibility into business activities. Making the right business decisions hinges on knowing the progress and dependencies of all units of work at any point in time.

Knowing what is going on is simple in a business that records everything in a single, central database. Unfortunately, the reality of today's business processes is far from such simplicity. Business processes typically grow step-by-step, buying or developing new aspects built on whatever technology happens to be available at the moment. Over time, disparate technologies (from mainframes with business logic in COBOL, via 3-tier applications in C/C++ and SQL, to e-commerce sites, web services written on C# or Java, etc.) coalesce as the process implementation evolves.

Even though the heterogeneous nature of enterprise processes severely aggravates the visibility problem, it is inherent to any distributed system. For example, departmental or other business units within an organization tend to insist on owning their processes and data, even where storage format and other consistencies would make consolidation possible. Decisions that occur outside the departmental level (e.g. business decisions or infrastructural policies) ultimately require some of this data be correlated across departments and concentrated for analysis or real-time monitoring (other data relegated to archive for less frequent tasks like problem investigation, etc.).

Data visibility might be supported by the Metadata registry and discovery services [5.5.6], Publish/subscribe service [5.5.7] etc.

5.5.5 Service: Shared space and accessibility

The idea behind a Shared space and accessibility service is to provide shared space in order to store and share data between users and systems. The service is probably a composition of information security services to handle access control [5.3.8], data storage services [5.5.2] (to handle data storage and -management) and metadata registry and discovery services [5.5.6] (to handle classification and searching).

This area could also incorporate Inter-Governmental Information Sharing Standards.

The Transatlantic Secure Collaboration Program (TSCP)

The Information Technology and Crisis Management (ITCM) project

5.5.6 Service: Metadata registry and discovery

Metadata registries (MDR), addresses the semantics of data, the representation of data, and the registration of the descriptions of that data. It is through these descriptions that an accurate understanding of the semantics and a useful depiction of the data are found.

Discovery metadata is data about available data (metadata for data/content discovery contained in a data instance catalogue or index).

Examples of MDRs:

- NASA has a Metadata registry compliant with ISO/IEC 11179 and uses an extended Dublin Core set.
- DISA runs the DoD Metadata Registry and Clearinghouse
- NATO is building a MDR and is working on NATO Discovery Metadata Specification based on the Dublin Core Initiative.

ISO/IEC 11179, Information Technology -- Metadata Registries (MDR)

Dublin Core Metadata Initiative (DCMI)

Parts of Dublin Core is standardised as different standards. For example the Metadata Element Set is captured as the following standards.

ISO 15836:2003 (February 2003):

http://www.niso.org/international/SC4/n515.pdf

NISO Standard Z39.85-2001 (September 2001):

http://www.niso.org/standards/resources/Z39-85.pdf

CEN Workshop Agreement CWA 13874 (March 2000, no longer available)

AGLS Metadata Standard

Resource Description Framework (RDF)

ISO 19115 - Geographic information – Metadata

DoD Discovery Metadata Specification (DDMS) (Draft in 2003, current status not known)

5.5.7 Service: Publish and subscribe

The observer pattern (sometimes known as publish subscribe) is a design pattern used in computer programming to observe the state of an object in a program.

The essence of this pattern is that one or more objects (called listeners) are registered (or register themselves) to hear an event which may be raised by the observed object. (The object which may raise an event generally holds a list of the listeners.)

When the event is raised each listener receives a callback (which may be either a virtual function of the listener class or a function pointer (more generally a function object or "functor") passed as an argument to the listener registration method).

The observed object normally has a Subscribe method for adding a new listener and an Unsubscribe method for removing a listener from the list of objects to be notified when the event is raised. It may also have methods for temporarily disabling and then reenabling calls to prevent inefficient cascading of a number of related updates. This is sometimes referred to as event compression.

The event-based communication style (also called implicit invocation or publish/subscribe event notification) has been considerably and increasingly deployed over the past years. The number of non-trivial case studies in which this paradigm is applied is significant, and ranges in scope from simple desktop applications to widely distributed and critical systems such as real-time, automotive, traffic control (including air and railway), e-commerce, workflow, and mobile computing. The acceptance of this paradigm is witnessed by its incorporation into standards such as CORBA and JMS, and commercial systems such as TIBCO. In fact, this paradigm is becoming the de-facto communication mechanism for loosely coupled software systems.

The idea behind the Publish/subscribe service is to implement the observer pattern on a service producer and consumer level. Service producers should be able to publish data and information. Service consumers should be able to subscribe to published data and information.

Web Services Notification (WS-Notification)

Web Services Base Notification (WS-Base Notification)

Web Services Brokered Notification (WS-BrokeredNotification)

Web Services Topics (WS-Topics)

Java Message Service (JMS)

OMG Data-Distribution Service (DDS)

Network Data Distribution Services (NDDS)

Real-Time Publish-Subscribe (RTPS) Wire Protocol (IEC/PAS 62030)

Jabber Software Foundation – JEP-0060: Publish-Subscribe

Really Simple Syndication (RSS)

5.5.8 Service: Data replication and synchronizing

In computer science, replication refers to the provision of redundant resources (software or hardware components) to improve reliability and fault-tolerance. Dynamic replication of data can also be used to improve performance. (See US Patent # 4432057). This applies especially in a multiplicity of computer systems (multiprocessors).

Storage or backup of the same data on multiple file systems exemplifies replication. Database replication can take place, for example, in PostgreSQL, usually with a master/slave relationship between the original and the copy. The master logs the updates, which then ripple through to the slave. The slave outputs a message stating that it has received the update successfully, thus allowing the sending (and potentially re-sending until successfully applied) of subsequent updates. Multimaster replication, where updates can be submitted to any location, and then "ripple" through to other servers, is often desired, but introduces substantially increased costs and complexity which may make it unusable.

File synchronization in computing is a two-way synchronization of files and directories rather than mirroring which is one-way. Synchronization in general is coordination with respect to time.

Data replication and synchronisation mechanisms are usually encapsulated in vendor specific products and solutions. Until some well-adopted replication standards are put forth and implemented, vendor lock-in will be a feature of most forms of data replication.

Multilateral Interoperability Programme (MIP)

Lightweight Directory Access Protocol (LDAP)

Network News Transport Protocol (NNTP)

Internet Relay Chat Protocol (IRC)

Open Mobile Alliance (OMA) SyncML Specification

The BitTorrent protocol

http://www.bittorrent.com

Project JXTA(TM)

http://www.jxta.org

The IRIS project

http://www.project-iris.net/

5.5.9 Service: Time synchronisation

Network Time Protocol (NTP)

Global Positioning System (GPS)

5.5.10 Service: Data warehousing

A data warehouse is a copy of transaction data specifically structured for querying and reporting. Data warehousing includes data access, data directory, data warehousing process and data mining.

SQL

Online Analytical Processing (OLAP)

Predictive Model Markup Language (PMML)

XML for Analysis and OLE DB for Data Mining

SQL/MM Part 6: Data Mining

Java Data Mining (JDM) - Java Specification Request 73 (JSR-73)

CRoss Industry Standard Process for Data Mining (CRISP-DM)

OMG Common Warehouse Metadata (CWM) for Data Mining

5.5.11 Service: Information fusion

The idea of information fusion is to collect data samples and to fuse these samples in order to enhance quality or other aspects of the data. Radar data might for example form a radar track that represents a collection of radar plots from one or many radar sensors and a collection of metrological data might be fused into a weather forecast.

Information fusion is a wide area with different history, solutions and techniques for different business areas. Information fusion represents fusion on a high level (information, knowledge), e.g. situation analysis. Information fusion is not the same as data fusion which is fusion on a low level, e.g. sensor fusion.

Please refer to, and compare with 5.5.12.

There are few standards that cover information fusion (at least specified as a service). Basic ideas and algorithms are standard but specific solutions and implementations are usually covered by secrecy due to national or business interests. Some standards that incorporate information (and data fusion) are the following military standards:

Multilateral Interoperability Programme (MIP)

Tactical Digital Information Links (TADIL)

5.5.12 Service: Data mediating

Data mediating services provide operations such as coordinate, transform and analyse.

Coordinating data is, for example, when retrieving data from two asynchronous sources, combine the result and finally distribute it as a synchronous stream. Transforming data is, for example, when converting a temperature from Celsius to Fahrenheit. Analysing data is, for example, when using Soundex to determine if a given string sounds like another. The examples given are very basic but should give an idea of how these services differ from the Information fusion services.

There might be dependencies to Metadata registry and discovery services (5.5.6) and Ontology related services (5.5.13).

Today, data mediating services functionality is mainly found in a mixture of integration technologies (CORBA, DCOM, JMS, MQ) and proprietary vendor adapters. Data mediating services is probably best built

using open service oriented standards so that they can be accessed and utilised by all other services in the information infrastructure. Open standards mean that an integrator can choose between competing vendors on the features they offer (provided those vendors adhere to the standards). It also means that the service can (re)use legacy systems and techniques to realize the mediating service.

Listed below are not specific open standards for data mediation but rather standards and solutions that might serve as a foundation when building data mediating services.

OASIS - Business Process Execution Language (BPEL)

OASIS - Electronic Business using eXtensible Markup Language (ebXML)

5.5.13 Concept: Ontology

Taxonomy, thesaurus, ontology's are all related and is each more complex than the next. Taxonomy is a structured list, or 'tree', formed into a hierarchy with broader terms at the top. A polyhierarchical taxonomy is an extended taxonomy where two different branches can point at the same element. A thesaurus is taxonomy with extras, it shows lateral connections ('related' and 'see also' terms), has an underlying index showing words that might spring to mind but which you should not use, and tells you what you should use instead ('preferred' and 'non-preferred' terms). It can be polyhierarchical, and contains scope notes to indicate exactly what the term means. A thesaurus lists concepts – the actual words used are not of paramount importance.

In information science, an ontology is the product of an attempt to formulate an exhaustive and rigorous conceptual schema about a domain. An ontology is typically a hierarchical data structure containing all the relevant entities and their relationships and rules within that domain (e.g., a domain ontology).

Information models and conceptual or logical data models are related to ontology's and can sometimes be used as ontology's and vice versa.

W3C – OWL Web Ontology Language Reference

ISO 2788:1986: Documentation - Guidelines for the establishment and development of monolingual thesauri

MIP – JC3IEDM

OMG – UML

IEEE Std 1002-1987, Standard Taxonomy for Software Engineering Standards

IEEE – ACM Taxonomy

IEEE – Suggested Upper Merged Ontology (SUMO)

5.5.14 Service: Sensor data access

The idea to have a general sensor data access service is quite appealing, especially within the military domain (with a long standing tradition of sensor data retrieval and processing). Sensor data does not however differentiate from other kind of data on an abstract and logical level. Sensor data have to be represented, stored, transferred, interpreted etc. as any other kind of information. What might separate sensor data from other kind of data within the given context might be some specific attributes. Examples might be huge amounts of very small data units that need to be handled in real time. This has to be seen as attributes of a specific sensor or type of sensor. It should be handled by a specific technical solution and the information infrastructure has to be able to support that solution. It should however not be seen as something that makes sensor data different from any other kind of data in the networked enabled information infrastructure.

Standards within this field should therefore be focused more towards the type of sensor than the fact that originated from a sensor. Certain requirements might affect other services in aspects like QoS, precision, performance, timing, storage, etc.

Open Geospatial Consortium (OGC) - Sensor Web Enablement

Sensor Model Language (SensorML)

ISO 19130 Geographic information - Sensor and data models for imagery and gridded data

5.5.15 Service: Sensor coverage information

Sensor coverage is an attribute to a specific sensor (both as a type and instance). It should be covered on a general level as a service property (type, metadata etc.) and further accessed by the sensor data access service (see 5.5.14).

5.6 Service area: Legislation

5.6.1 Service: Lawful interception

Lawful Interception (LI) used by law enforcement agencies and intelligence services is a major tool to combat organized crime and terrorism. LI systems provide overall coverage of any type of communication in any network used. LI in each country is based on national legislation in that country.

ETSI Technical Committee on Lawful Interception (TC LI)

This is the leading body for LI standardization.

http://portal.etsi.org/li/summary

ETSI ES 201 671 - Handover interface for the lawful interception of telecommunication traffic

ETSI TS 102 234 - Description for handover of Internet Access Information and TCP/IP information

ETSI TS 102 233 - Description for handover of E-mail messages

ETSI TS 102 232 - HI2 and HI3 interfaces for handover via IP networks

ETSI TS 101 671 - Handover Interface for the Lawful Interception of Telecommunications Traffic

ETSI TS 102 227 - Functional Entities, Information Flow and Reference Point Definitions; Lawful Interception

5.6.2 Other identified legislation items

- Export and import
- Concept: Personal integrity
- Concept: Safety
- Concept: Dangerous goods
- Concept: Environment

5.7 Service area: Traffic monitoring and control

5.7.1 General

This service area contains services built on geographic information services. Such services are used to monitor and control vehicles (and other mobile items such as pedestrians). The client of such a service may be moving with the vehicle (mobile client) or located at a central site.

5.7.2 Standards

ISO 19116 - Positioning services

ISO 19133 - Location based services for tracking and navigation

ISO 19134 - Multi-modal location based services for routing and navigation

ISO 19141 - Schema for moving features

ISO/TC 204 - Intelligent transport systems (several standards)

IEEE 1512 - Standards related to incident management and traffic incidents

5.7.3 Traffic management services

The purpose of traffic management services is to gather information on position, direction and speed of several vehicles in a geographic area in order to control their movements.

5.7.4 Route planning services

The purpose of route planning is to find, in some sense, the optimal route for a vehicle with goods or people. It may include multi-modal transportation aspects, for example changing from air to land transportation.

5.7.5 Navigation services

The purpose of navigation services is to, at any moment, advise a mobile vehicle what way to go in order to get to a certain position and to use its position, direction and speed to predict the outcome. Such services are typically mobile.

5.7.6 Vehicle tracking services

The purpose of tracking services is to get information on where vehicles are and what route they took.

5.8 Service area: Situation picture

5.8.1 General

A situational picture is a presentation of information, which describes the current status of objects, conditions of subjects, their behaviour and the interactions between them.

There is a set of systems available with a situational picture, mainly in the field of military. For NATO C3 Systems, the mandatory standards are defined in the NATO C3 System Technical Architecture (NC3TA). Nevertheless, there is no real standard for one service “situational picture”. Therefore, this structure for a situational picture service area should be used as a framework for implementing such services.

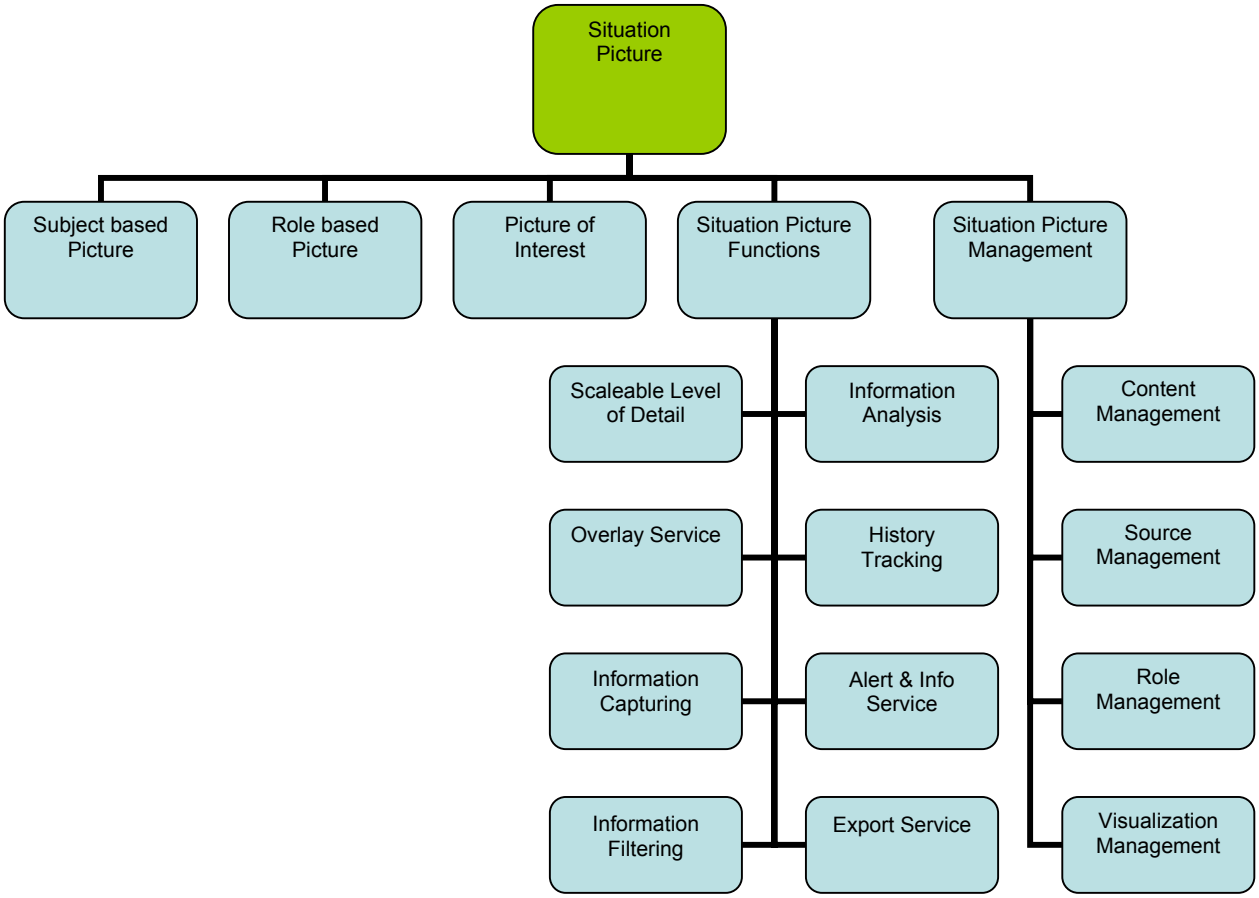

Figure 11 - The Situation picture service area structure

NC3TA Version 7.0

This document contains all current NATO C3 relevant Open System and communications standards and guidance for their use.
http://nc3ta.nc3a.nato.int

5.8.2 Service: Subject based picture

This service provides a situational picture of a specific subject (e.g. logistic, alarm status, recognized air picture).

5.8.3 Service: Role based picture

This service provides a situational picture for a group of users with the same tasks and responsibilities. Typically, the role based picture consists of a combination (fused) subject based pictures (e.g. Common Relevant Operational Picture “CROP”).

5.8.4 Service: Picture of interest

This service provides a situational picture for the specific needs of a user, beside or in addition to the role based picture. Typically, the picture of interest is event triggered by a new task of a user (e.g. managing an unforeseen catastrophe).

5.8.5 Service: Scaleable level of detail

This service provides the possibility to compose or to decompose the information of a situation picture to a certain level of detail.

5.8.6 Service: Overlay service

This service provides the possibility to import information into a situational picture without using the information for analysis purpose (e.g. intelligent merging).

5.8.7 Service: Information capturing

This service provides the possibility to add information into a situational picture from different sources (e.g. sensors, manually, internet)

5.8.8 Service: Information filtering

This service provides the possibility to search or to shrink the information.

5.8.9 Service: Information analysis

This service provides the possibility to evaluate and to generate new information (e.g. data fusion, intelligent merging).

5.8.10 Service: History tracking

This service provides the possibility to store and to compare situational picture for analysis purpose.

5.8.11 Service: Alert & info service

This service provides the possibility to notify users (e.g. via email) or services about an occurred event (e.g. fire alarm)

EDXL Emergency Data Exchange Language

This standard is a suite of emergency data message types including resource queries and requests, situation status, message routing instructions and the like, needed in the context of cross-disciplinary, cross-jurisdictional communications related to emergency response.

EDXL Resource Message (EDXL RM)

This standard is a part of the EDXL standard and describes a series of messages that allow local, tribal, state, federal and non-governmental agencies, stakeholders, and systems providers to rapidly share information on incident and event management resources. The Resource Message set facilitates requests, orders, and requests for information, demobilization and tracking of all types of resources (human resources, vehicles, equipment, supplies, and facilities, as well as packages/teams composed of many of these).

The Resource Messaging standard set of seven messages has been submitted to the OASIS Emergency Management Technical Committee for consideration.
http://www.oasis-open.org

Common Alerting Protocol, v. 1.0

This OASIS specification (OASIS Standard 200402, March 2004) addresses alerts and warnings to media, public and responders.

The Common Alerting Protocol (CAP) is a simple but general format for exchanging all hazard emergency alerts and public warnings over all kinds of networks. CAP allows a consistent warning message to be disseminated simultaneously over many different warning systems, thus increasing warning effectiveness while simplifying the warning task. CAP also facilitates the detection of emerging patterns in local warnings of various kinds, such as might indicate an undetected hazard or hostile act. And CAP provides a template for effective warning messages based on best practices identified in academic research and real-world

experience.
http://www.oasis-open.org/committees/emergency/

5.8.12 Service: Export service

This service provides information for non-service-oriented applications.

5.8.13 Service: Content management

This service provides the possibility to set and to change parameters for the content of situational picture (e.g. setting conditions for delivering multimedia content or “text only” content; setting the level of reliability for using information).

5.8.14 Service: Source management

This service provides the possibility for searching and choosing sources and to set and to change parameters for chosen sources (e.g. radars, services, internet, reference database, repositories).

5.8.15 Service: Role management

This service provides the possibility to define roles and content for situational pictures.

5.8.16 Service: Visualization management

This service provides the possibility for defining objects and rules for information representation within situational pictures.

5.9 Service area: Decision support services

- Expertise and knowledge support
- Medical expertise
- Medical services, health care, remote diagnostics
- Medical recipe services
- Chemical information support services
- Services giving access to expert knowledge
- Meteorological services
- Prediction service
- Training services

5.10 Other items specific for a community of interest

- Personnel information services
    - Refuge tracking services (Refuge information services)
    - Personnel tracking services
    - Population and demography services

Annex A
(informative)
Inventory of ongoing projects

This inventory list contains references to projects and initiatives in the NEA domain of interest. The list is a snap-shot of the current situation (2005) and there are no intentions to be exhaustive. The order is irrelevant.

Identification of Project	Scope	Interested and impacted parties	Service functionalities
LOI-NEC, 6 Nations Letter Of Intent – Network Enabled Capabilities	Military shared situation awareness	Defence industry in UK, France, Germany, Spain, Italy, Sweden	To be decided
IT-supported leadership in the Swiss Armed Forces	The project amalgamates and coordinates C2IS with special systems and special applications in the Swiss Armed Forces. It embeds the systems into the political and strategic processes, perfects the required resources and establishes connections with external agencies and also ensures integration into administration	Swiss Armed Forces, Swiss Neighbors based on MoU (D,A,I,F) Organizations UNO, OSZE, EAPC/PfP, CENCOOP, Neutral Nations: Finland, Sweden, Austria, Ireland	As delivered by the individual C2IS systems and applications on strategic, operation and tactical level
NATO´s approach to a NATO Network Enabled Capability - Concept	- Working definition of NNEC - NNEC Conceptual framework - "Net Ready Approach"	- NATO - NATO Nations - NATO´s Partner Nations - Defence Industry	Conceptual considerations providing a framework and a taxonomy for the development of NNEC
Siemens VDR Lawful interception http://europa.eu.int/agencies/enisa/index_en.htm	ENISA	- Europol - Eurojust - OLAF	Overall monitoring and recording Forensic readiness
Transatlantic Secure Collaboration Program	The Transatlantic Secure Collaboration Program (TSCP) is a **cooperative effort** by the leading defence and aerospace firms, supported by the US Department of Defense (DoD) and UK Ministry of Defence (MoD), to develop a **framework of policies, operating procedures, and mechanisms** to enable **secure collaboration across multiple jurisdictions**.	- UK Council for Electronic Business (UK CeB) - US Department of Defense - UK Ministry of Defence	▸ Provides industry-wide policies, procedures, and control mechanisms to address Export Control (EC) **compliance in a multi-jurisdictional environment** ▸ Focuses on **enabling policies, procedures and mechanisms** for Governance, Training, Information and Identity Management

Identification of Project	Scope	Interested and impacted parties	Service functionalities
OASIS	Open Advanced System for Improved Crisis management	Civil protection organisations and all actors involved in the management of the operations during a crisis in the case of natural disasters (flood, forest fire, earthquake…) or man made disasters: it concerns different organisations (fire brigades, police, …) at different level, national, regional, local, in control rooms or in the field	-Information Exchanges Services: reports on the situation … -Data management services: access from the field to different data bases as dangerous products databases for example useful in case of floods …, -Cartographic services: navigation services to find the best route to go to the place of the disaster taking into account the blocked roads, position of the crews in the field, localisation of the disaster, -C3I (Communication, Command, Control, Intelligence) services: resources management, situation establishment (Common operational picture) … -Decision support services: advanced C3 services in order to support the command level
Swedish Armed Forces Enterprise Architecture	Joint architecture including e.g. a description framework and around 20 concepts concepts such as Network Based defence concept and a Service concept	Swedish Armed Forces, Swedish Defence Materiel Administration	Infrastructure Application support Applications
LedsystT C3 project	Prototype, concept verification and demonstration project	Swedish Armed Forces and Swedish Defence Materiel Administration, many other national and international interested parties. Design partner including SAAB, Eriksson, Boeing and IBM.	All above, including 3 generations of infrastructures. Common situation picture and situation awareness. C3 Command support.
OpenSIS	Service Oriented Middleware enabling secure dynamic distributed	Ericsson, Sweden	Infrastructure

Identification of Project	Scope	Interested and impacted parties	Service functionalities
	cooperation. Tools for creating systems of systems.	Swedish Defence Materiel Administration	Tools and services for creating System of Systems
Artillery Computer Network – ADLER	The ADLER artillery computer network is the key component in the artillery system and distinctly improves artillery fire control, the quality of target acquisition and flexibility of use in an operational environment.	Army organisations and entities	Editing and distribution of commands, orders and messages ; Editing of all target and fire unit status information; Preparation of graphical information and situation presentation; Availability of all fire mission and artillery command and control information; Calculation of optimum use of weapons and ammunition for fire mission proposals; Planning and preparation of resource allocation; Coordination of target acquisition systems and weapon systems
Army Mobile C3I System – HEROS-2/1 Lot 2	The system accomplishes the Command and control support for corps, division and brigade.	Army organisations and entities at corps, division and brigade level. 1st GE/NL Corps, Eurocorps and 7th German Armoured Division	Data Base Management,; Map/situation processing; Object Cluster Editor; Data Aggregation; Order Processing; Tables & Overviews; Network management; Communications; MIP; Staff functions; Mail System LOTUS NOTES; Office functions
Integrated, Computer-supported, Transmission Control and Network Management System – IRIS	IRIS represents a C2 information and network management system for planning, implementing and secure operation of the telecommunications system of the Army	German Army	Network management for mission preparation, mission planning, issuance of orders, monitoring and problem analysis; staff area operations/functions (processing & issuance of orders, reporting system, staff functions, E-Mail, Web)
EF 2000 Cockpit Simulator	Realisation and customisation of Fixed-base fighter cockpit with Simulation of various WS and sensors within the same scenario and Link Network	Air Force	Fixed-base fighter cockpit with visual simulation, Scenario simulation, MIDS/Link16 simulation, service functionalities
TORNADO Cockpit System Simulator	Realisation of a Virtual Avionic System for TORNADO – - VASTOR	Air Force	Research in MMI optimisation; simulation of crew relevant avionics system; worldwide terrain and map data; scenario generator; available as pure simulation or

Identification of Project	Scope	Interested and impacted parties	Service functionalities
			as hybrid solution with original equipment; approval of solutions with aircrews during missions
MPA-TCS Demonstrator	Demonstrator for MPA - Tactical Command System (MPA - TCS) and Simulation of the MPA Link 16 Communication	Navy, Air Force	Mission planning and situation presentation with map data (3D), mission activities, SIM data, sensor data, scenario generation.
UH-Tiger Developmental Simulation	Simulation technology for modelling and development of avionic components	Army	Simulation of image formations, - terrain data basis, - netting features, - tactical environment. Modelling of avionic components, - symbol generators, - LAN - TCP/IP- DI
MIDS Data Link Simulator Network	Demonstrator for MPA - Tactical Command System (MPA - TCS) and Simulation of the MPA Link 16 Communication.	Navy	Mission planning and presentation with map data (3D), mission activities, - SIM data, sensor data, scenario generation.
ESG Simulation Environment	Netting of simulation equipments for land and air vehicles	All Parties which take part in Combined / Joint operations.	Connectivity, Link 16
RKES – NetOpFü (NCW)	RKES IV reconfigurable crew compartment development simulator	Army, Air Force	Netting & Integration of RKES simulation equipment with other simulation facilities / equipments for purposes like analysis of command and control systems; Mission Rehearsal, optimisation of MMI by rapid prototyping (Soldier-in-the-Loop), Analysis of new concepts (Hardware-in-the-Loop), Verification of system concepts in early project phase, Connection to other simulators (constructive, virtual, live).
Multilateral Interoperability Programme – MIP	Implementation of a prototype for MIP DEM (Data Exchange Mechanism) based on GE HEROS-2/1 Lot 2.	Army	Data modelling, data exchange mechanism (DEM), Info exchange procedures, system architecture, security concept
Simulation & C2 Info System	GE-US-Simulation & C2 Information		Netting of SIM-Sys with C2IS via C2SIM-Proxy (MIP/PSI-SA-Interface); Definition of

Identification of Project	Scope	Interested and impacted parties	Service functionalities
Connectivity Experiment - SINCE	System Connectivity Experiment		common Conceptual Reference Model (CRM), Mapping of Realtime Platform Reference (RPR) ←→ CRM
Architecture for NetOpFüBw (NCW)	Analysis of the command and control process: Tool-based (POPKIN System Architect) modelling of the Overarching Architecture for NetOpFüBw („OV“)	All	Generation of the Reference Architecture regarding the aspects for operational concept „Einsatzführung Bw“, operational connectivity, operational info exchange rqmts, activity models and business process.
Project LedsystT	Joint architecture including e.g. a description framework around Network Based defence concept and a Service concept Prototype, concept verification and demonstration project	Swedish Armed Forces, Swedish Defence Materiel Administration Saab, Ericsson Micro Wave, IBM, Boeing	Infrastructure Application support Applications
Network Centric Operations Industry Consortium, NCOIC http://www.ncoic.org	Industry working together with our customers to provide a Network Centric environment where all classes of information systems interoperate by integrating existing and emerging open standards into a common evolving global framework that employs a common set of principles and processes.	Members on Tier 1 Founding members are BAE Systems, Boeing, CACI, Carrillo Business Technologies, Cisco Systems, EADS, EMC Corporation, Ericsson, Factiva®-a Dow Jones and Reuters Company, Finmeccanica, General Dynamics, HP, Honeywell, IBM, Innerwall, L-3 Communications (Integrated Systems), Lockheed Martin, Microsoft, Northrop Grumman, Oracle, Raytheon, Rockwell Collins, SAAB, SAIC, Smiths Aerospace, Sun Microsystems, Thales, and Themis with The Open Group acting as the management company.	
NEO	High-level architectural standard for interoperability	Saab, Thales, EADS, BAES	
WEAG CEPA 6	Project in European defence	Saab	

Identification of Project	Scope	Interested and impacted parties	Service functionalities
	industry and government institutions for command and control and related Information and Communications technologies		
EU security related research initiative	Project with civ/mil shared situation awareness. Prototype including a demonstration. One part of the project is standards.	Saab and a lot of other companies in Sweden and Europe.	
WIS Web Based Information System	Swedish Emergency Management Agency (SEMA) has developed the system. SEMA is now managing the central part of the WIS. This is a commission by the Swedish government.	Primarily civilian crisis management actors on local, regional and central governmental level.	The purpose is to share open crisis information between crisis organisations of different actors in the society. The core of the WIS is a crisis event log.
TrustCoM http://www.eu-trustcom.com	Trustcom will develop a framework for trust, security and contract management in dynamically-evolving virtual organisations.	The TrustCoM team is formed as a consortium of end-users, technology and service providers, and experts in computing, economics and law, from industry, government and academia, who are actively involved in the development of technology and frameworks related to Virtual Organisations.	A realisation of the TrustCoM framework will be delivered by means of open-standards web services based specifications and a reference implementation. Validation will take place within industrial strength test-beds in the areas of collaborative design engineering (CE) and provision of ad-hoc, dynamic processes (ADP) for the on-demand provision aggregate electronic services.
Multilateral interoperability programme (MIP) http://www.mip-site.org	Statement of intent for the multilateral interoperability programme (MIP) (the Anzio agreement – 18 November 2003) Objectives. The members approving this Statement of Intent wish to achieve international interoperability of Command and Control Information Systems (C2IS) at all levels from corps to battalion, or	Forces in multinational operations in war and crises response operations.	It will build in an evolutionary way on the baseline of interoperability provided by the MIP and ATCCIS products. To do so they recognise the following objectives: Operational. To specify the detailed Information Exchange Requirements (IERs) to support military operations in war and crisis response operations (CRO) and provide

Identification of Project	Scope	Interested and impacted parties	Service functionalities
	lowest appropriate level, in order to support multinational (including NATO), combined and joint operations and the advancement of digitization in the international arena.		operational interfaces in fieldable form to enable the C2IS of the members involved to interoperate at and between specified levels of command. Procedural. To specify the procedural aspects of the MIP Information Exchange 2/7 Requirements (IERs) supporting the above operational goals, ensuring maximum commonality at formation and unit command levels. To support those IERs in the interface operating procedures devised under this programme. To provide feedback to the appropriate NATO Panel on the implications of implementing those IERs on automated systems. To continue development and maintenance of the (Land) C2 Information Exchange Data Model (L)C2IEDM and associated data management activities. Technical. To deliver tested specifications for the technical solution that satisfies the MIP IER's. To refine and maintain the MIP capability during its agreed in-service period. To examine communications solutions identified by other interoperability groups for exchanging data at all agreed levels.
Crisis management Initiative Founder President Martti Ahtisaari, Finland	To respond to new security challenges by enhancing the conflict prevention and crisis management	Organisations operating in the field of crisis management working towards interoperability at poiliticla,	

Identification of Project	Scope	Interested and impacted parties	Service functionalities
	capacity of the international community	organisational, field and technical level	
Coalition Warrior Interoperability Demonstration (CWID)	Demonstration of Interoperability of US and NATO C4I systems	US-DoD, NATO, Defence industry	c.f. MIP
Simulation and Testing Environment for the German Bundeswehr (SuTBw)	Simulation and testing workbench e.g. for CD&E	Germany	Simulation and Testing Services Simulation Data Visualisation and Analysis Services Infrastructure Services
Open Community	Implementation of military system interoperability on the basis of open civil and military standards across all member companies	German Industry	As required
VINACS	Tactical Command and Control System with Common Relevant Operational Picture	Switzerland	Blue Force Tracking Command and Control
C4I-Systems for Leo 2	Tactical Command and Control System with Common Relevant Operational Picture	Sweden, Spain, Greece, Rheinmetall Defence Electronics	Blue Force Tracking Command and Control
The Digital Geographic Information Working Group (DGIWG)	Metadata standards for spatial data. Participating in ISO/TC 211 with: 19139 Geographic information - Metadata - Implementation specification 19115 part 2 Geographic information - Metadata Part 2 - Metadata for imagery and gridded data project teams.	DGIWG is developing a comprehensive implementation profile of the ISO standards for use in coalition environments (including NATO) requiring a common metadata standard to produce, catalogue, share, discover and exploit geospatial intelligence.	Services related to geographic information