Integration Guide

WP-Number: 22300

Project Sponsor	State Secretariat for Economic Affairs SECO
Project Manager	Marc Zweiacker
Author	AdNovum Informatik AG
Number	22304
Classification	**Not classified**, internal, confidential, CLASSIFIED
Status	**Pending**, approved

List of Changes

Date	Version	Changes	Author
12.03.2018	1.0	Initial version of integration guide	AdNovum Informatik AG

Table of Contents

1 Introduction

1.1 Summary

The given IDV platform integration guide describes the steps that are required to integrate a relying party (RP) or identity provider (IdP) which may also act as attribute authority (IdP/AA) with one or more IDV domains. Furthermore it gives guidance on certain configuration options that are available as part of the integration.

1.2 Target Audience

The given IDV platform integration guide is targeted for participants of the IDV platform that want to integrate a RP / IdP with one or more IDV domains.

1.3 Status of this Document

The present version of the IDV platform integration guide is based on IDV Platform Interface Specification 1.0 ([IDV-IFC_SPEC]) and on IDV System Requirements 1.0 ([IDV-REQ]). The technical scope and protocols are frozen. The focus is on integration with one of the IDV integration pilot domains.

The document will be further refined based on the experience while integrating interested RP / IdP.

1.4 Notation

The key words “MUST”, “MUST NOT”, “REQUIRED”, “SHALL”, “SHALL NOT”, “SHOULD”, “SHOULD NOT”, “RECOMMENDED”, “MAY”, and “OPTIONAL” in this document are to be interpreted as described in [RFC2119].

Conventional XML namespace prefixes are used throughout the listings in this specification to stand for their respective namespaces as follows, whether or not a namespace declaration is present in the example:

Prefix	XML Namespace	Comments	Example
ds:	http://www.w3.org/2000/09/xmldsig#	This namespace is defined in the W3C XML Signature Syntax and Processing specification [XML-DSIG].	<ds:X509Certificate>
ext:	urn:oasis:names:tc:SAML:attributes:ext	SAML V2.0 attribute extensions [SAML-ATTR-EXT].	ext:OriginalIssuer
md:	urn:oasis:names:tc:SAML:2.0:metadata	SAML V2.0 metadata namespace defined in the SAML V2.0 metadata specification [SAML-META].	<md:EntityDescriptor>
mdattr:	urn:oasis:names:tc:SAML:metadata:attribute	SAML V2.0 metadata attribute namespace defined in the SAML V2.0 metadata extension for entity attributes [SAML-META-ATTR].	<mdattr:EntityAttributes>
mdui:	urn:oasis:names:tc:SAML:metadata:ui	SAML V2.0 metadata extension namespace defined in the SAML V2.0 metadata extensions specification for login and discovery user interface [SAML-META-UI].	<mdui:Logo>
saml2:	urn:oasis:names:tc:SAML:2.0:assertion	SAML V2.0 assertion namespace defined in the SAML 2.0 core specification [SAML-CORE].	<saml2:NameID>

saml2p:	urn:oasis:names:tc:SAML:2.0:protocol	SAML V2.0 protocol namespace defined in the SAML 2.0 core specification [SAML-CORE].	<saml2p:Response>
xenc:	http://www.w3.org/2001/04/xmlenc#	This namespace is defined in the W3C XML Encryption Syntax and Processing specification [XML-ENC].	<xenc:EncryptedData>
xsd:	http://www.w3.org/2001/XMLSchema	This namespace is defined in the W3C XML Schema specification [SCHEMA1].	xs:string

1.5 Terminology

A complete glossary for IDV is maintained in a separate document. The definitions of some important terms are copied here to simplify the look-up for the reader.

Term	Definition
Attribute Authority (AA)	Attribute Authority (AA) is an entity, usually a directory, offering a service to manage and query attributes regarding a subject. It is able to issue attribute assertions.
IDV Domain	The services of an IDV platform are provided for domains. In this sense IDV Schweiz is divided into domains, whereas a domain is a kind of circle of trust between an IDV domain manager, IdPs and RPs which all agree on a common domain policy, attribute set, and quality models which guide the authentication service provided by IDV for that domain.
Home Realm Discovery (HRD)	A user selects a suitable identity provider from a list of available identity providers. After selection, the user will be redirected to the IdP for authentication.
Identity Provider (IdP)	A kind of *service provider* that creates, maintains, and manages identity information for *principals* and provides principal authentication to other *service providers* within a *federation*, such as with web browser *profiles* [SAML-GLOSSARY].
IdP/AA	Stands for an identity provider (IdP) which is also an attribute authority, which is the case for most IdPs.
IDV	The project IDV Schweiz develops the necessary technical infrastructure and organizational measures for a Swiss-wide identity and authentication federation platform (IDV platform) based on the STIAM architecture standards according to eCH.
IDV Admin	The IDV admin application (short IDV admin) covers the functionality for management of the participating entities (service providers, identity providers, and attribute authorities). This part covers the so-called “definition-time” services.
IDV Broker	The IDV broker provides the so-called “runtime” functionality, which covers the authentication process of an end user for a service provider. The IDV broker implements an authentication brokering service based on [ECH-0168].
IDV Platform	Central platform (IDV platform) to link eGov services with matching identity providers and attribute authorities for the purpose of user authentication. The IDV platform should address government to citizen (G2C), government to business (G2B), and government to government (G2G) scenarios.
LoA	A Level of Assurance, as defined by the by ISO/IEC 29115 Standard, describes the degree of confidence in the processes leading up to and including an authentication. It provides assurance that the entity claiming a particular identity is the entity to which that identity was assigned.
PET	Privacy-Enhancing Technologies is a system of ICT measures protecting informational privacy by eliminating or minimizing personal data, thereby preventing unnecessary or unwanted processing of personal data without the loss of the functionality of the information system [PET-HANDBOOK].
PII	Personally identifiable information

Relying Party (RP)	A Relying Party (RP) is an entity which uses the IDV platform to authenticate users and obtain attributes regarding them in order to control access to its resources.
Service Provider (SP)	A Service Provider (SP) is used in the present document as a synonym of RP. Thus in the context of IDV, SPs are mostly governmental organizations operating web applications (eGov services).
SAML Requester	A *system entity* that utilizes the SAML protocol to request services from another system entity (a *SAML authority*, a *responder*). The term “client” for this notion is not used because many system entities simultaneously or serially act as both clients and servers. In cases where the SOAP binding for SAML is being used, the SAML requester is architecturally distinct from the *initial SOAP sender*[SAML-GLOSSARY].
SAML Responder	A *system entity* (a *SAML authority*) that utilizes the SAML protocol to respond to a request for services from another system entity (a *requester*). The term “server” for this notion is not used because many system entities simultaneously or serially act as both clients and servers. In cases where the SOAP binding for SAML is being used, the SAML responder is architecturally distinct from the *ultimate SOAP receiver* [SAML-GLOSSARY].
Single Page Application (SPA)	Web application that fits on a single web page with the goal of providing a user experience similar to that of a desktop application.
System Entity, Entity	An active element of a computer/network system. For example, an automated process or set of processes, a subsystem, a person or group of persons that incorporates a distinct set of functionality [RFC4949].
User Consent (UC)	To comply with data protection laws, the user has to give his consent when personal data is transmitted from one party (notably from an IdP/AA or an AA) to another party (normally a RP).

1.6 References

Reference	Description
[CAB-FORUM]	CA/Browser Forum https://cabforum.org/
[ECH-0097]	eCH (2015, Nov) eCH-0097: Datenstandard Unternehmensidentifikation [Online] https://www.ech.ch/vechweb/page?p=dossier&documentNumber=eCH-0097&documentVersion=3.0
[ECH-0107]	eCH (2013, Dec) eCH-0107: Gestaltungsprinzipien für die Identitäts- und Zugriffsverwaltung (IAM) [Online] http://www.ech.ch/vechweb/page?p=dossier&documentNumber=eCH-0107&documentVersion=2.0
[ECH-0113]	eCH (2012, Jun) eCH-0113: Spezifikation SuisseID [Online] http://www.ech.ch/vechweb/page?p=dossier&documentNumber=eCH-0113&documentVersion=1.0
[ECH-0167]	eCH (2014, Jun) eCH-0167: SuisseTrustIAM-Rahmenkonzept [Online] http://www.ech.ch/vechweb/page?p=dossier&documentNumber=eCH-0167&documentVersion=1.0
[ECH-0168]	eCH (2014, Nov) eCH-0168: SuisseTrustIAM technische Architektur und Prozesse [Online] http://www.ech.ch/vechweb/page?p=dossier&documentNumber=eCH-0168
[ECH-0170]	eCH (2014, Jun) eCH-0170: eID Qualitätsmodell, Version 1.0 [Online] http://www.ech.ch/vechweb/page?p=dossier&documentNumber=eCH-0170&documentVersion=1.0
[ECH-0170V2]	eCH (2017, Jan) eCH-0170: Qualitätsmodell zur Authentifizierung von Subjekten, Version 2.0 [Online] Version 2.0, Status Entwurf, Publiziert am 09.01.2017 https://www.ech.ch/vechweb/page?p=dossier&documentNumber=eCH-

	0170&documentVersion=2.0
[ECH-0174]	eCH (2015, Nov) eCH-0174: SuisseTrustIAM- Implementierung mit SAML 2.0. [Online] http://www.ech.ch/vechweb/page?p=dossier&documentNumber=eCH-0174&documentVersion=1.0[
[EIDAS]	EU regulation on electronic identification and trust services for electronic transactions in the European Single Market. The set of standards was established in EU regulation № 910/2014 of 23 July 2014 on electronic identification and repeals directive 1999/93/EC.http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32014R0910
[ID-META-INTEROP]	Identity Metasystem Interoperability Version 1.0, OASIS Standard, 1 July 2009. [Online] http://docs.oasis-open.org/imi/identity/v1.0/identity.html
[IDV-GLOSSARY]	IDV Glossary, State Secretariat for Economic Affairs SECO.
[IDV-IFC_SPEC]	IDV Platform Interface Specification, Version 1.0, 19.12.2017, State Secretariat for Economic Affairs SECO.
[IDV-REQ]	IDV System Requirements, Version 1.0, 26.04.2017, State Secretariat for Economic Affairs SECO.
[RFC2119]	RFC 2119, Key words for use in RFCs to Indicate Requirement Levels, BCP 14, March 1997. https://tools.ietf.org/html/rfc2119
[RFC2397]	RFC 2397, The "data" URL scheme, L. Masinter, August 1998. https://tools.ietf.org/html/rfc2397
[RFC4949]	RFC 4949, Internet Security Glossary, Version 2, Internet Engineering Task Force, August 2007. https://tools.ietf.org/html/rfc4949
[RFC5280]	RFC 5280, Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile, D. Cooper NIST, S. Santesson Microsoft, S. Farrell Trinity College Dublin, S. Boeyen Entrust, R. Housley Vigil Security, W. Polk NIST, May 2008. [Online] https://www.ietf.org/rfc/rfc5280.txt
[SAML-GLOSSARY]	Glossary for the OASIS Security Assertion Markup Language (SAML) V2.0, J. Hodges, R. Philpott and E. Maler, March 2005. [Online] https://www.oasis-open.org/committees/download.php/21111/saml-glossary-2.0-os.htm
[SAML-ATTR-EXT]	OASIS Standard, SAML V2.0 Attribute Extensions, Version 1.0, Committee Specification 01, 4 August 2009. [Online] http://docs.oasis-open.org/security/saml/Post2.0/sstc-saml-attribute-ext-cs-01.pdf
[SAML-BIND]	OASIS Standard, Bindings for the OASIS Security Assertion Markup Language (SAML) V2.0 - Errata Composite, Working Draft 06, 8 September 2015. [Online] https://www.oasis-open.org/committees/download.php/56779/sstc-saml-bindings-errata-2.0-wd-06.pdf
[SAML-CORE]	OASIS Standard, Assertions and Protocols for the OASIS Security Assertion Markup Language (SAML) V2.0 – Errata Composite, Working Draft 07, 8 September 2015. [Online] https://www.oasis-open.org/committees/download.php/56776/sstc-saml-core-errata-2.0-wd-07.pdf
[SAML-META]	OASIS Standard, Metadata for the OASIS Security Assertion Markup Language (SAML) V2.0 – Errata Composite, Working Draft 05, 8 September 2015. [Online] https://www.oasis-open.org/committees/download.php/56785/sstc-saml-metadata-errata-2.0-wd-05.pdf
[SAML-META-ATTR]	OASIS Standard, Security Assertion Markup Language (SAML) V2.0 Metadata Extension for Entity Attributes V1.0, 06 February 2009. [Online] http://docs.oasis-open.org/security/saml/Post2.0/sstc-metadata-attr-cd-01.pdf
[SAML-META-PREV]	OASIS Standard, Metadata for the OASIS Security Assertion Markup Language (SAML) V2.0 – Errata Composite, Working Draft 04, 1 December 2009. [Online] https://www.oasis-open.org/committees/download.php/35391/sstc-saml-metadata-errata-2.0-wd-

	04-diff.pdf
[SAML-META-UI]	OASIS Standard, SAML V2.0 Metadata Extensions for Login and Discovery User Interface, V1.0, 03 April 2012. [Online]http://docs.oasis-open.org/security/saml/Post2.0/sstc-saml-metadata-ui/v1.0/sstc-saml-metadata-ui-v1.0.pdf
[SAML-PROF]	OASIS Standard, Profiles for the OASIS Security Assertion Markup Language (SAML) V2.0 – Errata Composite, Working Draft 07, 8 September 2015. [Online] https://www.oasis-open.org/committees/download.php/56782/sstc-saml-profiles-errata-2.0-wd-07.pdf
[SCHEMA1]	H. S. Thompson et al. XML Schema Part 1: Structures. World Wide Web Consortium Recommendation, May 2001.http://www.w3.org/TR/2001/REC-xmlschema-1-20010502/
[STORK2]	**S**ecure iden**T**ity acr**O**ss bo**R**ders lin**K**ed 2.0 project aims to establish a European eID Interoperability Platform allowing citizens to establish new e-relations across borders, just by presenting their national eID. [Online] https://www.eid-stork2.eu/
[WEBTRUST]	AICPA/CICA WebTrust Program for Certification Authorities http://www.webtrust.net
[XML-DSIG]	XML Signature Syntax and Processing, W3C Recommendation. http://www.w3.org/TR/xmldsig-core/
[XML-ENC]	XML Encryption Syntax and Processing, W3C Recommendation. https://www.w3.org/TR/xmlenc-core/

2 General Procedure

In general, the integration of an RP / IdP includes the following steps:

- **Check integration requirements**:
    - Make sure that the RP / IdP that shall be integrated fulfills the requirements according to the IDV Interface Specification 1.0 ([IDV-IFC_SPEC]).
- **Specify participant specific integration parameters based on your use cases**:
    - Decide on which IDV domain you want to onboard your RP / IdP: IDVIntG2C or IDVIntG2G (see chapter Domains and Policies).
    - Decide which LoAs you want to support / request.
    - Decide which attributes you want to support / request.
- **Prepare and submit the participant metadata**
- **Download and integrate the specified IDV broker metadata**
- **Test your RP / IdP**

3 Integration of RP Participant

The given section precises the steps from chapter General Procedure to integrate a RP participant with an IDV domain.

3.1 Check Integration Requirements

Make sure that the RP participant that shall be integrated fulfills the requirements according to the IDV Interface Specification 1.0 ([IDV-IFC_SPEC]).

In particular, check chapter 3.3.2, RP runtime requirements.

3.2 Specify RP Participant Specific Integration Parameters

Based on your use cases define some RP specific integration parameters.

3.2.1 Choose Integration Domain

Decide on which IDV domain you want to onboard your RP: IDVIntG2C or IDVIntG2G

- Chapter Domains and Policies gives you an overview on the two IDV integration pilot domains

Depending on the use cases and the verification goals the same RP could also be registered separately in both integration pilot domains.

3.2.2 Decide on Requested LoAs

Based on the protection needs of the use cases of your RP decide on the requested LoA (see [LoA]).

If you have different requirements regarding the requested LoA it is possible to override the LoA per use case in the according SAML AuthnRequests as described in chapter 5.5.1, SAML AuthnRequest of [IDV-IFC_SPEC].

3.2.3 Decide on Required Attribute Set(s)

Check the attribute sets that are available in the domain you've selected and decide which set you want to request based on your use case:

- Domain Attribute Catalogue and Sets G2C Integration Domain
- Domain Attribute Catalogue and Sets G2G Integration Domain

3.3 Prepare RP Participant Metadata

See IDV-IFC_SPEC, chapter 5.1.1 RP Metadata

Considerations regarding RP Participant Metadata

Take into account the following considerations:

- Provide values for all elements/attributes that are declared on level 'MUST' in the interface specification.
- Provide values for all elements/attributes that are declared on level 'MAY' in the interface speci-

fication, if they are relevant for your use cases.

The metadata can be either provided as XML metadata file as indicated in the IDV-IFC_SPEC, chapter 5.1.1 RP Metadata, or as CSV file containing the values for the required elements/attributes.

3.3.1 Standard Metadata

Provide standard metadata as described in chapter IDV-IFC_SPEC, chapter 5.1.1, section 'Standard RP Metadata'.

Considerations regarding RP Standard Metadata

Take into account the following additional considerations:

- Minimal set of elemets/attributes you MUST provide: <md:EntityDescriptor> [entityID], <md:KeyDescriptor> [use="signing"], <md:AssertionConsumerService>
- The set of <md:RequestedAttribute> of an <md:AttributeConsumingService> MUST correspond to an attribute set that is available in the domain you've selected (according to the previous preparation step).

XML format:

```
<EntityDescriptor entityID="https://www.example.ch/rp">
     <SPSSODescriptor AuthnRequestsSigned="true"
           WantAssertionsSigned="true"
           protocolSupportEnumeration="urn:oasis:names:tc:SAML:2.0:protocol">
...
```

Submit the XML file as **metadata-rp.xml**.

Table format:

Element/Attribute	Value
<md:EntityDescriptor> [entityID]	https://www.example.ch/rp
...	...

Submit the table file as **metadata-rp.csv**. Certificates may also be submitted as **metadata-rp-signing.pem** and **metadata-rp-encryption.pem**.

3.3.2 Metadata Extensions for Login and Discovery User Interface

Provide metadata extension for login and discovery user interface as described in chapter IDV-IFC_SPEC, chapter 5.1.1, section 'Metadata Extensions for Login and Discovery User Interface'.

Considerations regarding Metadata Extensions for Login and Discovery User Interface

Take into account the following additional considerations:

- <mdui:UIInfo> container element MUST be populated with attributes.
- <mdui:Logo> may be delivered as png image file.

XML format:

```
...
     <Extensions>
            <mdui:UIInfo>
                  <mdui:DisplayName xml:lang="de">Online Schalter - Gemeinde
Example</mdui:DisplayName>
                  <mdui:DisplayName xml:lang="fr">Guichet en ligne - Municipal-
ité Example</mdui:DisplayName>
...
```

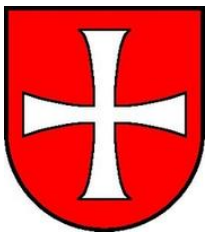
Submit as part of **metadata-rp.xml**.

Table format:

Attribute	Language	Value
DisplayName	de	Online Schalter - Gemeinde Example
DisplayName	fr	Guichet en ligne - Municipalité Example
...	...	...

Submit file as **metadata-rp-extension.csv**.

Image file example:



Submit the image file as **metadata-rp.png**.

3.3.3 IDV Specific RP Entity Attributes

Provide IDV specific RP entity attributes as described in chapter IDV-IFC_SPEC, chapter 5.1.1, section 'IDV Specific RP Entity Attributes'.

Considerations regarding IDV Specific RP Entity Attributes

Take into account the following additional considerations:

- Minimal set of elemets/attributes you MUST provide: entity attribute 'urn:oasis:names:tc:SAML:attribute:assurance-certification' (according to your previous selection).
- Optional entity attributes 'IdPPriorityList', 'IdPGroups' and 'originDisclosure' may be set after consulation with the IDV operations team.

- Optional entity attribute 'assertionDisclosure' is not yet supported.

The entity attributes can be added to metadata-rp.xml (XML format) or metadata-rp-extension.csv (table format).

3.4 Submit RP Participant Metadata

The metadata files must be zipped and submitted per mail with subject 'Registration of RP to IDV domain '<your domain>'* to idv-pilot@adnovum.ch:

Content	**Format 'XML Metadata'**	**Format 'CSV'**	**Optionally**
Standard Metadata	**metadata-rp.xml**	metadata-rp.csv	metadata-rp-signing.pem metadata-rp-encryption.pem
Metadata Extensions for Login and Discovery User Interface		metadata-rp-extension.csv	metadata-rp.png
IDV Specific RP Entity Attributes			

*<your domain> is the domain you selected before

3.5 Obtain IDV Broker Metadata

In order to enable trust between the participant RP and the IDV broker IdP/AA metadata must be exchanged. The IDV broker IdP/AA metadata can be retrieved from domain specific endpoint.

If the G2C domain has been selected for integration, download the IDV broker IdP/AA metadata from https://idv-int.adnovum.ch/IDVIntG2C/idp.

Otherwhise if the G2G domain has been selected download from https://idv-int.adnovum.ch/IDVIntG2G/idp.

3.6 Test your RP

Test your RP after the registration of your RP is confirmed.

4 Integration of IdP/AA Participant

The given section precises the steps from chapter General Procedure to integrate an IdP/AA participant with an IDV domain.

4.1 Check Integration Requirements

Make sure that the IdP/AA participant that shall be integrated fulfills the requirements according to the IDV Interface Specification 1.0 ([IDV-IFC_SPEC]).

In particular, check chapter 3.4.2, IdP/AA runtime requirements.

4.1.1 Choose Integration Domain

Decide on which IDV domain you want to onboard your IdP/AA: IDVIntG2C or IDVIntG2G

- Chapter Domains and Policies gives you an overview on the two IDV integration pilot domains

The same IdP/AA could be registered separately in different pilot domains.

4.1.2 Decide on Maximal Provided LoAs

Based on the protection needs that can be fulfilled with your IdP decide on the requested LoA (see [LoA]).

4.1.3 Decide on Attribute Sets you can Support

At domain registration time you have to declare which domain attributes your IdP/AA can serve.

Check the attribute catalogue that is available in the domain you've selected:

- Domain Attribute Catalogue and Sets G2C Integration Domain
- Domain Attribute Catalogue and Sets G2G Integration Domain

Handling of Unknown Values

If an IdP/AA does not know the attribute value of a registered attribute for a subject and if no exceptional value (such as "Unknown") is defined for that attribute, your IdP MUST omit the AttributeValue element and MUST provide an empty attribute element in the SAML response.

4.2 Prepare Participant Metadata

See IDV-IFC_SPEC, chapter 5.1.2 IdP/AA Metadata

Considerations regarding IdP/AA Participant Metadata

Take into account the following considerations:

- Provide values for all elements/attributes that are declared on level 'MUST' in the interface specification.

- Provide values for all elements/attributes that are declared on level 'MAY' in the interface specification, if they are relevant for your use cases.

The metadata can be either provided as XML metadata file as indicated in the IDV-IFC_SPEC, chapter 5.1.2 IdP/AA Metadata, or as CSV file containing the values for the required elements/attributes.

4.2.1 Standard Metadata

Provide standard metadata as described in chapter IDV-IFC_SPEC, chapter 5.1.2, section 'Standard IdP/AA Metadata'.

Considerations regarding IdP/AA Standard Metadata

Take into account the following additional considerations:

- Minimal set of elemets/attributes you MUST provide: <md:EntityDescriptor> [entityID], <md:KeyDescriptor> [use="signing"], <md:NameIDFormat>, <md:SingleSignOnService>, <saml:Attribute>
- The set of <md:RequestedAttribute> of an <md:AttributeConsumingService> MUST correspond to an attribute set that is available in the domain you've selected (according to the previous preparation step).

XML format:

```
<EntityDescriptor entityID="https://www.example.ch/idp">
     <IDPSSODescriptor
            WantAuthnRequestsSigned="true"
            protocolSupportEnumeration="urn:oasis:names:tc:SAML:2.0:protocol">
...
```

Submit the XML file as **metadata-idp.xml**.

Table format:

Attribute	Value
entityID	https://www.example.ch/idp
WantAuthnRequestsSigned	true
protocolSupportEnumeration	urn:oasis:names:tc:SAML:2.0:protocol
...	...

Submit the table file as **metadata-idp.csv**. Certificates may also be submitted as **metadata-idp-signing.pem**.

4.2.2 Metadata Extensions for Login and Discovery User Interface

Provide metadata extension for login and discovery user interface as described in chapter IDV-IFC_SPEC, chapter 5.1.2, section 'Metadata Extensions for Login and Discovery User Interface'.

Considerations regarding Metadata Extensions for Login and Discovery User Interface

Take into account the following additional considerations:

- <mdui:UIInfo> container element MUST be populated with attributes.
- <mdui:Logo> may be delivered as png image file.

XML format:

```
...
     <Extensions>
           <mdui:UIInfo>
                 <mdui:DisplayName xml:lang="de">Niederbipp Online-
Schalter</mdui:DisplayName>
                 <mdui:DisplayName xml:lang="fr">Guichet en ligne - Municipal-
ité Example</mdui:DisplayName>
...
```

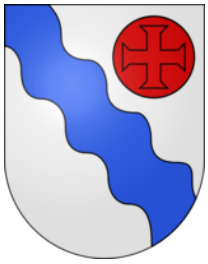
Submit as part of **metadata-idp.xml**.

Table format:

Attribute	Language	Value
DisplayName	de	Niederbipp Online-Schalter
DisplayName	fr	Niederbipp Guichet En Ligne
...	...	...

Submit file as **metadata-idp-extension.csv**.

Image file example:



Submit the image file as **metadata-idp.png**.

4.2.3 IDV Specific IdP/AA Entity Attributes

Provide IDV specific IdP/AA entity attributes as described in chapter IDV-IFC_SPEC, chapter 5.1.2, section 'IDV Specific IdP/AA Entity Attributes'.

Considerations regarding IDV Specific RP Entity Attributes

Take into account the following additional considerations:

- Minimal set of elemets/attributes you MUST provide: entity attribute 'urn:oasis:names:tc:SAML:attribute:assurance-certification' (according to your previous selection).

- Optional entity attribute 'ConsentObtainedByIdP' should not be set except for support of legacy IdPs.

The entity attributes can be added to metadata-idp.xml (XML format) or metadata-idp - extension.csv (table format).

4.3 Submit IdP/AA Participant Metadata

The metadata files must be zipped and submitted per mail with subject 'Registration of IdP/AA to IDV domain '<your domain>'* to idv-pilot@adnovum.ch:

Content	**Format 'XML Metadata'**	**Format 'CSV'**	**Optionally**
Standard Metadata	**metadata-idp.xml**	metadata-idp.csv	metadata-idp-signing.pem
Metadata Extensions for Login and Discovery User Interface		metadata-idp-extension.csv	metadata-idp.png
IDV Specific IdP/AA Entity Attributes			

*<your domain> is the domain you selected before

4.4 Obtain IDV Broker Metadata

In order to enable trust between the participant IdP/AA and the IDV broker SP metadata must be exchanged. The IDV broker SP metadata can be retrieved from domain specific endpoint.

If the G2C domain has been selected for integration, download the IDV broker SP metadata from https://idv-int.adnovum.ch/IDVIntG2C/sp.

Otherwhise if the G2G domain has been selected then download from https://idv-int.adnovum.ch/IDVIntG2G/sp.

4.5 Test your IdP/AA

Test your IdP/AA after the registration of your IdP/AA is confirmed with an own RP that is registered to the same domain or with one of the test RPs.

4.6 Customizing for Legacy IdPs

The IDV broker supports legacy and non-compliant IdPs to a certain degree.

In particular it is possible to apply the following transformations:

- Transformation of attribute names ("renaming")
- Transformation of attributes values ("reorganization")
- NameID transformations
- LoA transformations

Example Transformation

```
<idv:AuthnContextTransformations>
     <idv:AuthnContextTransformation
           SourceAuthn-
Context="urn:oasis:names:tc:SAML:2.0:ac:classes:unspecified"
```

```
            TargetAuthnContext="urn:stiam.gov.ch/authenticationassurance/level1"
/>
</idv:AuthnContextTransformations>
```

Get in contact with the IDV operation team in case you need transformations: idv-pilot@adnovum.ch.

5 Domains and Policies PRODINT

There are two domains on PRODINT: one for G2C use cases (IDVIntG2C) and one for G2G use cases (IDVIntG2G).

5.1 Domain Policies

Name	IDV-Broker Metadata	Comments
IDVIntG2C	https://idv-int.adnovum.ch/IDVIntG2C/sp https://idv-int.adnovum.ch/IDVIntG2C/idp	**Integration domain for G2C use cases** Characteristics: • The domain **has user consent** configured **on the IDV-Broker** • **Encryption of assertions** in case of LoA >= 2 • NameIDFormat: **persistent**, transient • Attributset G2C-Integrations-Domäne
IDVIntG2G	https://idv-int.adnovum.ch/IDVIntG2G/sp https://idv-int.adnovum.ch/IDVIntG2G/idp	**Integration domain for G2G use cases** Characteristics: • The domain has **no user consent** configured **on the IDV-Broker** • SAML requests with scoping element will be processed without 'home realm discovery screen' and without 'redirection screen' • **Encryption of assertions** in case of LoA >= 2 • NameIDFormat: transient • Attributset G2G-Integrations-Domäne

5.2 Domain Attribute Catalogue and Sets G2C Integration Domain

5.2.1 Attribute Catalogue

Friendly Name	Name	Comment
surname	http://schemas.xmlsoap.org/ws/2005/05/identity/claims/surname	
givenname	http://schemas.xmlsoap.org/ws/2005/05/identity/claims/givenname	
nationality	http://www.ech.ch/xmlns/eCH-0113/1/nationality	
gender	http://schemas.xmlsoap.org/ws/2005/05/identity/claims/gender	
date of birth	http://schemas.xmlsoap.org/ws/2005/05/identity/claims/dateofbirth	

5.2.2 Attribute Sets

Id	Name	Attributes
AS_G2C_01	Minimal attribute set	surname, name
AS_G2C_02	Extended attribute set	surname, name, nationality
AS_G2C_03	Full attribute set	surname, name, nationality, gender, date of birth

5.3 Domain Attribute Catalogue and Sets G2G Integration Domain

5.3.1 Attribute Catalogue

Friendly Name	Name	Comment
name	http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	
hasFunction	urn:oid:2.5.4.12	Specifies the function(s) the user occupies for the organization identified with memberOf
isMemberOf	urn:oid:2.5.4.10	Specifies the organization for which the user acts

5.3.2 Attribute Sets

Id	Name	Attributes
AS_G2G_01	Default attribute set	name, hasFunction, isMemberOf

6 Terms of Use Integration Pilot Integration Environment (Status: 05.03.2018)

- Integration pilot integration environment is online available for integration tests: 08:00 – 17:00
- Planned interrupts during office hours will be announced to integration pilot participants (e.g. during test phases)
- Access is limited to integration pilot participants
    - Do not give away the access credentials
    - In case of planned demos outside the office hours, announce it 48 h in advance to: idv-pilot@adnovum.ch
    - Feedback: idv-pilot@adnovum.ch