NATO | NORTH ATLANTIC COUNCIL
OTAN | CONSEIL DE L'ATLANTIQUE NORD

7 December 2011

NOTICE
AC/322-N(2011)0205
Silence Procedure ends:
03 Jan 2012 18:00

CONSULTATION, COMMAND AND CONTROL BOARD (C3B)

Core Enterprise Services Standards Recommendations

The Service Oriented Architecture (SOA) Baseline Profile

Note by the Secretary

References:	(a)	AC/322(SC/5)N(2010)0053, 29 November 2010
	(b)	AC/322-D(2010)0016 MULTI-REF, 28 April 2010
	(c)	AC/322(SC/5)N(2010)0053-ADD2, 17 January 2011
	(d)	C-M(2008)0116 (INV)

1. Ref(a) covered the first iteration of the 'Core Enterprise Services Implementation Specification', which had been produced by the former Core Enterprise Services Working Group (CESWG) in line with the tasking from Ref(b). Following one break of silence, and the receipt of one set of comments without breaking silence (Ref(c)), the Staff engaged with the Nations concerned, and the NC3A, to produce a revised document. This document, now re-titled 'Core Enterprise Services Standards Recommendations', is at Enclosure 1.

2. Unless the undersigned is notified to the contrary by **1800 hrs on Tuesday 3 January 2012**, it will be assumed that the C3B has approved Enclosure 1, and has agreed that the document should be publicly disclosed in line with the Ad Hoc procedure defined in Ref(d). Once approval has been granted, the Staff will take the necessary actions to have Enclosure 1 incorporated into the NATO Interoperability Standards and Profiles (NISP).

(Signed) M. ELLIOTT

Enclosure 1: Core Enterprise Services Standards Recommendations - the SOA Baseline Profile

Action Officer: Mr. J.R. Couture (Ext 4271)
1 Enclosure
Original: English

INTENTIONALLY

BLANK

ENCLOSURE 1 TO
AC/322-N(2011)0205

CORE ENTERPRISE SERVICES STANDARDS RECOMMENDATIONS

THE SOA BASELINE PROFILE

VERSION 1.7

11 November 2011

TABLE OF CONTENTS

This page is left blank intentionally

1. INTRODUCTION

1.1 DEVELOPMENT OF THIS DOCUMENT

The NNEC Feasibility Study (FS) of 2005 showed that NATO Network-Enabled Capability (NNEC) requires the dynamic networking of coalition forces to support information-sharing capabilities and to support the development and provision of information services. The name given to this key capability is the Networking and Information Infrastructure (NII).

The NNEC FS went on to name four main categories of services comprising the NII: Communications services, Information and Integration services (IIS), Information Assurance services and Service Management and Control.

One of the major design NNEC tenets has been to focus on an approach based on the principles of Service Oriented Architecture (SOA). Indeed, the NNEC FS postulated that the concept of SOA is key to meeting the NNEC operational requirements and is an essential part of the overall strategy.

The IIS services, in particular, are planned to provide the basic SOA foundation that future Alliance capability would build upon. These services are collectively known as the Core Enterprise Services (CES).

Another major vision of NNEC is that it will be approximately “10% NATO and 90% National”, meaning that the bulk of the capabilities will be provided by the Nations, and that the services provided by NATO and the Nations will be expected to be interoperable. The only way to facilitate this interoperability is to agree – throughout the NATO enterprise, as well as in close coordination with the Nations – exactly how these services will be developed and referenced. This involves not only coming up with a common architecture, but also agreeing the standards and interfaces that the specific services will implement.

The Core Enterprise Services Framework (CESF) – approved by the then NC3B[1] in spring 2009 – describes the high-level functionality of the Core Enterprise Services: the “what” of the CES. Building on the CESF, this Reference Document offers recommendations for the “profile” of standards to be implemented: the “how” of the CES services that will provide the underlying SOA baseline for the future Alliance Information and Communications Technology (ICT) environment.

The maturity of each of the CES comprising the IIS is not uniform – some of the services are more developed and in use compared with others. For this reason, the focus of this document is on an initial subset of services - the SOA baseline functionality that is best defined and for which the industry open standards are the most mature[2]. In the future some CES can be extended by new specifications.

[1] The NC3B has been re-titled as the Consultation, Command and Control Board (C3B).

[2] Note that this document is service specific and not infrastructure specific. When some services are not included in this initial subset of CES, it doesn’t mean that the functionality will not be part of the infrastructure (e.g. storage as infrastructure vs. storage “as a service”).

1.2 PURPOSE OF THIS RECOMMENDATION

NATO and some NATO nations are in an advanced planning stage to implement the CES in Allied Operations and Missions (AOM) and non-AOM. One example is the Afghanistan Mission Network (AMN), where a subset of the CES has been fielded as a pilot trial as part of the AMN information infrastructure.

This document recommends a consistent set of CES standards to be used at the interfaces between NATO and coalition partners. NATO and nations should adhere to these interfaces when participating in NATO operations with the aim of ensuring future interoperability, compatibility and longevity. In this recommendation we focus on the use of stable versions of the standards which are supported by industrial and open source implementations.

This CES standards recommendation is based upon the Web Services Interoperability Organization (WS-I), an industry consortium that promotes interoperability amongst the stack of Web services specifications (Web services are a common implementation of SOA.). WS-I does not propose its own standards, but instead profiles existing ones. The organization has developed what it calls the “Basic Profile”, which suggests a specific collection of standards for basic interoperability. In this document, the Basic Profile 1.1 Second Edition is recommended as the starting point for NATO’s future SOA implementations.

From there, this specification goes on to recommend a set of standards to fulfil an initial subset of the Core Enterprise Service requirements by providing a SOA baseline infrastructure, covering messaging, discovery, security, and so on. However, not all CES need to be implemented if not required. It is intended that applications that will use the SOA baseline – such as Functional Services and Community of Interest services – will follow these recommended standards; the others will be implemented by the CES themselves for compatibility with legacy services and/or national implementations.

Following the profile of standards recommended in this document does not by itself guarantee interoperability. However, agreeing on and implementing the SOA baseline as recommended in this document will give the widest range of interoperability scenarios in the near to medium term, as well as the greatest level of functionality.

1.3 THE CORE ENTERPRISE SERVICES

The former Core Enterprise Services Working Group (CESWG) of the NC3B SC/5 (Information Services Sub-Committee) produced the Core Enterprise Services Framework [NC3B CESF, 2009], which was agreed by the Nations in 2009 via the NC3B. As defined in the CESF , the CES are:

“technical services that facilitate other service and data providers on the enterprise network by providing and managing the underlying capabilities to deliver content and value to end-users. They can be thought of as the enablers used by other services and users across the whole network-enabled enterprise, acting as “building blocks” for developing more sophisticated COI, cross-COI and functional/application services. They are independent of business process and context; and are ubiquitous”.

The CESF (Figure 1) identifies a set of fourteen (14) services (12 Core Enterprise Services + Service Security (Information Assurance) and Enterprise Service Management) which together make up the CES. This service catalogue has also been carefully coordinated with the emerging NATO Overarching Architecture and the Information and Integration Services (IIS) Reference Architecture.

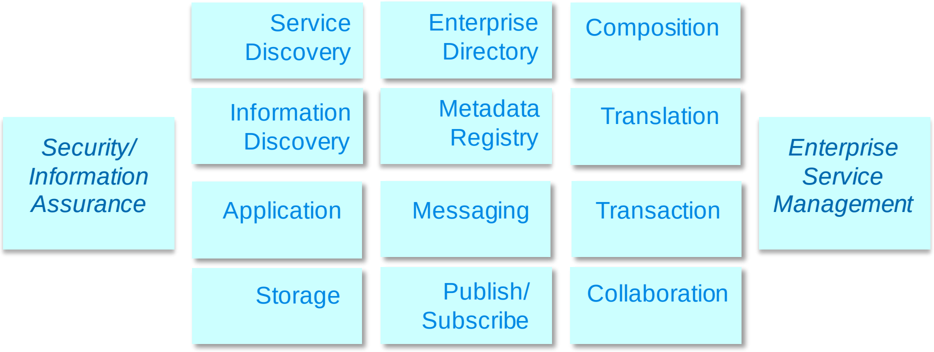

Figure 1 The NNEC Core Enterprise Services according with NATO CESF

1.4 THE SOA BASELINE

Not all of these services will be delivered at the same time – nor will they be installed on all networks at the same time. It is realistic to expect that the CES will be delivered in several phases. The Core Enterprise Services are described in more detail in [NC3B CESF, 2009].

The SOA Baseline subset includes the following core enterprise services:

- Messaging

  This service provides transport of information and forms a messaging infrastructure within the SOA.

- Publish/Subscribe

  This service provides automated distribution of information based on user needs. It also minimises traffic on the messaging infrastructure through the use of event-driven notification of changing data.

- Translation

  This service provides the automated means for the semantics of information to be translated from one structure to another.

- Service Discovery

  This service provides a mechanism to discover and locate service instances (i.e. services on the network including, but not limited to, Web services).

- Service Security

  The CES Security Services are a suite of services designed to enable Information Assurance. They provide a foundation to implement uniform, consistent, interoperable and effective service security.

- Metadata Registry

The purpose of this service is to provide a (conceptually) centralised source of technology-based representations of standards and specifications as implemented by different Communities of Interest (CoI) in order to improve visibility and enable interoperability.

- Enterprise Directory

  This service provides a means for synchronisation between directories or data repositories in NATO nations and NATO domains in order to harmonise and rationalise the information.

- Collaboration

  In this initial SOA baseline, the Instant messaging service is included. This document recognizes that there are additional collaboration services and more services will be addressed in future versions.

- Enterprise Service Management (ESM)

  These services will provide the suite of operational processes, procedures and technical capabilities needed to ensure that NNEC services are up and running, accessible and available to users, protected and secure, and that they are operating and performing within agreed-upon parameters.

The initial subset of the CES (Figure 2) reflects what the first – or SOA baseline– interfaces will look like for NNEC. These services are relatively well-defined, with relatively mature associated standards, and thus it is believed that the services are ready to be developed/procured in the short term.

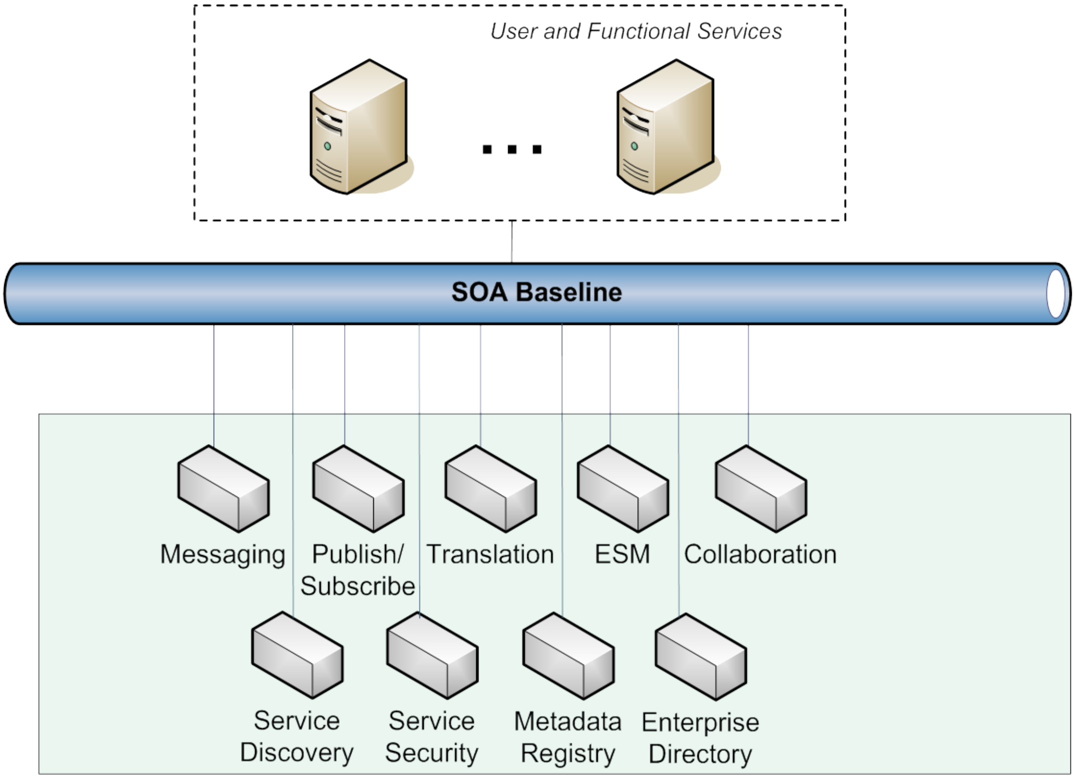

Figure 2 The CES (Basic SOA Infrastructure) Functionality

2. PROFILE

2.1 INTRODUCTION

As introduced in Section 1, the Core Enterprise Services Framework ([NC3B CESF, 2009]) described a set of Core Enterprise Services (CES) – the “what” of the CES. This section addresses the “how” by detailing the profile of functionality and recommended standards for each of the CES in this initial subset.

2.2 SOURCES OF RECOMMENDATIONS

When constructing a profile of standards to use within a large organisation, there are a wide range of sources that provide input into the choices that need to be made.

The specific standards that are presented in the following sections have been compiled from various sources, including standards bodies, NATO agreed documents and practical experience of conducting experiments with nations and within projects.

Because of the time that it takes to ratify a standard or profile, the standards that are recommended in the SOA Baseline may not be the most recent or up to date versions. Some of the most important sources for defining the recommended set of standards for use in NATO are described in the following sections.

2.2.1 The Web Services Interoperability (WS-I) Profiles

The Web Services Interoperability Organization has developed a collection of “profiles” that greatly simplify the interoperability of SOA Web services. Profiles provide implementation guidelines for how related Web services specifications should be used together for best interoperability between heterogeneous systems.

The general profile for service interoperability is called the Basic Profile, which describes how the core Web services specifications – such as Simple Object Access Protocol (SOAP), Web Service Description Language (WSDL) and Universal Description Discovery Integration (UDDI) – should be used together to develop interoperable Web services. Specifically, the profile identifies a set of non-proprietary Web services standards and specifications and provides clarifications, refinements, interpretations and amplifications of them that promote interoperability.

In addition, the WS-I has a number of other profiles that are adopted in this document. It recommends the WS-I basic profile 1.1 (Second Edition), the WS-I Basic Security Profile (version 1.1), the WS-I Simple SOAP Binding Profile (version 1.0) and the Attachments Profile (version 1.0). In this CES recommendation there are exceptions to the use of some of the specifications included in the WS-I profiles. These exceptions as noted in notes to relevant standards.

2.2.2 NATO Interoperability Standards and Profiles (NISP)

The NISP, otherwise known by its NATO reference, Allied Data Publication 34 (ADatP-34), is an agreed set of standards and profiles that are to be used to “provide the necessary guidance and technical components to support project implementations and transition to NATO Network Enabled Capability (NNEC)” [NATO NISP]. It is a six volume work that specifies which protocols are to be used at every level of the communications stack in the near, medium and long term.

As a ratified, official NATO document, it forms the primary NATO input into the standards that have been selected for implementation within the NNEC interoperability environment.

This CES standards recommendation will be submitted to the NISP as upgrades for those recommended in the NISP where applicable, and is recommended to be included in the mandatory section of future versions of the document.

2.3 RECOMMENDED STANDARDS

The following sections detail the recommended functionality and standards for each of the Core Enterprise Services that make up the SOA baseline. This profile of SOA standards is summarised in the following table. In the cases where a version of a standard in the table deviates from the version of the standard in the WS-I profiles, the table takes precedence - meaning that the version of the standard explicitly defined in the table replaces the related version of the standard in the profile.

The last column of the table indicates in which WS-I profile(s) the standard or profile is referenced (if any). Therefore if a profile is quoted, it is recommended to use it when implementing that service. The WS-I Profiles used are:

WS-I Profile	Comments
WS-I Basic Profile 1.1	[NATO NISP] vol. 2 lists WS-I Basic Profile (WS-I BP) 1.1 as a mandatory and WS—I Basic Profile 1.2 as an emerging standard. Request for change should be issued to NISP to consider the latest edition of the WS-BP 1.1. A migration path should be proposed to move from the WS-I BP 1.1 to WS-I BP 1.2.
WS-I Basic Security Profile 1.1	The WS-I Basic Security Profile is not referenced in the [NATO NISP] and should be provided as a RFCP
WS-I Simple SOAP Binding Profile 1.0	
WS-I Attachments Profile 1.0	Request for change should be issued to NISP to consider the latest edition of the WS-I Attachments Profile.

2.3.1 Use of XML

2.3.1.1 Overview

The main data format exchanged in the SOA environment is, and will continue to be, the Extensible Markup Language (XML). XML solves one of the fundamental problems of interoperability between different systems, which is the structure of exchanged messages. The XML Schema definition language is the most widely used method to describe the syntax (and partly the semantics) of XML data exchanged in a SOA environment. XML Schemas allow data managers to create different XML-based “dialects” for various CoIs and maintain logical separation within different namespaces.

2.3.1.2 Profile

Service	Standard Name	Recommended Version	Relationship with the WS-I profiles	Comments
XML	Extensible Markup Language (XML)	1.0	• WS-I Basic Profile • WS-I Simple SOAP Binding Profile • WS-I Attachments Profile	
	Namespaces in XML	1.0	• WS-I Basic Profile • WS-I Simple SOAP Binding Profile • WS-I Attachments Profile	Request for change should be issued to NISP to consider the latest edition of the Namespaces in XML.
	XML Schema Part 1: Structures	1.0	WS-I Basic Profile	
	XML Schema Part 2: Datatypes	1.0	WS-I Basic Profile	

2.3.2 Messaging Service

2.3.2.1 Overview

Messaging provides a federated, distributed, and fault-tolerant SOA machine-to-machine messaging capability which is realised via open standards. According to the Organisation for the Advancement of Structure Information Standards (OASIS), “Messaging provides a standard, interoperable way to guarantee message delivery to applications of Web services.” [OASIS WSRM 2004] It supports the configuration of service-level parameters for a message including its priority and precedence. In addition, it provides guaranteed delivery of messages to disconnected users or applications by queuing them for delivery on reconnection. A robust messaging infrastructure should ensure that “messages” (in the sense of Web service Messages, which are data containers for requests or responses) are delivered to their intended destination in a timely and consistent manner.

Messaging is what binds the entire service infrastructure together. Without a solid messaging infrastructure, there can be no reliance on services to deliver the capability for which they were designed.

In addition, the messaging infrastructure can provide a number of other useful features, such as the ability to minimise the bandwidth requirements for SOAP-based messaging through the use of compression and XML optimisation.

2.3.2.2 Profile

Service	Standard Name	Recommended Version	Relationship with the WS-I profiles	Comments
Messaging Service	HTTP	1.1	• WS-I Basic Profile • WS-I Simple SOAP Binding Profile	
	HTTP State Management Mechanism	RFC2965	WS-I Basic Profile	
	SOAP	1.1	• WS-I Basic Profile • WS-I Simple SOAP Binding Profile	
	WS-I Simple SOAP Binding Profile	1.0		
	WS-I Attachments Profile	1.0		
	WS-Reliable Messaging	1.2		
	WS-Addressing	1.0		
	SOAP Over UDP:	1.1		Usage: This specification defines a binding for SOAP envelopes to UDP datagrams. This specification should be used where HTTP/TCP is not feasible or requires too much available bandwidth. It also should be used to enable multicasting of SOAP messages

2.3.3 Publish and Subscribe Service

2.3.3.1 Overview

The main function of a Publish/Subscribe service is to minimise traffic on the messaging infrastructure through the use of event-driven notification of changing data. If an application subscribes to the results of a service, then it is notified about new events it subscribed to, rather than having to repeatedly connect, and request all changed data.

An additional benefit can be achieved through the use of a notification broker. The use of such a broker makes it possible to deliver information from a single source to multiple consumers. A Notification Broker is capable of subscribing to notifications, either on behalf of Notification Consumers, or for the purpose of messaging management. It is capable of disseminating notifications on behalf of Publishers to Notification Consumers. This is functionality which may increase flexibility related to information management in military networks. The goal of such a system is to avoid implementing redundant point-to-point connections and provide a coherent flow of information to various subscribers that depend on the data from a single source.

2.3.3.2 Profile

Service	Standard Name	Recommended Version	Relationship with the WS-I profiles	Comments
Pub/Sub Service	WS-BaseNotification	1.3		WS-Notification is actually a name for a set of specifications: WS-BaseNotification, WS-BrokeredNotification and WS-Topics, all of which are currently OASIS Standards
	WS-BrokeredNotification	1.3		
	WS-Topics	1.3		

2.3.4 Translation Service

2.3.4.1 Overview

A data Translation Service provides the automated means for the semantics of information to be translated from one structure to another (also known as “transformation”). It provides services to support translation between different message formats, through knowledge of the structure and semantics of both the source and destination data. In the context of this document, we focus on the specifications that are recommended to be used for XML transformation.

2.3.4.2 Profile

Service	Standard Name	Recommended Version	Relationship with the WS-I profiles	Comments
Translation Service	XSLT	1.0, 2.0[3]		Translations between data formats may be registered in the metadata registry and shared within coalitions. By default XSLT 1.0 should be used whenever possible. When it is not sufficient, XSLT 2.0 as a more powerful language could be used instead. Most XSLT 2.0 compliant processors are capable of processing XLST 1.0 as well. XSLT 2.0 should be proposed as an emerging standard in NISP.
	XQuery	1.0		
	XPath	1.0, 2.0		

[3] XSLT 1.0 uses XPath 1.0 and XSLT 2.0 is designed to be used with XPath 2.0

2.3.5 Service Discovery Service

2.3.5.1 Overview

This service provides a mechanism to discover and locate service instances (i.e. services on the network including, but not limited to, Web services). Discovery in this sense is the act of locating a machine-processable description of a service instance that may have been previously unknown and that meets certain functional criteria. The goal is to find an appropriate service to fulfil a particular need, whether this is at design-time, when the application is being written, or at run-time, when the application is running.

The Service Discovery Service(s) allows applications and application designers to find services that have been advertised. It also provides the mechanism to see which *instance(s)* of a particular service are available at that moment, and thus to bind to the selected instance of that service which best fits the current operational need of the application.

A distinction needs to be drawn between the Service Discovery Service, which provides a searchable interface for discovering the dynamic data (e.g. service endpoints) about a service, and the Metadata Registry Service (see paragraph 2.3.6 below), which allows the retrieval of static metadata about a service, such as a particular interface implementation or the data structures that are used.

2.3.5.2 Profile

Service	Standard Name	Recommended Version	Relationship with the WS-I profiles	Comments
Service Discovery Service	UDDI[4]	3.0.2	Deviation from WS-I Basic Profile 1.1 (second edition). UDDI version 2 should not be used.	
	WSDL	1.1	WS-I Basic Profile WS-I Simple SOAP Binding Profile WS-I Attachments Profile	

2.3.6 Metadata Registry Service

2.3.6.1 Overview

A Metadata Registry service combines the functionality of a registry (for storing metadata about artefacts, including a reference to them) and a repository (for storing artefacts themselves). As such it is a storage repository for the XML artefacts that act as a template for the XML documents, as well as other artefacts that are relevant throughout the enterprise. Within a repository, schemas (and parts of schemas) can be stored, referenced and searched. Registries are not limited to storing information about the structure of data within an organisation, however. It is also possible to store references to the services that implement particular schemas, how they can be called, and where the endpoints are located. In this role, it complements the Service Discovery Service, as the SDS provides the binding information to connect to instances of the services that are described in the Registry.

[4] UDDI is mainly suitable for static and design time discovery in support for e.g. SOA governance.

2.3.6.2 Profile

Service	Standard Name	Recommended Version	Relationship with the WS-I profiles	Comments
Metadata Registry Service	Electronic Business using XML (ebXML) Registry Information Model (ebXML RIM)	3.0		
	ebXML Registry Services and Protocols (ebXML RS)	3.0		

2.3.7 Security Services

2.3.7.1 Overview

The CES Security Services are a suite of services that provide a foundation to implement uniform, consistent, interoperable and effective service security. These Security Services provide a set of services based on widely accepted standards, that are implemented separately from the service producers, in order to offer a framework the services can use without having to implement authentication and access control logic themselves.

Due to the granular nature of the suite, and the loose coupling of the services, it is possible to use only a subset of these services to apply security to any service. Developers of services can substitute their own implementations of the security services (within given constraints), as long as the approach complements that taken by the Core Enterprise Services.

It should be noted that these security services contribute to, but are not alone sufficient to ensure the security of, a service. Implementers must ensure that the code underlying the application or service and the hosted environment follow standard INFOSEC guidelines. Furthermore, the security provided by the security services is coarse-grained. The security services manage access to the core and functional services, and provide a model for retrieving the identity of the consuming entity, but this is at the level of *subject-resource-action*. Any more fine-grained filtering of the application data should be performed by the application itself if required.

There are many elements that form a security framework, not all of which are addressed by the CES Security Services. This SOA baseline profile divides the incorporated security specifications into the following classes for readability: Transport Security, Message Security, Security Token, and Token Issuance.

PKI and cryptographic algorithms are outside the scope of this document, but need to be in place in support of some of these security standards.

2.3.7.2 Profile

Transport Security

Service	Standard Name	Recommended Version	Relationship with the WS-I profiles	Comments
Transport Security	HTTP Over TLS	RFC2818	WS-I Basic Profile WS-I Basic Security Profile	
	TLS	1.2 (RFC 5246)	WS-I Basic Profile WS-I Basic Security Profile	Recommended version is TLS 1.2. Fading specification is TLS 1.0 (RFC 2246).

Message Security

Service	Standard Name	Recommended Version	Relationship with the WS-I profiles	Comments
Message Security	WS-Security: SOAP Message Security	1.1 (OASIS Standard Specification, 1 February 2006)	WS-I Basic Security Profile	
	Web Services Security: SOAP Messages with Attachments (SwA) Profile	1.1, OASIS Standard, 1 February 2006	WS-I Basic Security Profile WS-I Attachments Profile	
	XML Encryption Syntax and Processing	W3C Recommendation 10 December 2002	WS-I Basic Security Profile	
	XML Signature Syntax and Processing	1.0 (Second Edition) W3C Recommendation 10 June 2008	WS-I Basic Security Profile	
	WS-Addressing	1.0		
	WS-Security Utility	1.0		

Security Token

Service	Standard Name	Recommended Version	Relationship with the WS-I profiles	Comments
Security Token	SAML	2.0		
	Web Services Security: SAML Token Profile	1.1 OASIS Standard, 1 February 2006	WS-I Basic Security Profile	

Confidentiality Label

Service	Standard Name	Recommended Version	Relationship with the WS-I profiles	Comments
Confidentiality Label	XML Confidentiality Label Syntax	[NATO RTO XML Conf. Label]		
	Binding of Metadata to Information Objects	[NATO RTO Metadata Binding]		

Token Issuing

Service	**Standard Name**	**Recommended Version**	**Relationship with the WS-I profiles**	**Comments**
Token Issuing	WS-Trust	1.4		
	WS-Federation	1.1		
	WS-Metadata Exchange	1.1		
	WS-Policy	1.5		
	WS-SecurityPolicy	1.3		

2.3.8 Enterprise Service Management

2.3.8.1 Overview

The Enterprise Service Management (ESM) aspect of Service Management and Control (SM&C) focuses on the coordination and management of SOA Web services across domain boundaries.

The overall function of SM&C is to provide end-to-end performance monitoring, configuration management and problem detection/resolution, as well as enterprise IT resource accounting and addressing, for example for users, systems and devices. In addition to the specifications included in this SOA baseline profile, the ESM services will require a suite of operational processes, procedures and technical capabilities needed to ensure that NNEC SOA services are up and running, accessible and available to users, protected and secure, and that they are operating and performing within agreed-upon parameters.

2.3.8.2 Profile

Service	**Standard Name**	**Recommended Version**	**Relationship with the WS-I profiles**	**Comments**
Enterprise Service Management	WS-Management	1.0		

2.3.9 Enterprise Directory Service

2.3.9.1 Overview

Within NATO nations and NATO domains, a range of separate directories or data repositories coexist with a sizeable overlap between the information contained within these various directories. There is a need for synchronisation between them to harmonise and rationalise the information and this is usually done by standing up an Enterprise Directory Service.

The Enterprise Directory Service can solve the synchronisation within the NATO organisation, but there is also a need to exchange a subset of the information between NATO and coalition partners in support of other services.

The agreed Enterprise Directory Schema is defined by the ACP 133, which also identifies the protocols to be used for synchronisation between directories.

2.3.9.2 Profile

Service	Standard Name	Recommended Version	Relationship with the WS-I profiles	Comments
Enterprise Directory Service	LDAP	3.0 (RFC 4510)		
	TLS	1.2	WS-I Basic Security Profile	Recommended version is TLS 1.2. Fading specification is TLS 1.0 (RFC 2246).
	SASL using Kerberos v5 (GSSAPI)	RFC 4422, RFC 4752		

2.3.10 Collaboration Services

2.3.10.1 Overview

The Collaboration Service will provide a tool suite of web-accessible capabilities that enable authorized enterprise information sharing and processing. This document recognizes that there may be additional collaboration services that are not included for development in the SOA baseline profile. Additional services will be addressed in future versions.

The initial version of the Collaboration Service will consist of:

Instant Messaging

- Capability to initiate synchronous communication instantly.
- Capability to discover persons/contacts including real time presence information.
- Ad hoc collaboration initiation and maintenance.
- Participation in a number of concurrent sessions.
- Chat Participation on workstations and laptops using thin and thick clients.

2.3.10.2 Profile

Service	Standard Name	Recommended Version	Relationship with the WS-I profiles	Comments
Collaboration Service	XMPP Core	RFC 3920		XEP extensions not recommended in the NISP. Recommend submitting RFCP to include them.
	XMPP Instant Messaging and Presence Protocol	RFC 3921		
	Service Discovery extension	XEP-0030		
	vcard-temp extension	XEP-0054		
	Multi-User Chat extension	XEP-0045		

REFERENCES

[NC3B CESF, 2009] “Core Enterprise Services Framework v1.2”, AC/322-D(2009)0027, dated 26 May 2009 and –AS1, dated 29 June 2009.

[NATO NISP] ADatP-34, NATO Interoperability Standards and Profiles, (NISP), AC/322-N(2011)0021-REV1, dated 14 March 2011 and –AS1, dated 28 March 2011.

[NATO NAF, 2007] “NATO Architecture Framework” Version 3, 2007.

[NC3B NDMS] NATO Consultation, Command and Control Board (NC3B), “Guidance On The Use Of Metadata Element Descriptions For Use In The NATO Discovery Metadata Specification (NDMS). Version 1.1”, AC/322-D(2006)0007, 14 Mar 2006.

[NNEC-DS] NATO Consultation, Command And Control (C3) Board, “NNEC Data Strategy”, AC/322(SC/5)N(2008)0040 (INV), 16 Oct 2008.

[NATO RTO Metadata Binding] A. Eggen, R. Haakseth, S. Oudkerk and A. Thummel, "Binding of Metadata to Data Objects - A Proposal for a NATO Specification", FFI-rapport 2010/00962 (NU), 2010.

[NATO RTO XML Conf. Label] A. Eggen, R. Haakseth, S. Oudkerk and A. Thummel, "XML Confidentiality Label Syntax - A Proposal for a NATO Specification", FFI-rapport 2010/00961 (NU), 2010.

[NATO RTO/IST-068 Final Report] NATO Research and Technology Organization document RTO RTG-031/IST-068 "XML in Cross-Domain Security Solutions, RTO, Paris, FR, 2010.

[OASIS SOA, 2006] OASIS “Reference Model for Service Oriented Architecture”, Version 1.0, 12 October 2006.

[OASIS WSRM, 2004] OASIS “Web Services Reliable Messaging”, Version 1.1, November 2004, http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=wsrm.

[W3C WS Architecture 2004] W3C “Web Services Architecture” http://www.w3.org/TR/ws-arch/ February 2004.

This page is left blank intentionally

ABBREVIATIONS

ACP	Allied Communication Publications
AES	Advanced Encryption Standard
AHWG	Ad Hoc Working Group
AIS	Automated Information System
AMN	Afghan Mission Network
API	Application Programming Interface
ARH	Alliance Replication Hub
ASN.1	Abstract Syntax Notation One
Bi-SC	Bi-Strategic Command
BPS	Boundary Protection Services
C2	Command and Control
C3	Consultation, Command and Control
C3B	Consultation, Command and Control Board (a Category I NATO Committee, reporting to the North Atlantic Council)
CES	Core Enterprise Services
CESF	Core Enterprise Services Framework
CESWG	CES Working Group
CIS	Communications and Information Systems
CM	Configuration Management
COI	Community of Interest
COTS	Commercial of the Shelf
CP	Capability Packages
CRL	Certificate Revocation List
CSV	Comma Separated Values
CVS	Certificate Validation Service
DHS	Document Handling System
DMTF	Distributed Management Task Force
DR	Disaster Recovery
DSA	Digital Signature Algorithm
DSML	Directory Services Markup Language
ebXML	Electronic Business using XML
ECDSA	Elliptic Curve Digital Signature Algorithm
ESB	Enterprise Service Bus
ESM	Enterprise Service Management
FAS	Functional Area Services
FFI	Norwegian Defence Research Establishment
FS	Feasibility Study
GIS	Geographic Information System
GOTS	Government of the Shelf
GUI	Graphical User Interface
HTTP(S)	Hypertext Transfer Protocol (Secure)

ABBREVIATIONS *(continued)*

IaaS	Infrastructure as a Service
IAM	Identity and Access Management
IdM	Identity Management
IEG	Information Exchange Gateway
IETF	Internet Engineering Task Force
IIS	Information and Integration Services
IKM	Information and Knowledge Management
ISO	International Standards Organisation
ISR	Intelligence, Surveillance, and Reconnaissance
ITU	International Telecommunication Union
J3IEDM	Joint C3 Information Exchange Data Model
JCOP	Joint Common Operating picture
KFOR	Kosovo Force
LDAP	Lightweight Directory Access Protocol
LDIF	LDAP Interchange Format
LAN	Local Area Network
MDR	Metadata Registry
MIP	Multilateral Interoperability Programme
MLS	Multi Level Security
MMR	Minimum Military Requirement
MOA	Memorandum of Agreement
MOM	Microsoft Operation Manager
NAF	NATO Architectural Framework
NC3B	NATO C3 Board (now re-titled as the C3B)
NCES	Net Centric Enterprise Services
NDMS	NATO Discovery Metadata Specification
NEDS	NATO Enterprise Directory Service
NFFI	NATO Friendly Forces Information
NGO	Non-Governmental Organisation
NII	Networking and Information Infrastructure
NIMA	NATO Information Management Authority
NIMP	NATO Information Management Policy
NISP	NATO Interoperability Standards and Profiles
NIST	National Institute of Standards and Technology
NMS	NATO Messaging System
NMRR	NATO Metadata Registry and Repository
NNEC	NATO Network Enabled Capability
NPKI	NATO Public Key Infrastructure
NSA	NATO Standardisation Agency
NVG	NATO Vector Graphics
OASIS	Organisation for the Advancement of Structure Information Standards
OGC	Open Geospatial Consortium

ABBREVIATIONS *(continued)*

PaaS	Platform as a Service
PAC	PKI Advisory Cell
PCN	Peer Competency Network
PDA	Personal Digital Assistant
PDP	Policy Decision Point
PEP	Policy Enforcement Point
PfP	Partnership for Peace
PKI	Public Key Infrastructure
QoS	Quality of Service
REST	Representational State Transfer
RFC	Request for Comments
RSA	Rivest, Shamir and Adleman
SaaS	Software as a Service
SAML	Security Assertion markup language
SAN	Storage Area Network
SDS	Service Discovery Service
SHA	Secure Hashing Algorithm
SLA	Service Level Agreement
SM&C	Service Management and Control
SMI	Security Management Infrastructure
SMTP	Simple Mail Transfer protocol
SNMP	Simple Network management protocol
SOA	Service Oriented Architecture
SOAP	Simple Object Access Protocol
SQL	Structured Query language
SSL	Secure Sockets Layer
STS	Security Token Service
TLS	Transport Level Security
UDDI	Universal Description Discovery Integration
URI	Uniform Resource Identifier
US MDR	U.S. Department of Defense Metadata Registry & Clearinghouse
VM	Virtual Machine
VPN	Virtual Private Network
W3C	World Wide Web Consortium
WAN	Wide Area Network
WS	Web Services
WS-I	Web Services Interoperability
WSDL	Web Service Description Language
WSDM	Web Services Distributed Management

ABBREVIATIONS *(continued)*

XACML	eXtensible Access Control Markup Language
XML	eXtensible Markup Language
XMLSWG	XML Management Services Working Group
XMPP	eXtensible Messaging and Presence Protocol
XSLT	eXtensible Stylesheet Language Transformations