NCI AGENCY

NATO Communications and Information Agency
Agence OTAN d'information et de communication

AGENCY INSTRUCTION

INSTR TECH 06.02.01

SERVICE INTERFACE PROFILE FOR SECURITY SERVICES

Effective date:

Revision No: Original

Issued by: Chief, Core Enterprise Services

Approved by: Director, Service Strategy

Table of Amendments

Amendment No	Date issued	Remarks

Author Details

Organization	Name	Contact Email/Phone
NCI Agency	R. Fiske	rui.fiske@ncia.nato.int
NCI Agency	M. Lehmann	marek.lehmann@ncia.nato.int
NCI Agency	R. Malewicz	robert.malwicz@ncia.nato.int
NCI Agency	L. Schenkels	leon.schenkels@ncia.nato.int
NCI Agency	D. Gujral	davinder.gujral@ncia.nato.int

Table of Contents

Page

0 PRELIMINARY INFORMATION 4

0.1 References ---- 4
0.2 Purpose ---- 4
0.3 Applicability ---- 4

1 INTRODUCTION 4

1.1 Audience ---- 5
1.2 Notational Conventions ---- 5
1.3 Terminology ---- 5
1.4 Namespaces ---- 6
1.5 Goals ---- 7
1.6 Non-Goals ---- 7
1.7 Relationships to Other Profiles and Specifications ---- 8

2 SECURITY FOR WEB SERVICES 8

2.1 Subject ---- 8
2.2 Supporting Infrastructure ---- 9

3 SECURITY TOKEN STRUCTURE 10

3.1 Purpose ---- 10
3.2 SAML Assertion ---- 11

4 REFERENCES 14

5 ABBREVIATIONS 16

List of Annexes

ANNEX 1 – XML SAMPLES ---- 17

AGENCY INSTRUCTION 06.02.01

SERVICE INTERFACE PROFILE FOR SECURITY SERVICES

0 PRELIMINARY INFORMATION

0.1 References

A. NCIA/GM/2012/235; Directive 1 Revision 1; dated 3 May 2013
B. NCIARECCEN-4-22852 DIRECTIVE 01.01, Agency Policy on Management and Control of Directives, Notices, Processes, Procedures and Instructions, dated 20 May 2014
C. NCIARECCEN-4-23297, Directive 06.00.01, Management and Control of Directives, Processes, Procedures and Instructions on Service Management, dated 03 June 2014

0.2 Purpose

This Technical Instruction (TI) provides detailed information, guidance, instructions, standards and criteria to be used when planning, programming, and designing Agency products and services. In this specific case the TI defines a Service Interface Profile (SIP) for one of NATO's Core Enterprise Services.

TIs are living documents and will be periodically reviewed, updated, and made available to Agency staff as part of the Service Strategy responsibility as Design Authority. Technical content of these instructions is the shared responsibility of SStrat/Service Engineering and Architecture Branch and the Service Line of the discipline involved.

TIs are primarily disseminated electronically[1], and will be announced through Agency Routine Orders. Hard copies or local electronic copies should be checked against the current electronic version prior to use to assure that the latest instructions are used.

0.3 Applicability

This TI applies to all elements of the Agency, in particular to all NCI Agency staff involved in development of IT services or software products. It is the responsibility of all NCI Agency Programme, Service, Product and Project Managers to ensure the implementation of this technical instruction and to incorporate its content into relevant contractual documentation for external suppliers.

1 INTRODUCTION

One of the main concepts of the future NATO Network Enabled Capabilities (NNEC) is that of a "network of networks"; that is, instead of a single, all-encompassing global network the NNEC environment will be made up of many NATO and national networks linked together. In order to ensure compatibility between services running in this environment there is a need for a standard (and standards-based) profile, mandatory for all service operations.

This Service Interface Profile (SIP) describes the key elements that make up the NNEC Core Enterprise Services (CES) Security Services. It describes the relationships between the various components, and any overarching data structures that are used by these components. The details of identified components are described in the respective SIPs (see [NCIA TR/2012/CPW007253/05, 2012], [NCIA TR/2012/CPW007253/06, 2012]).

This profile has evolved in response to the available technologies and mechanisms that can be used to apply security within a service-oriented environment. It aims to remain independent of

[1] https://servicestrategy.nr.ncia/SitePages/Agency%20Directives%20(Technical).aspx

implementation detail, and thus platform-neutral and technology-agnostic. The profile contained within this SIP has been tested against the service implementations of NATO and coalition member nations. Although the final implementation details have yet to be defined, which will be in the corresponding service interoperability points (SIOP), this SIP defines the high-level data structures that will be used between the components of the security services.

1.1 Audience

The target audience for this specification is the broad community of NNEC stakeholders, who are delivering capability in an NNEC environment, or anticipate that their services may be used in this environment.

These may include (but are not limited to):

- Project Managers procuring Bi-SC or NNEC related systems
- The architects and developers of service consumers and providers
- Coalition partners whose services may need to interact with NNEC services
- Systems integrators delivering systems into the NATO environment.

1.2 Notational Conventions

The following notational conventions apply to this document:

- The keywords "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in [IETF RFC 2119, 1997].
- Words in *italics* indicate terms referenced in Section 1.3.
- `Courier font` indicates syntax derived from the different open standards [OASIS WS-Security, 2006], [W3C WS-Addressing, 2006], [W3C XML-Signature, 2002], [OASIS SAML, 2005], [OASIS SAML Token Profile, 2006], and [WS-I Security, 2010].

1.3 Terminology

The following terminology is used in this SIP and its annexes.

Active Client	A Requestor that is able to make SOAP web service calls directly.
Attributes	Pieces of data concerning entities within a system.
Authentication	The process of establishing the identity of an entity.
Authorization	The process of establishing whether an entity is permitted to perform a particular operation on a resource.
Claims	The Attributes of an entity that are asserted by an entity contained within a Security Token.
Data Consumer	A service or application that calls other services in order to retrieve data.
Data Provider	A service that produces data for other services.
Header	The part of the Message that contains additional information about the message beyond the data that is being exchanged.
Identity Provider (IdP)	An entity that acts as an Authentication service to end-requestors and a data origin Authentication service to service providers. This is typically the role of a Security Token Service.
Message	The structure used for exchanging data between the Data Provider and Data Consumer.
Passive Client	A Requestor that is not able to make SOAP web service calls directly.
Policy Decision Point (PDP)	A service that provides Authorization decisions by evaluating policies against the Attributes of an entity.
Policy Enforcement Point (PEP)	A component that sits in the pipeline of the container of the Data Provider to ensure that security policies are applied.
Relying Party (RP)	This is the service that is protected by the PEP. It relies on the Authentication information presented in the Security Token. It is thus usually the Data Provider.
Requestor	An entity that is making a call to another service.
Security Token	A structure for distributing Claims between entities.
Security Token Service (STS)	A service that issues Security Tokens.

1.4 **Namespaces**

The following namespaces are used in this document and its annexes:

Abbreviation	Namespace	Reference	Version
saml	urn:oasis:names:tc:SAML:2.0:assertion	[OASIS SAML, 2005]	2.0
ds	http://www.w3.org/2000/09/xmldsig#	[W3C XML-Signature, 2002]	1.0
xenc	http://www.w3.org/2001/04/xmlenc#	[W3C XML-Encryption, 2002]	1.0
wsa	http://www.w3.org/2005/08/addressing	[W3C WS-Addressing, 2006]	1.0
wsse	http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-secext-1.0.xsd	[OASIS WS-Security, 2006]	1.0
wsse11	http://docs.oasis-open.org/wss/oasis-wss-wssecurity-secext-1.1.xsd	[OASIS WS-Security, 2006]	1.1
wsu	http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-1.0.xsd	[OASIS WS-Security, 2006]	1.0
wst	http://docs.oasis-open.org/ws-sx/ws-trust/200512	[OASIS WS-Trust, 2009]	1.3
wst14	http://docs.oasis-open.org/ws-sx/ws-trust/200802	[OASIS WS-Trust, 2009]	1.4
wsp	http://schemas.xmlsoap.org/ws/2004/09/policy *or* http://www.w3.org/ns/ws-policy	[OASIS WS-SecurityPolicy, 2009]	
fed	http://schemas.xmlsoap.org/ws/2006/12/federation	[WS-Federation, 2006]	1.1
soap	See [NCIA TR/2012/SPW008000/30, 2012]		

1.5 Goals

This SIP is intended to give directives, along with clarifications and amendments, on the use of mandatory and recommended interfaces and data structures to be implemented by the *STS* and *PEP* components of the NNEC CES Security Services. It also identifies the *PDP* as a separate logical component.

1.6 Non-Goals

The following topics are outside the scope of this profile:

- Recommendations for the use of products and platforms
- Modifications of the specification and the behaviours specified in any way

- Definitions of the *Attributes* and policies that will be used for making authorization decisions
- Specification of the transport or messaging formats for web service exchanges
- The specification for how the security requirements of a particular service will be exchanged with a consumer.

1.7 Relationships to Other Profiles and Specifications

1.7.1 Normative References

The following documents have fed into this specification, and are incorporated as normative references:

1.7.1.1 Security Assertion Markup Language (SAML) 2.0 (OASIS)

http://docs.oasis-open.org/security/saml/v2.0/saml-core-2.0-os.pdf

1.7.1.2 Web Services Security: SAML Token Profile 1.1(OASIS)

http://docs.oasis-open.org/wss/v1.1/wss-v1.1-spec-os-SAMLTokenProfile.pdf

1.7.1.3 XML Encryption Syntax and Processing 1.0 (W3C)

http://www.w3.org/TR/xmlenc-core/

1.7.1.4 XML Digital Signatures 1.0 (W3C)

http://www.w3.org/TR/xmldsig-core

1.7.1.5 WS-I Basic Security Profile 1.1(WS-I)

http://www.ws-i.org/Profiles/BasicSecurityProfile-1.1.html

2 SECURITY FOR WEB SERVICES

2.1 Subject

The purpose of the security services is to ensure the correct Authentication of users, and that they are authorized to perform particular actions. This is done through the distribution of identity information through the use of Security Tokens. The standard that is used to represent this identity with the NNEC CES Security Services is the Security Assertion Markup Language (SAML), version 2.0. This SIP describes how SAML tokens that are issued and used by the security services will be structured.

Figure 1 shows the logical view of the components that make up the suite of Security Services. A brief description of each is contained in Section 1.3. This SIP does not make any recommendations about the deployment of the components, some of which MAY be collocated with one another. The initial SIP proposals only cover interfaces and operations which are presented externally to the suite of security services, and so do not cover the *PDP*, which is internal, and only accessed by the *PEP*.

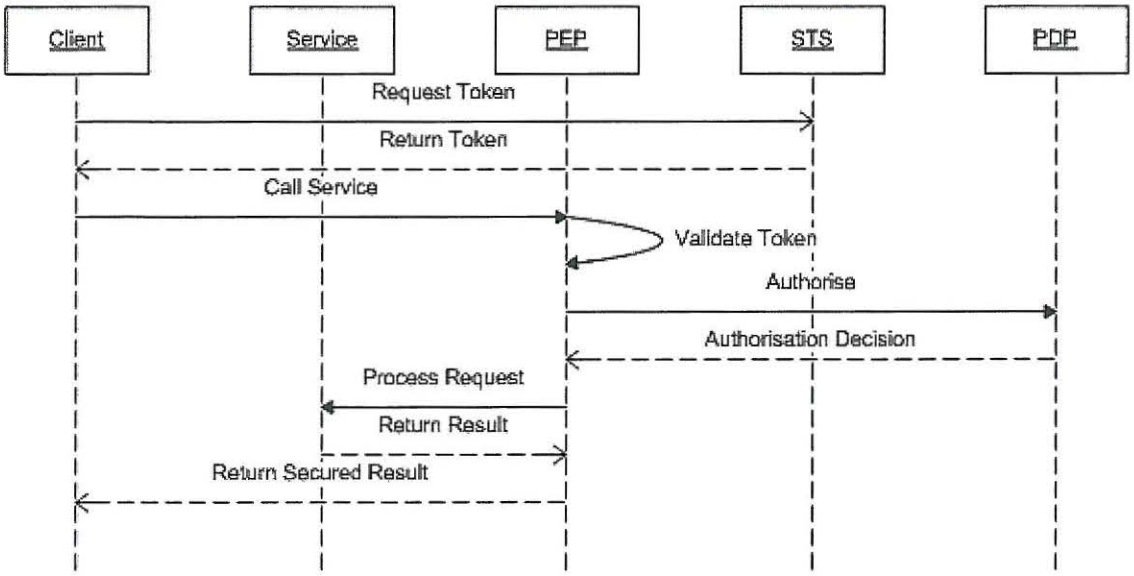

Figure 1 Security services sequence diagram

In order to access resources protected by the NNEC CES Security Services, the service consumer must present an extensible markup language (XML) *Security Token* for *Authentication*, that is, to present the credentials of the consuming entity to the service provider. Within the infrastructure of the CES, this token MUST be issued by a trusted party, or *IdP* typically implemented as an *STS*. For a more detailed description of the mechanisms used to protect services, see [NC3A RD-2814, 2009]. This SIP establishes the structure and content of the *Security Token* that will be used.

2.2 Supporting Infrastructure

2.2.1 Messaging

The SOAP messaging structure is described in [NCIA TR/2012/SPW008000/30, 2012]. However, for convenience, the high-level structure of both inbound and outbound messages used in secure exchanges is illustrated in Figure 2.

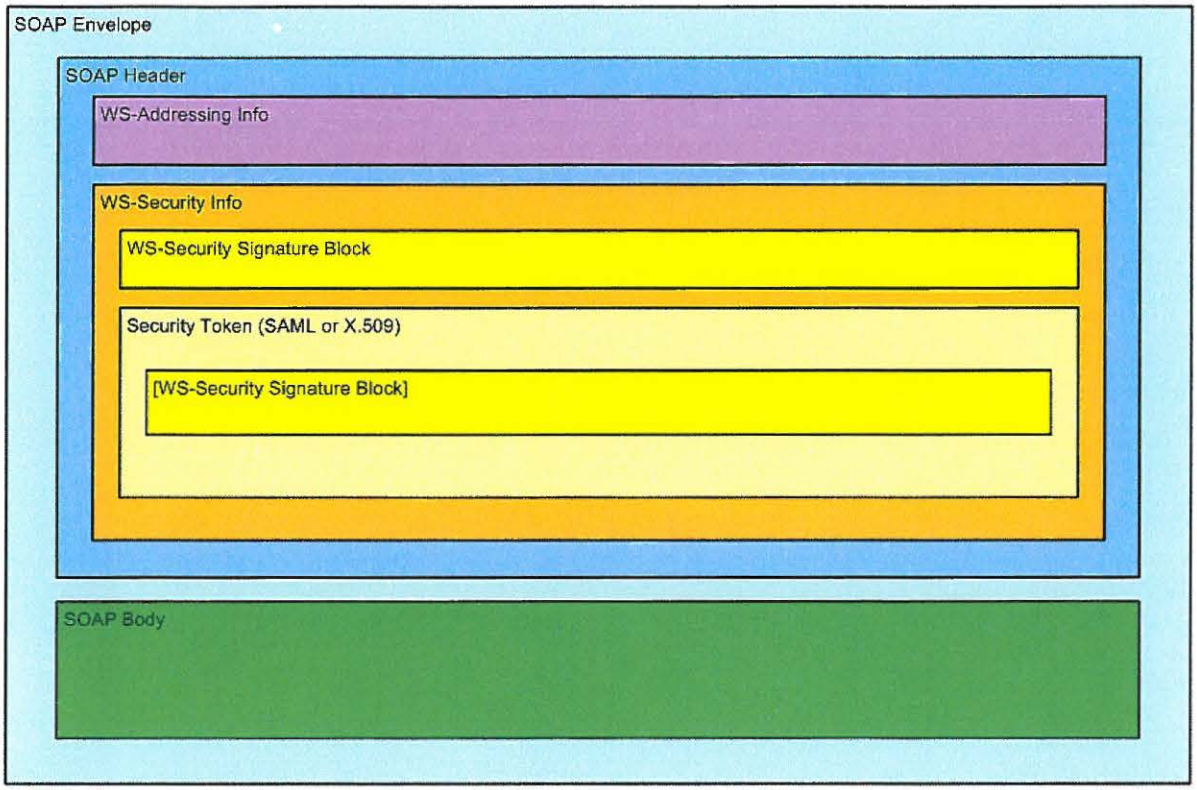

Figure 2 Message structure

In Figure 2, SAML security tokens are used for messages from the *Data Consumer* to the *Data Provider*, and the key from the SAML token is used for signing the message, whereas the responses from the provider to the consumer are signed with the asymmetric (private) key matching an X.509 binary security token. These structures are defined in more detail in [NCIA TR/2012/CPW007253/06, 2012].

2.2.2 Cryptography

In order to establish trust between the various components of the system, public key cryptography is used for both digital signatures and encryption. This SIP does not specify the cryptographic algorithms to be used, other than to state that:

NATO-approved algorithms MUST be used for both signatures and encryption. Within the NATO PKI it is unlikely that individual users will be issued with certificates in the early stages of deployment, but that services will be issued with certificates. This profile depends on the following PKI requirements:

- Each service MUST be issued with an X.509 v.3 certificate.
- Implementations of SAML MUST NOT rely on individual users having a certificate (see Section 3.2.3.1).

3 SECURITY TOKEN STRUCTURE

3.1 Purpose

The SAML assertion is used to evaluate authorization decisions for accessing a service, based on the *Claims* included within it. This SIP does not specify which *Attributes* will be contained within the token.

3.2 SAML Assertion

- The *Security Token* used by the security services MUST be an SAML 2.0 assertion.
- The SAML assertion MUST have the structure described below.
- The assertion MUST be signed internally, as per the SAML specification.
- The assertion MAY be encrypted for the *RP*. When encrypted for the *RP*, the public key from the certificate of the *RP* MUST be used for encrypting the token.

3.2.1.1 Encrypted assertions

The elements that will be present in the messages will also depend on whether the token is sent encrypted or unencrypted. The elements in an encrypted token are described in Section 3.2.2. When decrypted, the encrypted assertion MUST contain the same elements as an unencrypted assertion, as described in Section 3.2.3.

Examples of both encrypted and unencrypted tokens are given in Annex 1.

3.2.2 Elements (encrypted tokens)

Element	Notes
`/saml:EncryptedAssertion`	This element is a container for an `xenc:EncryptedData` element, which contains the encrypted *Security Token*. It is therefore REQUIRED, when encrypted tokens are used.
`/saml:EncryptedAssertion/xenc:EncryptedData`	This is a standard XML Encryption element which contains the encrypted SAML token. It is therefore REQUIRED.

3.2.3 Elements (unencrypted tokens)

Element	Notes
`/saml:Assertion`	This is the SAML token that contains the list of *Claims* that will be used for authorization of access to the service. It is REQUIRED.
`/saml:Assertion/saml:Issuer`	This specifies the URI of the *STS*. It is REQUIRED.
`/saml:Assertion/ds:Signature`	This contains the signature of elements in the SAML token, and so is REQUIRED.
`/saml:Assertion/saml:Subject`	The SAML Subject specifies who the end user is, and therefore is REQUIRED.
`/saml:Assertion/saml:Conditions`	This contains the constraints that should apply to acceptance of the token, and so it is RECOMMENDED. The RECOMMENDED *Attributes* are: `NotBefore` and `NotOnOrAfter`, which limits the time for which the token is valid. The RECOMMENDED child elements are: `<saml:AudienceRestriction>` element, which constrains the target for the *Security Token*.
`/saml:Assertion/saml:AttributeStatement`	This is the entire list of *Claims* that will be used for authorizing access to the protected service, and is therefore REQUIRED.
`/saml:Assertion/saml:AuthnStatement`	This specifies how the user was authenticated prior to issuance of the *Security Token*. As this may have an effect on the security requirements of a service, currently this is REQUIRED.

3.2.3.1 SubjectConfirmation

The `saml:SubjectConfirmation` element is used for "establishing the correspondence between the subject and *Claims* of SAML statements (in SAML assertions) and SOAP *Message* content" [OASIS SAML Token Profile, 2006]. It contains the key material that is used to sign the SOAP *Message*, and is therefore REQUIRED.

Element	Notes
/saml:Assertion/saml:Subject/saml:SubjectConfirmation	This MUST have a method attribute of value: urn:oasis:names:tc:SAML:2.0:cm:holder-of-key.
/saml:Assertion/saml:Subject/saml:SubjectConfirmation/saml:SubjectConfirmationData	This MUST contain a ds:KeyInfo element that is used to sign the elements within the *message* that are signed.
/saml:Assertion/saml:Subject/saml:SubjectConfirmation/saml:SubjectConfirmationData/ds:KeyInfo	The key used to sign the *Message* MAY be a symmetric key. Therefore any component handling SAML assertions MUST be able to accept a key that is not associated with a certificate (see Section 2.2.2). When a symmetric key is used, this key MUST be encrypted with the public key of the *RP*.

In accordance with [OASIS SAML Token Profile, 2006], the holder-of-key subject confirmation method MUST include a <ds:KeyInfo> element that identifies a public or secret (i.e. symmetric) key that can be used to confirm the identity of the subject. The attesting entity (i.e. the entity presenting the token) MUST demonstrate knowledge of the confirmation key. This SIP states that the attesting entity MUST use the confirmation key to sign the content within the message and include the resulting <ds:Signature> element in the <wsse:Security> header (outside of the <saml:Assertion> element).

When a symmetric confirmation key is used, it MUST be communicated by the attesting entity to the *STS* when requesting a *Security Token* as stated in [NCIA TR/2012/CPW007253/05, 2012].

3.2.3.2 Delegated Tokens

The structures for representing delegated tokens within a SAML assertion has yet to be finally standardized. However, the approach defined in [OASIS Delegation, 2009] is RECOMMENDED. Any other approach MUST be agreed between the *IdP* and the *RP* before delegated tokens will be accepted.

A delegated token SHOULD contain assertions for each of the delegates in the chain.

4 REFERENCES

[IETF RFC 2119, 1997]:
Internet Engineering Task Force Request for Comments 2119, "Key Words for Use in RFCs to Indicate Requirement Levels", S. Bradner, IETF, Sterling, Virginia, US, March 1997.

[NC3A RD-2814, 2009]:
NATO Consultation, Command and Control Agency Reference Document 2814, "Bi-SC AIS/NNEC SOA Implementation Guidance" *(provisional title)*, J. Busch, S. Brown, R. Fiske, G. Hallingstad, M. Lehman, NC3A, The Hague, Netherlands, unpublished document dated December 2009 (NATO Unclassified).

[NCIA TR/2012/CPW007253/05, 2012]:
NATO Communications and Information Agency Technical Report 2012/CPW007253/05, "Security Services Service Interface Profile Proposal for Security Token Service", R. Fiske, M. Lehmann, R. Malewicz, L. Schenkels, D. Gujral, NCIA, The Hague, Netherlands, October 2012 (NATO Unclassified).

[NCIA TR/2012/CPW007253/06, 2012]:
NATO Communications and Information Agency Technical Report 2012/CPW007253/06, "Security Services Service Interface Profile Proposal for A Policy Enforcement Point", R. Fiske, M. Lehmann, R. Malewicz, L. Schenkels, D.Gujral, NCIA, The Hague, Netherlands, October 2012 (NATO Unclassified).

[NCIA TR/2012/SPW008000/30, 2012]:
NATO Communications and Information Agency Technical Report 2012/SPW008000/30, "Messaging Service Interface Profile Proposal", R. Fiske, M. Lehmann, NCIA, The Hague, Netherlands, October 2012 (NATO Unclassified).

[OASIS Delegation, 2009]:
Organization for the Advancement of Structured Information Standards (on-line), http://www.oasis-open.org, SAML V2.0 Condition for Delegation Restriction Version 1.0, at http://docs.oasis-open.org/security/saml/Post2.0/sstc-saml-delegation.pdf, 15 November 2009, viewed 30 March 2011.

[OASIS SAML, 2005]:
Organization for the Advancement of Structured Information Standards (on-line), http://www.oasis-open.org, Assertions and Protocols for the OASIS Security Assertion Markup Language (SAML) V2.0., at http://docs.oasis-open.org/security/saml/v2.0/saml-core-2.0-os.pdf, 15 March 2005, viewed 30 March 2011.

[OASIS SAML Token Profile, 2006]:
Organization for the Advancement of Structured Information Standards (on-line), http://www.oasis-open.org, Web Services Security: SAML Token Profile 1.1, at http://docs.oasis-open.org/wss/v1.1/wss-v1.1-spec-os-SAMLTokenProfile.pdf, 1 February 2006, viewed 30 March 2011.

[OASIS WS-Security, 2006]:
Organization for the Advancement of Structured Information Standards (on-line), http://www.oasis-open.org, Web Services Security: SOAP Message Security 1.1, at http://docs.oasis-open.org/wss/v1.1/wss-v1.1-spec-os-SOAPMessageSecurity.pdf, 1 February 2006, viewed 30 March 2011.

[OASIS WS-SecurityPolicy, 2009]:
Organization for the Advancement of Structured Information Standards (on-line), http://www.oasis-open.org, WS-SecurityPolicy 1.3, at http://docs.oasis-open.org/ws-sx/ws-securitypolicy/v1.3/ws-securitypolicy.html, 2 February 2009, viewed 30 March 2011.

[OASIS WS-Trust, 2009]:
Organization for the Advancement of Structured Information Standards (on-line), http://www.oasis-open.org, "WS-Trust 1.4" at http://docs.oasis-open.org/ws-sx/ws-trust/v1.4/ws-trust.doc, 2 February 2009, viewed 30 March 2011.

[W3C WS-Addressing, 2006]:
World Wide Consortium (on-line), http://www.w3.org, Web Services Addressing 1.0 – Core, at http://www.w3.org/TR/2006/REC-ws-addr-core-20060509/, 9 May 2006, viewed 30 March 2011.

[W3C XML-Encryption, 2002]:
World Wide Consortium (on-line), http://www.w3.org, XML Encryption Syntax and Processing, at http://www.w3.org/TR/xmlenc-core/, 10 December 2002, viewed 30 March 2011.

[W3C XML-Signature, 2002]:
World Wide Consortium (on-line), http://www.w3.org, XML-Signature Syntax and Processing, at http://www.w3.org/TR/2002/REC-xmldsig-core-20020212/Overview.html, 12 February 2002, viewed 30 March 2011.

[WS-Federation, 2006]:
WS-Federation (on-line), Web Services Federation Language (WS Federation) Version 1.1, at http://specs.xmlsoap.org/ws/2006/12/federation/ws-federation.pdf, December 2006, viewed 30 March 2011.

[WS-I Security, 2010]:
Web Services Interoperability Organization (on-line), http://www.ws-i.org, Basic Security Profile Version 1.1, at http://www.ws-i.org/Profiles/BasicSecurityProfile-1.1.html, 24 January 2010, viewed 30 March 2011.

5 ABBREVIATIONS

CES	Core Enterprise Services
IdP	Identity provider
NNEC	NATO Network Enabled Capability
PDP	Policy decision point
PEP	Policy enforcement point
RP	Relying party
SAML	Security assertion markup language
SIOP	Service interoperability point
SIP	Service Interface Profile
STS	Security token service
XML	Extensible markup language

ANNEX 1 – XML SAMPLES

1.1 Token Samples

The following represents non-normative examples of encrypted and unencrypted tokens from the *Security Token Service*.

1.1.1 Encrypted SAML Token

```
<EncryptedAssertion xmlns="urn:oasis:names:tc:SAML:2.0:assertion">
  <xenc:EncryptedData Type="http://www.w3.org/2001/04/xmlenc#Element"
xmlns:xenc="http://www.w3.org/2001/04/xmlenc#">
    <xenc:EncryptionMethod Algorithm="http://www.w3.org/2001/04/xmlenc#aes256-
cbc"></xenc:EncryptionMethod>
    <KeyInfo xmlns="http://www.w3.org/2000/09/xmldsig#">
      <e:EncryptedKey xmlns:e="http://www.w3.org/2001/04/xmlenc#">
        <e:EncryptionMethod Algorithm="http://www.w3.org/2001/04/xmlenc#rsa-oaep-
mgf1p">

          <DigestMethod
     Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"></DigestMethod>
        </e:EncryptionMethod>
        <KeyInfo>
          <ds:X509Data xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
            <ds:X509IssuerSerial>
              <ds:X509IssuerName>..Cert Issuer..</ds:X509IssuerName>
              <ds:X509SerialNumber>..Cert Ref..</ds:X509SerialNumber>
            </ds:X509IssuerSerial>
          </ds:X509Data>
        </KeyInfo>
        <e:CipherData>
          <e:CipherValue>..Encrypted Key..</e:CipherValue>
        </e:CipherData>
      </e:EncryptedKey>
    </KeyInfo>
    <xenc:CipherData>
      <xenc:CipherValue>..Encrypted SAML Token..</xenc:CipherValue>
    </xenc:CipherData>
  </xenc:EncryptedData>
</EncryptedAssertion>
```

1.1.2 Unencrypted SAML token

```
<Assertion ID="_e3534d1e-a301-462c-ad72-46fe56c995c8" IssueInstant="2010-11-
23T12:14:18.382Z" Version="2.0" xmlns="urn:oasis:names:tc:SAML:2.0:assertion">
        <Issuer>..Token Issuer..</Issuer>
        <ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
    <ds:SignedInfo>
      <ds:CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-exc-
c14n#"></ds:CanonicalizationMethod>
      <ds:SignatureMethod Algorithm="http://www.w3.org/2001/04/xmldsig-more#rsa-
sha256"></ds:SignatureMethod>
      <ds:Reference URI="#_e3534d1e-a301-462c-ad72-46fe56c995c8">
        <ds:Transforms>
          <ds:Transform Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-
signature"></ds:Transform>
          <ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-
c14n#"></ds:Transform>
        </ds:Transforms>
        <ds:DigestMethod
Algorithm="http://www.w3.org/2001/04/xmlenc#sha256"></ds:DigestMethod>

<ds:DigestValue>C4uizWDjuFgPlRf9Eh8G6ssZsVByFp7rSf9Gd+butds=</ds:DigestValue>
```

```
      </ds:Reference>
    </ds:SignedInfo>
    <ds:SignatureValue>..Signature Value..</ds:SignatureValue>
    <KeyInfo xmlns="http://www.w3.org/2000/09/xmldsig#">
      <ds:X509Data>
        <ds:X509Certificate>..Base64 Encoded Issuer
Certificate..</ds:X509Certificate>
      </ds:X509Data>
    </KeyInfo>
  </ds:Signature>
  <Subject>
    <SubjectConfirmation Method="urn:oasis:names:tc:SAML:2.0:cm:holder-of-key">
      <SubjectConfirmationData a:type="KeyInfoConfirmationDataType"
xmlns:a="http://www.w3.org/2001/XMLSchema-instance">
        <KeyInfo xmlns="http://www.w3.org/2000/09/xmldsig#">
          <e:EncryptedKey xmlns:e="http://www.w3.org/2001/04/xmlenc#">
            <e:EncryptionMethod Algorithm="http://www.w3.org/2001/04/xmlenc#rsa-
oaep-mgf1p">
              <DigestMethod
Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"></DigestMethod>
            </e:EncryptionMethod>
            <KeyInfo>
              <ds:X509Data xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
                <ds:X509IssuerSerial>
                  <ds:X509IssuerName>..Cert Issuer..</ds:X509IssuerName>
                  <ds:X509SerialNumber>..Cert Ref..</ds:X509SerialNumber>
                </ds:X509IssuerSerial>
              </ds:X509Data>
            </KeyInfo>
            <e:CipherData>
              <e:CipherValue>..Encrypted Key..</e:CipherValue>
            </e:CipherData>
          </e:EncryptedKey>
        </KeyInfo>
      </SubjectConfirmationData>
    </SubjectConfirmation>
  </Subject>
  <Conditions NotBefore="2010-11-23T12:14:18.368Z" NotOnOrAfter="2010-11-
23T13:14:18.368Z">
    <AudienceRestriction>
      <Audience>..Relying Party URI..</Audience>
    </AudienceRestriction>
  </Conditions>
  <AttributeStatement>
    <Attribute Name="http://schemas.xmlsoap.org/claims/UPN">
      <AttributeValue>
        ..Value from Directory..
      </AttributeValue>
    </Attribute>
    <Attribute Name="http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name">
      <AttributeValue>
        ..Value from Directory..
      </AttributeValue>
      <AttributeValue>
        ..Value from Directory..
      </AttributeValue>
    </Attribute>
    <Attribute Name="http://schemas.xmlsoap.org/claims/EmailAddress">
      <AttributeValue>
        ..Value from Directory..
      </AttributeValue>
    </Attribute>
  </AttributeStatement>
  <AuthnStatement AuthnInstant="2010-11-23T12:14:18.315Z">
    <AuthnContext>
```

```
<AuthnContextClassRef>urn:federation:authentication:windows</AuthnContextClassRef>
    </AuthnContext>
  </AuthnStatement>
</Assertion>
```