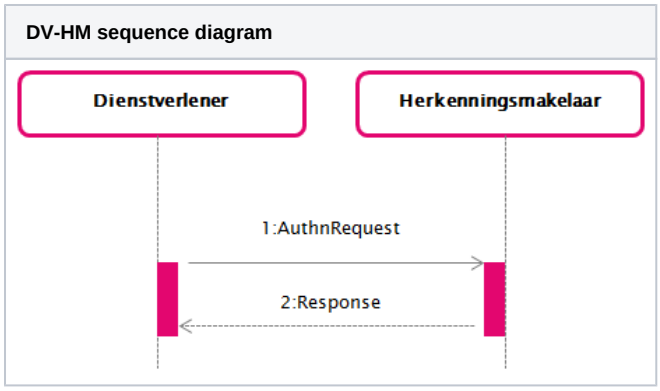
Interface specifications DV-HM



This page describes the messages for the interface specification between a Dienstverlener (DV) (service provider) and an Herkenningsmakelaar (HM) (broker).

The interface specification described in this document is used to implement the use case GUC1 Gebruiken eToegang als dienstafnemer (Use eToegang as service consumer) and MUST (with the exception of alternative 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 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)] [Rules for processing requests] [Response (2)] [HM Summary assertion] [AttributeStatement] [Rules for processing responses] [Copy all relevant] [LogoutRequest] [ProvideKeyMaterial]

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. 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 . If present, the participant MUST check whether the *@AssertionConsumerServiceUrl* is included in the DV's 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 SHOULD be used. The AttributeConsumingService MUST contain exactly *one* attribute with a name that is the same as a long formatted ServiceID. The AttributeConsumingService MAY contain attributes to be requested. Multiple AttributeConsumingService elements MAY be present in the 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 EntityIDs. 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. 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 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 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. 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 (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.
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, 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) (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.
    - 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.
  - the DV MUST show the logo of the applicable brand of the service classifier specified by the DV:

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:1.11:EntityConcernedID:eIDASLegalIdentifier	eHerkenning
Business, Consumer	1, 2, 2+, 3, 4	urn:etoegang:1.12:EntityConcernedID:PseudoID urn:etoegang:1.9:EntityConcernedID:Pseudo	eHerkenning
Consumer	2, 2+, 3, 4	urn:etoegang:1.9:EntityConcernedID:Consumer	Idensys
Citizen	3, 4	urn:etoegang:1.9:EntityConcernedID:BSN	Idensys
Citizen*	3, 4	urn:etoegang:1.12:EntityConcernedID:BSN	eHerkenning

  * Citizen: r1.12 only EU-citizens via eIDAS BerichtenService
  - in case an AD has multiple endpoints (SingleSignOnService elements): the user MUST be allowed to select one of the endpoints, based on the eme:name attribute of applicable SingleSignOnService endpoints, by listing an AD multiple times with the eme:name appended.
  - Alternatively a DV MAY choose to present only an "eIDAS" login option instead, to opt for the eIDAS-berichtenservice as an AD for login with an eIDAS-authentication scheme from another eIDAS-member state:
    - The Dienstverlener MUST use the OrganizationDisplayName as listed on the authentic list (signed by BO/HM) of accredited ADs to present the eIDAS.Berichtenservice to the user and use the EntityID to refer to the EB in the AuthnRequest to the HM.
    - Since this reference is static, a Dienstverlener is not bound to honour the update requirements of a refresh atleast once every 15 minutes as mentioned above.
    - The DV MAY allow the user to select an endpoint of the eIDAS-berichtenservice as AD for a member state using the eme: name attribute, see above.
    - When presenting "eIDAS" the "Idensys/eHerkenning" button MAY also be presented by the DV to allow access to the full list of regular ADs as specified above.
  - A DV MAY offer the user to save the selection of the AD as default. However, if an error occurs when authenticating at a user-preselected default AD, the DV MUST retrieve a current list of accredited AD's from the HM and prompt the user to choose an AD.

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 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) (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.
- MUST sanitize @ProviderName to remove any script or formatting before displaying
- MUST determine the branding to use based on the service classifier specified by the DV.

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:1.11:EntityConcernedID:eIDASLegalIdentifier	eHerkenning
Business, Consumer	1, 2, 2+, 3, 4	urn:etoegang:1.12:EntityConcernedID:PseudoID urn:etoegang:1.9:EntityConcernedID:Pseudo	eHerkenning
Consumer	2, 2+, 3, 4	urn:etoegang:1.9:EntityConcernedID:Consumer	Idensys
Citizen	3, 4	urn:etoegang:1.9:EntityConcernedID:BSN	Idensys
Citizen*	3, 4	urn:etoegang:1.12:EntityConcernedID:BSN	eHerkenning

* Citizen: r1.12 only EU-citizens via eIDAS BerichtenService

If one of the criteria is not met, the HM must handle this as a non-recoverable error (see 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.

- MUST return an error message (containing ResultMajor "RequesterError" and ResultMinor "NotSupported") when a request is directed at the eIDAS-berichtenservice (EB) for a service classified as a native-app in the Service-Catalog, since the EB does not support OAuth.
- In case a portal service request is made at the eIDAS-berichtenservice, the HM MUST return a error message containing ResultMajor "RequesterError" and ResultMinor "NotSupported"

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.
    - In such a scenario a HM MAY opt to only offer a selection list for AD's (GUC3 Aantonen identiteit). This facilitates the current common practice that the AD already knows the MR so that the user will not be confronted with a potential confusing new choice to make whilst this information is already known within the scheme. (However this does invoke the possibility that AD will be confronted with lacking logistic information; see processing rules HM-AD). In case of a Portal request the eIDAS-berichtenservice MUST NOT be offered in the list of AD's to be selected.

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

Example DV AuthnRequest

```
<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

```
<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), 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 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 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.
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.
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

```
<?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#"
    xmlns:xs="http://www.w3.org/2001/XMLSchema"
    xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
    ID="_5e702d5c-de06-11e4-a5a1-080027a35b78"
    InResponseTo="6984066c-de03-11e4-a571-080027a35b78"
    Version="2.0"
    Destination="https://..."
    IssueInstant="2015-04-08T16:30:06Z">
    <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="#_5e702d5c-de06-11e4-a5a1-080027a35b78">
                <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:Status>
        <samlp:StatusCode Value="urn:oasis:names:tc:SAML:2.0:status:Success" />
    </samlp:Status>
    <saml:Assertion Version="2.0"
        ID="_535162e2-de06-11e4-98a2-080027a35b78"
        IssueInstant="2015-04-08T16:30:05Z">
        <saml:Issuer>urn:etoegang:HM:...</saml:Issuer>
        ...
    </saml:Assertion>
</samlp: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 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 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 requires NameID to contain a TransientID or an ActingEntityID (DV connects to r1.09 or older, for older specifications see https://afsprakenstelsel.etoegang.nl/display/archief/Archief).
EncryptedID	0..1	Elektronische Toegangsdiensten: MUST NOT be included.
SubjectConfirmation	1...2	SAML: Contains the 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(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 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, 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 HM Assertion

```
<saml:Assertion Version="2.0"
    ID="_535162e2-de06-11e4-98a2-080027a35b78"
    IssueInstant="2015-04-08T16:30:05Z">
    <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="#_535162e2-de06-11e4-98a2-080027a35b78">
                <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>
    <saml:Subject>
        <saml:SubjectConfirmation Method="urn:oasis:names:tc:SAML:2.0:cm:bearer">
            <saml:SubjectConfirmationData Recipient="https://..." NotOnOrAfter="2015-04-08T16:40:03Z"
InResponseTo="_6984066c-de03-11e4-a571-080027a35b78"/>
        </saml:SubjectConfirmation>
    </saml:Subject>
    <saml:Conditions NotBefore="2015-04-08T16:29:04Z" NotOnOrAfter="2015-04-08T17:00:04Z">
        <saml:AudienceRestriction>
            <saml:Audience>urn:etoegang:DV:...</saml:Audience>
        </saml:AudienceRestriction>
    </saml:Conditions>
    <saml:Advice>
        <saml:Assertion IssueInstant="2015-04-08T16:30:04Z" ID="_8a792d9e-de07-11e4-9db2-080027a35b78"
Version="2.0">
            <saml:Issuer>urn:etoegang:AD:...</saml:Issuer>
            <!-- Verbatim copy of AD declaration of identity contents -->
        </saml:Assertion>
    </saml:Advice>
    <saml:AuthnStatement AuthnInstant="2015-04-08T16:30:04Z">
        <saml:AuthnContext>
            <saml:AuthnContextClassRef>urn:etoegang:core:assurance-class:loa4</saml:AuthnContextClassRef>
        </saml:AuthnContext>
    </saml:AuthnStatement>
    <saml:AttributeStatement>
        ...
    </saml:AttributeStatement>
</saml:Assertion>
```

Example HM Assertion for minimal DV request

```
 <saml:Assertion Version="2.0"
    ID="_535162e2-de06-11e4-98a2-080027a35b78"
    IssueInstant="2015-04-08T16:30:05Z">
    <saml:Issuer>urn:etoegang:HM:...</saml:Issuer>
    <ds:Signature>
        ...
    </ds:Signature>
    <saml:Subject>
        <saml:SubjectConfirmation Method="urn:oasis:names:tc:SAML:2.0:cm:bearer">
            <saml:SubjectConfirmationData Recipient="https://..." NotOnOrAfter="2015-04-08T16:40:03Z"
InResponseTo="_6984066c-de03-11e4-a571-080027a35b78"/>
        </saml:SubjectConfirmation>
    </saml:Subject>
    <saml:Conditions NotBefore="2015-04-08T16:29:04Z" NotOnOrAfter="2015-04-08T17:00:04Z">
        <saml:AudienceRestriction>
            <saml:Audience>urn:etoegang:DV:...</saml:Audience>
        </saml:AudienceRestriction>
    </saml:Conditions>
    <saml:Advice>
        <saml:Assertion IssueInstant="2015-04-08T16:30:04Z" ID="_8a792d9e-de07-11e4-9db2-080027a35b78"
Version="2.0">
            <saml:Issuer>urn:etoegang:AD:...</saml:Issuer>
            <!-- Verbatim copy of AD declaration of identity contents -->
        </saml:Assertion>
    </saml:Advice>
    <saml:AuthnStatement AuthnInstant="2015-04-08T16:30:04Z">
        <saml:AuthnContext>
            <saml:AuthnContextClassRef>urn:etoegang:core:assurance-class:loa4</saml:AuthnContextClassRef>
        </saml:AuthnContext>
    </saml:AuthnStatement>
    <saml:AttributeStatement>
        ...
    </saml:AttributeStatement>
</saml:Assertion>
```

Example HM Assertion for Representation

```
 Vraag het op bij de BO / Ask BO
```

Example HM Assertion for citizen domain

```
 <saml:Assertion Version="2.0"
    ID="_535162e2-de06-11e4-98a2-080027a35b78"
    IssueInstant="2015-04-08T16:30:05Z">
    <saml:Issuer>urn:etoegang:HM:...</saml:Issuer>
    <ds:Signature>
        ...
    </ds:Signature>
    <saml:Subject>
        <saml:SubjectConfirmation Method="urn:oasis:names:tc:SAML:2.0:cm:bearer">
            <saml:SubjectConfirmationData Recipient="https://..." NotOnOrAfter="2015-04-08T16:40:03Z"
InResponseTo="_6984066c-de03-11e4-a571-080027a35b78"/>
        </saml:SubjectConfirmation>
    </saml:Subject>
    <saml:Conditions NotBefore="2015-04-08T16:29:04Z" NotOnOrAfter="2015-04-08T17:00:04Z">
        <saml:AudienceRestriction>
            <saml:Audience>urn:etoegang:DV:...</saml:Audience>
        </saml:AudienceRestriction>
    </saml:Conditions>
    <saml:Advice>
        <saml:Assertion IssueInstant="2015-04-08T16:30:04Z" ID="_8a792d9e-de07-11e4-9db2-080027a35b78"
Version="2.0">
            <saml:Issuer>urn:etoegang:AD:...</saml:Issuer>
            <!-- Verbatim copy of AD declaration of identity contents -->
        </saml:Assertion>
        <saml:Assertion IssueInstant="2015-04-08T16:30:04Z" ID="_8a792d9e-de07-11e4-9db2-080027a35b78"
Version="2.0">
            <saml:Issuer>urn:etoegang:KR:...</saml:Issuer>
            <!-- Verbatim copy of KR declaration of sectoral identity contents -->
        </saml:Assertion>
    </saml:Advice>
    <saml:AuthnStatement AuthnInstant="2015-04-08T16:30:04Z">
        <saml:AuthnContext>
            <saml:AuthnContextClassRef>urn:etoegang:core:assurance-class:loa4</saml:AuthnContextClassRef>
        </saml:AuthnContext>
    </saml:AuthnStatement>
    <saml:AttributeStatement>
        ...
    </saml:AttributeStatement>
</saml: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	Elektronische Toegangsdiensten: Depending on Rules for processing request: • one or more ActingSubjectID's, **the identity of the acting (natural) person** • **EITHER** one or more LegalSubjectID **OR** one or more EntityConcernedID, **the identity of the ServiceConsumer** • ServiceID as multi-valued XACML attribute • **EITHER** exactly one IntermediateEntityID **OR IntermediateSubjectID**, the identity of **last** Intermediary **(in case of Ketenmachtiging)** • one or more ServiceRestrictions, eg ServiceRestriction:Vestigingsnr ~~**In case of Ketenmachtiging, MUST contain the attributeone IntermediateEntityID**~~

EncryptedAttribute	0..n	Depending on Rules for processing request • one or more EncryptedAttributes requested by the DV and provided by the AD and/or MR When using older versions of the interface specifications (e.g. 1.5 or 1.7), attributes MUST be passed according to the current specifications.

Example HM AttributeStatement for citizen domain

```
<saml:AttributeStatement>
    <saml:Attribute Name="urn:etoegang:core:ServiceUUID">
        <saml:AttributeValue xsi:type="xs:string">1ff84f14-df64-11e4-ba1a-080027a35b78</saml:AttributeValue>
    </saml:Attribute>
    <saml:Attribute Name="urn:etoegang:core:AuthorizationRegistryID">
        <saml:AttributeValue xsi:type="xs:string">urn:etoegang:AD:...</saml:AttributeValue>
    </saml:Attribute>
</saml:AttributeStatement>
```

Example HM AttributeStatement for consumer domain

```
<saml:AttributeStatement>
    <saml:Attribute Name="urn:etoegang:core:ServiceUUID">
        <saml:AttributeValue xsi:type="xs:string">0013c492-84cd-4c4b-8206-b13007ac2a1c</saml:AttributeValue>
    </saml:Attribute>
    <saml:EncryptedAttribute>
        <xenc:EncryptedData Id="_copy_Encrypted_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>
    </saml:EncryptedAttribute>
    <saml:EncryptedAttribute>
        <xenc:EncryptedData Id="_copy_Encrypted_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>
    </saml:EncryptedAttribute>
</saml:AttributeStatement>
```

Example HM AttributeStatement for business domain

```
<saml:AttributeStatement>
    <saml:Attribute Name="urn:etoegang:core:ServiceID">
        <saml:AttributeValue xsi:type="xs:string">urn:etoegang:DV:...:services:...</saml:AttributeValue>
    </saml:Attribute>
    <saml:Attribute Name="urn:etoegang:core:ServiceUUID">
        <saml:AttributeValue xsi:type="xs:string">dd4dae83-0f35-4695-b24a-29d470a63ea7</saml:AttributeValue>
    </saml:Attribute>
    <saml:Attribute Name="urn:etoegang:1.9:EntityConcernedID:KvKnr">
        <saml:AttributeValue xsi:type="xs:string">12345678</saml:AttributeValue>
    </saml:Attribute>
    <saml:Attribute Name="urn:etoegang:1.9:ServiceRestriction:Vestigingsnr">
        <saml:AttributeValue xsi:type="xs:string">123456789012</saml:AttributeValue>
    </saml:Attribute>
</saml:AttributeStatement>
```

Example HM AttributeStatement for business domain with multiple entityconcernedtypes

```
<saml:AttributeStatement>
    <saml:Attribute Name="urn:etoegang:core:ServiceID">
        <saml:AttributeValue xsi:type="xs:string">urn:etoegang:DV:...:services:...</saml:AttributeValue>
    </saml:Attribute>
    <saml:Attribute Name="urn:etoegang:core:ServiceUUID">
        <saml:AttributeValue xsi:type="xs:string">dd4dae83-0f35-4695-b24a-29d470a63ea7</saml:AttributeValue>
    </saml:Attribute>
    <saml:Attribute Name="urn:etoegang:1.9:EntityConcernedID:KvKnr">
        <saml:AttributeValue xsi:type="xs:string">12345678</saml:AttributeValue>
    </saml:Attribute>
    <saml:Attribute Name="urn:etoegang:1.9:EntityConcernedID:RSIN">
        <saml:AttributeValue xsi:type="xs:string">987654321</saml:AttributeValue>
    </saml:Attribute>
    <saml:Attribute Name="urn:etoegang:1.9:ServiceRestriction:Vestigingsnr">
        <saml:AttributeValue xsi:type="xs:string">123456789012</saml:AttributeValue>
    </saml:Attribute>
</saml: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.

- 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): 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* DV connects to r1.13 (or newer) AND non-represenation THEN copy AD-assertion: Subject.NameID.TransientID
    - *IF* DV connects to r1.13 (or newer) AND representation THEN copy MR-assertion: Subject.NameID.TransientID
    - *IF* DV connects to r1.11 (or older) *THEN* copy MR-assertion: XACMLAuthz-Decision.Subject.ActingEntityID
- HM MUST provide an <AttributeStatement> with the following <Attributes>
    - *IF* DV connects to r1.13 (or newer) *THEN* copy all relevant MR-Assertion: XACMLAuthz-Decision.Subject.ActingSubjectID (EncryptedID)
    - *IF* DV connects to r1.13 (or newer) *THEN* copy all relevant MR-Assertion: XACMLAuthz-Decision.Subject.LegalSubjectID (EncryptedID)
    - *IF* DV connects to r1.11 (or older) *AND* Representation *THEN* copy the MR-assertion: XACMLAuthz-Decision.Resource.EntityConcernedID
    - *IF* ServiceRestrictions are (requested by the DV and) provided by MR *THEN* copy all relevant MR-assertion: XACMLAuthz-Decision.Resource.ServiceRestrictions

    - *IF* Representation *THEN* copy MR-Assertion: XACMLAuthz-Decision.Statement.Request.Resource.ServiceID
    - *IF* Ketenmachtiging *THEN* copy MR-Assertion: XACMLAuthz-Decision.Statement.Request.Resource.IntermediateEntityID
    - HM MUST provide an <AttributeStatement> with the following <EncryptedAttributes>
        - Copy all relevant AD-assertion: AttributeStatement.EncryptedAttribute
        - *IF* representation *THEN* copy all relevant 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.

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).

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

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).
- MUST be able to process DeprecatedActingSubjectID to facilitate migration or replacements of identifiers.
- 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 wants to decrypt urn:etoegang:1.12:EntityConcernedID:PseudoID or urn:etoegang:1.12:EntityConcernedID:BSN the DV must use preinstalled BSNk-keymaterial and software to obtain the actual identifier.
- 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. This so that a Persistent Pseudonym as well as deprecatedID can be in use at the same time to access an account during migrations.

LogoutRequest

For single logout, the Single Logout Profile that is part of the SAML 2.0 Web Browser SSO Profile is applied, although considering that the logout message is sent to the AD via the HM. Only supported, is the DV's LogoutRequest where the user chooses to log out from the AD. The DV should never expect a LogoutRequest or a LogoutResponse. The interface for this message is described below.

@ID	SAML: Unique message characteristic
@Version	SAML: Version of the SAML protocol. The value MUST be '2.0'.
@IssueInstant	SAML: Time the message was created
@Destination	SAML: URL of the HM on which the message is offered.
NameID	Elektronische Toegangsdiensten: MUST contain a NameID element with the transient from the Subject of the concomitant AD assertion. This MUST NOT contain any identifier of the user.
Issuer	Elektronische Toegangsdiensten: MUST contain the EntityID of the DV.
Signature	Elektronische Toegangsdiensten: MUST contain the Digital signature of the DV for the envelopping message.

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. The HM can request the keys at the BSNk (see 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 I nterface 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.