DV metadata for HM

For each service, a Dienstverlener (DV) MUST supply metadata to the HM as a valid SAML file according to urn:oasis:names:tc:SAML:2.0:metadata with one signed EntityDescriptor element.Signing metadata MUST meet the requirements for signing and encrypting, see Digital signature. For eIDAS-outbound the EB and BRP MUST act in the same way as a Dienstverlener.

Metadata:

This section describes the layout of the metadata. Elements not listed in this table MUST NOT be included in the metadata.

Element/@Attribute	0..n	Description
EntityDesciptor	1	SAML: Required element to start Metadata
@EntityId	1	SAML: MUST contain the EntityID;
@Version	0..1	Elektronische toegangsdiensten: MAY contain an additional version attribute containing the version of the interface specifications on which the entity communicates;
Signature	1	SAML: MUST be included to verify the integrity of the message.
SPSSODescriptor	1	SAML: the SPSSODescriptor implements profiles specific to service providers
@AuthnRequestsSigned	1	Elektronische toegangsdiensten: Must be set to true
@WantsAssertionsSigned	1	Elektronische toegangsdiensten: Must be set to true
@ProtocolSupportEnumeration	1	SAML: Denotes the protocols which can be used. Currently scoped to SAML2.
KeyDescriptor	1..n	SAML: An SPSSODescriptor element MUST contain one or more KeyDescriptor elements with the use XML attribute with value "signing" and one or more KeyDescriptor elements with the use XML attribute with the value "encryption". Alternatively, at least one KeyDescriptor without a use XML attribute MAY be included, indicating the default that the key is for both signing and encryption. Every KeyDescriptor element marked for "signing" MUST contain a KeyName element and a valid PKIoverheid certificate with which the service provider its SAML messages and/or direct TLS connections can be authenticated. KeyDescriptors marked for "signing" are also the keys that will be used to specify the attesting Entity through Holder-of-Key-Subjectconfirmation in case of DienstBemiddeling. KeyDescriptors marked for "signing' MUST be valid and comply with the requirements in Secure connection. Every KeyDescriptor element marked for "encryption" MUST contain a KeyName element and a valid PKIoverheid certificate to be used to encrypt IDs and attributes for the DV. Note: HMs must process all of the described KeyDescriptor elements. KeyName in the signatures and protocol messages indicates which certificate in the metadata is used for the signature.
ArtifactResolutionService	1..n	Elektronische toegangsdiensten: The ArtifactResolutionService MUST be implemented at least once per service.
@Binding	1	SAML: The binding parameter denotes the type of binding used. In theArtifactResolutionService this is the SAML-SOAP binding only. The value of this attribute is an urn relating to: http://docs.oasis-open.org/security/saml/v2.0/saml-bindings-2.0-os.pdf
@Location	1	SAML: The URL of the SAML artifact resolution endpoint
@Index	1	SAML: The index of the binding, MUST be unique for all ArtifactResolutionService elements
AssertionConsumerService	1..n	SAML: The most common AssertionConsumerService is the HTTP-Artifact service binding. This binding is used by the web interface specifications. See Interface specifications for more information. A Service of a Dienstverlener (Service Provider) MAY be offered using only an endpoint with SOAP binding in the AssertionConsumerService of the SPSSODescriptor. In such a case, the Service MUST only be consumed via Dienstbemiddeling (service intermediation). A Service with both a HTTP (Artifact, GET or POST) and SOAP binding, is accessible directly and using Dienstbemiddeling
@Binding	1	SAML: The binding parameter denotes the type of binding used. This is an urn relating to: http://docs.oasis-open.org/security/saml/v2.0/saml-bindings-2.0-os.pdf
@Location	1	SAML: The URL of the SAML endpoint
@Index	1	SAML: The index of the binding, MUST be unique for all AssertionConsumerService elements.

@isDefault	0..1	If several AssertionConsumerService entries are included, one of these entries MUST be flagged as default by setting the isDefault XML attribute with value "true".
AttributeConsumingService	1..n	A service provider MUST include at least one service AttributeConsumingService element in which the service provider indicates which attributes are requested by default. A Service provider MAY include additional AttributeConsumingService elements containing different sets of attributes it wants to receive for the respective additional services. Multiple AttributeConsumingService elements MAY be present 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.
@Index	1	The index of the binding, has to be unique for each AttributeConsumingService.
@isDefault	0..1	In case multiple AttributeConsumingServices are defined, the 'isDefault' XML attribute on that AttributeConsumingService element MUST be used to indicate the default service.
ServiceName	1..n	SAML: Name of the service
@lang	0..1	SAML: Localized name of the service, must be in ISO 31661 alpha2 format
RequestedAttribute	1..n	Each AttributeConsumingService MUST contain exactly one attribute with the same name as ServiceID. This ServiceID MUST reference the entry for the Service of the requesting Dienstverlener (Service Provider) in the Service catalog. In case of Dienstbemiddeling (service intermediation) this ServiceID MUST reference the entry for the Service of the Dienstbemiddelaar (service intermediary). The AttributeConsumingService MAY contain one or more RequestedAttributes that are in the Attribuutcatalogus.
@Name	1	The name of the requested attribute. MUST correspond with attributes from Attribuutcatalogus.
@isRequired	0..1	For each requested attribute that is included, the service provider MAY use isRequired to indicate whether the attribute is required for the DV application to work properly. If isRequired is not defined, the default value 'false' is implied.

The XML schema for the DV Metadata is that of the SAML 2.0 Metadata specification (see https://docs.oasis-open.org/security/saml/v2.0/saml-schema-metadata-2.0.xsd). The optional version attribute is identical to the version attribute as defined in the Metadata for participants, to be used on the EntityDescriptor.

Processing Rules for the HM

- The HM MUST validate the metadata provided by the DV.
- The HM MUST validate the Required attributes based on the Attribuutcatalogus.
- The HM MUST validate the metadata based on the SAML specification
- The HM MAY validate the URL Location parameters in the AssertionConsumerService and ArtifactResolutionService.
- After successfull validation the HM MUST use the DV metadata. The HM MUST NOT use self generated metadata when DV metadata is available
- After successfull validation the HM MUST use the supplied DV metadata as input to create a derivative for the Dienstverlener (DV). The HM MAY use additional information as log as it does not overwrite the DV metadata.
- After successfull validation the HM MUST add the PKIoverheid certificate's in the KeyDescriptor element(s) marked for "encryption" into the ServiceCertificate of the corresponding ServiceInstance in the Service catalog . Note: In the case of DV's employing versions 1.9 or lower, the HM MAY add a valid PKIoverheid certificate of it's own (containing the OIN of the HM) for decryption purposes.
- The HM MAY archive this metadata for future use.

Example DV Metadata

```
<md:EntityDescriptor entityID="urn:etoegang:DV:...">
    <ds:Signature>...</ds:Signature>
    <md:SPSSODescriptor ...>
        ...
    </md:SPSSODescriptor>
</md:EntityDescriptor>
```

Example DV SPSSODescriptor

```
...
<md:SPSSODescriptor AuthnRequestsSigned="true"
    WantAssertionsSigned="true"
    protocolSupportEnumeration="urn:oasis:names:tc:SAML:2.0:protocol">

    <md:KeyDescriptor>...</md:KeyDescriptor>

    <md:ArtifactResolutionService Binding="urn:oasis:names:tc:SAML:2.0:bindings:SOAP" Location="https://..."
index="0" />
    <md:AssertionConsumerService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Artifact" Location="
https://..." index="1" isDefault="true"/>
    <md:AssertionConsumerService Binding="urn:etoegang:1.11:binding:native-app" Location="my-app://..." index="
2"/>

    <md:AttributeConsumingService isDefault="true" index="1">
        <md:ServiceName xml:lang="nl">Voorbeeld Dienst 1</md:ServiceName>
        <md:RequestedAttribute Name="urn:etoegang:DV:0000000312345678000:services:0001"/>
        <md:RequestedAttribute isRequired="false"
            Name="urn:etoegang:attribute:FirstName"/>
        <md:RequestedAttribute isRequired="true"
            Name="urn:etoegang:attribute:18OrOlder"/>
        <md:RequestedAttribute isRequired="false"
            Name="urn:etoegang:attribute:PlaceOfBirth"/>
    </md:AttributeConsumingService>
    <md:AttributeConsumingService isDefault="false" index="2">
        <md:ServiceName xml:lang="nl">Voorbeeld Dienst 50</md:ServiceName>
        <md:RequestedAttribute Name="urn:etoegang:DV:0000000312345678000:services:0050"/>
        <md:RequestedAttribute isRequired="false"
            Name="urn:etoegang:attribute:Gender"/>
        <md:RequestedAttribute isRequired="true"
            Name="urn:etoegang:attribute:DateOfBirth"/>
    </md:AttributeConsumingService>
</md:SPSSODescriptor>
...
```

Example DV KeyDescriptor

```
...
<md:KeyDescriptor use="signing">
        <ds:KeyInfo>
              <ds:KeyName>
2fd4e1c6 7a2d28fc ed849ee1 bb76e739 1b93eb12
              </ds:KeyName>
              <ds:X509Data>
                  <ds:X509Certificate>
...
                   </ds:X509Certificate>
                </ds:X509Data>
          </ds:KeyInfo>
</md:KeyDescriptor>
<md:KeyDescriptor use="encryption">
        <ds:KeyInfo>
              <ds:KeyName>
acfe784b 391916f1 0aedf8e7 9c503658 c71b437e
              </ds:KeyName>
              <ds:X509Data>
                  <ds:X509Certificate>
...
                   </ds:X509Certificate>
                </ds:X509Data>
          </ds:KeyInfo>
</md:KeyDescriptor>...
```