

Connectis Simplified eID Profile for Municipalities

Simplified eID Attribute Profile fully compatible with eIDAS/STORK regulations

Revisions:

Version	Date	Description
1.0	15-11-2016	Initial version
2.0	29-11-2016	External version

[Introduction](#)

[Simplified eID Profile](#)

[Compliance with EIDAS/STORK protocols](#)

[Simplified eID Profile for Natural Persons](#)

[Simplified eID Profile for Legal Persons](#)

[Simplified eID Profile Usage](#)

[SAML Authentication Request Example](#)

[SAML Authentication Response Example](#)

[Encryption](#)

[Adapters](#)

Introduction

This document covers the Simplified eID Profile for Municipalities offered by the Connectis Broker and explains how to translate these attributes into eIDAS/STORK equivalent sets.

Simplified eID Profile

Connectis is a key provider of Online Authentication software. In the biggest cross-border electronic identification project in the world, Connectis prepares the scene for the full-swing implementation of eIDAS in 2018. By the end of 2016, Connectis will act as a seamless translator between the Service Providers of 81 Dutch municipalities and up to 32 European countries, which will authenticate foreign citizens based on their own eID solutions.

Each country involved in the project can speak different protocols and can provide different authorization attributes. Therefore the Connectis Broker translates all of them into a simplified and common profile, that can be easily understood and used by the Dutch municipalities involved in the project.

The Connectis Broker is dependent on the attributes provided by the countries involved. The attribute comparison provided in this document describes the situation in which all attributes are provided. In the end, Connectis has no control over the attributes that are sent by each specific country.

Compliance with EIDAS/STORK protocols

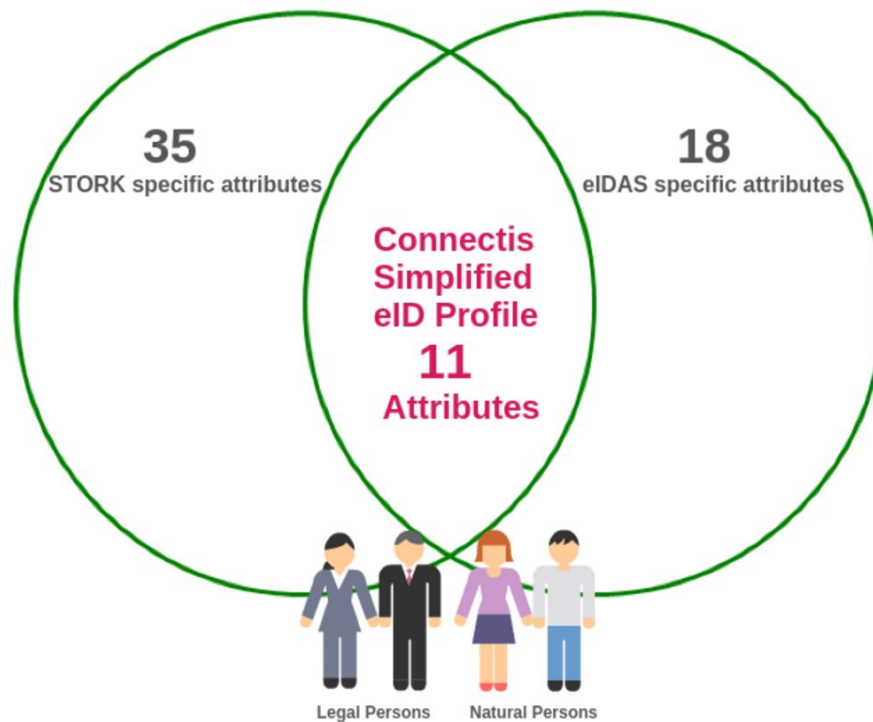
The eIDAS Attribute profile defines a set of 18 specific attributes¹ that can identify a user upon online authentication, out of which 8 attributes are for Natural Persons and 10 attributes are for Legal Persons.

STORK Attribute profile defines another set of 35 specific attributes², out of which 13 can be used for Natural Persons and 12 for Legal Persons. In addition to these, STORK also defines custom attributes for very specific domains like eHealth and eLearning, that were used for early pilots and proof of concept applications.

The Connectis Simplified eID Profile helps the Dutch municipalities involved in the project to refer to their users attributes in a standard and easier way, by mapping the common attributes of the two eIDAS and STORK SAML extensions.

¹ Full list of supported EIDAS attributes is defined [here](#).

² Full list of supported STORK attributes is defined [here](#).



The following sections translate the Connectis Simplified Profile for Municipalities to both eIDAS and STORK corresponding attributes.

The mandatory attributes are guaranteed to be returned by Citizen Home Countries upon authorization. The optional attributes may be returned, based on each country legal characteristics.

Simplified eID Profile for Natural Persons

Connectis simplified profile	STORK attribute profile	EIDAS attribute profile
<i>Mandatory attributes (based on EIDAS regulations)</i>		
PersonIdentifier	http://www.stork.gov.eu/1.0/eidentifier	http://eidas.europa.eu/attributes/naturalpersons/PersonIdentifier
CurrentFamilyName	http://www.stork.gov.eu/1.0/surname	http://eidas.europa.eu/attributes/naturalpersons/CurrentFamilyName
CurrentGivenName	http://www.stork.gov.eu/1.0/givenName	http://eidas.europa.eu/attributes/naturalpersons/CurrentGivenName
DateOfBirth	http://www.stork.gov.eu/1.0/dateOfBirth	http://eidas.europa.eu/attributes/naturalpersons/DateOfBirth

<i>Optional attributes (based on EIDAS regulations)</i>		
BirthName	http://www.stork.gov.eu/1.0/inheritedFamilyName	http://eidas.europa.eu/attributes/naturalperson/BirthName
PlaceOfBirth	http://www.stork.gov.eu/1.0/placeOfBirth	http://eidas.europa.eu/attributes/naturalperson/PlaceOfBirth
Gender	http://www.stork.gov.eu/1.0/gender	http://eidas.europa.eu/attributes/naturalperson/Gender
CurrentAddress	http://www.stork.gov.eu/1.0/textResidenceAddress	http://eidas.europa.eu/attributes/naturalperson/CurrentAddress

The Connectis Simplified eID Profile for Natural Persons is currently supported by the Connectis Broker.

Simplified eID Profile for Legal Persons

Connectis simplified profile	STORK attribute profile	EIDAS attribute profile
<i>Mandatory attributes (based on EIDAS regulations)</i>		
LegalName	http://www.stork.gov.eu/1.0/legalName	http://eidas.europa.eu/attributes/legalperson/LegalName
LegalPersonIdentifier	http://www.stork.gov.eu/1.0/eLPIdentifier	http://eidas.europa.eu/attributes/legalperson/LegalPersonIdentifier
<i>Optional attributes (based on EIDAS regulations)</i>		
LegalAddress	http://www.stork.gov.eu/1.0/registeredCanonicalAddress	http://eidas.europa.eu/attributes/legalperson/LegalAddress

The Connectis Simplified eID Profile for Legal Persons will be supported by the Connectis Broker before September 2018.

Simplified eID Profile Usage

SAML Authentication Request Example

In order to use the Simplified eID Profile and let the Connectis Broker take care of all translations between different protocols and Attribute Sets, the following Extensions must be included in the Authentication Request SAML message sent by the Service Provider:

```
<samlp:Extensions xmlns:req-attr="urn:oasis:names:tc:SAML:protocol:ext:req-attr"3
  xmlns:md="urn:oasis:names:tc:SAML:2.0:metadata">
  <req-attr:RequestedAttributes>
    <md:RequestedAttribute Name="PersonIdentifier" isRequired="true" />
    <md:RequestedAttribute Name="CurrentFamilyName" isRequired="true" />
    <md:RequestedAttribute Name="CurrentGivenName" isRequired="true" />
    <md:RequestedAttribute Name="DateOfBirth" isRequired="true" />
    <md:RequestedAttribute Name="BirthName" isRequired="false" />
    <md:RequestedAttribute Name="PlaceOfBirth" isRequired="false" />
    <md:RequestedAttribute Name="Gender" isRequired="false" />
    <md:RequestedAttribute Name="CurrentAddress" isRequired="false" />
  </req-attr:RequestedAttributes>
</samlp:Extensions>
```

SAML Authentication Response Example

This is a sample of how the Authentication Response Attributes section may look like after a successful authentication:

```
<saml:AttributeStatement>
  <saml:Attribute FriendlyName="PersonIdentifier"
    Name="http://eidas.europa.eu/attributes/naturalperson/PersonIdentifier"
    NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri">
    <saml:AttributeValue xmlns:xs="http://www.w3.org/2001/XMLSchema"
      xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
      xsi:type="eidas:PersonIdentifierType">2860620112233</saml:AttributeValue>
  </saml:Attribute>

  <saml:Attribute FriendlyName="CurrentFamilyName"
    Name="http://eidas.europa.eu/attributes/naturalperson/CurrentFamilyName"
    NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri">
    <saml:AttributeValue xmlns:xs="http://www.w3.org/2001/XMLSchema"
      xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
      xsi:type="eidas:CurrentFamilyNameType">Smith</saml:AttributeValue>
```

³ The req-attr extension is proposed by Connectis, in order to enable this Simplified eID Profile, and it is in the process of being standardized by the OASIS committee.

```
</saml:Attribute>
```

```
<saml:Attribute FriendlyName="CurrentGivenName"  
Name="http://eidas.europa.eu/attributes/naturalperson/CurrentGivenName"  
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri">  
  <saml:AttributeValue xmlns:xs="http://www.w3.org/2001/XMLSchema"  
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"  
xsi:type="eidas:CurrentGivenNameType">Anne</saml:AttributeValue>  
</saml:Attribute>
```

```
<saml:Attribute FriendlyName="BirthName" Name="http://eidas.europa.eu/attributes/naturalperson/BirthName"  
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri">  
  <saml:AttributeValue xmlns:xs="http://www.w3.org/2001/XMLSchema"  
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"  
xsi:type="eidas:BirthNameType">Davidson</saml:AttributeValue>  
</saml:Attribute>
```

```
<saml:Attribute FriendlyName="Gender" Name="http://eidas.europa.eu/attributes/naturalperson/Gender"  
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri">  
  <saml:AttributeValue xmlns:xs="http://www.w3.org/2001/XMLSchema"  
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xsi:type="eidas:GenderType">F</saml:AttributeValue>  
</saml:Attribute>
```

```
<saml:Attribute FriendlyName="DateOfBirth" Name="http://eidas.europa.eu/attributes/naturalperson/DateOfBirth"  
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri">  
  <saml:AttributeValue xmlns:xs="http://www.w3.org/2001/XMLSchema"  
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"  
xsi:type="eidas:DateOfBirthType">1986/06/20</saml:AttributeValue>  
</saml:Attribute>
```

```
</saml:AttributeStatement>
```

Encryption

The SAML Authentication Response is not encrypted at the moment, but in order to be fully eIDAS compliant the entire assertion will be encrypted once the eIDAS protocol becomes effective in the future. We expect Service Providers to decrypt messages once the Connectis Broker starts using this feature. Service Providers will receive a confirmation or time indication about when the encryption gets enabled.

Adapters

Connectis provides adapters in Java and ASP.NET. The Connectis Java Adapter allows Java developers to easily connect their application to the Connectis Identity Broker.

It is delivered as a java library (jar) and integration with a typical application can be done in 10 to 25 lines of code.

The Connectis ASP. Adapter allows .NET developers to easily connect their application to the Connectis Identity Broker. It is delivered as a .NET library (dll) and - just like the Java Adapter - integration with a typical application can be done in 10 to 25 lines of code.

These adapters are available in an adapted eIDAS version and allow customers to easily integrate their existing applications with the network for eIDAS. It bypasses the need to integrate the SAML Authentication Request. Additionally, the future implementation of encryption is bypassed for customers as well.

For more information about access to the adapters, please contact technicalsupport@connectis.nl