Logius Guide - Draft

Stelsel Toegang - SAML v1.0 - RC1

Logius Guide
Draft October 16, 2025

This version:
https://logius-standaarden.github.io/st-saml-spec/

Latest published version:
https://logius-standaarden.github.io/st-saml-spec/

Latest editor's draft:
https://logius-standaarden.github.io/st-saml-spec/

Editor:
Frans de Kok (Logius)

Authors:
Frans de Kok (Logius)
Jan Geert Koops (DICTU)
Mark Nijmeijer (DICTU)
Wiljan Pitlo (ICTU)
Carlo Huiden (ICTU)

Participate:
GitHub Logius-standaarden/st-saml-spec
File an issue
Commit history
Pull requests

This document is also available in these non-normative formats: Versie voor dienstverleners and PDF

Status of This Document

This is a draft that could be altered, removed or replaced by other documents. It is not a recommendation approved by TO.

Table of Contents

§ Conformance

As well as sections marked as non-normative, all authoring guidelines, diagrams, examples, and notes in this specification are non-normative. Everything else in this specification is normative.

The key words *MAY*, *MUST*, *MUST NOT*, *SHOULD*, and *SHOULD NOT* in this document are to be interpreted as described in BCP 14 [*RFC2119*] [*RFC8174*] when, and only when, they appear in all capitals, as shown here.

Abstract

This specification is intended for service providers (DV) who want to connect their webservices to DigiD and optionally DigiD-Machtigen and BVD-OG via a RD like TVS.

§ 1. Disclaimer

This version of the document must not in any way be considered to be a normative source for the purpose of conducting audits on participants. This topic will be addressed in future versions.

Errata, functional improvements and other developments will be added to this documentation in future versions. Version history for this document is included on the History page.

§ 2. History

Version	Changes	Distribution
[*ST-SAML1.0*] RC 1	Release Candidate 1: derived from [*eID SAML4.4*] Final with the following additional changes • Added support for BVD-OG in support of Stelsel Toegang release 1. • Added specifications for connection between RD and AD/BVD, based on [*eID SAML4.5*] specification	Internal

Version	Changes	Distribution

	• Change of structure to introduce two versions
	  ◦ Short version only covering DV and LC connecting to an RD (e.g. TVS)
	  ◦ Complete version also covering connections between RD and AD/BVD
	• All parts have been revised for improved clarity and consistency.
	• The specification now features extensive internal referencing, cross-linking and tooltips (aka 'Hover text') to improve navigation and context.	

§ 3. *Glossary*

§ 3.1 *Terms*

Term/abbreviation	English	Nederlands	Explanation
Artifact		Artefact	(SAML) Pointer to SAML message that is send through the front-channel, to avoid exposing sensitive data to the Webbrowser (UA) of the EU.
Assertion		Verklaring	A signed statement about a user's identity and mandates made by an AD or BVD. See SAML Assertion message.
Back channel	Back channel		Receiver (DV, LC, RD) uses an Artifact to collect the actual SAML message from the Sender (RD, AD or BVD). All SAML Back channel messages are placed in a SOAP envelope, the Webbrowser (UA) of the EndUser (EU) is not involved.
Front channel	Front channel		Communication between DV, LC, RD, AD and BVD via (a browser redirect of) the Webbrowser (UA) of the EndUser (EU).
BVD-DDM		Bevoegdheidsverklaringsdienst DigiD-Machtigen	A public instance of BVD specifically for mandates registered in DigiD-Machtigen only for public DV
BVD-OG		BevoegdheidsVerklaringsDienst Ouderlijk Gezag	A public instance of BVD specifically for legal representation concerning parental authority, based on Dutch national database of personal information (maintained by municipalities)
DigiD		DigiD	public IdP (AD) only for public DV
DigiD-Machtigen	DDM	DigiD-Machtigen	- public Mandate Registry. See also BVD-DDM
DigiD-CC		DigiD CombiConnect	See also DigiD CC1.1 interface specification.
EntityID			All systems in the network are identified by a unique EntityId in SAML Metadata, which is specified in the SAML metadata
ETD	Trust Framework	Afsprakenstelsel Elektronische Toegangsdiensten	Dutch Trust Framework, also known as 'eHerkenning'. See https://afsprakenstelsel.etoegang.nl/.
Legal Representation		Wettelijke Vertegenwoordiging	Legal Representation means that someone (EU) is allowed by law to act on behalf of another person (Represented Party).

Term/abbreviation	English	Nederlands	Explanation
LoA	Level of Assurance	Betrouwbaarheidsniveau	See supported Level of Assurance
Metadata	Metadata		Before a SAML connection can be established, all parties (DV, LC, RD, AD and BVD) must exchange connection properties. This is done through SAML Metadata.
Participant		Deelnemer	Any party that has a role in the authentication or representation processes that are within the scope of this specification. These include RD, AD and BVD.
Represented Party		Vertegenwoordigde	Service Consumer represented by EU
SAML	SAML		De SAML v 2.0 standard, also referred to as SAML 2.0. SAML is an acronym of Security Assertion Markup Language. See [*SAML2.TO*].
Service	Service	Dienst	Service offered by a DV
Service Catalog	Service Catalog	Dienstencatalogus of DC	Collection of Services offered by all Service Providers, kept by RD. The DV is responsible for keeping their Services in the Service Catalog up to date.
Service Consumer	Service Consumer	Belanghebbende	Service Consumer is the Entity Concerned: either EU when acting on its own behalf, or the Represented Party when EU is representing someone else.
ServiceUUID		Service Universally Unique IDentifier	ServiceUUID is an identifier of a service that is unique in the context of the network
SSO	Single Sign On	Eenmalig Inloggen	
SLO	Single Log Off	Federatief uitloggen	Single Log Off feature
ST-SAML		SAML specification for DV connecting via TVS (RD) to DigiD, DigiD-Machtigen and BVD-OG	SAML specification for a DV connecting via TVS (as RD) to DigiD, DigiD-Machtigen and BVD-OG
TVS	TVS	TVS	public RD only for public DV

§ 3.2 *Roles*

De following roles are used in this specification.

Abbreviation	Role/Actor	Description	Example
AD	Authenticatiedienst	Identity Provider (IdP)	DigiD, EB and AD in ETD
BVD	Bevoegdheidsverklaringsdienst	Service that provides assertions for representation relationships	The BVD-DDM (DigiD Machtigen), BVD-OG (parental authority)
DV	Dienstverlener	Service Provider	Website of municipality, hospital, government agency
EB	eIDAS Berichten Service	eIDAS Nederland knooppunt	
EU	EindGebruiker	End User	Natural Person acting on its own behalf to consume a Service OR acting on behalf of

Abbreviation	Role/Actor	Description	Example
			someone else (the Service Consumer).
LC	Leverancier Clusteraansluiting	Clusterconnection provider: This role assists the DV in connecting to RD. LC will handle all connectivity to RD for their registered DV	PaaS/SaaS providers within the health-care field
RD	Routeringsdienst	Routing Service Provides access to ADs and BVDs	TVS
UA	User Agent	User Agent is application controlled by the EU	WebBrowser

4. Introduction

This ST-SAML specification facilitates Stelsel Toegang release 1. [*ST-SAML1.0*] derived from [*eID SAML4.4*] and [*eID SAML4.5*]. It introduces the BVD-OG for an extra representation use case: legal representation of a minor by someone with parental authority (Ouderlijk Gezag). If a DV supports this use case, the RD (or DV) will offer the choice to do so to the EU.

ST-SAML specifies the communication between DV and RD and also between LC and RD. ST-SAML also specifies the communication between Routeringsdienst (RD) and BVD for parental authority (BVD-OG). [*eID SAML4.5*] specifies the communication between RD and DigiD (as AD) and between RD and BVD for registered mandates in DigiD-Machtigen: BVD-DDM. These DigiD specific specifications are out of scope for this ST-SAML specification.

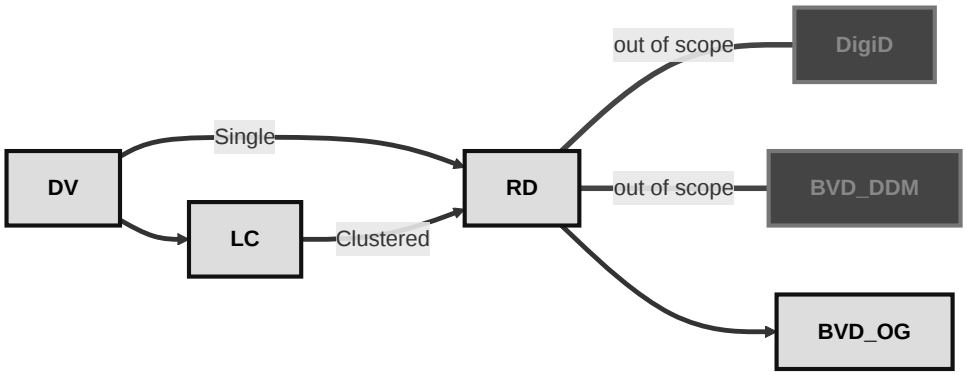

Figure 1 Stelsel Toegang SAML1.0

Routeringsdienst (RD) supports the use cases summarized below:

Use case	Description
Authentication	Authenticating an EU for a single Service, for a single purpose. This is the most basic use case scenario from a DV's point of view. Authentication always implies consent of the EU for accessing the Service and may include authorization if the EU is using representation.
Cluster connection connectivity	In a Cluster connection setting, a LC is technically responsible for connecting a DV to RD.
Authentication with representation	an EU authenticates with the intent to consume the Service on behalf of another person Represented Party using a Representation Relationship that is registered within a BVD context.
Authentication and/or representation via a RD	At a RD, an EU interactively selects an AD for which they own an authentication means, and/or a BVD in which a representation relation that they intend to use is registered, from multiple options. The RD redirects the EU to the selected AD and/or BVD.
Authentication with AD/BVD preselection	Authenticating an EU where selection for the AD or BVD is done at the DV prior to the authentication request to the RD in order to optimize the EU experience.

SAML specification

The document is not a complete SAML reference. It is assumed that the reader is familiar with SAML and will use the referenced documentation as well when needed.

- SAML Message specification - Contains message definitions of all interactions between DV/LC – RD and between RD – AD/BVD.
- SAML Metadata - Contains metadata definitions for DV, LC, RD, AD and BVD.

5. Frameworks

5.1 SAML generic

SAML Assertions and Protocols for the OASIS Security Assertion Markup Language (SAML) V2.0 [*SAML2*]

- saml-core-2.0-os [*SAML2.CORE*]
- saml-profiles-2.0-os [*SAML2.PROFILES*]
- saml-metadata-2.0-os [*SAML2.METADATA*]
- saml-bindings-2.0-os [*SAML2.BINDINGS*]
- saml errata [*SAML2.ERRATA.05*]

NORA, Nederlandse Overheid Referentie Architectuur [*NORA*].
NCSC ICT-beveiligingsrichtlijnen voor Transport Layer Security (TLS) [*NCSC.TLS*].

SAML profiles A SAML profile is a specific set of rules that are used for a specific use case. ST-SAML uses two profiles of the SAML standard, namely:

- Web Browser SSO Profile ([*SAML2.PROFILES*], par 4.1), with HTTP Post binding (see below).
- Single Logout Profile ([*SAML2.PROFILES*], par 4.4), with HTTP Post binding, issued by Session Participant to Identity Provider.

5.2 DV - SAML message flows & bindings

Only the bindings that are listed in the tables are supported between DV and LC

5.2.1 DV→RD authentication flow

The diagram below depicts the authentication flow between a DV and LC and the RD.

> See also DV-RD - SAML authentication messages

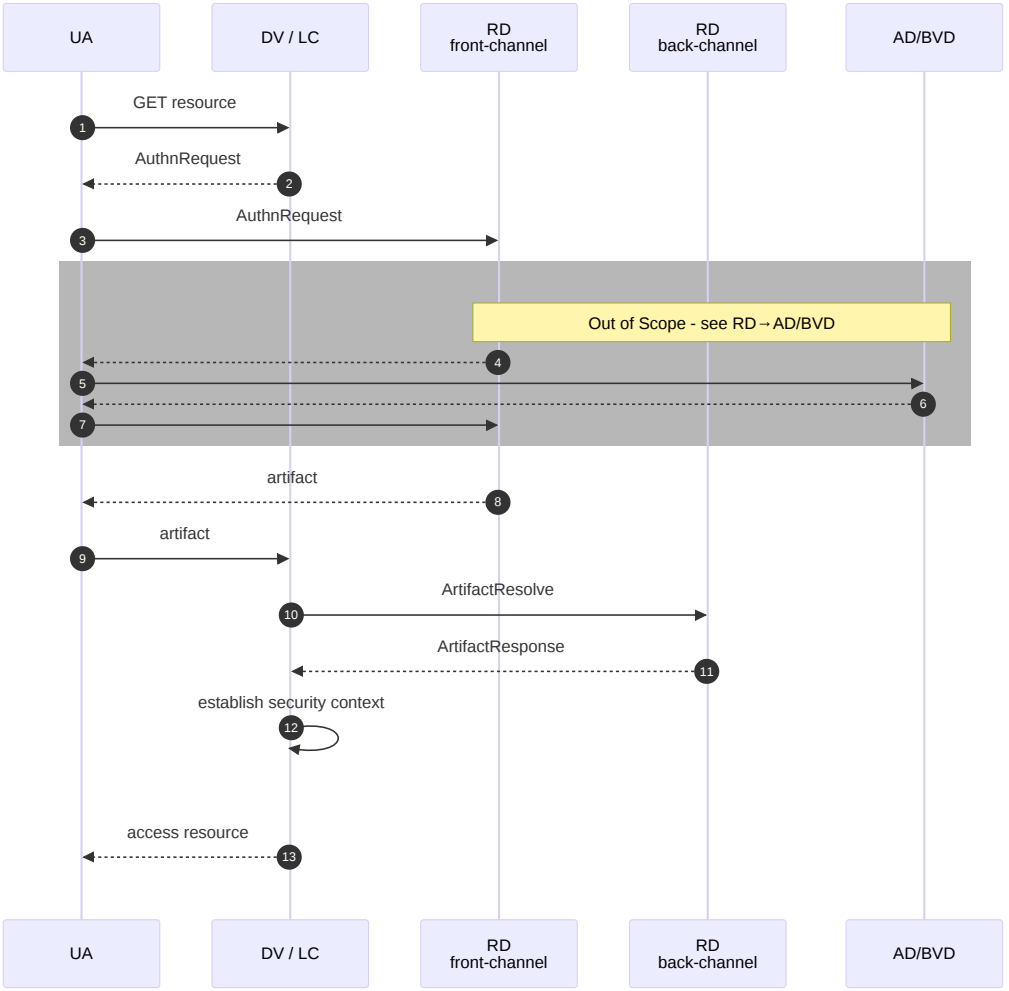

Figure 2 Authentication and representation flow - overview

§ *5.2.1.1 Front-channel (re)authentication*

Step #	Route	Message	Endpoint	Binding	Metadata
2 + 3	DV/LC (→UA)→RD	AuthN Request message	SingleSignOnService	HTTP-POST	RD→DV
8 + 9	RD (→UA)→DV/LC	Artifact binding message	AssertionConsumerService (DV) AssertionConsumerService (LC)	HTTP-Artifact	DV→RD LC→RD

§ *5.2.1.2 Back-channel (Assertion)*

Step #	Route	Message	Endpoint	Binding	Metadata
10	DV/LC→RD	Artifact Resolve message	ArtifactResolutionService	SOAP	RD→DV
11	RD→DV/LC	AuthN Response message	None, is a synchronous response	SOAP	

§ **5.2.2 DV→RD Federated Logout flow**

Only a limited form of SP (DV/LC) initiated logout is supported within the context of a SSO federation. IdP (AD) initiated Logout is NOT supported! On receiving a logout request from the EU via the UA (step 1) a DV/LC which participates in a SSO federation *MUST* send a LogoutRequest to RD (step 2 and 3). RD propagates the Logout Request to appropriate AD. If the AD replies success status, the RD will reply with a LogoutResponse with success status to the DV/LC.

The diagram below depicts the single logout flow between a DV and LC and the RD.

> Also see SAML Federated login and logout

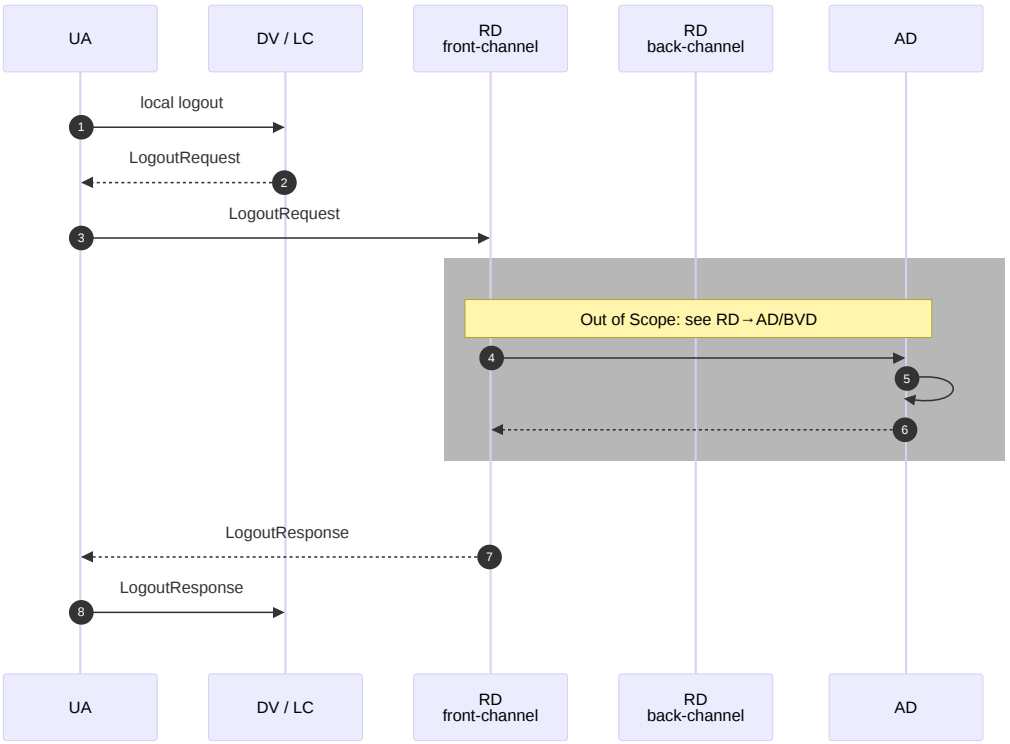

Figure 3 SAML Federated Logout overview

Step #	Route	Message	Endpoint	Binding	Meta-data
2 + 3	DV/LC (→UA)→RD	Logout Request	SingleLogoutService	HTTP-POST	RD→DV
7 + 8	RD (→UA)→DV/LC	Logout Response	SingleLogoutService (DV) SingleLogoutService (LC)	HTTP-POST	DV→RD LC→RD

5.3 RD - SAML message flows & bindings

Only the bindings that are listed in the tables are supported between RD and AD/BVD

5.3.1 RD→AD authentication flow

A RD helps the acting End User (EU) to select the authentication scenario based on registration a the Service in the Service Catalog. Based on the EU choices RD *MUST* propagate the authentication request of the DV or LC to the appropriate AD and in case of representation the appropriate BVD via the bindings that are listed in the tables below.

The diagram below depicts the authentication flow between a RD and an AD and BVD.

> See also RD→AD/BVD - SAML authentication proces

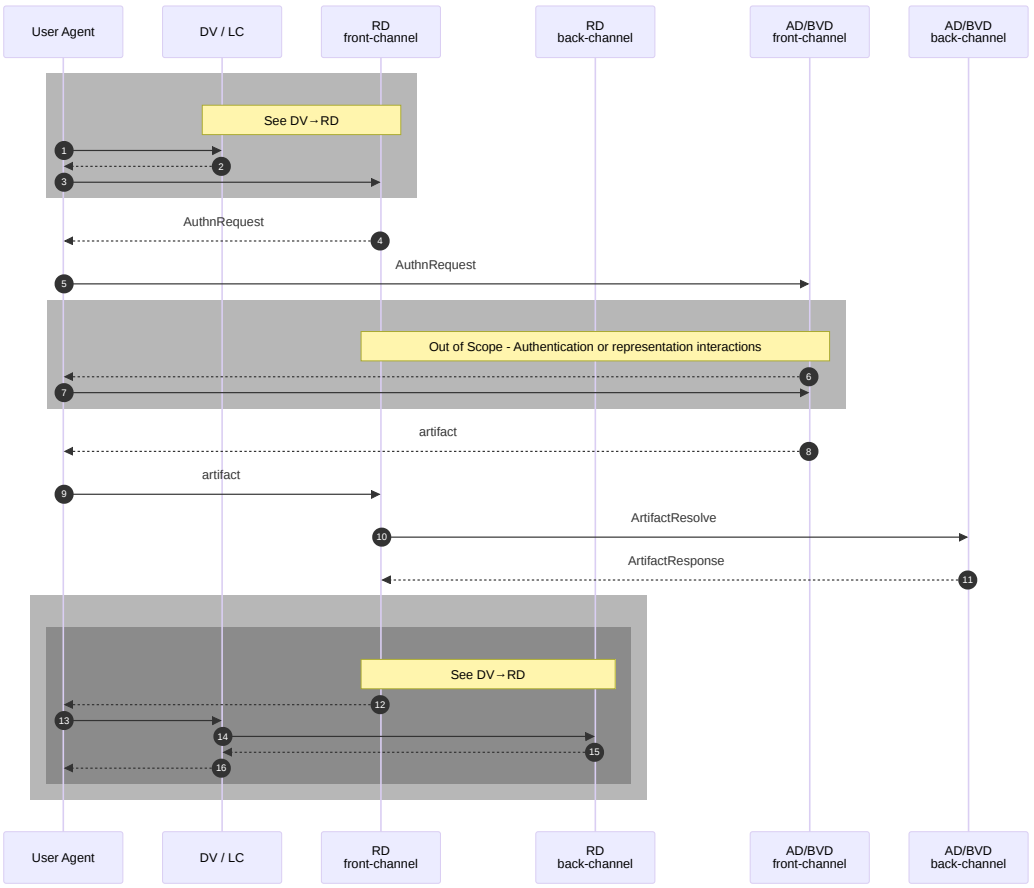

Figure 4 SAML authentication flow RD - AD/BVD

> This flow continues between DV and RD, see DV/LC←RD - authentication flow

§ *5.3.1.1 Front-channel (re)authentication*

Step #	Route	Message	Endpoint	Binding	Meta-data
4 + 5	RD (→UA)→AD/BVD	AuthN Request Message	SingleSignOnService	HTTP-POST	[AD/BVD](#ad-bvd-metadata 'AD/BVD metadata for RD)
8 + 9	AD/BVD (→UA)→RD	Artifact	AssertionConsumerService	HTTP-Artifact	RD

§ *5.3.1.2 Back-channel (Assertion)*

Step #	Route	Message	Endpoint	Binding	Meta-data
10	RD→AD/BVD	Artifact Resolve message	ArtifactResolutionService	SOAP	AD/BVD
11	AD/BVD →RD	ArtifactResponse	None, is a synchronous response	SOAP	

§ **5.3.2 RD - AD Single Logout**

A RD that supports SSO to DVs or LCs must propagate logout requests to the appropriate RD. The diagram below depicts the flow between a RD and an AD.

> See also RD→AD/BVD Federated login & logout

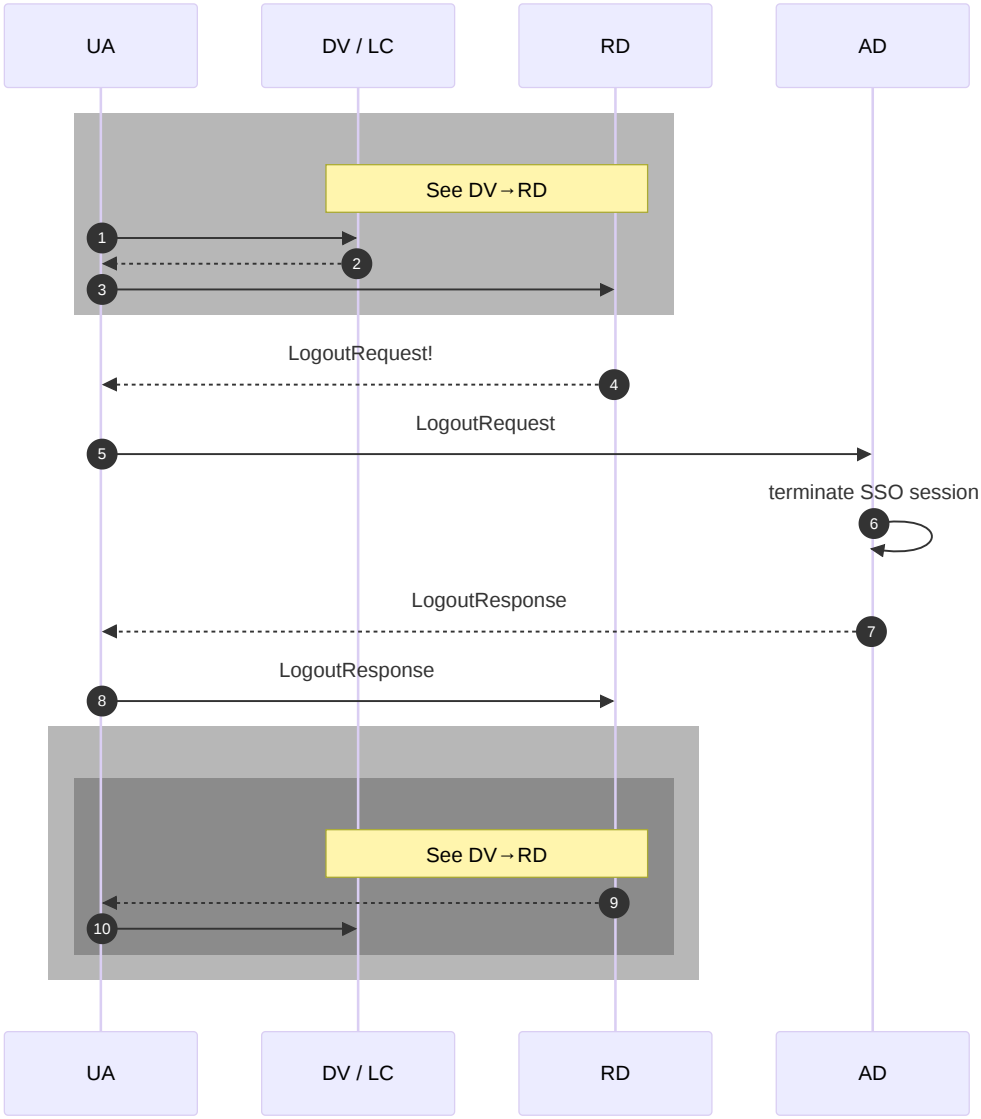

Figure 5 Single Logout RD - AD/BVD

> This flow continues between DV and RD, see DV/LC←RD - authentication flow

Step #	Route	Message	Endpoint	Binding	Meta-data
4 + 5	RD (→UA)→AD	Logout Request	SingleLogoutService	HTTP-POST	AD/BVD
7 + 8	AD/BVD (→UA) →RD	Logout Response	SingleLogoutService	HTTP-POST	RD

6. Supported Use Cases

6.1 Authentication

An EU intends to consume a Service on his/her own behalf, from a DV for which authentication is required.

6.1.1 Actors

Roles

- EU

- DV
- RD
- AD

For more information see also Roles

6.1.2 Functional description

An EU intends to consume a Service on his/her own behalf. The Service is offered on the web by a DV.

The EU visits the website of the Service, where the EU may have to interact to indicate the intent to consume the Service. As the Service requires authentication, this triggers the authentication process.

The DV will now redirect the EU to RD, requesting authentication of the EU for the Service. Note that in this use case the EU will not select to act on behalf of another. (See Authentication with Representation)

Next, the EU is redirected to the AD. After successful authentication the AD takes care the EU is redirected back to RD, who includes the attestation of identity in the relevant interface response to the DV. This response includes at minimum an identifier of the EU, the LoA attested to and the Service authenticated for. The LoA of the authentication is at minimum equal to or higher than the configured LoA for the Service within the Service Catalog. The RD now includes the attestation of identity and the attestation of representation relationship in the relevant interface response to the DV. This response includes at minimum an identifier of the EU and the Represented Party, the LoA attested to and the Service authenticated for.

The DV can now take an access control decision to its Service for the EU.

The technical steps in the authentication flow are described in DV SAML Authentication.

> NOTE
>
> Communication between RD and DigiD is specified in DigiD Combiconnect specification (DigiD-CC) and is out of scope of this specification.

6.2 Authentication with representation

An acting EU intends to consume a Service to represent another party, from a DV, for which authentication is required. The EU acting on behalf of a Represented Party, must be a Natural Person, using a representation relationship. The Represented Party must also be a Natural Person. The relationship must be formalized and a direct relationship.

The authentication of the acting EU takes place just like in the Authentication use case. Similarly, the representation information concerning both the acting EU, the Represented Party and the Service for which they have a representation relation will provided by a BVD, either

1. Standard representation aka DigiD-Machtigen by BVD-DDM
2. Legal representation by other BVDs eg. BVD-OG.

6.2.1 standard representation

The acting EU acts on behalf of the Represented Party (Service Consumer). The representation relationship underpinning this must be registered by Represented Party as a formalized mandate in a mandate registry (DigiD-Machtigen), prior to application in this use case.

> Rules governing representation and registration of a registration relationship are out of scope of this specification. Communication between RD and BVD-DDM is specified in DigiD-CC specification and is out of scope of this specification.

6.2.2 legal representation

The information about the type of legal representation concerning the EU and the Represented Party will provided by a BVD, eg BVD-OG for parental authority. To make this use case succeed, the relationship between the EU and the Represented Party must be registered in the applicable registry in such a way that it meets the legal requirements.

> Rules on governing legal representation are out of scope of this specification.

6.2.3 Actors

Roles

- EU
- DV
- RD
- AD
- BVD

6.2.4 Functional description

The EU visits the website of the Service, where the EU may have to interact to indicate the intent to consume the Service. As the Service requires authentication, this triggers the authentication process. The EU must be able to indicate the intent to consume the Service on behalf of a Represented Party (and not for his/herself) before the authentication process is triggered.

The DV (or LC) will now redirect the EU to RD, requesting authentication of the EU for the Service, including the request to authorize based on a representation relationship.

Next, the EU is redirected to the AD. After successful authentication, the AD redirects the EU to RD. RD will then redirect the EU to BVD-DDM. Here the EU selects the representation relationship to use, if multiple options are available. Afterwards the BVD redirects the EU back to RD.

RD now includes the attestation of identity and the attestation of the representation relationship in the relevant interface response to the DV (or LC) . This response includes an identifier of the EU and the Represented Party and in case of legal representation also the specific type of legal representation between both. Also the requested ServiceUUID and the LoA of the authentication is included in the response. The LoA is at minimum equal to or higher than the configured LoA for the Service within the Service Catalog.

The DV can now take an access control decision to its Service for the EU on behalf of the Represented Party.

The technical steps in the authentication flow are described here: DV SAML Authentication.

6.3 Cluster connection connectivity

In Software-as-a-Service (SaaS) or multi-tenant solutions, multiple DV's are hosted on a single environment operated by a software vendor. The software vendor can act as an LC. Functionally the LC itself is not actively taking part in any of the primary use cases, thus is not an actor in those use cases.

> NOTE
> Although above the Cluster is linked to SaaS solutions, the cluster connection can be applicable in Platform-as-a-Service (PaaS) offerings as well. This is only the case if the platform natively offers connectivity to RD; it is NOT applicable if the connectivity is built on top of the platform provided using PaaS.
>
> For Infrastructure-as-a-Service solutions (IaaS), the Cluster Connection is NOT applicable.

6.3.1 Actors

Roles	Description
DV	See also Roles
LC	
RD	

6.3.2 Technical description

The Cluster Connection is acknowledged during requests for authentication, as made in the supported use cases. The LC is registered at RD and is also responsible for registering all DV's he provides access for. Relationship between DV and LC must be established in the registration/on-boarding process with RD and in LC-metadata.

DV initiates authentication via the LC. The LC will send an AuthN Request Message to RD on behalf of DV.

Data in the response from RD will be encrypted only for the DV to decrypt, not the LC.

In this way, the LC can facilitate the authentication processes, but cannot access the sensitive information contained in the response.

> NOTE
>
> The way a DV interacts with a LC is not part of this specification.

6.4 Authentication with AD/BVD preselection

an EU intends to consume a Service on his/her own behalf, from a (semi-)governmental or public DV], for which authentication is required. The EU makes the selection for the AD at the DV , rather than at the RD. In order to improve [=EU=|user] experience (UX), this enables presenting the choice of AD at the DV at the most appropriate time and in the best fitting manner.

Additionally in a representation scenario, the EU can (also) select the BVD at the DV .

> NOTE
>
> Passing the choice for AD/BVD is solely offered for improving [=EU=|user] experience. It is explicitly not the intention that DV introduce a bias in the choice for the AD/BVD to use. Valid use cases for bypassing EU preference, where a DV selects a specific AD/BVD for an EU , are very rare and specific. DV should offer the choice for each AD/BVD in a non-discriminatory way for all applicable AD/BVD.

6.4.1 Actors

Roles

- EU
- DV
- RD
- AD
- BVD

For more information see also Roles

6.4.2 Functional description

This use case is a functional extension to Authentication. Instead of choosing the AD and/or BVD after being redirected to the RD, the EU selects the AD and/or BVD for usage at an earlier stage at the DV. The RD will apply the pre-selection as a filter on all available options. If, after filtering, alternative options are found, the RD will prompt the EU to further narrow down the selection.

The DV will offer the EU to make a choice from the list of applicable ADs before sending a request for authentication to the RD. Simultaneously with the choice for an AD, the choice to represent another will be offered the EU with (optionally) the BVD to be used. After making the choice for an AD, acting-as-a-representative and the choice for a BVD , these choices will be included in the request for authentication to the RD. In case the EU acts on behalf of another without pre-selecting a BVD, the choice for a BVD will be presented in a later stage at the RD.

The technical steps in the authentication flow are described in the SAML-Message-specification.

7. Message Specification

RD - Leeg

7.1 DV - SAML Message specification

7.1.1 DV→RD - SAML authentication proces

SAML authentication messages between DV (or LC) and RD are described in this chapter. First the authentication overview and the steps, then the specification of the individual SAML messages between DV and RD.

7.1.1.1 DV→RD - authentication - diagram

The diagram below contains the authentication steps that are made when an EU authenticates with a DV through the RD. When an LC is present between DV and RD the LC will take the role of DV in relation to the RD.

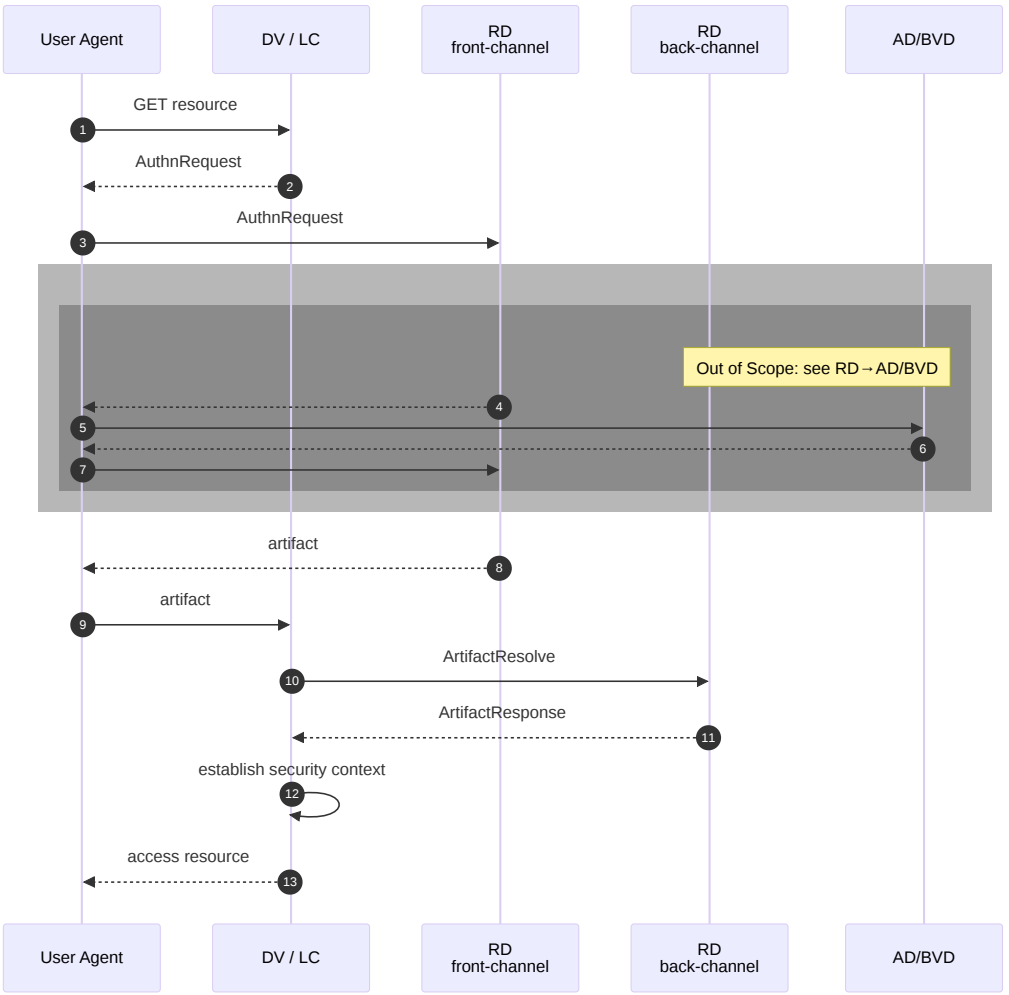

Figure 6 SAML authentication flow - DV/LC - RD

§ *7.1.1.2 DV→RD - authentication - steps*

Before the above authentication steps are explained, it is important to make a distinction between the Front channel and the Back channel. The Front channel is the communication between the DV or LC and RD via the UA of the EU (step 2 & 3 and step 8 & 9 in the figure above). The Back channel is the direct communication between the DV or LC and RD (step 10 and Step 11 in the figure above). This distinction is important because possibly sensitive data (such as a citizen service number) is never send via the Front channel, so that they can never be intercepted or changed by the UA.

Step 1

The EU with a UA wants to access a part on the web service of the DV that requires authentication of the EU.

Step 2 and 3

The DV or LC will send the EU to RD for authentication and or proof of representation.

Step 4 up to and including 7 (out of scope for this flow)

In this step the RD will offer the EU a choice of AD's and BVD's that fulfil the authentication requirements (e.g. minimum level of assurance required, type of mandate). Optionally, the DV can pass pre-selection information concerning the AD to query, and if representation will be used, to the RD.

If the EU hasn't already chosen in step 2, the EU chooses an authentication method that meets the minimum required LoA, and also chooses whether to use representation. The EU is presented with the corresponding AD login screen. The EU authenticates with the chosen means.

Optionally, the EU also chooses a representation method. The EU is presented with the corresponding screen with choice of who to represent. The EU chooses the correct Represented Party to represent.

Step 8 and 9

RD sends the EU back to the DV or LC via a redirect. An opaque Artifact generated by RD is send here. This Artifact refers to the actual Artifact Response message that is waiting at RD.

Even if the authentication starting in step 4 was unsuccessful or interrupted, an artifact is send to the DV or LC. This Artifact provides an error message with the Artifact Resolve request and cannot be exchanged for a valid Assertion.

Step 10

With the Artifact the DV/LC sends an Artifact Resolve request to the RD for the result of the (successful or unsuccessful) authentication and (optionally) representation via a Back channel.

Artifacts are stored by RD for a maximum of 15 minutes and can only be retrieved once by the DV/LC. Situations are possible (process breakdown, early logout) where RD saves an Artifact for less than 15 minutes.

Step 11

RD replies with an Artifact Response message that belongs to the Artifact. In this message, RD provides an Assertion that includes the authentication result and optionally the representation selection. And, if the authentication / representation selection was successful, the requested (encrypted) identifier(s) and attribute(s) of the EU and optionally the Represented Party. The identities and attributes are encrypted so that only the intended DV(s) can obtain the plain text value.

If the authentication or attempt to select representation was unsuccessful, it is indicated in the Status Code of the Response message and if possible, a reason is given so that the web service can inform the EU.

Step 12 & 13

Successful authentication / selection of representation gives the DV information needed for access control decision typically resulting in EU access to service in step 13.

§ 7.1.2 DV→RD - SAML messages

The SAML messages are specified in detail in the following sections. The following rules apply

> 1. The messages contain at least the elements that are specified as mandatory by the standard.
> 2. In addition, the messages also contain optional elements. It is indicated whether these elements are mandatory, conditional or optional. With optional elements, it is up to the participants to determine whether they are used.
> 3. Optional SAML elements that are not in this specification *SHOULD NOT* be included. When present they will be ignored when possible.

§ *7.1.2.1 DV→RD AuthnRequest*

When a principal (or an agent acting on the principal's behalf) wishes to obtain assertions containing authentication statements to establish a security context at one or more relying parties, it can use the authentication request protocol to send an AuthN Request message message element to a SAML authority and request that it returns a AuthN-Response message containing one or more such assertions.

§ 7.1.2.1.1 DV→RD AuthnRequest Diagram

The possible sender and recipient of the AuthnRequest message are the following:

Sender	Recipient
DV	RD
LC	RD

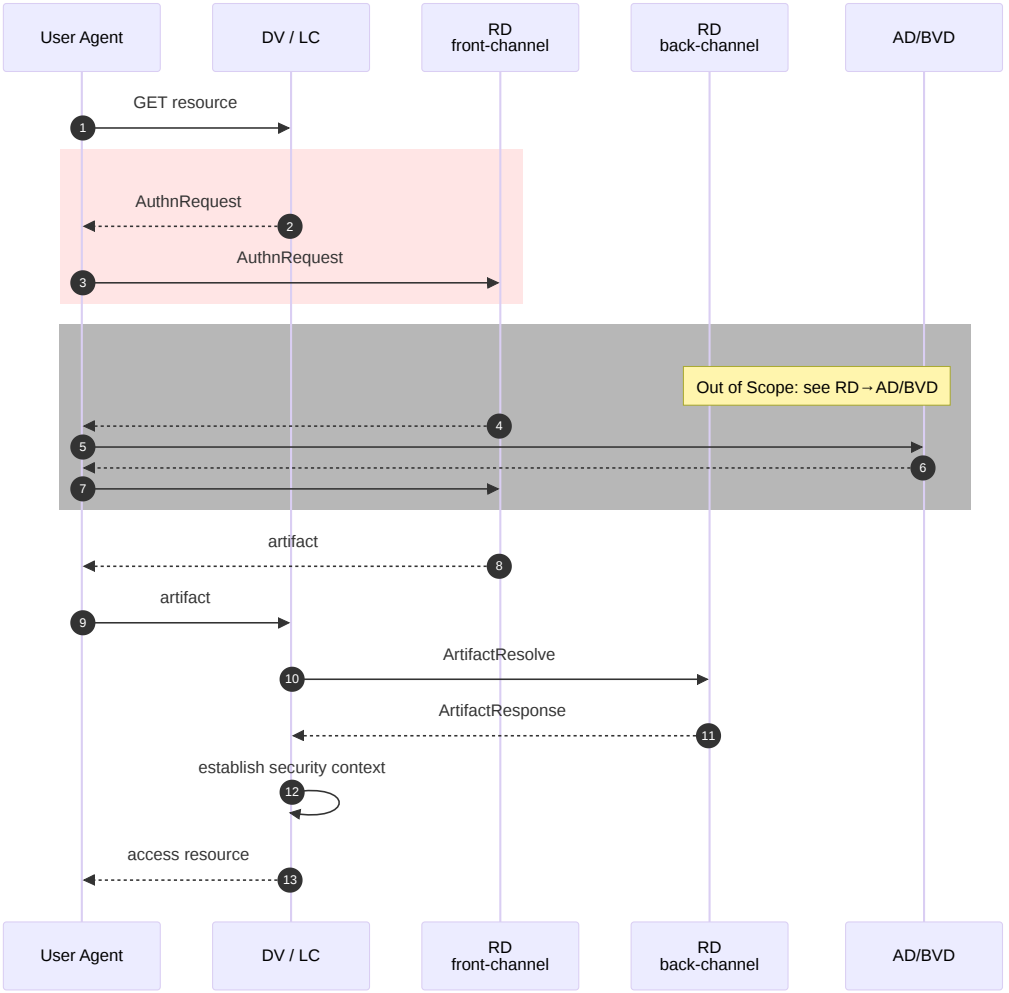

Figure 7 SAML authentication flow - DV/LC - RD - AuthN-Request

§ 7.1.2.1.2 DV→RD AuthnRequest Message

> See also Example AuthnRequest DV for RD

Element/@Attribute	0..n	Description Issuer = DV or LC Recipient = RD
@ID	1	Unique message identifier. *MUST* identify the message uniquely within the scope of the sender and receiver for a period of at least 12 months.
@Version	1	Version of the SAML protocol. The value *MUST* be `2.0`.
@IssueInstant	1	Time of issuing of the request.
@Destination	1	URL of the recipient on which the message is offered. *MUST* match SingleSignOnService in the metadata .
@ForceAuthn	0..1	The value `true` indicates that an existing SSO session *MUST NOT* be used for the request. If the value is `false` or empty or the attribute is missing, an existing SSO session *MAY* be used for the request.
@AssertionConsumerServiceIndex	1	This index *MUST* refer to an endpoint of an AssertionConsumerService in the issuer's metadata for the recipient. ***NOTE**: as a consequence, the `AssertionConsumerServiceURL` MUST NOT be included.*
@AttributeConsumingServiceIndex	0..1	Conditional. Only one of Extensions or @AttributeConsumingServiceIndex *MUST* be present.

Element/@Attribute	0..n	Description Issuer = DV or LC Recipient = RD
		***NOTE**: Also see the use of @AttributeConsumingServiceIndex and Extensions*
@ProviderName	0..1	Conditional. Reserved for use with eIDAS UIT to show information about the foreign DV and country in order to obtain EU consent. *SHOULD NOT* be used in other use cases and will be ignored if used.
Issuer	1	*MUST* contain the EntityID of the issuer as registered in the Metadata.
Signature	1	*MUST* contain the XML signature of the sender for the enveloped message. *MUST* contain a `KeyInfo` element with a `KeyName` or `X509Certificate` elements. See Signature
Extensions	0..1	Conditional. Only one of Extensions or AttributeConsumingServiceIndex *MUST* be present. And when `Extensions` is present, it *MUST* contain the attributes described below. ***NOTE**: Also see the use of @AttributeConsumingServiceIndex and Extensions*
-Attribute	1	An `Attribute` with the `@Name="urn:nl-eid-gdi:1.0:IntendedAudience"` *MUST* be present and contain an AttributeValue with the EntityID of the DV for which authentication is requested. ***NOTE**: (future) support for more than one audience where each audience receives the audience specific EncryptedID is provided by the Service Definition registered with the Service Catalog.*
-Attribute	1	An Attribute with the `@Name="urn:nl-eid-gdi:1.0:ServiceUUID"` *MUST* be present and contain an AttributeValue containing a `ServiceUUID` that is known at the Service Catalog of the receiving RD, AD and BVD.
-Attribute	0..1	Conditional. An `Attribute` with the `@Name="urn:nl-eid-gdi:1.0:IdpAssertion"`. ***NOTE**: This attribute MUST NOT be used (for DV→RD and LC→RD). See AuthN-Request differences for rules on using the Attribute with @Name="urn:nl-eid-gdi:1.0:IdpAssertion" for RD→AD/BVD*
Scoping	0..1	Conditional. Element *MAY* be used to limit the selection of AD's or BVD's at the RD. _**NOTE**: different rules for RD→AD/BVD, see AuthN-Request differences _
-IDPList	0..1	Conditional. List of IDP's - Element *MUST* be present in DV Authn-request message when Scoping element is present. ***NOTE**: MUST NOT be used for RD→AD/BVD, see AuthN-Request differences*
--IDPEntry	1..n	At least one IDPEntry (of an AD) *MUST* be present if the IDPList element is present. If no valid IDPEntry is present, the AuthnRequest will fail with a top level status code urn:oasis:names:tc:saml:2.0:status:Requester and second-level code depending on the condition according to [*SAML2.CORE*] section 3.2.2.2: urn:oasis:names:tc:SAML:2.0:status:NoSupportedIDP. If the list also contains the EntityID of a BVD. This indicates that representation using the BVD is optional in combination with the AD'(s) in the IDPList. The RD will let the EU choose whether to use representation with a BVD. The RD *MUST* limit the AD and BVD

Element/@Attribute	0..n	Description Issuer = DV or LC Recipient = RD
		selection list presented to EU's for AD's or combination of AD's and BVD's that are supported.
---@***ProviderID***	1	*MUST* contain the EntityID of a pre-selected AD or BVD
-***RequesterID***	0..n	Conditional. Element *MAY* be present if using authentication with representation. If used it *MUST* contain the EntityID of a BVD. If more than one RequesterID is included with different BVD's the RD *MUST* let the EU choose a BVD. If both RequesterID and IDPList are used, any BVD that is in a RequesterID *MUST* also be included in the IDPList. ***NOTE**: different rules for RD→AD/BVD, see AuthN-Request differences*

§ 7.1.2.1.2.1 The use of AttributeConsumingServiceIndex or Extensions for referring to service definitions

This specification uses the concept of a Service Catalog kept by RD, which contains amongst others `Service Definitions`. In the Service Catalog each '***Service Definition***' has a unique `ServiceUUID`. Each AuthN Request message must refer to a Service Definition using its `ServiceUUID`.

An AuthN Request message has two options for this `ServiceUUID` reference:

1. Only the DV *MAY* provide a `@AttributeConsumingServiceIndex` that *MUST* correspond to an `&#64;Index` attribute of an `AttributeConsumingService` entry in the DV Metadata. And this `AttributeConsumingService` entry *MUST* contain a **`ServiceUUID`**. When using the `AttributeConsumingServiceIndex` the RD will obtain the DV's EntityID from the `Issuer` element in the AuthN Request message.
2. Alternatively a DV *MAY* use the `Extensions` element in the AuthN Request message. All other Participants *MUST* use the `Extensions` element in the AuthN Request message. The `Extensions` element contains both the `EntityID` of the DV and the explicit **`ServiceUUID`**.

§ 7.1.2.1.3 DV→RD AuthnRequest Processing rules

In addition to the processing rules required by the SAML specification the following rule applies. If any of these validations fails, the authentication *MUST* fail:

1. RD *MUST* validate that the DV is registered for the requested ServiceUUID referenced by the index in the DV metadata or in the Extensions element of the DV AuthN-request and validate that the registration is valid;
2. IF an LC is involved THEN RD *MUST* validate that the DV is registered to use the requested ServiceUUID with the LC that sends the DV AuthN-Request message on behalf of the DV and that the registration is valid;

§ *7.1.2.2 DV←RD Artifact Binding*

The SAML response of a RD to a SAML request of a DV (or LC) uses an Artifact-Binding for extra security see [*SAML2.BINDINGS*] section 3.6.6. Therefor SAML Response does not return the actual SAML message with an Authentication Assertion but an Artifact as a reference to actual the SAML AuthN Response - Assertion message. The Artifact is used by the DV (or LC) to retrieve the SAML AuthN Response - Assertion at the RD.

§ 7.1.2.2.1 DV←RD - Artifact Binding - Diagram

The sender and recipient of this message are the following:

Sender	Recipient
RD	DV
RD	LC

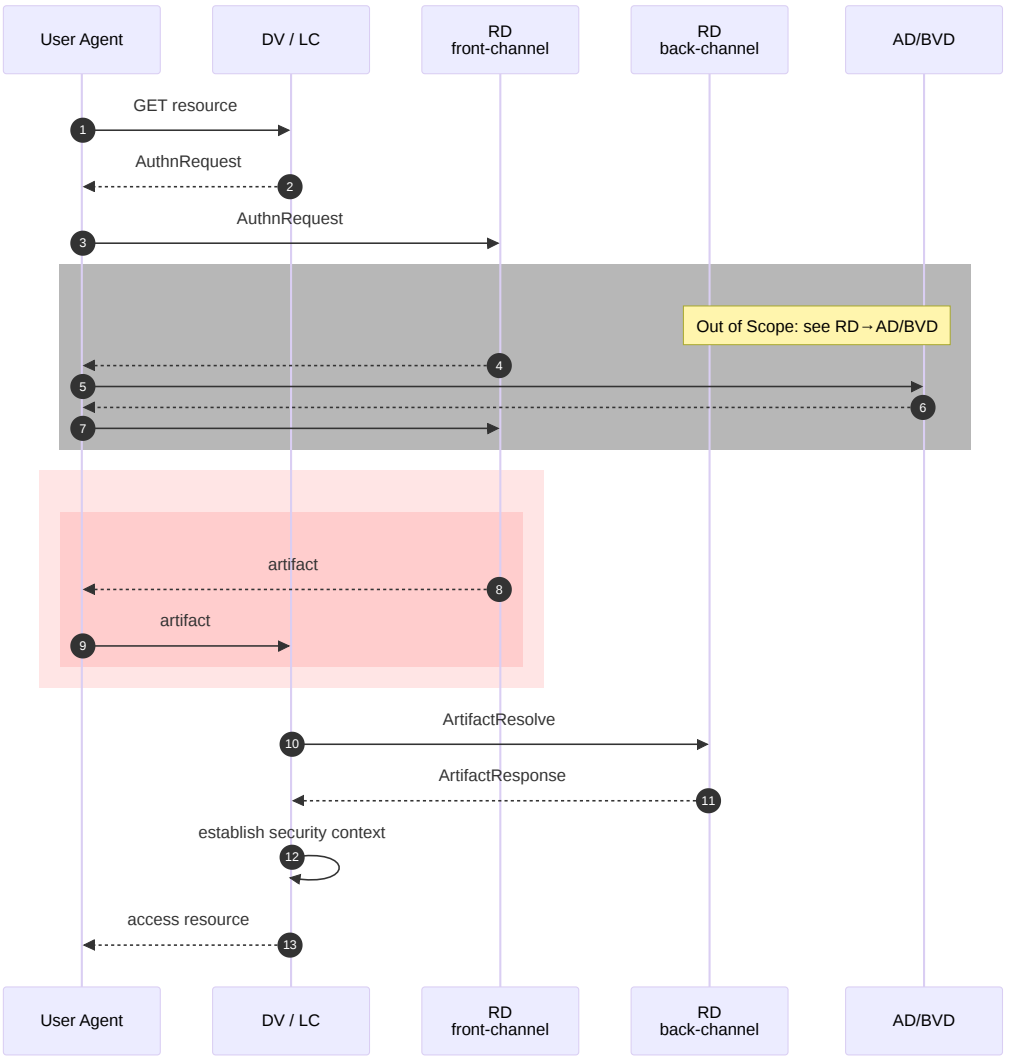

Figure 8 SAML authentication flow - DV/LC - RD - Artifact Response

§ 7.1.2.2.2 DV←RD - Artifact Binding - Message

The RD sends an Artifact via the Front channel to the DV/LC, using a HTTP-redirect of the webbrowser to the AssertionConsumerService referenced in the AuthN Request message.

> e.g. `https://dv.nl/SAML/ACS?SAMLart=AAQAAMh0dHA6Ly9pZHAuZXhhbXBsZS5jb20vU0FNTC9N&RelayState=xyz123`

The Artifact is only a reference to the SAML AuthN Response - Assertion. And even if no authentication has taken place, an Artifact will be send.

§ *7.1.2.3 DV→RD ArtifactResolve*

The DV/LC uses the Artifact to send an ArtifactResolve request to the RD via a SOAP binding over the Back channel. The Back channel is protected with two-sided TLS authentication.

§ 7.1.2.3.1 DV→RD ArtifactResolve Diagram

The sender and recipient of the Artifact Resolve are the following:

Sender	Recipient
DV	RD
LC	RD

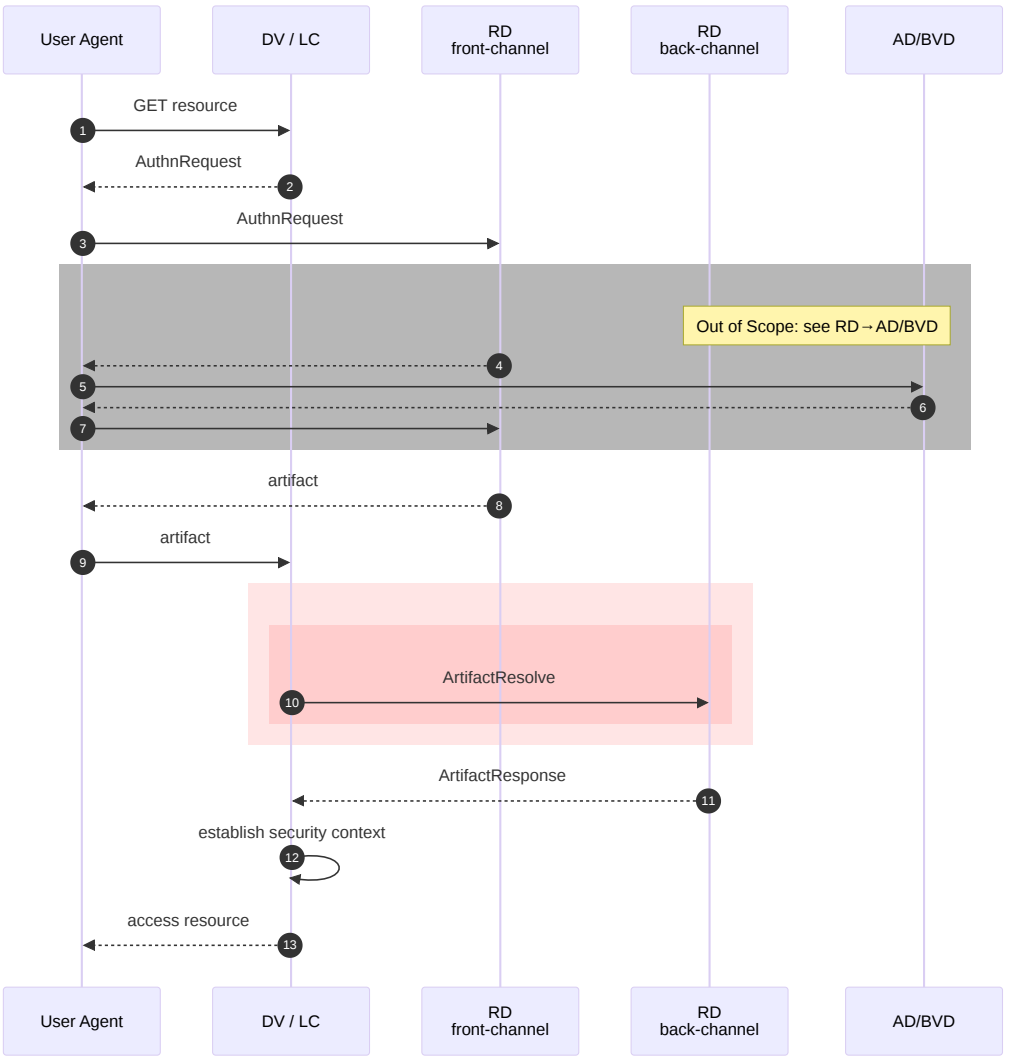

Figure 9 SAML authentication flow - DV/LC - RD - Artifact Resolve

§ 7.1.2.3.2 DV→RD ArtifactResolve Message

Element/@Attribute	0..n	Description
@ID	1	Unique message identifier. *MUST* identify the message uniquely within the scope of the sender and receiver for a period of at least 12 months.
@Version	1	Version of the SAML protocol. The value *MUST* be `2.0`.
@IssueInstant	1	Time at which the message was created.
@Destination	0..1	*MAY* be included. If included *MUST* contain the URL of the receiver on which the message is offered. *MUST* match one of the ArtifactResolutionService elements in the receiver's metadata.
Issuer	1	*MUST* contain the EntityID of the sender.

Element/@Attribute	0..n	Description
Signature	1	*MUST* contain the Digital signature of the sender for the enveloped message. *MUST* contain a `KeyInfo` element with either a `KeyName` or `X509Certificate` elements. See Signature.
Artifact	1	Contains the Artifact that was received as query parameter.

§ *7.1.2.4 DV←RD ArtifactResponse*

In response to the Artifact Resolve message, the RD will send an Artifact Response message back to the DV/LC via the SOAP binding over the Back channel. If successful this Artifact Response message contains the AuthN-Response Assertion for the original AuthN Request message.

§ 7.1.2.4.1 DV←RD ArtifactResponse Diagram

The sender and recipient of the Artifact Response message message are the following:

Sender	Recipient
RD	DV
RD	LC

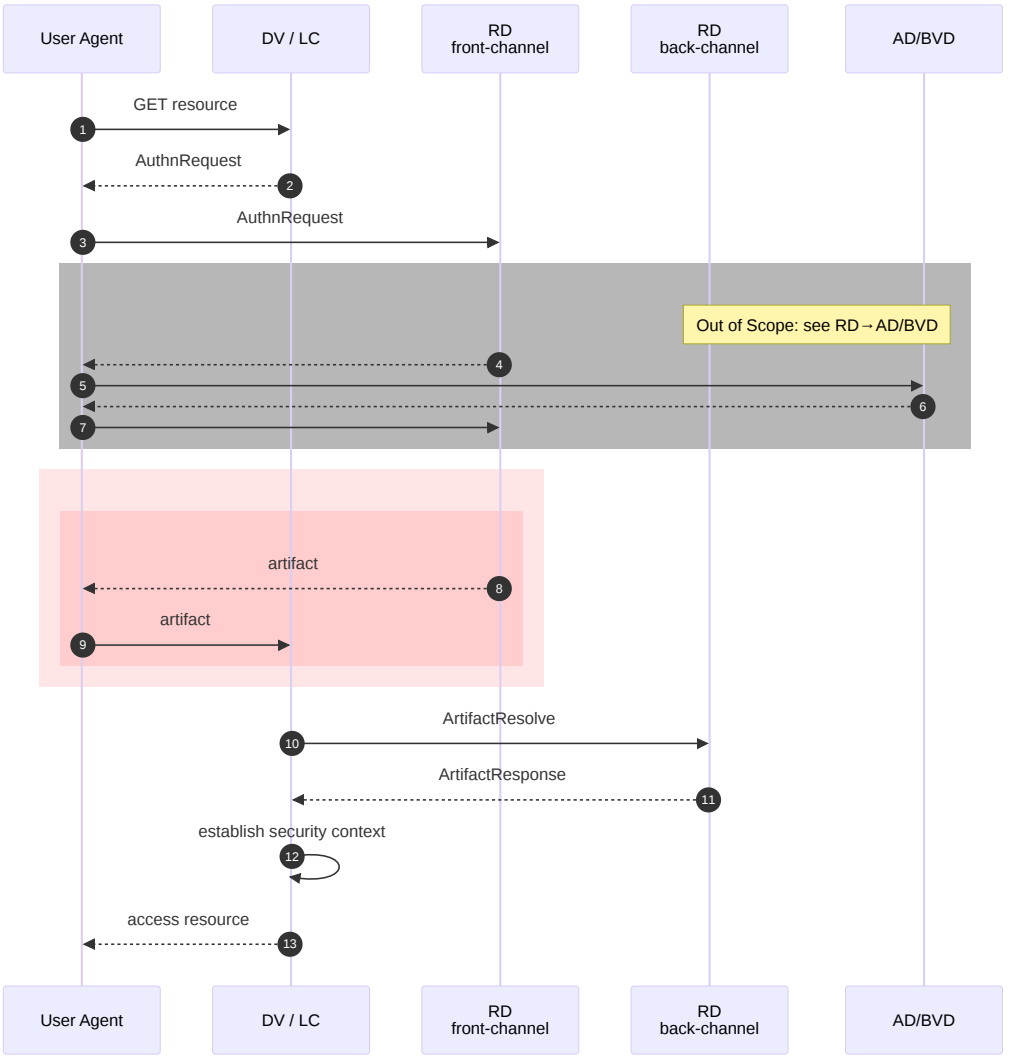

Figure 10 SAML authentication flow - DV/LC - RD - Artifact Response

§ 7.1.2.4.2 DV ← RD ArtifactResponse Message

Element/@Attribute	0..n	Description
@ID	1	Unique message identifier. *MUST* identify the message uniquely within the scope of the sender and receiver for a period of at least 12 months.
@InResponseTo	1	Unique ID attribute of the Artifact Resolve message request for which this ArtifactResponse message is the response.
@Version	1	Version of the SAML protocol. The value *MUST* be 2.0.
@IssueInstant	1	Time of issuing of the AuthN Response message.
Issuer	1	*MUST* contain the EntityID of the sender.
Signature	1	*MUST* contain the Digital signature of the sender for the enveloping message. *MUST* contain a KeyInfo element with a `KeyName` element. See Signature.
Status	1	*MUST* contain a StatusCode element with the status of the artifact resolve.
-StatusCode	1	*MUST* be present in a Status element.
-***@Value***	1	The Value of this StatusCode element *MUST* be from the top-level list provided in [*SAML2.CORE*] section 3.2.2.2 and follow the rules described in [*SAML2.BINDINGS*] section 3.6.6.
--StatusCode	0..1	Conditional. Should only be present if top-level StatusCode is not `urn:oasis:names:tc:SAML:2.0:status:Success`.
--***@Value***	1	If present *MUST* contain an URI reference indication details about the error.
-StatusMessage	0..1	Only present if top-level StatusCode is not `urn:oasis:names:tc:SAML:2.0:status:Success`. *MAY* contain a message detailing the error that occurred.
Response	0..1	Conditional. If the artifact resolves to a response this *MUST* contain the AuthN Response - Assertion to the AuthN Request message. The AuthN Response - Assertion is described below.

§ 7.1.2.4.2.1 Processing Rules for Status

Special processing rules for Status are described in [*SAML2.BINDINGS*] §3.6.6.

Even if the ArtifactResponse's Status indicates success it may still not contain a AuthN Response - Assertion conform [*SAML2.BINDINGS*] §3.6.6:

If the RD receives an Artifact Resolve message message that it can understand, it *MUST* return a AuthN Response message with a StatusCode value of urn:oasis:names:tc:SAML:2.0:status:Success`, even if it does not return the corresponding message (for example because the artifact requester is not authorized to receive the message or the artifact is no longer valid).

§ 7.1.2.4.3 DV ← RD AuthN Response - Message

Via the Artifact Response Message the RD sends the SAML AuthN-Response Message which is the response the original AuthN Request message of the DV/LC. The SAML AuthN-Response Message contains the AuthN Response - Assertion if authentication of the EU at the AD was successfull, and (when relevant) the BVD could establish a valid representation relationship.

Element/@Attribute	0..n	Description
@ID	1	Unique message characteristic. *MUST* identify the message uniquely within the scope of the sender and receiver for a period of at least 12 months.

Element/@Attribute	0..n	Description
@InResponseTo	1	Unique ID attribute of the AuthN Request message request for which this AuthN Response - Message is the response.
@Version	1	Version of the SAML protocol. The value *MUST* be 2.0.
@IssueInstant	1	Time of issuing of the AuthN Response - Assertion.
@Destination		URL of the endpoint on which the message is offered. *MUST* match a recipient's metadata AssertionConsumerService.
Issuer	1	*MUST* contain the EntityID of the sender.
Signature	0..1	*SHOULD NOT* be used as the AuthN Response - Assertion is part of the AuthN Response message messages which is already signed by RD. If included *MUST* contain the Digital signature of RD for the enveloping message. *MUST* contain a `KeyInfo` element with a `KeyName` or `X509Certificate` element.
Status	1	*MUST* contain a StatusCode element with the status of the authentication.
-StatusCode	1	*MUST* be present in a Status element.
-@Value	1	If not `urn:oasis:names:tc:SAML:2.0:status:Success` additional information *SHOULD* be provided in the embedded StatusCode element. The Value of this StatusCode element *MUST* be from the top-level list provided in SAML core section 3.2.2.2. See the codes listed in Error codes.
--StatusCode	0..1	Conditional. *SHOULD* only be present if top-level StatusCode is not `urn:oasis:names:tc:SAML:2.0:status:Success`.
--@Value	1	In the event of a cancellation or error, the element *MUST* be populated with the value `urn:oasis:names:tc:SAML:2.0:status:AuthnFailed`.
-StatusMessage	0..1	Only present if top-level StatusCode is not `urn:oasis:names:tc:SAML:2.0:status:Success`. *MAY* contain a message detailing the error that occurred, *MUST* contain exact phrase `Authentication cancelled` when authentication is cancelled (see also SAML Error codes)
Assertion	0..1	Conditional. *MUST* contain the AuthN Response - Assertion if the request was processed successfully (Status was `urn:oasis:names:tc:SAML:2.0:status:Success`). See AuthN Response - Assertion. Otherwise, *MUST* not be included.
EncryptedAssertion	0	*MUST NOT* be included.

§ 7.1.2.4.4 DV ← RD AuthN Response - Assertion

Element/@Attribute	0..n	Description
		Issuer = RD Recipient = DV or LC
@ID	1	Unique message identifier. *MUST* identify the message uniquely within the scope of the sender and receiver for a period of at least 12 months.
@Version	1	Version of the SAML protocol. The value *MUST* be `2.0`.
@IssueInstant	1	Time of issuanceing of the AuthN Response - Assertion.
Issuer	1	*MUST* contain the EntityID of RD.
Signature	1	*MUST* contain the Digital signature of the sender for the enveloped message. *MUST* contain a `KeyInfo` element with a `KeyName` element. See Signature.
Subject	1	*MUST* be included.
-NameID	1	NameID *MUST* contain a `TransientID`.
-SubjectConfirmation	1	Contains the SubjectConfirmation conform the WebSSO profile. See also: SubjectConfirmation.
Conditions	1	NotBefore and NotOnOrAfter limit the window during which the assertion can be delivered. See also: Conditions.
-@NotBefore	1	*MUST* be included.

Element/@Attribute	0..n	Description
-@***NotOnOrAfter***	1	*MUST* be included.
-***AudienceRestriction***	1	*MUST* be included.
--***Audience***	1..n	*MUST* contain an EntityID for all relevant parties that are intended to receive and process this assertion, as per SAML WebSSO profile. See below under Audience restriction)
AuthnStatement	1	*MUST* be included.
-@***AuthnInstant***	1	*MUST* contain the time of creation of the enclosing AuthN Response - Assertion.
-***SessionIndex***	0..1	Conditional, *MUST* contain the same TransientID as NameID. Is used to uniquely identify a session in case of a federated logout-request see Federated Logout-request message. ***NOTE****: For future proof better add SessionIndex element which will probably replace @NameID for LogOut request.*
-***AuthnContext***	1	*MUST* be included.
--***AuthnContextClassRef***	1	*MUST* contain the LoA at which authentication took place. Contains the obtained effective Level of assurance, see below under LoA. ***NOTE****: different rules for RD→AD/BVD*
--***AuthenticatingAuthority***	0..n	*MUST* contain the EntityID(s) of all authorities that were involved in the authentication and representation except for the assertion issuer.
AttributeStatement	0..1	Conditional. *MUST* be included if StatusCode is `urn:oasis:names:tc:SAML:2.0:status:Success`. *MUST NOT* be included otherwise. *MUST* contain a single attributestatement in accordance with the section Attributestatement below and the rules for processing an AuthN Response.
Advice	0..1	Conditional. *MUST NOT* be used for RD←AD/BVD. For DV/LC←RD *MUST* contain the original assertions received from the AD and BVD (if applicable) that were involved in processing the AuthN Request message. ***NOTE****: different rules for RD←AD/BVD*
-***Assertion***	1..n	Contains the original Assertion elements this assertion is composed of: *MUST* contain the original AD Assertion. *MAY* contain the original Assertion of the BVD in case of representation.

§ 7.1.2.4.4.1 Audience restriction - DV

The AudienceRestriction element in the AuthN Response - Assertion must be checked in terms of content. An AuthN Response - Assertion may only be processed if the AudienceRestriction contains the EntityID of the recipient.

> The values for DVs included in Audience are reflected in the Recipient attribute of the EncryptedID element in the Attributestatement. This does not apply to the LC or RD that is only included in the AudienceRestriction. The LC or RD is not, after all, an entity which may receive identities.

§ 7.1.2.4.4.2 Level of assurance validation

The AuthnContextClassRef in the AuthN Response - Assertion always states the authentication level at which the citizen has authenticated himself. DV's *MUST* be prepared for the AuthnContextClassRef to contain a higher LoA than the requested LoA. DV's *MUST* accept authentications with a level equal to or higher than the minimum level registered for the Service in the Service Catalog. DV must configure minimum LoA for the Service when providing information in the onboarding process. The AD is responsible for providing the correct LoA for a given authentication request (equal to or higher than the LoA registered for the Service in the Service Catalog)

§ 7.1.2.4.4.3 SubjectConfirmation - DV

The SubjectConfirmation exists in a Subject and is used to hold a bearer confirmation in a AuthN Response - Assertion to an AuthN Request message, to conform to the WebSSO profile. In case a relying party is requesting authentication of an EU according to the SAML Web SSO profile, a bearer SubjectConfirmation (see [*SAML2.PROFILES*], §3.3 and §4.1.4) must be provided. The NotOnOrAfter in the SubjectConfirmationData element limits the time during which the AuthN Response - Assertion result *MAY* be used to establish an authenticated session for the EU using the AuthN Response - Assertion. The NotOnOrAfter is initially set to +2 minutes relative to the time of issuance of the enclosing AuthN Response - Assertion. These values can be changed however in time. The `dv-authn-response-assertion/NotBefore` attribute *MUST NOT* be used.

Element/@Attribute	0..n	Description
SubjectConfirmation	1	Allows for association of client with assertion to conform to the SAML Web SSO profile.
-***@Method***	1	*MUST* contain the value `urn:oasis:names:tc:SAML:2.0:cm:bearer`.
-***SubjectConfirmationData***	1	*MUST* be included.
--***@NotOnOrAfter***	1	A time instance at which the subject can no longer be confirmed.
--***@Recipient***	1	The assertion consumer Service URL of the immediate requester to which an attesting entity can present the assertion.
--***@InResponseTo***	1	The ID of the AuthN Request message this AuthN Response - Assertion is in response to.

§ 7.1.2.4.4.4 Conditions

The NotBefore and NotOnOrAfter in the Conditions element limit the time during which the AuthN Response - Assertion is considered valid within a prior established authenticated EU session based on this AuthN Response - Assertion. The value of these attributes should be aligned with the maximum session duration (which may be dependent on the LoA) and typically is much longer than the validity of the SubjectConfirmation .

§ 7.1.2.4.5 AttributeStatement - DV

The AuthN Response - Assertion when present *MUST* contain an attributestatement. An attributestatement contains one or more Attribute elements and *MUST* contain exactly one Attribute with `@Name="urn:nl-eid-gdi:1.0:ActingSubjectID"`. It *MAY* contain exactly one Attribute element with `@Name="urn:nl-eid-gdi:1.0:LegalSubjectID"` indicating representation. Both ActingSubjectID and LegalSubjectID Attributes *MUST* contain one or more AttributeValues for one or more Recipients (e.g. DV). And these Recipients must be included in the AudienceRestriction element.

Element/@Attribute	0..n	Description
AttributeStatement	1	*MUST* be included.
-***Attribute***	1..n	See the tables below for details.
--***@Name***	1	*MUST* contain the type of the attribute.
--***AttributeValue***	1..n	The Attribute *MUST* contain one or more AttributeValues.

§ 7.1.2.4.6 EncryptedID

Both ActingSubjectID as LegalSubjectID (Attribute with `@Name="urn:nl-eid-gdi:1.0:ActingSubjectID"` respectivly `@Name="urn:nl-eid-gdi:1.0:LegalSubjectID"`) are unencrypted Attributes and *MUST* contain one or more AttributeValues. Each of these AttributeValues *MUST* contain exactly one EncryptedID element.

Element/@Attribute	0..n	Description
EncryptedID	1	*MUST* contain one encrypted `NameID` element. See below for details.
-EncryptedData	1..n	*MUST* contain the encrypted data containing the XML encrypted `NameID` which contains the identity.
-EncryptedKey	1..n	*MUST* contain the wrapped decryption keys, as defined by [*XML.ENC*]. This element *MUST* include the intended Recipient
--@Recipient	1	The recipient for which this EncryptedID is intended. This attribute *MUST* contain an EntityID.

See also: Example EncryptedID

§ 7.1.2.4.6.1 NameID - after decrypting EncryptedID

An EncryptedID *MUST* contain a SAML `NameID` after decryption, with the following properties:

- The `@Format` attribute *MUST* be set to `urn:oasis:names:tc:SAML:2.0:nameid-format:persistent`.
- The `@NameQualifier` attribute *MUST* be populated with the full name of the type of identifying attribute (see Attribute Identifier Types for the `@NameQualifier` types).
- The attributes `@SPNameQualifier` and `@SPProvidedID` *MUST NOT* be used.
- In case more than one certificate is listed for encryption for the recipient in the metadata, the content-encryption-key *MUST* be encrypted for each certificate. This will result in multiple EncryptedKey each with the same Recipient.

See also: Example NameID (after decryption)

§ 7.1.2.4.6.2 Multiple recipients

SAML and XML-encryption allow for multiple recipients of the same encrypted element. The construct for this is specified in more detail in errata E43 of [*SAML2.ERRATA.05*]. In case of multiple recipients:

- each EncryptedKey *MUST* have a `CarriedKeyName` equal to the `KeyName` used in the `KeyInfo` of the EncryptedData.
- each EncryptedKey *SHOULD* have a `ReferenceList` referring back to the data encrypted with the symmetric key contained.

Upon decryption, elements without an EncryptedKey intended for the decrypting recipient *MAY* be ignored and EncryptedKey for other recipients of encrypted elements *SHOULD* be ignored.

> **NOTE:**
> When copying encrypted XML elements (EncryptedID) to create a summary declaration RD substitutes XML identifiers for the EncryptedID's with a unique identifier. This *MAY* be accomplished by pre- or suffixing the original identifier in the copy.
>
> > Rationale: `@ID` values must uniquely identify the elements which bear them. Identifiers that appear in the summary assertion and also in the advice assertion(s) will break XML validation.
>
> If the type of identity is `urn:nl-eid-gdi:1.0:id:legacy-BSN`, only one EncryptedData element *MUST* be used in combination with one or more EncryptedKey elements (one for each recipient).
>
> Because a polymorphic identity or pseudonym of a single person will be distinct for different recipients by design, a single EncryptedData element cannot be used when encryption for multiple recipients is required. Therefore, for each recipient, one EncryptedData element paired with one EncryptedKey element *MUST* be used.
>
> Although a LC or RD may be an Audience as it will process the SAML Assertion, it is not a Subject Confirmation - @Recipient and will not be able to decrypt EncryptedID's.

§ *Generic attributes*

In all cases the following attributes will be provided as an unencrypted Attribute.

Attribute	1..n	Attribute Name	Description
ServiceUUID	1	Name="urn:nl-eid-gdi:1.0:ServiceUUID"	
-AttributeValue	1..n		The ServiceUUID of the Service Catalog for which this Assertions is intended as indicated in the AuthN Request message. In case of legal representation the ServiceUUID will be a copy of Attribute in AuthN Request message

§ *Attribute types in case of legal representation*

In case of legal representation, via BVD the following attribute will be provided as an unencrypted Attribute.

Type	1..n	Attribute Name	Description
RepresentationType	0-1	Name="urn:nl-eid-gdi:1.1:RepresentationType"	Optional for DigiD Machtigen, required for any type of legal representation by the BVD
-AttributeValue	1..n		The type of representation , to be used by Service Provider DV for access decision multiple values of Legal Representation allowed.

§ *Attribute types in case of authentication*

In case of authentication the following attributes will be provided as EncryptedID.

Attribute	1..n	Attribute Name	Description
ActingSubjectID	1	Name="urn:nl-eid-gdi:1.0:ActingSubjectID".	
-AttributeValue	1..n		All contain identities of the same EU.

§ *Attribute types issuer in case of representation*

In case of representation the following attributes will be provided as EncryptedID

Type	1..n	Attribute Name	Description
ActingSubjectID	1	Name="urn:nl-eid-gdi:1.0:ActingSubjectID"	Identity of the EndUser (EU)
-AttributeValue	1..n		The (encrypted) ActingSubjectID as received from the AD at which the EU was authenticated. All contain identities of the same EU.
LegalSubjectID	1	Name="urn:nl-eid-gdi:1.0:LegalSubjectID"	Identity of the Represented Party
-AttributeValue	1..n		The (encrypted) LegalSubjectID as received from BVD.

Type	1..n	Attribute Name	Description
			All contain identities of the same Represented Party.

§ *Attribute type conversion eTD*

In case of authentication with eTD the following Attributes will be provided as EncryptedID

Type	1..n	eTD Name	ST-SAML Name	Description
Attribute	0..1	urn:etoegang:core:ActingSubjectID	urn:nl-eid-gdi:1.0:ActingSubjectID	Identity of the EndUser (EU)
-- AttributeValue	1..n			All contain identities of the same EU.
Attribute	0..1	urn:etoegang:core:LegalSubjectID	urn:nl-eid-gdi:1.0:LegalSubjectID	Identity of the Represented Party
-- AttributeValue	1..n			All contain identities of the same Represented Party.

Other scenario's (e.g. support for IntermediarySubjectID) are not yet supported and may be added in future iterations of this specification. Attributes from eTD as included in the HM summary assertion will be copied unaltered into the AttributeStatement of the RD. They may contain either EncryptedID or EncryptedAttribute elements. See https://afsprakenstelsel.etoegang.nl/Startpagina/as/attribuutcatalogus

§ Example Attribute Statement for Legal Representation

```
<saml2:AttributeStatement>
    <saml2:Attribute Name="urn:nl-eid-gdi:1.1:RepresentationType">
         <saml2:AttributeValue>urn:nl-eid-gdi:1.1:RT:Zorg_Volledig_Gezag_Kind</saml2:Attribu
    </saml2:Attribute>
    …
    <saml2:Attribute Name="urn:nl-eid-gdi:1.0:ActingSubjectID">
        <saml2:AttributeValue>
            // EncryptedID with BSN of ActingSubject (ouder/voogd)
       </saml2:AttributeValue>
    </saml2:Attribute>
    <saml2:Attribute Name="urn:nl-eid-gdi:1.0:LegalSubjectID">
        <saml2:AttributeValue>
            // EncryptedID with BSN LegalSubject (kind)
       </saml2:AttributeValue>
    </saml2:Attribute>
</saml2:AttributeStatement>
```

§ Example EncryptedID

```
<saml2:EncryptedID xmlns:saml2="urn:oasis:names:tc:SAML:2.0:assertion"
     xmlns:xenc="http://www.w3.org/2001/04/xmlenc#"
     xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
    <xenc:EncryptedData
        xmlns:xenc="http://www.w3.org/2001/04/xmlenc#"
        Id="_cd52e15a16e2a0aa751725ce76a6b866"
        Type="http://www.w3.org/2001/04/xmlenc#Element">
        <xenc:EncryptionMethod
            Algorithm="http://www.w3.org/2001/04/xmlenc#aes256-cbc"
```

```
            xmlns:xenc="http://www.w3.org/2001/04/xmlenc#"/>
        <ds:KeyInfo xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
            <ds:RetrievalMethod
                Type="http://www.w3.org/2001/04/xmlenc#EncryptedKey"
                URI="#_15531f77a9f1e0b5e0cce442aa31bbd4" />
        </ds:KeyInfo>
        <xenc:CipherData xmlns:xenc="http://www.w3.org/2001/04/xmlenc#">
            <xenc:CipherValue>AZkW3hbBaQkxs...</xenc:CipherValue>
        </xenc:CipherData>
    </xenc:EncryptedData>
    <xenc:EncryptedKey xmlns:xenc="http://www.w3.org/2001/04/xmlenc#"
        Id="_449673558dd0810e91009297f56fd051"
        Recipient="urn:nl-eid-gdi:1.0:DV:00000009999999999004:entities:0000">
        <xenc:EncryptionMethod
            Algorithm="http://www.w3.org/2001/04/xmlenc#rsa-oaep-mgf1p"
            xmlns:xenc="http://www.w3.org/2001/04/xmlenc#">
            <ds:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1" />
        </xenc:EncryptionMethod>
        <ds:KeyInfo xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
            <ds:KeyName>...</ds:KeyName>
        </ds:KeyInfo>
        <xenc:CipherData xmlns:xenc="http://www.w3.org/2001/04/xmlenc#">
            <xenc:CipherValue>yRy923JJlgAi2MTgx1qohLiDBgi...</xenc:CipherValue>
        </xenc:CipherData>
        <xenc:ReferenceList>
            <xenc:DataReference URI="#_cd52e15a16e2a0aa751725ce76a6b866" />
        </xenc:ReferenceList>
    </xenc:EncryptedKey>
</saml2:EncryptedID>
```

§ Example nameID (after decryption)

```
<saml2:NameID
    xmlns:saml2="urn:oasis:names:tc:SAML:2.0:assertion"
    Format="urn:oasis:names:tc:SAML:2.0:nameid-format:persistent"
    NameQualifier="urn:nl-eid-gdi:1.0:id:legacy-BSN">999999047</saml2:NameID>
```

§ *DV←RD AuthN Response - Message processing rules for DV*

Regardless of the SAML binding used, the service provider *MUST* do the following:

1. Verify any signatures present on the AuthN Response - Assertion or the AuthN Response - Assertion.
2. Verify that the **dv-subjectconfirmation/@Recipient** attribute in any bearer Subject Confirmationdata matches the assertion consumer service URL to which the AuthN Response - Assertion or Artifact was delivered.
3. Verify that the @NotOnOrAfter attribute in any bearer Subject Confirmationdata has not passed, subject to allowable clock skew between the providers.
4. Verify that the @InResponseTo attribute in the bearer Subject Confirmationdata equals the @ID of its original AuthN Request message message.
5. Verify that it's EntityID is included as Audience in the AuthN Response - Assertion.
6. Verify that any assertions relied upon are valid in other respects.
7. Any assertion which is not valid, or whose subject confirmation requirements cannot be met *SHOULD* be discarded and *SHOULD NOT* be used to establish a security context for the principal.

§ 7.2 RD - SAML Message specification

7.2.1 RD→AD - SAML authentication proces

SAML authentication between RD and AD or BVD are described in this chapter. The RD→AD/BVD SAML messages are almost identical to the SAML messages of DV/LC→RD - SAML authentication. Therefor only a reference to the appropriate DV/LC→RD - SAML messages will be given and the differences described.

7.2.1.1 RD→AD - Authentication - diagram

The diagram below depicts the flow between a RD and an AD/BVD. The encompassing flow, between DV/LC and RD, is out of scope (see [[*eID SAML4.4*]] for details).

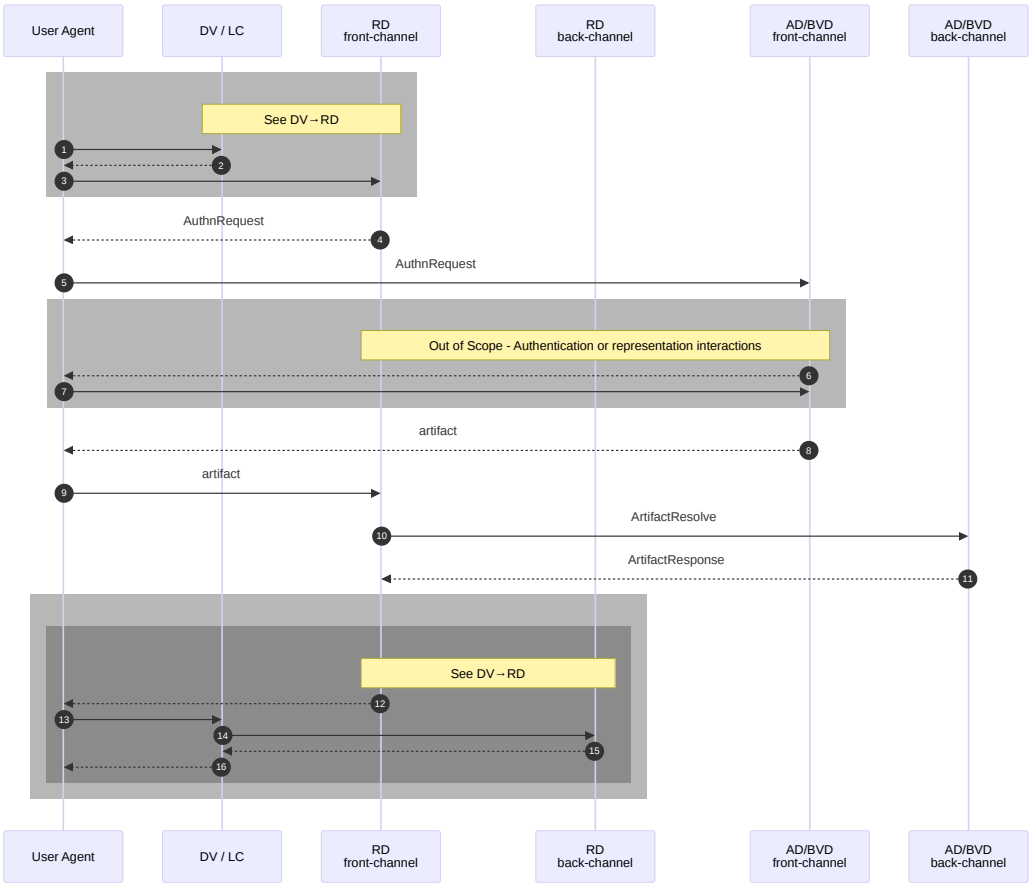

Figure 11 SAML authentication flow RD - AD/BVD

7.2.1.2 RD→AD - Authentication - steps

Step 1, 2 and 3 (out of scope for this specification)

For messages between AD and RD see DV-RD authentication diagram

Step 4 and 5

The RD will send the EU to an AD for authentication or to a BVD for proof of representation (or both).

Step 6 and 7 (out of scope for this specification)

In these steps the EU interacts with an AD or aBVD .

Step 8 and 9

The AD/BVD sends the EU back to the RD via a browser redirect. An opaque Artifact generated by AD/BVD is send here in the Artifact Response message. The Artifact refers to the actual SAML response message that is waiting at AD/BVD.

Even if the interactions in step 6 and 7 were unsuccessful or cancelled, an Artifact is send to the RD. This Artifact provides an error message with the Artifact Resolve message and cannot be exchanged for a valid Assertion.

Step 10

With the Artifact the result of the (successful or unsuccessful) authentication or representation can be retrieved from the Back channel.

An Artifact Response message is valid for a maximum of 15 minutes and can only be retrieved once by the RD. Situations are possible (process breakdown, early logout) where an Artifact is valid less than 15 minutes.

Step 11

AD/BVD replies with an Artifact Response message that belongs to the Artifact. In this message, AD/BVD provides an Assertion that includes the authentication result or the proof of representation. And, if the authentication / representation selection was successful, the requested (encrypted) identifier(s) and attribute(s) of the EU or the Represented Party. The identities and attributes are encrypted so that only the intended DV(s) can obtain the plain text value.

If the authentication or attempt to select representation was unsuccessful, it is indicated in the Status Code of the Response message and if possible, a reason is given so that the DV can inform the EU.

§ *7.2.1.3 RD→AD/BVD ArtifactResolve*

Step 12, 13, 14 and 15 (out of scope for this specification)

For messages between AD and RD see DV-RD authentication diagram

§ **7.2.2 RD→AD - SAML messages**

> 1. The messages contain at least the elements that are specified as mandatory by the standard.
> 2. In addition, the messages also contain optional elements. It is indicated whether these elements are mandatory, conditional or optional. With optional elements, it is up to the participants to determine whether they are used.
> 3. Optional SAML elements that are not in this specification *SHOULD NOT* be included. When present they will be ignored when possible.

§ *7.2.2.1 RD→AD AuthnRequest*

When a principal (or an agent acting on the principal's behalf) wishes to obtain assertions containing authentication statements to establish a security context at one or more relying parties, it can use the authentication request protocol to send an AuthN Request message message element to a SAML authority and request that it returns a AuthN-Response message containing one or more such assertions.

§ 7.2.2.1.1 RD→AD AuthnRequest Diagram

The possible sender and recipient of the AuthnRequest message are the following:

Sender	Recipient
RD	AD
RD	BVD

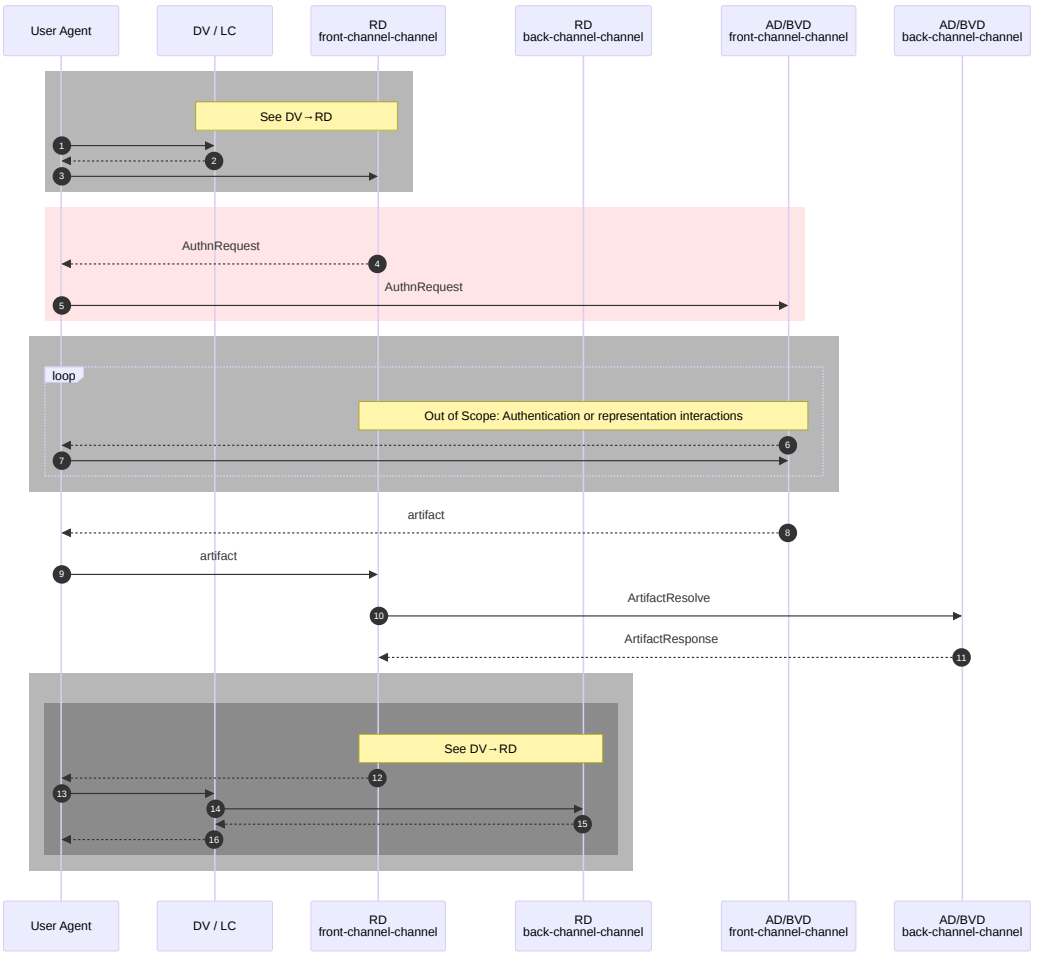

Figure 12 SAML authentication flow - RD - AD/BVD - AuthN-Request

§ 7.2.2.1.2 RD→AD AuthnRequest Message

> See also Example AuthnRequest with representation from RD to AD

> For message specification see DV/LC→RD - AuthN-Request Message

§ 7.2.2.1.3 AuthN-Request differences between DV/LC→RD, RD→AD and RD→BVD

Element/@Attribute	DV / LC→RD	RD→AD	RD→BVD
AttributeConsumingServiceIndex	If present, Extensions *MUST NOT* be present. Forbidden for LC	*MUST* not be present (ignored)	*MUST* not be present (ignored)
Extensions	If present, AttributeConsumingServiceIndex *MUST NOT* be present. Mandatory for LC	Mandatory	Mandatory
-Attribute with `@Name="urn:nl-eid-gdi:1.0:IntendedAudience"`	Mandatory if Extensions is present	Mandatory	Mandatory
-Attribute with `@Name="urn:nl-eid-gdi:1.0:IdpAssertion"`	*MUST NOT* be present (ignored)	*MUST NOT* be present (ignored)	*MUST* be present and contain an AttributeValue holding

Element/@Attribute	DV / LC→RD	RD→AD	RD→BVD
			an Assertion received from a compliant AD.
Scoping -RequesterID	Optional	Optional	*MUST NOT* be present (ignored)

§ 7.2.2.1.4 RD→AD AuthnRequest Processing rules

In addition to the processing rules required by the SAML specification the following rule applies. If any of these validations fails, the authentication *MUST* fail: 1. AD *MUST*:

- validate that the DV is registered for the requested ServiceUUID referenced by the index in the DV metadata or the Extensions element of the DV AuthN-request and that the registration is valid;
- (in case when an LC is involved) validate that the DV is registered to use the requested ServiceUUID with the LC that sends the AuthN Request Message on behalf of the DV and that the registration is valid;
- If any of these validations fails, the authentication *MUST* fail.

1. AD BVD *MUST* validate that the DV is registered for the requested ServiceUUID referenced by the index in the DV metadata or the Extensions element of the DV AuthN-request and that the registration is valid;

§ *7.2.2.2 RD←AD Response - Artifact Binding*

The SAML response of a AD or BVD to a SAML request of a RD uses an Artifact-Binding for extra security see [*SAML2.BINDINGS*] section 3.6.6. Therefor SAML Response does not return the actual SAML message with an Authentication Assertion but an Artifact as a reference to actual the SAML AuthN Response - Assertion message. The Artifact is used by the DV (or LC) to retrieve the SAML AuthN Response - Assertion at the RD.

§ 7.2.2.2.1 RD←AD Response - Artifact Binding - Diagram{#rd-response-artifact-binding}

The possible sender and recipient of the AuthnRequest message are the following:

Sender	Recipient
AD	RD
BVD	RD

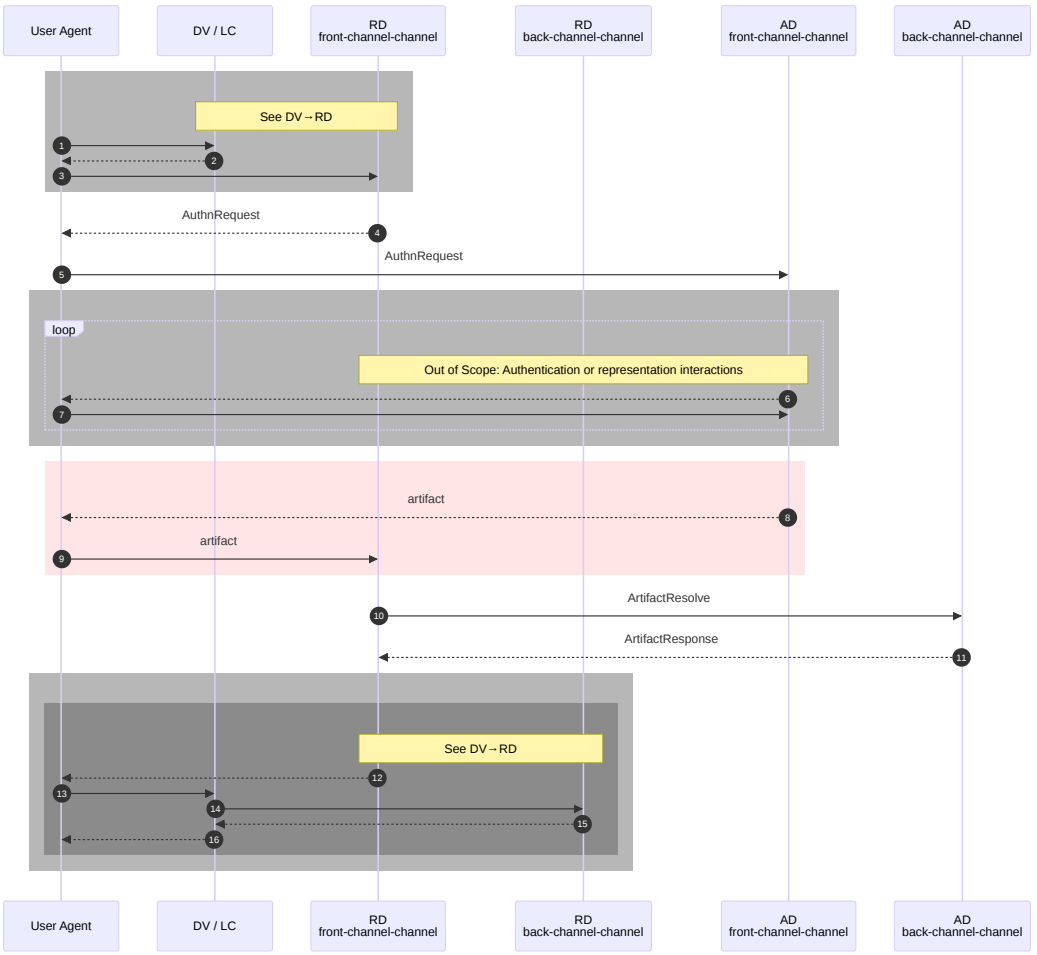

Figure 13 SAML authentication flow - RD - AD/BVD Artifact Binding

§ 7.2.2.2.2 RD ← AD Response - Artifact Binding - Message

The receiver of the previous AuthN Request message sends a SAML Artifact message via the front channel by a redirect to the AssertionConsumerService referenced in the AuthN Request message. An Artifact is a reference to the SAML AuthN Response - Assertion message. Even if no authentication has taken place, an Artifact will be send. The Artifact message is send to the recipient via an HTTP Redirect. The Artifact is used by the receiver to retrieve the SAML AuthN Response - Assertion at the sender.

§ *7.2.2.3 RD → AD ArtifactResolve*

§ 7.2.2.3.1 RD → AD ArtifactResolve Diagram

The Artifact Resolve request is send via a SOAP binding over the Back channel. The back channel is protected with two-sided TLS authentication. The receiver will return an AuthN Response message in the response message. The sender and recipient of the Artifact Resolve are the following:

Sender	Recipient
RD	AD
RD	BVD

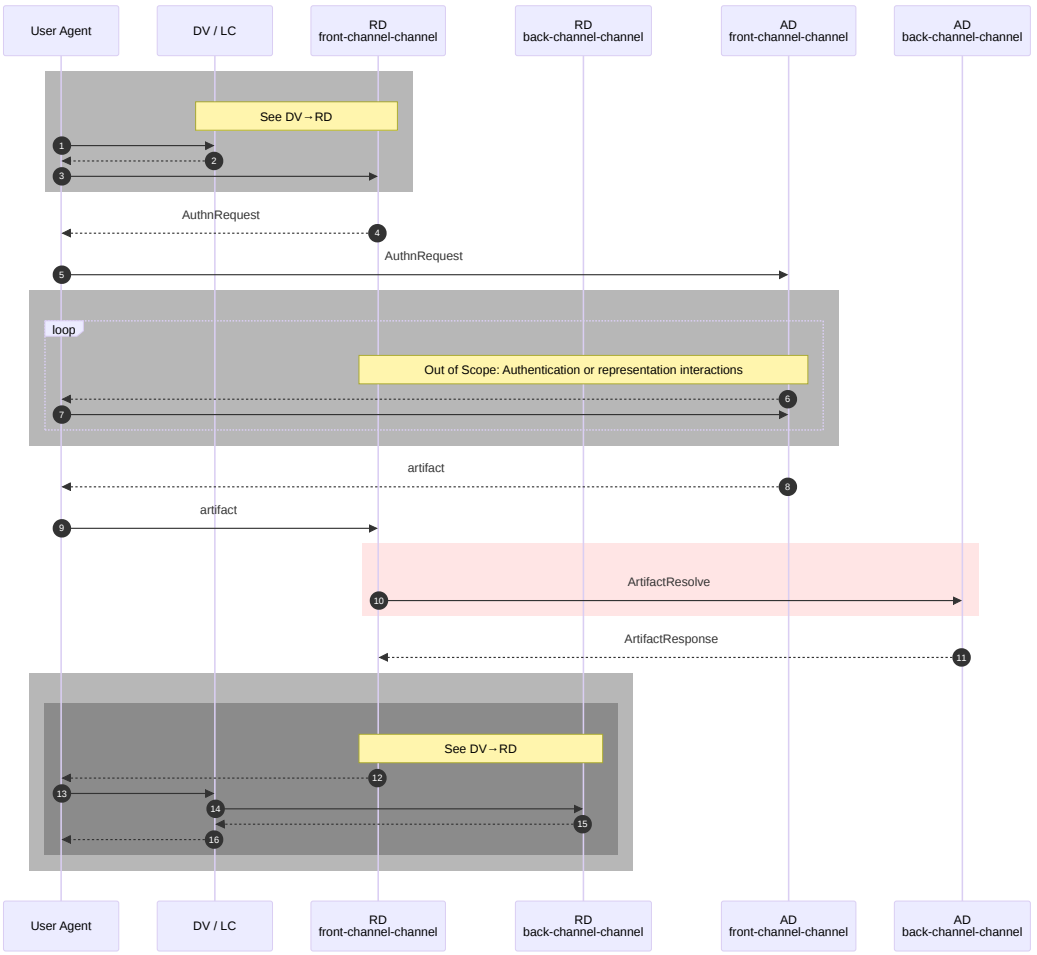

Figure 14 SAML authentication flow - RD - AD/BVD Artifact Resolve

§ 7.2.2.3.2 RD→AD ArtifactResolve Message

> For message specification see DV/LC→RD - ArtifactResolve Message

§ *7.2.2.4 RD→AD ArtifactResponse*

The AuthN Response message contains the response message to the Artifact Resolve request in a SOAP message. This response message in turn contains the AuthN Response - Assertion to the Original AuthN Request message. The sender will send the AuthN Response message in response to an Artifact Resolve request. If successful it contains the AuthN Response - Assertion to the AuthN Request message.

§ 7.2.2.4.1 RD←AD ArtifactResponse Diagram

The sender and recipient of the Artifact Response are the following:

Sender	Recipient
AD	RD
BVD	RD

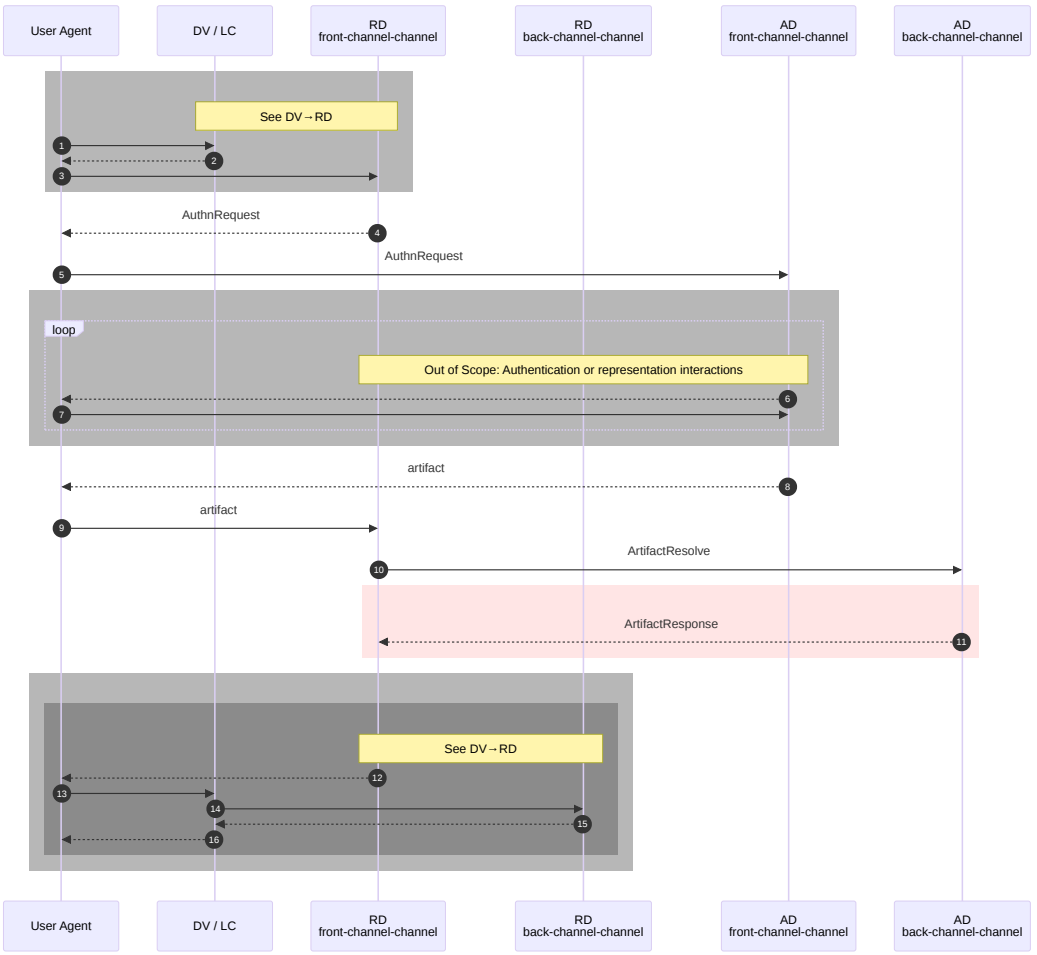

Figure 15 SAML authentication flow - RD - AD/BVD Artifact Response

§ 7.2.2.4.2 RD ← AD Artifact Response Message

> For message specification see DV/LC ← RD - ArtifactResponse Message

§ 7.2.2.4.3 RD ← AD AuthN Response - Message

The SAML Response Message to the AuthN Request message contains the authentication assertion if authentication was successful.

> For message specification see DV/LC ← RD - AuthN Response - Message

§ 7.2.2.4.4 RD ← AD AuthN Response - Assertion

> For Assertion specification see DV/LC ← RD - AuthN Response - Assertion

> For AttributeStatement specification see DV/LC ← RD - AuthN Response - AttributeStatement

§ 7.2.2.4.5 Assertion and AttributeStatement differences between DV/LC←RD and RD←AD/BVD

Element/@Attribute	DV / LC←RD	RD←AD	RD←BVD
Conditions -AudienceRestriction --Audience	*MUST* contain EntityID of DV and (if applicable) LC.	*MUST* contain EntityID of RD and (in case of representation)BVD .	*MUST* contain EntityID of RD.
AuthnStatement -AuthnContext --AuthnContextClassRef	*MUST* be present.	*MUST* be present.	*MUST* be `urn:oasis:names:tc:SAML:2.0:ac:classes:unsp`
--AuthenticatingAuthority	*MUST* contain the EntityID of AD and (in case of representation respectively legal representation) BVD-DDM or BVD-OG.	*MUST NOT* be present.	*MUST NOT* be present.
attributestatement -attribute with Name="urn:nl-eid-gdi:1.0:ActingSubjectID"	*MUST* be present and *MUST* be decipherable for DV.	*MUST* be present and *MUST* be decipherable for DV and (in case of representation respectively legal representation) BVD-DDM or BVD-OG.	*MUST* be present and *MUST* be decipherable for DV.
attributestatement -attribute with [=dv-attributestatement/=Name=]="urn:nl-eid-gdi:1.0:LegalSubjectID"	In case of representation *MUST* be present and *MUST* be decipherable for DV.	*MUST NOT* be present.	*MUST* be present and *MUST* be decipherable for DV.
attributestatement -attribute with Name="urn:nl-eid-gdi:1.1:RepresentationType"	In case of legal representation *MUST* be present and *MUST* be used by DV when deciding on access.	*MUST NOT* be present.	*MUST* be present
Advice	*MUST* be present.	*MUST NOT* be present.	*MUST NOT* be present.

§ 7.3 Federated Logout Message specification

§ 7.3.1 DV→RD login & logout

> **NOTE**
> Support for federated login and logout may be subject to change in future versions of this specification. DV/LCs which decide to make use of federated login and logout, as supported by this version of the specification, must be prepared to make all the necessary changes to their use of federated login and logout as soon as a later version of the specification mandates such changes.
>
> Support for federated login and logout in future versions of this specification will adhere to policies that are expected to emerge from the broader discussion about federated login and logout in the context of the eIDAS regulation.
>
> Most notably, support for IdP AD initiated logout may become mandatory in a future version of this specification.

§ *7.3.1.1 DV Federated Login*

Federated Login via a SSO federation is only supported for multiple connections (websites) of a single DV. Furthermore, DigiD does not support SSO federation between [*DigiD SAML3.x*] and [*eID SAML4.4*] (or later) connections.

A DV who wants to grant access to his services through SSO can do so via the SSO service from RD. The DV then participates in an SSO federation which may include several websites of the DV who all want to use the SSO functionality that is offered within the SSO federation. Details on the SSO service are provided by RD. In a number of cases, the EU is still asked to provide his credentials:

1. The Level of Assurance LoA that the DV website requests may be higher than the level of reliability that is stored in the existing SSO session.
2. The existing SSO session can apply to a different SSO federation than the DV website is a member of.
3. The DV website can include the `ForceAuthn` element in the authentication request, with the value True. If a value is not provided or the element is omitted, the default is "False"
4. The existing SSO session has expired.

§ *7.3.1.2 DV→RD logout Request - Diagram*

A DV or LC can send this message to RD when an EU logs out at an DV. A RD can send this message to an AD.

Sender	Recipient
DV	RD
LC	RD

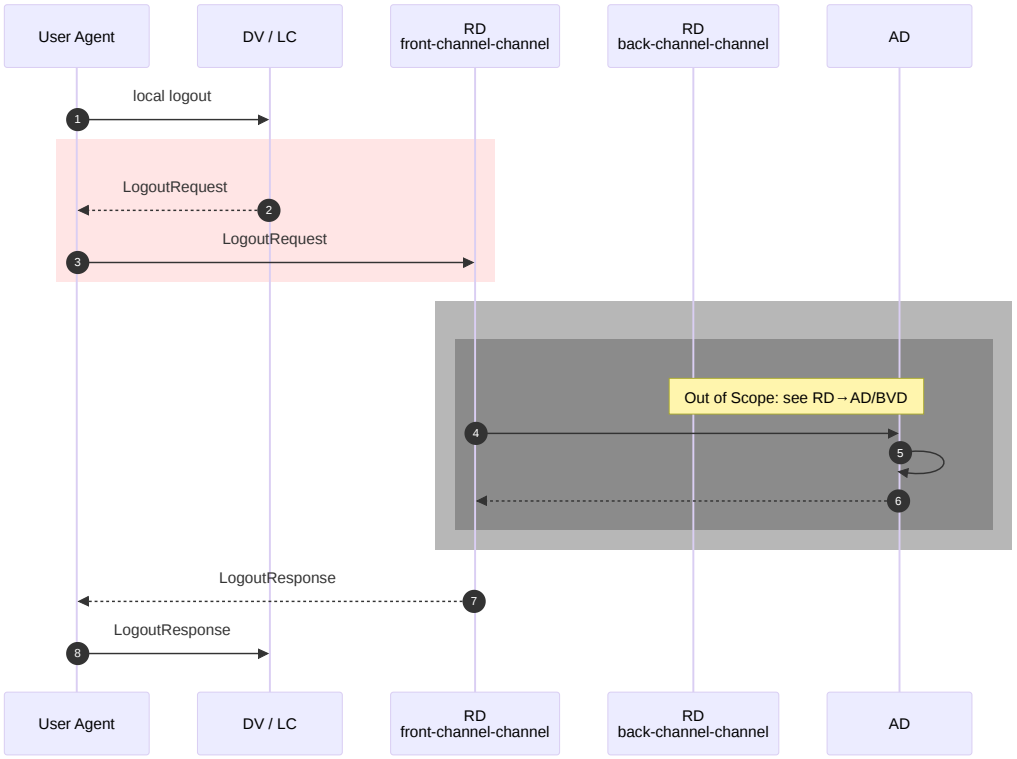

Figure 16 LogoutRequest DV/LC - RD

Only SP (DV) initiated logout is supported by RD. On receiving a logout request (1) a DV which participates in a SSO federation *MUST* send a Logout request to RD (2b).

This will result in RD to terminate the SSO session if it still was active. As a result, the EU will have to re-authenticate when accessing a DV even if that DV is part of the same SSO federation that was just terminated.

SP initiated logout is limited in the sense that any other active SSO originated sessions with DV's is not actively terminated upon receipt of a SP (DV) initiated logout message. Sessions with other active DV's within the same federation will continue to be active until the local DV session times out or the EU logs out of the DV.

§ *7.3.1.3 DV→RD logout Request - Message*

Element/@Attribute	0..n	Description
@ID	1	Unique message attribute
@Version	1	Version of the SAML protocol. The value *MUST* be '2.0'.
@IssueInstant	1	Time at which the message was created.
@Destination	1	URL of the recipient on which the message is offered.
Signature	1	*MUST* contain the Digital signature of the sender for the enveloped message (`@Algoritm="http://www.w3.org/2000/09/xmldsig#enveloped-signature"`). *MUST* contain a `KeyInfo` element with either a `KeyName` or `X509Certificate` elements. See Signature.
NameID	1	*MUST* contain the @NameID NameID element of the original Assertion.
SessionIndex	0..1	Conditional, *MUST* contain the TransientID SessionIndex element of the original Assertion.
Issuer	1	*MUST* contain the of the sender.

§ *7.3.1.4 DV←RD logout Response - Diagram*

In response to a Logout Request message the RD will send this message to the DV or LC, or a AD will send this message to the requesting RD.

Sender	Recipient
RD	DV
RD	LC

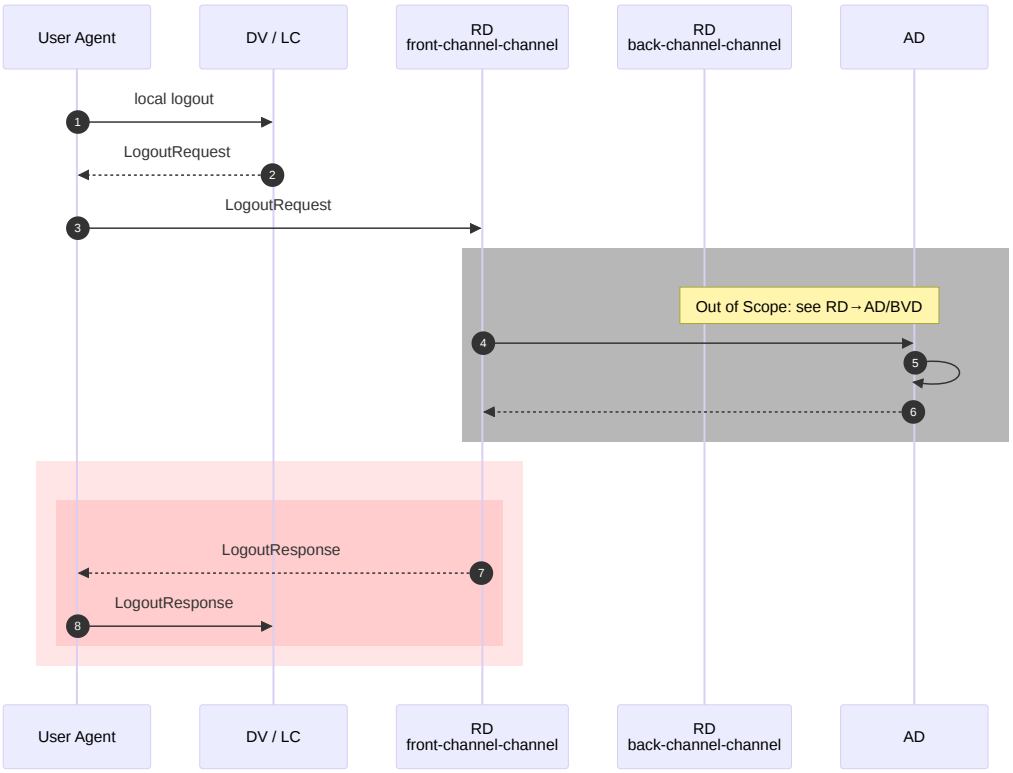

Figure 17 LogoutResponse DV/LC - RD

§ *7.3.1.5 DV←RD logout Response - Message*

Element/@Attribute	0..n	Description
@ID	1	Unique message attribute
@Version	1	Version of the SAML protocol. The value *MUST* be `2.0`.
@IssueInstant	1	Time at which the message was created.
@Destination	1	URL of the recipient on which the message is offered.
@InResponseTo	1	ID of the Logout Request message for which this Logout Response message is the answer.
Signature	1	*MUST* contain the Digital signature of the sender for the enveloped message (`@Algoritm="http://www.w3.org/2000/09/xmldsig#enveloped-signature"`). *MUST* contain a `KeyInfo` element with a `KeyName` element. See Signature.
Issuer	1	*MUST* contain the EntityID of the sender.
Status	1	*MUST* contain a StatusCode element with the status of the logout.
-StatusCode	1	*MUST* be present in a Status element.

§ **7.3.2 RD→AD login & logout**

This section is extending the DV/LC→RD SAML Federated login and logout between RD and AD.

A RD that supports SSO to DV s or LCs must propagate logout requests to the correct AD or ADs. The diagram below depicts the flow between a RD and an AD. The encompassing flow, between DV/LC and RD, is out of scope (see [[*eID SAML4.4*]] for details).

§ *7.3.2.1 RD→AD logout Request - Diagram*

A DV or LC can send this message to RD when a user logs out at an DV. A RD can send this message to an AD.

Sender	Recipient
RD	AD

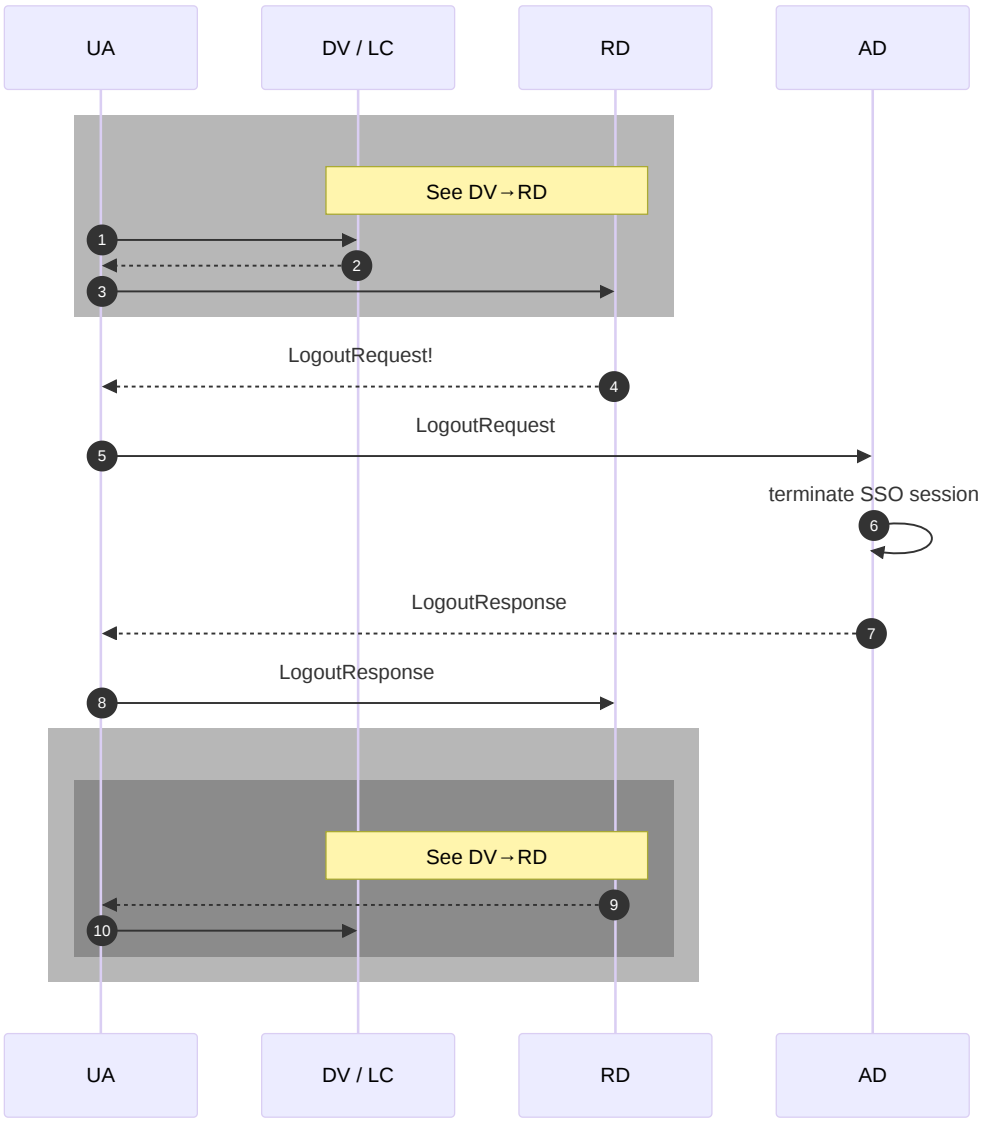

Figure 18 Logout Response RD -AD

§ *7.3.2.2 RD→AD logout Request - Message*

A DV or LC can send this message to RD when a user logs out at an DV. A RD can send this message to an AD. he message is identical to DV/LC→RD SAML Federated logout Request - Message

§ *7.3.2.3 RD←AD logout Response - Diagram*

In response to a Logout Request message from RD, an AD will send this message to the requesting RD.

Sender	Recipient
AD	RD

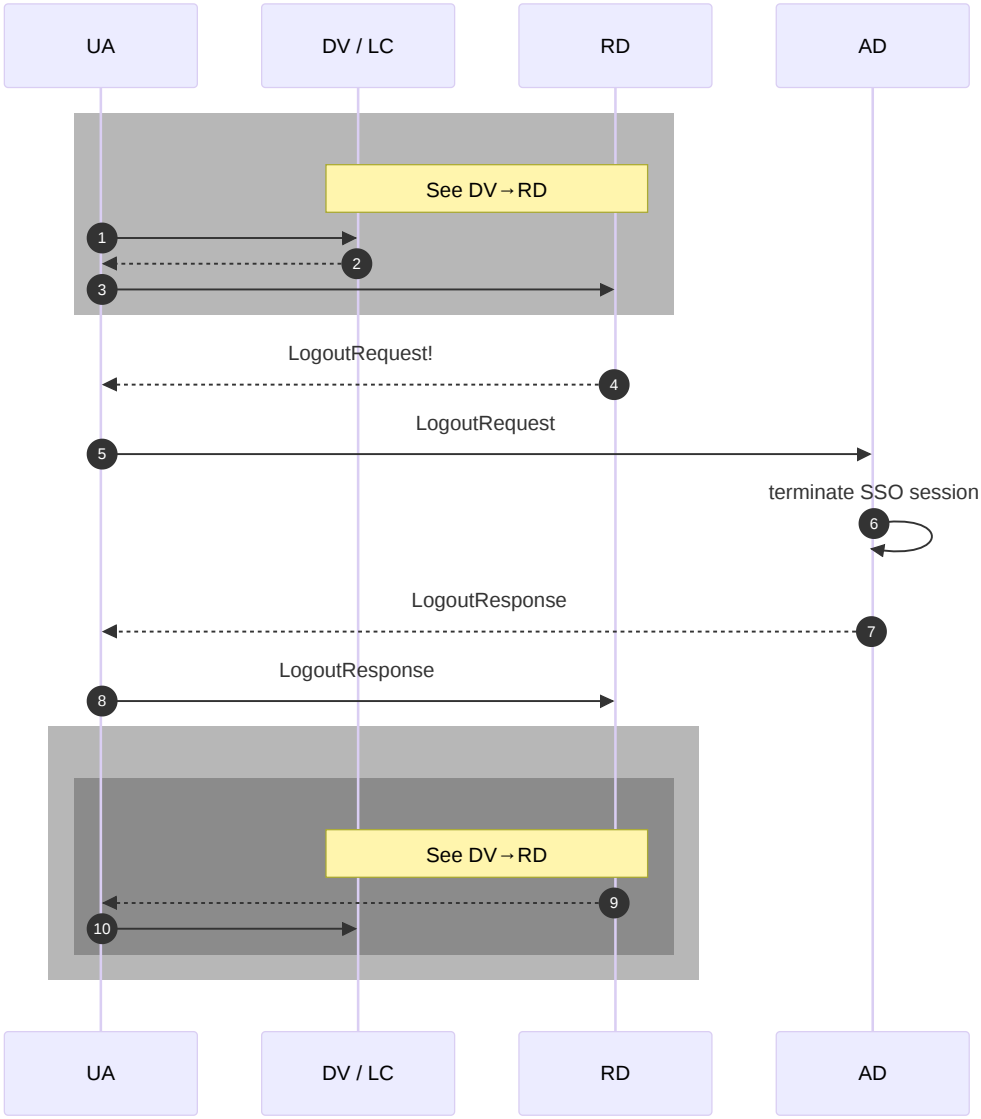

Figure 19 Logout Response RD -AD

§ *7.3.2.4 RD→AD logout Response - Message*

An AD can send this Federated logout response message to the requesting RD. The message is identical to DV/LC→RD SAML Federated logout Response - Message

§ 7.4 Error messages

§ 7.4.1 Toplevel codes

The standard SAML 2.0 error codes are used. For error handling, conformity regarding the interpretation of the status codes as used in the AuthN Response - Assertion element is critical. The following top-level status codes *MAY* be used:

Status code	Description
`urn:oasis:names:tc:SAML:2.0:status:Requester`	This status code is used for errors caused by the initiator of the SAML request. For example, because an assurance level is requested which is not supported by the recipient, or because the request message has expired.
`urn:oasis:names:tc:SAML:2.0:status:Responder`	This status code is used for errors caused by the recipient of the SAML request. For example, because of technical

Status code	Description
	failure or because the recipient does not support requested (optional) functionality.

7.4.2 Second-level status codes

The following second-level status codes *MAY* be used:

Status code	Description
urn:oasis:names:tc:SAML:2.0:status:AuthnFailed	This status code is used when a user cannot be authenticated for example because invalid credentials have been provided or the cancel button has been used.
urn:oasis:names:tc:SAML:2.0:status:NoAuthnContext	This status code is used when a user cannot be authenticated at the minimum level as specified in the Service Catalog.
urn:oasis:names:tc:SAML:2.0:status:RequestUnsupported	This status code is used when a message is correctly formatted by the requester, and understood by the recipient, but that functionality is requested which is not supported by the recipient.
urn:oasis:names:tc:SAML:2.0:status:RequestDenied	This status code is used when a SAML responder that refuses to perform a message exchange with the SAML requester, for example because a mandatory signature could not be verified.
urn:oasis:names:tc:SAML:2.0:status:NoSupportedIDP	Used to indicate that a RequesterID is not supported by the intermediary.

7.4.3 Cancelling

During the process of authenticating and authorizing, an EU may cancel the process by clicking on the cancel button.

If an EU cancels, the Participant *MUST* direct the EU automatically to the latest sender of a SAML request, accompanying a valid SAML AuthN Response - StatusMessage including valid SAML status codes (`urn:oasis:names:tc:SAML:2.0:status:Responder` with `urn:oasis:names:tc:SAML:2.0:status:AuthnFailed`). A AuthN Response - StatusMessage element *MUST* be included, containing the exact phrase `Authentication cancelled`.

If RD receives a cancellation message (from an AD or BVD), it *MUST* be forwarded to the DV or LC.

If a DV or LC receives a cancellation message (from RD), it *MUST* indicate to the EU that he is not logged in, and *MAY* offer the EU the option to re-authenticate.

7.4.4 Attributes not supported

A Participant can receive a message that matches the Interface specifications but cannot be processed by the recipient.

A Participant receiving such a message:

- *MUST* show the EU a message indicating that something went wrong (without revealing security sensitive details).
- *MAY* offer the EU the option to cancel, in that case the flow continues as stated in Cancelling.

7.4.5 Incorrect message (recoverable)

A Participant can receive a message that matches the interface specifications but cannot be processed by the recipient. The recipient *MUST* direct the EU to initiator of the SAML request, accompanying a valid SAML AuthN-response message including valid SAML status codes (`urn:oasis:names:tc:SAML:2.0:status:Responder` with `urn:oasis:names:tc:SAML:2.0:status:RequestUnsupported`). A AuthN Response - StatusMessage element *MUST* be included, containing a description of the problem (for example "Level of assurance not supported").

A Participant receiving such a response:

1. *MUST* show the EU a AuthN-response message indicating authentication has failed, including the contents of AuthN Response - StatusMessage.
2. If the Participant is a RD then the RD *MUST* ask the EU to re-select an AD or BVD or cancel. Except in case of Use Case AD-preselection, then the RD *MUST* forward the AuthN-response message to the DV or LC.

7.4.6 Incorrect message (non-recoverable)

A Participant can receive an invalid formatted message. Examples:

- Not a valid SAML message
- XML does not match XSD

Alternatively, the message can be valid according to SAML specifications, but it does not match the Interface specifications. Examples:

- Unknown issuer
- Invalid NotOnOrAfter in Authn Response Assertion or Authn Response Subject Confirmation
- Invalid signature
- The AuthN-request message contains invalid attributes
- The AuthN-response message contains attributes or a LoA that does not match the AuthN-request

Such messages are the result of either an incorrect implementation by a Participant, or an attempt to hack the system. The EU cannot always be send back to the requester, because the source of the message is unknown and/or cannot be trusted. If the message is an AuthN-response message, it would not make sense to send the EU back to the responder.

A Participant that receives a AuthN-response message in this category

- *MUST* investigate the nature of the error.
- *MUST* show the EU a message indicating a non-recoverable error has occurred, advising the EU how to resolve the problem if possible, in case a binding is used where the EU is involved;
- *MUST* return a AuthN-response message with status codes (`urn:oasis:names:tc:SAML:2.0:status:Requester` and `urn:oasis:names:tc:SAML:2.0:status:RequestUnsupported`) or an HTTP error in case a binding is used where a synchronous response is expected and can be returned, like SOAP.

8. SAML Metadata

8.1 Metadata

Before a SAML connection can be established, the participants must provide each other with configuration data about the connection. This indicates which services, locations of services and certificates are used for the connection.

8.1.1 TLS certificates in metadata

For TLS certificates see technical requirements on Signature and on Signing, encryption algorithms and hash functions

8.1.2 General processing requirements

Processing requirements for the consuming parties:

- The metadata *MUST* be validated by the consuming parties
- The consuming parties *MUST NOT* use the metadata if the validation is not successful

8.2 DV Metadata

8.2.1 DV→RD Metadata

Published by	Consumed by
DV that connects to RD directly	RD

This section describes the metadata that a DV with a direct connection to RD (not using a LC) must provide. This metadata *MAY* be published on a location known to RD or *MAY* be provided to RD by any other means supported.

See also Example SAML-metadata DV for RD

Element/@Attribute	0..n	Description
EntityDescriptor	1	The metadata *MUST* contain one EntityDescriptor with one SPSSODescriptor element.
-***@ID***	1	A document-unique identifier for the element, typically used as a reference point when signing.
-***@entityID***	1	Specifies the unique identifier of the SAML entity whose metadata is described by the element's contents. Contains the entityid of the DV.
-***@validUntil***	0..1	*MAY* contain a datetime at which the metadata expires. If validUntil is expired, the metadata is considered invalid. Either validUntil or cacheDuration *MUST* be present. (following OASIS specification [*SAML2.METADATA*])
-***@cacheDuration***	0..1	*MAY* contain cacheduration. Every Participant is advised to check for new Metadata after the given period. Either validUntil or cacheDuration *MUST* be present. (following OASIS specification [*SAML2.METADATA*])
-***Signature***	1	*MUST* contain the Digital signature of the DV to verify the integrity of this Metadata and *MUST* be generated with a (private signing key associated with a) PKIoverheid public-key certificate which contains the same OIN as used in the entityID. Also see technical requirements on Signature and on Signing, encryption algorithms and hash functions
-***SPSSODescriptor***	1	
--***@AuthnRequestsSigned***	1	*MUST* be set to `true`.
--***@protocolSupportEnumeration***	1	*MUST* be set to `urn:oasis:names:tc:SAML:2.0:protocol`
--***@WantAssertionsSigned***	1	*MUST* be set to `true`.
--***KeyDescriptor***	2..n	*MUST* contain KeyDescriptor element(s) that allow for signing of SAML messages and authenticating a TLS connection. This can be achieved by inclusion of 2 KeyDescriptor element with `@use="signing"` or a single certificate with `@use="signing"` that supports both functions. A second KeyDescriptor *MAY* be present for both of these keys to support certificate rollover. SAML message signing and TLS functions *MAY* be combined in a

Element/@Attribute	0..n	Description
		single certificate or in separate certificates. *MUST* contain at least 1 KeyDescriptor element that supports encryption (`@use="encryption"`). A second KeyDescriptor with `@use="encryption"` *MAY* be present to support certificate rollover. Also see technical requirements on Signing, encryption algorithms and hash functions
---***KeyInfo***	1	
----***KeyName***	1	Contains the name which identifies the key.
----***X509Data***	1	Contains the encoded PKIOverheid X509 certificate with the public key.
--***SingleLogoutService***	0..n	Conditional: *MUST* be present if the DV supports SSO. Describes the endpoint used to log the EU out of its current session if participating in a SSO session.
---***@Binding***	1	*MUST* contain the appropriate binding for the endpoint. The binding parameter denotes the type of binding used. This is an urn relating to [*SAML2.BINDINGS*]. At least one SingleLogoutService *MUST* contain the HTTP-POST binding.
---***@Location***	1	*MUST* contain the URL of the SingleLogoutService endpoint for the Binding.
--***AssertionConsumerService***	1..n	Must contain at least one URL to which the EU will be redirected after authentication. If more than one is included one *MUST* contain the attribute `@isDefault` with value `true`.
--***AttributeConsumingService***	0..n	Conditional: *MUST* be present when DV uses a corresponding AttributeConsumingServiceIndex in the DV AuthnRequest Message. *MUST NOT* be present in any other case or by any other Participant role. When used, AttributeConsumingService *MUST* contain 1 or more elements that describe the Service requested using an @Index to a Service Definition registered with Service Catalog kept by RD.
---***@Index***	1	*MUST* be present.
---***@isDefault***	0..1	*MUST* be present if more than one Index is specified in the metadata. *MAY* only be present once. If present indicates the default AttributeConsumingService which is used when no AttributeConsumingServiceIndex was referenced in the AuthN Request Message. It is advised to always include an AttributeConsumingServiceIndex in the AuthN Request Message.
---***ServiceName***	1..n	One or more language-qualified names for the service. Only one descriptor per language *MUST* be present.
---***RequestedAttribute***	1..n	At least one RequestedAttribute element *MUST* be present with `@name="urn:nl-eid-gdi:1.0:ServiceUUID"`.
----***AttributeValue***	1	*MUST* contain the ServiceUUID to be used for this authentication. The ServiceUUID must be pre-registered with Service Catalog kept by RD.

§ 8.2.2 LC→RD metadata

Published by	Consumed by
LC	RD

This section describes the metadata the LC publishes for the RD. The LC *MUST* provide the metadata for each DV it supports. The metadata *MUST* be signed by the LC. The metadata of all DVs using an LC *MUST* be supplied as a single file and *MAY* additionally be supplied as individual files.

This section describes the layout of the metadata. The XML schema for the Metadata is that of [*SAML2.METADATA*].

See also Example SAML-metadata LC for RD

Element/@Attribute	0..n	Description
EntitiesDescriptor	1	Required element to start metadata containing multiple EntityDescriptors.
-@ID	1	A document-unique identifier for the element, typically used as a reference point when signing.
-@validUntil	0..1	*MAY* contain a datetime at which the metadata expires. If validUntil is expired, the metadata is considered invalid. Either validUntil or cacheDuration *MUST* be present. (following OASIS specification [*SAML2.METADATA*]).
-@cacheDuration	0..1	*MAY* contain cache duration. Consumers are advised to check for new metadata after the given period. Either validUntil or cacheDuration *MUST* be present. (following OASIS specification [*SAML2.METADATA*]).
-Signature	1	*MUST* contain the Digital signature of the LC to verify the integrity of this Metadata and *MUST* be generated with a (private signing key associated with a) PKIoverheid public-key certificate which contains the same OIN as used in the entityID. Also see technical requirements on Signature and on Signing, encryption algorithms and hash functions
-EntityDescriptor	1..n	*MUST* contain the EntityDescriptor of the LC, see LC EntityDescriptor. *MUST* contain the EntityDescriptors of all DV's the LC supports, see DV EntityDescriptor.

§ *8.2.2.1 LC→RD **EntityDescriptor***

Element/@Attribute	0..n	Description
@ID	1	A document-unique identifier for the element, typically used as a reference point when signing.
@entityID	1	*MUST* contain the entityid of the LC.
@validUntil	0..1	*SHOULD NOT* be used as either validUntil or cacheDuration is already present at EntitiesDescriptor level. *MAY* contain a datetime at which the metadata expires. If validUntil is expired, the metadata is considered invalid.
@cacheDuration	0..1	*SHOULD NOT* be used as either validUntil or cacheDuration is already present at EntitiesDescriptor level. *MAY* contain cacheduration. RD is advised to check for new metadata after the given period.
@Signature	0..1	*SHOULD NOT* be used as the metadata is already signed at the EntitiesDescriptor level. If used it *MUST* be generated with the private signing key with an associated PKIoverheid public-key certificate which contains the same OIN as the entityid in the EntityDescriptor.
@SPSSODescriptor	1	The `SPSSODescriptor` implements profiles specific to service providers.
-@AuthnRequestsSigned	1	Must be set to `true`.
-@WantAssertionsSigned	1	Must be set to `true`.
-@protocolSupportEnumeration	1	*MUST* be set to: `urn:oasis:names:tc:SAML:2.0:protocol`.
-KeyDescriptor	1..4	*MUST* contain KeyDescriptor element(s) that allow for signing of SAML messages and authenticating a TLS connection. This can be achieved by inclusion of 2 KeyDescriptor element with `@use="signing"` or a single certificate with `@use="signing"` that supports both functions. A second KeyDescriptor *MAY* be present for both of these keys to support certificate rollover. SAML message signing and TLS functions *MAY* be combined in a single certificate or in separate certificates. ***NOTE**:Also see technical requirements on Signing, encryption algorithms and hash functions*
--KeyInfo	1	

Element/@Attribute	0..n	Description
---***KeyName***	1	Contains the name which identifies the key. *MAY* be any string. Common practice is using the SHA1 fingerprint stripped of colons.
---***X509Data***	1	Contains the encoded X509 certificate with the public key.
-***SingleLogoutService***	0..n	Conditional: *MUST* be present if the LC supports SSO. Describes the endpoint used to log the EU out of its current session if participating in a SSO session.
--@***Binding***	1	*MUST* contain the appropriate binding for the endpoint. The binding parameter denotes the type of binding used. This is a urn relating to [*SAML2.BINDINGS*]. At least one SingleLogoutService *MUST* contain the HTTP-POST binding.
--@***Location***	1	*MUST* contain the URL of the SingleLogoutService endpoint for the @Binding.
-***AssertionConsumerService***	1..n	Must contain at least one URL to which the EU will be redirected after authentication.
--@***Binding***	1	The binding parameter denotes the type of binding used. This is a urn relating to [*SAML2.BINDINGS*] At least one AssertionConsumerService binding *MUST* be set to `urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Artifact`. Other bindings are NOT supported.
--@***Location***	1	The URL of the SAML endpoint
--@***Index***	1	The index of the binding, *MUST* be unique for all AssertionConsumerService elements.
--@***isDefault***	0..1	If more than one AssertionConsumerService elements are included, one of these elements *MUST* be flagged as default by setting the isDefault XML attribute with value `true`.

§ *8.2.2.2 DV→RD* ***EntityDescriptor***

For each DV supported by an LC the following metadata must be included in the LC metadata.

Element/@Attribute	0..n	Description
@***ID***	1	A document-unique identifier for the element, typically used as a reference point when signing.
@***entityID***	1	Specifies the unique identifier of the SAML entity whose metadata is described by the element's contents. *MUST* contain the entityid of the DV.
@***validUntil***	0..1	*SHOULD NOT* be used as either validUntil or cacheDuration is already present at EntitiesDescriptor level. *MAY* contain a datetime at which the metadata expires. If validUntil is expired, the metadata is considered invalid.
@***cacheDuration***	0..1	*SHOULD NOT* be used as either validUntil or cacheDuration is already present at EntitiesDescriptor level. *MAY* contain cacheduration. RD is advised to check for new metadata after the given period.
Signature	0..1	*SHOULD NOT* be used as the metadata is already signed at the EntitiesDescriptor level. If used it *MUST* be generated with the private signing key with an associates PKIoverheid public-key certificate which contains the same OIN as the entityid in the DV EntityDescriptor. The public key certificate *MUST* be present in the KeyDescriptor metadata. *MUST* contain a `KeyInfo` element with a `KeyName` or `X509Certificate` elements.
SPSSODescriptor	1	
@-@***protocolSupportEnumeration***	1	Set to: `urn:oasis:names:tc:SAML:2.0:protocol`.

Element/@Attribute	0..n	Description
-KeyDescriptor	1..2	*MUST* contain at least 1 KeyDescriptor element that supports encryption (`@use="encryption"`). A second KeyDescriptor with `@use="encryption"` *MAY* be present to support certificate rollover. Also see technical requirements on Signing, encryption algorithms and hash functions
--KeyInfo	1	
---KeyName	1	Contains the name which identifies the key. *MAY* be any string. Common practice is using the SHA1 fingerprint stripped of colons.
---X509Data	1	Contains the encoded X509 certificate with the public key.
-AssertionConsumerService	1..n	According to saml-metadata-2.0 *MUST* contain at least one URL to which the EU will be redirected after authentication. *MUST* contain only one entry. *MUST* contain a copy of the AssertionConsumerService element in the LC's EntityDescriptor. This entry will be ignored as the AssertionConsumerService definitions in the LC EntityDescriptor *MUST* be used.

§ 8.2.3 RD→DV/LC metadata

Published by	Consumed by
RD	DV that connect directly with RD, LC

RD publishes metadata in accordance with [*SAML2.METADATA*] with one EntityDescriptor element. The metadata is signed in accordance with the SAML signature.

See also Example SAML-metadata a RD for DV

Element/@Attribute	0..n	Description
EntityDescriptor	1	
-@ID	1	A document-unique identifier for the element, typically used as a reference point when signing.
-@entityID	1	Specifies the unique identifier of the SAML entity whose metadata is described by the element's contents. Contains the entityid of RD.
-@validUntil	0..1	*MAY* contain a datetime at which the metadata expires. If validUntil is expired, the metadata is considered invalid. Either validUntil or cacheDuration *MUST* be present. (following OASIS specification [*SAML2.METADATA*])
-@cacheDuration	0..1	*MAY* contain cache duration. DV or LC is advised to check for new metadata after the given period. Either validUntil or cacheDuration *MUST* be present. (following OASIS specification [*SAML2.METADATA*])
-Signature	1	*MUST* contain the Digital signature of the RD to verify the integrity of this Metadata and *MUST* be generated with a (private signing key associated with a) PKIoverheid public-key certificate which contains the same OIN as used in the entityID. Also see technical requirements on Signature and on Signing, encryption algorithms and hash functions
-IDPSSODescriptor	1	
--@protocolSupportEnumeration	1	Set to: `urn:oasis:names:tc:SAML:2.0:protocol`
--@WantAuthnRequestsSigned	1	Set to `true` indication that AuthnRequest messages *MUST* be signed by the DV or LC.
--KeyDescriptor	1..n	Contains at least 1 KeyDescriptor element with `@use="signing"`
---KeyInfo	1	
----KeyName	1	Contains the name which identifies the key.
----X509Data	1	Contains the encoded X509 certificate with the public key.

Element/@Attribute	0..n	Description
--***ArtifactResolutionService***	1..n	The ArtifactResolutionService *MUST* be implemented at least once per service.
---***@Binding***	1	The binding parameter denotes the type of binding used. In the ArtifactResolutionService this is the SAML-SOAP binding only. The value of this attribute is a urn relating to [*SAML2.BINDINGS*].
---***@Location***	1	The URL of the SAML artifact resolution endpoint
---***@Index***	1	The index of the binding, *MUST* be unique for all ArtifactResolutionService elements
--***SingleSignOnService***	1..n	One or more elements of type EndpointType that describe endpoints that support the profiles of the Authentication Request protocol defined in [*SAML2.PROFILES*].
---***@Binding***	1	The binding parameter denotes the type of binding used. In the SingleSignOnService this is the HTTP-POST binding only. The value of this attribute is an urn relating to [*SAML2.BINDINGS*].
---***@Location***	1	The URL of the SAML SingleSignOnService endpoint
--***SingleLogoutService***	1..n	Describes the endpoint used to log the EU out of its current session if participating in a SSO session.
---***@Binding***	1	*MUST* be set to `urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST`. Other bindings are NOT supported.
---***@Location***	1	The URL of the SAML endpoint

8.3 RD metadata

8.3.1 RD→AD metadata

Published by	Consumed by
RD	AD , BVD

This section describes the Metadata the RD publishes for the AD/BVD (acting as the SAML-role of a DV). The RD *MUST* provide the Metadata for each DV it supports. The Metadata *MUST* be signed by the RD. The Metadata of all DVs using an RD *MUST* be supplied as a single file and *MAY* additionally be supplied as individual files.

This section describes the layout of the metadata. The XML schema for the Metadata is that of [*SAML2.METADATA*].

See also Example SAML-metadata RD for AD/BVD

Element/@Attribute	0..n	Description
EntitiesDescriptor	1	Required element to start metadata containing multiple EntityDescriptors.
-***@ID***	1	A document-unique identifier for the element, typically used as a reference point when signing.
-***@validUntil***	1	Contains a datetime at which the metadata expires. If validUntil is expired, the metadata is considered invalid. This element *MUST* be present. (following OASIS specification [*SAML2.METADATA*]).
-***Signature***	1	*MUST* contain the Digital signature of the RD to verify the integrity of this Metadata and *MUST* be generated with a (private signing key associated with a) PKIoverheid public-key certificate which contains the same OIN as used in the entityID. Also see technical requirements on Signature and on Signing, encryption algorithms and hash functions
-***EntityDescriptor***	1..n	*MUST* contain the EntityDescriptor of the RD (see EntityDescriptor). *MUST* contain the EntityDescriptors of all DV's the RD supports (see EntityDescriptors).

§ *8.3.1.1* ***EntityDescriptor***

Element/@Attribute	0..n	Description
@ID	1	A document-unique identifier for the element, typically used as a reference point when signing.
@entityID	1	*MUST* contain the entityID of the RD.
@validUntil	0..1	*SHOULD NOT* be used as validUntil is already present at EntitiesDescriptor level. *MAY* contain a datetime at which the metadata expires. If validUntil is expired, the metadata is considered invalid.
Signature	0..1	*SHOULD NOT* be used as the metadata is already signed at the EntitiesDescriptor level. If used it *MUST* be generated with the private signing key with an associated PKIoverheid public-key certificate which contains the same OIN as used in the entityID.
SPSSODescriptor	1	The `SPSSODescriptor` implements profiles specific to service providers.
-@AuthnRequestsSigned	1	Must be set to `true`.
-@WantAssertionsSigned	1	Must be set to `true`.
-@protocolSupportEnumeration	1	*MUST* be set to: `urn:oasis:names:tc:SAML:2.0:protocol`.
-KeyDescriptor	1..4	*MUST* contain KeyDescriptor element(s) that allow for signing of SAML messages and authenticating a TLS connection. This can be achieved by inclusion of 2 KeyDescriptor element with `@use="signing"` or a single certificate with `@use="signing"` that supports both functions. A second KeyDescriptor *MAY* be present for both of these keys to support certificate rollover. SAML message signing and TLS functions *MAY* be combined in a single certificate or in separate certificates. *MUST* contain at least 1 KeyDescriptor element that supports encryption (`@use="encryption"`). A second KeyDescriptor with `@use="encryption"` *MAY* be present to support certificate rollover. Also see technical requirements on Signing, encryption algorithms and hash functions
--KeyInfo	1	
---KeyName	1	Contains the name which identifies the key. *MAY* be any string. Common practice is using the SHA1 fingerprint stripped of colons.
---X509Data	1	Contains the encoded X509 certificate with the public key.
-SingleLogoutService	0..n	Conditional: *MUST* be present if the RD supports SSO. Describes the endpoint used to log the EU out of its current session if participating in a SSO session.
--@Binding	1	*MUST* contain the appropriate binding for the endpoint. The binding parameter denotes the type of binding used. This is a urn relating to [*SAML2.BINDINGS*]. At least one SingleLogoutService *MUST* contain the HTTP-POST binding.
--@Location	1	*MUST* contain the URL of the SingleLogoutService endpoint for the @Binding.
-AssertionConsumerService	1..n	Must contain at least one URL to which the EU will be redirected after authentication.
--@Binding	1	The binding parameter denotes the type of binding used. This is a urn relating to [*SAML2.BINDINGS*] At least one AssertionConsumerService binding *MUST* be set to `urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Artifact`. Other bindings are NOT supported.
--@Location	1	The URL of the SAML endpoint

Element/@Attribute	0..n	Description
--@***Index***	1	The index of the binding, *MUST* be unique for all AssertionConsumerService elements.
--@***isDefault***	0..1	If more than one AssertionConsumerService elements are included, one of these elements *MUST* be flagged as default by setting the isDefault XML attribute with value `true`.

§ *8.3.1.2 DV→AD* ***EntityDescriptor***

For each DV supported by an RD the following metadata must be included in the RD metadata.

Element/@Attribute	0..n	Description
@ID	1	A document-unique identifier for the element, typically used as a reference point when signing.
@entityID	1	Specifies the unique identifier of the SAML entity whose metadata is described by the element's contents. *MUST* contain the entityid of the DV .
@validUntil	0..1	*SHOULD NOT* be used as validUntil is already present at EntitiesDescriptor level. *MAY* contain a datetime at which the metadata expires. If validUntil is expired, the metadata is considered invalid.
@cacheDuration	0..1	*SHOULD NOT* be used as validUntil is already present at EntitiesDescriptor level. *MAY* contain cacheduration. AD is advised to check for new metadata after the given period.
Signature	0..1	*SHOULD NOT* be used as the metadata is already signed at the EntitiesDescriptor level. If used it *MUST* be generated with the private signing key with an associates PKIoverheid public-key certificate which contains the same OIN as the entityid in the DV EntityDescriptor. The public key certificate *MUST* be present in the KeyDescriptor metadata. *MUST* contain a `KeyInfo` element with a `KeyName` or `X509Certificate` elements.
SPSSODescriptor	1	
-@***protocolSupportEnumeration***	1	Set to: `urn:oasis:names:tc:SAML:2.0:protocol`.
-***KeyDescriptor***	1..2	*MUST* contain at least 1 KeyDescriptor element that supports encryption (`@use="encryption"`). A second KeyDescriptor with `@use="encryption"` *MAY* be present to support certificate rollover. Also see technical requirements on Signing, encryption algorithms and hash functions
--***KeyInfo***	1	
---***KeyName***	1	Contains the name which identifies the key. *MAY* be any string. Common practice is using the SHA1 fingerprint stripped of colons.
---***X509Data***	1	Contains the encoded X509 certificate with the public key.
-***AssertionConsumerService***	1..n	According to saml-metadata-2.0 *MUST* contain at least one URL to which the EU will be redirected after authentication. *MUST* contain only one entry. *MUST* contain a copy of the AssertionConsumerService element in the RD's EntityDescriptor. This entry will be ignored as the AssertionConsumerService definitions in the RD EntityDescriptor *MUST* be used.

§ **8.3.2 AD/BVD→RD metadata**

Published by	Consumed by
AD, BVD	RD

An AD/BVD publishes metadata in accordance with [*SAML2.METADATA*] with one EntityDescriptor element. The metadata is signed in accordance with the SAML signature.

Element/@Attribute	0..n	Description
EntityDescriptor	1	
-@ID	1	A document-unique identifier for the element, typically used as a reference point when signing.
-@entityID	1	Specifies the unique identifier of the SAML entity whose metadata is described by the element's contents. Contains the entityid of the AD/BVD.
-@validUntil	1	Contains a datetime at which the metadata expires. If validUntil is expired, the metadata is considered invalid. This element *MUST* be present. (following OASIS specification [*SAML2.METADATA*]).
-Signature	1	*MUST* contain the Digital signature of the AD to verify the integrity of this Metadata and *MUST* be generated with a (private signing key associated with a) PKIoverheid public-key certificate which contains the same OIN as used in the entityID. Also see technical requirements on Signature and on Signing, encryption algorithms and hash functions
-IDPSSODescriptor	1	
--@protocolSupportEnumeration	1	Set to: `urn:oasis:names:tc:SAML:2.0:protocol`
--@WantAuthnRequestsSigned	1	Set to `true` indication that AuthnRequest messages *MUST* be signed by the RD.
--KeyDescriptor	1..n	Contains at least 1 KeyDescriptor element with `@use="signing"`. A BVD *MUST* also provide at least 1 KeyDescriptor element that supports encryption (`@use="encryption"`) for receiving ActingSubjectID (see Attribute) with an EncryptedID's from an AD. A second KeyDescriptor with `@use="encryption"` *MAY* be present to support certificate rollover. Also see technical requirements on Signing, encryption algorithms and hash functions
---KeyInfo	1	
----KeyName	1	Contains the name which identifies the key.
----X509Data	1	Contains the encoded X509 certificate with the public key.
--ArtifactResolutionService	1..n	The ArtifactResolutionService *MUST* be implemented at least once per service.
---@Binding	1	The binding parameter denotes the type of binding used. In the ArtifactResolutionService this is the SAML-SOAP binding only. The value of this attribute is a urn relating to [*SAML2.BINDINGS*].
---@Location	1	The URL of the SAML artifact resolution endpoint
---@Index	1	The index of the binding, *MUST* be unique for all ArtifactResolutionService elements
--SingleSignOnService	1..n	One or more elements of type EndpointType that describe endpoints that support the profiles of the Authentication Request protocol defined in [*SAML2.PROFILES*].
---@Binding	1	The binding parameter denotes the type of binding used. In the SingleSignOnService this is the HTTP-POST binding only. The value of this attribute is an urn relating to [*SAML2.BINDINGS*].
---@Location	1	The URL of the SAML SingleSignOnService endpoint
--SingleLogoutService	0..1	*MUST* be present if the AD supports SSO. *MUST NOT* be present in the metadata of the BVD. Describes the endpoint used to log the EU out of its current session if participating in a SSO session.
---@Binding	1	*MUST* be set to `urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST`. Other bindings are NOT supported.
---@Location	1	The URL of the SAML endpoint

§ 9. Technical requirements and recommendations

§ 9.1 Signing, encryption algorithms and hash functions

ST-SAML does not support SHA1 except for the padding function (xmldsig # rsa-sha1). Only RSA is supported for signing as PKIoverheid certificates do not support other methods. For signing, the following list of signing algorithms is supported:

Signing algorithm	urn
RSAwithSHA256	`http://www.w3.org/2001/04/xmldsig-more#rsa-sha256`
RSAwithSHA384	`http://www.w3.org/2001/04/xmldsig-more#rsa-sha384`
RSAwithSHA512	`http://www.w3.org/2001/04/xmldsig-more#rsa-sha512`

(source: [*XML.SIG*] § 6.1)

At minimum, SHA256 must be used to calculate the message digest (`<ds:DigestMethod Algorithm = "http://www.w3.org/2001/04/xmlenc#sha256" />`).

Digest algorithm	urn
SHA256	`http://www.w3.org/2001/04/xmlenc#sha256`
SHA384	`http://www.w3.org/2001/04/xmldsig-more#sha384`
SHA512	`http://www.w3.org/2001/04/xmlenc#sha512`

(source: [*XML.SIG*] § 6.1)

All SAML messages that must be signed, must be signed with an Enveloped Signature Transform `http://www.w3.org/TR/2013/REC-xmldsig-core1-20130411/#enveloped-signature`

Participants are required to fully check signatures and associated messages according to standards including checking the correctness of the sender. This also applies to Metadata.

To guarantee authenticity, integrity and non-repudiation, each message described *MUST* be provided with a digital signature from the message sender. The message recipient *MUST* validate all of the digital signatures - except signatures in an Assertion/Advice as they are intended for evidence - in the message before processing it according to the processing rules required by PKIoverheid per Certificate Practice Statements (CPS) including checking the validity of the certificate.

- The recipient *MUST* check that the message is signed with a valid digital signature that envelopes the whole message with Enveloped Signature Transform.
- The recipient *MUST NOT* process the message if signature validation fails.

The following requirements apply to generating digital signatures:

- The digital signature is embedded in the message content with Enveloped Signature Transform `http://www.w3.org/2000/09/xmldsig#enveloped-signature`.
- Canonicalization *MUST* be carried out according to the exclusive c14n method without comments, as identified by `http://www.w3.org/2001/10/xml-exc-c14n#` (see [*XML.C14N.EXCL*])
- Digests *MUST* be calculated with at minimum the SHA256 algorithm except for the fore mentioned exception (padding with SHA1).
- The SignatureValue *MUST* be calculated with at minimum the RSAwithSHA256 algorithm.
- a Participant *MUST* sign messages and metadata with a PKIoverheid certificate with a key length of at least 2048 bits, and which contains the OIN of the Participant. PKIoverheid TLS certificates can be included as a signing certificate (in saml Metadata). Difference with normal signing certificate can be made via extended key usage. See [*SAML2.ERRATA.05*], E62. So the (extended) key usage of the certificate *MUST* allow use for signing.
- The Reference *MUST* refer to the signed element via an ID attribute in the local document, as per the signature profile of [*SAML2.CORE*] (§ 5.4) and [*SAML2.METADATA*] (§ 3.1).

9.2 Signature

Each `Signature` element in SAML messages generated by a DV or LC (see Signature in DV AuthN-request message) and in the DV or LC entries in the Service Catalog (see Signature in DV metadata) *MUST* contain either a `KeyInfo` element with a `X509Certificate` element OR a `KeyName` element containing a key name. The use of `KeyName` is preferred as this limits the amount of data exchanged. The `X509Certificate` or `KeyName` *MUST* match a X509Data or KeyName in the DV metadata KeyDescriptor element with `@use="signing"`.

Each `Signature` element in SAML messages generated by a RD (or any other Participant) and in the Metadata *MUST* contain a `KeyInfo` element with a `KeyName` element containing a key name that corresponds to a KeyName in a KeyDescriptor element in the Metadata for that Participant .

Certificates used to verify a `Signature` *MUST* be retrieved from the Participant's verified Metadata. The `X509Certificate` or `KeyName` in the `KeyInfo` of the Signature *MUST* only be used to retrieve the corresponding certificate from the Participant's verified Metadata.

9.3 Encryption

Encryption is used to guarantee confidentiality. Encryption in combination with SAML is achieved via XML-encryption (see EncryptedID). In case encryption *MAY* or *MUST* be used, one *MUST* use the block encryption algorithms identified by the following URI in conjunction with the use of XML Encryption

algorithm	urn
AES-256	`http://www.w3.org/2001/04/xmlenc#aes256-cbc`

For asymmetric encryption, used to encrypt keys, the RSA algorithm in combination with OAEP padding and a SHA digest *MUST* be used, as described at http://www.w3.org/TR/xmlenc-core1/#sec-RSA-OAEP. The SHA1 version *MUST* be used (`http://www.w3.org/2009/xmlenc11#mgf1sha1`).

9.4 TLS transport

RD requires that a service provider always protects http traffic with TLS v1.2 or higher in accordance with the NCSC directive with 'good' assessment (ICT security guidelines for Transport Layer Security (TLS)). The certificate used for this must be issued under PKIoverheid, and the certificate must have a key length or at least 2048 bits.

For the Back Channel between RD and the DV or LC, both parties must use a PKIoverheid certificate and mutual authentication is mandatory. This is also called two-sided or mutual TLS.

9.5 NotBefore and NotOnOrAfter

DVs and LCs must respect the NotBefore and NotOnOrAfter parameters in the message elements and reject messages that do not comply and cancel the authentication. With a re-authentication, the entire protocol handling must take place.

For this it is advisable to use NTP servers (for example from the nl.pool.ntp.org collection of NTP servers). This measure is taken because lag can make the web service vulnerable to certain attacks on the authentication protocol.

9.6 Levels of assurance

The Levels of Assurance (LoA) that are supported in the interface are listed in Level of Assurance.

9.7 Local session

The DV is responsible for keeping track of the local EU session. This session *MUST* be terminated after at most 15 minutes inactivity.

The DV must recognize replay attacks and ward off these attacks.

If the DV uses cookies to manage sessions, the "Secure" and "HttpOnly" parameters must be used.

> **NOTE**
> The setting of the SameSite policy still has to be determined as browsers show inconsistent behavior.

9.8 RelayState

DVs may provide a RelayState for their own session monitoring. RD returns the RelayState value provided without any verification. The monitoring of the content and integrity of the RelayState must be done by the service provider (DV).

The SAML standard uses a maximum of 80 bytes for the RelayState (see the SAML standard).

9.9 EU interaction

When a DV forwards an EU to RD this must be done in such a way that it is clear to the EU on which website they are and that they can actually check this. That is why the following requirements apply:

1. The EU must be redirected to RD in the same screen that the EU clicked on "Log in to DigiD".
2. The EU must see a browser window with the full address bar. This allows an EU to see on which website he is entering his data. The EU can check this by inspecting the certificate (green lock).
3. It is not allowed to invoke RD in a frame or iframe, or to embed these websites in another way in a webpage of the DV.

The DV must decide on the basis of the Assertion in the AuthN-response whether an EU can gain access to the Service or, in the case of re-authentication (applicable to SAML SSO), may continue his session.

If the status in the Assertion is not successful or the EU does not have the required LoA in the AuthnContext of the Assertion in the AuthN-response then:

1. The DV or LC *MUST* immediately end the current session of the EU.
2. *SHOULD* show an appropriate message (see SAML Error codes).

10. Type definitions

This page and underlying pages describe identifier types which are used by ST-SAML

- Attribute Identifier types
- Attribute representation Types
- EntityID Format
- Level of Assurance

10.1 Attribute identifier types

Stelsel Toegang SAML v1.0 specification describes the following attribute identifier types

Attribute	urn	Remarks
BSN	`urn:nl-eid-gdi:1.0:id:legacy-BSN`	BSN. encoded in 9-digits, padded with leading 0 if needed. Example: 123456789 or 012345678.
BSN	`urn:nl-eid-gdi:1.0:id:BSN`	Encrypted Identity (see [*BSNk.DEC*], Encrypted structures)
Pseudonym	`urn:nl-eid-gdi:1.0:id:Pseudonym`	Encrypted Pseudonym (see [*BSNk.DEC*] Encrypted structures)

The following attributes may be supplied additionally, only through ETD (see https://afsprakenstelsel.etoegang.nl/Startpagina/as/identificerende-kenmerken)

§ 10.2 Attribute representation types

The table shows the allowed representationTypes in URN format that are supported by the BVD (BVD-OG) and can be found in the Attribute Statement of the AuthN Response - Assertion as a unencrypted with @name Name="urn:nl-eid-gdi:1.1:RepresentationType". See attribute for legal representation

representation-types	urn	Sector	description
Zorg_Volledig_Gezag_Kind	urn:nl-eid-gdi:1.1:RT:Zorg_Volledig_Gezag_Kind	health care	Specific Parental authority for children under 12 years old in healthcare

§ 10.3 EntityID Format

The format of value of the @entityID attribute is: `urn:nl-eid-gdi:1.0:<ROLE>:<OIN>:entities:<index>`

`<OIN>`

The OIN of the organization.

`<ROLE>`

Indication of the role of the entity:

- AD
- DV
- BVD
- LC
- RD

`<index>`

The `<index>` is a number with 4 positions between 0000 and 8999 that can be selected by the Participant to define different endpoints (in the Metadata). Numbers between 9000 and 9999 are reserved for test systems.

§ 10.4 Level of Assurance

The table shows the four Levels of Assurance supported by ST-SAML and the corresponding urn's which are used in the SAML messages.

LoA	urn
Basis	`http://eID.logius.nl/LoA/basic`
Midden	`http://eidas.europa.eu/LoA/low`
Substantieel	`http://eidas.europa.eu/LoA/substantial`
Hoog	`http://eidas.europa.eu/LoA/high`

A. Example SAML messages

This section is non-normative.

A.1 Example - AuthnRequest

EXAMPLE 1: AuthnRequest

```
<?xml version="1.0" encoding="UTF-8"?>
<samlp:AuthnRequest AssertionConsumerServiceIndex="0" AttributeConsumingServiceIndex="1"
                    Destination="http://idp.example.com/request_authentication"
                    ID="_56ae2ef7ff51845153d8960e5b73d45128ad6d62" IssueInstant="2021-02-
                    xmlns:ds="http://www.w3.org/2000/09/xmldsig#" xmlns:ec="http://www.w3
                    xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion"
                    xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol">
    <saml:Issuer>urn:nl-eid-gdi:1.0:DV:00000009999999999001:entities:0000</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-sha
            <ds:Reference URI="#_56ae2ef7ff51845153d8960e5b73d45128ad6d62">
                <ds:Transforms>
                    <ds:Transform Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-
                    <ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#">
                        <ec:InclusiveNamespaces PrefixList="ds saml samlp xs"/>
                    </ds:Transform>
                </ds:Transforms>
                <ds:DigestMethod Algorithm="http://www.w3.org/2001/04/xmlenc#sha256"/>
                <ds:DigestValue>...</ds:DigestValue>
            </ds:Reference>
        </ds:SignedInfo>
        <ds:SignatureValue>...</ds:SignatureValue>
        <ds:KeyInfo>
            <ds:KeyName>4492219ba557ce9e547a933d15ab87b14a69788d</ds:KeyName>
        </ds:KeyInfo>
    </ds:Signature>
</samlp:AuthnRequest>
```

§ A.2 Example - AuthnRequest using Extensions

EXAMPLE 2: AuthnRequest using Extensions

```
<?xml version="1.0" encoding="UTF-8"?>
<samlp:AuthnRequest xmlns:ds="http://www.w3.org/2000/09/xmldsig#"
                    xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion"
                    xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol"
                    Destination="http://idp.example.com/request_authentication"
                    ForceAuthn="false" ID="_d68fdd07cb64ca845317aa145969187c1514129b"
                    IsPassive="false" IssueInstant="2021-04-15T14:20:38Z" Version="2.0">
    <saml:Issuer Format="urn:oasis:names:tc:SAML:2.0:nameid-format:entity">
        urn:nl-eid-gdi:1.0:DV:00000009999999999001:entities:0000
    </saml:Issuer>
    <ds:Signature Id="uuidd5e7c2bf-0178-146b-8597-ef90aa0f4487">
        <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-sha
            <ds:Reference URI="#_d68fdd07cb64ca845317aa145969187c1514129b">
                <ds:Transforms>
                    <ds:Transform Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-
                    <ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#">
                        <xc14n:InclusiveNamespaces xmlns:xc14n="http://www.w3.org/2001/10
                                                   PrefixList="samlp saml ds"></xc14n:Inc
                    </ds:Transform>
                </ds:Transforms>
                <ds:DigestMethod Algorithm="http://www.w3.org/2001/04/xmlenc#sha256"></ds
                <ds:DigestValue>...</ds:DigestValue>
            </ds:Reference>
        </ds:SignedInfo>
        <ds:SignatureValue>...</ds:SignatureValue>
    </ds:Signature>
    <samlp:Extensions>
        <saml:Attribute Name="urn:nl-eid-gdi:1.0:ServiceUUID">
            <saml:AttributeValue>336fa5edb569-13fb-b3e4-8968-86c62aea</saml:AttributeValu
        </saml:Attribute>
        <saml:Attribute Name="urn:nl-eid-gdi:1.0:IntendedAudience">
            <saml:AttributeValue>urn:nl-eid-gdi:1.0:DV:00000009999999999001:entities:0000
        </saml:Attribute>
    </samlp:Extensions>
</samlp:AuthnRequest>
```

§ A.3 Example - AuthnRequest with Representation

EXAMPLE 3: AuthnRequest with Representation

```
<?xml version="1.0" encoding="UTF-8"?>
<samlp:AuthnRequest AssertionConsumerServiceIndex="0" AttributeConsumingServiceIndex="1"
                    Destination="http://idp.example.com/request_authentication"
                    ID="_56ae2ef7ff51845153d8960e5b73d45128ad6d62" IssueInstant="2021-02-
                    xmlns:ds="http://www.w3.org/2000/09/xmldsig#" xmlns:ec="http://www.w3
                    xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion"
                    xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol">
    <saml:Issuer>urn:nl-eid-gdi:1.0:DV:00000009999999999001:entities:0000</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-sha
            <ds:Reference URI="#_56ae2ef7ff51845153d8960e5b73d45128ad6d62">
                <ds:Transforms>
                    <ds:Transform Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-
                    <ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#">
                        <ec:InclusiveNamespaces PrefixList="ds saml samlp xs"/>
                    </ds:Transform>
                </ds:Transforms>
                <ds:DigestMethod Algorithm="http://www.w3.org/2001/04/xmlenc#sha256"/>
                <ds:DigestValue>...</ds:DigestValue>
            </ds:Reference>
        </ds:SignedInfo>
        <ds:SignatureValue>...</ds:SignatureValue>
        <ds:KeyInfo>
            <ds:KeyName>4492219ba557ce9e547a933d15ab87b14a69788d</ds:KeyName>
        </ds:KeyInfo>
    </ds:Signature>
    <samlp:Scoping>
        <samlp:RequesterID>urn:nl-eid-gdi:1.0:BVD:00000004003214345001:entities:9000</sam
    </samlp:Scoping>
</samlp:AuthnRequest>
```

§ A.4 Example - ArtifactResponse with Legal Representation

EXAMPLE 4: ArtifactResponse with Legal Representation

```
<?xml version="1.0" encoding="UTF-8"?>
<soap11:Envelope xmlns:soap11="http://schemas.xmlsoap.org/soap/envelope/">
    <soap11:Body>
        <saml2p:ArtifactResponse xmlns:saml2p="urn:oasis:names:tc:SAML:2.0:protocol"
                                 ID="_0fb52522f6e41b750df938ef5ea50154"
                                 InResponseTo="_1ea090efda5655760b6a0c9dfa8884b66d475222"
                                 IssueInstant="2025-05-05T08:10:51.018Z" Version="2.0">
            <saml2:Issuer xmlns:saml2="urn:oasis:names:tc:SAML:2.0:assertion">
                urn:nl-eid-gdi:1.0:TD:00000004183317817000:entities:9000
            </saml2:Issuer>
            <ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
                <ds:SignedInfo>
                    <ds:CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-e
                    <ds:SignatureMethod Algorithm="http://www.w3.org/2001/04/xmldsig-more
                    <ds:Reference URI="#_0fb52522f6e41b750df938ef5ea50154">
                        <ds:Transforms>
                            <ds:Transform Algorithm="http://www.w3.org/2000/09/xmldsig#en
                            <ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c1
                        </ds:Transforms>
                        <ds:DigestMethod Algorithm="http://www.w3.org/2001/04/xmlenc#sha2
                        <ds:DigestValue>...</ds:DigestValue>
                    </ds:Reference>
                </ds:SignedInfo>
                <ds:SignatureValue>...</ds:SignatureValue>
                <ds:KeyInfo>
                    <ds:KeyName>356b4241808341cc9ff6295a43b01d00daab27406ddcd3f708a0a3761
                </ds:KeyInfo>
            </ds:Signature>
            <saml2p:Status>
                <saml2p:StatusCode Value="urn:oasis:names:tc:SAML:2.0:status:Success"/>
            </saml2p:Status>
            <saml2p:Response
                    Destination="sp.example.com"
                    ID="_31fa010c6af1bc61583f22c84b3a2b0d" InResponseTo="_a658d2c5c7426b1
                    IssueInstant="2021-10-06T08:10:51.018Z" Version="2.0">
                <saml2:Issuer xmlns:saml2="urn:oasis:names:tc:SAML:2.0:assertion">
                    urn:nl-eid-gdi:1.0:TD:00000004183317817000:entities:9000
                </saml2:Issuer>
                <saml2p:Status>
                    <saml2p:StatusCode Value="urn:oasis:names:tc:SAML:2.0:status:Success"
                </saml2p:Status>
                <saml2:Assertion xmlns:saml2="urn:oasis:names:tc:SAML:2.0:assertion"
                                 ID="_2a9deaff3a95b2193e74dbad4a69dfbf" IssueInstant="202
                                 Version="2.0">
                    <saml2:Issuer>urn:nl-eid-gdi:1.0:TD:00000004183317817000:entities:900
                    <ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
                        <ds:SignedInfo>
                            <ds:CanonicalizationMethod Algorithm="http://www.w3.org/2001/
                            <ds:SignatureMethod Algorithm="http://www.w3.org/2001/04/xmld
                            <ds:Reference URI="#_2a9deaff3a95b2193e74dbad4a69dfbf">
                                <ds:Transforms>
                                    <ds:Transform Algorithm="http://www.w3.org/2000/09/xm
                                    <ds:Transform Algorithm="http://www.w3.org/2001/10/xm
                                </ds:Transforms>
                                <ds:DigestMethod Algorithm="http://www.w3.org/2001/04/xml
                                <ds:DigestValue>...</ds:DigestValue>
                            </ds:Reference>
                        </ds:SignedInfo>
                        <ds:SignatureValue>...</ds:SignatureValue>
                        <ds:KeyInfo>
```

```
                        <ds:KeyName>356b4241808341cc9ff6295a43b01d00daab27406ddcd3f70
                    </ds:KeyInfo>
                </ds:Signature>
                <saml2:Subject>
                    <saml2:NameID Format="urn:oasis:names:tc:SAML:2.0:nameid-format:t
                        45e376c5-78a7-4cdc-a27d-a7dd5056e786
                    </saml2:NameID>
                    <saml2:SubjectConfirmation Method="urn:oasis:names:tc:SAML:2.0:cm
                        <saml2:SubjectConfirmationData InResponseTo="_a658d2c5c7426b1
                                                       NotOnOrAfter="2021-10-06T08:12
                                                       Recipient="http://sp.example.c
                    </saml2:SubjectConfirmation>
                </saml2:Subject>
                <saml2:Conditions NotBefore="2021-10-06T08:08:50.916Z" NotOnOrAfter="
                    <saml2:AudienceRestriction>
                        <saml2:Audience>urn:nl-eid-gdi:1.0:DV:00000009999999999004:en
                    </saml2:AudienceRestriction>
                </saml2:Conditions>
                <saml2:Advice>
                    <saml2:Assertion ID="_797775d153ac85fe682d1c89f668adc1" IssueInst
                                     Version="2.0" xmlns:saml2="urn:oasis:names:tc:SA
                        <saml2:Issuer>urn:nl-eid-gdi:1.0:AD:000000273813120000:entit
                        <ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
                            <ds:SignedInfo>
                                <ds:CanonicalizationMethod Algorithm="http://www.w3.o
                                <ds:SignatureMethod Algorithm="http://www.w3.org/2001
                                <ds:Reference URI="#_797775d153ac85fe682d1c89f668adc1
                                    <ds:Transforms>
                                        <ds:Transform
                                                Algorithm="http://www.w3.org/2000/09/
                                        <ds:Transform Algorithm="http://www.w3.org/20
                                    </ds:Transforms>
                                    <ds:DigestMethod Algorithm="http://www.w3.org/200
                                    <ds:DigestValue>...</ds:DigestValue>
                                </ds:Reference>
                            </ds:SignedInfo>
                            <ds:SignatureValue>...</ds:SignatureValue>
                            <ds:KeyInfo>
                                <ds:KeyName>24b1a2189f8af57114df0b93120f88b1d9cd38a0f
                                </ds:KeyName>
                            </ds:KeyInfo>
                        </ds:Signature>
                        <saml2:Subject>
                            <saml2:NameID Format="urn:oasis:names:tc:SAML:2.0:nameid-
                                45e376c5-78a7-4cdc-a27d-a7dd5056e786
                            </saml2:NameID>
                            <saml2:SubjectConfirmation Method="urn:oasis:names:tc:SAM
                                <saml2:SubjectConfirmationData
                                        InResponseTo="_a658d2c5c7426b11dfbdb1e30d4b0c
                                        NotOnOrAfter="2021-10-06T08:12:50.916Z"
                                        Recipient="http://sp.example.com"/>
                            </saml2:SubjectConfirmation>
                        </saml2:Subject>
                        <saml2:Conditions NotBefore="2021-10-06T08:08:50.916Z"
                                          NotOnOrAfter="2021-10-06T08:12:50.916Z">
                            <saml2:AudienceRestriction>
                                <saml2:Audience>urn:nl-eid-gdi:1.0:DV:000000099999999
                                </saml2:Audience>
                            </saml2:AudienceRestriction>
                        </saml2:Conditions>
                        <saml2:AuthnStatement AuthnInstant="2021-10-06T08:10:51.029Z"
                            <saml2:AuthnContext>
                                <saml2:AuthnContextClassRef>http://eid.logius.nl/LoA/
                                </saml2:AuthnContextClassRef>
                            </saml2:AuthnContext>
                        </saml2:AuthnStatement>
                        <saml2:AttributeStatement>
```

```
                        <saml2:Attribute Name="urn:nl-eid-gdi:1.0:ServiceUUID">
                            <saml2:AttributeValue>375b1cb114b7-12e9-3534-16cc-4d8
                        </saml2:Attribute>
                        <saml2:Attribute Name="urn:nl-eid-gdi:1.0:ActingSubjectID
                            <saml2:AttributeValue>
                                <saml2:EncryptedID>
                                    <xenc:EncryptedData xmlns:xenc="http://www.w3
                                                        Id="_e4ed5fc71f364184a43a
                                                        Type="http://www.w3.org/2
                                        <xenc:EncryptionMethod
                                                Algorithm="http://www.w3.org/2001
                                                xmlns:xenc="http://www.w3.org/200
                                        <ds:KeyInfo xmlns:ds="http://www.w3.org/2
                                            <ds:RetrievalMethod
                                                    Type="http://www.w3.org/2001/
                                                    URI="#_0cee1f147ad7e995e77e67
                                        </ds:KeyInfo>
                                        <xenc:CipherData xmlns:xenc="http://www.w
                                            <xenc:CipherValue>...</xenc:CipherVal
                                        </xenc:CipherData>
                                    </xenc:EncryptedData>
                                    <xenc:EncryptedKey xmlns:xenc="http://www.w3.
                                                       Id="_0cee1f147ad7e995e77e6
                                                       Recipient="urn:nl-eid-gdi:
                                        <xenc:EncryptionMethod
                                                Algorithm="http://www.w3.org/2001
                                                xmlns:xenc="http://www.w3.org/200
                                            <ds:DigestMethod xmlns:ds="http://www
                                                             Algorithm="http://ww
                                        </xenc:EncryptionMethod>
                                        <ds:KeyInfo xmlns:ds="http://www.w3.org/2
                                            <ds:KeyName>1d0bc832d839df789eca8bae6
                                        </ds:KeyInfo>
                                        <xenc:CipherData xmlns:xenc="http://www.w
                                            <xenc:CipherValue>...</xenc:CipherVal
                                        </xenc:CipherData>
                                        <xenc:ReferenceList>
                                            <xenc:DataReference URI="#_e4ed5fc71f
                                        </xenc:ReferenceList>
                                    </xenc:EncryptedKey>
                                            <xenc:EncryptedKey xmlns:xenc="http:/
                                                       Id="_0cee1f147ad7e995e77e6
                                                       Recipient="urn:nl-eid-gdi:
                                        <xenc:EncryptionMethod
                                                Algorithm="http://www.w3.org/2001
                                                xmlns:xenc="http://www.w3.org/200
                                            <ds:DigestMethod xmlns:ds="http://www
                                                             Algorithm="http://ww
                                        </xenc:EncryptionMethod>
                                        <ds:KeyInfo xmlns:ds="http://www.w3.org/2
                                            <ds:KeyName>2c0bc832d839df789eca8bae6
                                        </ds:KeyInfo>
                                        <xenc:CipherData xmlns:xenc="http://www.w
                                            <xenc:CipherValue>...</xenc:CipherVal
                                        </xenc:CipherData>
                                        <xenc:ReferenceList>
                                            <xenc:DataReference URI="#_e4ed5fc71f
                                        </xenc:ReferenceList>
                                    </xenc:EncryptedKey>
                                </saml2:EncryptedID>
                            </saml2:AttributeValue>
                        </saml2:Attribute>
                    </saml2:AttributeStatement>
                </saml2:Assertion>
                <saml2:Assertion ID="_c7a79a0e92311f0d3d2dadc247a855f6" IssueInst
                                 Version="2.0" xmlns:saml2="urn:oasis:names:tc:SA
                    <saml2:Issuer>urn:nl-eid-gdi:1.0:BVD:00000004003214345001:ent
```

```
<ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
    <ds:SignedInfo>
        <ds:CanonicalizationMethod Algorithm="http://www.w3.o
        <ds:SignatureMethod Algorithm="http://www.w3.org/2001
        <ds:Reference URI="#_c7a79a0e92311f0d3d2dadc247a855f6
            <ds:Transforms>
                <ds:Transform
                        Algorithm="http://www.w3.org/2000/09/
                <ds:Transform Algorithm="http://www.w3.org/20
            </ds:Transforms>
            <ds:DigestMethod Algorithm="http://www.w3.org/200
            <ds:DigestValue>...</ds:DigestValue>
        </ds:Reference>
    </ds:SignedInfo>
    <ds:SignatureValue>...</ds:SignatureValue>
    <ds:KeyInfo>
        <ds:KeyName>4202df88ba9faae2d2860a0d821d2bde10babc0a2
        </ds:KeyName>
    </ds:KeyInfo>
</ds:Signature>
<saml2:Subject>
    <saml2:NameID Format="urn:oasis:names:tc:SAML:2.0:nameid-
        45e376c5-78a7-4cdc-a27d-a7dd5056e786
    </saml2:NameID>
    <saml2:SubjectConfirmation Method="urn:oasis:names:tc:SAM
        <saml2:SubjectConfirmationData
                InResponseTo="_a658d2c5c7426b11dfbdb1e30d4b0c
                NotOnOrAfter="2021-10-06T08:12:50.916Z"
                Recipient="http://sp.example.com"/>
    </saml2:SubjectConfirmation>
</saml2:Subject>
<saml2:Conditions NotBefore="2021-10-06T08:08:50.916Z"
                  NotOnOrAfter="2021-10-06T08:12:50.916Z">
    <saml2:AudienceRestriction>
        <saml2:Audience>urn:nl-eid-gdi:1.0:DV:000000099999999
        </saml2:Audience>
    </saml2:AudienceRestriction>
</saml2:Conditions>
<saml2:AuthnStatement AuthnInstant="2021-10-06T08:10:51.090Z"
    <saml2:AuthnContext>
        <saml2:AuthnContextClassRef>http://eid.logius.nl/LoA/
        </saml2:AuthnContextClassRef>
    </saml2:AuthnContext>
</saml2:AuthnStatement>
<saml2:AttributeStatement>
    <saml2:Attribute Name="urn:nl-eid-gdi:1.0:ServiceUUID">
        <saml2:AttributeValue>375b1cb114b7-12e9-3534-16cc-4d8
    </saml2:Attribute>
        <saml2:Attribute Name="urn:nl-eid-gdi:1.1:Representat
          <saml2:AttributeValue>urn:nl-eid-gdi:1.1:RT:Zorg_Vo
    </saml2:Attribute>
    <saml2:Attribute Name="urn:nl-eid-gdi:1.0:ActingSubjectID
        <saml2:AttributeValue>
            <saml2:EncryptedID>
                <xenc:EncryptedData xmlns:xenc="http://www.w3
                                    Id="_d4eb5b0632d388373948
                                    Type="http://www.w3.org/2
                    <xenc:EncryptionMethod
                            Algorithm="http://www.w3.org/2001
                            xmlns:xenc="http://www.w3.org/200
                    <ds:KeyInfo xmlns:ds="http://www.w3.org/2
                        <ds:RetrievalMethod
                                Type="http://www.w3.org/2001/
                                URI="#_720276d2e729cdecd6889f
                    </ds:KeyInfo>
                    <xenc:CipherData xmlns:xenc="http://www.w
                        <xenc:CipherValue>...</xenc:CipherVal
```

```
                                    </xenc:CipherData>
                                </xenc:EncryptedData>
                                <xenc:EncryptedKey xmlns:xenc="http://www.w3.
                                                   Id="_720276d2e729cdecd6889
                                                   Recipient="urn:nl-eid-gdi:
                                    <xenc:EncryptionMethod
                                            Algorithm="http://www.w3.org/2001
                                            xmlns:xenc="http://www.w3.org/200
                                        <ds:DigestMethod xmlns:ds="http://www
                                                         Algorithm="http://ww
                                    </xenc:EncryptionMethod>
                                    <ds:KeyInfo xmlns:ds="http://www.w3.org/2
                                        <ds:KeyName>1d0bc832d839df789eca8bae6
                                    </ds:KeyInfo>
                                    <xenc:CipherData xmlns:xenc="http://www.w
                                        <xenc:CipherValue>...</xenc:CipherVal
                                    </xenc:CipherData>
                                    <xenc:ReferenceList>
                                        <xenc:DataReference URI="#_d4eb5b0632
                                    </xenc:ReferenceList>
                                </xenc:EncryptedKey>
                            </saml2:EncryptedID>
                        </saml2:AttributeValue>
                    </saml2:Attribute>
                    <saml2:Attribute Name="urn:nl-eid-gdi:1.0:LegalSubjectID"
                        <saml2:AttributeValue>
                            <saml2:EncryptedID>
                                <xenc:EncryptedData xmlns:xenc="http://www.w3
                                                    Id="_0fbab7451567b5041390
                                                    Type="http://www.w3.org/2
                                    <xenc:EncryptionMethod
                                            Algorithm="http://www.w3.org/2001
                                            xmlns:xenc="http://www.w3.org/200
                                    <ds:KeyInfo xmlns:ds="http://www.w3.org/2
                                        <ds:RetrievalMethod
                                                Type="http://www.w3.org/2001/
                                                URI="#_2cab7ef2667689c6064dda
                                    </ds:KeyInfo>
                                    <xenc:CipherData xmlns:xenc="http://www.w
                                        <xenc:CipherValue>...</xenc:CipherVal
                                    </xenc:CipherData>
                                </xenc:EncryptedData>
                                <xenc:EncryptedKey xmlns:xenc="http://www.w3.
                                                   Id="_2cab7ef2667689c6064dd
                                                   Recipient="urn:nl-eid-gdi:
                                    <xenc:EncryptionMethod
                                            Algorithm="http://www.w3.org/2001
                                            xmlns:xenc="http://www.w3.org/200
                                        <ds:DigestMethod xmlns:ds="http://www
                                                         Algorithm="http://ww
                                    </xenc:EncryptionMethod>
                                    <ds:KeyInfo xmlns:ds="http://www.w3.org/2
                                        <ds:KeyName>1d0bc832d839df789eca8bae6
                                    </ds:KeyInfo>
                                    <xenc:CipherData xmlns:xenc="http://www.w
                                        <xenc:CipherValue>...</xenc:CipherVal
                                    </xenc:CipherData>
                                    <xenc:ReferenceList>
                                        <xenc:DataReference URI="#_0fbab74515
                                    </xenc:ReferenceList>
                                </xenc:EncryptedKey>
                            </saml2:EncryptedID>
                        </saml2:AttributeValue>
                    </saml2:Attribute>
                </saml2:AttributeStatement>
            </saml2:Assertion>
        </saml2:Advice>
```

```
                <saml2:AuthnStatement AuthnInstant="2021-10-06T08:10:51.018Z" Session
                    <saml2:AuthnContext>
                        <saml2:AuthnContextClassRef>http://eid.logius.nl/LoA/basic</s
                        <saml2:AuthenticatingAuthority>urn:nl-eid-gdi:1.0:AD:00000002
                        </saml2:AuthenticatingAuthority>
                        <saml2:AuthenticatingAuthority>urn:nl-eid-gdi:1.0:BVD:0000000
                        </saml2:AuthenticatingAuthority>
                    </saml2:AuthnContext>
                </saml2:AuthnStatement>
                <saml2:AttributeStatement>
                    <saml2:Attribute Name="urn:nl-eid-gdi:1.0:ServiceUUID">
                        <saml2:AttributeValue>375b1cb114b7-12e9-3534-16cc-4d8997b0</s
                    </saml2:Attribute>
            <saml2:Attribute Name="urn:nl-eid-gdi:1.1:RepresentationType">
            <saml2:AttributeValue>urn:nl-eid-gdi:1.1:RT:Zorg_Volledig_Gezag_Kind</sam
            </saml2:Attribute>
                    <saml2:Attribute Name="urn:nl-eid-gdi:1.0:ActingSubjectID">
                        <saml2:AttributeValue>
                            <saml2:EncryptedID>
                                <xenc:EncryptedData xmlns:xenc="http://www.w3.org/200
                                                    Id="_c108a849ffb239e73ac6083348ad
                                                    Type="http://www.w3.org/2001/04/x
                                    <xenc:EncryptionMethod Algorithm="http://www.w3.o
                                                           xmlns:xenc="http://www.w3.
                                    <ds:KeyInfo xmlns:ds="http://www.w3.org/2000/09/x
                                        <ds:RetrievalMethod Type="http://www.w3.org/2
                                                            URI="#_df56cc944ecbb3a06f
                                    </ds:KeyInfo>
                                    <xenc:CipherData xmlns:xenc="http://www.w3.org/20
                                        <xenc:CipherValue>...</xenc:CipherValue>
                                    </xenc:CipherData>
                                </xenc:EncryptedData>
                                <xenc:EncryptedKey xmlns:xenc="http://www.w3.org/2001
                                                   Id="_df56cc944ecbb3a06fe5d0a0d45aa
                                                   Recipient="urn:nl-eid-gdi:1.0:DV:0
                                    <xenc:EncryptionMethod
                                            Algorithm="http://www.w3.org/2001/04/xmle
                                            xmlns:xenc="http://www.w3.org/2001/04/xml
                                        <ds:DigestMethod xmlns:ds="http://www.w3.org/
                                                         Algorithm="http://www.w3.org
                                    </xenc:EncryptionMethod>
                                    <ds:KeyInfo xmlns:ds="http://www.w3.org/2000/09/x
                                        <ds:KeyName>1d0bc832d839df789eca8bae611c3ad7e
                                    </ds:KeyInfo>
                                    <xenc:CipherData xmlns:xenc="http://www.w3.org/20
                                        <xenc:CipherValue>...</xenc:CipherValue>
                                    </xenc:CipherData>
                                    <xenc:ReferenceList>
                                        <xenc:DataReference URI="#_c108a849ffb239e73a
                                    </xenc:ReferenceList>
                                </xenc:EncryptedKey>
                            </saml2:EncryptedID>
                        </saml2:AttributeValue>
                    </saml2:Attribute>
                    <saml2:Attribute Name="urn:nl-eid-gdi:1.0:LegalSubjectID">
                        <saml2:AttributeValue>
                            <saml2:EncryptedID>
                                <xenc:EncryptedData xmlns:xenc="http://www.w3.org/200
                                                    Id="_5d50f7898d8afda532502d7f82e4
                                                    Type="http://www.w3.org/2001/04/x
                                    <xenc:EncryptionMethod Algorithm="http://www.w3.o
                                                           xmlns:xenc="http://www.w3.
                                    <ds:KeyInfo xmlns:ds="http://www.w3.org/2000/09/x
                                        <ds:RetrievalMethod Type="http://www.w3.org/2
                                                            URI="#_ea31225223bb330ed5
                                    </ds:KeyInfo>
                                    <xenc:CipherData xmlns:xenc="http://www.w3.org/20
```

```
                                    <xenc:CipherValue>...</xenc:CipherValue>
                                </xenc:CipherData>
                            </xenc:EncryptedData>
                            <xenc:EncryptedKey xmlns:xenc="http://www.w3.org/2001
                                               Id="_ea31225223bb330ed5fe42bb55f01
                                               Recipient="urn:nl-eid-gdi:1.0:DV:0
                                <xenc:EncryptionMethod
                                        Algorithm="http://www.w3.org/2001/04/xmle
                                        xmlns:xenc="http://www.w3.org/2001/04/xml
                                    <ds:DigestMethod xmlns:ds="http://www.w3.org/
                                                     Algorithm="http://www.w3.org
                                </xenc:EncryptionMethod>
                                <ds:KeyInfo xmlns:ds="http://www.w3.org/2000/09/x
                                    <ds:KeyName>1d0bc832d839df789eca8bae611c3ad7e
                                </ds:KeyInfo>
                                <xenc:CipherData xmlns:xenc="http://www.w3.org/20
                                    <xenc:CipherValue>...</xenc:CipherValue>
                                </xenc:CipherData>
                                <xenc:ReferenceList>
                                    <xenc:DataReference URI="#_5d50f7898d8afda532
                                </xenc:ReferenceList>
                            </xenc:EncryptedKey>
                        </saml2:EncryptedID>
                    </saml2:AttributeValue>
                </saml2:Attribute>
            </saml2:AttributeStatement>
        </saml2:Assertion>
    </saml2p:Response>
</saml2p:ArtifactResponse>
</soap11:Body>
</soap11:Envelope>
```

§ A.5 Example - ArtifactResolve

EXAMPLE 5: ArtifactResolve

```
<?xml version="1.0" encoding="UTF-8"?>
<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/">
    <soapenv:Body>
        <samlp:ArtifactResolve xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol"
                               xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion"
                               xmlns:ds="http://www.w3.org/2000/09/xmldsig#"
                               xmlns:ec="http://www.w3.org/2001/10/xml-exc-c14n#"
                               ID="_f0c06d3728f5da98c417b5add105d3c07cc3c868" Version="2.
                               IssueInstant="2021-06-03T10:38:38Z"
                               Destination="http://idp.example.com/resolve_artifact">
            <saml:Issuer>urn:nl-eid-gdi:1.0:DV:00000009999999999001:entities:0000</saml:I
            <ds:Signature>
                <ds:SignedInfo>
                    <ds:CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-e
                    <ds:SignatureMethod Algorithm="http://www.w3.org/2001/04/xmldsig-more
                    <ds:Reference URI="#_f0c06d3728f5da98c417b5add105d3c07cc3c868">
                        <ds:Transforms>
                            <ds:Transform Algorithm="http://www.w3.org/2000/09/xmldsig#en
                            <ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c1
                                <ec:InclusiveNamespaces PrefixList="ds saml samlp xs"/>
                            </ds:Transform>
                        </ds:Transforms>
                        <ds:DigestMethod Algorithm="http://www.w3.org/2001/04/xmlenc#sha2
                        <ds:DigestValue>...</ds:DigestValue>
                    </ds:Reference>
                </ds:SignedInfo>
                <ds:SignatureValue>...</ds:SignatureValue>
                <ds:KeyInfo>
                    <ds:KeyName>4492219ba557ce9e547a933d15ab87b14a69788d</ds:KeyName>
                </ds:KeyInfo>
            </ds:Signature>
            <samlp:Artifact>AAQAAHZHHN7zNFV4yhPfX5thN0sFe10xr4B3crRVEmPn4m3DE2V GisdfYs</
        </samlp:ArtifactResolve>
    </soapenv:Body>
</soapenv:Envelope>
```

§ A.6 Example - ArtifactResponse

EXAMPLE 6: ArtifactResponse

```
<?xml version="1.0" encoding="UTF-8"?>
<soap11:Envelope xmlns:soap11="http://schemas.xmlsoap.org/soap/envelope/">
    <soap11:Body>
        <saml2p:ArtifactResponse xmlns:saml2p="urn:oasis:names:tc:SAML:2.0:protocol"
                                 ID="_4d4d3e6984b2b2c036d7ee55d424ac78"
                                 InResponseTo="_8ecc43a04fc541f850fb66eb7259232b2d55627a"
                                 IssueInstant="2021-10-06T08:09:50.226Z" Version="2.0">
            <saml2:Issuer xmlns:saml2="urn:oasis:names:tc:SAML:2.0:assertion">
                urn:nl-eid-gdi:1.0:TD:00000004183317817000:entities:9000
            </saml2:Issuer>
            <ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
                <ds:SignedInfo>
                    <ds:CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-e
                    <ds:SignatureMethod Algorithm="http://www.w3.org/2001/04/xmldsig-more
                    <ds:Reference URI="#_4d4d3e6984b2b2c036d7ee55d424ac78">
                        <ds:Transforms>
                            <ds:Transform Algorithm="http://www.w3.org/2000/09/xmldsig#en
                            <ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c1
                        </ds:Transforms>
                        <ds:DigestMethod Algorithm="http://www.w3.org/2001/04/xmlenc#sha2
                        <ds:DigestValue>...</ds:DigestValue>
                    </ds:Reference>
                </ds:SignedInfo>
                <ds:SignatureValue>...</ds:SignatureValue>
                <ds:KeyInfo>
                    <ds:KeyName>356b4241808341cc9ff6295a43b01d00daab27406ddcd3f708a0a3761
                </ds:KeyInfo>
            </ds:Signature>
            <saml2p:Status>
                <saml2p:StatusCode Value="urn:oasis:names:tc:SAML:2.0:status:Success"/>
            </saml2p:Status>
            <saml2p:Response
                    Destination="http://sp.example.com"
                    ID="_99e95c51026d2af9914a2269a39519c5" InResponseTo="_e1234e91b147553
                    IssueInstant="2021-10-06T08:09:50.229Z" Version="2.0">
                <saml2:Issuer xmlns:saml2="urn:oasis:names:tc:SAML:2.0:assertion">
                    urn:nl-eid-gdi:1.0:TD:00000004183317817000:entities:9000
                </saml2:Issuer>
                <saml2p:Status>
                    <saml2p:StatusCode Value="urn:oasis:names:tc:SAML:2.0:status:Success"
                </saml2p:Status>
                <saml2:Assertion xmlns:saml2="urn:oasis:names:tc:SAML:2.0:assertion"
                                 ID="_12bb5ba7a77b6e09983fa26af000cfac" IssueInstant="202
                                 Version="2.0">
                    <saml2:Issuer>urn:nl-eid-gdi:1.0:TD:00000004183317817000:entities:900
                    <ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
                        <ds:SignedInfo>
                            <ds:CanonicalizationMethod Algorithm="http://www.w3.org/2001/
                            <ds:SignatureMethod Algorithm="http://www.w3.org/2001/04/xmld
                            <ds:Reference URI="#_12bb5ba7a77b6e09983fa26af000cfac">
                                <ds:Transforms>
                                    <ds:Transform Algorithm="http://www.w3.org/2000/09/xm
                                    <ds:Transform Algorithm="http://www.w3.org/2001/10/xm
                                </ds:Transforms>
                                <ds:DigestMethod Algorithm="http://www.w3.org/2001/04/xml
                                <ds:DigestValue>...</ds:DigestValue>
                            </ds:Reference>
                        </ds:SignedInfo>
                        <ds:SignatureValue>...</ds:SignatureValue>
                        <ds:KeyInfo>
```

```
                        <ds:KeyName>356b4241808341cc9ff6295a43b01d00daab27406ddcd3f70
                    </ds:KeyInfo>
                </ds:Signature>
                <saml2:Subject>
                    <saml2:NameID Format="urn:oasis:names:tc:SAML:2.0:nameid-format:t
                        6cdd6d85-a822-45cf-98f2-87792ab4c930
                    </saml2:NameID>
                    <saml2:SubjectConfirmation Method="urn:oasis:names:tc:SAML:2.0:cm
                        <saml2:SubjectConfirmationData InResponseTo="_e1234e91b147553
                                                       NotOnOrAfter="2021-10-06T08:11
                                                       Recipient="http://sp.example.c
                    </saml2:SubjectConfirmation>
                </saml2:Subject>
                <saml2:Conditions NotBefore="2021-10-06T08:07:48.953Z" NotOnOrAfter="
                    <saml2:AudienceRestriction>
                        <saml2:Audience>urn:nl-eid-gdi:1.0:DV:00000009999999999004:en
                    </saml2:AudienceRestriction>
                </saml2:Conditions>
                <saml2:Advice>
                    <saml2:Assertion ID="_8de0f8271f4938285bfb6f66541a3b33" IssueInst
                                     Version="2.0" xmlns:saml2="urn:oasis:names:tc:SA
                        <saml2:Issuer>urn:nl-eid-gdi:1.0:AD:000000273813120000:entit
                        <ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
                            <ds:SignedInfo>
                                <ds:CanonicalizationMethod Algorithm="http://www.w3.o
                                <ds:SignatureMethod Algorithm="http://www.w3.org/2001
                                <ds:Reference URI="#_8de0f8271f4938285bfb6f66541a3b33
                                    <ds:Transforms>
                                        <ds:Transform
                                                Algorithm="http://www.w3.org/2000/09/
                                        <ds:Transform Algorithm="http://www.w3.org/20
                                    </ds:Transforms>
                                    <ds:DigestMethod Algorithm="http://www.w3.org/200
                                    <ds:DigestValue>...</ds:DigestValue>
                                </ds:Reference>
                            </ds:SignedInfo>
                            <ds:SignatureValue>...</ds:SignatureValue>
                            <ds:KeyInfo>
                                <ds:KeyName>24b1a2189f8af57114df0b93120f88b1d9cd38a0f
                                </ds:KeyName>
                            </ds:KeyInfo>
                        </ds:Signature>
                        <saml2:Subject>
                            <saml2:NameID Format="urn:oasis:names:tc:SAML:2.0:nameid-
                                6cdd6d85-a822-45cf-98f2-87792ab4c930
                            </saml2:NameID>
                            <saml2:SubjectConfirmation Method="urn:oasis:names:tc:SAM
                                <saml2:SubjectConfirmationData
                                        InResponseTo="_e1234e91b14755343ff8c69c046cc4
                                        NotOnOrAfter="2021-10-06T08:11:48.953Z"
                                        Recipient="http://sp.example.com"/>
                            </saml2:SubjectConfirmation>
                        </saml2:Subject>
                        <saml2:Conditions NotBefore="2021-10-06T08:07:48.953Z"
                                          NotOnOrAfter="2021-10-06T08:11:48.953Z">
                            <saml2:AudienceRestriction>
                                <saml2:Audience>urn:nl-eid-gdi:1.0:DV:000000099999999
                                </saml2:Audience>
                            </saml2:AudienceRestriction>
                        </saml2:Conditions>
                        <saml2:AuthnStatement AuthnInstant="2021-10-06T08:09:50.300Z"
                            <saml2:AuthnContext>
                                <saml2:AuthnContextClassRef>http://eid.logius.nl/LoA/
                                </saml2:AuthnContextClassRef>
                            </saml2:AuthnContext>
                        </saml2:AuthnStatement>
                        <saml2:AttributeStatement>
```

```
                        <saml2:Attribute Name="urn:nl-eid-gdi:1.0:ServiceUUID">
                            <saml2:AttributeValue>375b1cb114b7-12e9-3534-16cc-4d8
                        </saml2:Attribute>
                        <saml2:Attribute Name="urn:nl-eid-gdi:1.0:ActingSubjectID
                            <saml2:AttributeValue>
                                <saml2:EncryptedID>
                                    <xenc:EncryptedData xmlns:xenc="http://www.w3
                                                        Id="_d0d48b29e94d76c6a0ee
                                                        Type="http://www.w3.org/2
                                        <xenc:EncryptionMethod
                                                Algorithm="http://www.w3.org/2001
                                                xmlns:xenc="http://www.w3.org/200
                                        <ds:KeyInfo xmlns:ds="http://www.w3.org/2
                                            <ds:RetrievalMethod
                                                    Type="http://www.w3.org/2001/
                                                    URI="#_ab71ea3bafb606b8a89c47
                                        </ds:KeyInfo>
                                        <xenc:CipherData xmlns:xenc="http://www.w
                                            <xenc:CipherValue>
                                                5q5RNYI9w79gCyq78PC8Pd3IY7GPaW3yc
                                            </xenc:CipherValue>
                                        </xenc:CipherData>
                                    </xenc:EncryptedData>
                                    <xenc:EncryptedKey xmlns:xenc="http://www.w3.
                                                       Id="_ab71ea3bafb606b8a89c4
                                                       Recipient="urn:nl-eid-gdi:
                                        <xenc:EncryptionMethod
                                                Algorithm="http://www.w3.org/2001
                                                xmlns:xenc="http://www.w3.org/200
                                            <ds:DigestMethod xmlns:ds="http://www
                                                             Algorithm="http://ww
                                        </xenc:EncryptionMethod>
                                        <ds:KeyInfo xmlns:ds="http://www.w3.org/2
                                            <ds:KeyName>1d0bc832d839df789eca8bae6
                                        </ds:KeyInfo>
                                        <xenc:CipherData xmlns:xenc="http://www.w
                                            <xenc:CipherValue>
                                                YoXfK3SOPgipqMg8bvkQ2hDOWwp6sbWrp
                                            </xenc:CipherValue>
                                        </xenc:CipherData>
                                        <xenc:ReferenceList>
                                            <xenc:DataReference URI="#_d0d48b29e9
                                        </xenc:ReferenceList>
                                    </xenc:EncryptedKey>
                                </saml2:EncryptedID>
                            </saml2:AttributeValue>
                        </saml2:Attribute>
                    </saml2:AttributeStatement>
                </saml2:Assertion>
            </saml2:Advice>
            <saml2:AuthnStatement AuthnInstant="2021-10-06T08:09:50.236Z" Session
                <saml2:AuthnContext>
                    <saml2:AuthnContextClassRef>http://eid.logius.nl/LoA/basic</s
                    <saml2:AuthenticatingAuthority>urn:nl-eid-gdi:1.0:AD:00000002
                    </saml2:AuthenticatingAuthority>
                </saml2:AuthnContext>
            </saml2:AuthnStatement>
            <saml2:AttributeStatement>
                <saml2:Attribute Name="urn:nl-eid-gdi:1.0:ServiceUUID">
                    <saml2:AttributeValue>375b1cb114b7-12e9-3534-16cc-4d8997b0</s
                </saml2:Attribute>
                <saml2:Attribute Name="urn:nl-eid-gdi:1.0:ActingSubjectID">
                    <saml2:AttributeValue>
                        <saml2:EncryptedID>
                            <xenc:EncryptedData xmlns:xenc="http://www.w3.org/200
                                                Id="_91c893eba1c1f87099c1d5a10b87
                                                Type="http://www.w3.org/2001/04/x
```

```
                                    <xenc:EncryptionMethod Algorithm="http://www.w3.o
                                                           xmlns:xenc="http://www.w3.
                                    <ds:KeyInfo xmlns:ds="http://www.w3.org/2000/09/x
                                        <ds:RetrievalMethod Type="http://www.w3.org/2
                                                            URI="#_449673558dd0810e91
                                    </ds:KeyInfo>
                                    <xenc:CipherData xmlns:xenc="http://www.w3.org/20
                                        <xenc:CipherValue>...</xenc:CipherValue>
                                    </xenc:CipherData>
                                </xenc:EncryptedData>
                                <xenc:EncryptedKey xmlns:xenc="http://www.w3.org/2001
                                                   Id="_449673558dd0810e91009297f56fd
                                                   Recipient="urn:nl-eid-gdi:1.0:DV:0
                                    <xenc:EncryptionMethod
                                            Algorithm="http://www.w3.org/2001/04/xmle
                                            xmlns:xenc="http://www.w3.org/2001/04/xml
                                        <ds:DigestMethod xmlns:ds="http://www.w3.org/
                                                         Algorithm="http://www.w3.org
                                    </xenc:EncryptionMethod>
                                    <ds:KeyInfo xmlns:ds="http://www.w3.org/2000/09/x
                                        <ds:KeyName>1d0bc832d839df789eca8bae611c3ad7e
                                    </ds:KeyInfo>
                                    <xenc:CipherData xmlns:xenc="http://www.w3.org/20
                                        <xenc:CipherValue>...</xenc:CipherValue>
                                    </xenc:CipherData>
                                    <xenc:ReferenceList>
                                        <xenc:DataReference URI="#_91c893eba1c1f87099
                                    </xenc:ReferenceList>
                                </xenc:EncryptedKey>
                            </saml2:EncryptedID>
                        </saml2:AttributeValue>
                    </saml2:Attribute>
                </saml2:AttributeStatement>
            </saml2:Assertion>
        </saml2p:Response>
    </saml2p:ArtifactResponse>
</soap11:Body>
</soap11:Envelope>
```

§ A.7 Example - ArtifactResponse with Representation

EXAMPLE 7: ArtifactResponse with Representation

```
<?xml version="1.0" encoding="UTF-8"?>
<soap11:Envelope xmlns:soap11="http://schemas.xmlsoap.org/soap/envelope/">
    <soap11:Body>
        <saml2p:ArtifactResponse xmlns:saml2p="urn:oasis:names:tc:SAML:2.0:protocol"
                                 ID="_0fb52522f6e41b750df938ef5ea50154"
                                 InResponseTo="_1ea090efda5655760b6a0c9dfa8884b66d475222"
                                 IssueInstant="2021-10-06T08:10:51.018Z" Version="2.0">
            <saml2:Issuer xmlns:saml2="urn:oasis:names:tc:SAML:2.0:assertion">
                urn:nl-eid-gdi:1.0:TD:00000004183317817000:entities:9000
            </saml2:Issuer>
            <ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
                <ds:SignedInfo>
                    <ds:CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-e
                    <ds:SignatureMethod Algorithm="http://www.w3.org/2001/04/xmldsig-more
                    <ds:Reference URI="#_0fb52522f6e41b750df938ef5ea50154">
                        <ds:Transforms>
                            <ds:Transform Algorithm="http://www.w3.org/2000/09/xmldsig#en
                            <ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c1
                        </ds:Transforms>
                        <ds:DigestMethod Algorithm="http://www.w3.org/2001/04/xmlenc#sha2
                        <ds:DigestValue>...</ds:DigestValue>
                    </ds:Reference>
                </ds:SignedInfo>
                <ds:SignatureValue>...</ds:SignatureValue>
                <ds:KeyInfo>
                    <ds:KeyName>356b4241808341cc9ff6295a43b01d00daab27406ddcd3f708a0a3761
                </ds:KeyInfo>
            </ds:Signature>
            <saml2p:Status>
                <saml2p:StatusCode Value="urn:oasis:names:tc:SAML:2.0:status:Success"/>
            </saml2p:Status>
            <saml2p:Response
                    Destination="sp.example.com"
                    ID="_31fa010c6af1bc61583f22c84b3a2b0d" InResponseTo="_a658d2c5c7426b1
                    IssueInstant="2021-10-06T08:10:51.018Z" Version="2.0">
                <saml2:Issuer xmlns:saml2="urn:oasis:names:tc:SAML:2.0:assertion">
                    urn:nl-eid-gdi:1.0:TD:00000004183317817000:entities:9000
                </saml2:Issuer>
                <saml2p:Status>
                    <saml2p:StatusCode Value="urn:oasis:names:tc:SAML:2.0:status:Success"
                </saml2p:Status>
                <saml2:Assertion xmlns:saml2="urn:oasis:names:tc:SAML:2.0:assertion"
                                 ID="_2a9deaff3a95b2193e74dbad4a69dfbf" IssueInstant="202
                                 Version="2.0">
                    <saml2:Issuer>urn:nl-eid-gdi:1.0:TD:00000004183317817000:entities:900
                    <ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
                        <ds:SignedInfo>
                            <ds:CanonicalizationMethod Algorithm="http://www.w3.org/2001/
                            <ds:SignatureMethod Algorithm="http://www.w3.org/2001/04/xmld
                            <ds:Reference URI="#_2a9deaff3a95b2193e74dbad4a69dfbf">
                                <ds:Transforms>
                                    <ds:Transform Algorithm="http://www.w3.org/2000/09/xm
                                    <ds:Transform Algorithm="http://www.w3.org/2001/10/xm
                                </ds:Transforms>
                                <ds:DigestMethod Algorithm="http://www.w3.org/2001/04/xml
                                <ds:DigestValue>...</ds:DigestValue>
                            </ds:Reference>
                        </ds:SignedInfo>
                        <ds:SignatureValue>...</ds:SignatureValue>
                        <ds:KeyInfo>
```

```
                        <ds:KeyName>356b4241808341cc9ff6295a43b01d00daab27406ddcd3f70
                    </ds:KeyInfo>
                </ds:Signature>
                <saml2:Subject>
                    <saml2:NameID Format="urn:oasis:names:tc:SAML:2.0:nameid-format:t
                        45e376c5-78a7-4cdc-a27d-a7dd5056e786
                    </saml2:NameID>
                    <saml2:SubjectConfirmation Method="urn:oasis:names:tc:SAML:2.0:cm
                        <saml2:SubjectConfirmationData InResponseTo="_a658d2c5c7426b1
                                                       NotOnOrAfter="2021-10-06T08:12
                                                       Recipient="http://sp.example.c
                    </saml2:SubjectConfirmation>
                </saml2:Subject>
                <saml2:Conditions NotBefore="2021-10-06T08:08:50.916Z" NotOnOrAfter="
                    <saml2:AudienceRestriction>
                        <saml2:Audience>urn:nl-eid-gdi:1.0:DV:00000009999999999004:en
                    </saml2:AudienceRestriction>
                </saml2:Conditions>
                <saml2:Advice>
                    <saml2:Assertion ID="_797775d153ac85fe682d1c89f668adc1" IssueInst
                                     Version="2.0" xmlns:saml2="urn:oasis:names:tc:SA
                        <saml2:Issuer>urn:nl-eid-gdi:1.0:AD:000000273813120000:entit
                        <ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
                            <ds:SignedInfo>
                                <ds:CanonicalizationMethod Algorithm="http://www.w3.o
                                <ds:SignatureMethod Algorithm="http://www.w3.org/2001
                                <ds:Reference URI="#_797775d153ac85fe682d1c89f668adc1
                                    <ds:Transforms>
                                        <ds:Transform
                                                Algorithm="http://www.w3.org/2000/09/
                                        <ds:Transform Algorithm="http://www.w3.org/20
                                    </ds:Transforms>
                                    <ds:DigestMethod Algorithm="http://www.w3.org/200
                                    <ds:DigestValue>...</ds:DigestValue>
                                </ds:Reference>
                            </ds:SignedInfo>
                            <ds:SignatureValue>...</ds:SignatureValue>
                            <ds:KeyInfo>
                                <ds:KeyName>24b1a2189f8af57114df0b93120f88b1d9cd38a0f
                                </ds:KeyName>
                            </ds:KeyInfo>
                        </ds:Signature>
                        <saml2:Subject>
                            <saml2:NameID Format="urn:oasis:names:tc:SAML:2.0:nameid-
                                45e376c5-78a7-4cdc-a27d-a7dd5056e786
                            </saml2:NameID>
                            <saml2:SubjectConfirmation Method="urn:oasis:names:tc:SAM
                                <saml2:SubjectConfirmationData
                                        InResponseTo="_a658d2c5c7426b11dfbdb1e30d4b0c
                                        NotOnOrAfter="2021-10-06T08:12:50.916Z"
                                        Recipient="http://sp.example.com"/>
                            </saml2:SubjectConfirmation>
                        </saml2:Subject>
                        <saml2:Conditions NotBefore="2021-10-06T08:08:50.916Z"
                                          NotOnOrAfter="2021-10-06T08:12:50.916Z">
                            <saml2:AudienceRestriction>
                                <saml2:Audience>urn:nl-eid-gdi:1.0:DV:000000099999999
                                </saml2:Audience>
                            </saml2:AudienceRestriction>
                        </saml2:Conditions>
                        <saml2:AuthnStatement AuthnInstant="2021-10-06T08:10:51.029Z"
                            <saml2:AuthnContext>
                                <saml2:AuthnContextClassRef>http://eid.logius.nl/LoA/
                                </saml2:AuthnContextClassRef>
                            </saml2:AuthnContext>
                        </saml2:AuthnStatement>
                        <saml2:AttributeStatement>
```

```
<saml2:Attribute Name="urn:nl-eid-gdi:1.0:ServiceUUID">
    <saml2:AttributeValue>375b1cb114b7-12e9-3534-16cc-4d8
</saml2:Attribute>
<saml2:Attribute Name="urn:nl-eid-gdi:1.1:RepresentationT
    <saml2:AttributeValue>OG0-11</saml2:AttributeValue>
</saml2:Attribute>
<saml2:Attribute Name="urn:nl-eid-gdi:1.0:ActingSubjectID
    <saml2:AttributeValue>
        <saml2:EncryptedID>
            <xenc:EncryptedData xmlns:xenc="http://www.w3
                                Id="_e4ed5fc71f364184a43a
                                Type="http://www.w3.org/2
                <xenc:EncryptionMethod
                        Algorithm="http://www.w3.org/2001
                        xmlns:xenc="http://www.w3.org/200
                <ds:KeyInfo xmlns:ds="http://www.w3.org/2
                    <ds:RetrievalMethod
                            Type="http://www.w3.org/2001/
                            URI="#_0cee1f147ad7e995e77e67
                </ds:KeyInfo>
                <xenc:CipherData xmlns:xenc="http://www.w
                    <xenc:CipherValue>...</xenc:CipherVal
                </xenc:CipherData>
            </xenc:EncryptedData>
            <xenc:EncryptedKey xmlns:xenc="http://www.w3.
                               Id="_0cee1f147ad7e995e77e6
                               Recipient="urn:nl-eid-gdi:
                <xenc:EncryptionMethod
                        Algorithm="http://www.w3.org/2001
                        xmlns:xenc="http://www.w3.org/200
                    <ds:DigestMethod xmlns:ds="http://www
                                     Algorithm="http://ww
                </xenc:EncryptionMethod>
                <ds:KeyInfo xmlns:ds="http://www.w3.org/2
                    <ds:KeyName>1d0bc832d839df789eca8bae6
                </ds:KeyInfo>
                <xenc:CipherData xmlns:xenc="http://www.w
                    <xenc:CipherValue>...</xenc:CipherVal
                </xenc:CipherData>
                <xenc:ReferenceList>
                    <xenc:DataReference URI="#_e4ed5fc71f
                </xenc:ReferenceList>
            </xenc:EncryptedKey>
        </saml2:EncryptedID>
    </saml2:AttributeValue>
</saml2:Attribute>
<saml2:Attribute Name="urn:nl-eid-gdi:1.0:LegalSubjectID"
    <saml2:AttributeValue>
        <saml2:EncryptedID>
            <xenc:EncryptedData xmlns:xenc="http://www.w3
                                Id="_46e926d560129ac37728
                                Type="http://www.w3.org/2
                <xenc:EncryptionMethod
                        Algorithm="http://www.w3.org/2001
                        xmlns:xenc="http://www.w3.org/200
                <ds:KeyInfo xmlns:ds="http://www.w3.org/2
                    <ds:RetrievalMethod
                            Type="http://www.w3.org/2001/
                            URI="#_0d819bc6f2168e97c83c58
                </ds:KeyInfo>
                <xenc:CipherData xmlns:xenc="http://www.w
                    <xenc:CipherValue>...</xenc:CipherVal
                </xenc:CipherData>
            </xenc:EncryptedData>
            <xenc:EncryptedKey xmlns:xenc="http://www.w3.
                               Id="_0d819bc6f2168e97c83c5
                               Recipient="urn:nl-eid-gdi:
```

```
                                    <xenc:EncryptionMethod
                                            Algorithm="http://www.w3.org/2001
                                            xmlns:xenc="http://www.w3.org/200
                                        <ds:DigestMethod xmlns:ds="http://www
                                                         Algorithm="http://ww
                                    </xenc:EncryptionMethod>
                                    <ds:KeyInfo xmlns:ds="http://www.w3.org/2
                                        <ds:KeyName>1d0bc832d839df789eca8bae6
                                    </ds:KeyInfo>
                                    <xenc:CipherData xmlns:xenc="http://www.w
                                        <xenc:CipherValue>...</xenc:CipherVal
                                    </xenc:CipherData>
                                    <xenc:ReferenceList>
                                        <xenc:DataReference URI="#_46e926d560
                                    </xenc:ReferenceList>
                                </xenc:EncryptedKey>
                            </saml2:EncryptedID>
                        </saml2:AttributeValue>
                    </saml2:Attribute>
                </saml2:AttributeStatement>
            </saml2:Assertion>
            <saml2:Assertion ID="_c7a79a0e92311f0d3d2dadc247a855f6" IssueInst
                             Version="2.0" xmlns:saml2="urn:oasis:names:tc:SA
                <saml2:Issuer>urn:nl-eid-gdi:1.0:BVD:00000004003214345001:ent
                <ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
                    <ds:SignedInfo>
                        <ds:CanonicalizationMethod Algorithm="http://www.w3.o
                        <ds:SignatureMethod Algorithm="http://www.w3.org/2001
                        <ds:Reference URI="#_c7a79a0e92311f0d3d2dadc247a855f6
                            <ds:Transforms>
                                <ds:Transform
                                        Algorithm="http://www.w3.org/2000/09/
                                <ds:Transform Algorithm="http://www.w3.org/20
                            </ds:Transforms>
                            <ds:DigestMethod Algorithm="http://www.w3.org/200
                            <ds:DigestValue>...</ds:DigestValue>
                        </ds:Reference>
                    </ds:SignedInfo>
                    <ds:SignatureValue>...</ds:SignatureValue>
                    <ds:KeyInfo>
                        <ds:KeyName>4202df88ba9faae2d2860a0d821d2bde10babc0a2
                        </ds:KeyName>
                    </ds:KeyInfo>
                </ds:Signature>
                <saml2:Subject>
                    <saml2:NameID Format="urn:oasis:names:tc:SAML:2.0:nameid-
                        45e376c5-78a7-4cdc-a27d-a7dd5056e786
                    </saml2:NameID>
                    <saml2:SubjectConfirmation Method="urn:oasis:names:tc:SAM
                        <saml2:SubjectConfirmationData
                                InResponseTo="_a658d2c5c7426b11dfbdb1e30d4b0c
                                NotOnOrAfter="2021-10-06T08:12:50.916Z"
                                Recipient="http://sp.example.com"/>
                    </saml2:SubjectConfirmation>
                </saml2:Subject>
                <saml2:Conditions NotBefore="2021-10-06T08:08:50.916Z"
                                  NotOnOrAfter="2021-10-06T08:12:50.916Z">
                    <saml2:AudienceRestriction>
                        <saml2:Audience>urn:nl-eid-gdi:1.0:DV:000000099999999
                        </saml2:Audience>
                    </saml2:AudienceRestriction>
                </saml2:Conditions>
                <saml2:AuthnStatement AuthnInstant="2021-10-06T08:10:51.090Z"
                    <saml2:AuthnContext>
                        <saml2:AuthnContextClassRef>http://eid.logius.nl/LoA/
                        </saml2:AuthnContextClassRef>
                    </saml2:AuthnContext>
```

```
                    </saml2:AuthnStatement>
                    <saml2:AttributeStatement>
                        <saml2:Attribute Name="urn:nl-eid-gdi:1.0:ServiceUUID">
                            <saml2:AttributeValue>375b1cb114b7-12e9-3534-16cc-4d8
                        </saml2:Attribute>
                        <saml2:Attribute Name="urn:nl-eid-gdi:1.0:ActingSubjectID
                            <saml2:AttributeValue>
                                <saml2:EncryptedID>
                                    <xenc:EncryptedData xmlns:xenc="http://www.w3
                                                        Id="_d4eb5b0632d388373948
                                                        Type="http://www.w3.org/2
                                        <xenc:EncryptionMethod
                                                Algorithm="http://www.w3.org/2001
                                                xmlns:xenc="http://www.w3.org/200
                                        <ds:KeyInfo xmlns:ds="http://www.w3.org/2
                                            <ds:RetrievalMethod
                                                    Type="http://www.w3.org/2001/
                                                    URI="#_720276d2e729cdecd6889f
                                        </ds:KeyInfo>
                                        <xenc:CipherData xmlns:xenc="http://www.w
                                            <xenc:CipherValue>...</xenc:CipherVal
                                        </xenc:CipherData>
                                    </xenc:EncryptedData>
                                    <xenc:EncryptedKey xmlns:xenc="http://www.w3.
                                                       Id="_720276d2e729cdecd6889
                                                       Recipient="urn:nl-eid-gdi:
                                        <xenc:EncryptionMethod
                                                Algorithm="http://www.w3.org/2001
                                                xmlns:xenc="http://www.w3.org/200
                                            <ds:DigestMethod xmlns:ds="http://www
                                                             Algorithm="http://ww
                                        </xenc:EncryptionMethod>
                                        <ds:KeyInfo xmlns:ds="http://www.w3.org/2
                                            <ds:KeyName>1d0bc832d839df789eca8bae6
                                        </ds:KeyInfo>
                                        <xenc:CipherData xmlns:xenc="http://www.w
                                            <xenc:CipherValue>...</xenc:CipherVal
                                        </xenc:CipherData>
                                        <xenc:ReferenceList>
                                            <xenc:DataReference URI="#_d4eb5b0632
                                        </xenc:ReferenceList>
                                    </xenc:EncryptedKey>
                                </saml2:EncryptedID>
                            </saml2:AttributeValue>
                        </saml2:Attribute>
                        <saml2:Attribute Name="urn:nl-eid-gdi:1.0:LegalSubjectID"
                            <saml2:AttributeValue>
                                <saml2:EncryptedID>
                                    <xenc:EncryptedData xmlns:xenc="http://www.w3
                                                        Id="_0fbab7451567b5041390
                                                        Type="http://www.w3.org/2
                                        <xenc:EncryptionMethod
                                                Algorithm="http://www.w3.org/2001
                                                xmlns:xenc="http://www.w3.org/200
                                        <ds:KeyInfo xmlns:ds="http://www.w3.org/2
                                            <ds:RetrievalMethod
                                                    Type="http://www.w3.org/2001/
                                                    URI="#_2cab7ef2667689c6064dda
                                        </ds:KeyInfo>
                                        <xenc:CipherData xmlns:xenc="http://www.w
                                            <xenc:CipherValue>...</xenc:CipherVal
                                        </xenc:CipherData>
                                    </xenc:EncryptedData>
                                    <xenc:EncryptedKey xmlns:xenc="http://www.w3.
                                                       Id="_2cab7ef2667689c6064dd
                                                       Recipient="urn:nl-eid-gdi:
                                        <xenc:EncryptionMethod
```

```
                                        Algorithm="http://www.w3.org/2001
                                        xmlns:xenc="http://www.w3.org/200
                                    <ds:DigestMethod xmlns:ds="http://www
                                                     Algorithm="http://ww
                                </xenc:EncryptionMethod>
                                <ds:KeyInfo xmlns:ds="http://www.w3.org/2
                                    <ds:KeyName>1d0bc832d839df789eca8bae6
                                </ds:KeyInfo>
                                <xenc:CipherData xmlns:xenc="http://www.w
                                    <xenc:CipherValue>...</xenc:CipherVal
                                </xenc:CipherData>
                                <xenc:ReferenceList>
                                    <xenc:DataReference URI="#_0fbab74515
                                </xenc:ReferenceList>
                            </xenc:EncryptedKey>
                        </saml2:EncryptedID>
                    </saml2:AttributeValue>
                </saml2:Attribute>
            </saml2:AttributeStatement>
        </saml2:Assertion>
    </saml2:Advice>
    <saml2:AuthnStatement AuthnInstant="2021-10-06T08:10:51.018Z" Session
        <saml2:AuthnContext>
            <saml2:AuthnContextClassRef>http://eid.logius.nl/LoA/basic</s
            <saml2:AuthenticatingAuthority>urn:nl-eid-gdi:1.0:AD:00000002
            </saml2:AuthenticatingAuthority>
            <saml2:AuthenticatingAuthority>urn:nl-eid-gdi:1.0:BVD:0000000
            </saml2:AuthenticatingAuthority>
        </saml2:AuthnContext>
    </saml2:AuthnStatement>
    <saml2:AttributeStatement>
        <saml2:Attribute Name="urn:nl-eid-gdi:1.0:ServiceUUID">
            <saml2:AttributeValue>375b1cb114b7-12e9-3534-16cc-4d8997b0</s
        </saml2:Attribute>
        <saml2:Attribute Name="urn:nl-eid-gdi:1.0:ActingSubjectID">
            <saml2:AttributeValue>
                <saml2:EncryptedID>
                    <xenc:EncryptedData xmlns:xenc="http://www.w3.org/200
                                        Id="_c108a849ffb239e73ac6083348ad
                                        Type="http://www.w3.org/2001/04/x
                        <xenc:EncryptionMethod Algorithm="http://www.w3.o
                                               xmlns:xenc="http://www.w3.
                        <ds:KeyInfo xmlns:ds="http://www.w3.org/2000/09/x
                            <ds:RetrievalMethod Type="http://www.w3.org/2
                                                URI="#_df56cc944ecbb3a06f
                        </ds:KeyInfo>
                        <xenc:CipherData xmlns:xenc="http://www.w3.org/20
                            <xenc:CipherValue>...</xenc:CipherValue>
                        </xenc:CipherData>
                    </xenc:EncryptedData>
                    <xenc:EncryptedKey xmlns:xenc="http://www.w3.org/2001
                                       Id="_df56cc944ecbb3a06fe5d0a0d45aa
                                       Recipient="urn:nl-eid-gdi:1.0:DV:0
                        <xenc:EncryptionMethod
                                Algorithm="http://www.w3.org/2001/04/xmle
                                xmlns:xenc="http://www.w3.org/2001/04/xml
                            <ds:DigestMethod xmlns:ds="http://www.w3.org/
                                             Algorithm="http://www.w3.org
                        </xenc:EncryptionMethod>
                        <ds:KeyInfo xmlns:ds="http://www.w3.org/2000/09/x
                            <ds:KeyName>1d0bc832d839df789eca8bae611c3ad7e
                        </ds:KeyInfo>
                        <xenc:CipherData xmlns:xenc="http://www.w3.org/20
                            <xenc:CipherValue>...</xenc:CipherValue>
                        </xenc:CipherData>
                        <xenc:ReferenceList>
                            <xenc:DataReference URI="#_c108a849ffb239e73a
```

```
                                    </xenc:ReferenceList>
                                </xenc:EncryptedKey>
                            </saml2:EncryptedID>
                        </saml2:AttributeValue>
                    </saml2:Attribute>
                    <saml2:Attribute Name="urn:nl-eid-gdi:1.0:LegalSubjectID">
                        <saml2:AttributeValue>
                            <saml2:EncryptedID>
                                <xenc:EncryptedData xmlns:xenc="http://www.w3.org/200
                                                    Id="_5d50f7898d8afda532502d7f82e4
                                                    Type="http://www.w3.org/2001/04/x
                                    <xenc:EncryptionMethod Algorithm="http://www.w3.o
                                                           xmlns:xenc="http://www.w3.
                                    <ds:KeyInfo xmlns:ds="http://www.w3.org/2000/09/x
                                        <ds:RetrievalMethod Type="http://www.w3.org/2
                                                            URI="#_ea31225223bb330ed5
                                    </ds:KeyInfo>
                                    <xenc:CipherData xmlns:xenc="http://www.w3.org/20
                                        <xenc:CipherValue>...</xenc:CipherValue>
                                    </xenc:CipherData>
                                </xenc:EncryptedData>
                                <xenc:EncryptedKey xmlns:xenc="http://www.w3.org/2001
                                                   Id="_ea31225223bb330ed5fe42bb55f01
                                                   Recipient="urn:nl-eid-gdi:1.0:DV:0
                                    <xenc:EncryptionMethod
                                            Algorithm="http://www.w3.org/2001/04/xmle
                                            xmlns:xenc="http://www.w3.org/2001/04/xml
                                        <ds:DigestMethod xmlns:ds="http://www.w3.org/
                                                         Algorithm="http://www.w3.org
                                    </xenc:EncryptionMethod>
                                    <ds:KeyInfo xmlns:ds="http://www.w3.org/2000/09/x
                                        <ds:KeyName>1d0bc832d839df789eca8bae611c3ad7e
                                    </ds:KeyInfo>
                                    <xenc:CipherData xmlns:xenc="http://www.w3.org/20
                                        <xenc:CipherValue>...</xenc:CipherValue>
                                    </xenc:CipherData>
                                    <xenc:ReferenceList>
                                        <xenc:DataReference URI="#_5d50f7898d8afda532
                                    </xenc:ReferenceList>
                                </xenc:EncryptedKey>
                            </saml2:EncryptedID>
                        </saml2:AttributeValue>
                    </saml2:Attribute>
                </saml2:AttributeStatement>
            </saml2:Assertion>
        </saml2p:Response>
    </saml2p:ArtifactResponse>
</soap11:Body>
</soap11:Envelope>
```

A.8 Example - LogoutRequest

EXAMPLE 8: LogoutRequest

```
<?xml version="1.0" encoding="UTF-8"?>
<samlp:LogoutRequest Destination="http://idp.example.com/request_logout"
                     ID="_2c952f14396dbab5f8c214d074e8e51272de9faa" IssueInstant="2021-10
                     xmlns:ds="http://www.w3.org/2000/09/xmldsig#" xmlns:ec="http://www.w
                     xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion"
                     xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol">
    <saml:Issuer>urn:nl-eid-gdi:1.0:DV:00000009999999999004:entities:0000</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-sha
            <ds:Reference URI="#_2c952f14396dbab5f8c214d074e8e51272de9faa">
                <ds:Transforms>
                    <ds:Transform Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-
                    <ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#">
                        <ec:InclusiveNamespaces PrefixList="ds saml samlp xs"/>
                    </ds:Transform>
                </ds:Transforms>
                <ds:DigestMethod Algorithm="http://www.w3.org/2001/04/xmlenc#sha256"/>
                <ds:DigestValue>...</ds:DigestValue>
            </ds:Reference>
        </ds:SignedInfo>
        <ds:SignatureValue>...</ds:SignatureValue>
        <ds:KeyInfo>
            <ds:KeyName>1d0bc832d839df789eca8bae611c3ad7ec5c5074</ds:KeyName>
        </ds:KeyInfo>
    </ds:Signature>
    <saml:SessionIndex>45e376c5-78a7-4cdc-a27d-a7dd5056e786</saml:SessionIndex>
    <saml:NameID>45e376c5-78a7-4cdc-a27d-a7dd5056e786</saml:NameID>
</samlp:LogoutRequest>
```

§ A.9 Example - LogoutResponse

EXAMPLE 9: LogoutResponse

```
<?xml version="1.0" encoding="UTF-8"?>
<samlp:LogoutResponse xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol"
                      xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion" xmlns:ds="http:/
                      ID="_1d0f30ecbc082449c36286d14063dcb4" Version="2.0" IssueInstant="
                      Destination="http://idp.example.com/single_logout_service"
                      InResponseTo="_4565109c3326bc3ab8c680d8efeaba7e22b7e304">
    <saml:Issuer>urn:nl-eid-gdi:1.0:TD:00000004183317817000:entities:9000</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-sha
            <ds:Reference URI="#_1d0f30ecbc082449c36286d14063dcb4">
                <ds:Transforms>
                    <ds:Transform Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-
                    <ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>
                </ds:Transforms>
                <ds:DigestMethod Algorithm="http://www.w3.org/2001/04/xmlenc#sha256"/>
                <ds:DigestValue>...</ds:DigestValue>
            </ds:Reference>
        </ds:SignedInfo>
        <ds:SignatureValue>...</ds:SignatureValue>
        <ds:KeyInfo>
            <ds:KeyName>24b1a2189f8af57114df0b93120f88b1d9cd38a0f06780377f6f8ace82fb0b18<
        </ds:KeyInfo>
    </ds:Signature>
    <samlp:Status>
        <samlp:StatusCode Value="urn:oasis:names:tc:SAML:2.0:status:Success"/>
    </samlp:Status>
</samlp:LogoutResponse>
```

§ B. Example SAML metadata

This section is non-normative.

§ B.1 Example - Metadata DV for RD

EXAMPLE 10: SAML metadata DV for RD

```
<md:EntityDescriptor xmlns:md="urn:oasis:names:tc:SAML:2.0:metadata"
                     xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion"
                     xmlns:dsig="http://www.w3.org/2000/09/xmldsig#"
                     xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
                     xmlns:xs="http://www.w3.org/2001/XMLSchema"
                     ID="_d611bce3fb2b4ee587bd508acfb89f2f1154815b"
                     entityID="urn:nl-eid-gdi:1.0:DV:00000004000000010000:entities:9002"
                     validUntil="2021-03-03T10:00:00Z"
>
    <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.org2001/04/xmldsig-more#rsa-sha256"/>
            <dsig:Reference
                    URI="#_d611bce3fb2b4ee587bd508acfb89f2f1154815b">
                <dsig:Transforms>
                    <dsig:Transform
                            Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signat
                    <dsig:Transform
                            Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>
                </dsig:Transforms>
                <dsig:DigestMethod
                        Algorithm="http://www.w3.org/2001/04/xmldsig-more#sha256"/>
                <dsig:DigestValue>...</dsig:DigestValue>
            </dsig:Reference>
        </dsig:SignedInfo>
        <dsig:SignatureValue>...</dsig:SignatureValue>
        <dsig:KeyInfo>
            <dsig:X509Data>
                <dsig:X509Certificate>...</dsig:X509Certificate>
            </dsig:X509Data>
        </dsig:KeyInfo>
    </dsig:Signature>
    <md:SPSSODescriptor AuthnRequestsSigned="true" WantAssertionsSigned="true"
                        protocolSupportEnumeration="urn:oasis:names:tc:SAML:2.0:protocol"
        <md:KeyDescriptor use="signing">
            <dsig:KeyInfo>
                <dsig:KeyName>dec5ed105fc56a8a6b85f83d1a4e7b64af0eb378</dsig:KeyName>
                <dsig:X509Data>
                    <dsig:X509Certificate>...</dsig:X509Certificate>
                </dsig:X509Data>
            </dsig:KeyInfo>
        </md:KeyDescriptor>
        <md:KeyDescriptor use="encryption">
            <dsig:KeyInfo>
                <dsig:KeyName>cdb948c5dfde5c9a53bf4916763dc973d55e8dd0</dsig:KeyName>
                <dsig:X509Data>
                    <dsig:X509Certificate>...</dsig:X509Certificate>
                </dsig:X509Data>
            </dsig:KeyInfo>
        </md:KeyDescriptor>
        <md:SingleLogoutService
                Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"
                Location="https://login.dv.test/saml/sp/logout"/>
        <md:AssertionConsumerService
                Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Artifact"
                Location="https://login.dv.test/saml/sp/acs" index="0" isDefault="true"/>
        <md:AttributeConsumingService index="0" isDefault="true">
```

```
            <md:ServiceName xml:lang="nl-NL">Dienstnaam 1</md:ServiceName>
            <md:RequestedAttribute Name="urn:nl-eid-gdi:1.0:ServiceUUID">
                <saml:AttributeValue xsi:type="xs:string">f847dc11-ac24-47b2-
                    84a8-a057440ce56d
                </saml:AttributeValue>
            </md:RequestedAttribute>
        </md:AttributeConsumingService>
    </md:SPSSODescriptor>
</md:EntityDescriptor>
```

§ B.2 Example - Metadata LC for RD

EXAMPLE 11: SAML metadata LC for RD

```
<md:EntitiesDescriptor xmlns:md="urn:oasis:names:tc:SAML:2.0:metadata"
                       xmlns:dsig="http://www.w3.org/2000/09/xmldsig#"
                       ID="_e611bce3fb2b4ee587bd508acfb89f2f1154815c"
                       validUntil="2021-03-03T10:00:00Z"
>
    <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-sha256"/>
            <dsig:Reference
                    URI="#_e611bce3fb2b4ee587bd508acfb89f2f1154815c">
                <dsig:Transforms>
                    <dsig:Transform
                            Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signat
                    <dsig:Transform
                            Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>
                </dsig:Transforms>
                <dsig:DigestMethod
                        Algorithm="http://www.w3.org/2001/04/xmldsig-more#sha256"/>
                <dsig:DigestValue>...</dsig:DigestValue>
            </dsig:Reference>
        </dsig:SignedInfo>
        <dsig:SignatureValue>...</dsig:SignatureValue>
        <dsig:KeyInfo>
            <dsig:X509Data>
                <dsig:X509Certificate>...</dsig:X509Certificate>
            </dsig:X509Data>
        </dsig:KeyInfo>
    </dsig:Signature>
    <md:EntityDescriptor xmlns:md="urn:oasis:names:tc:SAML:2.0:metadata"
                         xmlns:dsig="http://www.w3.org/2000/09/xmldsig#"
                         ID="_5d9c0e0ccb144714937dabffbf36e90ee57ee8ea"
                         entityID="urn:nl-eid-gdi:1.0:LC:00000008000000020000:entities:90
                         validUntil="2021-03-03T10:00:00Z"
    >
        <md:SPSSODescriptor AuthnRequestsSigned="true" WantAssertionsSigned="true"
                            protocolSupportEnumeration="urn:oasis:names:tc:SAML:2.0:proto
            <md:KeyDescriptor use="signing">
                <dsig:KeyInfo>
                    <dsig:KeyName>5138f7018e8a9f81dade8cf0e554134c4cefaf06</dsig:KeyName>
                    <dsig:X509Data>
                        <dsig:X509Certificate>...</dsig:X509Certificate>
                    </dsig:X509Data>
                </dsig:KeyInfo>
            </md:KeyDescriptor>
            <md:KeyDescriptor use="signing">
                <dsig:KeyInfo>
                    <dsig:KeyName>6cfed4024668054e3cbf327c060aed4b050e0e7e</dsig:KeyName>
                    <dsig:X509Data>
                        <dsig:X509Certificate>...</dsig:X509Certificate>
                    </dsig:X509Data>
                </dsig:KeyInfo>
            </md:KeyDescriptor>
            <md:SingleLogoutService
                    Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"
                    Location="https://login.lc.test/saml/sp/logout"/>
            <md:AssertionConsumerService
                    Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Artifact"
```

```
                    Location="https://login.lc.test/saml/sp/acs" index="0" isDefault="tru
        </md:SPSSODescriptor>
    </md:EntityDescriptor>
    <md:EntityDescriptor xmlns:md="urn:oasis:names:tc:SAML:2.0:metadata"
                         xmlns:dsig="http://www.w3.org/2000/09/xmldsig#"
                         ID="_d611bce3fb2b4ee587bd508acfb89f2f1154815b"
                         entityID="urn:nl-eid-gdi:1.0:DV:00000004000000010000:entities:90
                         validUntil="2021-03-03T10:00:00Z"
    >
        <md:SPSSODescriptor AuthnRequestsSigned="true" WantAssertionsSigned="true"
                            protocolSupportEnumeration="urn:oasis:names:tc:SAML:2.0:proto
            <md:KeyDescriptor use="encryption">
                <dsig:KeyInfo>
                    <dsig:KeyName>cdb948c5dfde5c9a53bf4916763dc973d55e8dd0</dsig:KeyName>
                    <dsig:X509Data>
                        <dsig:X509Certificate>...</dsig:X509Certificate>
                    </dsig:X509Data>
                </dsig:KeyInfo>
            </md:KeyDescriptor>
            <md:AssertionConsumerService
                    Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Artifact"
                    Location="https://login.lc.test/saml/sp/acs" index="0" isDefault="tru
        </md:SPSSODescriptor>
    </md:EntityDescriptor>
    <md:EntityDescriptor xmlns:md="urn:oasis:names:tc:SAML:2.0:metadata"
                         xmlns:dsig="http://www.w3.org/2000/09/xmldsig#"
                         ID="_c611bce3fb2b4ee587bd508acfb89f2f1154815a"
                         entityID="urn:nl-eid-gdi:1.0:DV:00000004000000020000:entities:90
                         validUntil="2021-03-03T10:00:00Z"
    >
        <md:SPSSODescriptor AuthnRequestsSigned="true" WantAssertionsSigned="true"
                            protocolSupportEnumeration="urn:oasis:names:tc:SAML:2.0:proto
            <md:KeyDescriptor use="encryption">
                <dsig:KeyInfo>
                    <dsig:KeyName>b459c1ecee731f2be4f50f68abe9bb070b5e2509</dsig:KeyName>
                    <dsig:X509Data>
                        <dsig:X509Certificate>...</dsig:X509Certificate>
                    </dsig:X509Data>
                </dsig:KeyInfo>
            </md:KeyDescriptor>
            <md:KeyDescriptor use="encryption">
                <dsig:KeyInfo>
                    <dsig:KeyName>45214df11fbed62751adf608d768f65d7fcd1e25</dsig:KeyName>
                    <dsig:X509Data>
                        <dsig:X509Certificate>...</dsig:X509Certificate>
                    </dsig:X509Data>
                </dsig:KeyInfo>
            </md:KeyDescriptor>
            <md:AssertionConsumerService
                    Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Artifact"
                    Location="https://login.lc.test/saml/sp/acs" index="0" isDefault="tru
        </md:SPSSODescriptor>
    </md:EntityDescriptor>
</md:EntitiesDescriptor>
```

B.3 Example - Metadata RD for DV

EXAMPLE 12: SAML metadata RD for DV

```
<md:EntityDescriptor xmlns:md="urn:oasis:names:tc:SAML:2.0:metadata"
                     xmlns:dsig="http://www.w3.org/2000/09/xmldsig#"
                     ID="_c92a6365a0d0ff7e3187ef1ca6cc14918f390db3"
                     entityID="urn:nl-eid-gdi:1.0:RD:00000004000000149000:entities:9002"
                     validUntil="2021-05-01T12:00:00Z">
    <dsig:Signature xmlns:dsig="http://www.w3.org/2000/09/xmldsig#" Id="Id000159766399661
        <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-sha256"/>
            <dsig:Reference
                    URI="#_c92a6365a0d0ff7e3187ef1ca6cc14918f390db3">
                <dsig:Transforms>
                    <dsig:Transform
                            Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signat
                    <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>...</dsig:DigestValue>
            </dsig:Reference>
        </dsig:SignedInfo>
        <dsig:SignatureValue>...</dsig:SignatureValue>
        <dsig:KeyInfo xmlns:dsig="http://www.w3.org/2000/09/xmldsig#" Id="Id0001597663996
            <dsig:KeyName>07c3d08bc6c3303a85c5e0c9547dfd91047f7c58</dsig:KeyName>
        </dsig:KeyInfo>
    </dsig:Signature>
    <md:IDPSSODescriptor WantAuthnRequestsSigned="true"
                         protocolSupportEnumeration="urn:oasis:names:tc:SAML:2.0:protocol
        <md:KeyDescriptor use="signing">
            <dsig:KeyInfo>
                <dsig:KeyName>07c3d08bc6c3303a85c5e0c9547dfd91047f7c58</dsig:KeyName>
                <dsig:X509Data>
                    <dsig:X509Certificate>...</dsig:X509Certificate>
                </dsig:X509Data>
            </dsig:KeyInfo>
        </md:KeyDescriptor>
        <md:ArtifactResolutionService
                Binding="urn:oasis:names:tc:SAML:2.0:bindings:SOAP"
                Location="https://artifact-pp2.toegang.overheid.nl/kvs/rd/resolve_artifac
                index="0"/>
        <md:SingleLogoutService
                Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"
                Location="https://pp2.toegang.overheid.nl/kvs/rd/request_logout"/>
        <md:SingleSignOnService
                Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"
                Location="https://pp2.toegang.overheid.nl/kvs/rd/request_authentication"/
    </md:IDPSSODescriptor>
</md:EntityDescriptor>
```

C. List of Figures

D. Index

D.1 Terms defined by this specification

X509Data

definition of §8.2.1

definition of §8.2.2.1

definition of §8.2.2.2

definition of §8.2.3

definition of §8.3.1.1

definition of §8.3.1.2

definition of §8.3.2

§ D.2 Terms defined by reference

§ E. References

§ E.1 Normative references

[BSNk.DEC]
BSNk PP technische specificaties. Logius. URL: https://gitlab.com/logius/bsnk/bsnk-techspecs/bsnk/-/raw/main/BPTSlive.pdf

[DigiD SAML3.x]
DigiD SAML3.x - legacy SAML specification for DigiD. LOGIUS. URL: https://www.logius.nl/domeinen/toegang/digid/documentatie/koppelvlakspecificatie-digid-saml-authenticatie

[eID SAML4.4]
eID SAML4.4 specification for DigiD. LOGIUS. URL: https://logius.gitlab.io/eid-saml/4.4/index.html

[eID SAML4.5]
eID SAML4.5 specification for DigiD. LOGIUS.

[NCSC.TLS]
ICT-beveiligingsrichtlijnen voor Transport Layer Security (TLS). NCSC. URL: https://www.ncsc.nl/documenten/publicaties/2019/mei/01/ict-beveiligingsrichtlijnen-voor-transport-layer-security-tls

[NORA]
Nederlandse Overheid Referentie Architectuur. URL: https://www.noraonline.nl/wiki/NORA_online

[RFC2119]
Key words for use in RFCs to Indicate Requirement Levels. S. Bradner. IETF. March 1997. Best Current Practice. URL: https://www.rfc-editor.org/rfc/rfc2119

[RFC8174]
Ambiguity of Uppercase vs Lowercase in RFC 2119 Key Words. B. Leiba. IETF. May 2017. Best Current Practice. URL: https://www.rfc-editor.org/rfc/rfc8174

[SAML2]
Security Assertion Markup Language (SAML) V2.0. OASIS. URL: https://www.oasis-open.org/standard/saml/

[SAML2.BINDINGS]
Bindings for the OASIS Security Assertion Markup Language (SAML) V2.0 – Errata Composite. OASIS. URL: https://groups.oasis-open.org/higherlogic/ws/public/download/56779/sstc-saml-bindings-errata-2.0-wd-06.pdf

[SAML2.CORE]
Assertions and Protocols for the OASIS Security Assertion Markup Language (SAML) V2.0 – Errata Composite. OASIS. URL: https://groups.oasis-open.org/higherlogic/ws/public/download/56776/sstc-saml-core-errata-2.0-wd-07.pdf

[SAML2.ERRATA.05]
SAML Version 2.0 Errata 05. OASIS. URL: https://docs.oasis-open.org/security/saml/v2.0/sstc-saml-approved-errata-2.0.html

[SAML2.METADATA]
Metadata for the OASIS Security Assertion Markup Language (SAML) V2.0 – Errata Composite. OASIS. URL: https://groups.oasis-open.org/higherlogic/ws/public/download/56785/sstc-saml-metadata-errata-2.0-wd-05.pdf

[SAML2.PROFILES]
Profiles for the OASIS Security Assertion Markup Language (SAML) V2.0 – Errata Composite. OASIS. URL: https://groups.oasis-open.org/higherlogic/ws/public/download/56782/sstc-saml-profiles-errata-2.0-wd-07.pdf

[SAML2.TO]
Security Assertion Markup Language (SAML) V2.0 Technical Overview. OASIS. URL: https://docs.oasis-open.org/security/saml/Post2.0/sstc-saml-tech-overview-2.0.html

[ST-SAML1.0]
Stelsel Toegang SAML v1.0 specification. LOGIUS. URL: https://logius.gitlab.io/digid-combiconnect

[XML.C14N.EXCL]
Exclusive XML Canonicalization. W3C. URL: https://www.w3.org/TR/xml-exc-c14n/

[XML.ENC]
XML Encryption Syntax and Processing. W3C. URL: https://www.w3.org/TR/2002/REC-xmlenc-core-20021210/

[XML.SIG]
XML Signature Syntax and Processing. W3C. URL: https://www.w3.org/TR/xmldsig-core/

↑