Assertion Protocol Specification 2.0 Revision 1.2

*Written By Philip Vendil,* [p.vendil@logica.com](mailto:p.vendil@logica.com) *+46709885814*

Table of Contents

1 Introduction 3

1.1 Document History 3

1.2 Notation 3

1.3 Schema Organization and Namespaces 4

2 Assertion Data Structures used in CSMessage 2.0 Messages 5

2.1 Assertion Data Structure Overview 5

2.2 Distributed Authorization Request 5

2.3 Distributed Authorization Ticket 6

2.4 User Data Request 9

2.5 User Data Ticket 9

2.6 Approval Ticket 13

# 1 Introduction

This document defines the data structures for generating assertions. These data structures are based on the SAML 2.0 specification.

## 1.1 Document History

|  |  |  |  |
| --- | --- | --- | --- |
| ***Version*** | ***Date*** | ***Author*** | ***Comment*** |
| 2.0 r1.0 | 2015-02-09 | Philip Vendil | Initial Version |
| 2.0 r1.1 | 2015-09-01 | Philip Vendil | Added TokenType to UserData Request and Response |
| 2.0 r1.2 | 2017-03-09 | Philip Vendil | Added DEPARTMENT attribute to Distributed Authorization Ticket. |

## 1.2 Notation

In this document is the terms credential and certificate used in the context of this document mean the same thing. But the term credential could in the future be extended to other forms of identification.

The keywords "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this specification are to be interpreted as described in IETF RFC 2119.

This specification uses schema documents conforming to W3C XML Schema and normative text to describe the syntax and semantics of XML-encoded messages. Conventional XML namespace prefixes are used throughout the listings in this specification to stand for their respective namespaces as follows, whether or not a namespace declaration is present in the example:

|  |  |  |
| --- | --- | --- |
| Prefix | XML Namespace | **Comments** |
| cs: | http://certificateservices.org/xsd/csmessages2\_0 | This is the namespace of the core parts of the CS message protocol |
| cm | http://certificateservices.org/xsd/credmanagement2\_0 | Namespace of Credential Management Payloads of the CS message protocol. |
| ds: | [http://www.w3.org/2000/09/xmldsig#](http://www.w3.org/2000/09/xmldsig%23) | This namespace is defined in the XML Signature Syntax and Processing specification and its governing schema. |
| saml: | urn:oasis:names:tc:SAML:2.0:assertion | This is the SAML V2.0 assertion namespace, defined in a  schema [SAML-XSD]. The prefix is generally elided in  mentions of SAML assertion-related elements in text. |
| xenc: | http://www.w3.org/2001/04/xmlenc# | This namespace is defined in the XML Encryption Syntax  and Processing specification [XMLEnc] and its governing  schema [XMLEnc-XSD]. |

## 1.3 Schema Organization and Namespaces

This message schema uses the SAML2 Core namespaces defined in:

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

# 2 Assertion Data Structures used in CSMessage 2.0 Messages

## 2.1 Assertion Data Structure Overview

The assertion data structures is based on the SAML 2.0 standard and used in the CSMessage protocol to have distributed authorization, approval workflows and the fetch User Data from a local repository.

There are five kinds of assertion request or tickets that can be generated, and each is described in a separate subsection below:

* Distributed Authorization Request and Ticket, used when authorization (role) should be done from a local repository (such as AD) towards the central service.
* User Data Request and Ticket, Used when requesting user data from a local repository (AD) for credentials issued centrally.
* Approval Ticket, for request that have been approved using an approval workflow.

## 2.2 Distributed Authorization Request

To request a set of roles from an IDP should the following request message be sent:

* IssueInstant: Time the request was generated
* Version: SAML version (always 2.0)
* ID: Unique id of the request, should be a random generated string.
* Subject with NameId: The unique id of the user to look-up, could be UPN or SAM account name depending on implementation.
* Attribute: Should have the name = “Roles” and an empty set of AttributeValues
* Signature: Signature by the requester.

|  |
| --- |
| <?xml version="1.0" encoding="UTF-8"?><samlp:AttributeQuery xmlns:ds="http://www.w3.org/2000/09/xmldsig#" xmlns:xenc="http://www.w3.org/2001/04/xmlenc#" xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion" xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol" ID="\_E5EC8C6C-A9C9-424F-aD4E-467F3673029A" Version="2.0" IssueInstant="2015-07-07T16:26:53.000+02:00">  <saml:Subject>  <saml:NameID>SomeSubjectId@someorg</saml:NameID>  </saml:Subject>  <saml:Attribute Name="Roles"/>  </samlp:AttributeQuery> |

## 2.3 Distributed Authorization Ticket

Upon receiving an authorization request attribute query should the following ticket be returned. If the user doesn’t have any applicable roles should the attribute value (inside the encrypted value) be and empty string.

* IssueInstant: Time the request was generated
* Version: SAML version (always 2.0)
* InResponseTo: The is of the request this is a response to.
* ID: Unique id of the samp response, should be a random generated string.
* Status: If request was successful or not, standard SAML 2.0 status codes are used. (3.2.2.2 in SAML 2.0 Core), a descriptive status message is required.
* Assertion:
  + Subject with NameId, The unique id of the related user, could be UPN or SAM account name depending on implementation.
  + Conditions with NotBefore and NotOnOfAfter, the timespan for which this ticket is valid.
  + An AttributeStatement with attributes:
    - A ‘Type’ attribute with the value ‘AUTHORIZATION\_TICKET’.
    - The ‘Roles’ Attribute encrypted with the receiving service key. At minimum should the EncryptedData contain type: [http://www.w3.org/2001/04/xmlenc#Element](http://www.w3.org/2001/04/xmlenc%23element)but could also contain encryption key information if applicable. For example should cs-proxy encrypt the role data with the cs-admins private key, this to restrict the requester for seeing the role data for the use case he is querying someone else than himself and to prevent information leakage.  
        
      The encrypted SAML Attribute statement should have the name Roles and a set of AttributeValue containing a string of each role.
    - An optional ‘Departments’ specifying the departments the requester belongs to. This attribute if exists is encrypted using the same specification as ‘Roles’ attribute.

Each value specifies an authorized department and the special reserved value ‘ALL\_DEPARTMENTS’ indicates that the user has access to all an organisations departments.

|  |
| --- |
| <?xml version="1.0" encoding="UTF-8"?><samlp:Response xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol" xmlns:ds="http://www.w3.org/2000/09/xmldsig#" xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion" xmlns:xenc="http://www.w3.org/2001/04/xmlenc#" ID="\_FD178D0E-CB06-4543-b324-C2D8E01BF9AB" InResponseTo="\_123456789" IssueInstant="2015-07-07T16:26:53.000+02:00" Version="2.0">  <samlp:Status>  <samlp:StatusCode Value="urn:oasis:names:tc:SAML:2.0:status:Success"/>  </samlp:Status>  <saml:Assertion ID="\_91C7D7C7-0302-436C-8660-D149F754FF57" IssueInstant="2015-07-07T16:26:53.000+02:00" Version="2.0">  <saml:Issuer>someIssuer</saml:Issuer>  <ds:Signature xmlns="http://www.w3.org/2000/09/xmldsig#">  <SignedInfo>  <CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>  <SignatureMethod Algorithm="http://www.w3.org/2001/04/xmldsig-more#rsa-sha256"/>  <Reference URI="#\_91C7D7C7-0302-436C-8660-D149F754FF57">  <Transforms>  <Transform Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature"/>  </Transforms>  <DigestMethod Algorithm="http://www.w3.org/2001/04/xmlenc#sha256"/>  <DigestValue>kLUMxbDERfNsGkJxgBRZiBxcCNcAWoeDSP7iMvApSWQ=</DigestValue>  </Reference>  </SignedInfo>  <SignatureValue>AKye…</SignatureValue>  <KeyInfo>  <X509Data>  <X509Certificate>MIID0jCC…..X509Certificate>  </X509Data>  </KeyInfo>  </ds:Signature>  <saml:Subject>  <saml:NameID>SomeSubject</saml:NameID>  </saml:Subject>  <saml:Conditions NotBefore="2015-07-07T16:26:52.427+02:00" NotOnOrAfter="2015-07-07T16:28:32.427+02:00"/>  <saml:AttributeStatement>  <saml:Attribute Name="Type">  <saml:AttributeValue xmlns:xs="http://www.w3.org/2001/XMLSchema" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xsi:type="xs:string">AUTHORIZATION\_TICKET</saml:AttributeValue>  </saml:Attribute>  <saml:EncryptedAttribute>  <xenc:EncryptedData Type="http://www.w3.org/2001/04/xmlenc#Element">  <xenc:EncryptionMethod Algorithm="http://www.w3.org/2001/04/xmlenc#aes256-cbc"/>  <ds:KeyInfo>  <xenc:EncryptedKey>  <xenc:EncryptionMethod Algorithm="http://www.w3.org/2001/04/xmlenc#rsa-oaep-mgf1p"/>  <ds:KeyInfo>  <ds:KeyName>A2a5JrfZL6oHCSexVqT9GyeV66QaYYY1YbqU+/eDkyc=</ds:KeyName>  </ds:KeyInfo>  <xenc:CipherData>  <xenc:CipherValue>8sDqzwvAsU5A..</xenc:CipherValue>  </xenc:CipherData>  </xenc:EncryptedKey>  <xenc:EncryptedKey>  <xenc:EncryptionMethod Algorithm="http://www.w3.org/2001/04/xmlenc#rsa-oaep-mgf1p"/>  <ds:KeyInfo>  <ds:KeyName>yrhA2ngreu9CwRBvbfKReRFRmZk/GB50/vT6IhgT8no=</ds:KeyName>  </ds:KeyInfo>  <xenc:CipherData>  <xenc:CipherValue>zuXPqCH00HgHQ…</xenc:CipherValue>  </xenc:CipherData>  </xenc:EncryptedKey>  </ds:KeyInfo>  <xenc:CipherData>  <xenc:CipherValue>…</xenc:CipherValue>  </xenc:CipherData>  </xenc:EncryptedData>  </saml:EncryptedAttribute>  </saml:AttributeStatement>  </saml:Assertion>  </samlp:Response> |

## 2.4 User Data Request

The User Data Request is almost identical to the Authorization Request with the difference that the attribute name should be ‘UserData’ and an attribute ‘TokenType’ specifying the token type to fetch data for.

|  |
| --- |
| <?xml version="1.0" encoding="UTF-8"?><samlp:AttributeQuery xmlns:ds="http://www.w3.org/2000/09/xmldsig#" xmlns:xenc="http://www.w3.org/2001/04/xmlenc#" xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion" xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol" ID="\_7136B451-CB2B-4CF5-b49E-FAE16A5C9D09" Version="2.0" IssueInstant="2015-07-07T16:26:53.000+02:00">  <saml:Subject>  <saml:NameID>SomeSubjectId@someorg</saml:NameID>  </saml:Subject>  <saml:Attribute Name=“UserData”/>  <saml:Attribute Name=“TokenType"/>  <saml:AttributeValue >SomeTokenType</saml:AttributeValue>  </saml:Attribute>  </samlp:AttributeQuery> |

## 2.5 User Data Ticket

The User Data ticket is identical to the Authorization ticket but with the following changes:

* Subject with NameId, The unique id of the related user, should be the same as in the User Data Request.
* The Conditions element have the OneTimeUse element which indicates that this UserData ticket might only be used once.
* The AttributeStatement should contain three attributes:
  + One Attribute with type ‘TokenType’ specifying which token type the UserData is valid for.
  + One Attribute with name ‘DisplayName’, an unencrypted attribute containing one AttributeValue containing the display name of the user.
  + One Attriubte with name ‘Type’ and value ‘USER\_DATA’
  + One EncryptedAttribute containing a Attribute element with name ‘UserData’ and a AttributeValue containing a cm:TokenRequest where all fields where data exists should be set, or if schema says required and no data is valid should ‘NOTSET’. The UserData will override the administrator specified token values in the TokenRequest sent.

|  |
| --- |
| <?xml version="1.0" encoding="UTF-8"?><samlp:Response xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol" xmlns:ds="http://www.w3.org/2000/09/xmldsig#" xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion" xmlns:xenc="http://www.w3.org/2001/04/xmlenc#" ID="\_F862E7FA-590D-467D-aD53-05FCB46BFA00" InResponseTo="\_123456789" IssueInstant="2015-07-07T16:26:53.000+02:00" Version="2.0">  <samlp:Status>  <samlp:StatusCode Value="urn:oasis:names:tc:SAML:2.0:status:Success"/>  </samlp:Status>  <saml:Assertion ID="\_16C80D9F-2FF2-467B-b6DD-C7362A5EC1F0" IssueInstant="2015-07-07T16:26:53.000+02:00" Version="2.0">  <saml:Issuer>someIssuer</saml:Issuer>  <ds:Signature xmlns="http://www.w3.org/2000/09/xmldsig#">  <SignedInfo>  <CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>  <SignatureMethod Algorithm="http://www.w3.org/2001/04/xmldsig-more#rsa-sha256"/>  <Reference URI="#\_16C80D9F-2FF2-467B-b6DD-C7362A5EC1F0">  <Transforms>  <Transform Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature"/>  </Transforms>  <DigestMethod Algorithm="http://www.w3.org/2001/04/xmlenc#sha256"/>  <DigestValue>/ofQyVfPjciJcpD9KGoMXopkz5F155NcadWHZl/NSdc=</DigestValue>  </Reference>  </SignedInfo>  <SignatureValue>oeQ..</SignatureValue>  <KeyInfo>  <X509Data>  <X509Certificate>MIID….X509Certificate>  </X509Data>  </KeyInfo>  </ds:Signature>  <saml:Subject>  <saml:NameID>SomeSubject</saml:NameID>  </saml:Subject>  <saml:Conditions NotBefore="2015-07-07T16:26:52.427+02:00" NotOnOrAfter="2015-07-07T16:28:32.427+02:00"/>  <saml:AttributeStatement>  <saml:Attribute Name="Type">  <saml:AttributeValue xmlns:xs="http://www.w3.org/2001/XMLSchema" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xsi:type="xs:string">USER\_DATA</saml:AttributeValue>  </saml:Attribute>  <saml:Attribute Name="TokenType">  <saml:AttributeValue xmlns:xs="http://www.w3.org/2001/XMLSchema" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xsi:type="xs:string">SomeTokenType</saml:AttributeValue>  </saml:Attribute>  <saml:Attribute Name="DisplayName">  <saml:AttributeValue xmlns:xs="http://www.w3.org/2001/XMLSchema" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xsi:type="xs:string">SomeDisplayName</saml:AttributeValue>  </saml:Attribute>  <saml:EncryptedAttribute>  <xenc:EncryptedData Type="http://www.w3.org/2001/04/xmlenc#Element">  <xenc:EncryptionMethod Algorithm="http://www.w3.org/2001/04/xmlenc#aes256-cbc"/>  <ds:KeyInfo>  <xenc:EncryptedKey>  <xenc:EncryptionMethod Algorithm="http://www.w3.org/2001/04/xmlenc#rsa-oaep-mgf1p"/>  <ds:KeyInfo>  <ds:KeyName>A2a5JrfZL6oHCSexVqT9GyeV66QaYYY1YbqU+/eDkyc=</ds:KeyName>  </ds:KeyInfo>  <xenc:CipherData>  <xenc:CipherValue>aAD..</xenc:CipherValue>  </xenc:CipherData>  </xenc:EncryptedKey>  <xenc:EncryptedKey>  <xenc:EncryptionMethod Algorithm="http://www.w3.org/2001/04/xmlenc#rsa-oaep-mgf1p"/>  <ds:KeyInfo>  <ds:KeyName>yrhA2ngreu9CwRBvbfKReRFRmZk/GB50/vT6IhgT8no=</ds:KeyName>  </ds:KeyInfo>  <xenc:CipherData>  <xenc:CipherValue>zX94… </xenc:CipherValue>  </xenc:CipherData>  </xenc:EncryptedKey>  </ds:KeyInfo>  <xenc:CipherData>  <xenc:CipherValue>gx7…..</xenc:CipherValue>  </xenc:CipherData>  </xenc:EncryptedData>  </saml:EncryptedAttribute>  </saml:AttributeStatement>  </saml:Assertion>  </samlp:Response> |

## 2.6 Approval Ticket

Approval Ticket is generated by the approval engine after an approval request has been approved.The returned data structure is not a SAMLP response but directly a signed assertion.

* IssueInstant: Time the request was generated
* Version: SAML version (always 2.0)
* ID: Unique id of the assertion, should be a random generated string.
* Saml Attribute with name ‘Type’ and value ‘APPROVAL\_TICKET’
* Saml Attribute with name ‘DestinationId’ and value the id of the destination system that should process the ticket. (Optional)
* Saml Attribute with name “ApprovalId” and the for the request unique approval id as attribute value. Only one AttributeValue
* Saml Attribute called “ApprovedRequest” containing one or more AttributeValue with the digest values of the calculated request actions. It’s up to the approval workflow engine to to determine how the digest is calculated from an approval request and how to verify that subsequent request matches the given approval.
* One encrypted attribute with name ‘Approvers’ containing a list of Approver elements defined in CS Message Core XSD. Each approver contains information about who approved the request and should be encrypted to the request processing system only and not clients.

Under Conditions is OneTimeUse element not applicable, it’s up to the verifying approval engine to determine if the assertion have been used or not.

|  |
| --- |
| <?xml version="1.0" encoding="UTF-8"?><saml:Assertion xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion" xmlns:ds="http://www.w3.org/2000/09/xmldsig#" xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol" xmlns:xenc="http://www.w3.org/2001/04/xmlenc#" ID="\_CD0028B3-0AFA-4C05-951D-CEB64AB43AAF" IssueInstant="2015-07-07T16:26:53.000+02:00" Version="2.0">  <saml:Issuer>someIssuer</saml:Issuer>  <ds:Signature xmlns="http://www.w3.org/2000/09/xmldsig#">  <SignedInfo>  <CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>  <SignatureMethod Algorithm="http://www.w3.org/2001/04/xmldsig-more#rsa-sha256"/>  <Reference URI="#\_CD0028B3-0AFA-4C05-951D-CEB64AB43AAF">  <Transforms>  <Transform Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature"/>  </Transforms>  <DigestMethod Algorithm="http://www.w3.org/2001/04/xmlenc#sha256"/>  <DigestValue>CiG93httreL6aMqZdSKlzrjHVgbTzP8rd/BaY7DSo1I=</DigestValue>  </Reference>  </SignedInfo>  <SignatureValue>h7s2…SignatureValue>  <KeyInfo>  <X509Data>  <X509Certificate>MII…</X509Certificate>  </X509Data>  </KeyInfo>  </ds:Signature>  <saml:Subject>  <saml:NameID>SomeSubject</saml:NameID>  </saml:Subject>  <saml:Conditions NotBefore="2015-07-07T16:26:52.427+02:00" NotOnOrAfter="2015-07-07T16:28:32.427+02:00"/>  <saml:AttributeStatement>  <saml:Attribute Name="Type">  <saml:AttributeValue xmlns:xs="http://www.w3.org/2001/XMLSchema" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xsi:type="xs:string">APPROVAL\_TICKET</saml:AttributeValue>  </saml:Attribute>  <saml:Attribute Name="DestinationId">  <saml:AttributeValue xmlns:xs="http://www.w3.org/2001/XMLSchema" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xsi:type="xs:string">SomeDestination</saml:AttributeValue>  </saml:Attribute>  <saml:Attribute Name="ApprovalId">  <saml:AttributeValue xmlns:xs="http://www.w3.org/2001/XMLSchema" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xsi:type="xs:string">1234</saml:AttributeValue>  </saml:Attribute>  <saml:Attribute Name="ApprovedRequests">  <saml:AttributeValue xmlns:xs="http://www.w3.org/2001/XMLSchema" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xsi:type="xs:string">abcdef</saml:AttributeValue>  <saml:AttributeValue xmlns:xs="http://www.w3.org/2001/XMLSchema" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xsi:type="xs:string">defcva</saml:AttributeValue>  </saml:Attribute>  <saml:EncryptedAttribute>  <xenc:EncryptedData Type="http://www.w3.org/2001/04/xmlenc#Element">  <xenc:EncryptionMethod Algorithm="http://www.w3.org/2001/04/xmlenc#aes256-cbc"/>  <ds:KeyInfo>  <xenc:EncryptedKey>  <xenc:EncryptionMethod Algorithm="http://www.w3.org/2001/04/xmlenc#rsa-oaep-mgf1p"/>  <ds:KeyInfo>  <ds:KeyName>A2a5JrfZL6oHCSexVqT9GyeV66QaYYY1YbqU+/eDkyc=</ds:KeyName>  </ds:KeyInfo>  <xenc:CipherData>  <xenc:CipherValue>RnxY…xenc:CipherValue>  </xenc:CipherData>  </xenc:EncryptedKey>  <xenc:EncryptedKey>  <xenc:EncryptionMethod Algorithm="http://www.w3.org/2001/04/xmlenc#rsa-oaep-mgf1p"/>  <ds:KeyInfo>  <ds:KeyName>yrhA2ngreu9CwRBvbfKReRFRmZk/GB50/vT6IhgT8no=</ds:KeyName>  </ds:KeyInfo>  <xenc:CipherData>  <xenc:CipherValue>llf..</xenc:CipherValue>  </xenc:CipherData>  </xenc:EncryptedKey>  </ds:KeyInfo>  <xenc:CipherData>  <xenc:CipherValue>eFX7…xenc:CipherValue>  </xenc:CipherData>  </xenc:EncryptedData>  </saml:EncryptedAttribute>  </saml:AttributeStatement>  </saml:Assertion> |