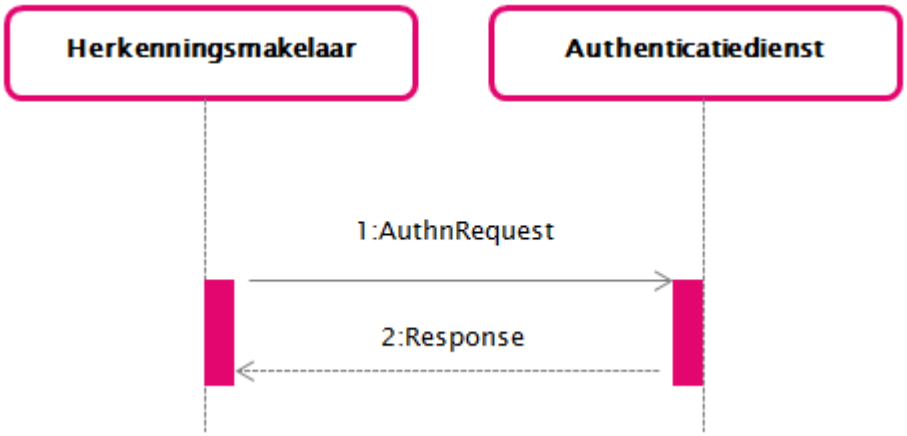
Interface specifications HM-AD

Sequence diagram HM-AD



This page describes the messages that are exchanged between an Herkenningsmakelaar (HM) and an Authenticatiedienst (AD) (identity provider).In the interface described here, the use case 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.

For eIDAS Outbound, the eIDAS Berichtenservice acts as a DV, and as Dienstbemiddelaar (DB) for the BRP. Any statement in this page about the DV should therefore be interpreted as "DV and/or EB".

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] [Response (2)] [Authentication assertion] [AttributeStatement] [Rules for processing response] [No valid Data Center license found] [No valid Data Center license found] [ ] [Determine appropriate ECTA and Identifiers:] [LogoutRequest]

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 MUST use an existing SSO session if one exists, and is applicable (see Single sign-on and user sessions RFC2390).

@IsPassive	Elektronische Toegangsdiensten: MAY be included. If IsPassive is included, the value MUST be 'false'.
@ProtocolBinding	SAML: MUST NOT be included because 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 MUST match an index at the assertion consumer service in the HM's metadata.
@AssertionConsumerServiceURL	SAML: MUST NOT be included because 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 provider.
Issuer	Elektronische Toegangsdiensten: MUST contain the EntityID of the HM. The attributes NameQualifier, SPNameQualifier, Format and SPProvidedID MUST NOT be included.
Signature	Elektronische Toegangsdiensten: MUST contain the Digital signature of the HM for the enveloping message.
Extensions	Elektronische Toegangsdiensten: MUST contain the attributes IntendedAudience, ServiceID and the corresponding ServiceUUID. If the DV queries additional attributes (via an AttributeConsumingService as described in Interface specifications DV-HM and the 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 and MUST be declared as RequestedAttribute in the 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. 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 required by the DV. When RequestedAuthnContext is included in the request, then it must contain a Level of assurance (AuthnContextClassRef) equal to or lower than the level of assurance included in the Service catalog for the requested service.
Scoping	Elektronische Toegangsdiensten: MUST NOT be included

XML schema saml protocol extensions

```
<?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

```
<?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.
- The AD MUST determine the branding to be used.
  - If IntendedAudience is eIDAS Berichtenservice, use eIDAS Outbound branding as described in Richtlijnen communicatie eIDAS.
  - Else, base the branding on the information elements listed in the table below.

Domain	LoA in request	EntityConcernedType in service catalog	Branding
Business	1, 2, 2+, 3, 4	urn:etoegang:1.9:EntityConcernedID:KvKnr urn:etoegang:1.9:EntityConcernedID:RSIN urn:etoegang:1.13:EntityConcernedID:PROBASnr urn:etoegang:1.13:EntityConcernedID:TRR-BD urn:etoegang:1.11:EntityConcernedID:eIDASLegalIdentifier	eHerkenning
Business, Consumer	1, 2, 2+, 3, 4	urn:etoegang:1.12:EntityConcernedID:PseudoID urn:etoegang:1.9:EntityConcernedID:Pseudo	eHerkenning
Citizen*	3, 4	urn:etoegang:1.12:EntityConcernedID:BSN	eHerkenning

  * Citizen: r1.12 only EU-citizens via eIDAS BerichtenService
- The AD MUST process the ActingSubjectTypesAllowed list AND the EntityConcernedID:Pseudo.

If one of the criteria is not met, the AD MUST handle this as a non-recoverable error (see 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 of the AD. The attributes NameQualifier, SPNameQualifier, Format and SPProvidedID MUST NOT be included.
Signature	Elektronische Toegangsdiensten: MUST contain the 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 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

```
<?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 sent 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 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 element that meets the Web Browser SSO profile MUST be included. 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. Note that for eIDAS Outbound, the eIDAS Berichtenservice has the role of Dienstverlener. So the notation of the EntityID is identical as for the DV (with ROLE "DV" and not "EB"). 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 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. In case of representation: • ActingSubjectID (EncryptedID@MR) with the internal pseudonym of the acting user MUST be included. • IF an additional ActingSubjectID is requested by the EB in the servicecatalog, the ASTA will be Encrypted for the EB (as an EncryptedID@EB) and MUST contain all identifiers in ASTA-set as described in the service catalogue for the service. • If the ASTA-set can not be delivered by the AD, the AD MUST respond with a recoverable error (Attributes not supported). See Error handling for more details.

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:
		
		• 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 - multi-valued SAML-attribute
		  ○ ServiceUUID - multi-valued SAML attribute
		• MAY include:
		  • AuthorizationRegistryID (see EntityID).
		
		Other Attribute elements MUST NOT be included.

EncryptedAttribute	0..n	Depending on Rules for processing request • Additional attributes 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.
- MUST encrypt any other identity according to the rules specified in SAML encryption and added as Attribute in the AttributeStatement.
- MUST ensure that a user consents to authentication for:
  - the ServiceProvider,
  - ServiceName
  - (optional/if applicable) "@ProviderName"
  - Personal attributes and/or BSN of the ActingPerson FOR the Intermediated Service and/or Intermediating Service

- MUST ensure only to provide a BSN to receipients on the BSN AutorisationList otherwise respond with a non-recoverable error. See Error handling for more details
- MUST determine appropriate identity(s) according to Determine appropriate ECTA and Identifiers:
- In case of no representation:
  - An AD MUST include all appropriate (ECTA) identifiers of the acting user for the DV in ActingSubjectID, as described in the service catalogue for the service
  - If an AD can not provide any of these requested ECTA-identifiers the AD MUST respond with a recoverable error (Attributes not supported). See Error handling for more details
- In case of Representation
  - An AD MUST include the internal pseudonym of the acting user for the MR in ActingSubjectID

    - If additional ASTA-identifiers are requested by the EB (in the ServiceCatalog) then an AD MUST include all appropriate ASTA-identifiers of the acting user for the DV* in ActingSubjectID, as described in the service catalogue for the service
        - ActingSubjectID MUST contain an EncryptedID encrypted only for the receiving DA/DB that requested the specific ASTA. The recipient of the ASTA for the DA and DB SHOULD be taken from the IntendedAudience element in the request.
            - In case of a DA for whom only the OIN is known, the notation 'urn:etoegang:DV:*<OIN>*' is to be used as recipient.
    - If an AD can not provide any of these requested ASTA-identifiers the AD MUST respond with a recoverable error (Attributes not supported). See Error handling for more details
- In case of Service Intermediation
    - An AD MUST ensure ServiceProvider is authorised to use service intermediation as stated on the list AllowedForServiceIntermediation IF the AD does not want to use the service catalog to determine that the ServiceProvider is authorised to intermediate the intermediated service
    - If the AD does configure the AllowedForServiceIntermediation list locally, An the AD MUST use the ServiceCatalog to determine that the ensure ServiceProvider is authorised to intermediate the intermediated service as stated in the ServiceCatalog
    - An AD MUST add ASTA- and ECTA-identifiers for the intermediated service as stated in the ServiceCatalog using the same above processing rules as for the DV
- 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

Reference implementation processing rules for Identities

- DV.ServiceProviderID = ServiceCatalog(request.ServiceUUID).ServiceProviderID
- DV.IntermediatedService = ServiceCatalog(request.ServiceUUID).IntermediatedService
- DV.ASTA-sets = ServiceCatalog(DV.ServiceUUID).ActingSubjectTypeAllowed
- DV.ECTA-sets = ServiceCatalog(DV.ServiceUUID).EntityConcernedTypeAllowed
- IF non-representation THEN
    - Determine approperiate.Identities (DV.ECTA-sets, DV.ServiceProviderID, DV.Type)
    - MUST include all appropriate.Identities (Type and Value) as an EncryptedID@DV in ActingSubjectID
- IF representation THEN
    - MUST include Internal pseudonym of the user for the appropriate MachtigingRegister as an EncryptedID@MR in ActingSubjectID
    - IF DV.ASTA-sets THEN
        - Determine appropriate.Identities (DV.ASTA-sets, DV.ServiceProviderID, DV.Type)
        - MUST include all appropriate.Identities (Type and Value) as an EncryptedID@DV in ActingSubjectID
- **# ico Service Intermediation via service-catalog, DB authorization must be checked in service catalog**
- **IF DV.IntermediatedService AND DV.ServiceProviderID IS IN Config (AllowedForServiceIntermediation) THEN**
    - **DA.ServiceUUID = DV.IntermediatedService**
    - **DA.ServiceProviderID = ServiceCatalog(DA.ServiceUUID).ServiceProviderID**
    - **DA.@intermediationAllowed = ServiceCatalog(DA.ServiceUUID).@intermediationAllowed**
    - **DA.ServiceIntermediationAllowed = ServiceCatalog(DA.ServiceUUID). ServiceIntermediationAllowed**
    - **DA.ASTA-sets = ServiceCatalog(DA.ServiceUUID).ActingSubjectTypeAllowed**
    - **DA.ECTA-sets = ServiceCatalog(DA.ServiceUUID).EntityConcernedTypeAllowed**

- **IF DA.@intermediationAllowed = “generalAvailable” OR (DA.@intermediationAllowed = “requiresApproval” AND DV.ServiceProviderID IS IN DA.ServiceIntermediationAllowed) THEN**
    - **IF non-representation THEN**
        - **Determine approperiate.Identities (DA.ECTA-sets, DA.ServiceProviderID)**
        - **MUST include all appropriate.Identities (Type and Value) as an EncryptedID@DA in ActingSubjectID**
    - **IF representation AND DA.ASTA-sets THEN**
        - **Determine appropriate.Identities (DA.ASTA-sets, DA.ServiceProviderID)**
            - **MUST include all appropriate.Identities (Type and Value) as an EncryptedID@DA in ActingSubjectID**

Determine appropriate.Identities for (ECTA- or ASTA-) Sets for Recepient (DV of DA)

DetermineAppropriateIdentifiers (sets, Recipient.ServiceProviderID)

- GROUP ecta/acta-sets BY setNumber in sets
- ORDER sets ASSENDING BY setNumer
- FOR EACH set IN sets
    - # check IF all IdentityTypes in set can and may be provided for het user
    - FOR EACH IdentifierType IN set
        - IF IdentifierType=BSN AND Recipient.ServiceProviderID NOT on the BSN AutorisationList THEN respond with a unrecoverable error (Attributes not supported). See Error handling for more details.
        - IF IdentifierType can not be provided for this user THEN next set
    - # all IdentifierTypes are checked, current Set = *appropriate* set
    - # Add the Identifiers of the user for all IdentifierTypes (Identificerende kenmerken) in the *appropriate set to appropriate.Identities*
    - FOR EACH IdentifierType IN set
        - appropriate.Identities[IdentifierType] = IdentifierValue of IdentifierType for the user and Receipient combination
    - RETURN appropriate.Identities
- # No appropriate Set can be provides for this user - start error handling
- respond with a recoverable error (Attributes not supported). See Error handling for more details.

Note: At this moment the use of ASTA-sets and Service Intermediarion is limited to the EB for eIDAS Outgoing.

Attributes:

- MUST include additional attributes as an AttributeStatement.EncryptedAttribute that are requested by the DV (Dienstaanbieder/DienstBemiddelaar) as specified in the Service catalog and consented by the user.
- IF required attributes cannot be provided (because of consent of not available) MUST act according to UC on not providing Attributes (see Attributen niet leverbaar of niet toegestaan) : stop the authentication flow and start error flow.
- MUST encrypt attributes according to the rules specified in 3. SAML encryption and added as an Encrypted Attribute in the AttributeStatement.
- MUST ensure user consent according to rules of the Attribute Policy (see Attributenbeleid)
- MUST ensure that only attributes are provided that are listed for the requested service in the service catalog
- If additional required atributes are requested by the DV (in the HM-request) then an AD MUST include these Attributes
- If an AD can not provide a requested required atttributes the AD MUST respond with a recoverable error (Attributes not supported). See Error handling for more details
- If additional optional atributes are requested by the DV (in the HM-request) then an AD SHOULD include these Attribute

---

Reference Implementation of Processing Rules for Attributes

- IF Request.RequestedAttributes THEN
  - FOR EACH attribute IN Request.RequestedAttributes
    - attribute.isRequired = **ServiceCatalog(DV.ServiceUUID).RequestedAttribute [attribute].isRequired**
    - IF attribute available AND user-consent THEN MUST
      - include attribute as EncryptedAttribute@DV with 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).
    - ELSE IF attribute.isRequired THEN respond with a recoverable error). See Error handling for more details.

LevelOfAssurance:

- An AD 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.
- 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 of EntityConcernedTypes with the same set number in the 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

```
<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

```
<?xml version="1.0" encoding="UTF-8"?>
<saml:Assertion xmlns:saml="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#"
    ID="_f0ba7712-50e4-4d30-8bb5-e63a771507de"
```

```
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="#_f0ba7712-50e4-4d30-8bb5-e63a771507de">
            <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>
<saml:Subject>
    <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="#_15531f77a9f1e0b5e0cce442aa31bbd4" />
            </ds:KeyInfo>
            <xenc:CipherData>
                <xenc:CipherValue>...</xenc:CipherValue>
            </xenc:CipherData>
        </xenc:EncryptedData>
        <xenc:EncryptedKey Id="_15531f77a9f1e0b5e0cce442aa31bbd4"
            Recipient="urn:etoegang:MR:...">
            <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:SubjectConfirmation Method="urn:oasis:names:tc:SAML:2.0:cm:bearer">
        <saml:SubjectConfirmationData InResponseTo="_4b5af9ca-33ef-400f-9c97-398ab0c8e9c7"
            NotOnOrAfter="2015-04-10T11:18:28Z" Recipient="https://..." />
    </saml:SubjectConfirmation>
</saml:Subject>
<saml:Conditions NotBefore="2015-04-10T11:16:28Z" NotOnOrAfter="2015-04-10T11:18:28Z">
    <saml:AudienceRestriction>
        <saml:Audience>urn:etoegang:HM:...</saml:Audience>
        <saml:Audience>urn:etoegang:MR:...</saml:Audience>
        <saml:Audience>urn:etoegang:DV:...</saml:Audience>
    </saml:AudienceRestriction>
</saml:Conditions>
<saml:AuthnStatement AuthnInstant="2015-04-10T11:16:28Z">
    <saml:AuthnContext>
        <saml:AuthnContextClassRef>urn:etoegang:core:assurance-class:loa4</saml:AuthnContextClassRef>
```

```
            <saml:AuthenticatingAuthority>...</saml:AuthenticatingAuthority>
        </saml:AuthnContext>
    </saml:AuthnStatement>
    <saml:AttributeStatement>
        <saml:Attribute Name="urn:etoegang:core:Representation">
            <saml:AttributeValue>true</saml:AttributeValue>
        </saml:Attribute>
        <saml:Attribute Name="urn:etoegang:core:ServiceUUID">
            <saml:Attribute>bf83ccef-6c9d-443f-ac11-9df0a0a9d299</saml:Attribute>
        </saml:Attribute>
        <saml:Attribute Name="urn:etoegang:core:ActingSubjectID">
            <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="#_15531f77a9f1e0b5e0cce442aa31bbd4" />
                        </ds:KeyInfo>
                        <xenc:CipherData>
                            <xenc:CipherValue>...</xenc:CipherValue>
                        </xenc:CipherData>
                    </xenc:EncryptedData>
                    <xenc:EncryptedKey Id="_15531f77a9f1e0b5e0cce442aa31bbd4"
                        Recipient="urn:etoegang:MR:...">
                        <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>

 </saml:AttributeStatement>

</saml:Assertion>
```


Example AD Assertion - citizen domain


```
<?xml version="1.0" encoding="UTF-8"?>
<saml:Assertion xmlns:saml="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#"
    ID="_f0ba7712-50e4-4d30-8bb5-e63a771507de"
    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="#_f0ba7712-50e4-4d30-8bb5-e63a771507de">
                <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>
    <saml:Subject>
        <saml:NameID Format="urn:oasis:names:tc:SAML:2.0:nameid-format:transient">d6730e65-500a-44e2-
961e-cca53e7c60a4</saml:NameID>
        <saml:SubjectConfirmation Method="urn:oasis:names:tc:SAML:2.0:cm:bearer">
            <saml:SubjectConfirmationData InResponseTo="_4b5af9ca-33ef-400f-9c97-398ab0c8e9c7"
                NotOnOrAfter="2015-04-10T11:18:28Z" Recipient="https://..." />
        </saml:SubjectConfirmation>
    </saml:Subject>
    <saml:Conditions NotBefore="2015-04-10T11:16:28Z" NotOnOrAfter="2015-04-10T11:18:28Z">
        <saml:AudienceRestriction>
            <saml:Audience>urn:etoegang:HM:...</saml:Audience>
            <saml:Audience>urn:etoegang:KR:...</saml:Audience>
            <saml:Audience>urn:etoegang:DV:...</saml:Audience>
        </saml:AudienceRestriction>
    </saml:Conditions>
    <saml:AuthnStatement AuthnInstant="2015-04-10T11:16:28Z">
        <saml:AuthnContext>
            <saml:AuthnContextClassRef>urn:etoegang:core:assurance-class:loa4</saml:AuthnContextClassRef>
            <saml:AuthenticatingAuthority>...</saml:AuthenticatingAuthority>
        </saml:AuthnContext>
    </saml:AuthnStatement>
    <saml:AttributeStatement>
        <saml:Attribute Name="urn:etoegang:core:Representation">
            <saml:AttributeValue>false</saml:AttributeValue>
        </saml:Attribute>
        <saml:Attribute Name="urn:etoegang:core:ServiceUUID">
            <saml:Attribute>bf83ccef-6c9d-443f-ac11-9df0a0a9d299</saml:Attribute>
        </saml:Attribute>
        <saml:Attribute Name="urn:etoegang:core:ActingSubjectID">
            <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="#_15531f77a9f1e0b5e0cce442aa31bbd4" />
                        </ds:KeyInfo>
                        <xenc:CipherData>
                            <xenc:CipherValue>...</xenc:CipherValue>
                        </xenc:CipherData>
                    </xenc:EncryptedData>
                    <xenc:EncryptedKey Id="_15531f77a9f1e0b5e0cce442aa31bbd4"
                        Recipient="urn:etoegang:KR:...">
                        <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>...</xenc:CipherValue>
                        </xenc:CipherData>
                        <xenc:ReferenceList>
                            <xenc:DataReference URI="#_cd52e15a16e2a0aa751725ce76a6b866" />
                        </xenc:ReferenceList>
                    </xenc:EncryptedKey>
                </saml:EncrypedID>
            </saml:AttributeValue>
        </saml:Attribute>
    </saml:AttributeStatement>
</saml:Assertion>
```


Example AD Assertion - consumer domain


```
<?xml version="1.0" encoding="UTF-8"?>
<saml:Assertion xmlns:saml="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#"
    ID="_f0ba7712-50e4-4d30-8bb5-e63a771507de"
    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="#_f0ba7712-50e4-4d30-8bb5-e63a771507de">
                <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>
    <saml:Subject>
        <saml:NameID Format="urn:oasis:names:tc:SAML:2.0:nameid-format:transient">d6730e65-500a-44e2-
961e-cca53e7c60a4</saml:NameID>
        <saml:SubjectConfirmation Method="urn:oasis:names:tc:SAML:2.0:cm:bearer">
            <saml:SubjectConfirmationData InResponseTo="_4b5af9ca-33ef-400f-9c97-398ab0c8e9c7"
                NotOnOrAfter="2015-04-10T11:18:28Z" Recipient="https://..." />
        </saml:SubjectConfirmation>
    </saml:Subject>
    <saml:Conditions NotBefore="2015-04-10T11:16:28Z" NotOnOrAfter="2015-04-10T11:18:28Z">
        <saml:AudienceRestriction>
            <saml:Audience>urn:etoegang:HM:...</saml:Audience>
            <saml:Audience>urn:etoegang:DV:...</saml:Audience>
        </saml:AudienceRestriction>
    </saml:Conditions>
    <saml:AuthnStatement AuthnInstant="2015-04-10T11:16:28Z">
        <saml:AuthnContext>
            <saml:AuthnContextClassRef>urn:etoegang:core:assurance-class:loa4</saml:AuthnContextClassRef>
            <saml:AuthenticatingAuthority>...</saml:AuthenticatingAuthority>
        </saml:AuthnContext>
    </saml:AuthnStatement>
    <saml:AttributeStatement>
        <saml:Attribute Name="urn:etoegang:core:Representation">
```

```
            <saml:AttributeValue>false</saml:AttributeValue>
        </saml:Attribute>
        <saml:Attribute Name="urn:etoegang:core:ServiceUUID">
            <saml:Attribute>bf83ccef-6c9d-443f-ac11-9df0a0a9d299</saml:Attribute>
        </saml:Attribute>
        <saml:Attribute Name="urn:etoegang:core:ActingSubjectID">
            <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="#_15531f77a9f1e0b5e0cce442aa31bbd4" />
                        </ds:KeyInfo>
                        <xenc:CipherData>
                            <xenc:CipherValue>...</xenc:CipherValue>
                        </xenc:CipherData>
                    </xenc:EncryptedData>
                    <xenc:EncryptedKey Id="_15531f77a9f1e0b5e0cce442aa31bbd4"
                        Recipient="urn:etoegang:DV:...">
                        <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>...</xenc:CipherValue>
                        </xenc:CipherData>
                        <xenc:ReferenceList>
                            <xenc:DataReference URI="#_cd52e15a16e2a0aa751725ce76a6b866" />
                        </xenc:ReferenceList>
                    </xenc:EncryptedKey>
                </saml:EncrypedID>
            </saml:AttributeValue>
        </saml:Attribute>

        <saml:EncryptedAttribute>
            <xenc:EncryptedData Id="Encrypted_urn_etoegang_1.9_attribute_FirstName" Type="http://www.w3.
org/2001/04/xmlenc#Element">
                <xenc:EncryptionMethod Algorithm="http://www.w3.org/2001/04/xmlenc#aes256-cbc" />
                <ds:KeyInfo>
                    <ds:Keyname>...</ds:Keyname>
                </ds:KeyInfo>
                <xenc:CipherData>
                    <xenc:CipherValue>...</xenc:CipherValue>
                </xenc:CipherData>
            </xenc:EncryptedData>
            <xenc:EncryptedKey>
                    ...
            </xenc:EncryptedKey>
        </saml:EncryptedAttribute>
        <saml:EncryptedAttribute>
            <xenc:EncryptedData Id="Encrypted_urn_etoegang_1.9_attribute_18OrOlder" Type="http://www.w3.
org/2001/04/xmlenc#Element">
                <xenc:EncryptionMethod Algorithm="http://www.w3.org/2001/04/xmlenc#aes256-cbc" />
                <ds:KeyInfo>
                    <ds:Keyname>...</ds:Keyname>
                </ds:KeyInfo>
                <xenc:CipherData>
                    <xenc:CipherValue>...</xenc:CipherValue>
                </xenc:CipherData>
            </xenc:EncryptedData>
            <xenc:EncryptedKey>
```

```
                ...
            </xenc:EncryptedKey>
        </saml:EncryptedAttribute>

    </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 of the HM.
Signature	Elektronische Toegangsdiensten: MUST contain the Digital signature of the HM for the enveloped message.