Signicat Documentation

Connecting Your Application

With the Connectis Identity Broker

In this section, you can find information on connecting your application(s) to the Connectis Identity Broker using different protocols or applications. For different options or additional questions related to connecting your application, please contact us on sales@connectis.com.

Initial steps

In order to start with connecting to the Connectis Identity Broker (CIB), please start with the initial steps as described on this page. Without following these important steps you may experience delays, technical difficulties and/or even unnecessary expenses.

In order to set-up your CIB environment, Connectis requires a subdomain reserved through DNS for the use of the Connectis Identity Broker. This will enable you to make use of the different Identity Providers (IdP's).

Step 1: Setting up a domain name

The Connectis Identity Broker will per default be hosted on a domain name in the following format:

```
1 your-organisation-name.cib.connectis.com
```

If required, you can migrate this environment to another domain name. DigiD, for instance, requires that the Connectis Identity Broker runs on a domain name that is managed by your organisation, instead of by Connectis. Please follow these steps to alter your domain name:

1. Choose a new domain name for your instance of the Connectis Identity Broker and send an email to technicalsupport@connectis.com with the new domain name and subdomains you'll be making available for use with the CIB. Ensure that these subdomains do not exist yet and/or are not in use for a production website. Preferably, please provide us with a subdomain for both your pre-production and production environments.

For example:

Pre-production - https://pre-login.yourwebsite.com

Production - https://login.yourwebsite.com

2. We also require the Organisation Identification Number (OIN) corresponding to the Service Provider. This will be needed by the Connectis Technical Support department for the next step.

Note: Connectis uses several techniques to secure the login flow. HTTP Strict Transport Security is one of these. All traffic to and from the domain and all subdomains will be forced to use a secure connection. Please keep this in mind when deciding on a domain name because this will also force other traffic to that same domain to be secure.

Step 2: Purchase PKIo certificates using Certificate Signing Requests (CSRs)

The Connectis Technical Support department will generate Certificate Signing Requests (CSRs) based on the subdomain URLs and OIN you have provided. With these CSRs you'll be able to purchase PKI Overheid G3 certificates, these are mandatory for DigiD and eRecognition.

Please ensure that:

1. You make use of the CSR's provided by Connectis and do not independently purchase the certificates.
2. You do not purchase any other kind of certificate than PKI Overheid G3.

Once you have received the certificates, send the public part of the certificates (which will have the .pem or .cert file extension) to the Connectis Technical Support department. (technicalsupport@connectis.com)

Step 3: DNS changes

With the certificates, the Connectis Technical Support department will start setting up your CIB environment. They will also notify you of the required DNS changes, so that your subdomains (mentioned in step 1) redirect to the Connectis servers. You will receive a DNS entry containing a CNAME. Configure this entry into your DNS server.

Step 4: Invitation to set up your MyConnectis account

Once your CIB environment has been set-up, you'll receive a notification from the Connectis Technical Support department and an invitation to start configuring your MyConnectis account.

In case any of the steps mentioned above are unclear, please contact our Technical Support team.

SAML 2.0
Connect using SAML 2.0

If your service supports SAML 2.0, you can connect it to the Connectis Identity Broker. Please follow these steps:

- Familiarise yourself with the SAML 2.0 protocol, see SAML 2.0 information.
- Identify which SAML 2.0 binding you want to use to send SAML Requests and receive SAML Responses.
- Obtain a certificate for signing.
- Generate SAML 2.0 metadata for your service, containing the signing certificate and endpoints for receiving SAML Responses through the binding of your choice, and send it to Connectis. Contact the supplier of your service if you need additional help with generating metadata.
- Contact technicalsupport@connectis.com to receive metadata of the Connectis Identity Broker and configure it in your service.

Contact the supplier of your service if you need additional help in configuring SAML 2.0 connections on your service. Contact technicalsupport@connectis.com if you need to troubleshoot your connection.

Example messages

Authn Request

DigiD

```
<samlp:AuthnRequest ID="id-47ecada9-32bb-4223-aa0e-ec0c916bffca" Version="2.0" IssueInstant
    xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol">
    <Issuer xmlns="urn:oasis:names:tc:SAML:2.0:assertion">xxx</Issuer>
    <samlp:NameIDPolicy Format="urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified" Allo
</samlp:AuthnRequest>
```

eHerkenning (via Connectis Identity Broker)

For direct connections to the eHerkenning broker, see: Example messages

```
<samlp:AuthnRequest AssertionConsumerServiceIndex="2" AttributeConsumingServiceIndex="0001"
    xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion"
    xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol">
    <saml:Issuer>urn:etoegang:DV:xxx:entities:0001</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-sha25
            <ds:Reference URI="#AuthnRequest-0-b6ce8ee89889814f3f1f7a521028fcd0">
                <ds:Transforms>
                    <ds:Transform Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-s
                    <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>Xp1651fdH6eN6W3H0aXA5aCCHlBLyZChq9mpQuJCUQo=</ds:DigestValu
            </ds:Reference>
        </ds:SignedInfo>
        <ds:SignatureValue>xxx</ds:SignatureValue>
        <ds:KeyInfo>
            <ds:KeyName>xxx</ds:KeyName>
        </ds:KeyInfo>
    </ds:Signature>
    <samlp:RequestedAuthnContext Comparison="minimum">
        <saml:AuthnContextClassRef>urn:etoegang:core:assurance-class:loa3</saml:AuthnContex
    </samlp:RequestedAuthnContext>
</samlp:AuthnRequest>
```

Response

DigiD

```
<samlp:Response xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol" xmlns:ds="http://www.w3
    <saml:Issuer>xxx</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="xxx">
<ds:Transforms>
<ds:Transform Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature"/>
<ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#">
<ec:InclusiveNamespaces xmlns:ec="http://www.w3.org/2001/10/xml-exc-c14n#" PrefixList="xacm
</ds:Transform>
</ds:Transforms>
<ds:DigestMethod Algorithm="http://www.w3.org/2001/04/xmlenc#sha256"/>
<ds:DigestValue>xxx</ds:DigestValue>

</ds:Reference>
</ds:SignedInfo>
<ds:SignatureValue>xxx
</ds:SignatureValue>
</ds:Signature><samlp:Status>
        <samlp:StatusCode Value="urn:oasis:names:tc:SAML:2.0:status:Success"/>
    </samlp:Status>
    <saml:Assertion xmlns:xacml-saml="urn:oasis:xacml:2.0:saml:assertion:schema:os" ID="xx
        <saml:Issuer>xxx</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="xxx">
<ds:Transforms>
<ds:Transform Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature"/>
<ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#">
<ec:InclusiveNamespaces xmlns:ec="http://www.w3.org/2001/10/xml-exc-c14n#" PrefixList="xacr
</ds:Transform>
</ds:Transforms>
<ds:DigestMethod Algorithm="http://www.w3.org/2001/04/xmlenc#sha256"/>
<ds:DigestValue>xxx</ds:DigestValue>
</ds:Reference>
</ds:SignedInfo>
<ds:SignatureValue>xxx
</ds:SignatureValue>
</ds:Signature><saml:Subject>
        <saml:NameID Format="urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified" NameQua
    <saml:SubjectConfirmation Method="urn:oasis:names:tc:SAML:2.0:cm:bearer">
        <saml:SubjectConfirmationData InResponseTo="xxx" NotOnOrAfter="2020-05-28T13:04:15
        </saml:SubjectConfirmationData>
    </saml:SubjectConfirmation>
</saml:Subject>        <saml:Conditions NotBefore="2020-05-28T12:59:15.477Z" NotOnOrAfter="
            <saml:AudienceRestriction>
                <saml:Audience>xxx</saml:Audience>
            </saml:AudienceRestriction>
        </saml:Conditions>
        <saml:AuthnStatement AuthnInstant="2020-05-28T12:59:15.477Z" SessionIndex="xxx">
            <saml:AuthnContext>
                <saml:AuthnContextClassRef>urn:oasis:names:tc:SAML:2.0:ac:classes:MobileTwo
            </saml:AuthnContext>
        </saml:AuthnStatement>
    </saml:Assertion>
</samlp:Response>
```

eHerkenning (via Connectis Identity Broker)

For direct connections to the eHerkenning broker, see: Example messages

```
<samlp:ArtifactResponse xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol"
    xmlns="urn:oasis:names:tc:SAML:2.0:assertion" ID="_f30b7b53-8cd8-3c04-b620-ed6f5d506388
    <Issuer>xx</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-sha25
            <ds:Reference URI="#_f30b7b53-8cd8-3c04-b620-ed6f5d506388">
                <ds:Transforms>
                    <ds:Transform Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-s
                    <ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#">
```

```
                    <ec:InclusiveNamespaces xmlns:ec="http://www.w3.org/2001/10/xml-exc
                </ds:Transform>
            </ds:Transforms>
            <ds:DigestMethod Algorithm="http://www.w3.org/2001/04/xmlenc#sha256"/>
            <ds:DigestValue>rqigiYI/ONomPuYLQf2og/1w6OrY44nf1VK6CS6+7cU=</ds:DigestValu
        </ds:Reference>
    </ds:SignedInfo>
    <ds:SignatureValue>xxx
    </ds:SignatureValue>
    <ds:KeyInfo>
        <ds:KeyName>xxx</ds:KeyName>
    </ds:KeyInfo>
</ds:Signature>
<samlp:Status>
    <samlp:StatusCode Value="urn:oasis:names:tc:SAML:2.0:status:Success"/>
</samlp:Status>
<samlp:Response xmlns:ds="http://www.w3.org/2000/09/xmldsig#"
    xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion"
    xmlns:xs="http://www.w3.org/2001/XMLSchema"
    xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" Destination="xxx" ID="_5b8f9
    <saml:Issuer>xxx</saml:Issuer>
    <ds:Signature>
        <ds:SignedInfo>
            <ds:CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-exc-c14
            <ds:SignatureMethod Algorithm="http://www.w3.org/2001/04/xmldsig-more#rsa-s
            <ds:Reference URI="#_5b8f9918-66e3-3db3-b712-0287f727b000">
                <ds:Transforms>
                    <ds:Transform Algorithm="http://www.w3.org/2000/09/xmldsig#envelope
                    <ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#">
                        <ec:InclusiveNamespaces xmlns:ec="http://www.w3.org/2001/10/xml
                    </ds:Transform>
                </ds:Transforms>
                <ds:DigestMethod Algorithm="http://www.w3.org/2001/04/xmlenc#sha256"/>
                <ds:DigestValue>hzCInhpX40Hoz3hYC/OHiWnJQTBAAac+lZ0IrtjDiS0=</ds:Diges
            </ds:Reference>
        </ds:SignedInfo>
        <ds:SignatureValue>xxx
        </ds:SignatureValue>
        <ds:KeyInfo>
            <ds:KeyName>xxx</ds:KeyName>
        </ds:KeyInfo>
    </ds:Signature>
    <samlp:Status>
        <samlp:StatusCode Value="urn:oasis:names:tc:SAML:2.0:status:Success"/>

    </samlp:Status>
    <saml:Assertion xmlns:xacml-saml="urn:oasis:xacml:2.0:saml:assertion:schema:os" ID=
        <saml:Issuer>xxx</saml:Issuer>
        <saml:Subject>
            <saml:NameID Format="urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified"
            <saml:SubjectConfirmation Method="urn:oasis:names:tc:SAML:2.0:cm:bearer">
                <saml:SubjectConfirmationData InResponseTo="AuthnRequest-0-b6ce8ee8988
                </saml:SubjectConfirmationData>
```

```
                </saml:SubjectConfirmation>
            </saml:Subject>
            <saml:Conditions NotBefore="2020-05-29T06:15:41Z" NotOnOrAfter="2020-05-29T06:1
                <saml:AudienceRestriction>
                    <saml:Audience>urn:etoegang:DV:xxx:entities:0001</saml:Audience>
                </saml:AudienceRestriction>
            </saml:Conditions>
            <saml:AuthnStatement AuthnInstant="2020-05-29T06:15:41Z">
                <saml:AuthnContext>
                    <saml:AuthnContextClassRef>urn:etoegang:core:assurance-class:loa3</saml
                    <saml:AuthenticatingAuthority>urn:etoegang:HM:00000003244440010000:ent
                </saml:AuthnContext>
            </saml:AuthnStatement>
            <saml:AttributeStatement>
                <saml:Attribute Name="urn:etoegang:core:ServiceID">
                    <saml:AttributeValue xsi:type="xs:string">urn:etoegang:DV:xxx:services
                </saml:Attribute>
                <saml:Attribute Name="urn:etoegang:core:ServiceUUID">
                    <saml:AttributeValue xsi:type="xs:string">xxx</saml:AttributeValue>
                </saml:Attribute>
                <saml:Attribute Name="urn:etoegang:1.9:EntityConcernedID:KvKnr">
                    <saml:AttributeValue xsi:type="xs:string">xxx</saml:AttributeValue>
                </saml:Attribute>
                <saml:Attribute FriendlyName="urn:etoegang:1.11:attribute-represented:Compa
                    <saml:AttributeValue xsi:type="xs:string">xxx</saml:AttributeValue>
                </saml:Attribute>
                <saml:Attribute FriendlyName="urn:etoegang:1.13:EntityConcernedID:Pseudo" N
                    <saml:AttributeValue xsi:type="xs:string">xxx</saml:AttributeValue>
                </saml:Attribute>
            </saml:AttributeStatement>
        </saml:Assertion>
    </samlp:Response>
</samlp:ArtifactResponse>
```

OpenID Connect

Connect using OpenID Connect

If your service supports OpenID Connect, you can connect it to the Connectis Identity Broker.

Please follow these steps:

- Familiarise yourself with the OpenID Connect protocol, see OpenID Connect information. The Connectis Identity Broker supports the **Authorisation Code** flow.
- Configure your service to use the **Authorisation Code** flow by setting the correct value for the **response_type** parameter when calling the Connectis Identity Broker authorisation endpoint. Use “code” for **Authorisation Code**.
-

- Before a connection can be established between your service and the Connectis Identity Broker, Connectis needs to know the following credentials of your service:
  - **Client_id** and the **client_secret** (only for **Authorisation Code Grant** flow) parameters. Contact Connectis for instructions on how to define these.
  - **Redirect_uri**, a URL on your service where the response will be sent.

As soon as the minimum information as described above is defined on your side, send it to technicalsupport@connectis.com to start enabling the connection.

- Connectis will provide the credentials of the Connectis Identity Broker containing all the endpoints required, together with the certificates that your service should use for checking the signed JWTs. Configure it in your service.

Contact the supplier of your service if you need additional help in configuring OpenID Connect connections on your service. Contact technicalsupport@connectis.com if you need to troubleshoot your connection.

OAUTH 2.0

Connect using OAuth 2.0

If your service supports OAUTH 2.0, you can connect it to the Connectis Identity Broker.

Please follow these steps:

- Familiarise yourself with the OAUTH 2.0 protocol, see OAUTH 2.0 information.
- Depending on your type of application, choose the applicable flow: **Authorisation Code Grant** flow for regular web apps running on a server or **Implicit Grant** flow, which is suitable for single-page applications running in a browser.
- Configure your service to use the appropriate value for the **response_type** parameter in the authorisation request to select the required flow. Use “code” for **Authorisation Code Grant** or “token” for **Implicit Grant**.
- Before a connection can be established between your service and the Connectis Identity Broker, Connectis needs to know the following credentials of your service:
  - **Client_id** and the **client_secret** (only for **Authorisation Code Grant** flow) parameters. Contact Connectis for instructions on how to define these.
  - **Redirect_uri**, a URL on your service where the response will be sent.

As soon as the minimum information as described above is defined on your side, send it to technicalsupport@connectis.com to start enabling the connection.

- Connectis will provide the credentials of the Connectis Identity Broker containing all the endpoints required for your chosen flow (e.g. authorise endpoint, access_token endpoint, etc.). Configure it in your

service.

Contact the supplier of your service if you need additional help in configuring OAUTH 2.0 connections on your service. Contact technicalsupport@connectis.com if you need to troubleshoot your connection.

Connectis SAML 2.0 Adapter

Connect using the Connectis SAML 2.0 Adapter

When you want to make use of the Signicat SAML 2.0 Adapter, follow the following steps:

- Signcat tact technicalsupport@connectis.com to receive the EULA of the Connectis SAML 2.0 Adapter.
- Sign the EULA and send it back to Signicat.
- You will receive the Signicat SAML 2.0 Adapter, together with documentation on how to easily integrate the adapter into your application and how to setup up the connection to the Signicat Identity Broker.
- Identify which SAML 2.0 binding you want to use to send SAML Requests and receive SAML Responses. See SAML 2.0 information.
- Follow the received Signicat SAML 2.0 Adapter documentation to establish the connection and integrate the adapter into your software.

ADFS

Connect using ADFS

This guide assumes that you already have an ADFS server configured (including a valid SSL certificate) and that it already serves one or more relying party trusts (such as web applications that need identity services).

- First check that the server is properly configured for SAML metadata exchange by checking the Federation metadata endpoint. As described in that document, the metadata URL is https://your-org-name.com/FederationMetadata/2007-06/FederationMetadata.xml (replace <your-org-name.com> with the name of your ADFS server instance).
- Use the metadata file from the step above, exactly as described in the generic flow for using SAML 2.0, to connect to the Connectis Identity Broker. Please note that Artifact binding might be hard to configure or have certain limitations. Resources like this one might be useful if you need to configure Artifact binding. If you change the endpoint configuration, you will need to retrieve the updated metadata.
- Once the ADFS metadata is sent to technicalsupport@connectis.com and the Connectis Identity Broker metadata is received from support, create a new Claims Provider Trust to model the connection to the Connectis Identity Broker.
- At this point, relying party trusts should already be able to authenticate using the Connectis Identity Broker. However, depending on your configuration, it is likely that not all of the attributes are returned in the authentication response, as ADFS might not be configured to include the claims or the subject in the

response. In order for this to happen, you should create a rule for the new claims provider trust so that the desired claims are passed through. Afterwards you need to create a similar rule for the relying party trust so that the claims are also passed through via that connection.
- Test the new connection. Contact technicalsupport@connectis.com if you need to troubleshoot your connection. You can find the ADFS events and errors in Event Viewer, under Applications / ADFS.

Please note that advanced users might find it more convenient and powerful (i.e. there are more configuration options available) to use PowerShell for configuring ADFS.

Managing Connectis Identity Broker metadata in ADFS

This document describes how to manage the Connectis Identity Broker metadata in ADFS. The examples used in this document are from AD FS Management version 10.0.0.0. This document will assume the ADFS server is already setup and operational.

Connect ADFS as service-provider

Use a metadata url (preferred)

1. Request the URL of the ADFS-compatible metadata of the Connectis Identity Broker from technicalsupport@connectis.nl. You can verify that the metadata on this URL is ADFS-compatible, by checking that signature element contains an x509Certificate element. If this element is not present please contact our technical support.
2. Open ADFS management
3. Click on “Claims Provider Trusts”
4. Click on “Add Claims Provider Trusts”
5. Start the wizard
6. Select the first option: “Import data about the claims provider published online or on a local network”
7. Supply the metadata URL of the Connectis Identity Broker.
8. Give a meaningful display name.
9. Finish the wizard.

For more information: https://docs.microsoft.com/en-us/windows-server/identity/ad-fs/operations/create-a-claims-provider-trust

Use a metadata file

1. Alternatively, request a copy of the ADFS-compatible metadata of the Connectis Identity Broker from techncalsupport@connectis.nl. You can verify that the metadata file is ADFS-compatible, by checking

that signature element contains an x509Certificate element. If this element is not present please contact our technical support.

2. Open ADFS management
3. Click on “Claims Provider Trusts”
4. Click on “Add Claims Provider Trusts”
5. Start the wizard
6. Select the first option: “Import data about the claims provider from a file”
7. Select the downloaded Connectis Identity Broker metadata
8. Give a meaningful display name.
9. Finish the wizard.

Add new signing certificate

Trust is created via metadata URL

ADFS will periodically check the configured metadata URL to see if there are any changes and load in the new metadata. It is possible to do this manually:

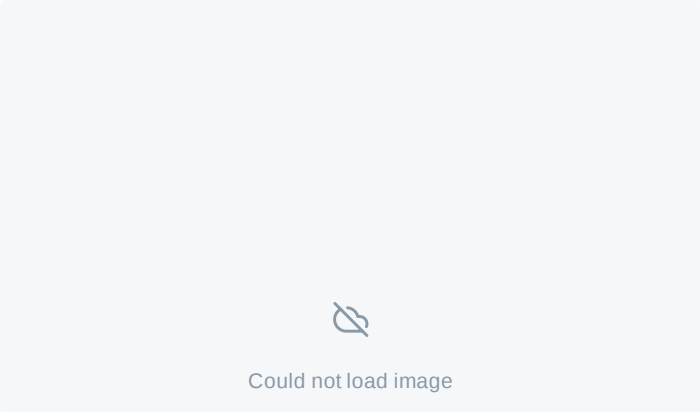
1. Go to created trust
2. Right-click on the trust
3. Select “Update from Federation Metadata”
4. The new metadata is loaded.

Trust is created from file

It is possible to add manually a new signing certificate:

1. Save the new certificate as a pem file.

Copy the public part of the new signing certificate from the Connectis Identity Broker metadata page in the IDPSSODescriptor X509Certificate element :



In a new file place it between:

```
-----BEGIN CERTIFICATE-----
<insert public part here>
-----END CERTIFICATE----
```

And save it with extension *.pem

1. Go to created trust
2. Right-click on the trust
3. Select “Properties”
4. Goto tab certificates
5. Click “Add”
6. Change on the right the file options to “All Files”, so pem files are visible.
7. Select the pem and click open.
8. Click “Apply” and the new certificate is added.

Other third party software

Connect using other third party software

The Connectis Identity Broker is compatible with, amongst others, the following third party services:

- Salesforce
- SAP
- PingFederate
- Channeltivity

If your third party software is not listed, but it features SAML 2.0, OAUTH 2.0 or OpenID Connect, then follow the steps in the section about the specific protocols.

Changing the look & feel of the Connectis Identity Broker

You can optionally alter the look & feel of the Connectis Identity Broker, so that it displays pages in your corporate identity. Please follow these steps to alter the look & feel:

- Contact technicalsupport@connectis.com to receive a copy of your current templates. If you do not have your own set of templates yet, we can provide you with default templates.
- The templates are in HTML format, with variables to substitute information coming from the Connectis Identity Broker. Alter the templates until they set to your likings.
- Send the templates back to technicalsupport@connectis.com. We will notify you once they have been deployed.
- Test the templates after they have been deployed.

Connecting to the Connectis eHerkenning Broker

eHerkenning enables enterprises to log in with numerous service providers in the Netherlands.

The eHerkenning network also interfaces with eIDAS, a system that connects various EU countries' national log-in systems. So, for example, German nationals can use their German log-in to access a Dutch service.

This document explains all you need to know to quickly and efficiently connect your service to the Connectis eHerkenning broker.

If you are using software with its own eHerkenning interface, you can make a direct connection. A connection can be set up within one working day, and the average turnaround time is two weeks.

Connection checklist

Preparation

Contract

The contract between you and Connectis must be signed and sent to sales@connectis.nl. We cannot start the set-up process until we have received the signed contract.

Declaration

You need to sign the declaration agreeing to abide by the requirements and arrangements of the trust framework (https://afsprakenstelsel.etoegang.nl), and send it to technicalsupport@connectis.nl. A declaration is required for any service that is connected to eHerkenning and eIDAS. This declaration needs to be signed by a legal representative of the company.

Application

Your application must be capable of supporting eIDAS and eHerkenning 1.11 and the functions you wish to enable. The interface specifications are available here:

https://afsprakenstelsel.etoegang.nl/display/as/Interface+specifications. Please note that the attributes and identifying characteristics returned by eHerkenning and eIDAS differ. More information about identifying characteristics can be found, under EntityConcernedTypesAllowed.

Connectis Adapter

Connectis has developed various adapters that make it easy to interface with the Connectis Identity Broker. Java and .NET versions of the adapters are available. If you would like an adapter (and supporting documentation), please mail your account manager. To use one of our adapters, you will need to sign an EULA.

For more inforrmation regarding the Connectis Adapters, see the section in API Documentation.

Applying for a connection

PKI Government certificate

You need to have two PKI Overheid (Government) CA 2020 certificates with at least 2048-bit encryption (one certificate for preproduction and one for production). The certificates are used to sign the eHerkenning messages. Existing PKI Government certificates can be reused.

Things you need to decide

Services and assurance levels
You need to decide which services you want connected to eIDAS and eHerkenning. We will need the following details of each service:

- Name
- Description
- Web page
- Assurance level

Connectis can provide guidance on appropriate assurance levels, naming, and the granularity and structure of the authorisation model.

Identifying characteristic type

eIDAS and eHerkenning can return various types of identifying characteristic (EntityConcernedTypes). You can indicate which identifying characteristic your service can accept by selecting an EntityConcernedTypesAllowed.

Attributes

You can request any of the attributes specified in the attribute catalog for eIDAS and eHerkenning (https://afsprakenstelsel.etoegang.nl/display/as/Attribuutcatalogus).
However, please be aware that the delivery of requested attributes is not guaranteed within eIDAS and

eHerkenning, but users whose attributes are not provided must nevertheless be able to log in successfully. See RequestedAttributes for details of the attributes you can request.

Realisation

Step 1 - Pre-production

Send pre-production SAML metadata to Connectis

The SAML metadata consists of an XML file detailing the URLs and certificates used on the various interfaces. You need to generate the file within your software, and then send it to technicalsupport@connectis.nl. Further information about generating metadata is available here: https://afsprakenstelsel.etoegang.nl/display/as/DV+metadata+for+HM

Send eHerkenning service catalog to Connectis

An eIDAS and eHerkenning service catalog is an XML file defining the services that you want to be accessible using eIDAS or eHerkenning. A template service catalog is provided later in this document. Connectis will load the metadata and service catalog into its eIDAS and eHerkenning test network.

Incorporate the pre-production metadata from Connectis into your application

You need to process the SAML metadata file provided by Connectis. All the information you need to connect to Connectis's test environment is available here: https://eh01.connectis.nl/metadata/ (under Pre-production Metadata).

Perform pre-production interface tests

To test your eHerkenning interface, you need to log in using the pre-production accounts set up by Connectis. Pre-production accounts can be applied for here: https://connectis.com/nl/testmiddel-aanvragen/. You do not need to test the interface with each of the various authentication services; it is up to Connectis and the authentication services in question to ensure that they work properly. Test accounts for eIDAS-enabled services can be requested by mailing technicalsupport@connectis.nl.
Please note that, with eHerkenning, the responses you receive make use of SAML Artifact Binding. Consequently, your server must be capable of establishing a connection to the Connectis Identity Broker to retrieve the response message. A common problem for service providers is that their firewall prevents their webserver establishing a connection to the Connectis Identity Broker. Therefore, if your application is not receiving responses as it should, please review your firewall settings.

Step 2 - Preparation for production rollout

Connectis will distribute your service catalog

Once you have successfully completed the test procedures, you should authorise Connectis to distribute your service catalog within the eIDAS and eHerkenning network. That will make your service (or services) accessible to all eHerkenning users.

Please note that access for eHerkenning users is not universally enabled until distribution is complete. It is

Update your website content

You may want to tell your website users that a new log-in system is being introduced. It is a good idea to make information available explaining how eHerkenning log-ins are obtained and used.

Make sure that your support staff and other personnel know about eIDAS/eHerkenning

Your support staff need to understand what eIDAS and eHerkenning are, and what the new system's introduction means for your customers.

Step 3 - Production

Inform Connectis about your production rollout date
Connectis should be put on standby to implement a release on your chosen date. We can then reserve the necessary capacity and arrange for heightened surveillance in the period after the connection goes live.

Send production SAML metadata to Connectis

You need to generate a production SAML metadata file and send it to technicalsupport@connectis.nl.

Incorporate the production metadata from Connectis into your application

You need to process the SAML metadata file provided by Connectis. All the information you need to connect to Connectis's production environment is available here: https://eh01.connectis.nl/metadata/ (under Production Metadata).

Once the interface has been activated, it is available for immediate use by your customers. Connectis will be on standby when the connection goes live, so that any problems that might arise can be dealt with promptly.

Communication

Once you have an eHerkenning connection, it is important to tell your customers about the new set-up in good time, so that they are ready for the change. They need to know that the way they log in is changing, and that they will need to have an eHerkenning log-in. Good internal and external communication is therefore essential.

The eHerkenning Communication Guide provides step-by-step advice on communicating information to the relevant people. The latest version of the Guide is available here: https://www.eherkenning.nl/communicatie

The eHerkenning logo, log-in buttons and assurance levels can be downloaded here: https://bit.ly/2NM9KMH

Interface management

The connection will be maintained, supported and improved by Connectis

You are entitled to preventive and corrective maintenance and break-fix support in order to assure service

continuity.

Break-fix support

Break-fix support involves the investigation and resolution of suspected faults with Connectis's services.

Maintenance

Preventive maintenance involves the continuous refinement and upgrading of software and infrastructure, as necessary to assure service security and stability. That will include ensuring compliance with any new requirements and implementing any mandatory additional eHerkenning interfaces.

Corrective maintenance involves resolving software and infrastructure faults.

Service catalog submission

A service catalog is a file specifying the level assigned to each of your services. The catalog can include details of multiple services and levels. Further information about the service catalog is available here: https://afsprakenstelsel.etoegang.nl/display/as/Service+catalog

A service catalog is created by pasting the following information into a text file, and then completing the various fields.

```
<?xml version="1.0" encoding="UTF-8"?>
<esc:ServiceCatalogue xmlns:esc="urn:etoegang:1.13:service-catalog" xmlns:md="urn:oasis:nar
                      xmlns:ds="http://www.w3.org/2000/09/xmldsig#" xmlns:saml="urn:oasis:n
                      esc:IssueInstant="2019-12-28T10:19:57Z" esc:Version="urn:etoegang:1.1
                      ID="198d678c-239e-43c4-acf7-b4f6f1f6d8c0">
    <esc:ServiceProvider esc:IsPublic="true">
        <esc:ServiceProviderID><!--OIN van organistatie--></esc:ServiceProviderID>
        <esc:OrganizationDisplayName xml:lang="nl"><!--Naam van organistatie--></esc:Organ
        <esc:ServiceDefinition esc:IsPublic="true">
            <esc:ServiceUUID><!--unieke ID genereren via uuidgenerator.net--></esc:ServiceU
            <esc:ServiceName xml:lang="nl"><!--Naam van de Service--></esc:ServiceName>
            <esc:ServiceName xml:lang="en"><!--Naam van de Service--></esc:ServiceName>
            <esc:ServiceDescription xml:lang="nl"><!--Beschrijving van de Service--></esc:S
            <esc:ServiceDescription xml:lang="en"><!--Beschrijving van de Service--></esc:S
            <esc:ServiceDescriptionURL xml:lang="nl">http://example.etoegang.nl</esc:Servic
            <saml:AuthnContextClassRef>urn:etoegang:core:assurance-class:<!--Loa van de Se
            <esc:HerkenningsmakelaarId>00000003244440010000</esc:HerkenningsmakelaarId>
            <esc:EntityConcernedTypesAllowed>urn:etoegang:1.9:EntityConcernedID:KvKnr</esc
              <esc:ServiceRestrictionsAllowed>urn:etoegang:1.9:ServiceRestriction:Vestigin
        </esc:ServiceDefinition>
        <esc:ServiceInstance esc:IsPublic="true">
            <esc:ServiceID>urn:etoegang:DV:<!--OIN -->:services:<!--Service Index--></esc:S
            <esc:ServiceUUID><!--unieke ID genereren via uuidgenerator.net--></esc:ServiceU
            <esc:InstanceOfService><!-- UUID of service definition--></esc:InstanceOfServic
            <esc:ServiceURL xml:lang="nl">vul hier een service url in</esc:ServiceURL>
            <esc:ServiceURL xml:lang="en">vul hier een service url in</esc:ServiceURL>
            <esc:PrivacyPolicyURL xml:lang="nl">vul hier een privacy url in</esc:PrivacyPol
            <esc:PrivacyPolicyURL xml:lang="en">vul hier een privacy url in</esc:PrivacyPol
```

```
            <esc:HerkenningsmakelaarId>00000003244440010000</esc:HerkenningsmakelaarId>
            <esc:SSOSupport><!-- a boolean that indicates if the service supports SingleSi
            <esc:ServiceCertificate>
        <md:KeyDescriptor use="encryption">
          <ds:KeyInfo>
            <ds:KeyName>.............</ds:KeyName>
            <ds:X509Data>
              <ds:X509Certificate>.............</ds:X509Certificate>
            </ds:X509Data>
          </ds:KeyInfo>
        </md:KeyDescriptor>
      </esc:ServiceCertificate>
        </esc:ServiceInstance>
    </esc:ServiceProvider>
</esc:ServiceCatalogue>
```

Your finished file should be sent to technicalsupport@connectis.nl. Connectis will then update the eHerkenning and eIDAS network accordingly.

Classifier

The Classifier is used to connect your service to eHerkenning or eIDAS.

Classifier	Description
No <Classifier> element	The service is connected to eHerkenning.
A <Classifier> element with <Classifier>eIDAS-inbound<Classifier>, as in the example	The service is connected to eIDAS.

EntityConcernedTypesAllowed

The EntityConcernedTypeAllowed field is used to specify the type or types of users who can log in to your service. Various types are possible, depending on whether the service is connected to eHerkenning or eIDAS.

eHerkenning

With eHerkenning, the following EntityConcernedTypesAllowed can be used.

EntityConcernedType	Description
	This option is used if the user is to be identified from the Legal Persons and Partnerships

EntityConcernedID:RSIN	Identification Number of the service user/intermediary that the user represents.
EntityConcernedID:KvKnr	The Trade Register number of the service user/intermediary that the user represents, or an equivalent number.
ServiceRestriction:Vestigingsnr	This option can be used only in combination with EntityConcernedID:KvKnr. The branch number (new format) of the represente service user.

If you enter ServiceRestriction:Vestigingsnr in the EntityConcernedTypeAllowed field, users can log in even if they are subject to a restriction in the authorisations register, allowing them to access the service only on behalf of a particular branch. You, the service provider, must enforce the restriction within your application, so that the user is able to act only on behalf of the branch specified in the response.

eIDAS

EntityConcernedType	**Description**
EntityConcernedID:eIDASLegalIdentifier	An identifying characteristic that is used to identify a Non-Natural Person in eHerkenning via eIDAS within Electronic Access Services.
EntityConcernedID:Pseudo	Used to identify a consumer within eIDAS.

RequestedAttributes

The RequestedAttributes option is used to request additional information about the users accessing your service. Use of RequestedAttributes is optional. Within eHerkenning, provision of the requested attributes is not guaranteed. In eIDAS, however, you are always assured of receiving the requested attributes in incoming responses, providing that they are mandatory attributes. Optional attributes are provided only if they are available for the user in question.

See the trust framework's Attribute Catalogue for more information:

Natural Persons Attribute Catalogue

Non-natural Persons Attribute Catalogue

Generic Attribute Catalogue

```
<esc:EntityConcernedTypesAllowed>urn:etoegang:1.9:EntityConcernedID:Pseudo</esc:EntityConce
  <esc:RequestedAttribute Name="urn:etoegang:1.9:attribute:FirstName" isRequired="true">
     <esc:PurposeStatement xml:lang="en">For testing purposes.</esc:PurposeStatement>
     <esc:PurposeStatement xml:lang="nl">Voor testdoeleinden.</esc:PurposeStatement>
```

```
</esc:RequestedAttribute>
<esc:RequestedAttribute Name="urn:etoegang:1.9:attribute:FamilyName" isRequired="true">
   <esc:PurposeStatement xml:lang="en">For testing purposes.</esc:PurposeStatement>
   <esc:PurposeStatement xml:lang="nl">Voor testdoeleinden.</esc:PurposeStatement>
</esc:RequestedAttribute>
<esc:RequestedAttribute Name="urn:etoegang:1.9:attribute:DateOfBirth" isRequired="true">
   <esc:PurposeStatement xml:lang="en">For testing purposes.</esc:PurposeStatement>
   <esc:PurposeStatement xml:lang="nl">Voor testdoeleinden.</esc:PurposeStatement>
</esc:RequestedAttribute>
```

Example messages

SAML Authn Request

eH 1.13

```
<S11:Envelope xmlns:S11="http://schemas.xmlsoap.org/soap/envelope/">
    <S11:Body>
        <samlp:ArtifactResponse xmlns="urn:oasis:names:tc:SAML:2.0:assertion"
            xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol" ID="xxx" InResponseTo="xxx"
            <Issuer>urn:etoegang:DV:xxx:entities:0098</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
                    <ds:SignatureMethod Algorithm="http://www.w3.org/2001/04/xmldsig-more#
                    <ds:Reference URI="#xxx">
                        <ds:Transforms>
                            <ds:Transform Algorithm="http://www.w3.org/2000/09/xmldsig#enve
                            <ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n
                                <ec:InclusiveNamespaces xmlns:ec="http://www.w3.org/2001/10
                            </ds:Transform>
                        </ds:Transforms>
                        <ds:DigestMethod Algorithm="http://www.w3.org/2001/04/xmlenc#sha256
                        <ds:DigestValue>xxx</ds:DigestValue>
                    </ds:Reference>
                </ds:SignedInfo>
                <ds:SignatureValue>xxx
                </ds:SignatureValue>
                <ds:KeyInfo>
                    <ds:KeyName>xxx</ds:KeyName>
                </ds:KeyInfo>
            </ds:Signature>
            <samlp:Status>
                <samlp:StatusCode Value="urn:oasis:names:tc:SAML:2.0:status:Success"/>
            </samlp:Status>
            <samlp:AuthnRequest xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion" Assertio
                <saml:Issuer>urn:etoegang:DV:xxx:entities:0098</saml:Issuer>
                <ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
```

```
                    <ds:SignedInfo>
                        <ds:CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xm
                        <ds:SignatureMethod Algorithm="http://www.w3.org/2001/04/xmldsig-m
                        <ds:Reference URI="#_xxx">
                            <ds:Transforms>
                                <ds:Transform Algorithm="http://www.w3.org/2000/09/xmldsig
                                <ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc
                                    <ec:InclusiveNamespaces xmlns:ec="http://www.w3.org/20
                                </ds:Transform>
                            </ds:Transforms>
                            <ds:DigestMethod Algorithm="http://www.w3.org/2001/04/xmlenc#sh
                            <ds:DigestValue>xxx</ds:DigestValue>
                        </ds:Reference>
                    </ds:SignedInfo>
                    <ds:SignatureValue>xxx
                    </ds:SignatureValue>
                    <ds:KeyInfo>
                        <ds:KeyName>xxx</ds:KeyName>
                    </ds:KeyInfo>
                </ds:Signature>
                <samlp:RequestedAuthnContext Comparison="minimum">
                    <saml:AuthnContextClassRef>urn:etoegang:core:assurance-class:loa3</sam
                </samlp:RequestedAuthnContext>
            </samlp:AuthnRequest>
        </samlp:ArtifactResponse>
    </S11:Body>
</S11:Envelope>
```

eH 1.11 (eIDAS)

```
<samlp:AuthnRequest xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol"
                    xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion"
                    ForceAuthn="True"
                    AssertionConsumerServiceURL="https://forms.xxxxx.nl/acs"
                    AttributeConsumingServiceIndex="3"
                    Destination="https://eh01.staging.connectis.nl/broker/sso/1.11"
                    ID="_xxxxxxxxxxxxxxxxxxxx"
                    IssueInstant="2020-05-29T06:59:51.9038041Z"
                    Version="2.0">
    <saml:Issuer>urn:etoegang:DV:0000000xxxxxxxxx000:entities:xxxx</saml:Issuer>
    <samlp:RequestedAuthnContext Comparison="minimum">
        <saml:AuthnContextClassRef>urn:etoegang:core:assurance-class:loa2</saml:AuthnConte
    </samlp:RequestedAuthnContext>
    <Signature xmlns="http://www.w3.org/2000/09/xmldsig#">xxxxx</Signature>
</samlp:AuthnRequest>
```

eH 1.9

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

```
                    xmlns="urn:oasis:names:tc:SAML:2.0:assertion" AssertionConsumerServiceU
    <saml:Issuer xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion">urn:etoegang:DV:000000(
    <dsig:Signature xmlns:dsig="http://www.w3.org/2000/09/xmldsig#">
        <dsig:SignedInfo>
            <dsig:CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-exc-c14n
            <dsig:SignatureMethod Algorithm="http://www.w3.org/2001/04/xmldsig-more#rsa-sha
            <dsig:Reference URI="_xxxxxxxxxxxxxxxxxxxx">
                <dsig:Transforms>
                    <dsig:Transform Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-
                    <dsig:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>
                </dsig:Transforms>
                <dsig:DigestMethod Algorithm="http://www.w3.org/2001/04/xmlenc#sha256"/>
                <dsig:DigestValue>xxxx=</dsig:DigestValue>
            </dsig:Reference>
        </dsig:SignedInfo>
        <dsig:SignatureValue>xxxx</dsig:SignatureValue>
        <dsig:KeyInfo>
            <dsig:KeyValue>
                <dsig:RSAKeyValue>

                    <dsig:Modulus>xxxx</dsig:Modulus>
                    <dsig:Exponent>xxxx</dsig:Exponent>
                </dsig:RSAKeyValue>
            </dsig:KeyValue>
        </dsig:KeyInfo>
    </dsig:Signature>
    <samlp:NameIDPolicy AllowCreate="true" Format="urn:oasis:names:tc:SAML:2.0:nameid-forma
    <samlp:RequestedAuthnContext Comparison="minimum">
        <saml:AuthnContextClassRef xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion">urn:e
    </samlp:RequestedAuthnContext>
</samlp:AuthnRequest>
```

eH Chain authorization

```
<?xml version="1.0" encoding="UTF-8" standalone="no"?><md:EntityDescriptor xmlns:md="urn:oa
<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="#_a311f029-0cbd-4508-b56b-62eeca738ce4">
<ds:Transforms>
<ds:Transform Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature"/>
<ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#">
<ec:InclusiveNamespaces xmlns:ec="http://www.w3.org/2001/10/xml-exc-c14n#" PrefixList="xacr
</ds:Transform>
</ds:Transforms>
<ds:DigestMethod Algorithm="http://www.w3.org/2001/04/xmlenc#sha256"/>
<ds:DigestValue>ntI/CmN+1HBtiGPeLU84V8A5rNhjfhyYfvoUTyTCYeM=</ds:DigestValue>
</ds:Reference>
</ds:SignedInfo>
```

SAML Response

eH 1.13

```
<samlp:ArtifactResponse xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol"
    xmlns="urn:oasis:names:tc:SAML:2.0:assertion" ID="xxx" InResponseTo="xxx" IssueInstant=
    <Issuer>urn:etoegang:HM:00000003244440010000:entities:1135</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-sha25
            <ds:Reference URI="#xxx">
                <ds:Transforms>
                    <ds:Transform Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-s
                    <ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#">
                        <ec:InclusiveNamespaces xmlns:ec="http://www.w3.org/2001/10/xml-exc

                    </ds:Transform>
                </ds:Transforms>
                <ds:DigestMethod Algorithm="http://www.w3.org/2001/04/xmlenc#sha256"/>
                <ds:DigestValue>xxx</ds:DigestValue>
            </ds:Reference>
        </ds:SignedInfo>
        <ds:SignatureValue>xxx
        </ds:SignatureValue>
        <ds:KeyInfo>
            <ds:KeyName>xxx</ds:KeyName>
        </ds:KeyInfo>
    </ds:Signature>
    <samlp:Status>
        <samlp:StatusCode Value="urn:oasis:names:tc:SAML:2.0:status:Success"/>
    </samlp:Status>
    <samlp:Response xmlns:ds="http://www.w3.org/2000/09/xmldsig#"
        xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion"
        xmlns:xs="http://www.w3.org/2001/XMLSchema"
        xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" Destination="xxx" ID="xxx" In
        <saml:Issuer>urn:etoegang:HM:00000003244440010000:entities:1135</saml:Issuer>
        <ds:Signature>
            <ds:SignedInfo>
                <ds:CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-exc-c14
                <ds:SignatureMethod Algorithm="http://www.w3.org/2001/04/xmldsig-more#rsa-s
                <ds:Reference URI="#xxx">
                    <ds:Transforms>
                        <ds:Transform Algorithm="http://www.w3.org/2000/09/xmldsig#envelope
                        <ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#">
                            <ec:InclusiveNamespaces xmlns:ec="http://www.w3.org/2001/10/xml
                        </ds:Transform>
                    </ds:Transforms>
                    <ds:DigestMethod Algorithm="http://www.w3.org/2001/04/xmlenc#sha256"/>
                    <ds:DigestValue>xxx</ds:DigestValue>
```

```
            </ds:Reference>
        </ds:SignedInfo>
        <ds:SignatureValue>xxx
        </ds:SignatureValue>
        <ds:KeyInfo>
            <ds:KeyName>xxx</ds:KeyName>
        </ds:KeyInfo>
    </ds:Signature>
    <samlp:Status>
        <samlp:StatusCode Value="urn:oasis:names:tc:SAML:2.0:status:Success"/>
    </samlp:Status>
    <saml:Assertion xmlns:xacml-saml="urn:oasis:xacml:2.0:saml:assertion:schema:os" ID=
        <saml:Issuer>urn:etoegang:HM:00000003244440010000:entities:1135</saml:Issuer>
        <ds:Signature>
            <ds:SignedInfo>
                <ds:CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-exc
                <ds:SignatureMethod Algorithm="http://www.w3.org/2001/04/xmldsig-more#
                <ds:Reference URI="#xxx">
                    <ds:Transforms>
                        <ds:Transform Algorithm="http://www.w3.org/2000/09/xmldsig#enve

                        <ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n
                            <ec:InclusiveNamespaces xmlns:ec="http://www.w3.org/2001/10
                        </ds:Transform>
                    </ds:Transforms>
                    <ds:DigestMethod Algorithm="http://www.w3.org/2001/04/xmlenc#sha256
                    <ds:DigestValue>xxx</ds:DigestValue>
                </ds:Reference>
            </ds:SignedInfo>
            <ds:SignatureValue>xxx
            </ds:SignatureValue>
            <ds:KeyInfo>
                <ds:KeyName>xxx</ds:KeyName>
            </ds:KeyInfo>
        </ds:Signature>
        <saml:Subject>
            <saml:NameID Format="urn:oasis:names:tc:SAML:2.0:nameid-format:transient" N
            <saml:SubjectConfirmation Method="urn:oasis:names:tc:SAML:2.0:cm:bearer">
                <saml:SubjectConfirmationData InResponseTo="xxx" NotOnOrAfter="2020-05-
                </saml:SubjectConfirmationData>
            </saml:SubjectConfirmation>
        </saml:Subject>
        <saml:Conditions NotBefore="2020-05-28T12:42:03Z" NotOnOrAfter="2020-05-28T12:4
            <saml:AudienceRestriction>
                <saml:Audience>urn:etoegang:DV:xxx:entities:0098</saml:Audience>
            </saml:AudienceRestriction>
        </saml:Conditions>
        <saml:Advice>
            <saml:Assertion ID="xxx" IssueInstant="2020-05-28T12:42:02Z" Version="2.0"
                <saml:Issuer>urn:etoegang:AD:00000003341423870000:entities:0113</saml:I
                <ds:Signature>
                    <ds:SignedInfo>
                        <ds:CanonicalizationMethod Algorithm="http://www.w3.org/2001/10
                        <ds:SignatureMethod Algorithm="http://www.w3.org/2001/04/xmlds
```

```
                        <ds:Reference URI="#xxx">
                            <ds:Transforms>
                                <ds:Transform Algorithm="http://www.w3.org/2000/09/xmlc
                                <ds:Transform Algorithm="http://www.w3.org/2001/10/xml-
                            </ds:Transforms>
                            <ds:DigestMethod Algorithm="http://www.w3.org/2001/04/xmlen
                            <ds:DigestValue>xxx</ds:DigestValue>
                        </ds:Reference>
                    </ds:SignedInfo>
                    <ds:SignatureValue>xxx
                    </ds:SignatureValue>
                    <ds:KeyInfo>
                        <ds:KeyName>xxx</ds:KeyName>
                    </ds:KeyInfo>
                </ds:Signature>
                <saml:Subject>
                    <saml:NameID Format="urn:oasis:names:tc:SAML:2.0:nameid-format:tran
                    <saml:SubjectConfirmation Method="urn:oasis:names:tc:SAML:2.0:cm:be
                        <saml:SubjectConfirmationData InResponseTo="xxx" NotOnOrAfter="
                    </saml:SubjectConfirmation>
                </saml:Subject>
                <saml:Conditions NotBefore="2020-05-28T12:32:02Z" NotOnOrAfter="2020-05
                    <saml:AudienceRestriction>
                        <saml:Audience>urn:etoegang:HM:00000003244440010000:entities:11
                        <saml:Audience>urn:etoegang:DV:xxx:entities:0098</saml:Audience
                        <saml:Audience>urn:etoegang:MR:00000003341423870000:entities:01
                    </saml:AudienceRestriction>
                </saml:Conditions>
                <saml:AuthnStatement AuthnInstant="2020-05-28T12:42:01Z">
                    <saml:AuthnContext>
                        <saml:AuthnContextClassRef>urn:etoegang:core:assurance-class:lo
                        <saml:AuthenticatingAuthority>00000003341423870000</saml:Authen
                    </saml:AuthnContext>
                </saml:AuthnStatement>
                <saml:AttributeStatement>
                    <saml:Attribute Name="urn:etoegang:core:Representation">
                        <saml:AttributeValue xsi:type="xs:boolean">true</saml:Attribute
                    </saml:Attribute>
                    <saml:Attribute Name="urn:etoegang:core:ServiceUUID">
                        <saml:AttributeValue xsi:type="xs:string">xxx</saml:AttributeVa
                    </saml:Attribute>
                    <saml:Attribute Name="urn:etoegang:core:AuthorizationRegistryID">
                        <saml:AttributeValue xsi:type="xs:string">urn:etoegang:MR:0000(
                    </saml:Attribute>
                    <saml:Attribute Name="urn:etoegang:core:ActingSubjectID">
                        <saml:AttributeValue>
                            <saml:EncryptedID>
                                <xenc:EncryptedData xmlns:xenc="http://www.w3.org/2001/
                                    <xenc:EncryptionMethod Algorithm="http://www.w3.org
                                    <ds:KeyInfo>
                                        <ds:RetrievalMethod Type="http://www.w3.org/200
                                    </ds:KeyInfo>
                                    <xenc:CipherData>
```

```
                                        <xenc:CipherValue>xxx=</xenc:CipherValue>
                                    </xenc:CipherData>
                                </xenc:EncryptedData>
                                <xenc:EncryptedKey xmlns:xenc="http://www.w3.org/2001/0
                                    <xenc:EncryptionMethod Algorithm="http://www.w3.org
                                        <ds:DigestMethod Algorithm="http://www.w3.org/2
                                    </xenc:EncryptionMethod>
                                    <ds:KeyInfo>
                                        <ds:KeyName>xxx</ds:KeyName>
                                    </ds:KeyInfo>
                                    <xenc:CipherData>
                                        <xenc:CipherValue>xxx</xenc:CipherValue>
                                    </xenc:CipherData>
                                    <xenc:ReferenceList>
                                        <xenc:DataReference URI="#xxx"/>
                                    </xenc:ReferenceList>
                                </xenc:EncryptedKey>
                            </saml:EncryptedID>
                        </saml:AttributeValue>
                    </saml:Attribute>
                </saml:AttributeStatement>
            </saml:Assertion>
            <saml2:Assertion xmlns:saml2="urn:oasis:names:tc:SAML:2.0:assertion" ID="xx
                <saml2:Issuer>urn:etoegang:MR:00000003341423870000:entities:0113</saml2
                <ds:Signature>
                    <ds:SignedInfo>
                        <ds:CanonicalizationMethod Algorithm="http://www.w3.org/2001/10
                        <ds:SignatureMethod Algorithm="http://www.w3.org/2001/04/xmldsi
                        <ds:Reference URI="#xxx">
                            <ds:Transforms>
                                <ds:Transform Algorithm="http://www.w3.org/2000/09/xmld
                                <ds:Transform Algorithm="http://www.w3.org/2001/10/xml-
                                    <ec:InclusiveNamespaces xmlns:ec="http://www.w3.org
                                </ds:Transform>
                            </ds:Transforms>
                            <ds:DigestMethod Algorithm="http://www.w3.org/2001/04/xmlen
                            <ds:DigestValue>xxx</ds:DigestValue>
                        </ds:Reference>
                    </ds:SignedInfo>
                    <ds:SignatureValue>xxx</ds:SignatureValue>
                    <ds:KeyInfo>
                        <ds:KeyName>xxx</ds:KeyName>
                    </ds:KeyInfo>
                </ds:Signature>
                <saml2:Subject>
                    <saml2:NameID Format="urn:oasis:names:tc:SAML:2.0:nameid-format:tra
                </saml2:Subject>
                <saml2:Conditions NotBefore="2020-05-28T12:42:03Z" NotOnOrAfter="2020-0
                <saml2:Advice>
                    <saml2:AssertionIDRef>xxx</saml2:AssertionIDRef>
                </saml2:Advice>
                <saml2:Statement xsi:type="xacml-saml:XACMLAuthzDecisionStatementType">
                    <xacml-context:Response xmlns:xacml-context="urn:oasis:names:tc:xac
```

```
                        <xacml-context:Result>
                            <xacml-context:Decision>Permit</xacml-context:Decision>
                            <xacml-context:Status>
                                <xacml-context:StatusCode Value="urn:oasis:names:tc:xa
                            </xacml-context:Status>
                        </xacml-context:Result>
                    </xacml-context:Response>
                    <xacml-context:Request xmlns:xacml-context="urn:oasis:names:tc:xacr
                        <xacml-context:Subject SubjectCategory="urn:oasis:names:tc:xacr
                            <xacml-context:Attribute AttributeId="urn:etoegang:core:Ac
                                <xacml-context:AttributeValue>xxx</xacml-context:Attri
                            </xacml-context:Attribute>
                            <xacml-context:Attribute AttributeId="urn:etoegang:core:Ac
                                <xacml-context:AttributeValue>
                                    <saml2:EncryptedID>
                                        <xenc:EncryptedData xmlns:xenc="http://www.w3.
                                            <xenc:EncryptionMethod Algorithm="http://w
                                            <ds:KeyInfo>
                                                <ds:RetrievalMethod Type="http://www.w
                                            </ds:KeyInfo>
                                            <xenc:CipherData>
                                                <xenc:CipherValue>xxx</xenc:CipherValu
                                            </xenc:CipherData>
                                        </xenc:EncryptedData>
                                        <xenc:EncryptedKey xmlns:xenc="http://www.w3.o
                                            <xenc:EncryptionMethod Algorithm="http://w
                                                <ds:DigestMethod Algorithm="http://www
                                            </xenc:EncryptionMethod>
                                            <ds:KeyInfo>
                                                <ds:KeyName>xxx</ds:KeyName>
                                            </ds:KeyInfo>
                                            <xenc:CipherData>
                                                <xenc:CipherValue>xxx</xenc:CipherValu
                                            </xenc:CipherData>
                                            <xenc:ReferenceList>
                                                <xenc:DataReference URI="#xxx"/>
                                            </xenc:ReferenceList>
                                        </xenc:EncryptedKey>
                                    </saml2:EncryptedID>
                                </xacml-context:AttributeValue>
                            </xacml-context:Attribute>
                            <xacml-context:Attribute AttributeId="urn:etoegang:core:Li
                                <xacml-context:AttributeValue>xxx</xacml-context:Attri
                            </xacml-context:Attribute>
                            <xacml-context:Attribute AttributeId="urn:etoegang:core:Le
                                <xacml-context:AttributeValue>
                                    <saml2:EncryptedID>
                                        <xenc:EncryptedData xmlns:xenc="http://www.w3.
                                            <xenc:EncryptionMethod Algorithm="http://w
                                            <ds:KeyInfo>
                                                <ds:RetrievalMethod Type="http://www.w
                                            </ds:KeyInfo>
                                            <xenc:CipherData>
```

```
                                        <xenc:CipherValue>xxx</xenc:CipherValue
                                    </xenc:CipherData>
                                </xenc:EncryptedData>
                                <xenc:EncryptedKey xmlns:xenc="http://www.w3.o
                                    <xenc:EncryptionMethod Algorithm="http://w
                                        <ds:DigestMethod Algorithm="http://www
                                    </xenc:EncryptionMethod>
                                    <ds:KeyInfo>
                                        <ds:KeyName>xxx</ds:KeyName>
                                    </ds:KeyInfo>
                                    <xenc:CipherData>
                                        <xenc:CipherValue>xxx</xenc:CipherValue
                                    </xenc:CipherData>
                                    <xenc:ReferenceList>
                                        <xenc:DataReference URI="#_xxx"/>
                                    </xenc:ReferenceList>
                                </xenc:EncryptedKey>
                            </saml2:EncryptedID>
                        </xacml-context:AttributeValue>
                    </xacml-context:Attribute>
                </xacml-context:Subject>
                <xacml-context:Resource>
                    <xacml-context:ResourceContent>
                        <saml2:EncryptedAttribute>
                            <xenc:EncryptedData xmlns:xenc="http://www.w3.org/2
                                <xenc:EncryptionMethod Algorithm="http://www.w3
                                <ds:KeyInfo>
                                    <ds:RetrievalMethod Type="http://www.w3.org
                                </ds:KeyInfo>
                                <xenc:CipherData>
                                    <xenc:CipherValue>xxx</xenc:CipherValue>
                                </xenc:CipherData>
                            </xenc:EncryptedData>
                            <xenc:EncryptedKey xmlns:xenc="http://www.w3.org/20
                                <xenc:EncryptionMethod Algorithm="http://www.w3
                                    <ds:DigestMethod Algorithm="http://www.w3.o
                                </xenc:EncryptionMethod>
                                <ds:KeyInfo>
                                    <ds:KeyName>xxx</ds:KeyName>
                                </ds:KeyInfo>
                                <xenc:CipherData>
                                    <xenc:CipherValue>xxx</xenc:CipherValue>
                                </xenc:CipherData>
                                <xenc:ReferenceList>
                                    <xenc:DataReference URI="#encrypted_urn_etc
                                </xenc:ReferenceList>
                            </xenc:EncryptedKey>
                        </saml2:EncryptedAttribute>
                    </xacml-context:ResourceContent>
                    <xacml-context:Attribute AttributeId="urn:etoegang:core:Le
                        <xacml-context:AttributeValue>urn:etoegang:core:assura
                    </xacml-context:Attribute>
```

```
                            <xacml-context:Attribute AttributeId="urn:etoegang:core:Se
                                <xacml-context:AttributeValue>urn:etoegang:DV:xxx:serv
                            </xacml-context:Attribute>
                            <xacml-context:Attribute AttributeId="urn:etoegang:core:Se
                                <xacml-context:AttributeValue>xxx</xacml-context:Attril
                            </xacml-context:Attribute>
                            <xacml-context:Attribute AttributeId="urn:etoegang:1.9:Ent
                                <xacml-context:AttributeValue>xxx</xacml-context:Attril
                            </xacml-context:Attribute>
                            <xacml-context:Attribute AttributeId="urn:etoegang:core:Lev
                                <xacml-context:AttributeValue>urn:etoegang:core:assuran
                            </xacml-context:Attribute>
                        </xacml-context:Resource>
                        <xacml-context:Action>
                            <xacml-context:Attribute AttributeId="urn:oasis:names:tc:xa
                                <xacml-context:AttributeValue>Authenticate</xacml-conte
                            </xacml-context:Attribute>
                        </xacml-context:Action>
                        <xacml-context:Environment/>
                    </xacml-context:Request>
                </saml2:Statement>

            </saml2:Assertion>
        </saml:Advice>
        <saml:AuthnStatement AuthnInstant="2020-05-28T12:42:03Z">
            <saml:AuthnContext>
                <saml:AuthnContextClassRef>urn:etoegang:core:assurance-class:loa3</saml
                <saml:AuthenticatingAuthority>urn:etoegang:AD:00000033414238700000:ent
            </saml:AuthnContext>
        </saml:AuthnStatement>
        <saml:AttributeStatement>
            <saml:Attribute Name="urn:etoegang:core:ServiceUUID">
                <saml:AttributeValue xsi:type="xs:string">xxx</saml:AttributeValue>
            </saml:Attribute>
            <saml:Attribute Name="urn:etoegang:core:ActingSubjectID">
                <saml:AttributeValue>
                    <saml:EncryptedID xmlns:xenc="http://www.w3.org/2001/04/xmlenc#">
                        <xenc:EncryptedData Id="_xxx" Type="http://www.w3.org/2001/04/x
                            <xenc:EncryptionMethod Algorithm="http://www.w3.org/2001/04
                            <ds:KeyInfo>
                                <ds:RetrievalMethod Type="http://www.w3.org/2001/04/xml
                            </ds:KeyInfo>
                            <xenc:CipherData>
                                <xenc:CipherValue>xxx</xenc:CipherValue>
                            </xenc:CipherData>
                        </xenc:EncryptedData>
                        <xenc:EncryptedKey Id="xxx" Recipient="urn:etoegang:DV:xxx:ent
                            <xenc:EncryptionMethod Algorithm="http://www.w3.org/2001/04
                                <ds:DigestMethod Algorithm="http://www.w3.org/2000/09/x
                            </xenc:EncryptionMethod>
                            <ds:KeyInfo>
                                <ds:KeyName>xxx</ds:KeyName>
                            </ds:KeyInfo>
                            <xenc:CipherData>
```

```
                                <xenc:CipherValue>xxx</xenc:CipherValue>
                            </xenc:CipherData>
                            <xenc:ReferenceList>
                                <xenc:DataReference URI="#_xxx"/>
                            </xenc:ReferenceList>
                        </xenc:EncryptedKey>
                    </saml:EncryptedID>
                </saml:AttributeValue>
            </saml:Attribute>
            <saml:Attribute Name="urn:etoegang:core:LegalSubjectID">
                <saml:AttributeValue>
                    <saml:EncryptedID xmlns:xenc="http://www.w3.org/2001/04/xmlenc#">
                        <xenc:EncryptedData Id="_xxx" Type="http://www.w3.org/2001/04/x
                            <xenc:EncryptionMethod Algorithm="http://www.w3.org/2001/04
                            <ds:KeyInfo>
                                <ds:RetrievalMethod Type="http://www.w3.org/2001/04/xm
                            </ds:KeyInfo>
                            <xenc:CipherData>
                                <xenc:CipherValue>xxx</xenc:CipherValue>
                            </xenc:CipherData>
                        </xenc:EncryptedData>

                        <xenc:EncryptedKey Id="_xxx" Recipient="urn:etoegang:DV:xxx:ent
                            <xenc:EncryptionMethod Algorithm="http://www.w3.org/2001/04
                                <ds:DigestMethod Algorithm="http://www.w3.org/2000/09/x
                            </xenc:EncryptionMethod>
                            <ds:KeyInfo>
                                <ds:KeyName>xxx</ds:KeyName>
                            </ds:KeyInfo>
                            <xenc:CipherData>
                                <xenc:CipherValue>xxx</xenc:CipherValue>
                            </xenc:CipherData>
                            <xenc:ReferenceList>
                                <xenc:DataReference URI="#_xxx"/>
                            </xenc:ReferenceList>
                        </xenc:EncryptedKey>
                    </saml:EncryptedID>
                </saml:AttributeValue>
            </saml:Attribute>
            <saml:Attribute Name="urn:etoegang:core:ServiceID">
                <saml:AttributeValue xsi:type="xs:string">urn:etoegang:DV:xxx:services
            </saml:Attribute>
            <saml:EncryptedAttribute xmlns:xenc="http://www.w3.org/2001/04/xmlenc#">
                <xenc:EncryptedData Id="_xxx" Type="http://www.w3.org/2001/04/xmlenc#El
                    <xenc:EncryptionMethod Algorithm="http://www.w3.org/2001/04/xmlenc#
                    <ds:KeyInfo>
                        <ds:RetrievalMethod Type="http://www.w3.org/2001/04/xmlenc#Enc
                    </ds:KeyInfo>
                    <xenc:CipherData>
                        <xenc:CipherValue>xxx</xenc:CipherValue>
                    </xenc:CipherData>
                </xenc:EncryptedData>
                <xenc:EncryptedKey Id="_xxx" Recipient="urn:etoegang:DV:xxx:entities:00
```

```
                        <xenc:EncryptionMethod Algorithm="http://www.w3.org/2001/04/xmlenc
                        <ds:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#
                        </xenc:EncryptionMethod>
                        <ds:KeyInfo>
                            <ds:KeyName>xxx</ds:KeyName>
                        </ds:KeyInfo>
                        <xenc:CipherData>
                            <xenc:CipherValue>xxx</xenc:CipherValue>
                        </xenc:CipherData>
                        <xenc:ReferenceList>
                            <xenc:DataReference URI="#_xxx"/>
                        </xenc:ReferenceList>
                    </xenc:EncryptedKey>
                </saml:EncryptedAttribute>
            </saml:AttributeStatement>
        </saml:Assertion>
    </samlp:Response>
</samlp:ArtifactResponse>
```

eH 1.11 (eIDAS)

```
<samlp:Response xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol"
                xmlns:ds="http://www.w3.org/2000/09/xmldsig#"
                xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion"
                xmlns:xs="http://www.w3.org/2001/XMLSchema"
                xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
                Destination="https://forms.toverijs7.nl/acs"
                ID="_xxxxxxxxxxxxxxxxxxxx"
                InResponseTo="_xxxxxxxxxxxxxxxxxxxx"
                IssueInstant="2020-05-29T07:00:13Z"
                Version="2.0">
    <saml:Issuer>urn:etoegang:HM:0000000xxxxxxxxx000:entities:xxxx</saml:Issuer>
    <ds:Signature>xxxx</ds:Signature>
    <samlp:Status>
        <samlp:StatusCode Value="urn:oasis:names:tc:SAML:2.0:status:Success"/>
    </samlp:Status>
    <saml:Assertion
            ID="_xxxxxxxxxxxxxxxxxxxx"
            IssueInstant="2020-05-29T07:00:13Z"
            Version="2.0">
        <saml:Issuer>urn:etoegang:HM:0000000xxxxxxxxx000:entities:xxxx</saml:Issuer>
        <ds:Signature>xxxx</ds:Signature>
        <saml:Subject>
            <saml:EncryptedID xmlns:xenc="http://www.w3.org/2001/04/xmlenc#">
                <xenc:EncryptedData Id="_xxxxxxxxxxxxxxxxxxxx"
                                    Type="http://www.w3.org/2001/04/xmlenc#Element">
                    <xenc:EncryptionMethod Algorithm="http://www.w3.org/2001/04/xmlenc#aes
                    <ds:KeyInfo>
                        <ds:RetrievalMethod Type="http://www.w3.org/2001/04/xmlenc#Encrypte
                                            URI="#_xxxxxxxxxxxxxxxxxxxx"/>
                    </ds:KeyInfo>
                    <xenc:CipherData>
```

```
                    <xenc:CipherValue>xxxx</xenc:CipherValue>
                </xenc:CipherData>
            </xenc:EncryptedData>
            <xenc:EncryptedKey Id="_xxxxxxxxxxxxxxxxxxxx"
                               Recipient="urn:etoegang:DV:0000000xxxxxxxxx000:entities
                <xenc:EncryptionMethod Algorithm="http://www.w3.org/2001/04/xmlenc#rsa-
                    <ds:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"
                </xenc:EncryptionMethod>
                <ds:KeyInfo>
                    <ds:KeyName>xxxx</ds:KeyName>
                </ds:KeyInfo>
                <xenc:CipherData>
                    <xenc:CipherValue>xxxx</xenc:CipherValue>
                </xenc:CipherData>
                <xenc:ReferenceList>
                    <xenc:DataReference URI="_xxxxxxxxxxxxxxxxxxxx"/>
                </xenc:ReferenceList>
            </xenc:EncryptedKey>
        </saml:EncryptedID>

        <saml:SubjectConfirmation Method="urn:oasis:names:tc:SAML:2.0:cm:bearer">
            <saml:SubjectConfirmationData InResponseTo="_xxxxxxxxxxxxxxxxxxxx"
                                          NotOnOrAfter="2020-05-29T07:05:13Z"
                                          Recipient="https://forms.xxxxxx.nl/acs"/>
        </saml:SubjectConfirmation>
    </saml:Subject>
    <saml:Conditions NotBefore="2020-05-29T07:00:13Z"
                     NotOnOrAfter="2020-05-29T07:05:13Z">
        <saml:AudienceRestriction>
            <saml:Audience>urn:etoegang:DV:0000000xxxxxxxxx000:entities:xxxx</saml:Aud
        </saml:AudienceRestriction>
    </saml:Conditions>
    <saml:Advice>
        <saml:Assertion ID="sxxxxxxxxxxxxxxxxxxxx"
                        IssueInstant="2020-05-29T07:00:12Z"
                        Version="2.0">
            <saml:Issuer>urn:etoegang:DV:0000000xxxxxxxxx000:entities:xxxx</saml:Issue
            <ds:Signature>
                <ds:SignedInfo>
                    <ds:CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml
                    <ds:SignatureMethod Algorithm="http://www.w3.org/2001/04/xmldsig-mo
                    <ds:Reference URI="_xxxxxxxxxxxxxxxxxxxx">
                        <ds:Transforms>
                            <ds:Transform Algorithm="http://www.w3.org/2000/09/xmldsig#
                            <ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-
                        </ds:Transforms>
                        <ds:DigestMethod Algorithm="http://www.w3.org/2001/04/xmlenc#sh
                        <ds:DigestValue>xxxx=</ds:DigestValue>
                    </ds:Reference>
                </ds:SignedInfo>
                <ds:SignatureValue>xxxx</ds:SignatureValue>
                <ds:KeyInfo>
                    <ds:KeyName>xxxx</ds:KeyName>
```

```
                </ds:KeyInfo>
            </ds:Signature>
            <saml:Subject>
                <saml:NameID Format="urn:oasis:names:tc:SAML:2.0:nameid-format:transie
                <saml:SubjectConfirmation Method="urn:oasis:names:tc:SAML:2.0:cm:beare
                    <saml:SubjectConfirmationData InResponseTo="_xxxxxxxxxxxxxxxxxxxx"
                                                  NotOnOrAfter="2020-05-29T07:10:12Z"
                                                  Recipient="https://eh01.staging.conn
                </saml:SubjectConfirmation>
            </saml:Subject>
            <saml:Conditions NotBefore="2020-05-29T06:50:12Z"
                             NotOnOrAfter="2020-05-29T07:10:12Z">
                <saml:AudienceRestriction>
                    <saml:Audience>urn:etoegang:HM:0000000xxxxxxxxx000:entities:xxxx</s
                    <saml:Audience>urn:etoegang:DV:0000000xxxxxxxxx000:entities:xxxx</s
                </saml:AudienceRestriction>
            </saml:Conditions>
            <saml:AuthnStatement AuthnInstant="2020-05-29T07:00:07Z">
                <saml:AuthnContext>
                    <saml:AuthnContextClassRef>urn:etoegang:core:assurance-class:loa2<
                    <saml:AuthenticatingAuthority>xxxx</saml:AuthenticatingAuthority>
                </saml:AuthnContext>
            </saml:AuthnStatement>
            <saml:AttributeStatement>
                <saml:Attribute Name="urn:etoegang:core:Representation">
                    <saml:AttributeValue xsi:type="xs:boolean">false</saml:AttributeVa
                </saml:Attribute>
                <saml:Attribute Name="urn:etoegang:core:ServiceUUID">
                    <saml:AttributeValue xsi:type="xs:string">xxxx</saml:AttributeValue
                </saml:Attribute>
                <saml:Attribute Name="urn:etoegang:core:ActingSubjectID">
                    <saml:AttributeValue>
                        <saml:EncryptedID>
                            <xenc:EncryptedData xmlns:xenc="http://www.w3.org/2001/04/x
                                                Id="_xxxxxxxxxxxxxxxxxxxx"
                                                Type="http://www.w3.org/2001/04/xmlenc
                                <xenc:EncryptionMethod Algorithm="http://www.w3.org/20
                                <ds:KeyInfo>
                                    <ds:RetrievalMethod Type="http://www.w3.org/2001/04
                                                        URI="_xxxxxxxxxxxxxxxxxxxx"/>
                                </ds:KeyInfo>
                                <xenc:CipherData>
                                    <xenc:CipherValue>xxxx</xenc:CipherValue>
                                </xenc:CipherData>
                            </xenc:EncryptedData>
                            <xenc:EncryptedKey xmlns:xenc="http://www.w3.org/2001/04/xm
                                               Id="_xxxxxxxxxxxxxxxxxxxx"
                                               Recipient="urn:etoegang:DV:0000000xxxxx
                                <xenc:EncryptionMethod Algorithm="http://www.w3.org/20
                                    <ds:DigestMethod Algorithm="http://www.w3.org/2000/
                                </xenc:EncryptionMethod>
                                <ds:KeyInfo>
                                    <ds:KeyName>xxxx</ds:KeyName>
```

```
                                    </ds:KeyInfo>
                                    <xenc:CipherData>
                                        <xenc:CipherValue>xxxx</xenc:CipherValue>
                                    </xenc:CipherData>
                                    <xenc:ReferenceList>
                                        <xenc:DataReference URI="_xxxxxxxxxxxxxxxxxxxx"/>
                                    </xenc:ReferenceList>
                                </xenc:EncryptedKey>
                            </saml:EncryptedID>
                        </saml:AttributeValue>
                    </saml:Attribute>
                    <saml:EncryptedAttribute>
                        <xenc:EncryptedData xmlns:xenc="http://www.w3.org/2001/04/xmlenc#"
                                            Id="encrypted_urn_etoegang_1.9_attribute_DateO
                                            Type="http://www.w3.org/2001/04/xmlenc#Element"
                            <xenc:EncryptionMethod Algorithm="http://www.w3.org/2001/04/xm
                            <ds:KeyInfo>
                                <ds:RetrievalMethod Type="http://www.w3.org/2001/04/xmlenc
                                                    URI="_xxxxxxxxxxxxxxxxxxxx"/>

                            </ds:KeyInfo>
                            <xenc:CipherData>
                                <xenc:CipherValue>xxxx</xenc:CipherValue>
                            </xenc:CipherData>
                        </xenc:EncryptedData>
                        <xenc:EncryptedKey xmlns:xenc="http://www.w3.org/2001/04/xmlenc#"
                                           Id="_xxxxxxxxxxxxxxxxxxxx"
                                           Recipient="urn:etoegang:DV:0000000xxxxxxxxx000:c
                            <xenc:EncryptionMethod Algorithm="http://www.w3.org/2001/04/xm
                                <ds:DigestMethod Algorithm="http://www.w3.org/2000/09/xmlds
                            </xenc:EncryptionMethod>
                            <ds:KeyInfo>
                                <ds:KeyName>xxxx</ds:KeyName>
                            </ds:KeyInfo>
                            <xenc:CipherData>
                                <xenc:CipherValue>xxxx</xenc:CipherValue>
                            </xenc:CipherData>
                            <xenc:ReferenceList>
                                <xenc:DataReference URI="#encrypted_urn_etoegang_1.9_attrib
                            </xenc:ReferenceList>
                        </xenc:EncryptedKey>
                    </saml:EncryptedAttribute>
                    <saml:EncryptedAttribute>
                        <xenc:EncryptedData xmlns:xenc="http://www.w3.org/2001/04/xmlenc#"
                                            Id="encrypted_urn_etoegang_1.9_attribute_Family
                                            Type="http://www.w3.org/2001/04/xmlenc#Element"
                            <xenc:EncryptionMethod Algorithm="http://www.w3.org/2001/04/xm
                            <ds:KeyInfo>
                                <ds:RetrievalMethod Type="http://www.w3.org/2001/04/xmlenc
                                                    URI="_xxxxxxxxxxxxxxxxxxxx"/>
                            </ds:KeyInfo>
                            <xenc:CipherData>
                                <xenc:CipherValue>xxxx</xenc:CipherValue>
```

```
                        </xenc:CipherData>
                    </xenc:EncryptedData>
                    <xenc:EncryptedKey xmlns:xenc="http://www.w3.org/2001/04/xmlenc#"
                                       Id="_xxxxxxxxxxxxxxxxxxxx"
                                       Recipient="urn:etoegang:DV:0000000xxxxxxxxx000:e
                    >
                        <xenc:EncryptionMethod Algorithm="http://www.w3.org/2001/04/xm
                            <ds:DigestMethod Algorithm="http://www.w3.org/2000/09/xmlds
                        </xenc:EncryptionMethod>
                        <ds:KeyInfo>
                            <ds:KeyName>xxxxx</ds:KeyName>
                        </ds:KeyInfo>
                        <xenc:CipherData>
                            <xenc:CipherValue>xxxxx</xenc:CipherValue>
                        </xenc:CipherData>
                        <xenc:ReferenceList>
                            <xenc:DataReference URI="#encrypted_urn_etoegang_1.9_attri
                        </xenc:ReferenceList>
                    </xenc:EncryptedKey>
                </saml:EncryptedAttribute>
                <saml:EncryptedAttribute>
                    <xenc:EncryptedData xmlns:xenc="http://www.w3.org/2001/04/xmlenc#"
                                        Id="encrypted_urn_etoegang_1.9_attribute_FirstN
                                        Type="http://www.w3.org/2001/04/xmlenc#Element"
                        <xenc:EncryptionMethod Algorithm="http://www.w3.org/2001/04/xm
                        <ds:KeyInfo>
                            <ds:RetrievalMethod Type="http://www.w3.org/2001/04/xmlenc
                                                URI="_xxxxxxxxxxxxxxxxxxxx"/>
                        </ds:KeyInfo>
                        <xenc:CipherData>
                            <xenc:CipherValue>xxx</xenc:CipherValue>
                        </xenc:CipherData>
                    </xenc:EncryptedData>
                    <xenc:EncryptedKey xmlns:xenc="http://www.w3.org/2001/04/xmlenc#"
                                       Id="_1c10d90e8b53461cb794fa23b1f72f55"
                                       Recipient="urn:etoegang:DV:0000000xxxxxxxxx000:e
                        <xenc:EncryptionMethod Algorithm="http://www.w3.org/2001/04/xm
                            <ds:DigestMethod Algorithm="http://www.w3.org/2000/09/xmlds
                        </xenc:EncryptionMethod>
                        <ds:KeyInfo>
                            <ds:KeyName>xxxx</ds:KeyName>
                        </ds:KeyInfo>
                        <xenc:CipherData>
                            <xenc:CipherValue>xxxx</xenc:CipherValue>
                        </xenc:CipherData>
                        <xenc:ReferenceList>
                            <xenc:DataReference URI="#encrypted_urn_etoegang_1.9_attri
                        </xenc:ReferenceList>
                    </xenc:EncryptedKey>
                </saml:EncryptedAttribute>
            </saml:AttributeStatement>
        </saml:Assertion>
    </saml:Advice>
```

```
        <saml:AuthnStatement AuthnInstant="2020-05-29T07:00:13Z">
            <saml:AuthnContext>
                <saml:AuthnContextClassRef>urn:etoegang:core:assurance-class:loa2</saml:Au
                <saml:AuthenticatingAuthority>urn:etoegang:AD:0000000xxxxxxxxx000:entities
            </saml:AuthnContext>
        </saml:AuthnStatement>
        <saml:AttributeStatement>
            <saml:Attribute Name="urn:etoegang:core:ServiceUUID">
                <saml:AttributeValue xsi:type="xs:string">xxxx</saml:AttributeValue>
            </saml:Attribute>
            <saml:EncryptedAttribute xmlns:xenc="http://www.w3.org/2001/04/xmlenc#">
                <xenc:EncryptedData Id="_07151871-ab7d-337d-a4c2-aa6f0c23148d"
                                    Type="http://www.w3.org/2001/04/xmlenc#Element">
                    <xenc:EncryptionMethod Algorithm="http://www.w3.org/2001/04/xmlenc#aes
                    <ds:KeyInfo>
                        <ds:RetrievalMethod Type="http://www.w3.org/2001/04/xmlenc#Encrypte
                                            URI="_xxxxxxxxxxxxxxxxxxxx"/>
                    </ds:KeyInfo>
                    <xenc:CipherData>
                        <xenc:CipherValue>xxxx</xenc:CipherValue>
                    </xenc:CipherData>
                </xenc:EncryptedData>
                <xenc:EncryptedKey Id="_xxxxxxxxxxxxxxxxxxxx"
                                   Recipient="urn:etoegang:DV:0000000xxxxxxxxx000:entities
                    <xenc:EncryptionMethod Algorithm="http://www.w3.org/2001/04/xmlenc#rsa
                        <ds:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"
                    </xenc:EncryptionMethod>
                    <ds:KeyInfo>
                        <ds:KeyName>xxxx</ds:KeyName>
                    </ds:KeyInfo>
                    <xenc:CipherData>
                        <xenc:CipherValue>xxxx</xenc:CipherValue>
                    </xenc:CipherData>
                    <xenc:ReferenceList>
                        <xenc:DataReference URI="_xxxxxxxxxxxxxxxxxxxx"/>
                    </xenc:ReferenceList>
                </xenc:EncryptedKey>
            </saml:EncryptedAttribute>
        </saml:AttributeStatement>
    </saml:Assertion>
</samlp:Response>

```

eH 1.9

```
<samlp:Response xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol" xmlns:ds="http://www.w3
                Version="2.0">
    <saml:Issuer>urn:etoegang:HM:0000000xxxxxxxxx000:entities:xxxx</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-sha25
            <ds:Reference URI="_xxxxxxxxxxxxxxxxxxxx">
                <ds:Transforms>
                    <ds:Transform Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-s
                    <ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#">
                        <ec:InclusiveNamespaces xmlns:ec="http://www.w3.org/2001/10/xml-exc
                    </ds:Transform>
                </ds:Transforms>
                <ds:DigestMethod Algorithm="http://www.w3.org/2001/04/xmlenc#sha256"/>
                <ds:DigestValue>xxxx=</ds:DigestValue>
            </ds:Reference>
        </ds:SignedInfo>
        <ds:SignatureValue>xxxx</ds:SignatureValue>
    </ds:Signature>
    <samlp:Status>
        <samlp:StatusCode Value="urn:oasis:names:tc:SAML:2.0:status:Success"/>
    </samlp:Status>
    <saml:Assertion ID="_xxxxxxxxxxxxxxxxxxxx" IssueInstant="2020-05-28T13:02:33Z" Versio
        <saml:Issuer>urn:etoegang:HM:0000000xxxxxxxxx000:entities:xxxx</saml:Issuer>
        <ds:Signature>
            <ds:SignedInfo>
                <ds:CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-exc-c1
                <ds:SignatureMethod Algorithm="http://www.w3.org/2001/04/xmldsig-more#rsa-
                <ds:Reference URI="_xxxxxxxxxxxxxxxxxxxx">
                    <ds:Transforms>
                        <ds:Transform Algorithm="http://www.w3.org/2000/09/xmldsig#envelope
                        <ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#">
                            <ec:InclusiveNamespaces xmlns:ec="http://www.w3.org/2001/10/xml
                        </ds:Transform>
                    </ds:Transforms>
                    <ds:DigestMethod Algorithm="http://www.w3.org/2001/04/xmlenc#sha256"/>
                    <ds:DigestValue>xxxx=</ds:DigestValue>
                </ds:Reference>
            </ds:SignedInfo>
            <ds:SignatureValue>xxxx</ds:SignatureValue>
        </ds:Signature>
        <saml:Subject>
            <saml:NameID Format="urn:oasis:names:tc:SAML:2.0:nameid-format:persistent" Name
            <saml:SubjectConfirmation Method="urn:oasis:names:tc:SAML:2.0:cm:bearer">
                <saml:SubjectConfirmationData InResponseTo="_xxxxxxxxxxxxxxxxxxxx" NotOnO
                </saml:SubjectConfirmationData>
            </saml:SubjectConfirmation>
        </saml:Subject>
        <saml:Conditions NotBefore="2020-05-28T13:02:33Z" NotOnOrAfter="2020-05-28T13:07:3
            <saml:AudienceRestriction>
                <saml:Audience>urn:etoegang:DV:0000000xxxxxxxxx000:entities:xxxx</saml:Aud
            </saml:AudienceRestriction>
        </saml:Conditions>
        <saml:AuthnStatement AuthnInstant="2020-05-28T13:02:33Z">
            <saml:AuthnContext>
                <saml:AuthnContextClassRef>urn:etoegang:core:assurance-class:loa2plus</sam
                <saml:AuthenticatingAuthority>urn:etoegang:HM:0000000xxxxxxxxx000:entities
            </saml:AuthnContext>
```

```
        </saml:AuthnStatement>
        <saml:AttributeStatement>
            <saml:Attribute Name="urn:etoegang:1.9:EntityConcernedID:KvKnr">
                <saml:AttributeValue xsi:type="xs:string">xxxx</saml:AttributeValue>
            </saml:Attribute>
            <saml:Attribute Name="urn:etoegang:core:ServiceID">
                <saml:AttributeValue xsi:type="xs:string">urn:etoegang:DV:0000000xxxxxxxxx
            </saml:Attribute>
        </saml:AttributeStatement>
    </saml:Assertion>
</samlp:Response>

```

eH Chain authorization

```
<?xml version="1.0" encoding="UTF-8" standalone="no"?>
<samlp:Response
    xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol"
    xmlns:ds="http://www.w3.org/2000/09/xmldsig#"
    xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion"
    xmlns:xs="http://www.w3.org/2001/XMLSchema"
    xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" Destination="xxx" ID="xxx" InResp
    <saml:Issuer>xxx</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-sha2
            <ds:Reference URI="#xxx">
                <ds:Transforms>
                    <ds:Transform Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-s
                    <ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#">
                        <ec:InclusiveNamespaces
                            xmlns:ec="http://www.w3.org/2001/10/xml-exc-c14n#" PrefixList="
                        </ds:Transform>
                    </ds:Transforms>
                    <ds:DigestMethod Algorithm="http://www.w3.org/2001/04/xmlenc#sha256"/>
                    <ds:DigestValue>xxx</ds:DigestValue>
                </ds:Reference>
            </ds:SignedInfo>
            <ds:SignatureValue>xxx
</ds:SignatureValue>
            <ds:KeyInfo>
                <ds:KeyName>xxx</ds:KeyName>
            </ds:KeyInfo>
        </ds:Signature>
        <samlp:Status>
            <samlp:StatusCode Value="urn:oasis:names:tc:SAML:2.0:status:Success"/>
        </samlp:Status>
        <saml:Assertion
            xmlns:xacml-saml="urn:oasis:xacml:2.0:saml:assertion:schema:os" ID="xxx" Issue
            <saml:Issuer>xxx</saml:Issuer>
```

```
            <saml:Subject>
                <saml:NameID Format="urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified"
                <saml:SubjectConfirmation Method="urn:oasis:names:tc:SAML:2.0:cm:bearer">
                    <saml:SubjectConfirmationData InResponseTo="xxx" NotOnOrAfter="2020-05-
                </saml:SubjectConfirmation>
            </saml:Subject>
            <saml:Conditions NotBefore="2020-05-20T12:30:40Z" NotOnOrAfter="2020-05-20T12:3
                <saml:AudienceRestriction>
                    <saml:Audience>xxx</saml:Audience>
                </saml:AudienceRestriction>
            </saml:Conditions>
            <saml:AuthnStatement AuthnInstant="2020-05-20T12:30:40Z">
                <saml:AuthnContext>
                    <saml:AuthnContextClassRef>urn:oasis:names:tc:SAML:2.0:ac:classes:Passw
                    <saml:AuthenticatingAuthority>urn:etoegang:HM:00000003244440010000:ent
                </saml:AuthnContext>
            </saml:AuthnStatement>
            <saml:AttributeStatement>
                <saml:Attribute Name="urn:etoegang:core:ServiceID">
                    <saml:AttributeValue xsi:type="xs:string">urn:etoegang:DV:xxx:services
                </saml:Attribute>
                <saml:Attribute Name="urn:etoegang:core:ServiceUUID">
                    <saml:AttributeValue xsi:type="xs:string">xxx</saml:AttributeValue>
                </saml:Attribute>
                <saml:Attribute Name="urn:etoegang:1.9:EntityConcernedID:KvKnr">
                    <saml:AttributeValue xsi:type="xs:string">11----118</saml:AttributeValu
                </saml:Attribute>
                <saml:Attribute Name="urn:etoegang:1.9:IntermediateEntityID:KvKnr">
                    <saml:AttributeValue xsi:type="xs:string">271---01</saml:AttributeValue
                </saml:Attribute>
                <saml:Attribute FriendlyName="urn:etoegang:1.13:EntityConcernedID:Pseudo" N
                    <saml:AttributeValue xsi:type="xs:string">xxx</saml:AttributeValue>
                </saml:Attribute>
            </saml:AttributeStatement>
        </saml:Assertion>
    </samlp:Response>

```

Connecting to the Connectis eHerkenning Broker (NL)

Met eHerkenning kunnen ondernemers inloggen bij een groot aantal dienstverleners in Nederland

Het eHerkenningnetwerk koppelt ook met eIDAS. eIDAS is een europees systeem dat verschillende nationale inlogsystemen aan elkaar koppelt. Hiermee kan bijvoorbeeld iemand met een Duitse nationaliteit inloggen met zijn Duitse inlogmiddel op een Nederlandse dienst.

In dit document vindt u alle benodigde informatie om de aansluiting van uw dienst op de eHerkenningsmakelaar van Connectis snel en efficiënt te realiseren.

Indien u gebruik maakt van software die al geschikt is om te koppelen met eHerkenning dan kunt u direct

aansluiten. Een aansluiting kan al binnen één werkdag gerealiseerd worden. De gemiddelde doorlooptijd is 2 weken.

Checklist aansluiten

Voorbereiding

Contract

De overeenkomst met Connectis moet ondertekend verzonden worden naar sales@connectis.nl. De realisatie kan niet starten zonder een ondertekende overeenkomst.

Ondertekenen Zelfverklaring

De ondertekende zelfverklaring waarin u instemt op de eisen en afspraken die opgesteld zijn in het afsprakenstelsel (https://afsprakenstelsel.etoegang.nl) kunt u sturen naar technicalsupport@connectis.nl. Dit moet voor alle diensten die aangesloten worden op eHerkenning & eIDAS.

Deze zelfverklaring moet door een bevoegd vertegenwoordiger van de rechtspersoon worden ondertekend.

Applicatie

De applicatie moet geschikt zijn om eIDAS & eHerkenning 1.11 en de door u gewenste functies te ondersteunen. De interface specificaties vindt u op https://afsprakenstelsel.etoegang.nl/display/as/Interface+specifications. Let hierbij op dat de attributen en identificerende kenmerken die u terugkrijgt verschillen bij eHerkenning en eIDAS. Meer informatie over identificerende kenmerken vindt u in het hoofdstuk EntityConcernedTypesAllowed.

Adapter Connectis

Connectis heeft verschillende adapters ontwikkeld die het makkelijker maken om te koppelen met de Connectis Identity Broker. De adapters zijn beschikbaar in Java en .NET. Om een van de adapters (incl. documentatie) te ontvangen, dient u een email te sturen naar uw accountmanager. Er dient hiervoor een EULA getekend te worden.

Voor meer informatie over de Connectis adapters, zie de verschillende secties in API Documentation

---

Aanvragen

PKI Overheid Certificaat
U dient te beschikken over twee PKIoverheid CA 2020 certificaten met minimaal 2048 bits versleuteling (één voor preproductie en één voor productie). Deze worden gebruikt om de eHerkenning-berichten te ondertekenen. Een bestaand PKIO certificaat kan hergebruikt worden.

Besluiten

Diensten en betrouwbaarheidsniveaus

Er dient een besluit genomen te worden over welke diensten aangesloten dienen te worden op eIDAS & eHerkenning. Per dienst is de volgende informatie benodigd:
- Naam
- Omschrijving
- Webpagina
- Betrouwbaarheidsniveau

Connectis kan u ondersteunen bij het bepalen van het benodigde betrouwbaarheidsniveau voor de desbetreffende dienst, de naamgeving en de granulariteit en opbouw van het autorisatiemodel.

Type identificerend kenmerk

Voor eIDAS en eHerkenning kunnen verschillende typen identificerende kenmerken (EntityConcernedTypes) worden teruggestuurd. U kunt aangeven met welk identificerend kenmerk uw dienst kan omgaan door het kiezen van een EntityConcernedTypesAllowed.

Attributen

Attributen kunnen uitgevraagd worden zoals gespecificeerd in de attribuutcatalogus van eIDAS & eHerkenning (https://afsprakenstelsel.etoegang.nl/display/as/Attribuutcatalogus).
Hierbij dient er rekening te worden gehouden dat de levering van deze attributen niet is gegarandeerd binnen eIDAS & eHerkenning: ook gebruikers waarvan de attributen niet worden meegeleverd moeten succesvol kunnen inloggen. Zie RequestedAttributes welke attributen u kunt kiezen.

Realisatie

Stap 1 - Pre-productie

Verstuur SAML metadata pre-productie naar Connectis

SAML metadata is een XML bestand voor het beschrijven van de URL's en certificaten die worden gebruikt op de verschillende koppelvlakken. Het bestand dient gegenereerd te worden met uw software en dient verstuurt te worden naar technicalsupport@connectis.nl. Meer informatie over het maken van metadata vindt u op de volgende pagina: https://afsprakenstelsel.etoegang.nl/display/as/DV+metadata+for+HM

Verstuur eHerkenning dienstencatalogus naar Connectis

eIDAS & eHerkenning Dienstencatalogus is een XML-bestand waarin de diensten gedefinieerd staan die u wilt aanbieden via eIDAS of eHerkenning. Een template hiervoor vindt u verderop in dit document. Connectis verwerkt de metadata en dienstencatalogus in het testnetwerk van eIDAS & eHerkenning.

Verwerk Connectis pre-productie metadata op uw applicatie

U verwerkt het SAML metadata bestand van Connectis. Alle gegevens die nodig zijn om te koppelen met de testomgeving van Connectis staan op https://eh01.connectis.nl/metadata/ onder Metadata Preproductie.

Test de koppeling op pre-productie

U test de koppeling met eHerkenning door hiermee in te loggen via de bij Connectis aangevraagde pre-productie accounts. Het pre-productie account kan worden aangevraagd via https://connectis.com/nl/testmiddel-aanvragen/. Het is in principe niet nodig om met alle verschillende authenticatie diensten te testen; dit is de verantwoordelijkheid van Connectis en de aangesloten authenticatie diensten. Een testmiddel voor een dienst aangesloten op eIDAS kunt u aanvragen via technicalsupport@connectis.nl.
Belangrijk om te weten is dat bij eHerkenning de responses worden teruggestuurd via de zogenaamde SAML Artifact Binding. Dit betekent dat de server van de dienstverlener zelf een connectie moet kunnen opzetten met de Connectis Identity Broker om het response-bericht te kunnen ophalen van de Connectis Identity Broker. Een veelvoorkomend probleem is dat de firewall de webserver van de dienstverlener blokkeert wanneer deze de connectie met de Connectis Identity Broker probeert op te zetten. Dit is iets om in gedachten te houden indien de antwoorden niet correct lijken aan te komen bij uw applicatie.

Stap 2 - Voorbereiding in productiename

Distribueer dienstencatalogus (door Connectis)

Na het met succes doorlopen van de testprocedures dient u toestemming te geven aan Connectis om de dienstencatalogus in het netwerk van eIDAS & eHerkenning te distribueren. Hiermee wordt uw dienst (of diensten) beschikbaar gemaakt voor alle gebruikers binnen eHerkenning.
Let op: Pas na afronding van de distributie kunnen alle gebruikers een machtiging krijgen op uw diensten. Geef daarom tijdig opdracht om de dienstencatalogus te distribueren.

Pas content website aan

U kunt op de website aankondigen dat er met een nieuwe manier van inloggen zal worden gestart. De website kan informatie bevatten over het verkrijgen en het gebruiken van een middel.

Informeer uw (support) collega's over eIDAS/eHerkenning

Uw supportmedewerkers moeten begrijpen wat eIDAS/eHerkenning is en wat het betekent voor uw klanten.

Stap 3 - Productie

Geef datum in productiename door aan Connectis

U geeft aan wanneer Connectis standby moet staan voor het uitvoeren van een release. Connectis reserveert hiervoor capaciteit en zorgt voor een verhoogde dijkbewaking voor de dagen na de in productiename van de verbinding.

Verstuur SAML metadata productie naar Connectis

U genereert de SAML metadata voor Productie en verstuurt dit naar technicalsupport@connectis.nl.

Verwerk Connectis productie metadata op uw applicatie

U verwerkt het SAML metadata bestand van Connectis. Alle gegevens die nodig zijn om te koppelen met de productieomgeving van Connectis staan op https://eh01.connectis.nl/metadata/ onder Metadata Productie.

Na het activeren van de koppeling kan deze direct gebruikt worden door eindgebruikers. Connectis staat standby op het moment van doorvoeren van deze koppeling zodat eventuele problemen snel verholpen kunnen worden.

Communicatie

Eenmaal aangesloten op eHerkenning is het belangrijk dat u uw klanten tijdig voorbereidt op het gebruik van eHerkenning. Zij dienen te weten dat ze op een andere manier moeten gaan inloggen en moeten tijdig een eHerkenning inlogmiddel kunnen aanvragen. Zorg daarom voor goede interne en externe communicatie.

In de Handleiding communicatie eHerkenning zijn een aantal stappen uitgewerkt waarmee u uw communicatie vorm kunt geven. De meest recente Handleiding communicatie vindt u hier: https://www.eherkenning.nl/communicatie

Het beeldmerk, login buttons en betrouwbaarheidsniveaus eHerkenning kunt u hier downloaden: https://bit.ly/2NM9KMH

Beheer

De verbinding wordt onderhouden, ondersteund en verbeterd door Connectis

U heeft recht op preventief en correctief onderhoud, alsmede break-fix support om de continuïteit van haar dienstverlening te waarborgen.

Break-fix support:

Onder break-fix support valt het onderzoeken en oplossen van vermoedelijke verstoringen in de dienstverlening zoals geleverd door Connectis.

Onderhoud

Onder preventief onderhoud valt het continu verbeteren en vernieuwen van de software en infrastructuur, voor zover dat noodzakelijk is om de dienstverlening veilig en stabiel aan u te kunnen leveren. Ook nieuwe verplichte eisen of koppelvlakken binnen eHerkenning worden als onderdeel van preventief onderhoud geïmplementeerd.

Onder correctief onderhoud valt het oplossen van verstoring in de software en infrastructuur.

Dienstencatalogus aanleveren

In een dienstencatalogus staat aangeven welk niveau wordt toegekend aan uw diensten. Het is mogelijk om meerdere diensten op te nemen in deze catalogus op diverse niveau’s. Meer informatie over de DC vindt u

op de volgende pagina: https://afsprakenstelsel.etoegang.nl/display/as/Service+catalog

Om een dienstencatalogus te creëren, dient u de onderstaande informatie te plakken in een tekstbestand en de velden in te vullen.

```
<?xml version="1.0" encoding="UTF-8"?>
<esc:ServiceCatalogue xmlns:esc="urn:etoegang:1.13:service-catalog" xmlns:md="urn:oasis:nar
                      xmlns:ds="http://www.w3.org/2000/09/xmldsig#" xmlns:saml="urn:oasis:n
                      esc:IssueInstant="2019-12-28T10:19:57Z" esc:Version="urn:etoegang:1.1
                      ID="198d678c-239e-43c4-acf7-b4f6f1f6d8c0">
    <esc:ServiceProvider esc:IsPublic="true">
        <esc:ServiceProviderID><!--OIN van organistatie--></esc:ServiceProviderID>
        <esc:OrganizationDisplayName xml:lang="nl"><!--Naam van organistatie--></esc:Organ
        <esc:ServiceDefinition esc:IsPublic="true">
            <esc:ServiceUUID><!--unieke ID genereren via uuidgenerator.net--></esc:ServiceU
            <esc:ServiceName xml:lang="nl"><!--Naam van de Service--></esc:ServiceName>
            <esc:ServiceName xml:lang="en"><!--Naam van de Service--></esc:ServiceName>
            <esc:ServiceDescription xml:lang="nl"><!--Beschrijving van de Service--></esc:S
            <esc:ServiceDescription xml:lang="en"><!--Beschrijving van de Service--></esc:S
            <esc:ServiceDescriptionURL xml:lang="nl">http://example.etoegang.nl</esc:Servic
            <saml:AuthnContextClassRef>urn:etoegang:core:assurance-class:<!--Loa van de Se
            <esc:HerkenningsmakelaarId>00000003244440010000</esc:HerkenningsmakelaarId>
            <esc:EntityConcernedTypesAllowed>urn:etoegang:1.9:EntityConcernedID:KvKnr</esc
              <esc:ServiceRestrictionsAllowed>urn:etoegang:1.9:ServiceRestriction:Vestigin
        </esc:ServiceDefinition>
        <esc:ServiceInstance esc:IsPublic="true">
            <esc:ServiceID>urn:etoegang:DV:<!--OIN -->:services:<!--Service Index--></esc:S
            <esc:ServiceUUID><!--unieke ID genereren via uuidgenerator.net--></esc:ServiceU
            <esc:InstanceOfService><!-- UUID of service definition--></esc:InstanceOfServic
            <esc:ServiceURL xml:lang="nl">vul hier een service url in</esc:ServiceURL>
            <esc:ServiceURL xml:lang="en">vul hier een service url in</esc:ServiceURL>
            <esc:PrivacyPolicyURL xml:lang="nl">vul hier een privacy url in</esc:PrivacyPol
            <esc:PrivacyPolicyURL xml:lang="en">vul hier een privacy url in</esc:PrivacyPol
            <esc:HerkenningsmakelaarId>00000003244440010000</esc:HerkenningsmakelaarId>
            <esc:SSOSupport><!-- a boolean that indicates if the service supports SingleSig
            <esc:ServiceCertificate>
        <md:KeyDescriptor use="encryption">
          <ds:KeyInfo>
            <ds:KeyName>.............</ds:KeyName>
            <ds:X509Data>
              <ds:X509Certificate>.............</ds:X509Certificate>
            </ds:X509Data>
          </ds:KeyInfo>
        </md:KeyDescriptor>
      </esc:ServiceCertificate>
        </esc:ServiceInstance>
    </esc:ServiceProvider>
</esc:ServiceCatalogue>
```

U verstuurt dit bestand naar technicalsupport@connectis.nl. Connectis voert vervolgens uw wijzigingen door in het netwerk van eHerkenning en eIDAS.

Classifier

Met de Classifier koppelt u de dienst aan eHerkenning of eIDAS.

Classifier	Omschrijving
Geen <Classifier> element	De dienst wordt gekoppeld aan eHerkenning
Een <Classifier> element met <Classifier>eIDAS-inbound<Classifier>, zoals in het voorbeeld	De dienst wordt gekoppeld aan eIDAS

EntityConcernedTypesAllowed

Met het veld EntityConcernedTypeAllowed bepaalt u wat voor soort gebruikers mogen inloggen op de dienst. Afhankelijk of de dienst gekoppeld is aan eHerkenning of eIDAS zijn er andere opties beschikbaar.

eHerkenning

In eHerkenning zijn de onderstaande EntityConcernedTypesAllowed beschikbaar.

EntityConcernedTypesAllowed	Omschrijving
EntityConcernedID:RSIN	Wordt gebruikt om een gebruiker te herkenning a/ hand van het Rechtspersonen en Samenwerkingsverbanden Identificatienummer van de vertegenwoordigde dienstafnemer/intermediair
EntityConcernedID:KvKnr	Het KvK nummer van de vertegenwoordigde dienstafnemer/intermediair of vergelijkbaar nummer
ServiceRestriction:Vestigingsnr	Kan alleen gebruikt worden in combinatie met EntityConcernedID:KvKnr. Het vestigingsnummer (nieuwe formaat) van de vertegenwoordigde dienstafnemer

Indien u ServiceRestriction:Vestigingsnr opgeeft als EntityConcernedTypeAllowed veld, dan kunnen gebruikers ook inloggen als zij een restrictie hebben in het machtigingenregister om alleen te maken inloggen op de dienst namens een specifieke vestiging. U moet als dienstverlener deze restrictie

handhaven, hetgeen betekent dat de gebruiker in uw applicatie vervolgens alleen maar mag handelen

eIDAS

EntityConcernedTypesAllowed	Omschrijving
EntityConcernedID:eIDASLegalIdentifier	Een identificerend kenmerk dat wordt gebruikt om een Niet Natuurlijk Persoon bij Herkenning via eIDAS te identificeren binnen Elektronische Toegangsdiensten.
EntityConcernedID:Pseudo	Wordt gebruikt om een consument te identificeren binnen eIDAS.

RequestedAttributes

Met Requested Attributes is het mogelijk om extra gegevens op te vragen van de gebruikers die gebruik maken van uw dienst. U kunt hier optioneel gebruik van maken. Voor eHerkenning is echter aflevering van deze attributen niet gegarandeerd. Bij eIDAS krijgt u de Requested Attributes wel altijd terug in de respons indien dit z.g. verplichte attributen zijn. De optionele attributen levert eIDAS terug als deze bekend zijn voor de desbetreffende gebruiker.

Zie de Attribuutcatalogus op het Afsprakenstelsel voor meer informatie:

- Attribuutcatalogus natuurlijke personen
- Attributencatalogus niet-natuurlijke personen
- Attribuutcatalogus generiek

```
<esc:EntityConcernedTypesAllowed>urn:etoegang:1.9:EntityConcernedID:Pseudo</esc:EntityConc
  <esc:RequestedAttribute Name="urn:etoegang:1.9:attribute:FirstName" isRequired="true">
     <esc:PurposeStatement xml:lang="en">For testing purposes.</esc:PurposeStatement>
     <esc:PurposeStatement xml:lang="nl">Voor testdoeleinden.</esc:PurposeStatement>
  </esc:RequestedAttribute>
  <esc:RequestedAttribute Name="urn:etoegang:1.9:attribute:FamilyName" isRequired="true">
     <esc:PurposeStatement xml:lang="en">For testing purposes.</esc:PurposeStatement>
     <esc:PurposeStatement xml:lang="nl">Voor testdoeleinden.</esc:PurposeStatement>
  </esc:RequestedAttribute>
  <esc:RequestedAttribute Name="urn:etoegang:1.9:attribute:DateOfBirth" isRequired="true">
     <esc:PurposeStatement xml:lang="en">For testing purposes.</esc:PurposeStatement>
     <esc:PurposeStatement xml:lang="nl">Voor testdoeleinden.</esc:PurposeStatement>
  </esc:RequestedAttribute>

```

Voorbeeldberichten

SAML Authn Request

eH 1.13

```
<S11:Envelope xmlns:S11="http://schemas.xmlsoap.org/soap/envelope/">
    <S11:Body>
        <samlp:ArtifactResponse xmlns="urn:oasis:names:tc:SAML:2.0:assertion"
            xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol" ID="xxx" InResponseTo="xxx"
            <Issuer>urn:etoegang:DV:xxx:entities:0098</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
                    <ds:SignatureMethod Algorithm="http://www.w3.org/2001/04/xmldsig-more#
                    <ds:Reference URI="#xxx">
                        <ds:Transforms>
                            <ds:Transform Algorithm="http://www.w3.org/2000/09/xmldsig#enve
                            <ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n
                                <ec:InclusiveNamespaces xmlns:ec="http://www.w3.org/2001/10
                            </ds:Transform>
                        </ds:Transforms>
                        <ds:DigestMethod Algorithm="http://www.w3.org/2001/04/xmlenc#sha256
                        <ds:DigestValue>xxx</ds:DigestValue>
                    </ds:Reference>
                </ds:SignedInfo>
                <ds:SignatureValue>xxx
                </ds:SignatureValue>
                <ds:KeyInfo>
                    <ds:KeyName>xxx</ds:KeyName>
                </ds:KeyInfo>
            </ds:Signature>
            <samlp:Status>
                <samlp:StatusCode Value="urn:oasis:names:tc:SAML:2.0:status:Success"/>
            </samlp:Status>
            <samlp:AuthnRequest xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion" Assertio
                <saml:Issuer>urn:etoegang:DV:xxx:entities:0098</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
                        <ds:SignatureMethod Algorithm="http://www.w3.org/2001/04/xmldsig-mo
                        <ds:Reference URI="#_xxx">
                            <ds:Transforms>
                                <ds:Transform Algorithm="http://www.w3.org/2000/09/xmldsig#
                                <ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-
                                    <ec:InclusiveNamespaces xmlns:ec="http://www.w3.org/200
                                </ds:Transform>
                            </ds:Transforms>
                            <ds:DigestMethod Algorithm="http://www.w3.org/2001/04/xmlenc#sh
                            <ds:DigestValue>xxx</ds:DigestValue>
                        </ds:Reference>
                    </ds:SignedInfo>
```

```
                    <ds:SignatureValue>xxx
                    </ds:SignatureValue>
                    <ds:KeyInfo>
                        <ds:KeyName>xxx</ds:KeyName>
                    </ds:KeyInfo>
                </ds:Signature>
                <samlp:RequestedAuthnContext Comparison="minimum">
                    <saml:AuthnContextClassRef>urn:etoegang:core:assurance-class:loa3</sam
                </samlp:RequestedAuthnContext>
            </samlp:AuthnRequest>
        </samlp:ArtifactResponse>
    </S11:Body>
</S11:Envelope>
```

eH 1.11 (eIDAS)

```
<samlp:AuthnRequest xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol"
                    xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion"
                    ForceAuthn="True"
                    AssertionConsumerServiceURL="https://forms.xxxxx.nl/acs"
                    AttributeConsumingServiceIndex="3"
                    Destination="https://eh01.staging.connectis.nl/broker/sso/1.11"
                    ID="_xxxxxxxxxxxxxxxxxxxx"
                    IssueInstant="2020-05-29T06:59:51.9038041Z"
                    Version="2.0">
    <saml:Issuer>urn:etoegang:DV:0000000xxxxxxxxx000:entities:xxxx</saml:Issuer>
    <samlp:RequestedAuthnContext Comparison="minimum">
        <saml:AuthnContextClassRef>urn:etoegang:core:assurance-class:loa2</saml:AuthnContex
    </samlp:RequestedAuthnContext>
    <Signature xmlns="http://www.w3.org/2000/09/xmldsig#">xxxxx</Signature>
</samlp:AuthnRequest>
```

eH 1.9

```
<samlp:AuthnRequest xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol"
                    xmlns="urn:oasis:names:tc:SAML:2.0:assertion" AssertionConsumerServiceU
    <saml:Issuer xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion">urn:etoegang:DV:000000
    <dsig:Signature xmlns:dsig="http://www.w3.org/2000/09/xmldsig#">
        <dsig:SignedInfo>
            <dsig:CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-exc-c14n
            <dsig:SignatureMethod Algorithm="http://www.w3.org/2001/04/xmldsig-more#rsa-sha
            <dsig:Reference URI="_xxxxxxxxxxxxxxxxxxxx">
                <dsig:Transforms>
                    <dsig:Transform Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-
                    <dsig:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>
                </dsig:Transforms>
                <dsig:DigestMethod Algorithm="http://www.w3.org/2001/04/xmlenc#sha256"/>
                <dsig:DigestValue>xxxx=</dsig:DigestValue>
            </dsig:Reference>
```

```
        </dsig:SignedInfo>
        <dsig:SignatureValue>xxxx</dsig:SignatureValue>
        <dsig:KeyInfo>
            <dsig:KeyValue>
                <dsig:RSAKeyValue>
                    <dsig:Modulus>xxxx</dsig:Modulus>
                    <dsig:Exponent>xxxx</dsig:Exponent>
                </dsig:RSAKeyValue>
            </dsig:KeyValue>

        </dsig:KeyInfo>
    </dsig:Signature>
    <samlp:NameIDPolicy AllowCreate="true" Format="urn:oasis:names:tc:SAML:2.0:nameid-forma
    <samlp:RequestedAuthnContext Comparison="minimum">
        <saml:AuthnContextClassRef xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion">urn:e
    </samlp:RequestedAuthnContext>
</samlp:AuthnRequest>
```

eH Ketenmachtiging

```
<?xml version="1.0" encoding="UTF-8" standalone="no"?><md:EntityDescriptor xmlns:md="urn:oa
<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="#_a311f029-0cbd-4508-b56b-62eeca738ce4">
<ds:Transforms>
<ds:Transform Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature"/>
<ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#">
<ec:InclusiveNamespaces xmlns:ec="http://www.w3.org/2001/10/xml-exc-c14n#" PrefixList="xacm
</ds:Transform>
</ds:Transforms>
<ds:DigestMethod Algorithm="http://www.w3.org/2001/04/xmlenc#sha256"/>
<ds:DigestValue>ntI/CmN+1HBtiGPeLU84V8A5rNhjfhyYfvoUTyTCYeM=</ds:DigestValue>
</ds:Reference>
</ds:SignedInfo>
```

SAML Response

eH 1.13

```
<samlp:ArtifactResponse xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol"
    xmlns="urn:oasis:names:tc:SAML:2.0:assertion" ID="xxx" InResponseTo="xxx" IssueInstant=
    <Issuer>urn:etoegang:HM:00000003244440010000:entities:1135</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-sha25
```

```
            <ds:Reference URI="#xxx">
                <ds:Transforms>
                    <ds:Transform Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-s
                    <ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#">
                        <ec:InclusiveNamespaces xmlns:ec="http://www.w3.org/2001/10/xml-exc
                    </ds:Transform>
                </ds:Transforms>
                <ds:DigestMethod Algorithm="http://www.w3.org/2001/04/xmlenc#sha256"/>
                <ds:DigestValue>xxx</ds:DigestValue>

            </ds:Reference>
        </ds:SignedInfo>
        <ds:SignatureValue>xxx
        </ds:SignatureValue>
        <ds:KeyInfo>
            <ds:KeyName>xxx</ds:KeyName>
        </ds:KeyInfo>
    </ds:Signature>
    <samlp:Status>
        <samlp:StatusCode Value="urn:oasis:names:tc:SAML:2.0:status:Success"/>
    </samlp:Status>
    <samlp:Response xmlns:ds="http://www.w3.org/2000/09/xmldsig#"
        xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion"
        xmlns:xs="http://www.w3.org/2001/XMLSchema"
        xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" Destination="xxx" ID="xxx" I
        <saml:Issuer>urn:etoegang:HM:00000003244440010000:entities:1135</saml:Issuer>
        <ds:Signature>
            <ds:SignedInfo>
                <ds:CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-exc-c1
                <ds:SignatureMethod Algorithm="http://www.w3.org/2001/04/xmldsig-more#rsa-
                <ds:Reference URI="#xxx">
                    <ds:Transforms>
                        <ds:Transform Algorithm="http://www.w3.org/2000/09/xmldsig#envelope
                        <ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#">
                            <ec:InclusiveNamespaces xmlns:ec="http://www.w3.org/2001/10/xml
                        </ds:Transform>
                    </ds:Transforms>
                    <ds:DigestMethod Algorithm="http://www.w3.org/2001/04/xmlenc#sha256"/>
                    <ds:DigestValue>xxx</ds:DigestValue>
                </ds:Reference>
            </ds:SignedInfo>
            <ds:SignatureValue>xxx
            </ds:SignatureValue>
            <ds:KeyInfo>
                <ds:KeyName>xxx</ds:KeyName>
            </ds:KeyInfo>
        </ds:Signature>
        <samlp:Status>
            <samlp:StatusCode Value="urn:oasis:names:tc:SAML:2.0:status:Success"/>
        </samlp:Status>
        <saml:Assertion xmlns:xacml-saml="urn:oasis:xacml:2.0:saml:assertion:schema:os" ID=
            <saml:Issuer>urn:etoegang:HM:00000003244440010000:entities:1135</saml:Issuer>
            <ds:Signature>
                <ds:SignedInfo>
```

```
                    <ds:CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-exc
                    <ds:SignatureMethod Algorithm="http://www.w3.org/2001/04/xmldsig-more#
                    <ds:Reference URI="#xxx">
                        <ds:Transforms>
                            <ds:Transform Algorithm="http://www.w3.org/2000/09/xmldsig#enve
                            <ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n
                                <ec:InclusiveNamespaces xmlns:ec="http://www.w3.org/2001/10
                            </ds:Transform>
                        </ds:Transforms>

                        <ds:DigestMethod Algorithm="http://www.w3.org/2001/04/xmlenc#sha256
                        <ds:DigestValue>xxx</ds:DigestValue>
                    </ds:Reference>
                </ds:SignedInfo>
                <ds:SignatureValue>xxx
                </ds:SignatureValue>
                <ds:KeyInfo>
                    <ds:KeyName>xxx</ds:KeyName>
                </ds:KeyInfo>
            </ds:Signature>
            <saml:Subject>
                <saml:NameID Format="urn:oasis:names:tc:SAML:2.0:nameid-format:transient" N
                <saml:SubjectConfirmation Method="urn:oasis:names:tc:SAML:2.0:cm:bearer">
                    <saml:SubjectConfirmationData InResponseTo="xxx" NotOnOrAfter="2020-05-
                    </saml:SubjectConfirmationData>
                </saml:SubjectConfirmation>
            </saml:Subject>
            <saml:Conditions NotBefore="2020-05-28T12:42:03Z" NotOnOrAfter="2020-05-28T12:4
                <saml:AudienceRestriction>
                    <saml:Audience>urn:etoegang:DV:xxx:entities:0098</saml:Audience>
                </saml:AudienceRestriction>
            </saml:Conditions>
            <saml:Advice>
                <saml:Assertion ID="xxx" IssueInstant="2020-05-28T12:42:02Z" Version="2.0"
                    <saml:Issuer>urn:etoegang:AD:00000003341423870000:entities:0113</saml:I
                    <ds:Signature>
                        <ds:SignedInfo>
                            <ds:CanonicalizationMethod Algorithm="http://www.w3.org/2001/10
                            <ds:SignatureMethod Algorithm="http://www.w3.org/2001/04/xmldsi
                            <ds:Reference URI="#xxx">
                                <ds:Transforms>
                                    <ds:Transform Algorithm="http://www.w3.org/2000/09/xmld
                                    <ds:Transform Algorithm="http://www.w3.org/2001/10/xml-
                                </ds:Transforms>
                                <ds:DigestMethod Algorithm="http://www.w3.org/2001/04/xmlen
                                <ds:DigestValue>xxx</ds:DigestValue>
                            </ds:Reference>
                        </ds:SignedInfo>
                        <ds:SignatureValue>xxx
                        </ds:SignatureValue>
                        <ds:KeyInfo>
                            <ds:KeyName>xxx</ds:KeyName>
                        </ds:KeyInfo>
```

```
                </ds:Signature>
                <saml:Subject>
                    <saml:NameID Format="urn:oasis:names:tc:SAML:2.0:nameid-format:tra
                    <saml:SubjectConfirmation Method="urn:oasis:names:tc:SAML:2.0:cm:be
                        <saml:SubjectConfirmationData InResponseTo="xxx" NotOnOrAfter="
                    </saml:SubjectConfirmation>
                </saml:Subject>
                <saml:Conditions NotBefore="2020-05-28T12:32:02Z" NotOnOrAfter="2020-05
                    <saml:AudienceRestriction>
                        <saml:Audience>urn:etoegang:HM:00000003244440010000:entities:1
                        <saml:Audience>urn:etoegang:DV:xxx:entities:0098</saml:Audience
                        <saml:Audience>urn:etoegang:MR:00000003341423870000:entities:0
                    </saml:AudienceRestriction>
                </saml:Conditions>
                <saml:AuthnStatement AuthnInstant="2020-05-28T12:42:01Z">
                    <saml:AuthnContext>
                        <saml:AuthnContextClassRef>urn:etoegang:core:assurance-class:lo
                        <saml:AuthenticatingAuthority>00000003341423870000</saml:Authen
                    </saml:AuthnContext>
                </saml:AuthnStatement>
                <saml:AttributeStatement>
                    <saml:Attribute Name="urn:etoegang:core:Representation">
                        <saml:AttributeValue xsi:type="xs:boolean">true</saml:Attribute
                    </saml:Attribute>
                    <saml:Attribute Name="urn:etoegang:core:ServiceUUID">
                        <saml:AttributeValue xsi:type="xs:string">xxx</saml:AttributeVa
                    </saml:Attribute>
                    <saml:Attribute Name="urn:etoegang:core:AuthorizationRegistryID">
                        <saml:AttributeValue xsi:type="xs:string">urn:etoegang:MR:0000
                    </saml:Attribute>
                    <saml:Attribute Name="urn:etoegang:core:ActingSubjectID">
                        <saml:AttributeValue>
                            <saml:EncryptedID>
                                <xenc:EncryptedData xmlns:xenc="http://www.w3.org/2001/
                                    <xenc:EncryptionMethod Algorithm="http://www.w3.org
                                    <ds:KeyInfo>
                                        <ds:RetrievalMethod Type="http://www.w3.org/200
                                    </ds:KeyInfo>
                                    <xenc:CipherData>
                                        <xenc:CipherValue>xxx=</xenc:CipherValue>
                                    </xenc:CipherData>
                                </xenc:EncryptedData>
                                <xenc:EncryptedKey xmlns:xenc="http://www.w3.org/2001/0
                                    <xenc:EncryptionMethod Algorithm="http://www.w3.org
                                        <ds:DigestMethod Algorithm="http://www.w3.org/2
                                    </xenc:EncryptionMethod>
                                    <ds:KeyInfo>
                                        <ds:KeyName>xxx</ds:KeyName>
                                    </ds:KeyInfo>
                                    <xenc:CipherData>
                                        <xenc:CipherValue>xxx</xenc:CipherValue>
                                    </xenc:CipherData>
                                    <xenc:ReferenceList>
```

```
                                    <xenc:DataReference URI="#xxx"/>
                                </xenc:ReferenceList>
                            </xenc:EncryptedKey>
                        </saml:EncryptedID>
                    </saml:AttributeValue>
                </saml:Attribute>
            </saml:AttributeStatement>
        </saml:Assertion>
        <saml2:Assertion xmlns:saml2="urn:oasis:names:tc:SAML:2.0:assertion" ID="xx
            <saml2:Issuer>urn:etoegang:MR:00000003341423870000:entities:0113</saml2
            <ds:Signature>
                <ds:SignedInfo>
                    <ds:CanonicalizationMethod Algorithm="http://www.w3.org/2001/10
                    <ds:SignatureMethod Algorithm="http://www.w3.org/2001/04/xmlds
                    <ds:Reference URI="#xxx">
                        <ds:Transforms>
                            <ds:Transform Algorithm="http://www.w3.org/2000/09/xmlc
                            <ds:Transform Algorithm="http://www.w3.org/2001/10/xml-
                                <ec:InclusiveNamespaces xmlns:ec="http://www.w3.org
                            </ds:Transform>
                        </ds:Transforms>
                        <ds:DigestMethod Algorithm="http://www.w3.org/2001/04/xmlen
                        <ds:DigestValue>xxx</ds:DigestValue>
                    </ds:Reference>
                </ds:SignedInfo>
                <ds:SignatureValue>xxx</ds:SignatureValue>
                <ds:KeyInfo>
                    <ds:KeyName>xxx</ds:KeyName>
                </ds:KeyInfo>
            </ds:Signature>
            <saml2:Subject>
                <saml2:NameID Format="urn:oasis:names:tc:SAML:2.0:nameid-format:tra
            </saml2:Subject>
            <saml2:Conditions NotBefore="2020-05-28T12:42:03Z" NotOnOrAfter="2020-0
            <saml2:Advice>
                <saml2:AssertionIDRef>xxx</saml2:AssertionIDRef>
            </saml2:Advice>
            <saml2:Statement xsi:type="xacml-saml:XACMLAuthzDecisionStatementType">
                <xacml-context:Response xmlns:xacml-context="urn:oasis:names:tc:xac
                    <xacml-context:Result>
                        <xacml-context:Decision>Permit</xacml-context:Decision>
                        <xacml-context:Status>
                            <xacml-context:StatusCode Value="urn:oasis:names:tc:xac
                        </xacml-context:Status>
                    </xacml-context:Result>
                </xacml-context:Response>
                <xacml-context:Request xmlns:xacml-context="urn:oasis:names:tc:xacm
                    <xacml-context:Subject SubjectCategory="urn:oasis:names:tc:xacm
                        <xacml-context:Attribute AttributeId="urn:etoegang:core:Act
                            <xacml-context:AttributeValue>xxx</xacml-context:Attrib
                        </xacml-context:Attribute>
                        <xacml-context:Attribute AttributeId="urn:etoegang:core:Act
                            <xacml-context:AttributeValue>
```

```
                                <saml2:EncryptedID>
                                    <xenc:EncryptedData xmlns:xenc="http://www.w3.o
                                        <xenc:EncryptionMethod Algorithm="http://w
                                        <ds:KeyInfo>
                                            <ds:RetrievalMethod Type="http://www.w3
                                        </ds:KeyInfo>
                                        <xenc:CipherData>
                                            <xenc:CipherValue>xxx</xenc:CipherValue
                                        </xenc:CipherData>
                                    </xenc:EncryptedData>
                                    <xenc:EncryptedKey xmlns:xenc="http://www.w3.o
                                        <xenc:EncryptionMethod Algorithm="http://w
                                            <ds:DigestMethod Algorithm="http://www
                                        </xenc:EncryptionMethod>
                                        <ds:KeyInfo>
                                            <ds:KeyName>xxx</ds:KeyName>
                                        </ds:KeyInfo>
                                        <xenc:CipherData>
                                            <xenc:CipherValue>xxx</xenc:CipherValue
                                        </xenc:CipherData>
                                        <xenc:ReferenceList>
                                            <xenc:DataReference URI="#xxx"/>
                                        </xenc:ReferenceList>
                                    </xenc:EncryptedKey>
                                </saml2:EncryptedID>
                            </xacml-context:AttributeValue>
                        </xacml-context:Attribute>
                        <xacml-context:Attribute AttributeId="urn:etoegang:core:Lin
                            <xacml-context:AttributeValue>xxx</xacml-context:Attrib
                        </xacml-context:Attribute>
                        <xacml-context:Attribute AttributeId="urn:etoegang:core:Leg
                            <xacml-context:AttributeValue>
                                <saml2:EncryptedID>
                                    <xenc:EncryptedData xmlns:xenc="http://www.w3.o
                                        <xenc:EncryptionMethod Algorithm="http://w
                                        <ds:KeyInfo>
                                            <ds:RetrievalMethod Type="http://www.w3
                                        </ds:KeyInfo>
                                        <xenc:CipherData>
                                            <xenc:CipherValue>xxx</xenc:CipherValue
                                        </xenc:CipherData>
                                    </xenc:EncryptedData>
                                    <xenc:EncryptedKey xmlns:xenc="http://www.w3.o
                                        <xenc:EncryptionMethod Algorithm="http://w
                                            <ds:DigestMethod Algorithm="http://www
                                        </xenc:EncryptionMethod>
                                        <ds:KeyInfo>
                                            <ds:KeyName>xxx</ds:KeyName>
                                        </ds:KeyInfo>
                                        <xenc:CipherData>
                                            <xenc:CipherValue>xxx</xenc:CipherValue
                                        </xenc:CipherData>
                                        <xenc:ReferenceList>
```

```
                                        <xenc:DataReference URI="#_xxx"/>
                                    </xenc:ReferenceList>
                                </xenc:EncryptedKey>
                            </saml2:EncryptedID>
                        </xacml-context:AttributeValue>
                    </xacml-context:Attribute>
                </xacml-context:Subject>
                <xacml-context:Resource>
                    <xacml-context:ResourceContent>
                        <saml2:EncryptedAttribute>
                            <xenc:EncryptedData xmlns:xenc="http://www.w3.org/
                                <xenc:EncryptionMethod Algorithm="http://www.w
                                <ds:KeyInfo>
                                    <ds:RetrievalMethod Type="http://www.w3.org
                                </ds:KeyInfo>
                                <xenc:CipherData>
                                    <xenc:CipherValue>xxx</xenc:CipherValue>
                                </xenc:CipherData>
                            </xenc:EncryptedData>
                            <xenc:EncryptedKey xmlns:xenc="http://www.w3.org/2
                                <xenc:EncryptionMethod Algorithm="http://www.w
                                    <ds:DigestMethod Algorithm="http://www.w3.
                                </xenc:EncryptionMethod>
                                <ds:KeyInfo>
                                    <ds:KeyName>xxx</ds:KeyName>
                                </ds:KeyInfo>
                                <xenc:CipherData>
                                    <xenc:CipherValue>xxx</xenc:CipherValue>
                                </xenc:CipherData>
                                <xenc:ReferenceList>
                                    <xenc:DataReference URI="#encrypted_urn_et
                                </xenc:ReferenceList>
                            </xenc:EncryptedKey>
                        </saml2:EncryptedAttribute>
                    </xacml-context:ResourceContent>
                    <xacml-context:Attribute AttributeId="urn:etoegang:core:Le
                        <xacml-context:AttributeValue>urn:etoegang:core:assura
                    </xacml-context:Attribute>
                    <xacml-context:Attribute AttributeId="urn:etoegang:core:Se
                        <xacml-context:AttributeValue>urn:etoegang:DV:xxx:serv
                    </xacml-context:Attribute>
                    <xacml-context:Attribute AttributeId="urn:etoegang:core:Se
                        <xacml-context:AttributeValue>xxx</xacml-context:Attri
                    </xacml-context:Attribute>
                    <xacml-context:Attribute AttributeId="urn:etoegang:1.9:Ent
                        <xacml-context:AttributeValue>xxx</xacml-context:Attri
                    </xacml-context:Attribute>
                    <xacml-context:Attribute AttributeId="urn:etoegang:core:Le
                        <xacml-context:AttributeValue>urn:etoegang:core:assura
                    </xacml-context:Attribute>
                </xacml-context:Resource>
                <xacml-context:Action>
                    <xacml-context:Attribute AttributeId="urn:oasis:names:tc:x
```

```
                                <xacml-context:AttributeValue>Authenticate</xacml-conte
                            </xacml-context:Attribute>
                        </xacml-context:Action>
                        <xacml-context:Environment/>
                    </xacml-context:Request>
                </saml2:Statement>
            </saml2:Assertion>
        </saml:Advice>
        <saml:AuthnStatement AuthnInstant="2020-05-28T12:42:03Z">
            <saml:AuthnContext>

                <saml:AuthnContextClassRef>urn:etoegang:core:assurance-class:loa3</saml
                <saml:AuthenticatingAuthority>urn:etoegang:AD:00000003341423870000:ent
            </saml:AuthnContext>
        </saml:AuthnStatement>
        <saml:AttributeStatement>
            <saml:Attribute Name="urn:etoegang:core:ServiceUUID">
                <saml:AttributeValue xsi:type="xs:string">xxx</saml:AttributeValue>
            </saml:Attribute>
            <saml:Attribute Name="urn:etoegang:core:ActingSubjectID">
                <saml:AttributeValue>
                    <saml:EncryptedID xmlns:xenc="http://www.w3.org/2001/04/xmlenc#">
                        <xenc:EncryptedData Id="_xxx" Type="http://www.w3.org/2001/04/x
                            <xenc:EncryptionMethod Algorithm="http://www.w3.org/2001/04
                            <ds:KeyInfo>
                                <ds:RetrievalMethod Type="http://www.w3.org/2001/04/xm
                            </ds:KeyInfo>
                            <xenc:CipherData>
                                <xenc:CipherValue>xxx</xenc:CipherValue>
                            </xenc:CipherData>
                        </xenc:EncryptedData>
                        <xenc:EncryptedKey Id="xxx" Recipient="urn:etoegang:DV:xxx:ent
                            <xenc:EncryptionMethod Algorithm="http://www.w3.org/2001/04
                                <ds:DigestMethod Algorithm="http://www.w3.org/2000/09/x
                            </xenc:EncryptionMethod>
                            <ds:KeyInfo>
                                <ds:KeyName>xxx</ds:KeyName>
                            </ds:KeyInfo>
                            <xenc:CipherData>
                                <xenc:CipherValue>xxx</xenc:CipherValue>
                            </xenc:CipherData>
                            <xenc:ReferenceList>
                                <xenc:DataReference URI="#_xxx"/>
                            </xenc:ReferenceList>
                        </xenc:EncryptedKey>
                    </saml:EncryptedID>
                </saml:AttributeValue>
            </saml:Attribute>
            <saml:Attribute Name="urn:etoegang:core:LegalSubjectID">
                <saml:AttributeValue>
                    <saml:EncryptedID xmlns:xenc="http://www.w3.org/2001/04/xmlenc#">
                        <xenc:EncryptedData Id="_xxx" Type="http://www.w3.org/2001/04/x
                            <xenc:EncryptionMethod Algorithm="http://www.w3.org/2001/04
```

```
                                <ds:KeyInfo>
                                    <ds:RetrievalMethod Type="http://www.w3.org/2001/04/xm
                                </ds:KeyInfo>
                                <xenc:CipherData>
                                    <xenc:CipherValue>xxx</xenc:CipherValue>
                                </xenc:CipherData>
                            </xenc:EncryptedData>
                            <xenc:EncryptedKey Id="_xxx" Recipient="urn:etoegang:DV:xxx:en
                                <xenc:EncryptionMethod Algorithm="http://www.w3.org/2001/04
                                    <ds:DigestMethod Algorithm="http://www.w3.org/2000/09/x
                                </xenc:EncryptionMethod>

                                <ds:KeyInfo>
                                    <ds:KeyName>xxx</ds:KeyName>
                                </ds:KeyInfo>
                                <xenc:CipherData>
                                    <xenc:CipherValue>xxx</xenc:CipherValue>
                                </xenc:CipherData>
                                <xenc:ReferenceList>
                                    <xenc:DataReference URI="#_xxx"/>
                                </xenc:ReferenceList>
                            </xenc:EncryptedKey>
                        </saml:EncryptedID>
                    </saml:AttributeValue>
                </saml:Attribute>
                <saml:Attribute Name="urn:etoegang:core:ServiceID">
                    <saml:AttributeValue xsi:type="xs:string">urn:etoegang:DV:xxx:services
                </saml:Attribute>
                <saml:EncryptedAttribute xmlns:xenc="http://www.w3.org/2001/04/xmlenc#">
                    <xenc:EncryptedData Id="_xxx" Type="http://www.w3.org/2001/04/xmlenc#E
                        <xenc:EncryptionMethod Algorithm="http://www.w3.org/2001/04/xmlenc
                        <ds:KeyInfo>
                            <ds:RetrievalMethod Type="http://www.w3.org/2001/04/xmlenc#Enc
                        </ds:KeyInfo>
                        <xenc:CipherData>
                            <xenc:CipherValue>xxx</xenc:CipherValue>
                        </xenc:CipherData>
                    </xenc:EncryptedData>
                    <xenc:EncryptedKey Id="_xxx" Recipient="urn:etoegang:DV:xxx:entities:0
                        <xenc:EncryptionMethod Algorithm="http://www.w3.org/2001/04/xmlenc
                            <ds:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#s
                        </xenc:EncryptionMethod>
                        <ds:KeyInfo>
                            <ds:KeyName>xxx</ds:KeyName>
                        </ds:KeyInfo>
                        <xenc:CipherData>
                            <xenc:CipherValue>xxx</xenc:CipherValue>
                        </xenc:CipherData>
                        <xenc:ReferenceList>
                            <xenc:DataReference URI="#_xxx"/>
                        </xenc:ReferenceList>
                    </xenc:EncryptedKey>
                </saml:EncryptedAttribute>
            </saml:AttributeStatement>
```

```
        </saml:Assertion>
    </samlp:Response>
</samlp:ArtifactResponse>
```

eH 1.11 (eIDAS)

```
<samlp:Response xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol"
                xmlns:ds="http://www.w3.org/2000/09/xmldsig#"
                xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion"
                xmlns:xs="http://www.w3.org/2001/XMLSchema"
                xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
                Destination="https://forms.toverijs7.nl/acs"
                ID="_xxxxxxxxxxxxxxxxxxxx"
                InResponseTo="_xxxxxxxxxxxxxxxxxxxx"
                IssueInstant="2020-05-29T07:00:13Z"
                Version="2.0">
    <saml:Issuer>urn:etoegang:HM:0000000xxxxxxxxx000:entities:xxxx</saml:Issuer>
    <ds:Signature>xxxx</ds:Signature>
    <samlp:Status>
        <samlp:StatusCode Value="urn:oasis:names:tc:SAML:2.0:status:Success"/>
    </samlp:Status>
    <saml:Assertion
            ID="_xxxxxxxxxxxxxxxxxxxx"
            IssueInstant="2020-05-29T07:00:13Z"
            Version="2.0">
        <saml:Issuer>urn:etoegang:HM:0000000xxxxxxxxx000:entities:xxxx</saml:Issuer>
        <ds:Signature>xxxx</ds:Signature>
        <saml:Subject>
            <saml:EncryptedID xmlns:xenc="http://www.w3.org/2001/04/xmlenc#">
                <xenc:EncryptedData Id="_xxxxxxxxxxxxxxxxxxxx"
                                    Type="http://www.w3.org/2001/04/xmlenc#Element">
                    <xenc:EncryptionMethod Algorithm="http://www.w3.org/2001/04/xmlenc#aes
                    <ds:KeyInfo>
                        <ds:RetrievalMethod Type="http://www.w3.org/2001/04/xmlenc#Encrypte
                                            URI="#_xxxxxxxxxxxxxxxxxxxx"/>
                    </ds:KeyInfo>
                    <xenc:CipherData>
                        <xenc:CipherValue>xxxx</xenc:CipherValue>
                    </xenc:CipherData>
                </xenc:EncryptedData>
                <xenc:EncryptedKey Id="_xxxxxxxxxxxxxxxxxxxx"
                                   Recipient="urn:etoegang:DV:0000000xxxxxxxxx000:entities
                    <xenc:EncryptionMethod Algorithm="http://www.w3.org/2001/04/xmlenc#rsa-
                        <ds:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"
                    </xenc:EncryptionMethod>
                    <ds:KeyInfo>
                        <ds:KeyName>xxxx</ds:KeyName>
                    </ds:KeyInfo>
                    <xenc:CipherData>
                        <xenc:CipherValue>xxxx</xenc:CipherValue>
                    </xenc:CipherData>
```

```
                    <xenc:ReferenceList>
                        <xenc:DataReference URI="_xxxxxxxxxxxxxxxxxxx"/>
                    </xenc:ReferenceList>
                </xenc:EncryptedKey>
            </saml:EncryptedID>
            <saml:SubjectConfirmation Method="urn:oasis:names:tc:SAML:2.0:cm:bearer">
                <saml:SubjectConfirmationData InResponseTo="_xxxxxxxxxxxxxxxxxxx"
                                              NotOnOrAfter="2020-05-29T07:05:13Z"
                                              Recipient="https://forms.xxxxxx.nl/acs"/>
            </saml:SubjectConfirmation>
        </saml:Subject>
        <saml:Conditions NotBefore="2020-05-29T07:00:13Z"
                         NotOnOrAfter="2020-05-29T07:05:13Z">
            <saml:AudienceRestriction>
                <saml:Audience>urn:etoegang:DV:0000000xxxxxxxxx000:entities:xxxx</saml:Aud
            </saml:AudienceRestriction>
        </saml:Conditions>
        <saml:Advice>
            <saml:Assertion ID="sxxxxxxxxxxxxxxxxxxxx"
                            IssueInstant="2020-05-29T07:00:12Z"
                            Version="2.0">
                <saml:Issuer>urn:etoegang:DV:0000000xxxxxxxxx000:entities:xxxx</saml:Issue
                <ds:Signature>
                    <ds:SignedInfo>
                        <ds:CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xm
                        <ds:SignatureMethod Algorithm="http://www.w3.org/2001/04/xmldsig-m
                        <ds:Reference URI="_xxxxxxxxxxxxxxxxxxxx">
                            <ds:Transforms>
                                <ds:Transform Algorithm="http://www.w3.org/2000/09/xmldsig
                                <ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc
                            </ds:Transforms>
                            <ds:DigestMethod Algorithm="http://www.w3.org/2001/04/xmlenc#sh
                            <ds:DigestValue>xxxx=</ds:DigestValue>
                        </ds:Reference>
                    </ds:SignedInfo>
                    <ds:SignatureValue>xxxx</ds:SignatureValue>
                    <ds:KeyInfo>
                        <ds:KeyName>xxxx</ds:KeyName>
                    </ds:KeyInfo>
                </ds:Signature>
                <saml:Subject>
                    <saml:NameID Format="urn:oasis:names:tc:SAML:2.0:nameid-format:transie
                    <saml:SubjectConfirmation Method="urn:oasis:names:tc:SAML:2.0:cm:beare
                        <saml:SubjectConfirmationData InResponseTo="_xxxxxxxxxxxxxxxxxxxx"
                                                      NotOnOrAfter="2020-05-29T07:10:12Z"
                                                      Recipient="https://eh01.staging.conn
                    </saml:SubjectConfirmation>
                </saml:Subject>
                <saml:Conditions NotBefore="2020-05-29T06:50:12Z"
                                 NotOnOrAfter="2020-05-29T07:10:12Z">
                    <saml:AudienceRestriction>
                        <saml:Audience>urn:etoegang:HM:0000000xxxxxxxxx000:entities:xxxx</s
```

```
                    <saml:Audience>urn:etoegang:DV:0000000xxxxxxxxx000:entities:xxxx</s
                </saml:AudienceRestriction>
            </saml:Conditions>
            <saml:AuthnStatement AuthnInstant="2020-05-29T07:00:07Z">
                <saml:AuthnContext>
                    <saml:AuthnContextClassRef>urn:etoegang:core:assurance-class:loa2<
                    <saml:AuthenticatingAuthority>xxxx</saml:AuthenticatingAuthority>
                </saml:AuthnContext>
            </saml:AuthnStatement>

            <saml:AttributeStatement>
                <saml:Attribute Name="urn:etoegang:core:Representation">
                    <saml:AttributeValue xsi:type="xs:boolean">false</saml:AttributeVa
                </saml:Attribute>
                <saml:Attribute Name="urn:etoegang:core:ServiceUUID">
                    <saml:AttributeValue xsi:type="xs:string">xxxx</saml:AttributeValue
                </saml:Attribute>
                <saml:Attribute Name="urn:etoegang:core:ActingSubjectID">
                    <saml:AttributeValue>
                        <saml:EncryptedID>
                            <xenc:EncryptedData xmlns:xenc="http://www.w3.org/2001/04/x
                                                Id="_xxxxxxxxxxxxxxxxxxxx"
                                                Type="http://www.w3.org/2001/04/xmlenc#
                                <xenc:EncryptionMethod Algorithm="http://www.w3.org/200
                                <ds:KeyInfo>
                                    <ds:RetrievalMethod Type="http://www.w3.org/2001/04
                                                        URI="_xxxxxxxxxxxxxxxxxxxx"/>
                                </ds:KeyInfo>
                                <xenc:CipherData>
                                    <xenc:CipherValue>xxxx</xenc:CipherValue>
                                </xenc:CipherData>
                            </xenc:EncryptedData>
                            <xenc:EncryptedKey xmlns:xenc="http://www.w3.org/2001/04/xm
                                               Id="_xxxxxxxxxxxxxxxxxxxx"
                                               Recipient="urn:etoegang:DV:0000000xxxxx
                                <xenc:EncryptionMethod Algorithm="http://www.w3.org/200
                                    <ds:DigestMethod Algorithm="http://www.w3.org/2000/
                                </xenc:EncryptionMethod>
                                <ds:KeyInfo>
                                    <ds:KeyName>xxxx</ds:KeyName>
                                </ds:KeyInfo>
                                <xenc:CipherData>
                                    <xenc:CipherValue>xxxx</xenc:CipherValue>
                                </xenc:CipherData>
                                <xenc:ReferenceList>
                                    <xenc:DataReference URI="_xxxxxxxxxxxxxxxxxxxx"/>
                                </xenc:ReferenceList>
                            </xenc:EncryptedKey>
                        </saml:EncryptedID>
                    </saml:AttributeValue>
                </saml:Attribute>
                <saml:EncryptedAttribute>
                    <xenc:EncryptedData xmlns:xenc="http://www.w3.org/2001/04/xmlenc#"
                                        Id="encrypted_urn_etoegang_1.9_attribute_DateO
```

```
                                        Type="http://www.w3.org/2001/04/xmlenc#Element"
                        <xenc:EncryptionMethod Algorithm="http://www.w3.org/2001/04/xm
                        <ds:KeyInfo>
                            <ds:RetrievalMethod Type="http://www.w3.org/2001/04/xmlenc
                                                URI="_xxxxxxxxxxxxxxxxxxxx"/>
                        </ds:KeyInfo>
                        <xenc:CipherData>
                            <xenc:CipherValue>xxxx</xenc:CipherValue>
                        </xenc:CipherData>

                    </xenc:EncryptedData>
                    <xenc:EncryptedKey xmlns:xenc="http://www.w3.org/2001/04/xmlenc#"
                                       Id="_xxxxxxxxxxxxxxxxxxxx"
                                       Recipient="urn:etoegang:DV:0000000xxxxxxxx000:c
                        <xenc:EncryptionMethod Algorithm="http://www.w3.org/2001/04/xm
                            <ds:DigestMethod Algorithm="http://www.w3.org/2000/09/xmlds
                        </xenc:EncryptionMethod>
                        <ds:KeyInfo>
                            <ds:KeyName>xxxx</ds:KeyName>
                        </ds:KeyInfo>
                        <xenc:CipherData>
                            <xenc:CipherValue>xxxx</xenc:CipherValue>
                        </xenc:CipherData>
                        <xenc:ReferenceList>
                            <xenc:DataReference URI="#encrypted_urn_etoegang_1.9_attri
                        </xenc:ReferenceList>
                    </xenc:EncryptedKey>
                </saml:EncryptedAttribute>
                <saml:EncryptedAttribute>
                    <xenc:EncryptedData xmlns:xenc="http://www.w3.org/2001/04/xmlenc#"
                                        Id="encrypted_urn_etoegang_1.9_attribute_Family
                                        Type="http://www.w3.org/2001/04/xmlenc#Element"
                        <xenc:EncryptionMethod Algorithm="http://www.w3.org/2001/04/xm
                        <ds:KeyInfo>
                            <ds:RetrievalMethod Type="http://www.w3.org/2001/04/xmlenc
                                                URI="_xxxxxxxxxxxxxxxxxxxx"/>
                        </ds:KeyInfo>
                        <xenc:CipherData>
                            <xenc:CipherValue>xxxx</xenc:CipherValue>
                        </xenc:CipherData>
                    </xenc:EncryptedData>
                    <xenc:EncryptedKey xmlns:xenc="http://www.w3.org/2001/04/xmlenc#"
                                       Id="_xxxxxxxxxxxxxxxxxxxx"
                                       Recipient="urn:etoegang:DV:0000000xxxxxxxx000:c
                    >
                        <xenc:EncryptionMethod Algorithm="http://www.w3.org/2001/04/xm
                            <ds:DigestMethod Algorithm="http://www.w3.org/2000/09/xmlds
                        </xenc:EncryptionMethod>
                        <ds:KeyInfo>
                            <ds:KeyName>xxxxx</ds:KeyName>
                        </ds:KeyInfo>
                        <xenc:CipherData>
                            <xenc:CipherValue>xxxxx</xenc:CipherValue>
```

```
                        </xenc:CipherData>
                        <xenc:ReferenceList>
                            <xenc:DataReference URI="#encrypted_urn_etoegang_1.9_attri
                        </xenc:ReferenceList>
                    </xenc:EncryptedKey>
                </saml:EncryptedAttribute>
                <saml:EncryptedAttribute>
                    <xenc:EncryptedData xmlns:xenc="http://www.w3.org/2001/04/xmlenc#"
                                        Id="encrypted_urn_etoegang_1.9_attribute_FirstN
                                        Type="http://www.w3.org/2001/04/xmlenc#Element"
                        <xenc:EncryptionMethod Algorithm="http://www.w3.org/2001/04/xm
                        <ds:KeyInfo>
                            <ds:RetrievalMethod Type="http://www.w3.org/2001/04/xmlenc
                                                URI="_xxxxxxxxxxxxxxxxxxxx"/>
                        </ds:KeyInfo>
                        <xenc:CipherData>
                            <xenc:CipherValue>xxx</xenc:CipherValue>
                        </xenc:CipherData>
                    </xenc:EncryptedData>
                    <xenc:EncryptedKey xmlns:xenc="http://www.w3.org/2001/04/xmlenc#"
                                       Id="_1c10d90e8b53461cb794fa23b1f72f55"
                                       Recipient="urn:etoegang:DV:0000000xxxxxxxxx000:e
                        <xenc:EncryptionMethod Algorithm="http://www.w3.org/2001/04/xm
                            <ds:DigestMethod Algorithm="http://www.w3.org/2000/09/xmlds
                        </xenc:EncryptionMethod>
                        <ds:KeyInfo>
                            <ds:KeyName>xxxx</ds:KeyName>
                        </ds:KeyInfo>
                        <xenc:CipherData>
                            <xenc:CipherValue>xxxx</xenc:CipherValue>
                        </xenc:CipherData>
                        <xenc:ReferenceList>
                            <xenc:DataReference URI="#encrypted_urn_etoegang_1.9_attri
                        </xenc:ReferenceList>
                    </xenc:EncryptedKey>
                </saml:EncryptedAttribute>
            </saml:AttributeStatement>
        </saml:Assertion>
    </saml:Advice>
    <saml:AuthnStatement AuthnInstant="2020-05-29T07:00:13Z">
        <saml:AuthnContext>
            <saml:AuthnContextClassRef>urn:etoegang:core:assurance-class:loa2</saml:Au
            <saml:AuthenticatingAuthority>urn:etoegang:AD:0000000xxxxxxxxx000:entities
        </saml:AuthnContext>
    </saml:AuthnStatement>
    <saml:AttributeStatement>
        <saml:Attribute Name="urn:etoegang:core:ServiceUUID">
            <saml:AttributeValue xsi:type="xs:string">xxxx</saml:AttributeValue>
        </saml:Attribute>
        <saml:EncryptedAttribute xmlns:xenc="http://www.w3.org/2001/04/xmlenc#">
            <xenc:EncryptedData Id="_07151871-ab7d-337d-a4c2-aa6f0c23148d"
                                Type="http://www.w3.org/2001/04/xmlenc#Element">
                <xenc:EncryptionMethod Algorithm="http://www.w3.org/2001/04/xmlenc#aes
```

```
                    <ds:KeyInfo>
                        <ds:RetrievalMethod Type="http://www.w3.org/2001/04/xmlenc#Encrypte
                                            URI="_xxxxxxxxxxxxxxxxxxx"/>
                    </ds:KeyInfo>
                    <xenc:CipherData>
                        <xenc:CipherValue>xxxx</xenc:CipherValue>
                    </xenc:CipherData>
                </xenc:EncryptedData>
                <xenc:EncryptedKey Id="_xxxxxxxxxxxxxxxxxxx"
                                   Recipient="urn:etoegang:DV:0000000xxxxxxxxx000:entities
                    <xenc:EncryptionMethod Algorithm="http://www.w3.org/2001/04/xmlenc#rsa-
                        <ds:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"
                    </xenc:EncryptionMethod>
                    <ds:KeyInfo>
                        <ds:KeyName>xxxx</ds:KeyName>
                    </ds:KeyInfo>
                    <xenc:CipherData>
                        <xenc:CipherValue>xxxx</xenc:CipherValue>
                    </xenc:CipherData>
                    <xenc:ReferenceList>
                        <xenc:DataReference URI="_xxxxxxxxxxxxxxxxxxx"/>
                    </xenc:ReferenceList>
                </xenc:EncryptedKey>
            </saml:EncryptedAttribute>
        </saml:AttributeStatement>
    </saml:Assertion>
</samlp:Response>

```

eH 1.9

```
<samlp:Response xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol" xmlns:ds="http://www.w3
                Version="2.0">
    <saml:Issuer>urn:etoegang:HM:0000000xxxxxxxxx000:entities:xxxx</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-sha25
            <ds:Reference URI="_xxxxxxxxxxxxxxxxxxxx">
                <ds:Transforms>
                    <ds:Transform Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-s
                    <ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#">
                        <ec:InclusiveNamespaces xmlns:ec="http://www.w3.org/2001/10/xml-exc
                    </ds:Transform>
                </ds:Transforms>
                <ds:DigestMethod Algorithm="http://www.w3.org/2001/04/xmlenc#sha256"/>
                <ds:DigestValue>xxxx=</ds:DigestValue>
            </ds:Reference>
        </ds:SignedInfo>
        <ds:SignatureValue>xxxx</ds:SignatureValue>
    </ds:Signature>
```

```
    <samlp:Status>
        <samlp:StatusCode Value="urn:oasis:names:tc:SAML:2.0:status:Success"/>
    </samlp:Status>
    <saml:Assertion ID="_xxxxxxxxxxxxxxxxxxxx" IssueInstant="2020-05-28T13:02:33Z" Versio
        <saml:Issuer>urn:etoegang:HM:0000000xxxxxxxxx000:entities:xxxx</saml:Issuer>
        <ds:Signature>
            <ds:SignedInfo>
                <ds:CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-exc-c1
                <ds:SignatureMethod Algorithm="http://www.w3.org/2001/04/xmldsig-more#rsa-

                <ds:Reference URI="_xxxxxxxxxxxxxxxxxxxx">
                    <ds:Transforms>
                        <ds:Transform Algorithm="http://www.w3.org/2000/09/xmldsig#envelop
                        <ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#">
                            <ec:InclusiveNamespaces xmlns:ec="http://www.w3.org/2001/10/xm
                        </ds:Transform>
                    </ds:Transforms>
                    <ds:DigestMethod Algorithm="http://www.w3.org/2001/04/xmlenc#sha256"/>
                    <ds:DigestValue>xxxx=</ds:DigestValue>
                </ds:Reference>
            </ds:SignedInfo>
            <ds:SignatureValue>xxxx</ds:SignatureValue>
        </ds:Signature>
        <saml:Subject>
            <saml:NameID Format="urn:oasis:names:tc:SAML:2.0:nameid-format:persistent" Nam
            <saml:SubjectConfirmation Method="urn:oasis:names:tc:SAML:2.0:cm:bearer">
                <saml:SubjectConfirmationData InResponseTo="_xxxxxxxxxxxxxxxxxxxx" NotOnO
                </saml:SubjectConfirmationData>
            </saml:SubjectConfirmation>
        </saml:Subject>
        <saml:Conditions NotBefore="2020-05-28T13:02:33Z" NotOnOrAfter="2020-05-28T13:07:3
            <saml:AudienceRestriction>
                <saml:Audience>urn:etoegang:DV:0000000xxxxxxxxx000:entities:xxxx</saml:Aud
            </saml:AudienceRestriction>
        </saml:Conditions>
        <saml:AuthnStatement AuthnInstant="2020-05-28T13:02:33Z">
            <saml:AuthnContext>
                <saml:AuthnContextClassRef>urn:etoegang:core:assurance-class:loa2plus</sam
                <saml:AuthenticatingAuthority>urn:etoegang:HM:0000000xxxxxxxxx000:entities
            </saml:AuthnContext>
        </saml:AuthnStatement>
        <saml:AttributeStatement>
            <saml:Attribute Name="urn:etoegang:1.9:EntityConcernedID:KvKnr">
                <saml:AttributeValue xsi:type="xs:string">xxxx</saml:AttributeValue>
            </saml:Attribute>
            <saml:Attribute Name="urn:etoegang:core:ServiceID">
                <saml:AttributeValue xsi:type="xs:string">urn:etoegang:DV:0000000xxxxxxxxx
            </saml:Attribute>
        </saml:AttributeStatement>
    </saml:Assertion>
</samlp:Response>

```

eH Ketenmachtiging

```
<?xml version="1.0" encoding="UTF-8" standalone="no"?>
<samlp:Response
    xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol"
    xmlns:ds="http://www.w3.org/2000/09/xmldsig#"
    xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion"
    xmlns:xs="http://www.w3.org/2001/XMLSchema"
    xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" Destination="xxx" ID="xxx" InResp
    <saml:Issuer>xxx</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-sha25
            <ds:Reference URI="#xxx">
                <ds:Transforms>
                    <ds:Transform Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-s
                    <ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#">
                        <ec:InclusiveNamespaces
                            xmlns:ec="http://www.w3.org/2001/10/xml-exc-c14n#" PrefixList="
                        </ds:Transform>
                    </ds:Transforms>
                    <ds:DigestMethod Algorithm="http://www.w3.org/2001/04/xmlenc#sha256"/>
                    <ds:DigestValue>xxx</ds:DigestValue>
                </ds:Reference>
            </ds:SignedInfo>
            <ds:SignatureValue>xxx
</ds:SignatureValue>
            <ds:KeyInfo>
                <ds:KeyName>xxx</ds:KeyName>
            </ds:KeyInfo>
        </ds:Signature>
        <samlp:Status>
            <samlp:StatusCode Value="urn:oasis:names:tc:SAML:2.0:status:Success"/>
        </samlp:Status>
        <saml:Assertion
            xmlns:xacml-saml="urn:oasis:xacml:2.0:saml:assertion:schema:os" ID="xxx" Issue
            <saml:Issuer>xxx</saml:Issuer>
            <saml:Subject>
                <saml:NameID Format="urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified
                <saml:SubjectConfirmation Method="urn:oasis:names:tc:SAML:2.0:cm:bearer">
                    <saml:SubjectConfirmationData InResponseTo="xxx" NotOnOrAfter="2020-05
                </saml:SubjectConfirmation>
            </saml:Subject>
            <saml:Conditions NotBefore="2020-05-20T12:30:40Z" NotOnOrAfter="2020-05-20T12:
                <saml:AudienceRestriction>
                    <saml:Audience>xxx</saml:Audience>
                </saml:AudienceRestriction>
            </saml:Conditions>
            <saml:AuthnStatement AuthnInstant="2020-05-20T12:30:40Z">
                <saml:AuthnContext>
                    <saml:AuthnContextClassRef>urn:oasis:names:tc:SAML:2.0:ac:classes:Passw
```

```
                    <saml:AuthenticatingAuthority>urn:etoegang:HM:00000003244440010000:ent
                </saml:AuthnContext>
            </saml:AuthnStatement>
            <saml:AttributeStatement>
                <saml:Attribute Name="urn:etoegang:core:ServiceID">
                    <saml:AttributeValue xsi:type="xs:string">urn:etoegang:DV:xxx:services
                </saml:Attribute>
                <saml:Attribute Name="urn:etoegang:core:ServiceUUID">
                    <saml:AttributeValue xsi:type="xs:string">xxx</saml:AttributeValue>
                </saml:Attribute>
                <saml:Attribute Name="urn:etoegang:1.9:EntityConcernedID:KvKnr">
                    <saml:AttributeValue xsi:type="xs:string">11----118</saml:AttributeValu
                </saml:Attribute>
                <saml:Attribute Name="urn:etoegang:1.9:IntermediateEntityID:KvKnr">
                    <saml:AttributeValue xsi:type="xs:string">271---01</saml:AttributeValue
                </saml:Attribute>
                <saml:Attribute FriendlyName="urn:etoegang:1.13:EntityConcernedID:Pseudo" N
                    <saml:AttributeValue xsi:type="xs:string">xxx</saml:AttributeValue>
                </saml:Attribute>
            </saml:AttributeStatement>
        </saml:Assertion>
    </samlp:Response>
```