# Interface specifications DV-HM

|  |
| --- |
| **DV-HM sequence diagram** |
| C:\423037a0fd79d949bf0435f3bac36777 |

This page describes the messages for the interface specification between a [Dienstverlener (DV)](file:///H:\pages\viewpage.action%3fpageId=13926456) (service provider) and an [Herkenningsmakelaar (HM)](file:///H:\pages\viewpage.action%3fpageId=13926461) (broker).

The interface specification described in this document is used to implement the use case [GUC1 Gebruiken eToegang als dienstafnemer](file:///H:\display\BEHEERAS\GUC1+Gebruiken+eToegang+als+dienstafnemer) (Use eToegang as service consumer) and MUST (with the exception of alternative [Bindings](file:///H:\display\BEHEERAS\Bindings)) be implemented by every Herkenningsmakelaar and offered to their customers, the DVs. This is in order to prevent lock-in and enables middleware suppliers to write generic code that can be used by all Herkenningsmakelaars.

In the interface described here, the use case [GUC1 Gebruiken eToegang als dienstafnemer](file:///H:\display\BEHEERAS\GUC1+Gebruiken+eToegang+als+dienstafnemer) is populated with an SAML 2.0 AuthnRequest and Response.

The specific contents of these messages is described below. A column in a message description that starts with 'SAML:' indicates that this is a standard value within the official SAML specification. A value that starts with 'Elektronische Toegangsdiensten' indicates that the value is specific to Elektronische Toegangsdiensten.

[ [AuthnRequest (1)](#InterfacespecificationsDV-HM-AuthnReque) ] [ [Rules for processing requests](#InterfacespecificationsDV-HM-Rulesforpr) ] [ [Response (2)](#InterfacespecificationsDV-HM-Response(2) ] [ [HM Summary assertion](#InterfacespecificationsDV-HM-HMSummarya) ] [ [AttributeStatement](#InterfacespecificationsDV-HM-AttributeS) ] [ [Rules for processing responses](#InterfacespecificationsDV-HM-Rulesforpr) ] [ [LogoutRequest](#InterfacespecificationsDV-HM-LogoutRequ) ] [ [ProvideKeyMaterial](#InterfacespecificationsDV-HM-ProvideKey) ]

### AuthnRequest (1)

This section describes regular Authentication Requests.

|  |  |  |
| --- | --- | --- |
| **Element/@Attribute** | **0..n** | **Description** |
| **@ID** | 1 | SAML: Unique message characteristic. MUST identify the message uniquely within the scope of the sender and receiver for a period of at least 12 months. |
| **@Version** | 1 | SAML: Version of the SAML protocol. The value MUST be '2.0'. |
| **@IssueInstant** | 1 | SAML: Time of issuing of the request. |
| **@Destination** | 1 | SAML: URL of the HM on which the message is offered. MUST match the HM's metadata. |
| **@Consent** | 0..1 | Elektronische Toegangsdiensten: MAY be included. When Consent is included, the default value MUST contain urn:oasis:names:tc:SAML:2.0:consent:unspecified. |
| **@ForceAuthn** | 0..1 | Elektronische Toegangsdiensten: The value 'true' indicates that an existing single sign-on session MUST NOT be used for the request in question. If the value is 'false' or empty or the specification is missing, the AD MAY use an existing SSO session if present. |
| **@IsPassive** | 0..1 | Elektronische Toegangsdiensten: MAY be included. If IsPassive is included, the value MUST be 'false'. |
| **@ProtocolBinding** | 0..1 | SAML: Specifies the used binding. MUST only be used when an @AssertionConsumerServiceURL is used, MUST NOT be used in combination with an @AssertionConsumerServiceIndex. |
| **@AssertionConsumerServiceIndex** | 0..1 | Elektronische Toegangsdiensten: This attribute element specifies the URL to which the HM sends the response for the DV. If present this index MUST refer to an endpoint of an AssertionConsumerService in the [DV metadata for HM](file:///H:\display\BEHEERAS\DV+metadata+for+HM).  MUST NOT be present if @AssertionConsumerServiceURL is present.  If neither @AssertionConsumerServiceIndex or @AssertionConsumerServiceURL is present, the HM MUST send the response to the endpoint in the metadata that is marked with 'isDefault=true' |
| **@AssertionConsumerServiceURL** | 0..1 | SAML: If present, URL MUST point to a SAML endpoint acknowlegded in the [DV metadata for HM](file:///H:\display\BEHEERAS\DV+metadata+for+HM). If present, the participant MUST check whether the @AssertionConsumerServiceUrl is included in the DV's [DV metadata for HM](file:///H:\display\BEHEERAS\DV+metadata+for+HM). If it is not included in the metadata, the participant MUST reject the message with the status code RequestDenied.  MUST NOT be present if @AssertionConsumerServiceIndex is present. |
| **@AttributeConsumingServiceIndex** | 0..1 | SAML: If present, MUST refer to an AttributeConsumingService in the DV's metadata. If absent, the AttributeConsumingService marked as default in the [DV metadata for HM](file:///H:\display\BEHEERAS\DV+metadata+for+HM) SHOULD be used.  The AttributeConsumingService MUST contain exactly one attribute with a name that is the same as a long formatted [ServiceID](file:///H:\display\BEHEERAS\ServiceID). The AttributeConsumingService MAY contain attributes to be requested.  Multiple AttributeConsumingService elements MAY be present in the [DV metadata for HM](file:///H:\display\BEHEERAS\DV+metadata+for+HM) and can be mapped to the same ServiceID. This allows DVs to request authentication for a single service with varying attributes depending on the context. The union of all attributes that may be queried for a ServiceID MUST be declared in the Service Catalog.  An application that cannot pass an AttributeConsumingServiceIndex can now retrieve different services and/or attribute contracts by exchanging metadata between different [EntityID](file:///H:\display\BEHEERAS\EntityID)s. Current applications for the 1.5 interface and earlier versions can include an AttributeConsumingService in the metadata for the different services for which the Index is the same as the short [ServiceID](file:///H:\display\BEHEERAS\ServiceID). This enables the current systems to continue working without hindrance. |
| **@ProviderName** | 0..1 | Elektronische Toegangsdiensten (DV): MAY contain a more detailed description of the service, complimentary to the entry in the service catalog  Elektronische Toegangsdiensten MAY NOT contain personally identifiable information |
| **Issuer** | 1 | Elektronische Toegangsdiensten: MUST contain the [EntityID](file:///H:\display\BEHEERAS\EntityID) of the DV. |
| **@NameQualifier** | 0 | Elektronische Toegangsdiensten: MUST NOT be included. |
| **@SPNameQualifier** | 0 | Elektronische Toegangsdiensten: MUST NOT be included. |
| **@Format** | 0 | Elektronische Toegangsdiensten: MUST NOT be included. |
| **@SPProvidedID** | 0 | Elektronische Toegangsdiensten: MUST NOT be included. |
| **Signature** | 1 | Elektronische Toegangsdiensten: MUST contain the [Digital signature](file:///H:\display\BEHEERAS\Digital+signature) of the DV for the envelopping message. |
| **Extensions** | 0 | Elektronische Toegangsdiensten: MUST NOT be included. |
| **Subject** | 0 | Elektronische Toegangsdiensten: MUST NOT be included. |
| **NameIDPolicy** | 0 | Elektronische Toegangsdiensten: MUST NOT be included. |
| **Conditions** | 0 | Elektronische Toegangsdiensten: MUST NOT be included. |
| **RequestedAuthnContext** | 0..1 | Elektronische Toegangsdiensten: MAY be used to explicitly request a specific LoA. If specified, the HM summary response will communicate the detailed LoA, rather than SAML 'unspecified'.  If present it MUST be used to request a equal to or lower than the level of assurance specified in the [Service catalog](file:///H:\display\BEHEERAS\Service+catalog). A lower LoA can for instance be used in requests to allow read-only access to services.  If RequestedAuthnContext is absent, then the request will be further processed, using the [Level of assurance](file:///H:\display\BEHEERAS\Level+of+assurance) (AuthnContextClassRef) as specified in the service catalog for the requested service. |
| **@Comparison** | 1 | MUST use the value 'minimum'. |
| **AuthnContextClassRef** | 1 | MUST be one of the following requested [Level of assurance](file:///H:\display\BEHEERAS\Level+of+assurance). |
| **Scoping** | 0**..**1 | Elektronische Toegangsdiensten: MUST be included in case an AD is pre-selected by the user at the DV, MUST NOT be included otherwise. |
| **IDPList** | 1 | MUST be present in case of pre-selection of an AD. |
| **IDPEntry** | 1 | MUST be present in case of pre-selection of an AD. |
| **@ProviderID** | 1 | EntityID of the AD selected by the user. |
| **@Name** | 0 | MUST NOT be present. |
| **@Loc** | 0..1 | In case an AD has multiple endpoints in the [Network metadata](file:///H:\display\BEHEERAS\Network+metadata), the endpoint selected by the user MUST be provided. |

#### Rules for processing requests

A requesting DV:

* MUST sign the <AuthnRequest>.
* MUST request a serviceID that is listed for that ServiceProvider itself in the Service Catalog. Requesting services of other Service Providers is not allowed. A [Dienstbemiddelaar (DB)](file:///H:\pages\viewpage.action%3fpageId=25280904) (Service Intermediary) can intermediate another service, if permitted by the Dienstaanbieder (Service Supplier), by indicating this in the Service Catalog (@IntermediatedService in ServiceInstance).
* MAY use the @AttributeConsumingServiceIndex to reference the service (as specified in the metadata).
* MAY use the <RequestedAuthnContext> to indicate a requested level of assurance, optionally lower than the LoA listed in the Service Catalogue for the requested Service.   
  NB. Using the <RequestedAuthnContext> indicates the DV can accept/process the LoA in the <AuthnContextClassRef> in the response as well. (NB. this may restrict out-of-box-processing by appliances!)
* MAY pass AD pre-selected for authentication. In this case:
  + the DV MUST use an authentic list (signed by BO/HM) of accredited ADs. The list SHOULD be updated at least once every 15 minutes, the list MUST NOT be older than 30 minutes.
  + the DV MUST show the OrganizationDisplayName of all valid, applicable ADs, in alphabetic order and equal appearance. Applicable means an AD supporting at least a LevelOfAssurance equal to or greater than the minimum requested level of assurance and the requested NameIDFormat(s) (=EntityConcernedType). The OrganizationDisplayName MUST be taken from the beforementioned list of accredited ADs, which MUST contain an exact copy from the [Network metadata](file:///H:\display\BEHEERAS\Network+metadata).
    - In case of a Portal request the eIDAS-berichtenservice MUST NOT be offered in the list of AD's to be selected.
    - In case of multiple OrganizationDisplayNames: if a user-specified preference or user interface language is available, the DV MUST present the OrganizationDisplayName with a matching LanguageQualifier; else if an OrganizationDisplayName with LanguageQualifier "nl" is present, this Dutch OrganizationDisplayName MUST be displayed; else if an OrganizationDisplayName with LanguageQualifier "en" is present, this English OrganizationDisplayName MUST be displayed; else, the first OrganizationDisplayName with a different LanguageQualifier MUST be displayed.

A responding HM:

* MUST only process requests from contracted DVs.
* MUST validate all signatures to be valid before further processing any request. Message (elements) MUST be signed using a certificate as listed in the [DV Metadata for HM](https://afsprakenstelsel.etoegang.nl/display/as/DV+metadata+for+HM) for the purpose of signing for a SPSSODescriptor of the requesting DV.
* MUST verify the structure and contents of the request.
* MUST request authentication, authorization, sectorIDs and attributes on behalf of the DV, as applicable to the requested Service and User's choices.
* In case of service intermediation the HM MUST verify the Service Intermediary is still authorized by the [Dienstaanbieder (DA)](file:///H:\pages\viewpage.action%3fpageId=25280901) (Service Supplier) by verifying the authorization status of the mediated service (@intermediationAllowed) in the Service Catalog.
* MUST support the IDPEntry element from the Scoping element in the AuthnRequest. In case the element Scoping is present, the HM MUST use the IDPEntry as reference for the AD selected by the user, bypassing the AD-selection page (applying use case GUC1-alt and GUC3-alt).
* MUST verify the chosen AD and optional endpoint provided in the IDPEntry element reference a valid AD/EB as listed in the [Network metadata](file:///H:\display\BEHEERAS\Network+metadata).
* MUST sanitize @ProviderName to remove any script or formatting before displaying
* If one of the criteria is not met, the HM must handle this as a non-recoverable error (see [Error handling](file:///H:\display\BEHEERAS\Error+handling)).
* Note: When a HM receives a DV request on a specific version of the DV-HM interface, it should only show AD’s that list eme:version in the Metadata with the same, or higher version.
* Note: When a HM receives a response from an AD, and the AD specifies an MR that is not of the same version, the HM must handle this as a non-recoverable error.

With regards to determining the user's choice of AD/MR, the following processing rules apply;

* A HM MAY maintain user preferences (selected AD and MR, and 'Representation' use), and use these values for determining applicable AD/MR queries, else;
* When the EntityConcernedTypesAllowed for the requested service signify a representation scenario (i.e. KVK, RSIN etc.), the HM MUST NOT query the user if it wants to authenticate on behalf of himself or another.

Note: The examples below show only the AuthnRequest. Additional wrapping elements can be present in case of HTTP Artifact binding.

**Example DV AuthnRequest**  Bron uitklappen

<samlp:AuthnRequest xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol"

ID="\_6984066c-de03-11e4-a571-080027a35b78"

ForceAuthn="true"

IsPassive="false"

Destination="https://..."

ProtocolBinding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Artifact"

AssertionConsumerServiceURL="https://"

AttributeConsumingServiceIndex="1"

IssueInstant="2015-04-08T16:30:03Z"

Version="2.0">

<saml:Issuer xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion">urn:etoegang:DV:...</saml: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:SignatureMethod Algorithm="http://www.w3.org/2001/04/xmldsig-more#rsa-sha256"/>

<ds:Reference URI=" ">

<ds:Transforms>

<ds:Transform Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature"/>

<ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>

</ds:Transforms>

<ds:DigestMethod Algorithm="http://www.w3.org/2001/04/xmlenc#sha256"/>

<ds:DigestValue>...</ds:DigestValue>

</ds:Reference>

</ds:SignedInfo>

<ds:SignatureValue>...</ds:SignatureValue>

<ds:KeyInfo>

<ds:KeyName>...</ds:KeyName>

</ds:KeyInfo>

</ds:Signature>

<samlp:RequestedAuthnContext Comparison="minimum">

<saml:AuthnContextClassRef xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion">urn:etoegang:core:assurance-class:loa3</saml:AuthnContextClassRef>

</samlp:RequestedAuthnContext>

</samlp:AuthnRequest>

**Example DV AuthnRequest - minimal**  Bron uitklappen

<samlp:AuthnRequest xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol"

ID="\_2962ac7c-de04-11e4-9801-080027a35b78"

Destination="https://..."

IssueInstant="2015-04-08T16:30:07Z"

Version="2.0">

<saml:Issuer xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion">urn:etoegang:DV:...</saml: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:SignatureMethod Algorithm="http://www.w3.org/2001/04/xmldsig-more#rsa-sha256"/>

<ds:Reference URI="#\_2962ac7c-de04-11e4-9801-080027a35b78">

<ds:Transforms>

<ds:Transform Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature"/>

<ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>

</ds:Transforms>

<ds:DigestMethod Algorithm="http://www.w3.org/2001/04/xmlenc#sha256"/>

<ds:DigestValue>...</ds:DigestValue>

</ds:Reference>

</ds:SignedInfo>

<ds:SignatureValue>...</ds:SignatureValue>

<ds:KeyInfo>

<ds:KeyName>...</ds:KeyName>

</ds:KeyInfo>

</ds:Signature>

</samlp:AuthnRequest>

### Response (2)

For chain authorizations ([Interface specifications HM-MR chain authorization](file:///H:\display\BEHEERAS\Interface+specifications+HM-MR+chain+authorization)), the identification number of the represented service consumer are included in the assertion for the HM in the same way as for single authorizations. The additional information about the chain is stored in a separate attribute.

Note: The HM will not identify the MRs from which the underlying assertions originate. Additional attributes relate to the represented service consumer or the user. There is no mechanism to include an additional attribute that relates specifically to an intermediary.

|  |  |  |
| --- | --- | --- |
| **Element/@Attribute** | **0..n** | **Description** |
| **@ID** | 1 | SAML: Unique message characteristic. MUST identify the message uniquely within the scope of the sender and receiver for a period of at least 12 months. |
| **@InResponseTo** | 1 | SAML: Unique attribute of the AuthnRequest for which this Response message is the answer. |
| **@Version** | 1 | SAML: Version of the SAML protocol. The value MUST be '2.0'. |
| **@IssueInstant** | 1 | SAML: Time of issuing of the Response. |
| **@Destination** | 1 | SAML: URL of the endpoint of the DV on which the message is offered. MUST match the DV's metadata. |
| **@Consent** | 0..1 | Elektronische Toegangsdiensten: MAY be included. When Consent is included, the default value MUST contain urn:oasis:names:tc:SAML:2.0:consent:unspecified. |
| **Issuer** | 1 | Elektronische Toegangsdiensten: MUST contain the [EntityID](file:///H:\display\BEHEERAS\EntityID) of the HM. |
| **@NameQualifier** | 0 | Elektronische Toegangsdiensten: MUST NOT be included. |
| **@SPNameQualifier** | 0 | Elektronische Toegangsdiensten: MUST NOT be included. |
| **@Format** | 0 | Elektronische Toegangsdiensten: MUST NOT be included. |
| **@SPProvidedID** | 0 | Elektronische Toegangsdiensten: MUST NOT be included. |
| **Signature** | 0..1 | Elektronische Toegangsdiensten: MUST contain the [Digital signature](file:///H:\display\BEHEERAS\Digital+signature) of the HM for the enveloping message.  When communicated within a ArtifactResolveResponse the signature on the SAML:Response MAY be omitted, since the parent message already guarantees the integrity. |
| **Extensions** | 0 | Elektronische Toegangsdiensten: MUST NOT be included. |
| **Status** | 1 | Elektronische Toegangsdiensten: MUST contain a StatusCode element with the status of the authentication. See [Error handling](file:///H:\display\BEHEERAS\Error+handling). |
| **StatusCode** | 1 | SAML: MUST be present in a Status element. |
| **@Value** | 1 | If not 'success' additional information should be provided. (conform Elektronische Toegangsdiensten specifications). |
| **StatusCode** | 0..1 | Only present if top-level StatusCode is not 'success'. |
| **@Value** | 1 | In the event of a cancellation or error, the element MUST be populated with the value AuthnFailed. See [Error handling](file:///H:\display\BEHEERAS\Error+handling). |
| **StatusMessage** | 0..1 | Only present if top-level StatusCode is not 'success'. |
| **StatusDetail** | 0 | Elektronische Toegangsdiensten: MUST NOT be included. |
| **Assertion** | 0..1 | Elektronische Toegangsdiensten: MUST contain the <Assertion> that is delivered in the response, if the request was processed successfully. See below. |
| **EncryptedAssertion** | 0 | Elektronische Toegangsdiensten: MUST NOT be included. |

**Example message**  Bron uitklappen

### <?xml version="1.0" encoding="UTF-8"?>

### <saml2p:Response Destination="https://....." ID="\_982734bdb26b1a9a8bdd9a95a36294456" InResponseTo="\_$eb5767755a74f58e2fe83b86abe51f2" IssueInstant="2019-02-26T10:35:43.000Z" Version="2.0" xmlns:saml2p="urn:oasis:names:tc:SAML:2.0:protocol" xmlns:xs="http://www.w3.org/2001/XMLSchema">

### <saml2:Issuer xmlns:saml2="urn:oasis:names:tc:SAML:2.0:assertion">urn:etoegang:HM:000000033333333310000:entities:7611</saml2: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:SignatureMethod Algorithm="http://www.w3.org/2001/04/xmldsig-more#rsa-sha256"/>

### <ds:Reference URI="#\_353aabdb26b1a9a8bdd9a95a36294456">

### <ds:Transforms>

### <ds:Transform Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature"/>

### <ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#">

### <ec:InclusiveNamespaces PrefixList="xs" xmlns:ec="http://www.w3.org/2001/10/xml-exc-c14n#"/>

### </ds:Transform>

### </ds:Transforms>

### <ds:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>

### <ds:DigestValue/>

### </ds:Reference>

### </ds:SignedInfo>

### <ds:SignatureValue/>

### <ds:KeyInfo xmlns:ds="http://www.w3.org/2000/09/xmldsig#">

### <ds:KeyName>f04a58c387f4f8b5f1fa3a614f79f073f3f08953</ds:KeyName>

### </ds:KeyInfo>

### </ds:Signature>

### <saml2p:Status xmlns:saml2p="urn:oasis:names:tc:SAML:2.0:protocol">

### <saml2p:StatusCode Value="urn:oasis:names:tc:SAML:2.0:status:Success"/>

### </saml2p:Status>

### <saml2:Assertion ID="\_89c245645645768401dc1b7274106731ca6" IssueInstant="2019-02-26T10:35:43.000Z" Version="2.0" xmlns:saml2="urn:oasis:names:tc:SAML:2.0:assertion" xmlns:xs="http://www.w3.org/2001/XMLSchema">

### . . . . . . . .

### </saml2:Assertion>

### </saml2p:Response>

### HM Summary assertion

This paragraph describes a HM summary <Assertion>

|  |  |  |
| --- | --- | --- |
| **Element/@Attribute** | **0..1** | **Description** |
| **@ID** | 1 | SAML: MUST identify the <Assertion> uniquely within the scope of the Issuer for a period of at least 12 months. |
| **@Version** | 1 | SAML: Version of the SAML protocol. The value MUST be '2.0'. |
| **@IssueInstant** | 1 | SAML: Time of issuing of the assertion. |
| **Issuer** | 1 | Elektronische Toegangsdiensten: MUST contain the [EntityID](file:///H:\display\BEHEERAS\EntityID) of the HM |
| **@NameQualifier** | 0 | Elektronische Toegangsdiensten: MUST NOT be included. |
| **@SPNameQualifier** | 0 | Elektronische Toegangsdiensten: MUST NOT be included. |
| **@Format** | 0 | Elektronische Toegangsdiensten: MUST NOT be included. |
| **@SPProvidedID** | 0 | Elektronische Toegangsdiensten: MUST NOT be included. |
| **Signature** | 1 | Elektronische Toegangsdiensten: MUST contain the [Digital signature](file:///H:\display\BEHEERAS\Digital+signature) of the Issuer (HM) for the enveloping Assertion. |
| **Subject** | 1 | Elektronische Toegangsdiensten: MUST be included. |
| **BaseID** | 0 | Elektronische Toegangsdiensten: MUST NOT be included. |
| **NameID** | 0..1 | [**Rules for processing request**](https://wiki.eherkenning.nl/display/cake/Interface+specifications+DV-HM+RFC2246#InterfacespecificationsDV-HMRFC2246-Rules4Responses)**require NameID to contain a TransientID** |
| **EncryptedID** | 0..1 | Elektronische Toegangsdiensten: MUST NOT be included. |
| **SubjectConfirmation** | 1...2 | SAML: Contains the [SubjectConfirmation](file:///H:\display\BEHEERAS\SubjectConfirmation) conform the WebSSO profile. In case of Dienstbemiddeling (Service intermediation), contains the SubjectConfirmation conform 'holder-of-key' for the Dienstbemiddelaar (service intermediary) as well.  Other SubjectConfirmation or SubjectConfirmationData elements MUST NOT be included. |
| **Conditions** | 1 | Elektronische Toegangsdiensten: MUST be included. |
| **@NotBefore** | 1 | Elektronische Toegangsdiensten: MUST be included. |
| **@NotOnOrAfter** | 0..1 | Elektronische Toegangsdiensten: MAY be included. |
| **Condition** | 0 | Elektronische Toegangsdiensten: MUST NOT be used. |
| **AudienceRestriction** | 1 | SAML: MUST be included. |
| **Audience** | 1 | Elektronische Toegangsdiensten: Contains the [EntityID](file:///H:\display\BEHEERAS\EntityID)(s) for all relevant parties that are intended to receive and process this assertion, as per SAML WebSSO profile. In case of Dienstbemiddeling (service intermediation), both the Dienstaanbieder (service supplier) and Dienstbemiddelaar (service intermediary) are a relevant party and must be listed as audience. For a Dienstaanbieder for whom only the OIN is known, the notation 'urn:etoegang:DV: <OIN>' is to be used. |
| **ProxyRestriction** | 0 | Elektronische Toegangsdiensten: MUST NOT be included. |
| **Advice** | 0..1 | Elektronische Toegangsdiensten: SHOULD be included. See below under processing rules. |
| **AssertionIDRef** | 0 | Elektronische Toegangsdiensten: MUST NOT be included. |
| **AssertionURIRef** | 0 | Elektronische Toegangsdiensten: MUST NOT be included. |
| **Assertion** | 1 | Elektronische Toegangsdiensten: Contains the original <Assertion> elements this assertion is composed of. |
| **EncryptedAssertion** | 0 | Elektronische Toegangsdiensten: MUST NOT be included. |
| **AuthnStatement** | 1 | Elektronische Toegangsdiensten: MUST be included.  The AuthenticatingAuthority element MUST be populated with the [EntityID](file:///H:\display\BEHEERAS\EntityID) of the AD that performed the authentication. |
| **@AuthnInstant** | 1 | Elektronische Toegangsdiensten: MUST contain the time of authentication. |
| **@SessionIndex** | 0..1 | Elektronische Toegangsdiensten: MAY be included. |
| **AuthnContext** | 1 | Elektronische Toegangsdiensten: MUST be included. |
| **AuthnContextClassRef** | 1 | Elektronische Toegangsdiensten: MUST be included. Contains either the value 'urn:oasis:names:tc:SAML:2.0:ac:classes:unspecified' (default) or the obtained effective [Level of assurance](file:///H:\display\BEHEERAS\Level+of+assurance), see below under "rules for processing responses". |
| **AttributeStatement** | 1 | Elektronische Toegangsdiensten: MUST contain an <AttributeStatement> in accordance with the following section and the rules for processing responses. |

### Example

<saml2:Assertion ID="\_67d2200a8bd8401dc1b7274106731ca6" IssueInstant="2019-02-26T10:35:43.000Z" Version="2.0" xmlns:saml2="urn:oasis:names:tc:SAML:2.0:assertion" xmlns:xs="http://www.w3.org/2001/XMLSchema">

<saml2:Issuer xmlns:saml2="urn:oasis:names:tc:SAML:2.0:assertion">urn:etoegang:HM:00000003271247010000:entities:7611</saml2: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:SignatureMethod Algorithm="http://www.w3.org/2001/04/xmldsig-more#rsa-sha256"/>

<ds:Reference URI="#\_67d2200a8bd8401dc1b7274106731ca6">

<ds:Transforms>

<ds:Transform Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature"/>

<ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#">

<ec:InclusiveNamespaces PrefixList="xs" xmlns:ec="http://www.w3.org/2001/10/xml-exc-c14n#"/>

</ds:Transform>

</ds:Transforms>

<ds:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>

<ds:DigestValue/>

</ds:Reference>

</ds:SignedInfo>

<ds:SignatureValue/>

<ds:KeyInfo xmlns:ds="http://www.w3.org/2000/09/xmldsig#">

<ds:KeyName>f04a58c387f4f8b5f1fa3a614f79f073f3f08953</ds:KeyName>

</ds:KeyInfo>

</ds:Signature>

<saml:Subject xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion">

<saml:NameID Format="urn:oasis:names:tc:SAML:2.0:nameid-format:transient" xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion">ed3d5655-b6ee-47bf-87d5-fb77302e14b4</saml:NameID>

<saml:SubjectConfirmation Method="urn:oasis:names:tc:SAML:2.0:cm:bearer" xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion">

<saml:SubjectConfirmationData InResponseTo="\_d3fda417414c17b2667995961cf79fc5" NotOnOrAfter="2019-02-26T10:37:39Z" Recipient="https://brk.eid-tst.ad.nl/brk/HM1CServiceProvider" xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion"/>

</saml:SubjectConfirmation>

</saml:Subject>

<saml2:Conditions NotBefore="2019-02-26T10:35:43Z" NotOnOrAfter="2019-02-26T10:37:43Z" xmlns:saml2="urn:oasis:names:tc:SAML:2.0:assertion">

<saml2:AudienceRestriction>

<saml2:Audience>urn:etoegang:DV:00000001111111110000:entities:9113</saml2:Audience>

<saml2:Audience>urn:etoegang:DV:00000002222222220000:entities:9113</saml2:Audience>

</saml2:AudienceRestriction>

</saml2:Conditions>

<saml:AuthnStatement AuthnInstant="2019-04-08T16:30:07Z">

<saml:AuthnContext>

<saml:AuthnContextClassRef>urn:etoegang:core:assurance-class:loa4</saml:AuthnContextClassRef>

</saml:AuthnContext>

</saml:AuthnStatement>

<saml2:Advice>

<saml:Assertion IssueInstant="2019-04-08T16:30:04Z" ID="\_8a792d9e-de07-11e4-9db2-080027a35b78" Version="2.0">

<saml:Issuer> urn:etoegang:AD:00000004444444445001:entities:9042</saml:Issuer>

*<!-- Verbatim copy of AD declaration of identity contents -->*

</saml:Assertion>

<saml:Assertion IssueInstant="2019-04-08T16:30:07Z" ID="dd4dae83-0f35-4695-b24a-29d470a63ea7" Version="2.0">

<saml:Issuer> urn:etoegang:MR:00000005555555555001:entities:9042</saml:Issuer>

*<!-- Verbatim copy of MR declaration of identity contents -->*

</saml:Assertion>

</saml2:Advice>

<saml2:AuthnStatement AuthnInstant="2019-02-26T10:35:43Z" xmlns:saml2="urn:oasis:names:tc:SAML:2.0:assertion">

<saml2:AuthnContext>

<saml2:AuthnContextClassRef>urn:etoegang:core:assurance-class:loa4</saml2:AuthnContextClassRef>

<saml2:AuthenticatingAuthority>urn:etoegang:AD:00000004444444445001:entities:9042</saml2:AuthenticatingAuthority>

</saml2:AuthnContext>

</saml2:AuthnStatement>

<saml2:AttributeStatement xmlns:saml2="urn:oasis:names:tc:SAML:2.0:assertion">

. . . . .

</saml2:AttributeStatement>

</saml2:Assertion>

### AttributeStatement

The <AttributeStatement> in the summary assertion MUST hold the relevant attribute values obtained in the assertions of the authentication process. The HM MUST NOT add any attributes that are not present in the gathered assertion.

|  |  |  |
| --- | --- | --- |
| **Element/@Attribute** | **0..1** | **Description** |
| **Attribute** | 0..n | Depending on [Rules for processing request](file:///H:\Application%20Data\Microsoft%20Office\Outlook\SecureTempFolder\Interface+specifications+DV-HM.mht):   * MUST include   + ActingSubjectID – multi-valued containing one ore more SAML <EncryptedID> (see SAML encryption) as value, each containing an applicable identifier of the acting (natural) person for a specific Relying Party (eg DienstVerlener, DienstAanbieder and/or DienstBemiddelaar)   + ActingSubjectID – multi-valued containing identity(s) of the acting (natural) person per a specific service provider   + LegalSubjectID – multi-valued containing with identity(s) of the ServiceConsumer   + ServiceID - multi-valued SAML attribute   + [ServiceUUI](https://afsprakenstelsel.etoegang.nl/display/as/ServiceUUID) - multi-valued SAML attribute * MAY include   + IntermediateEntityID - containing the identity of the **last** Intermediary **(in case of**[**Ketenmachtiging**](mhtml:file://H:\Application%20Data\Microsoft%20Office\Outlook\SecureTempFolder\Interface+specifications+DV-HM.mht!file:///C:\display\BEHEERAS\Ketenmachtiging)**)**   + one or more ServiceRestrictions, eg ServiceRestriction:Vestigingsnr   + AuthorizationRegistryID (see [EntityID](file:///H:\display\BEHEERAS\EntityID)).   Other Attribute elements MUST NOT be included. |
| **EncryptedAttribute** | 0..n | Additional attributes that are requested by the DV and provided by the AD and/or MR as EncryptedAttribute, MUST be included here. |

**Example 1 – Simple mandate**

* One ServiceProvider (no service intermediation)
* One Mandate (no authorisation chain/ketenmachtiging)
* No service restriction
* No (extra) attributes

<saml2:AttributeStatement xmlns:saml2="urn:oasis:names:tc:SAML:2.0:assertion">

<saml2:Attribute Name="urn:etoegang:core:ServiceUUID">

<saml2:AttributeValue xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xsi:type="xs:string">dafca82e-4806-408e-956e-3a7092643e54</saml2:AttributeValue>

</saml2:Attribute>

<saml2:Attribute Name="urn:etoegang:core:ServiceID">

<saml2:AttributeValue xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xsi:type="xs:string">urn:etoegang:DV:00000001111111110000:services:8002</saml2:AttributeValue>

</saml2:Attribute>

<saml:Attribute Name="urn:etoegang:core:Representation" xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion">

<saml:AttributeValue xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xsi:type="xs:boolean">true</saml:AttributeValue>

</saml:Attribute>

<! # ActingSubjectID voor de DV>

<saml:Attribute Name="urn:etoegang:core:ActingSubjectID" xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion">

<saml:AttributeValue>

<saml:EncrypedID>

<xenc:EncryptedData Id="\_cd52e15a16e2a0aa751725ce76a6b866" Type="http://www.w3.org/2001/04/xmlenc#Element">

<xenc:EncryptionMethod Algorithm="http://www.w3.org/2001/04/xmlenc#aes256-cbc" />

<ds:KeyInfo>

<ds:RetrievalMethod Type="http://www.w3.org/2001/04/xmlenc#EncryptedKey"URI="#\_15531f42aa31bbd4" />

</ds:KeyInfo>

<xenc:CipherData>

<xenc:CipherValue>...</xenc:CipherValue>

</xenc:CipherData>

</xenc:EncryptedData>

<xenc:EncryptedKey Id="\_15531f77a9f1e0b5e0cce442aa31bbd4" Recipient="urn:etoegang:DV:00000001111111110000:entities:9613">

<xenc:EncryptionMethod Algorithm="http://www.w3.org/2001/04/xmlenc#rsa-oaep-mgf1p">

<ds:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1" />

</xenc:EncryptionMethod>

<ds:KeyInfo>

<ds:KeyName>...</ds:KeyName>

</ds:KeyInfo>

<xenc:CipherData>

<xenc:CipherValue>yRy923JJlgAi2MTgx1qohLiDBgi...</xenc:CipherValue>

</xenc:CipherData>

<xenc:ReferenceList>

<xenc:DataReference URI="#\_cd52e15a16e2a0aa751725ce76a6b866" />

</xenc:ReferenceList>

</xenc:EncryptedKey>

</saml:EncrypedID>

</saml:AttributeValue>

</saml:Attribute>

<! # LegalSubjectID voor de DV>

<saml:Attribute Name="urn:etoegang:core:LegalSubjectID" xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion">

<saml:AttributeValue>

<saml:EncryptedID>

<xenc:EncryptedData xmlns:xenc="http://www.w3.org/2001/04/xmlenc#" Id="\_6bc1c98ef545444da370efd74371ff6f" Type="http://www.w3.org/2001/04/xmlenc#Element">

<xenc:EncryptionMethod Algorithm="http://www.w3.org/2001/04/xmlenc#aes256-cbc" />

<ds:KeyInfo xmlns:ds="http://www.w3.org/2000/09/xmldsig#">

<ds:RetrievalMethod URI="#\_105e787ebce14ea2b6655adb4d736b86" Type="http://www.w3.org/2001/04/xmlenc#EncryptedKey" />

</ds:KeyInfo>

<xenc:CipherData>

<xenc:CipherValue>lx922tGEfI9T7WgoduHAZ941XA....</xenc:CipherValue>

</xenc:CipherData>

</xenc:EncryptedData>

<xenc:EncryptedKey xmlns:xenc="http://www.w3.org/2001/04/xmlenc#" Id="\_105e787ebce14ea2b6655adb4d736b86" Recipient="urn:etoegang:DV:00000001111111110000:entities:9613">

<xenc:EncryptionMethod Algorithm="http://www.w3.org/2001/04/xmlenc#rsa-oaep-mgf1p">

<ds:DigestMethod xmlns:ds="http://www.w3.org/2000/09/xmldsig#" Algorithm="http://www.w3.org/2000/09/xmldsig#sha1" />

</xenc:EncryptionMethod>

<ds:KeyInfo xmlns:ds="http://www.w3.org/2000/09/xmldsig#">

<ds:KeyName>022A8DEA6C6F6CFA466BF18AF714F4CD0611DF3A4CAF23CF67B8BB8F7FC07CAF</ds:KeyName>

</ds:KeyInfo>

<xenc:CipherData>

<xenc:CipherValue>gNDIheioi3mgjeyCTviEXDui3.....</xenc:CipherValue>

</xenc:CipherData>

<xenc:ReferenceList>

<xenc:DataReference URI="#\_6bc1c98ef545444da370efd74371ff6f" />

</xenc:ReferenceList>

</xenc:EncryptedKey>

</saml:EncryptedID>

</saml:AttributeValue>

</saml:Attribute>

</saml2:AttributeStatement>

**Example 2 – complex mandates**

* two ServiceProviders (service intermediation)
* One Mandate (no authorisation chain/ketenmachtiging)
* Service restriction
* Extra attributes

<saml2:AttributeStatement xmlns:saml2="urn:oasis:names:tc:SAML:2.0:assertion">

<saml2:Attribute Name="urn:etoegang:core:ServiceUUID">

<saml2:AttributeValue xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xsi:type="xs:string">dafca82e-4806-408e-956e-3a7092643e54</saml2:AttributeValue>

</saml2:Attribute>

<saml2:Attribute Name="urn:etoegang:core:ServiceID">

<saml2:AttributeValue xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xsi:type="xs:string">urn:etoegang:DV:00000001111111110000:services:8002</saml2:AttributeValue>

</saml2:Attribute>

<saml:Attribute Name="urn:etoegang:core:Representation" xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion">

<saml:AttributeValue xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xsi:type="xs:boolean">true</saml:AttributeValue>

</saml:Attribute>

*<! igv de service via de Service Catalog vraagt om een ServiceRestriction en de MR>*

*<! heeft een service restriction bij de machtiging. Vb restrictie op KvK Vestigingsnr>*

<saml:Attribute Name="urn:etoegang:1.9:ServiceRestriction:Vestigingsnr">

<saml:AttributeValue xsi:type="xs:string">123456789012</saml:AttributeValue>

</saml:Attribute>

<saml:Attribute Name="urn:etoegang:core:**ActingSubjectID**" xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion">

<saml:AttributeValue>

<! # ActingSubjectID voor de DV1 (bijv DienstBemiddelaar)>

<saml:EncrypedID>

<xenc:EncryptedData Id="\_cd52e15a16e2a0aa751725ce76a6b866" Type="http://www.w3.org/2001/04/xmlenc#Element">

<xenc:EncryptionMethod Algorithm="http://www.w3.org/2001/04/xmlenc#aes256-cbc" />

<ds:KeyInfo>

<ds:RetrievalMethod Type="http://www.w3.org/2001/04/xmlenc#EncryptedKey"URI="#\_15531f42aa31bbd4" />

</ds:KeyInfo>

<xenc:CipherData>

<xenc:CipherValue>...</xenc:CipherValue>

</xenc:CipherData>

</xenc:EncryptedData>

<xenc:EncryptedKey Id="\_15531f77a9f1e0b5e0cce442aa31bbd4" Recipient="urn:etoegang:DV:00000001111111110000:entities:9613">

<xenc:EncryptionMethod Algorithm="http://www.w3.org/2001/04/xmlenc#rsa-oaep-mgf1p">

<ds:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1" />

</xenc:EncryptionMethod>

<ds:KeyInfo>

<ds:KeyName>...</ds:KeyName>

</ds:KeyInfo>

<xenc:CipherData>

<xenc:CipherValue>yRy923JJlgAi2MTgx1qohLiDBgi...</xenc:CipherValue>

</xenc:CipherData>

<xenc:ReferenceList>

<xenc:DataReference URI="#\_cd52e15a16e2a0aa751725ce76a6b866" />

</xenc:ReferenceList>

</xenc:EncryptedKey>

</saml:EncrypedID>

</saml:AttributeValue>

<saml:AttributeValue><! # ActingSubjectID voor de DV2 (Bijv DienstAanbieder)>

<saml:EncrypedID>

<xenc:EncryptedData Id="\_ed3457856888ad576a0aa751725ce76a6b866" Type="http://www.w3.org/2001/04/xmlenc#Element">

<xenc:EncryptionMethod Algorithm="http://www.w3.org/2001/04/xmlenc#aes256-cbc" />

<ds:KeyInfo>

<ds:RetrievalMethod Type="http://www.w3.org/2001/04/xmlenc#EncryptedKey"URI="#\_4567788aa31bbd4" />

</ds:KeyInfo>

<xenc:CipherData>

<xenc:CipherValue>...</xenc:CipherValue>

</xenc:CipherData>

</xenc:EncryptedData>

<xenc:EncryptedKey Id="\_15531f77a9f1e0b5e0cce442aa31bbd4" Recipient="urn:etoegang:DV: 00000002222222220000:entities:9613">

<xenc:EncryptionMethod Algorithm="http://www.w3.org/2001/04/xmlenc#rsa-oaep-mgf1p">

<ds:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1" />

</xenc:EncryptionMethod>

<ds:KeyInfo>

<ds:KeyName>...</ds:KeyName>

</ds:KeyInfo>

<xenc:CipherData>

<xenc:CipherValue>UtEw923JJlgAi2MTgx1qohLiDBgi...</xenc:CipherValue>

</xenc:CipherData>

<xenc:ReferenceList>

<xenc:DataReference URI="#\_cd52e15a16e2a0aa751725ce76a6b866" />

</xenc:ReferenceList>

</xenc:EncryptedKey>

</saml:EncrypedID>

</saml:AttributeValue>

</saml:Attribute>

<saml:Attribute Name="urn:etoegang:core:**LegalSubjectID**" xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion">

<saml:AttributeValue>

<! # LegalSubjectID voor de DV1 (Bijv DienstBemiddelaar)>

<saml:EncryptedID>

<xenc:EncryptedData xmlns:xenc="http://www.w3.org/2001/04/xmlenc#" Id="\_6bc1c98ef545444da370efd74371ff6f" Type="http://www.w3.org/2001/04/xmlenc#Element">

<xenc:EncryptionMethod Algorithm="http://www.w3.org/2001/04/xmlenc#aes256-cbc" />

<ds:KeyInfo xmlns:ds="http://www.w3.org/2000/09/xmldsig#">

<ds:RetrievalMethod URI="#\_105e787ebce14ea2b6655adb4d736b86" Type="http://www.w3.org/2001/04/xmlenc#EncryptedKey" />

</ds:KeyInfo>

<xenc:CipherData>

<xenc:CipherValue>lx922tGEfI9T7WgoduHAZ941XA....</xenc:CipherValue>

</xenc:CipherData>

</xenc:EncryptedData>

<xenc:EncryptedKey xmlns:xenc="http://www.w3.org/2001/04/xmlenc#" Id="\_105e787ebce14ea2b6655adb4d736b86" Recipient="urn:etoegang:DV:00000001111111110000:entities:9613">

<xenc:EncryptionMethod Algorithm="http://www.w3.org/2001/04/xmlenc#rsa-oaep-mgf1p">

<ds:DigestMethod xmlns:ds="http://www.w3.org/2000/09/xmldsig#" Algorithm="http://www.w3.org/2000/09/xmldsig#sha1" />

</xenc:EncryptionMethod>

<ds:KeyInfo xmlns:ds="http://www.w3.org/2000/09/xmldsig#">

<ds:KeyName>022A8DEA6C6F6CFA466BF18AF714F4CD0611DF3A4CAF23CF67B8BB8F7FC07CAF</ds:KeyName>

</ds:KeyInfo>

<xenc:CipherData>

<xenc:CipherValue>gNDIheioi3mgjeyCTviEXDui3.....</xenc:CipherValue>

</xenc:CipherData>

<xenc:ReferenceList>

<xenc:DataReference URI="#\_6bc1c98ef545444da370efd74371ff6f" />

</xenc:ReferenceList>

</xenc:EncryptedKey>

</saml:EncryptedID>

</saml:AttributeValue>

<saml:AttributeValue>

<! # LegalSubjectID voor de DV2 (Bijv DienstAanbieder)>

<saml:EncryptedID>

<xenc:EncryptedData xmlns:xenc="http://www.w3.org/2001/04/xmlenc#" Id="\_789bc1c98ef545444da370efd7436f" Type="http://www.w3.org/2001/04/xmlenc#Element">

<xenc:EncryptionMethod Algorithm="http://www.w3.org/2001/04/xmlenc#aes256-cbc" />

<ds:KeyInfo xmlns:ds="http://www.w3.org/2000/09/xmldsig#">

<ds:RetrievalMethod URI="#\_105e787ebce14ea2b6655adb4d736b86" Type="http://www.w3.org/2001/04/xmlenc#EncryptedKey" />

</ds:KeyInfo>

<xenc:CipherData>

<xenc:CipherValue>lx922tGEfI9T7WgoduHAZ941XA....</xenc:CipherValue>

</xenc:CipherData>

</xenc:EncryptedData>

<xenc:EncryptedKey xmlns:xenc="http://www.w3.org/2001/04/xmlenc#" Id="\_105e787ebce14ea2b6655adb4d736b86" Recipient="urn:etoegang:DV:00000002222222220000:entities:9613">

<xenc:EncryptionMethod Algorithm="http://www.w3.org/2001/04/xmlenc#rsa-oaep-mgf1p">

<ds:DigestMethod xmlns:ds="http://www.w3.org/2000/09/xmldsig#" Algorithm="http://www.w3.org/2000/09/xmldsig#sha1" />

</xenc:EncryptionMethod>

<ds:KeyInfo xmlns:ds="http://www.w3.org/2000/09/xmldsig#">

<ds:KeyName>022A8DEA6C6F6CFA466BF18AF714F4CD0611DF3A4CAF23CF67B8BB8F7FC07CAF</ds:KeyName>

</ds:KeyInfo>

<xenc:CipherData>

<xenc:CipherValue> WWbG5oodaNbZdRQPXepQjlw3bn....</xenc:CipherValue>

</xenc:CipherData>

<xenc:ReferenceList>

<xenc:DataReference URI="#\_8bc1c98ef545444da370efd74371f36e3" />

</xenc:ReferenceList>

</xenc:EncryptedKey>

</saml:EncryptedID>

</saml:AttributeValue>

</saml:Attribute>

*<! Optioneel ook nog versleutelde attributen met bijv naam, geboortedatum etc.>*

<saml:EncryptedAttribute>

<xenc:EncryptedData xmlns:xenc="http://www.w3.org/2001/04/xmlenc#" Id="\_67947663adfasdf9410780097b9bf2f04fa8" Type="http://www.w3.org/2001/04/xmlenc#Element">

<xenc:EncryptionMethod Algorithm="http://www.w3.org/2001/04/xmlenc#rsa-oaep-mgf1p">

<ds:DigestMethod xmlns:ds="http://www.w3.org/2000/09/xmldsig#" Algorithm="http://www.w3.org/2000/09/xmldsig#sha1" />

</xenc:EncryptionMethod>

<ds:KeyInfo>

<ds:KeyName>57890EA6C6F6CFA466BF18AF714F4CD0611DF3A4CAF23CF67B8BB8F7FC07CAF</ds:KeyName>

</ds:KeyInfo>

<xenc:CipherData>

<xenc:CipherValue>WYuIOsaf1aNbZdRQPXepQjlw4Tg...</xenc:CipherValue>

</xenc:CipherData>

</xenc:EncryptedData>

</saml:EncryptedAttribute>

</saml2:AttributeStatement>

#### Rules for processing responses

On a successful authentication the HM MUST generate a 'Summary Assertion' based on the Assertions gathered during the authentication process, using the following processing rules.

~~A responding HM MUST:~~

* MUST sign the enclosed <Assertion> as well as the <Response> (and/or the enclosing <ArtifactResponse>).
* MUST verify each collected assertion has at minimum the Level of Assurance as requested by the DV. If verification fails, MUST handle the received responses as an unrecoverable error.
* MUST provide an <AuthnContextClassRef>:
  + By default fill the AuthnContextClassRef with the value 'urn:oasis:names:tc:SAML:2.0:ac:classes:unspecified'.
  + When a DV explicitly requests a detailed LoA by including an AuthnContextClassRef in its AuthnRequest (see above)
  + When a DV explicitly requests a detailed LoA by including an AuthnContextClassRef in its AuthnRequest (see above): The HM MUST communicate the effective Level of Assurance of the combined assertions. The effective Level of assurance is the minimum of the LoA of the Authentication assertion and (if applicable) the LoA of the Representation authorization assertion(s).  
    *The MR communicates two Levels of Assurance in its Assertion. A LevelOfAssurance (requested) and a LevelOfAssuranceUsed (actually obtained). The HM MUST use the LevelOfAssuranceUsed from the MR Assertion as the LoA of the Representation authorization*
* **HM MUST provide an <Subject> with the following <NameID>**
  + ***IF* non-represenation *THEN* copy AD-assertion: Subject.NameID.TransientID**
  + ***IF* representation *THEN*copy MR-assertion: Subject.NameID.TransientID**
* **HM MUST provide an <AttributeStatement> with the following <Attributes>**
  + [**copy all relevant**](file:///C:\Users\FRkok\AppData\Local\Microsoft\Windows\INetCache\IE\GC0OTILY\Interface+specifications+DV-HM+RFC2246.doc#InterfacespecificationsDV-HMRFC2246-Cop) **MR-Assertion: XACMLAuthz-Decision.Subject.ActingSubjectID (EncryptedID)**
  + [**copy all relevant**](file:///C:\Users\FRkok\AppData\Local\Microsoft\Windows\INetCache\IE\GC0OTILY\Interface+specifications+DV-HM+RFC2246.doc#InterfacespecificationsDV-HMRFC2246-Cop) **MR-Assertion: XACMLAuthz-Decision.Subject.LegalSubjectID (EncryptedID)**
  + **IF ServiceRestrictions are (requested by the DV and) provided by MR THEN**[**copy all relevant**](file:///C:\Users\FRkok\AppData\Local\Microsoft\Windows\INetCache\IE\GC0OTILY\Interface+specifications+DV-HM+RFC2246.doc#InterfacespecificationsDV-HMRFC2246-Cop) **MR-assertion: XACMLAuthz-Decision.Resource.ServiceRestrictions**
  + **IF Representation THEN copy MR-Assertion: XACMLAuthz-Decision.Statement.Request.Resource.ServiceID**
  + **IF**[**Ketenmachtiging**](file:///C:\display\BEHEERAS\Ketenmachtiging)**THEN copy MR-Assertion: XACMLAuthz-Decision.Statement.Request.Resource.IntermediateEntityID**
* **HM MUST provide an <AttributeStatement> with the following <EncryptedAttributes>**
  + [**copy all relevant**](file:///C:\Users\FRkok\AppData\Local\Microsoft\Windows\INetCache\IE\GC0OTILY\Interface+specifications+DV-HM+RFC2246.doc#InterfacespecificationsDV-HMRFC2246-Cop) **AD-assertion: AttributeStatement.EncryptedAttribute**
  + **IF representation THEN**[**copy all relevant**](file:///C:\Users\FRkok\AppData\Local\Microsoft\Windows\INetCache\IE\GC0OTILY\Interface+specifications+DV-HM+RFC2246.doc#InterfacespecificationsDV-HMRFC2246-Cop) **MR-assertion: XACMLAuthz-Decision.Resource.EncryptedAttributes**
* MUST provide an <Advice>, by default filled with verbatim copy of all Assertions – so that original signatures over the assertions remains verifiable – gathered during the authentication process. HM MAY offer their DV to omit this information, if they archive this information and allow for later retrieval.

**"Copy all relevant"**

**For <EncryptedID> and <EncryptedAttribute> elements HM MUST  only copy the <EncryptedKey> with the recipient matching the DV with the <EncryptedData> into the HM Summary Assertion. However IF Dienstbemiddeling (service intermediation) THEN HM MUST also copy the <EncryptedKey> with the recipient matching the Dienstbemiddelaar with the <EncryptedData> into the HM Summary Assertion**

NOTE: When copying encrypted XML elements (<EncryptedID>, <EncryptedAttribute>) to create the summary declaration the HM MUST substitute used XML identifiers to point at the EncryptedTypes for a guaranteed unique identifier. This MAY be accomplished by pre- or suffixing the used identifier in the copy.

(Rationale: @ID values must uniquely identify the elements which bear them. Identifiers that appear once in the summary assertion and once in the advice assertion(s) will break schema validation of assertions).

A receiving DV:

* MUST verify the response matches with the Request responded to.
* MUST validate the signature on the Assertion as well as the Response (and/or the enclosing ArtifactResponse). Message (elements) MUST be signed using a certificate as listed in the SAML metadata of the HM for the purpose of signing for an IDPSSODescriptor of the responding HM. (NB this should correspond to the certificate as published in the network metadata).
* SHOULD verify the structure and contents of the Response.
* SHOULD validate the signature and linking of the Evidence assertions.
* In case the receiving DV is a Dienstbemiddelaar, the Dienstbemiddelaar MUST provide a verbatim copy of the assertion – so that original signatures over the assertions remains verifiable – to the Dienstaanbieder (service supplier).
* IF the DV receives a pseudonym THEN the DV SHOULD create a mapping from the obtained Pseudonym to a user account, rather than using the obtained pseudoniem directly as unique key for an account.
* MUST decrypt an Encrypted Pseudonym or Encrypted Identity in the EncryptedID in the Attribute Statement of the Assertion using preinstalled keymaterial and software to obtain the actual identifier.
  + - SHOULD create a mapping from the obtained identifier to a user account, rather than using the obtained identifier directly as unique key for an account.

**RequestKeyMaterial**

The DV may request the HM for DV-specific key material which the DV can use to decrypt the EncryptedPseudonym into a DV-specific pseudonym or BSN, as per [AUC9 Verstrekken sleutelmateriaal Dienstverleners](file:///H:\display\BEHEERAS\AUC9+Verstrekken+sleutelmateriaal+Dienstverleners). The HM can request the keys at the BSNk (see [Interface specifications aux HM-BSNk - ProvideDVkeys](file:///H:\display\BEHEERAS\Interface+specifications+aux+HM-BSNk+-+ProvideDVkeys)).

A PKIo-certificate of the DV is required, the PKIo-certificate MUST have a (extended) key usage that allows for keyEncipherment. If the DV may request a BSN, the PKIo-certificate MUST have a Subject.serialNumber containing the organizations OIN.

### ****ProvideKeyMaterial****

The Herkenningsmakelaar MUST transfer the PKIo-encrypted key material to the DV unaltered. The HM will receive the DV-keys from the BSNk (see [Interface specifications aux HM-BSNk - ProvideDVkeys](file:///H:\display\BEHEERAS\Interface+specifications+aux+HM-BSNk+-+ProvideDVkeys)).

The DV can decrypt the DV-keys using its private key corresponding with the PKIo-certificate used in the request.

# 2. SubjectConfirmation

The SubjectConfirmation exists in a Subject, and is used in two manners on Subjects:

* To hold a 'bearer' confirmation in a response to an AuthnRequest, to conform to the WebSSO profile.
* To hold a 'holder-of-key' in a response to an AuthnRequest when a Service Intermediary is involved.

A <Subject> in an <Assertion> can contain two different types of  <SubjectConfirmation> elements. Below is a description for each of these usages. Note that both bearer and holder-of-key confirmations MAY be applicable to a single Assertion.

### SubjectConfirmation for bearer confirmation (WebSSO)

In case a relying party is requesting authentication of a user according to the SAML Web SSO profile, a 'bearer' SubjectConfirmation (see SAML 2.0 Profiles, §3.3 and §4.1.4).

| **Element/@Attribute** | **0..n** | **Description** |
| --- | --- | --- |
| <SubjectConfirmation> | 0..1 | (Only for the Declaration of Identity or a HM Summary Declaration to the DV)  Allows for association of client with assertion to conform to the SAML Web SSO profile. |
| @Method | 1 | MUST contain the value 'urn:oasis:names:tc:SAML:2.0:cm:bearer'. |
| <SubjectConfirmationData> | 1 |  |
| @NotBefore | 0 | MUST NOT be used. |
| @NotOnOrAfter | 1 | Indicates maximum validity of the assertion |
| @Recipient | 1 | The assertion consumer Service index of the immediate requester to which an attesting entity can present the assertion |
| @InResponseTo | 1 | The ID of the request this assertion is in response to |
| @Address | 0 | MUST NOT be used. |

### SubjectConfirmation for holder-of-key confirmation (HoK)

In case of Dienstbemiddeling (service intermediary), the user is not directly interacting with the Dienstaanbieder using his user agent. In this case a 'holder-of-key' confirmation is used, to strongly bind the Assertions to the usage via the Dienstbemiddelaar (service intermediary). The Dienstbemiddelaar (DB) has to prove possession of the referenced key (i.e. via TLS authentication, message signature or other means), as confirmation to the Dienstaanbieder that the DB is an authentic and acceptable attesting entity for the assertion. See SAML 2.0 Profiles, §3.1.

| **Element/@Attribute** | **0..n** | **Description** |
| --- | --- | --- |
| <SubjectConfirmation> | 0..1 | (Only for the Declaration of Identity or a HM Summary Declaration to the DV)  Allows for association of client with assertion in scenario's with Service Intermediaries.  When there is more than 1 relying party, contains a HoK subjectconfirmation associated with the certificate of the original requesting party (the DB).  This allows the relying party (the Dienstaanbieder) to treat the entity presenting the assertion (the DB) as one that the asserting entity (eHerkenning-network) has associated with the principal identified in the assertion; thus allowing the DB to present the assertion on behalf of the user. |
| @Method | 1 | MUST contain the value 'urn:oasis:names:tc:SAML:2.0:cm:holder-of-key' |
| <SubjectConfirmationData> | 1 | MUST NOT contain any attributes in case of a holder-of-key confirmation method. |
| <KeyInfo> | 1 | MUST be present. |
| <X509Data> | 1 | MUST contain a reference to the certificate of the Dienstbemiddelaar (service intermediary) originally requesting authentication. |
| <X509IssuerSerial> | 1 | MUST be present. |
| <X509IssuerName> | 1 | MUST contain the name of the issuer of the certificate of the Dienstbemiddelaar. Note that the issuer's name should be formatted as defined in [RFC4514](https://tools.ietf.org/html/rfc4514) (as per XML-signature specification). |
| <X509SerialNumber> | 1 | MUST contain the serial number of the certificate of the Dienstbemiddelaar. Note that the serial number should be decimal (as per the XML-signature specification). |

**Example SubjectConfirmation WebSSO**  Bron uitklappen

...

<saml:Subject>

...

<saml:SubjectConfirmation Method="urn:oasis:names:tc:SAML:2.0:cm:bearer">

<saml:SubjectConfirmationData InResponseTo="\_52B816C631C564BACF59E758CBA91717" NotOnOrAfter="2016-02-05T09:11:48Z" Recipient="https://..."/>

</saml:SubjectConfirmation>

</saml:Subject>

...

**Example SubjectConfirmation HoK**  Bron uitklappen

...

<saml:Subject>

...

<SubjectConfirmation Method="urn:oasis:names:tc:SAML:2.0:cm:holder-of-key">

<SubjectConfirmationData xsi:type="saml:KeyInfoConfirmationDataType">

<ds:KeyInfo>

<ds:X509Data>

 <ds:X509IssuerSerial>

 <ds:X509IssuerName>CN=...,...,O=...,C=NL</ds:X509IssuerName>

<ds:X509SerialNumber>...834756977854956...</ds:X509SerialNumber>

</ds:X509IssuerSerial>

</ds:X509Data>

 </ds:KeyInfo>

</SubjectConfirmationData>

</SubjectConfirmation>

</saml:Subject>

...

**Example SubjectConfirmation WebSSO & HoK (Dienstbemiddeling)**  Bron uitklappen

...

<saml:Subject>

...

<saml:SubjectConfirmation Method="urn:oasis:names:tc:SAML:2.0:cm:bearer">

<saml:SubjectConfirmationData InResponseTo="\_52B816C631C564BACF59E758CBA91717" NotOnOrAfter="2016-02-05T09:11:48Z" Recipient="https://..."/>

</saml:SubjectConfirmation>

<SubjectConfirmation Method="urn:oasis:names:tc:SAML:2.0:cm:holder-of-key">

<SubjectConfirmationData xsi:type="saml:KeyInfoConfirmationDataType">

<ds:KeyInfo>

<ds:X509Data>

<ds:X509IssuerSerial>

 <ds:X509IssuerName>CN=...,...,O=...,C=NL</ds:X509IssuerName>

<ds:X509SerialNumber>...834756977854956...</ds:X509SerialNumber>

</ds:X509IssuerSerial>

</ds:X509Data>

</ds:KeyInfo>

</SubjectConfirmationData>

</SubjectConfirmation>

</saml:Subject>

...

# Interface specifications HM-AD

|  |
| --- |
| **Sequence diagram HM-AD** |
| C:\cf15c6d1af606c092490002a734f3c01 |

This page describes the messages that are exchanged between an [Herkenningsmakelaar (HM)](file:///H:\pages\viewpage.action%3fpageId=13926461) and an [Authenticatiedienst (AD)](file:///H:\pages\viewpage.action%3fpageId=13926418) (identity provider).In the interface described here, the use case [GUC3 Aantonen identiteit](file:///H:\display\BEHEERAS\GUC3+Aantonen+identiteit) consists of an SAML 2.0 AuthnRequest and Response. The specific content of these messages is described below. Detailed information about the value of fields can be found in [Attribute elements](file:///H:\display\BEHEERAS\Attribute+elements).

A column in a message description that starts with 'SAML' indicates that this is the standard value. A value that starts with 'Elektronische Toegangsdiensten' indicates that the value is specific to Elektronische Toegangsdiensten.

[ [Rules for processing requests](#InterfacespecificationsHM-AD-Rulesforpr) ] [ [Response (2)](#InterfacespecificationsHM-AD-Response(2) ] [ [Authentication assertion](#InterfacespecificationsHM-AD-Authentica) ] [ [Rules for processing response](#InterfacespecificationsHM-AD-Rulesforpr) ] [ [LogoutRequest](#InterfacespecificationsHM-AD-LogoutRequ) ]

AuthnRequest (1)

|  |  |
| --- | --- |
| **@ID** | SAML: Unique message attribute |
| **@Version** | SAML: Version of the SAML protocol. The value MUST be '2.0'. |
| **@IssueInstant** | SAML: Time at which the message was created. |
| **@Destination** | SAML: URL of the AD on which the message is offered. MUST match the AD's metadata. |
| **@Consent** | Elektronische Toegangsdiensten: MUST NOT be included. |
| **@ForceAuthn** | The value 'true' indicates that an existing single sign-on session MUST NOT be used for the request in question. If the value is 'false' or empty or the specification is missing, the AD MAY use an existing SSO session if one is open. |
| **@IsPassive** | Elektronische Toegangsdiensten: MAY be included. If IsPassive is included, the value MUST be 'false'. |
| **@ProtocolBinding** | SAML: MUST NOT be included because [AssertionConsumerServiceIndex](file:///H:\display\BEHEERAS\AssertionConsumerServiceIndex) is required in Elektronische Toegangsdiensten. |
| **@AssertionConsumerServiceIndex** | Elektronische Toegangsdiensten: This attribute element indicates the URL to which the response must be sent. The value of [AssertionConsumerServiceIndex](file:///H:\display\BEHEERAS\AssertionConsumerServiceIndex) MUST match an index at the assertion consumer service in the HM's metadata. |
| **@AssertionConsumerServiceURL** | SAML: MUST NOT be included because [AssertionConsumerServiceIndex](file:///H:\display\BEHEERAS\AssertionConsumerServiceIndex) is required in Elektronische Toegangsdiensten. |
| **@AttributeConsumingServiceIndex** | Elektronische Toegangsdiensten: The value MUST be '4'. Indicates that it is about the interface described in this document. |
| **@ProviderName** | Elektronische Toegangsdiensten: MAY contain a more detailed description of the service. |
| **Issuer** | Elektronische Toegangsdiensten: MUST contain the [EntityID](file:///H:\display\BEHEERAS\EntityID) of the HM.  The attributes NameQualifier, SPNameQualifier, Format and SPProvidedID MUST NOT be included. |
| **Signature** | Elektronische Toegangsdiensten: MUST contain the [Digital signature](file:///H:\display\BEHEERAS\Digital+signature) of the HM for the enveloping message. |
| **Extensions** | Elektronische Toegangsdiensten: MUST contain the attributes [IntendedAudience](file:///H:\display\BEHEERAS\IntendedAudience), [ServiceID](file:///H:\display\BEHEERAS\ServiceID) and the corresponding [ServiceUUID](file:///H:\display\BEHEERAS\ServiceUUID).  If the DV queries additional attributes (via an AttributeConsumingService as described in [Interface specifications DV-HM](file:///H:\display\BEHEERAS\Interface+specifications+DV-HM) and the [DV metadata for HM](file:///H:\display\BEHEERAS\DV+metadata+for+HM)), they MUST be included here by the HM. To this extent, one Elektronische Toegangsdiensten specific RequestedAttributes (see schema below) element MUST be included containing the RequestedAttribute elements reflecting the DV's request. The requested attribute(s) MUST be defined in the [Attribuutcatalogus](file:///H:\display\BEHEERAS\Attribuutcatalogus) and MUST be declared as RequestedAttribute in the [Service catalog](file:///H:\display\BEHEERAS\Service+catalog) entry for the requested service. An AD not able to provide these attributes MUST act as specified in the alternative use case described in [Attributen niet leverbaar of niet toegestaan](file:///H:\display\BEHEERAS\Attributen+niet+leverbaar+of+niet+toegestaan).  Other XML attributes MUST NOT be included.  Other elements MUST NOT be included. |
| **Subject** | Elektronische Toegangsdiensten: MUST NOT be included |
| **NameIDPolicy** | Elektronische Toegangsdiensten: MUST NOT be included. |
| **Conditions** | Elektronische Toegangsdiensten: MUST NOT be included. |
| **RequestedAuthnContext** | Elektronische Toegangsdiensten: MAY contain an attribute Comparison='minimum' and an element AuthnContextClassRef that contains the minimum [Level of assurance](file:///H:\display\BEHEERAS\Level+of+assurance) required by the DV.  When RequestedAuthnContext is included in the request, then it must contain a [Level of assurance](file:///H:\display\BEHEERAS\Level+of+assurance) (AuthnContextClassRef) equal to or lower than the level of assurance included in the [Service catalog](file:///H:\display\BEHEERAS\Service+catalog) for the requested service. |
| **Scoping** | Elektronische Toegangsdiensten: MUST NOT be included |

**XML schema saml protocol extensions**  Bron uitklappen

<?xml version="1.0" encoding="UTF-8"?>

<xs:schema targetNamespace="urn:etoegang:1.9:samlp-extension"

xmlns:xs="http://www.w3.org/2001/XMLSchema"

xmlns:md="urn:oasis:names:tc:SAML:2.0:metadata"

elementFormDefault="qualified"

attributeFormDefault="unqualified">

 <xs:element name="RequestedAttributes">

<xs:complexType>

<xs:sequence>

<xs:element ref="md:RequestedAttribute" maxOccurs="unbounded"/>

</xs:sequence>

</xs:complexType>

</xs:element>

</xs:schema>

**Example message**  Bron uitklappen

<?xml version="1.0" encoding="UTF-8"?>

<samlp:AuthnRequest xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol"

xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion"

xmlns:ds="http://www.w3.org/2000/09/xmldsig#"

xmlns:md="urn:oasis:names:tc:SAML:2.0:metadata"

xmlns:esp="urn:etoegang:1.9:samlp-extension"

 ID="\_4b5af9ca-33ef-400f-9c97-398ab0c8e9c7"

Destination="https://..."

ForceAuthn="true"

AssertionConsumerServiceIndex="1"

AttributeConsumingServiceIndex="4"

ProviderName="DV Name"

IssueInstant="2015-04-10T12:30:03Z"Version="2.0">

<saml:Issuer/>urn:etoegang:HM:...</saml:Issuer>

<ds:Signature>

<ds:SignedInfo>

<ds:CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#" />

<ds:SignatureMethod Algorithm="http://www.w3.org/2001/04/xmldsig-more#rsa-sha256" />

<ds:Reference URI="#\_4b5af9ca-33ef-400f-9c97-398ab0c8e9c7">

<ds:Transforms>

<ds:Transform Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature" />

<ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#" />

</ds:Transforms>

<ds:DigestMethod Algorithm="http://www.w3.org/2001/04/xmlenc#sha256" />

<ds:DigestValue>...</ds:DigestValue>

</ds:Reference>

</ds:SignedInfo>

<ds:SignatureValue>...</ds:SignatureValue>

<ds:KeyInfo>

<ds:KeyName>...</ds:KeyName>

</ds:KeyInfo>

</ds:Signature>

<samlp:Extensions>

<saml:Attribute Name="urn:etoegang:core:IntendedAudience">

<saml:AttributeValue>urn:etoegang:DV:...:entities:...</saml:AttributeValue>

</saml:Attribute>

<saml:Attribute Name="urn:etoegang:core:ServiceID">

<saml:AttributeValue>urn:etoegang:DV:...:services:...</saml:AttributeValue>

</saml:Attribute>

<saml:Attribute Name="urn:etoegang:core:ServiceUUID">

<saml:AttributeValue>bf83ccef-6c9d-443f-ac11-9df0a0a9d299</saml:AttributeValue>

</saml:Attribute>

<esp:RequestedAttributes>

<md:RequestedAttribute Name="urn:etoegang:1.9:attribute:FirstName" IsRequired="false" />

</esp:RequestedAttributes>

</samlp:Extensions>

<samlp:RequestedAuthnContext Comparison="minimum">

<saml:AuthnContextClassRef>urn:etoegang:core:assurance-class:loa3</saml:AuthnContextClassRef>

</samlp:RequestedAuthnContext>

</samlp:AuthnRequest>

#### Rules for processing requests

A requesting HM:

* MUST propagate @ProviderName of the party initiating the Request.

A receiving AD:

* MUST verify a requested service is defined in the Service Catalog and requested accordingly.
* MUST sanitize @ProviderName to remove any script or formatting before displaying.
* In case of Dienstbemiddeling (service intermediation), MUST verify the Dienstbemiddelaar (Service Intermediary) is still authorized by the Dienstaanbieder (Service Supplier) by verifying the authorization status of the mediated service in the Service Catalog.

If one of the criteria is not met, the AD MUST handle this as a non-recoverable error (see [Error handling](file:///H:\display\BEHEERAS\Error+handling)).

Note: When an AD specifies a MR for the HM to use as the next hop, the AD may only specify a MR of the same version.

### Response (2)

|  |  |
| --- | --- |
| **@ID** | SAML: Unique message characteristic. |
| **@InResponseTo** | SAML: Unique attribute of the AuthnRequest for which this response message is the answer. |
| **@Version** | SAML: Version of the SAML protocol. The value MUST be '2.0' |
| **@IssueInstant** | SAML: Time at which the message was created. |
| **@Destination** | SAML: URL of the HM on which the message is offered. MUST match the HM's metadata. |
| **@Consent** | Elektronische Toegangsdiensten: MUST NOT be included. |
| **Issuer** | Elektronische Toegangsdiensten: MUST contain the [EntityID](file:///H:\display\BEHEERAS\EntityID) of the AD.  The attributes NameQualifier, SPNameQualifier, Format and SPProvidedID MUST NOT be included. |
| **Signature** | Elektronische Toegangsdiensten: MUST contain the [Digital signature](file:///H:\display\BEHEERAS\Digital+signature) of the AD for the enveloped message. |
| **Extensions** | Elektronische Toegangsdiensten: MUST NOT be included |
| **Status** | Elektronische Toegangsdiensten: MUST be filled conform SAML 2.0 specs when the request is successfully processed.  MUST be filled according to [Error handling](file:///H:\display\BEHEERAS\Error+handling) in case of an error or when the request was cancelled. |
| **Assertion** | Elektronische Toegangsdiensten: MUST contain an assertion about the authentication (see the next section). |

**Example AD Response**  Bron uitklappen

<?xml version="1.0" encoding="UTF-8"?>

<samlp:Response xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol"

xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion"

xmlns:ds="http://www.w3.org/2000/09/xmldsig#"

 Destination="https://..."

ID="\_62619615-e452-47d3-a44b-93da2d5a76f9"

InResponseTo="\_4b5af9ca-33ef-400f-9c97-398ab0c8e9c7"

IssueInstant="2015-04-10T11:16:28Z"

Version="2.0">

<saml:Issuer>urn:etoegang:AD:...</saml:Issuer>

<ds:Signature>

<ds:SignedInfo>

<ds:CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>

<ds:SignatureMethod Algorithm="http://www.w3.org/2001/04/xmldsig-more#rsa-sha256"/>

<ds:Reference URI="#\_62619615-e452-47d3-a44b-93da2d5a76f9">

<ds:Transforms>

<ds:Transform Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature"/>

<ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>

</ds:Transforms>

<ds:DigestMethod Algorithm="http://www.w3.org/2001/04/xmlenc#sha256"/>

<ds:DigestValue>...</ds:DigestValue>

</ds:Reference>

</ds:SignedInfo>

<ds:SignatureValue>...</ds:SignatureValue>

<ds:KeyInfo>

<ds:KeyName>...</ds:KeyName>

</ds:KeyInfo>

</ds:Signature>

<samlp:Status>

<samlp:StatusCode Value="urn:oasis:names:tc:SAML:2.0:status:Success"/>

</samlp:Status>

<saml:Assertion ID="\_f0ba7712-50e4-4d30-8bb5-e63a771507de" IssueInstant="2015-04-10T11:16:28Z" Version="2.0">

<saml:Issuer xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion">urn:etoegang:AD:...</saml:Issuer>

....

</saml:Assertion>

</samlp:Response>

Note: the above example only provides the response. The response will be send via an Artifact binding.

### Authentication assertion

|  |  |  |
| --- | --- | --- |
| Assertion | **@Version** | SAML: Version of the SAML protocol. The value MUST be '2.0' |
|  | **@ID** | SAML: Unique reference to the assertion |
|  | **@IssueInstant** | SAML: Time at which the assertion was created |
|  | **Issuer** | Elektronische Toegangsdiensten: MUST contain the [EntityID](file:///H:\display\BEHEERAS\EntityID) of the AD.  The attributes NameQualifier, SPNameQualifier, Format and SPProvidedID MUST NOT be included. |
|  | **Signature** | Elektronische Toegangsdiensten: MUST be included |
|  | **Subject** | Elektronische Toegangsdiensten: MUST contain a <NameID> with a Transient ID.  A [SubjectConfirmation](file:///H:\display\BEHEERAS\SubjectConfirmation) element that meets the Web Browser SSO profile MUST be included.  In case of Dienstbemiddeling (Service intermediation), contains the SubjectConfirmation conform 'holder-of-key' for the Dienstbemiddelaar (service intermediary) as well. Other SubjectConfirmation or SubjectConfirmationData elements MUST NOT be included. |
|  | **Conditions** | Elektronische Toegangsdiensten: MUST be included. The attributes NotBefore and NotOnOrAfter MAY be included but should be ignored by the receiver.  An Audience element in the AudienceRestriction element that meets the Web Browser SSO profile MUST be included.  Other audience elements MUST include relevant parties: EntityIDs of the requesting DV and the MR/KR/HM (if applicable) to whom the assertion will be targeted. In case of Dienstbemiddeling (service intermediation), both the Dienstaanbieder (service supplier) and Dienstbemiddelaar (service intermediary) are a relevant party and must be listed as audience. For a Dienstaanbieder for whom only the OIN is known, the notation 'urn:etoegang:DV:<OIN>' is to be used.  Other conditions MUST NOT be included. |
|  | **Advice** | Elektronische Toegangsdiensten: MUST NOT be included |
|  | **AuthnStatement** | Elektronische Toegangsdiensten: The attribute AuthnInstant MUST contain the time of authentication.  The AuthnContext element MUST contain an AuthnContextClassRef element containing the level of assurance at which authentication took place and an AuthenticatingAuthority element containing the [OIN format](file:///H:\display\BEHEERAS\OIN+format) of the KvK number of the AD.  In the case of proxying, AuthenticatingAuthority element MUST be populated with a unique identifying attribute for the party that carried out the authentication.  Other attributes and elements MUST NOT be included. |
|  | **Optional Attribute-Statement** | Elektronische Toegangsdiensten:   * MUST be included if StatusCode is 'Success'. MUST NOT be included otherwise. |

### AttributeStatement

The <AttributeStatement> in the summary assertion MUST hold the relevant attribute values obtained in the assertions of the authentication process. The HM MUST NOT add any attributes that are not present in the gathered assertion.

|  |  |  |
| --- | --- | --- |
| **Element/@Attribute** | **0..1** | **Description** |
| **Attribute** | 0..n | Depending on [Rules for processing request](file:///H:\Application%20Data\Microsoft%20Office\Outlook\SecureTempFolder\Interface+specifications+DV-HM.mht):   * MUST include:   + ActingSubjectID – multi-valued containing one ore more SAML <EncryptedID> (see SAML encryption) as value, each containing an applicable identifier of the acting (natural) person for a specific Relying Party (eg DienstVerlener, DienstAanbieder, DienstBemiddelaar or MachtigingsRegister).   + LegalSubjectID – multi-valued containing one ore more SAML <EncryptedID> (see SAML encryption) as value, each containing an applicable identifier(s) of the ServiceConsumer for a specific Relying Party (eg DienstVerlener, DienstAanbieder, DienstBemiddelaar or MachtigingsRegister).   + [ServiceID](https://afsprakenstelsel.etoegang.nl/display/as/ServiceID) - multi-valued SAML-attribute   + [ServiceUUI](https://afsprakenstelsel.etoegang.nl/display/as/ServiceUUID) - multi-valued SAML attribute * MAY include:   + AuthorizationRegistryID (see [EntityID](file:///H:\display\BEHEERAS\EntityID)).   Other Attribute elements MUST NOT be included. |
| **EncryptedAttribute** | 0..n | Depending on [Rules for processing request](file:///H:\Application%20Data\Microsoft%20Office\Outlook\SecureTempFolder\Interface+specifications+DV-HM.mht):   * Additional attributes requested for which the user has granted consent MAY be included here only if the StatusCode is 'Success'.   Other EncryptedAttribute elements MUST NOT be included. |

#### Rules for processing response

A responding AD:

Identifiers:

* MUST include a transient identifier as a <NameID> in Subject; see [Linking of Assertions](https://afsprakenstelsel.etoegang.nl/display/as/Linking+of+Assertions).
* MUST encrypt any other identity according to the rules specified in 3. SAML encryption
* MUST determine appropriate identity(s) according to Determine appropriate ECTA and Identifiers:
* IF representation THEN MUST include an [Internal pseudonym](https://afsprakenstelsel.etoegang.nl/display/as/Internal+pseudonym) of the user for the applicable MR as an <EncryptedID> in ActingSubjectID.
* IF non-representation AND NOT service intermediation THEN MUST include the appropriate identity(s) of the user for the Dienstverlener (DV) as an <EncryptedID> in ActingSubjectID
* IF non-representation AND service intermediation THEN MUST include the appropriate identity(s) of the user for both Dienstverleners (DienstBemiddelaar (DB) and Dienstaanbieder (DA)) as an <EncryptedID> in ActingSubjectID

Attributes:

* MUST include additional attributes as an AttributeStatement.EncryptedAttribute that are requested by the DV (Dienstaanbieder/DienstBemiddelaar) as specified in the [Service catalog](https://afsprakenstelsel.etoegang.nl/display/as/Service+catalog) and consented by the user.
* MUST encrypt attributes according to the rules specified in 3. SAML encryption
* MUST ensure user consent according to rules of the Attribute Policy (see Attributenbeleid)
* IF required attributes cannot be provided (because of consent of not available) MUST act according to [UC on not providing Attributes](https://afsprakenstelsel.etoegang.nl/display/as/Attributen+niet+leverbaar+of+niet+toegestaan): stop the authentication flow and start error flow.

LevelOfAssurance:

* MUST include the Level of Assurance at which the authentication was realized. This realization is the minimum of the Level of Assurance of the registration process of the authenticated user and the Level of Assurance of the authentication mechanism applied. An AD MUST NOT include a level for which it is not certified.

|  |
| --- |
| Determine appropriate ECTA and Identifiers:  * all the EntityConcernedTypes in an [Identifier Set](https://afsprakenstelsel.etoegang.nl/display/as/Identifier+Set) of EntityConcernedTypes with the same set number in the [Service catalog](https://afsprakenstelsel.etoegang.nl/display/as/Service+catalog). * IF no set numbers are used, only one EntityConcernedType is allowed THEN handle this EntityConcernedType as if it was in 1 set. * all the EntityConcernedTypes in the identifier set with the lowest possible set number the AD/MR can provide for this response.LegalSubject. * IF AD/MR can't  provide for any Identifier Set THEN start Error Handling * Determine the response.EntityConcernedTypes and the corresponding response.LegalSubject.Identifiers for the selected identifier set. * For ECTA=BSN the applicable service provider MUST be listed on the BSN Autorisation List OTHERWISE start Error Handling |

**Example attribute after decryption**  Bron uitklappen

<saml:Attribute Name="urn:etoegang:1.9:attribute:FirstName"

xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion"

xmlns:attrext="urn:oasis:names:tc:SAML:attributes:ext"

xmlns:xs="http://www.w3.org/2001/XMLSchema"

xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"

attrext:OriginalIssuer="urn:etoegang:1.9:attribute-sourceid:NLWID"

attrext:LastModified="2015-03-31T12:00:00Z">

<saml:AttributeValue xsi:type="xs:string">...</saml:AttributeValue>

</saml:Attribute>

**Example AD Assertion - representation**  Bron uitklappen

<saml:Assertion IssueInstant="2019-04-18T11:27:55.6592462Z" Version="2.0" ID="\_3d3b90d7-c8ea-4859-9f7c-89017bc2a3b1" xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion">

<saml:Issuer>urn:etoegang:AD:00000003390787490000:entities:9132</saml:Issuer>

<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="#\_3d3b90d7-c8ea-4859-9f7c-89017bc2a3b1">

<Transforms>

<Transform Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature"/>

<Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>

</Transforms>

<DigestMethod Algorithm="http://www.w3.org/2001/04/xmlenc#sha256"/>

<DigestValue>2KTc4ELS13/Tm7svvn0fmKfFSQDiFJwAheaQqJbOGPQ=</DigestValue>

</Reference>

</SignedInfo>

<SignatureValue>YED…..==</SignatureValue>

<KeyInfo>

<KeyName>z2018pp</KeyName>

</KeyInfo>

</Signature>

<saml:Subject>

<saml:NameID Format="urn:oasis:names:tc:SAML:2.0:nameid-format:transient">480F9A2AFA0F420E972F04B16BE0A11840119B0D96054BBCB8F7C5588B2C6580</saml:NameID>

<saml:SubjectConfirmation Method="urn:oasis:names:tc:SAML:2.0:cm:bearer">

<saml:SubjectConfirmationData InResponseTo="\_73b6d7bb-deb4-306e-bfa5-5533450fb66a" NotOnOrAfter="2019-04-18T11:29:55.6592462Z" Recipient="https://eh01.staging.connectis.nl/broker/acs/1.13"/>

</saml:SubjectConfirmation>

</saml:Subject>

<saml:Conditions NotOnOrAfter="2019-04-18T11:29:55.6592462Z" NotBefore="2019-04-18T11:27:55.6592462Z">

<saml:AudienceRestriction>

<saml:Audience>urn:etoegang:HM:00000003244440010000:entities:9632</saml:Audience>

<saml:Audience>urn:etoegang:MR:00000003390787490000:entities:9132</saml:Audience>

<saml:Audience>urn:etoegang:DV:00000003244440010000:entities:9613</saml:Audience>

</saml:AudienceRestriction>

</saml:Conditions>

<saml:AuthnStatement AuthnInstant="2019-04-18T11:27:55.6592462Z">

<saml:AuthnContext>

<saml:AuthnContextClassRef>urn:etoegang:core:assurance-class:loa1</saml:AuthnContextClassRef>

<saml:AuthenticatingAuthority>00000003390787490000</saml:AuthenticatingAuthority>

</saml:AuthnContext>

</saml:AuthnStatement>

<saml:AttributeStatement>

<saml:Attribute Name="urn:etoegang:core:Representation">

<saml:AttributeValue xsi:type="xs:boolean" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xmlns:xs="http://www.w3.org/2001/XMLSchema">1</saml:AttributeValue>

</saml:Attribute>

<saml:Attribute Name="urn:etoegang:core:AuthorizationRegistryID">

<saml:AttributeValue xsi:type="xs:string" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xmlns:xs="http://www.w3.org/2001/XMLSchema">urn:etoegang:MR:00000003390787490000:entities:9132</saml:AttributeValue>

</saml:Attribute>

<saml:Attribute Name="urn:etoegang:core:ActingSubjectID">

<! # ActingSubjectID voor de MR zodat deze de machtiging er bij kan zoeken>

<! # bij de “xenc:EncryptedKey” kan je zien dat de Recipient en MR is. >

<! # Op dit moment bepaalt de MR de identiteit van de Handelende Persoon voor de DV>

<saml:AttributeValue>

<saml:EncryptedID xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion">

<xenc:EncryptedData Type="http://www.w3.org/2001/04/xmlenc#Element" Id="\_deeab93923c945f992f9dd0615633740" xmlns:xenc="http://www.w3.org/2001/04/xmlenc#">

<xenc:EncryptionMethod Algorithm="http://www.w3.org/2001/04/xmlenc#aes256-cbc"/>

<ds:KeyInfo xmlns:ds="http://www.w3.org/2000/09/xmldsig#">

<ds:RetrievalMethod URI="#\_ea5421ff539d41f6a5926eb884a0891b" Type="http://www.w3.org/2001/04/xmlenc#EncryptedKey"/>

</ds:KeyInfo>

<xenc:CipherData>

<xenc:CipherValue>……==</xenc:CipherValue>

</xenc:CipherData>

</xenc:EncryptedData>

<xenc:EncryptedKey Recipient="urn:etoegang:MR:00000003390787490000:entities:9132" Id="\_ea5421ff539d41f6a5926eb884a0891b" xmlns:xenc="http://www.w3.org/2001/04/xmlenc#">

<xenc:EncryptionMethod Algorithm="http://www.w3.org/2001/04/xmlenc#rsa-oaep-mgf1p">

<ds:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1" xmlns:ds="http://www.w3.org/2000/09/xmldsig#"/>

</xenc:EncryptionMethod>

<ds:KeyInfo xmlns:ds="http://www.w3.org/2000/09/xmldsig#">

<ds:KeyName>z2018pp</ds:KeyName>

</ds:KeyInfo>

<xenc:CipherData>

<xenc:CipherValue>….==</xenc:CipherValue>

</xenc:CipherData>

<xenc:ReferenceList>

<xenc:DataReference URI="#\_deeab93923c945f992f9dd0615633740"/>

</xenc:ReferenceList>

</xenc:EncryptedKey>

</saml:EncryptedID>

</saml:AttributeValue>

</saml:Attribute>

<saml:Attribute Name="urn:etoegang:core:ServiceUUID">

<saml:AttributeValue xsi:type="xs:string" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xmlns:xs="http://www.w3.org/2001/XMLSchema">c67fdee4-ebfe-4192-8bc3-1933e451723f</saml:AttributeValue>

</saml:Attribute>

</saml:AttributeStatement>

</saml:Assertion>

### LogoutRequest

For single logout, the Single Logout Profile that is part of the SAML 2.0 Web Browser SSO Profile is applied on the understanding that the logout message is sent to the AD through the HM. The interface for this message is described below.

|  |  |
| --- | --- |
| **@ID** | SAML: Unique message attribute |
| **@Version** | SAML: Version of the SAML protocol. The value MUST be '2.0'. |
| **@IssueInstant** | SAML: Time at which the message was created. |
| **@Destination** | SAML: URL of the AD on which the message is offered. |
| **NameID** | Elektronische Toegangsdiensten: MUST contain a NameID element, this MUST NOT contain the Internal pseudonym or Specific pseudonym of the user. |
| **Issuer** | Elektronische Toegangsdiensten: MUST contain the [EntityID](https://afsprakenstelsel.etoegang.nl/display/as/EntityID) of the HM. |
| **Signature** | Elektronische Toegangsdiensten: MUST contain the [Digital signature](https://afsprakenstelsel.etoegang.nl/display/as/Digital+signature) of the HM for the enveloped message. |

# 3. SAML encryption

Encryption in combination with SAML is achieved via XML-encryption. This paragraph provides an explanation of encrypted elements as well as elements encrypted to multiple recipients.

#### Service Certificate

If the relying party is a DV than the service certificate included in the service catalogue MUST be used for encryption. If the relying party is a participant than the service certificate included in the [Metadata for participants](https://afsprakenstelsel.etoegang.nl/display/as/Metadata+for+participants) MUST be used for encryption. In case more than one certificate is listed for encryption for the relying party, the EncryptedID and EncryptedAttribute MUST be encrypted for each certificate. This will result in multiple EncryptedID’s or EncryptedAttributes (and associated EncryptedKeys)~~. In case of Dienstbemiddeling, additional attributes MUST be encrypted for the Dienstaanbieder (service supplier); the Dienstbemiddelaar MUST NOT be a recipient of the EncryptedAttribute.~~

#### EncryptedID

An <EncryptedID> MUST contain a SAML <NameID> after decryption, with the following properties:

* The Format attribute MUST be set to 'urn:oasis:names:tc:SAML:2.0:nameid-format:persistent'.
* The NameQualifier attribute MUST be populated with the full name of the type of identifying attribute (e.g. 'urn:etoegang:EntityConcernedID:KvKnr').
  + For [Intern pseudoniem](file:///C:\display\BEHEERAS\Intern+pseudoniem) identifiers, the NameQualifier MUST contain the [OIN format](file:///C:\display\BEHEERAS\OIN+format) of the EntityID (KvK number) of the "Authenticatiedienst".
  + For other [Identificerende kenmerken](file:///C:\display\BEHEERAS\Identificerende+kenmerken), the NameQualifier MUST contain the identifing attribute's name, in URI format. For instance for a BSN the value is 'urn:etoegang:1.9:EntityConcernedID:BSN' and for a Specific pseudonym the value is 'urn:etoegang:1.9:EntityConcernedID:Pseudo'.
* The attributes SPNameQualifier and SPProvidedID MUST NOT be used.

#### EncryptedAttribute

Each encrypted attribute is assigned a unique Encrypted\_DATA\_ID that is the same as the attribute name in the attribute catalogue (e.g. urn:etoegang:1.9:attribute:FirstName).

#### Encrypted elements

Any element (eg EncryptedAttribute) that will be encrypted has to conform to the following:

* The element MUST be encrypted using applicable encryption algorithms, as defined in [Encryption](file:///C:\display\BEHEERAS\Encryption).
* A new, cryptographically sound randomly generated symmetric key MUST be used per encrypted element.
* The @Recipient of the resulting <EncryptedKey> MUST be set to the EntityID of the recipient.
* XML contents in the encrypted element MUST have all namespace definitions.

#### Multiple recipients

SAML and XML-encryption allow for multiple recipients of the same encrypted element. The construct for this is specified in more detail in errata E43 of [SAML 2.0 errata 05](http://docs.oasis-open.org/security/saml/v2.0/errata05/os/saml-v2.0-errata05-os.html). In case of multiple recipients:

* each EncryptedKey MUST have a CarriedKeyName equal to the KeyName used in the KeyInfo of the EncryptedData.
* each EncryptedKey SHOULD have a ReferenceList, refering back to the data encrypted with the symmetric key contained.
* Upon decryption, elements without an EncryptedKey intended for the decrypting recipient MAY be ignored and EncryptedKeys for other recipients of encrypted elements SHOULD be ignored.

#### EncryptedAttribute

An <EncryptedAttribute> MUST contain a SAML <Attribute> after decryption, with the following properties:

* The @Name attribute MUST be present.
* One <AttributeValue> per value of the attribute MUST be used.
* A cipher value is included in the encrypted attribute. This cipher value contains the encrypted value of the request attribute that is encrypted with the key of the DV in the service catalogue.

#### Examples

Below two examples are given, with encryption and after decryption. the EncryptedID example is for a single recipient, the EncryptedAttribute example is for multiple recipients. The same construct for single / multiple recipient can be used in the other encrypted element types.

**Example EncryptedID**  Bron uitklappen  <saml2:EncryptedID xmlns:saml2="urn:oasis:names:tc:SAML:2.0:assertion"

xmlns:xenc="http://www.w3.org/2001/04/xmlenc#"

xmlns:ds="http://www.w3.org/2000/09/xmldsig#">

<xenc:EncryptedData xmlns:xenc="http://www.w3.org/2001/04/xmlenc#"

Id="\_cd52e15a16e2a0aa751725ce76a6b866" Type="http://www.w3.org/2001/04/xmlenc#Element">

<xenc:EncryptionMethod Algorithm="http://www.w3.org/2001/04/xmlenc#aes256-cbc" />

<ds:KeyInfo>

<ds:RetrievalMethod Type="http://www.w3.org/2001/04/xmlenc#EncryptedKey"

URI="#\_15531f77a9f1e0b5e0cce442aa31bbd4" />

</ds:KeyInfo>

<xenc:CipherData>

<xenc:CipherValue>AZkW3hbBaQkxs...</xenc:CipherValue>

</xenc:CipherData>

</xenc:EncryptedData>

<xenc:EncryptedKey Id="\_15531f77a9f1e0b5e0cce442aa31bbd4"

Recipient="urn:etoegang:...">

<xenc:EncryptionMethod Algorithm="http://www.w3.org/2001/04/xmlenc#rsa-oaep-mgf1p">

<ds:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1" />

</xenc:EncryptionMethod>

<ds:KeyInfo>

<ds:KeyName>...</ds:KeyName>

</ds:KeyInfo>

<xenc:CipherData>

<xenc:CipherValue>yRy923JJlgAi2MTgx1qohLiDBgi...</xenc:CipherValue>

</xenc:CipherData>

<xenc:ReferenceList>

<xenc:DataReference URI="#\_cd52e15a16e2a0aa751725ce76a6b866" />

</xenc:ReferenceList>

</xenc:EncryptedKey>

</saml2:EncryptedID>

**Example NameID after decryption**  Bron uitklappen

<saml2:NameID xmlns:saml2="urn:oasis:names:tc:SAML:2.0:assertion" Format="urn:oasis:names:tc:SAML:2.0:nameid-format:persistent" NameQualifier="urn:etoegang:1.9:EntityConcernedID:BSN">999999047</saml2:NameID>

**Example EncryptedAttribute - multiple recipients**  Bron uitklappen

 <saml2:EncryptedAttribute xmlns:saml2="urn:oasis:names:tc:SAML:2.0:assertion"

xmlns:xenc="http://www.w3.org/2001/04/xmlenc#"

xmlns:ds="http://www.w3.org/2000/09/xmldsig#">

<xenc:EncryptedData Id="\_3c63798db8a16b54ade207ea0df28ad4" Type="http://www.w3.org/2001/04/xmlenc#Element">

<xenc:EncryptionMethod xmlns:xenc="http://www.w3.org/2001/04/xmlenc#"

Algorithm="http://www.w3.org/2001/04/xmlenc#aes256-cbc" />

<ds:KeyInfo>

<ds:KeyName>\_dd0d7a0215f94ea81b170a2e65834ce8</ds:KeyName>

</ds:KeyInfo>

<xenc:CipherData>

<xenc:CipherValue>5efOYLEoY1PD2145...</xenc:CipherValue>

</xenc:CipherData>

</xenc:EncryptedData>

<xenc:EncryptedKey Id="\_fd73ad54daf1ca14a4aac30ea850340a" Recipient="urn:etoegang:...">

<xenc:EncryptionMethod Algorithm="http://www.w3.org/2001/04/xmlenc#rsa-oaep-mgf1p">

<ds:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1" />

</xenc:EncryptionMethod>

<ds:KeyInfo>

<ds:KeyName>...</ds:KeyName>

</ds:KeyInfo>

<xenc:CipherData>

<xenc:CipherValue>H5nzimm7fAZuzdnZ...</xenc:CipherValue>

</xenc:CipherData>

<xenc:ReferenceList>

<xenc:DataReference URI="#\_3c63798db8a16b54ade207ea0df28ad4" />

</xenc:ReferenceList>

<xenc:CarriedKeyName>\_dd0d7a0215f94ea81b170a2e65834ce8</xenc:CarriedKeyName>

</xenc:EncryptedKey>

<xenc:EncryptedKey Id="\_e152fcf0772b8921f09ec0c1a45f1fa4" Recipient="urn:etoegang:...">

<xenc:EncryptionMethod Algorithm="http://www.w3.org/2001/04/xmlenc#rsa-oaep-mgf1p">

<ds:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1" />

</xenc:EncryptionMethod>

<ds:KeyInfo>

<ds:KeyName>...</ds:KeyName>

</ds:KeyInfo>

<xenc:CipherData xmlns:xenc="http://www.w3.org/2001/04/xmlenc#">

<xenc:CipherValue>xyH8nQscJYAaYwJopGaLPk...</xenc:CipherValue>

</xenc:CipherData>

<xenc:ReferenceList>

<xenc:DataReference URI="#\_3c63798db8a16b54ade207ea0df28ad4" />

</xenc:ReferenceList>

<xenc:CarriedKeyName>\_dd0d7a0215f94ea81b170a2e65834ce8</xenc:CarriedKeyName>

</xenc:EncryptedKey>

</saml2:EncryptedAttribute>

**Example Attribute after decryption**  Bron uitklappen

<saml2:Attribute xmlns:saml2="urn:oasis:names:tc:SAML:2.0:assertion" xmlns:attrext="urn:oasis:names:tc:SAML:attributes:ext" Name="urn:etoegang:attribute:18OrOlder" attrext:OriginalIssuer="urn:etoegang:1.9:attribute-sourceid:NLWID" attrext:LastModified="2015-03-31T12:00:00Z">

<saml2:AttributeValue>false</saml2:AttributeValue>

</saml2:Attribute>

# 4. Digital signature

To guarantee authenticity, integrity and non-repudiation, each message described MUST be provided with a digital signature from the message sender. The message recipient MUST validate all of the digital signatures in the message before processing it.

* The recipient MUST check that the message is signed with a valid digital signature that envelopes the whole message with Enveloped Signature Transform.
* The recipient MUST NOT process the message if it contains parts that are not signed with a valid digital signature.

The following requirements apply to generating digital signatures:

* The digital signature is embedded in the message content with Enveloped Signature Transform <http://www.w3.org/2000/09/xmldsig#enveloped-signature>.
* Canonicalization MUST be carried out according to the exclusive c14n method without comments, as identified by '[http://www.w3.org/2001/10/xml-exc-c14n#](http://www.w3.org/2001/10/xml-exc-c14n)' (see <http://www.w3.org/TR/xml-exc-c14n/>)
* Digests MUST be calculated with the SHA256 algorithm.
* The SignatureValue MUST be calculated with the RSA-SHA256 algorithm.
* The sender MUST sign messages with a PKIoverheid (G2, G3 or newer, or a PKIo EV) certificate with a key length of at least 2048 bits. The (extended) key usage of the used certificate MUST allow use for signing.
* In case of signing metadata, the <Signature> element MUST contain only an <X509Data> element with an <X509Certificate> element.  
  In all other cases, The signature MAY contain a <KeyInfo> element that contains a <KeyName>. The <KeyName> MUST match the <KeyName> stated in the metadata of the sender for the respective role. The signature MUST NOT contain other elements (such as <X509Data>). If a <KeyInfo> element is not included in the message, the metadata MUST contain at least one (1) valid certificate against which the message can be validated. If the metadata contains more than one certificate, the participant MUST validate the message against each valid certificate. The participant MAY agree with its service consumers to limit the period in which the metadata contains more than one certificate. This enables the high utilization of the system to be controlled.
* The Reference MUST refer to the signed element via an ID attribute in the local document, as per the signature profile of SAML2.0 core (§5.4) and SAML 2.0 Metadata (§3.1).