Logius
Ministerie van Binnenlandse Zaken en Koninkrijksrelaties

eID SAML4.4 specification

Datum	16 september 2020
Versie	4.4 final
Status	Definitief

Table of Contents

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 eID 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.

The 4.4 version of the eID SAML specification describes the exchange of representation information between the DV/LC and the RD, but this functionality will not be available initially. The exchange of representation information in eID SAML 4.4 has been described with forward compatibility in mind. At this point in time, it cannot be ruled out that DV/LC parties will need to implement a future version of the SAML eID spec to take full advantage of all representation functionality.

2 History

Version	Changes	Distribution
4.4 RC1	initial version	Public
4.4 RC2	corrections related to test findings	Internal
4.4 RC3	• added optional @Providername to AuthnRequest to support eIDAS • corrected typo's in the metadata specification • support of multi use certificates in metadata • use of sender/receiver instead of specific roles (DV/LC/RD)	Public
4.4 final	Final version of the 4.4 specifications. Changes • added support for optional element requestorID in SAML AuthnRequest to support use-cases where representation is mandatory. Errata • Fixed inconsistencies in naming-scheme: o Base URN is now urn:nl-eid-gdi:1.0 (in some cases urn:nl-eid-gdi:core was used) o Consistent use of colon (:) and period (.) in URN for Attribute Identifier types and entityID • validUntil / cacheDuration attributes in metadata o Fixed to match OASIS specification • Certificate-use in signatures. Principles regarding use of and references to certificates in signatures are described and applied.	Public

3 Frameworks

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

- saml-core-2.0-os
- saml-profiles-2.0-os
- saml-metadata-2.0-os
- saml-bindings-2.0-os
- saml errata

NORA, Nederlandse Overheid Referentie Architectuur (link).

NCSC ICT-beveiligingsrichtlijnen voor Transport Layer Security (TLS) (link)

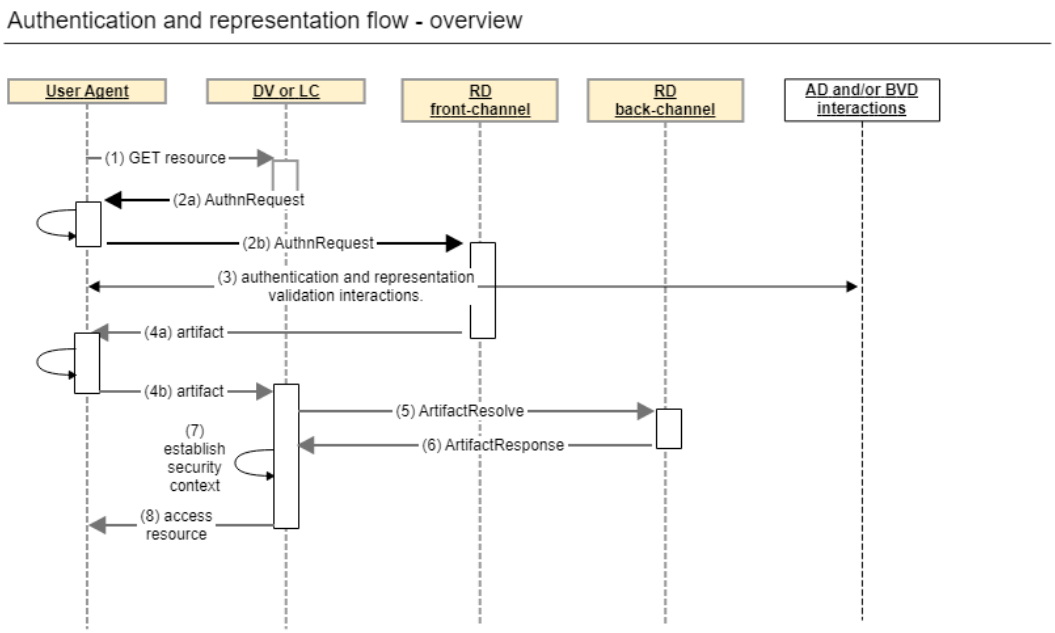
3.1 SAML profiles

A SAML profile is a specific set of rules that are used for a specific use case. SAML eID 4.4 uses two profiles of the SAML standard, namely:
• Web browser SSO profile, with HTTP Post binding (see below).

• Single Logout profile, with HTTP Post binding, issued by Session Participant to Identity Provider.

3.1.1 SAML message flows and bindings

Only the bindings that are listed in the tables are supported.



Front-channel (re)authentication.

#	Route	Bericht	Endpoint element	Binding	Meta-data
Step 2	DV/LC => Browser => RD	AuthnRequest	SingleSignOnService	HTTP-POST	RD IdP

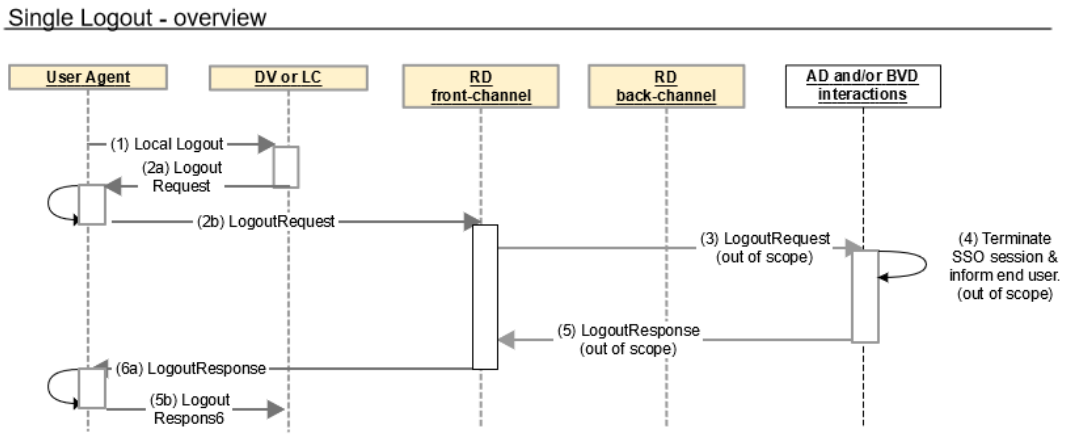
Step 4	RD => Browser => DV/LC	Artifact	AssertionConsumerService	HTTP-Artifact	DV/LC SP

Back-channel (Assertion)

#	Route	Bericht	Endpoint element	binding	Meta-data
Step 5	DV/LC => RD	ArtifactResolve	ArtifactResolutionService	SOAP	RD IdP
Step 6	RD => DV/LC	ArtifactResponse	None, is a direct response	SOAP	

3.1.1.1 SingleLogout messages and bindings

Only a limited form of SP initiated logout is supported by the RD within the context of an SSO federation. IdP initiated Logout is NOT supported. On receiving a logout request (step 1) a DV which participates in a SSO federation MUST send a Logout request to the RD (step 2a/b). The RD validates the LogoutRequest, and if the RD still maintains an active session with that User's webbrowser, the RD will terminate that session. In any case the RD will reply with a LogoutResponse with succes status if the LogoutRequest was valid.



#	Route	Bericht	Endpoint element	binding	Meta-data
Step 2	DV/LC => Browser => RD	LogoutRequest	SingleLogoutService	HTTP-POST	RD IdP
Step 6	RD => Browser => DV/LC	LogoutResponse	SingleLogoutService	HTTP-POST	DV/LC SP

4 Glossary

Begrip/afkorting	English	Nederlands	Explanation
Artifact	Artifact		(SAML) Pointer to SAML message that is sent through the front-channel, to avoid exposing sensitive data to the UA of the End-User.
Assertion	Assertion		SAML Assertion.
Back channel	Back channel		Communication-channel between DV/LC, RD, AD, BVD, eTD. (not interacting with end-user)
LoA	Level of Assurance, LoA	Betrouwbaarheidsniveau	See also Levels of Assurance
BVD	BVD	Role: Bevoegdheidsverklaringsdienst	See also Roles
DV	SP		See also Roles
Service	Service	Dienst	Service offered by a DV,
SSO	Single Sign On	Eenmalig Inloggen	
End User		Eindgebruiker	Citizen/actor authenticating himself to consume a Service on his own behalf, or to represent someone else.
Front channel	Front channel		Communication between DV/LC, RD, AD or BVD and UA of End-user.
Identity Provider (IDP)	Identity Provider (IDP)	De AuthenticatieDienst (AD)	See also Roles
LC	Cluster Connection Provider	Leverancier Clusteraansluiting	See also Roles
Metadata	Metadata		Before a SAML connection can be established, all parties, DV/LC and RD must exchange connection properties. This is done through Metadata. See

Begrip/afkorting	English	Nederlands	Explanation
			SAML Metadata for more information.
Participant	Participant	Deelnemer	Any party that has a role in the authentication or representation processes that are withi the scope of this specification. These include DV, RD, LC AD and BVD.
RD	Routeringsdienst	Routeringsdienst	See also Roles
RV	Routeringsvoorziening	Routeringsvoorziening	See also Roles
SAML	SAML		De SAML v 2.0 standaard, ook SAML2.0 genoemd. SAML staat voor Security Assertion Markup Language.
SLO	SLO	Federatief uitloggen	Single Log Off, feature
UA	UA		User Agent van de Eindgebruiker (bijvoorbeeld een browser).

4.1 Roles

De volgende rollen worden gebruikt.

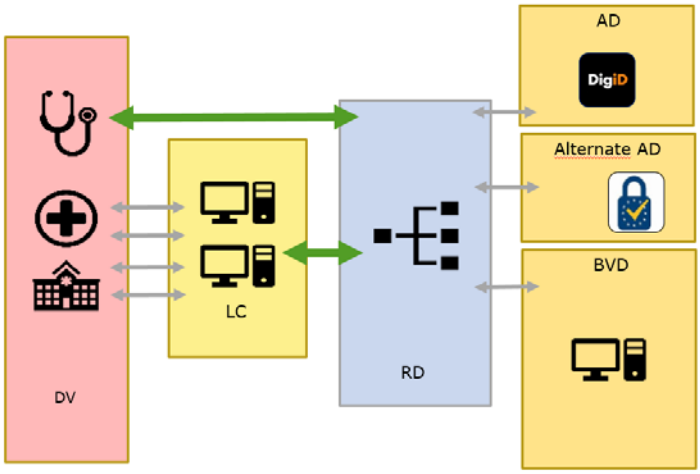
Afkorting	Rol	Description	Example
AD	Authenticatiedienst	Identity Provider (IDP)	DigiD, eTD AD, eIDAS out
DV	Dienstverlener	Service Provider (SP)	Gemeente, huisarts, overheidsinstelling
RD	Routeringsdienst	Realization of one of the (technical) implementations of the Routeringsvoorziening.	TVS, IdentityBridge
RV	Routeringsvoorziening	Facility which unburdens Service Providers when accepting multiple Identity Providers.	Beheerorganisatie Routeringsvoorziening
LC	Leverancier Clusteraansluiting	Clusterconnection provider: This role assists the DV in connecting to the RD. LC's will handle all	SaaS providers within the health-care field.

Afkorting	Rol	Description	Example
		connectivity to the RD for their registered DV's.	
BVD	Bevoegdheidsverklaringsdienst	Service that provides assertions for representation relationships. Within eTD, eTD MR's also have this role.	De BVD van programma Machtigen
MR	Mandate Register (or *Machtigingenregister* in Dutch)	Public or Private entity registering and attesting to a (formalized) representation relationship.	eHerkenning MR's, Publiek Machtigingsregister bij programma Machtigen (voorheen DigiD Machtigen)

5 Introduction

5.1 Introduction

eID SAML 4.4 specifies the communication between Dienstverlener (DV) and Routeringsdienst (RD) and between Leverancier Clusteraansluiting (LC) and RD, as shown by the green lines in figure 1.



.

eID SAML 4.4 supports the use cases summarized below:

Authentication	Authenticating a User for a single Service, for a single purpose. This is the most basic use case scenario from a Service Provider's point of view. Authentication always implies consent of the user for accessing the service and may include authorization if the User is using representation.
Cluster connection connectivity	In a Cluster connection setting, a LC is technically responsible for connecting a DV to the RD.
Authentication with representation	A User authenticates with the intent to consume the Service on behalf of another person using a Representation Relationship that is registered within an MR.
Authentication with AD/BVD preselection	Authenticating a User where selection for the Identity Provider (IDP) or BVD is done at the Service Provider prior to the authentication request to the RD in order to optimize the user experience.

SAML specification

The document is not a complete SAML reference. (see http://docs.oasis-open.org/security/saml/Post2.0/sstc-saml-tech-overview-2.0.html)

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 - RD and LC - RD.
- SAML Metadata - Contains metadata definitions for DV, LC and RD.

Additional guidance

Additional guidance is provided for topics that do relate to this SAML specification, but are not part of the formal specification.

Additional guidance can be found here:
https://logius.nl/diensten/routeringsvoorziening/documentatie

5.2 Interface versioning

Version	Description	Status
4.4	Fisrt version of the eID SAML specifications to be used for connecting to a RD. Scope for this version is limited to the interactions between the roles DV-RD and LC-RD.	Final
4.0	DigiD CA 4.0 Specification. New version of DigiD specification, introducing Encrypted BSN and support for LC	Pilot

6 Supported Usecases (DV/LC - RD)

6.1 Authentication

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

6.1.1 Actors

Roles
End User
DV
RD
AD

For more information see also Roles

6.1.2 Functional description

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

The End User visits the website of the Service, where the End User 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 User to the RD, requesting authentication of the End User for the Service. At the RD the End User selects the AD of his/her choice. Note that in this use case the End User will *not* select to act on behalf of another. (See Authentication with representation)

Next, the End User is redirected to the selected AD. After successful authentication the AD takes care the End User is redirected back to the RD, who includes the attestation of identity in the relevant interface response to the DV. This response includes at minimum an identifier of the End User, the Levels of Assurance attested to and the Service authenticated for.

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

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

6.2 Authentication with representation

An acting End User intends to consume a Service to represent another party, from a DV, for which authentication is required. The End User, or Acting End User on behalf of a represented party, can act in the role of a Natural Person or as a Legal entity, using a representation relationship. The represented party can also be either a Natural Person or a Legal Entity. The relationship has to be formalized and may be either a direct relationship, either voluntarily on legal grounds, or a chain of representation relationships.

In the context of this specification, any (legal) form of representation is included. A non exhaustive list of examples includes: voluntary authorization, representative assigned by court order (guardian, administrator), statutory signatory (director, president), limited authorized signatory, etc...

The Acting End User acts on behalf of the represented party. The representation relationship underpinning this must be registered as a formalized authorization in a Machtigingenregister (MR), prior to application in this use case.

The authentication of the Acting End User can take place at any supporting AD, just like in the Authentication usecase. Similarly, the representation information concerning both the Acting End User, the represented party and the service(s) for which they have a representation relation can come from multiple MR's. A BVD offers a single point of contact through which multiple MR's are available. Also available through the RD is the eTD framework which offers information from eHerkenning MR's. At the moment, this specification describes how such information from either route is made available through the RD. More complex cases where a part of a representation relationship is available through one route, and a part through the other (ketenmachtiging over eTD and BVD), are not yet supported.

> Rules governing representation and registration of a registration relationship are out of scope of this specification.

6.2.1 Actors

Role	Role description
Acting End User	A User intending to consume a Service on behalf of another Person.
Represented party	A Natural Person or Legal entity who is represented by an Acting End User.
DV	More information: Roles
RD	More information: Roles
AD	More information: Roles
BVD	More information: Roles

6.2.2 Functional description

The Acting End User visits the website of the Service, where the User may have to interact to indicate the intent to consume the Service. As the Service requires authentication, this triggers the authentication process. Optionally, the Acting End User may be able to indicate the intent to consume the Service on behalf of someone else.

The DV will now redirect the Acting End User to the RD, requesting authentication of the User for the Service, optionally including the request to authorize based on a representation relationship. The User will now have to choose the AD of choice and the applicable BVD. If not yet passed with the request, the Acting End User will have to select the option to act on behalf of another Represented party.

Next, the Acting End User is redirected to the selected AD. After successful authentication, the AD redicrects the Acting End User to the RD. The RD will then redirect the Acting End User to a BVD. Here the Acting End User selects the representation relationship to use, if multiple options are available. Afterwards the BVD redirects the User back to the RD.

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 User and the Service Consumer, the Levels of Assurance attested to and the Service authenticated for.

The DV can now take an access control decision to its Service for the User on behalf of the Service Consumer.

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

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.

> 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 directly offers eID-connectivity; 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 Usecases (DV/LC - RD). The LC is registered with the 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 the RD and in LC-metadata.

DV initiates authentication via the LC. The LC will send an AuthnRequest to the RD for the DV.

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

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

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

6.4 Authentication with AD/BVD preselection

A User intends to consume a Service on his/her own behalf, from a (semi-)governmental or public Service Provider, for which authentication is required. The User makes the selection for the AD at the DV, rather than at the RD. In order to improve 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 User can (also) select the BVD at the DV.

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

6.4.1 Actors

Role	
End-User	
DV	See also: Roles
RD	
AD	
BVD	

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 RouteringsDienst, the User selects the AD and/or BVD for usage at an earlier stage at the Service Provider. 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 User to further narrow down the selection.

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

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

7 SAML Message specification

7.1 SAML authentication steps

The diagram below contains the authentication steps that are made when an end user 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.

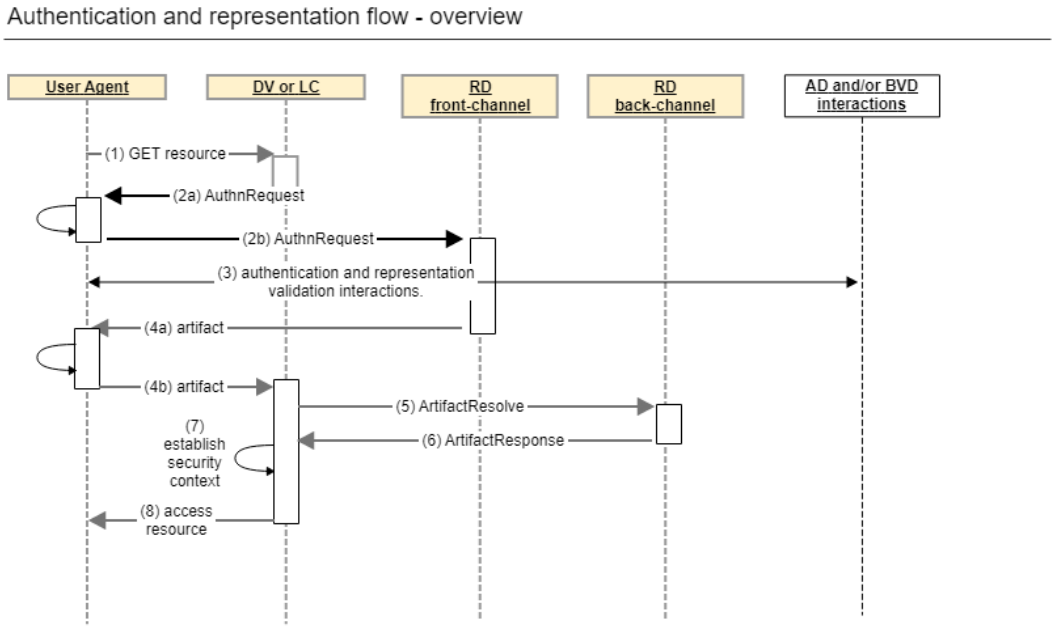


Figure 1 SAML authentication flow

Figure SAML authentication flow

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 end user's Browser, or Step 1 and Step 5 in the figure above. The back channel is the direct communication between the DV or LC and RD (step 6 and Step 7 in the figure above). This distinction is important because the user-defined attributes (such as the citizen service number) are never sent via the front channel, so that they can never be intercepted or changed by the end user's browser. All SAML back channel messages are placed in a SOAP envelope.

Step 1

The end user with a browser as User Agent (UA) wants to access a part on the web service of the service provider that requires authentication of the end user.

Step 2

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

Step 3 (out of scope for this specification)

In this step the RD will offer the user 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 end user hasn't already chosen in step 2, the end user chooses an authentication method that meets the minimum required Level of Assurance, and also chooses whether to use representation. The end user is presented with the corresponding AD login screen. The end user authenticates with the chosen means.

Optionally, the end user also chooses a representation method. The end user is presented with the corresponding screen with choice of who to represent. The end user chooses the correct legal subject to represent.

Step 4

The RD sends the end user back to the DV or LC via a redirect. A meaningless artifact generated by RD is sent here. This artifact refers to the actual SAML response message (ArtifactResponse) that is stored at the RD. In step 5, the DV or LC requests the response message via the back channel based on the artifact.

Even if the authentication in step 3 was unsuccessful or interrupted, an artifact is sent to the DV or LC. This artifact provides an error message with the ArtifactResolve and cannot be exchanged for a valid Assertion.

Step 5

With the artifact, the DV or LC retrieves the authentication & representation message from RD via the back channel. With the artifact from the artifact message the result of the (successful or unsuccessful) authentication and representation can be retrieved via the back channel.

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

Step 6

RD replies with the ArtifactResponse 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) identitie(s) and attrubute(s) of the end user and optionally the represented party. The identities end attributes are encrypted so that only the intended DV(s) can obtain 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 end user.

Step 7 & 8

Successful authentication / selection of representation gives the DV information needed for access control decision typically resulting in user access to service in step 8.

7.2 SAML Message specification

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.**

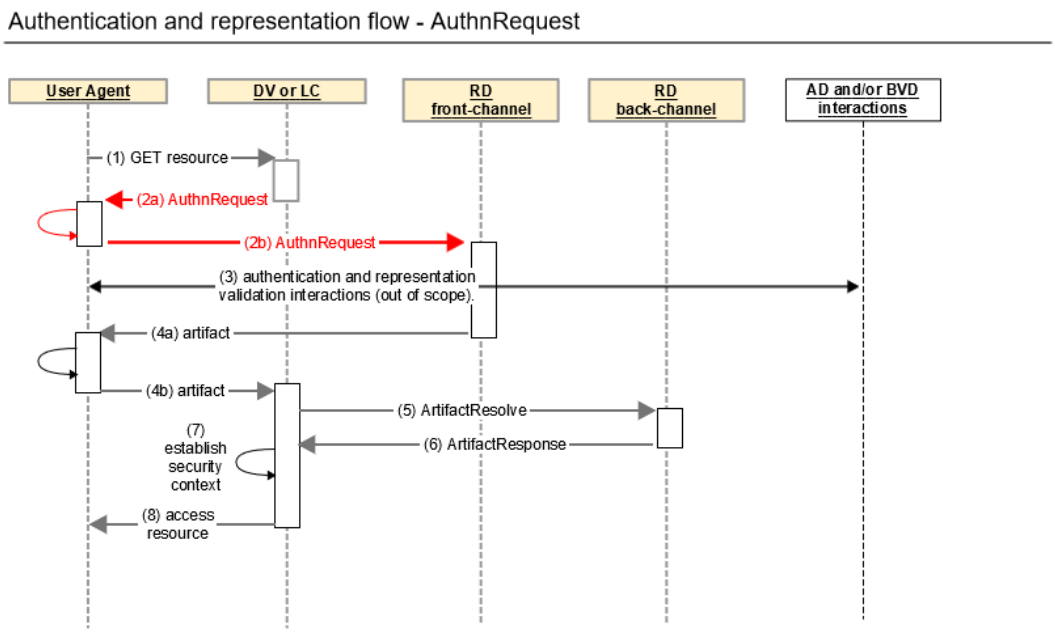
3. **Optional SAML elements that are not in this specification SHOULD NOT be included. When present they will be ignored when possible.**

7.3 SAML 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 <AuthnRequest> message element to a SAML authority and request that it return a <Response> message containing one or more such assertions.

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

Sender	DV	LC
Recipient	RD	RD



7.3.1 <AuthnRequest>

AuthnRequest examples

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 the metadata.
@ForceAuthn	0..1	The value 'true' indicates that an existing single sign-on session MUST NOT be used for the request in question. If the value is 'false' or empty or the attribute is missing, the AD MAY use an existing SSO session if present and applicable.
@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 inluded.
@ProviderName	0..1	Conditional. Reserved for use with eIDAS UIT to show information about the foreign service Provider and country in order to obtain user 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 Technical requirements and recommendations for details.
AttributeConsumingServiceIndex	0..1	Conditional. Only one of <Extensions> or <AttributeConsumerServiceIndex> MUST be present. This element MAY only be used if the issuer is a DV. This element MUST NOT be used in other cases. If present, MUST refer to an AttributeConsumingService in the DV's metadata.
Extensions	0..1	Conditional. Only one of <Extensions> or <AttributeConsumerServiceIndex> MUST be present. This element MUST be included if the issuer is not a DV. This element MAY be used when the issuer is a DV. If present MUST contain the attributes IntendedAudience and ServiceUUID. See "The use of <AttributeConsumingService> or <Extensions> for referring to service definitions" below.
-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: support for more than one audience where each audience receives the audience specific EncryptedID

		is provided by the Service Definition registered with the Service Catalogus.
-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 catalogus of the receiver.
Scoping	0..1	OPTIONAL element.
-IDPList	0..1	OPTIONAL element. MAY be used to limit the selection of AD's or BVD's at the RD.
--IDPEntry	1..n	At least one IDPEntry 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 saml-core-2.0-os , section 3.2.2.2: • urn:oasis:names:tc:SAML:2.0:status:NoSupportedIDP MUST contain at least the EntityID of one AD. If the list also contains the EnityID 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 user choose whether to use representation with a BVD. The RD MUST limit the AD and BVD selection list presented tu users to 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	Optional element. MAY be used to make representation with a BVD mandatory for this AuthnRequest. If used it MUST contain one or more EntityID's of BVD's and use of representation is mandatory for this AuthnRequest.

7.3.1.1 The use of <AttributeConsumingService> or <Extensions> for referring to service definitions

This specification uses the concept of a services catalog which contains amongst others "service definitions". A service definition has a unique UUID (ServiceUUID) to identify a service definition in the service catalog. However, in the SAML messages the reference may use the concept of providing the AttributeConsumingServiceIndex to refer to an AttributeConsumingService entry in the DV metadata. The AttributeConsumingService of the DV MUST contain a reference to the requested ServiceUUID. Only a DV MAY use the AttributeConsumingServiceIndex. All other participants MUST use the <Extensions>.element in the AuthnRequest which supplies both the EntityID of the DV and the ServiceUUID thus enabling the RD to identify the ServiceUUID. A DV MAY use either the <AttributeConsumingServiceIndex> or the <Extensions> element. When using the AttributeConsumingService the RD will retrieve the DV's EntityID form the <Issuer> element in the AuthnRequest.

7.3.1.2 Processing rules:

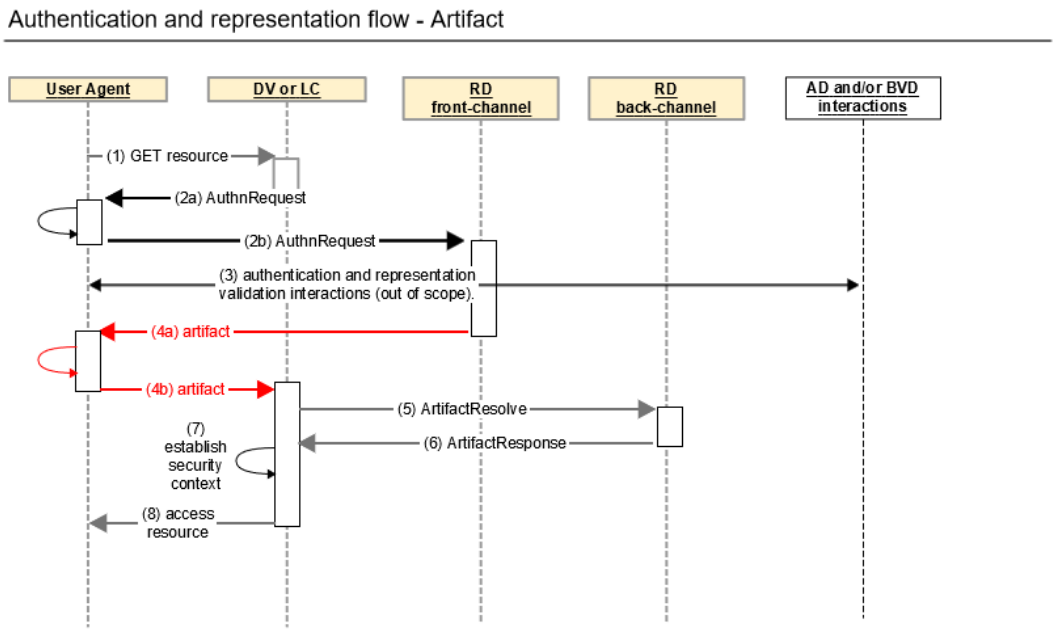
In addition to the processing rules required by the SAML specification the following rules apply:

1. The RD MUST:
    a. validate that the DV is registered for the requested Servicedefinition (serviceUUID) referenced by the ServiceIndex in the DV metadata or the <Extensions> and that the registration is valid;
    b. (in case when an LC is involved) validate that the DV is registered to use the requested ServiceUUID with the LC that sends the Authnrequest on behalf of the DV and that the registration is valid;
    c. If any of these validations fails, the authenentication MUST fail.

7.4 SAML AuthnRequest response message

The sender and recipient of this message are the following:

Sender	DV	LC
Recipient	RD	RD



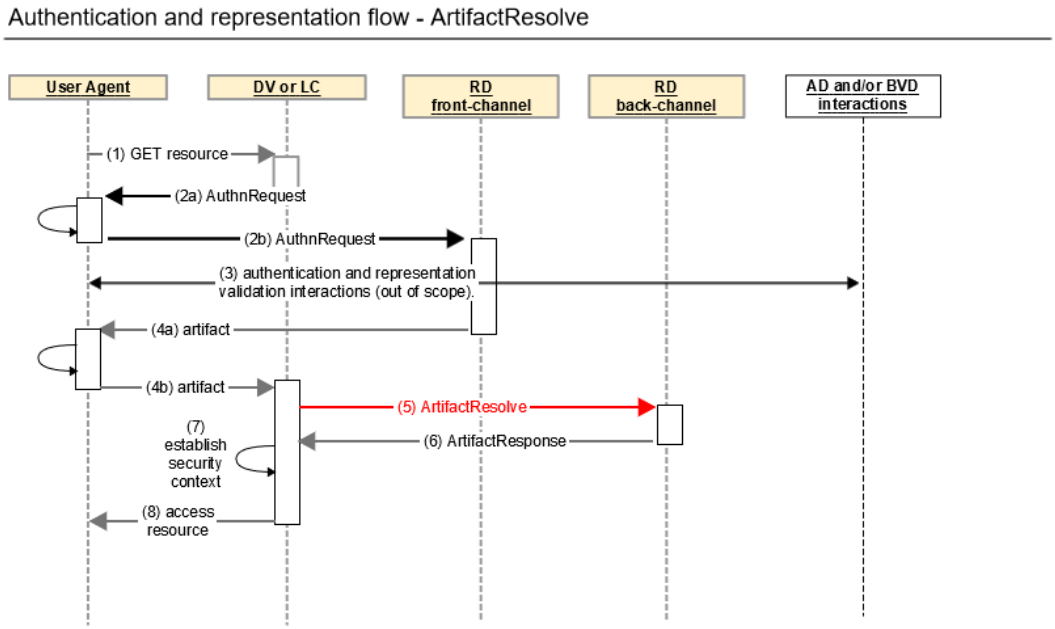
The receiver of the previous <AuthnRequest> message sends a SAML-artifact message via the front channel by a redirect to the AssertionConsumerService referenced in the AuthnRequest. An artifact is a reference to the SAML Response message. Even if no authentication has taken place, an artifact will be sent. The artifact message is sent to the recipient via an HTTP Redirect. The artifact is used by the receiver to retrieve the SAML response at the sender.

7.5 SAML ArtifactResolve

The ArtifactResolve request is sent via a SOAP binding over the back channel. The back channel is protected with two-sided TLS authentication. The receiver will return an ArtifactResponse in the response message.

The sender and recipient of the Authnrequest message are the following:

Sender	DV	LC
Recipient	RD	RD



7.5.1 <ArtifactResolve>

Examples of <ArtifactResolve> messages.

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.

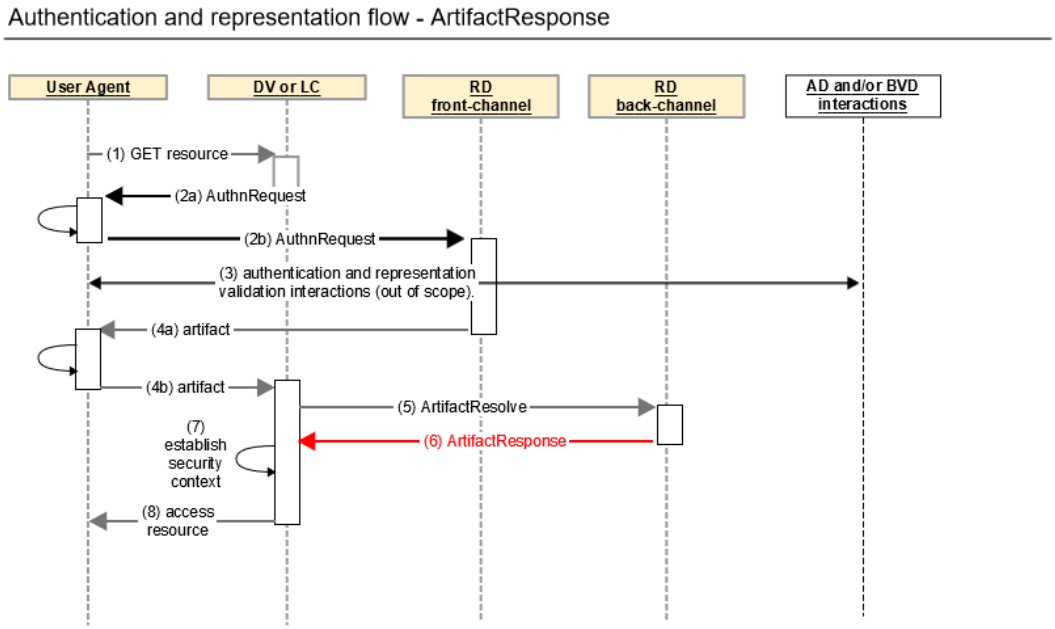
Signature	1	MUST contain the Digital signature of the sender for the enveloped message. MUST contain a <KeyInfo> element with either a <KeyName> or <X509Certificate> elements. See Technical requirements and recommendations for details.
Artifact	1	Contains the Artifact that was received as query parameter.

7.6 SAML ArtifactResponse

The <ArtifactReponse> contains the response message to the <ArtifactResolve> request in a SOAP message. This response message in turn contains the <Response> to the Original AuthnRequest message. The sender will send the <ArtifactResponse> in response to an ArtifactResolve request. If successful it contains the Response to the AuthnRequest.

The sender and recipient of the ArtifactResponse message are the following:

Sender	RD	RD
Recipient	DV	LC



7.6.1 <ArtifactResponse>

Examples: ArtifactResponse examples

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 ArtifactResolve request for which this 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 Response.
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 Technical requirements and recommendations for details.
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 SAML core section 3.2.2.2 and follow the rules described in SAML-bindings section 3.6.6.
--StatusCode	0..1	Conditional. Should only be present if top-level <StatusCode> is not '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 'Success'. MAY contain a message detailling the error that occurred.
Response	0..1	Conditional. If the artifact resolves to a response this MUST contain the <Response> to the AuthnRequest. The <Response> is described below.

<Status>

Special processing rules for <Status> are described in SAML-bindings §3.6.6.

Even if the ArtifactResponse's <Status> indicates "Succes" it may still not contain a <Response> conform SAML-bindings §3.6.6: *"If the issuer of an artifact receives a <samlp:ArtifactResolve> message that it can understand, it MUST return a <samlp:ArtifactResponse> with a <samlp: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)."*

7.6.2 <Response>

The <Response> to the AuthnRequest contains the authentication assertion if authentication was successful.

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.
@InResponseTo	1	Unique @ID attribute of the AuthnRequest request for which this 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 Response.
@Destination	1	URL of the endpoint on which the message is offered. MUST match a recipients metadata AssertionConsumerService.
Issuer	1	MUST contain the EntityID of the sender.
Signature	0..1	SHOULD NOT be used as the <Response> is part of the <ArtifactResponse> messages which is already signed by the RD. If included MUST contain the Digital signature of the 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 'Success' (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 'Success'.
--@Value	1	In the event of a cancellation or error, the element MUST be populated with the value "AuthnFailed".
-StatusMessage	0..1	Only present if top-level StatusCode is not 'Success'. MAY contain a message detailling the error that occurred, MUST contain exact phrase 'Authentication cancelled' when authentication is cancelled (see also Error codes)
Assertion	0..1	Conditional. MUST contain the <Assertion> if the request was processed successfully (Status was "Success"). See the section 'SAML eID Assertion'. Otherwise MUST not be included.
EncryptedAssertion	0	MUST NOT be included.

7.6.3 SAML 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 assertion.
Issuer	1	MUST contain the EntityID of the issuer.
Signature	1	MUST contain the Digital signature of the sender for the enveloped message. MUST contain a <KeyInfo> element with a <KeyName> element. See Technical requirements and recommendations for details.
Subject	1	MUST be included.
-NameID	1	NameID MUST contain a TransientID.
-SubjectConfirmation	1	Contains the <SubjectConfirmation> conform the WebSSO profile. See below.
Conditions	1	NotBefore and NotOnOrAfter limit the window during which the assertion can be delivered.
-@NotBefore	1	MUST be included.
-@NotOnOrAfter	1	MUST be included.
-AudienceRestriction	1	MUST be included.
--Audience	1..n	MUST contain the EntityID(s) for all relevant parties that are intended to receive and process this assertion, as per SAML WebSSO profile. See below under "AudienceRestriction". MUST always contain the DV's EntityID. In cases where an LC is involved it MUST also contain the EntityID of the LC.
AuthnStatement	1	MUST be included.
-@AuthnInstant	1	MUST contain the time of creation of the enclosing Assertion.
-AuthnContext	1	MUST be included.
--AuthnContextClassRef	1	MUST contain the level of assurance at which authentication took place. Contains the obtained effective Level of assurance, see below under "level of assurance validation".
--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 'Success'. MUST NOT be included otherwise. MUST contain a single <AttributeStatement> in accordance with the section

		AttributeStatement below and the rules for processing responses.
Advice	1	MUST be included. Contains the original assertions received from the AD and BVD that were involved in processing the <AuthnRequest>.
-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.

7.6.3.1 Audience Restriction

The <AudienceRestriction> element in the Assertion must be checked in terms of content. An Assertion may only be processed if the <AudienceRestriction> contains the <EntityID> of the recipient.
Note: the values for DVs included in <Audience> are reflected in the @Recipient attribute of the <EncryptedID> element in the Assertion / <AttributeStatement>. This does not apply to the LC that is only included in the <AudienceRestriction>. The LC is not, after all, an entity which may receive identities.

7.6.3.2 Level of assurance validation

The <AuthnContextClassRef> in the <Assertion> element always states the authentication level at which the citizen has authenticated himself. DV's MUST be prepared for the <AuthnContextClassRef> to contain a higher level of assurance than the requested level of assurance. DV's MUST accept authentications with a level equal to or higher than the minimum level registered for the service. 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 then the LoA configured for the Service)

7.6.3.3 SubjectConfirmation

The <SubjectConfirmation> exists in a <Subject>, and is used to hold a 'bearer' confirmation in a response to an AuthnRequest, to conform to the WebSSO profile.

In case a relying party is requesting authentication of a user according to the SAML Web SSO profile, a 'bearer' <SubjectConfirmation> (see SAML 2.0 Profiles, §3.3 and §4.1.4) must be provided.

The @NotOnOrAfter in the **<SubjectConfirmation>** element limits the time during which the Assertion result MAY be used to establish an authenticated session for the End User using the Assertion. The @NotOnOrAfter is initially set to +2 minutes relative to the time of creation of the Assertion. These values can be changed however in time. The @NotBefore and 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 <Authnrequest> this <Assertion> is in response to. A receiving DV or LC MUST verify that this value corresponds to the initiating <Authnrequest> @ID.

Conditions

The @NotBefore and @NotOnOrAfter in the **<Conditions>** element limit the time during which the Assertion is considered valid within a prior established authenticated user session based on this 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>.

7.6.3.4 AttributeStatement

The <Assertion> when present MUST contain an <AttributeStatement>. An <AttributeStatement> contains one or more <Attribute> elements and MUST contain at least one <Attribute> with @Name="urn:nl-eid-gdi:1.0:ActingSubjectID"**.** It MAY contain an <Attribute> element with @Name="urn:nl-eid-gdi:1.0:LegalSubjectID" indicating representation.

These Attributes MUST contain one or more <AttributeValues> one for every recipient (e.g. for the requesting DV and the Machtigingendienst). These recipeints must be inluded in the <AudienceRestriction> element. Note that although the LC may be an <Audience> as it will process the SAML Assertion, is not a <Recipient> and will not be able to decrypt EncrytedID's or attributes.

Each <AttributeValue> contains 1 <EncryptedID> element. The input data for the <EncryptedID> is a <NameID> element with a @NameQualifier attribute indicating the type of identity (e.g. "urn:nl-eid-gdi:1.0:id:legacy-BSN" and the value ("123456789"). The format of the NameID MUST be "urn:oasis:names:tc:SAML:2.0:nameid-format:persistent".

Element/@Attribute	**0..n**	**Description**
AttributeStatement	1	MUST be included.
-Attribute	1..n	See the tables bellow for details.
--@Name	1	MUST contain the type of the attribute.
--AttributeValue	1..n	The Attribute MUST contain one or more <AttributeValues> one for each recipient.
---EncryptedID	1	MUST contain one encrypted <NameID> element. See bellow for details.
----EncryptedData	1	MUST contain the encrypted data containing the XML encrypted NameID which contains the BSN.
----EncryptedKey	1..n	MUST contain the wrapped decryption keys, as defined by [XMLEnc]. This element MUST include the intended Recipient.
-----@Recipient	1	The recipient (DV, of LC or RD) for which this EncryptedID is intended. This attribute MUST contain an EntityID.

NOTE: When copying encrypted XML elements (<EncryptedID>) to create the summary declaration the RD MUST substitute used XML identifiers to

point at the EncryptedTypes for a guaranteed unique identifier. This MAY be accomplished by pre- or suffixing the used identifier in the copy.

(Rationale: *@ID* values must uniquely identify the elements which bear them. Identifiers that appear once in the summary assertion and once in the advice assertion(s) will break schema validation of assertions).

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 SAML 2.0 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 refering 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 EncryptedKeys for other recipients of encrypted elements SHOULD be ignored.

In all cases the following Attributes will be provided as an unencrypted <Attribute>.

Attribute	**1..n**	**Attribute @name SAML eID 4.4**	**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 Authnrequest.

7.6.3.4.1 Attribute types in case of authentication

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

Attribute	**1..n**	**Attribute @name SAML eID 4.4**	**Description**
-ActingSubjectID	1	@name="urn:nl-eid-gdi:1.0:ActingSubjectID".	
--AttributeValue	1..n		All contain the same identity.

7.6.3.4.2 Attribute types issuer in case of representation

In case of representation the following Attributes will be provided as EncryptedID.

Type	**1..n**	**Attribute @name SAML eID 4.4**	**Description**
ActingSubjectID	1	@name="urn:nl-eid-gdi:1.0:ActingSubjectID"	

--AttributeValue	1..n		The (encrypted) ActingSubjectID as received from the AD at which the acting subject was authenticated. All contain the same identity.
LegalSubjectID	1..n	@name="urn:nl-eid-gdi:1.0:LegalSubjectID"	SAML eID 4.4 will only support 1 LegalSubjectID.
--AttributeValue	1..n		The (encrypted) LegalSubjectiD as received from BVD. All contain the same identity.

7.6.3.4.3 Attribute type conversion eTD

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

Type	1..n	eTD @name	Attribute @name SAML eID 4.4	Description
Attribute	0..1	urn:etoegang:core:ActingSubjectID	urn:nl-eid-gdi:1.0:ActingSubjectID	ActingSubjectID
--AttributeValue	1..n			All contain the same identity.
Attribute	0..1	urn:etoegang:core:LegalSubjectID	urn:nl-eid-gdi:1.0:LegalSubjectID	LegalSubjectID
--AttributeValue	1..n			All contain the same identity.

Other scenario's (e.g. support for IntermediarySubjectID) are not yet supported and may be added in future iterations of this specification. Attributes form 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/display/as/Attribuutcatalogus

7.6.3.4.4 EncryptedID

Identifiers (NameID) are contained in SAML <EncryptedID> elements in all cases. The specific type of identifier is communicated through a @NameQualifier attribute within the <NameID>. All identifiers are XML encrypted in such a way that only the intended recipient(s) (e.g. DV) is able to decrypt the identifier. The intended recipient is communicated through the @Recipient attribute within the EncryptedKey element.
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.

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>
```

7.6.3.5 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 assertion(s) or the response
2. Verify that the Recipient attribute in any bearer <SubjectConfirmationData> matches the assertion consumer service URL to which the <Response> or artifact was delivered
3. Verify that the @NotOnOrAfter attribute in any bearer <SubjectConfirmationData> has not passed, subject to allowable clock skew between the providers
4. Verify that the @InResponseTo attribute in the bearer <SubjectConfirmationData> equals the ID of its original <AuthnRequest> message.
5. Verify that it's EntityID is included as <Audience> in the <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.

7.6.3.6 NameQualifier types

The <NameID> @NameQualifier types that are used are listed here: Attribute Identifier types

7.7 Federated login and logout

SSO is defined at the AD level. This means that there is no SSO over AD's unless the AD's mutually agree to provide such a service.

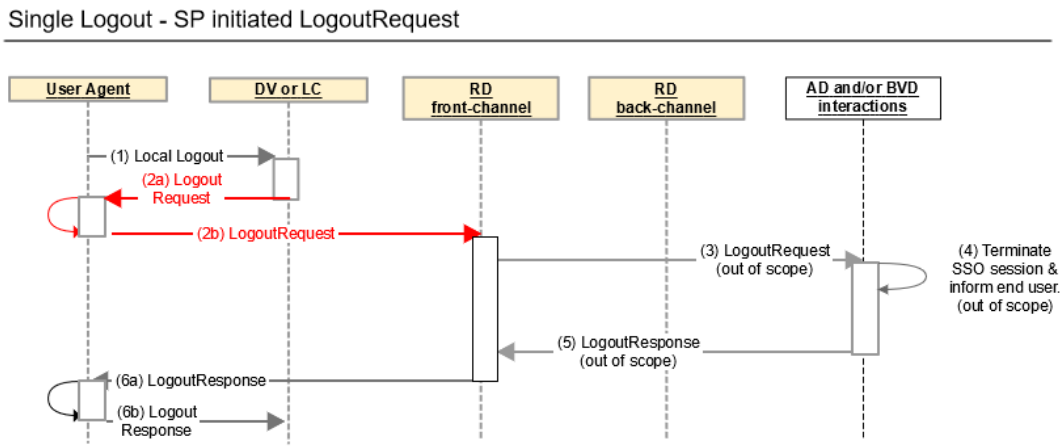
Note that support for federated login and logout may be subject to change in future versions of this specification. DV/LCs which decide to make use of federated login and logout, as supported by this version of the specification, must be prepared to make all the necessary changes to their use of federated login and logout as soon as a later version of the specification mandates such changes. SPs/LCs deciding to do so are at their own risk.

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.

A DV who wants to grant access to his services through SSO can do so via the SSO service from the AD if the AD offers SSO. The DV then participates in an SSO federation which includes several service providers who all want to use the SSO functionality that is offered within the SSO federation. Details on the SSO service are to be provided by the AD.

In a number of cases, the end user is still asked to provide his credentials:

1. The Level of Assurance that the service provider 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 service provider is a member of.
3. The service provider can include the <ForceAuthn> element in the authentication request, with the value True. If a value is not provided or the element is omited, the default is "False"
4. The existing SSO session has expired.



Only a limited form of SP initiated logout is supported by the RD within the context of an SSO federation. On receiving a logout request (1) a DV which participates in a SSO federation MUST send a Logout request to the RD (2b).

This will result in the AD that was involved in the SSO federation to terminate the SSO session if it still was active. As a result the user 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 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 user logs out of the DV.

7.7.1 SP initiated <LogoutRequest>

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

Sender	DV	LC	RD
Recipient	RD	RD	AD

Example of an SP initiated LogoutRequest message.

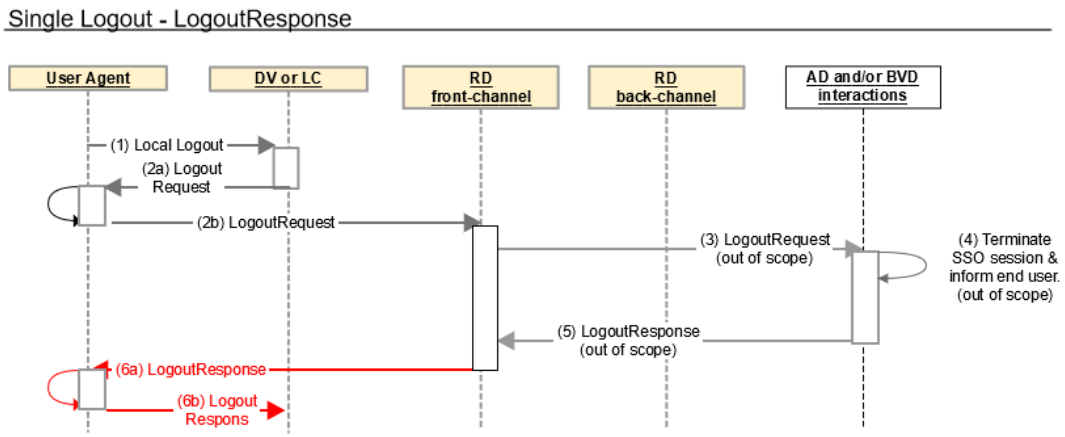
Element/@Attribute	0..n	Description
@ID	1	Unique message attribute

@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 DV or LC 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 Technical requirements and recommendations for details. In case the sender is a RD it MUST contain a <KeyInfo> element with a <KeyName> element.
NameID	1	MUST contain the TransientID <NameID> element from the <Subject> of the original Assertion.
Issuer	1	MUST contain the EntityID of the sender.

7.7.2 IdP <LogoutResponse>

In response to a LogoutRequest a RD will send this message to the DV or LC .

Sender	RD	RD	AD
Recipient	DV	LC	RD



Example of a LogoutResponse 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 LogoutRequest for which this Response message is the answer.
Signature	1	MUST contain the Digital signature of the DV or LC for the enveloped message (Algoritm="http://www.w3.org/2000/09/xmldsig#enveloped-signature"). MUST contain a <KeyInfo> element with a <KeyName> or <X509Certificate> elements. See Technical requirements and recommendations veID-SAML-4.4-definitief for details. In case the sender is a RD it MUST contain a <KeyInfo> element with a <KeyName> element.
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.

7.8 Error codes

7.8.1 Toplevel code

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

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

7.8.2 Second-level status codes

The following second-level status codes MAY be used:

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 dienstencatalogus (DC).
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 none of the identity providers in an <IDPList> are supported by the intermediary.

7.8.3 Cancelling

During the process of authenticating and authorizing, a user may cancel the process by clicking on the cancel button.

If a user cancels, the participant MUST direct the user automatically to the latest sender of a SAML request, accompanying a valid SAML 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:AuthnFailed). A <StatusMessage> element MUST be included, containing the exact phrase "Authentication cancelled".

If a RD receives a cancellation message (from an AD or BVD), it MUST ask the user to re-select an AD or BVD or cancel, but only if selection had taken place at the RD. Otherwise, the cancellation message must be forwarded to the DV or LC.

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

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

7.8.5 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 user to initiator of the SAML request, accompanying a valid SAML 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 <StatusMessage> element MUST be included, containing a description of the problem (for example "Level of assurance not supported").

A participant receiving such a response

- MUST show the user a message indicating authentication has failed, including the contents of <StatusMessage>. If the participant is a RD, and no interaction had taken place with the user, the message must be forwarded to the DV or LC.
- If the participant is a RD, it MUST ask the user to re-select an AD or BVD or cancel, but only if selection had taken place at the RD.

7.8.6 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 NotValidOnOrAfter
- Invalid signature
- The request contains invalid ServiceID, attributes or EntityConcernedTypes
- The response contains ServiceID, attributes, EntityConcernedTypes or a Level of assurance that does not match the request

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

A participant that receives a message in this category

- MUST investigate the nature of the error.
- MUST show the user a message indicating a non-recoverable error has occured, advising the user how to resolve the problem if possible, in case a binding is used where the user is involved;
- MUST return a SAML 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 synchronuous response is expected and can be returned, like SOAP.
- If the participant is a RD and the message is not an AuthnRequest, it MUST ask the user to re-select an AD or BVD or cancel.

7.9 Example SAML messages

7.9.1 AuthnRequest examples

```
<samlp:AuthnRequest xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol"
                    xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion"
                    ID="_fd540805f496007802fd66424e4cfcc50bf72dfdb0"
                    Version="2.0"
                    IssueInstant="2020-08-17T12:17:17Z"

Destination="https://pp2.toegang.overheid.nl/kvs/rd/request_authentication"
                    ForceAuthn="true"
                    AttributeConsumingServiceIndex="0"
                    AssertionConsumerServiceIndex="0"
                    >
    <saml:Issuer>urn:nl-eid-
gdi:1.0:DV:00000004000000010000:entities:9002</saml:Issuer>
    <ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
        <ds:SignedInfo>
            <ds:CanonicalizationMethod
Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#" />
            <ds:SignatureMethod
Algorithm="http://www.w3.org/2001/04/xmldsig-more#rsa-sha256" />
            <ds:Reference
URI="#_fd540805f496007802fd66424e4cfcc50bf72dfdb0">
                <ds:Transforms>
                    <ds:Transform
Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature" />
                    <ds:Transform Algorithm="http://www.w3.org/2001/10/xml-
exc-c14n#" />
                </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:X509Data>
                <ds:X509Certificate>...</ds:X509Certificate>
            </ds:X509Data>
        </ds:KeyInfo>
    </ds:Signature>
</samlp:AuthnRequest>
```

Code Block 1 DV-RD AuthnRequest using AttributeConsumingServiceIndex

```
<samlp:AuthnRequest xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol"
                    xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion"
                    ID="_fd540805f496007802fd66424e4cfcc50bf72dfdb0"
                    Version="2.0"
                    IssueInstant="2020-08-17T12:17:17Z"

Destination="https://pp2.toegang.overheid.nl/kvs/rd/request_authentication"
                    ForceAuthn="true"
                    AssertionConsumerServiceIndex="0"
                    >
    <saml:Issuer>urn:nl-eid-
gdi:1.0:DV:00000004000000010000:entities:9002</saml:Issuer>
    <ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
        <ds:SignedInfo>
            <ds:CanonicalizationMethod
Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#" />
            <ds:SignatureMethod
Algorithm="http://www.w3.org/2001/04/xmldsig-more#rsa-sha256" />
            <ds:Reference
URI="#_fd540805f496007802fd66424e4cfcc50bf72dfdb0">
                <ds:Transforms>
                    <ds:Transform
Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature" />
                    <ds:Transform Algorithm="http://www.w3.org/2001/10/xml-
exc-c14n#" />
                </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:X509Data>
                <ds:X509Certificate>...</ds:X509Certificate>
            </ds:X509Data>
        </ds:KeyInfo>
    </ds:Signature>
    <samlp:Extensions>
        <saml:Attribute Name="urn:nl-eid-gdi:1.0:IntendedAudience">
            <saml:AttributeValue>urn:nl-eid-
gdi:1.0:DV:00000004000000010000:entities:9002</saml:AttributeValue>
        </saml:Attribute>
        <saml:Attribute Name="urn:nl-eid-gdi:1.0:ServiceUUID">
            <saml:AttributeValue>f847dc11-ac24-47b2-84a8-
a057440ce56d</saml:AttributeValue>
        </saml:Attribute>
    </samlp:Extensions>
</samlp:AuthnRequest>
```

Code Block 2 DV-RD AuthnRequest using extensions

```
<samlp:AuthnRequest xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol"
                    xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion"
                    ID="_fd540805f496007802fd66424e4cfcc50bf72dfdb0"
                    Version="2.0"
                    IssueInstant="2020-08-17T12:17:17Z"

Destination="https://pp2.toegang.overheid.nl/kvs/rd/request_authentication"
                    ForceAuthn="true"
                    AssertionConsumerServiceIndex="0"
                    >
    <saml:Issuer>urn:nl-eid-
gdi:1.0:LC:00000008000000020000:entities:9011</saml:Issuer>
    <ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
        <ds:SignedInfo>
            <ds:CanonicalizationMethod
Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#" />
            <ds:SignatureMethod
Algorithm="http://www.w3.org/2001/04/xmldsig-more#rsa-sha256" />
            <ds:Reference
URI="#_fd540805f496007802fd66424e4cfcc50bf72dfdb0">
                <ds:Transforms>
                    <ds:Transform
Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature" />
                    <ds:Transform Algorithm="http://www.w3.org/2001/10/xml-
exc-c14n#" />
                </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:X509Data>
                <ds:X509Certificate>...</ds:X509Certificate>
            </ds:X509Data>
        </ds:KeyInfo>
    </ds:Signature>
    <samlp:Extensions>
        <saml:Attribute Name="urn:nl-eid-gdi:1.0:IntendedAudience">
            <saml:AttributeValue>urn:nl-eid-
gdi:1.0:DV:00000004000000010000:entities:9002</saml:AttributeValue>
        </saml:Attribute>
        <saml:Attribute Name="urn:nl-eid-gdi:1.0:ServiceUUID">
            <saml:AttributeValue>f847dc11-ac24-47b2-84a8-
a057440ce56d</saml:AttributeValue>
        </saml:Attribute>
    </samlp:Extensions>
</samlp:AuthnRequest>
```

Code Block 3 LC-RD AuthnRequest using extensions

7.9.2 ArtifactResolve examples

```
<samlp:ArtifactResolve xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol"
xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion"
ID="_86c57b606f259c18c7daba99de5b4db22276df5af1" Version="2.0"
IssueInstant="2020-08-17T12:17:31Z" Destination="https://artifact-
pp2.toegang.overheid.nl/kvs/rd/resolve_artifact">
    <saml:Issuer>urn:nl-eid-
gdi:1.0:DV:00000004000000010000:entities:9002</saml:Issuer>
    <ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
        <ds:SignedInfo>
            <ds:CanonicalizationMethod
Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>
            <ds:SignatureMethod
Algorithm="http://www.w3.org/2001/04/xmldsig-more#rsa-sha256"/>
            <ds:Reference
URI="#_86c57b606f259c18c7daba99de5b4db22276df5af1">
                <ds:Transforms>
                    <ds:Transform
Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature"/>
                    <ds:Transform Algorithm="http://www.w3.org/2001/10/xml-
exc-c14n#"/>
                </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:X509Data>
                <ds:X509Certificate>...</ds:X509Certificate>
            </ds:X509Data>
        </ds:KeyInfo>
    </ds:Signature>

<samlp:Artifact>AAQAAC++9v4UQ3mOG7AEGSVSddlO0YmaRCGk1jkVRoStga0sICMv4wAAAA
A=</samlp:Artifact>
</samlp:ArtifactResolve>
```

Code Block 4 DV-RD ArtifactResolve

```
<samlp:ArtifactResolve xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol"
xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion"
ID="_86c57b606f259c18c7daba99de5b4db22276df5af1" Version="2.0"
IssueInstant="2020-08-17T12:17:31Z" Destination="https://artifact-
pp2.toegang.overheid.nl/kvs/rd/resolve_artifact">
    <saml:Issuer>urn:nl-eid-
gdi:1.0:LC:00000008000000020000:entities:9011</saml:Issuer>
    <ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
        <ds:SignedInfo>
            <ds:CanonicalizationMethod
Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>
            <ds:SignatureMethod
Algorithm="http://www.w3.org/2001/04/xmldsig-more#rsa-sha256"/>
            <ds:Reference
URI="#_86c57b606f259c18c7daba99de5b4db22276df5af1">
                <ds:Transforms>
                    <ds:Transform
Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature"/>
                    <ds:Transform Algorithm="http://www.w3.org/2001/10/xml-
exc-c14n#"/>
                </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:X509Data>
                <ds:X509Certificate>...</ds:X509Certificate>
            </ds:X509Data>
        </ds:KeyInfo>
    </ds:Signature>

<samlp:Artifact>AAQAAC++9v4UQ3mOG7AEGSVSddlO0YmaRCGk1jkVRoStga0sICMv4wAAAA
A=</samlp:Artifact>
</samlp:ArtifactResolve>
```

Code Block 5 LC-RD Artifactresolve message

7.9.3 ArtifactResponse examples

```
<samlp:ArtifactResponse xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion"
xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol"
ID="_967ea45f7bbe430692354fad90dcbaef"
InResponseTo="_86c57b606f259c18c7daba99de5b4db22276df5af1" IssueInstant="2020-08-
17T12:17:31Z" Version="2.0">
    <saml:Issuer>urn:nl-eid-
gdi:1.0:RD:00000004000000149000:entities:9002</saml:Issuer>
    <dsig:Signature xmlns:dsig="http://www.w3.org/2000/09/xmldsig#" Id="Id-
0001597666651857-ffffffffb8b83bbe-1">
        <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="#_967ea45f7bbe430692354fad90dcbaef">
                <dsig:Transforms>
                    <dsig:Transform
Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature"/>
                    <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="Id-
0001597666651857-ffffffffb8b83bbe-2">

<dsig:KeyName>07c3d08bc6c3303a85c5e0c9547dfd91047f7c58</dsig:KeyName>
        </dsig:KeyInfo>
    </dsig:Signature>
    <samlp:Status>
        <samlp:StatusCode
Value="urn:oasis:names:tc:SAML:2.0:status:Success"/>
    </samlp:Status>
    <samlp:Response ID="_6c8a68f42b1b4087af3b678e9b5d85ce"
InResponseTo="_fd540805f496007802fd66424e4cfcc50bf72dfdb0" IssueInstant="2020-08-
17T12:17:31Z" Destination="https://login.dv.test/saml/sp/acs" Version="2.0">
        <saml:Issuer>urn:nl-eid-
gdi:1.0:RD:00000004000000149000:entities:9002</saml:Issuer>
        <samlp:Status>
            <samlp:StatusCode
Value="urn:oasis:names:tc:SAML:2.0:status:Success"/>
        </samlp:Status>
        <saml:Assertion ID="_3406c06524ad497aa57a5859ab48f876"
IssueInstant="2020-08-17T12:17:31Z" Version="2.0">
            <saml:Issuer>urn:nl-eid-
gdi:1.0:RD:00000004000000149000:entities:9002</saml:Issuer>
            <dsig:Signature xmlns:dsig="http://www.w3.org/2000/09/xmldsig#"
Id="Id-0001597666651854-0000000016a2ce56-1">
                <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="#_3406c06524ad497aa57a5859ab48f876">
                        <dsig:Transforms>
                            <dsig:Transform
Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature"/>
```

```
                            <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="Id-0001597666651854-0000000016a2ce56-2">

<dsig:KeyName>07c3d08bc6c3303a85c5e0c9547dfd91047f7c58</dsig:KeyName>
                </dsig:KeyInfo>
            </dsig:Signature>
            <saml:Subject>

<saml:NameID>ef904537461642eeb923ffda73110cb1</saml:NameID>
                <saml:SubjectConfirmation
Method="urn:oasis:names:tc:SAML:2.0:cm:bearer">
                    <saml:SubjectConfirmationData
InResponseTo="_fd540805f496007802fd66424e4cfcc50bf72dfdb0" NotOnOrAfter="2020-
08-17T12:19:31Z" Recipient="https://login.dv.test/saml/sp/acs"/>
                </saml:SubjectConfirmation>
            </saml:Subject>
            <saml:Conditions NotBefore="2020-08-17T12:15:31Z"
NotOnOrAfter="2020-08-17T12:19:31Z">
                <saml:AudienceRestriction>
                    <saml:Audience>urn:nl-eid-
gdi:1.0:DV:00000004000000010000:entities:9002</saml:Audience>
                </saml:AudienceRestriction>
            </saml:Conditions>
            <saml:Advice>
                <saml2:Assertion
xmlns:saml2="urn:oasis:names:tc:SAML:2.0:assertion"
ID="_6fabd6f522c7b8d45c12deab9a034a0e" IssueInstant="2020-08-17T12:17:31.180Z"
Version="2.0">
                    <!-- DigiD Assertion -->
                </saml2:Assertion>
            </saml:Advice>
            <saml:AuthnStatement AuthnInstant="2020-08-17T12:17:31Z">
                <saml:AuthnContext>

<saml:AuthnContextClassRef>http://eID.logius.nl/LoA/basic</saml:AuthnConte
xtClassRef>
                    <saml:AuthenticatingAuthority>urn:nl-eid-
gdi:1.0:AD:00000004166909913000:entities:9000</saml:AuthenticatingAuthorit
y>
                </saml:AuthnContext>
            </saml:AuthnStatement>
            <saml:AttributeStatement
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xmlns:xs="http://www.w3.org/2001/XMLSchema">
                <saml:Attribute Name="urn:nl-eid-gdi:1.0:ActingSubjectID">
                    <saml:AttributeValue>
                        <saml2:EncryptedID
xmlns:saml2="urn:oasis:names:tc:SAML:2.0:assertion">
                            <xenc:EncryptedData
xmlns:xenc="http://www.w3.org/2001/04/xmlenc#"
Id="_3be99fdeb24071bd673ad3b034f5a932-1"
Type="http://www.w3.org/2001/04/xmlenc#Element">
                                <xenc:EncryptionMethod
Algorithm="http://www.w3.org/2001/04/xmlenc#aes256-cbc"/>
```

```
                                    <ds:KeyInfo
xmlns:ds="http://www.w3.org/2000/09/xmldsig#">

<ds:KeyName>_3aeb112dde722c18565edba24e0c6ae5-1</ds:KeyName>
                                    </ds:KeyInfo>
                                    <xenc:CipherData>

<xenc:CipherValue>...</xenc:CipherValue>
                                    </xenc:CipherData>
                                </xenc:EncryptedData>
                                <xenc:EncryptedKey
xmlns:xenc="http://www.w3.org/2001/04/xmlenc#"
Id="_5b83145d20a13f9986425223ea841363-1" Recipient="urn:nl-eid-
gdi:1.0:DV:00000004000000010000:entities:9002">
                                    <xenc:EncryptionMethod
Algorithm="http://www.w3.org/2001/04/xmlenc#rsa-oaep-mgf1p"/>
                                    <ds:KeyInfo
xmlns:ds="http://www.w3.org/2000/09/xmldsig#" Id="Id-0001561625437040-
000000005818a91d-2">

<ds:KeyName>cdb948c5dfde5c9a53bf4916763dc973d55e8dd0</ds:KeyName>
                                    </ds:KeyInfo>
                                    <xenc:CipherData>

<xenc:CipherValue>...</xenc:CipherValue>
                                    </xenc:CipherData>
                                    <xenc:ReferenceList>
                                        <xenc:DataReference
URI="#_3be99fdeb24071bd673ad3b034f5a932-1"/>
                                    </xenc:ReferenceList>

<xenc:CarriedKeyName>_3aeb112dde722c18565edba24e0c6ae5-
1</xenc:CarriedKeyName>
                                </xenc:EncryptedKey>
                            </saml2:EncryptedID>
                        </saml:AttributeValue>
                    </saml:Attribute>
                    <saml:Attribute Name="urn:nl-eid-gdi:1.0:ServiceUUID"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri">
                        <saml:AttributeValue xsi:type="xs:string">f847dc11-ac24-
47b2-84a8-a057440ce56d</saml:AttributeValue>
                    </saml:Attribute>
                </saml:AttributeStatement>
            </saml:Assertion>
        </samlp:Response>
    </samlp:ArtifactResponse>
```

Code Block 6 RD-DV ArtifactResponse

```
<samlp:ArtifactResponse xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion"
xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol"
ID="_967ea45f7bbe430692354fad90dcbaef"
InResponseTo="_86c57b606f259c18c7daba99de5b4db22276df5af1" IssueInstant="2020-08-
17T12:17:31Z" Version="2.0">
    <saml:Issuer>urn:nl-eid-
gdi:1.0:RD:00000004000000149000:entities:9002</saml:Issuer>
    <dsig:Signature xmlns:dsig="http://www.w3.org/2000/09/xmldsig#" Id="Id-
0001597666651857-ffffffffb8b83bbe-1">
        <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="#_967ea45f7bbe430692354fad90dcbaef">
                <dsig:Transforms>
                    <dsig:Transform
Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature"/>
                    <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="Id-
0001597666651857-ffffffffb8b83bbe-2">

<dsig:KeyName>07c3d08bc6c3303a85c5e0c9547dfd91047f7c58</dsig:KeyName>
        </dsig:KeyInfo>
    </dsig:Signature>
    <samlp:Status>
        <samlp:StatusCode
Value="urn:oasis:names:tc:SAML:2.0:status:Success"/>
    </samlp:Status>
    <samlp:Response ID="_6c8a68f42b1b4087af3b678e9b5d85ce"
InResponseTo="_fd540805f496007802fd66424e4cfcc50bf72dfdb0" IssueInstant="2020-08-
17T12:17:31Z" Destination="https://login.lc.test/saml/sp/acs" Version="2.0">
        <saml:Issuer>urn:nl-eid-
gdi:1.0:RD:00000004000000149000:entities:9002</saml:Issuer>
        <samlp:Status>
            <samlp:StatusCode
Value="urn:oasis:names:tc:SAML:2.0:status:Success"/>
        </samlp:Status>
        <saml:Assertion ID="_3406c06524ad497aa57a5859ab48f876"
IssueInstant="2020-08-17T12:17:31Z" Version="2.0">
            <saml:Issuer>urn:nl-eid-
gdi:1.0:RD:00000004000000149000:entities:9002</saml:Issuer>
            <dsig:Signature xmlns:dsig="http://www.w3.org/2000/09/xmldsig#"
Id="Id-0001597666651854-0000000016a2ce56-1">
                <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="#_3406c06524ad497aa57a5859ab48f876">
                        <dsig:Transforms>
                            <dsig:Transform
Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature"/>
```

```
                            <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="Id-0001597666651854-0000000016a2ce56-2">

<dsig:KeyName>07c3d08bc6c3303a85c5e0c9547dfd91047f7c58</dsig:KeyName>
                </dsig:KeyInfo>
            </dsig:Signature>
            <saml:Subject>

<saml:NameID>ef904537461642eeb923ffda73110cb1</saml:NameID>
                <saml:SubjectConfirmation
Method="urn:oasis:names:tc:SAML:2.0:cm:bearer">
                    <saml:SubjectConfirmationData
InResponseTo="_fd540805f496007802fd66424e4cfcc50bf72dfdb0" NotOnOrAfter="2020-
08-17T12:19:31Z" Recipient="https://login.lc.test/saml/sp/acs"/>
                </saml:SubjectConfirmation>
            </saml:Subject>
            <saml:Conditions NotBefore="2020-08-17T12:15:31Z"
NotOnOrAfter="2020-08-17T12:19:31Z">
                <saml:AudienceRestriction>
                    <saml:Audience>urn:nl-eid-
gdi:1.0:LC:00000008000000020000:entities:9011</saml:Audience>
                    <saml:Audience>urn:nl-eid-
gdi:1.0:DV:00000004000000010000:entities:9002</saml:Audience>
                </saml:AudienceRestriction>
            </saml:Conditions>
            <saml:Advice>
                <saml2:Assertion
xmlns:saml2="urn:oasis:names:tc:SAML:2.0:assertion"
ID="_6fabd6f522c7b8d45c12deab9a034a0e" IssueInstant="2020-08-17T12:17:31.180Z"
Version="2.0">
                    <!-- DigiD Assertion -->
                </saml2:Assertion>
            </saml:Advice>
            <saml:AuthnStatement AuthnInstant="2020-08-17T12:17:31Z">
                <saml:AuthnContext>

<saml:AuthnContextClassRef>http://eID.logius.nl/LoA/basic</saml:AuthnConte
xtClassRef>
                    <saml:AuthenticatingAuthority>urn:nl-eid-
gdi:1.0:AD:00000004166909913000:entities:9000</saml:AuthenticatingAuthorit
y>
                </saml:AuthnContext>
            </saml:AuthnStatement>
            <saml:AttributeStatement
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xmlns:xs="http://www.w3.org/2001/XMLSchema">
                <saml:Attribute Name="urn:nl-eid-gdi:1.0:ActingSubjectID">
                    <saml:AttributeValue>
                        <saml2:EncryptedID
xmlns:saml2="urn:oasis:names:tc:SAML:2.0:assertion">
                            <xenc:EncryptedData
xmlns:xenc="http://www.w3.org/2001/04/xmlenc#"
Id="_3be99fdeb24071bd673ad3b034f5a932-1"
Type="http://www.w3.org/2001/04/xmlenc#Element">
```

```
                                    <xenc:EncryptionMethod
Algorithm="http://www.w3.org/2001/04/xmlenc#aes256-cbc"/>
                                    <ds:KeyInfo
xmlns:ds="http://www.w3.org/2000/09/xmldsig#">

<ds:KeyName>_3aeb112dde722c18565edba24e0c6ae5-1</ds:KeyName>
                                    </ds:KeyInfo>
                                    <xenc:CipherData>

<xenc:CipherValue>...</xenc:CipherValue>
                                    </xenc:CipherData>
                                </xenc:EncryptedData>
                                <xenc:EncryptedKey
xmlns:xenc="http://www.w3.org/2001/04/xmlenc#"
Id="_5b83145d20a13f9986425223ea841363-1" Recipient="urn:nl-eid-
gdi:1.0:DV:00000004000000010000:entities:9002">
                                    <xenc:EncryptionMethod
Algorithm="http://www.w3.org/2001/04/xmlenc#rsa-oaep-mgf1p"/>
                                    <ds:KeyInfo
xmlns:ds="http://www.w3.org/2000/09/xmldsig#" Id="Id-0001561625437040-
000000005818a91d-2">

<ds:KeyName>cdb948c5dfde5c9a53bf4916763dc973d55e8dd0</ds:KeyName>
                                    </ds:KeyInfo>
                                    <xenc:CipherData>

<xenc:CipherValue>...</xenc:CipherValue>
                                    </xenc:CipherData>
                                    <xenc:ReferenceList>
                                        <xenc:DataReference
URI="#_3be99fdeb24071bd673ad3b034f5a932-1"/>
                                    </xenc:ReferenceList>

<xenc:CarriedKeyName>_3aeb112dde722c18565edba24e0c6ae5-
1</xenc:CarriedKeyName>
                                </xenc:EncryptedKey>
                            </saml2:EncryptedID>
                        </saml:AttributeValue>
                    </saml:Attribute>
                    <saml:Attribute Name="urn:nl-eid-gdi:1.0:ServiceUUID"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri">
                        <saml:AttributeValue xsi:type="xs:string">f847dc11-ac24-
47b2-84a8-a057440ce56d</saml:AttributeValue>
                    </saml:Attribute>
                </saml:AttributeStatement>
            </saml:Assertion>
        </samlp:Response>
    </samlp:ArtifactResponse>
```

Code Block 7 RD-LC ArtifactResponse

```
<samlp:ArtifactResponse xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion"
xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol"
ID="_967ea45f7bbe430692354fad90dcbaef"
InResponseTo="_86c57b606f259c18c7daba99de5b4db22276df5af1" IssueInstant="2020-08-
17T12:17:31Z" Version="2.0">
    <saml:Issuer>urn:nl-eid-
gdi:1.0:RD:00000004000000149000:entities:9002</saml:Issuer>
    <dsig:Signature xmlns:dsig="http://www.w3.org/2000/09/xmldsig#" Id="Id-
0001597666651857-ffffffffb8b83bbe-1">
        <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="#_967ea45f7bbe430692354fad90dcbaef">
                <dsig:Transforms>
                    <dsig:Transform
Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature"/>
                    <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="Id-
0001597666651857-ffffffffb8b83bbe-2">

<dsig:KeyName>07c3d08bc6c3303a85c5e0c9547dfd91047f7c58</dsig:KeyName>
        </dsig:KeyInfo>
    </dsig:Signature>
    <samlp:Status>
        <samlp:StatusCode
Value="urn:oasis:names:tc:SAML:2.0:status:Success"/>
    </samlp:Status>
    <samlp:Response ID="_6c8a68f42b1b4087af3b678e9b5d85ce"
InResponseTo="_fd540805f496007802fd66424e4cfcc50bf72dfdb0" IssueInstant="2020-08-
17T12:17:31Z" Destination="https://login.dv.test/saml/sp/acs" Version="2.0">
        <saml:Issuer>urn:nl-eid-
gdi:1.0:RD:00000004000000149000:entities:9002</saml:Issuer>
        <samlp:Status>
            <samlp:StatusCode
Value="urn:oasis:names:tc:SAML:2.0:status:Responder">
                <samlp:StatusCode
Value="urn:oasis:names:tc:SAML:2.0:status:AuthnFailed"/>
            </samlp:StatusCode>
            <samlp:StatusMessage>Authentication
cancelled</samlp:StatusMessage>
        </samlp:Status>
    </samlp:Response>
</samlp:ArtifactResponse>
```

Code Block 8 RD-DV ArtifactResponse cancel

```
<samlp:ArtifactResponse xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion"
xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol"
ID="_967ea45f7bbe430692354fad90dcbaef"
InResponseTo="_86c57b606f259c18c7daba99de5b4db22276df5af1" IssueInstant="2020-08-
17T12:17:31Z" Version="2.0">
    <saml:Issuer>urn:nl-eid-
gdi:1.0:RD:00000004000000149000:entities:9002</saml:Issuer>
    <dsig:Signature xmlns:dsig="http://www.w3.org/2000/09/xmldsig#" Id="Id-
0001597666651857-ffffffffb8b83bbe-1">
        <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="#_967ea45f7bbe430692354fad90dcbaef">
                <dsig:Transforms>
                    <dsig:Transform
Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature"/>
                    <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="Id-
0001597666651857-ffffffffb8b83bbe-2">

<dsig:KeyName>07c3d08bc6c3303a85c5e0c9547dfd91047f7c58</dsig:KeyName>
        </dsig:KeyInfo>
    </dsig:Signature>
    <samlp:Status>
        <samlp:StatusCode
Value="urn:oasis:names:tc:SAML:2.0:status:Success"/>
    </samlp:Status>
    <samlp:Response ID="_6c8a68f42b1b4087af3b678e9b5d85ce"
InResponseTo="_fd540805f496007802fd66424e4cfcc50bf72dfdb0" IssueInstant="2020-08-
17T12:17:31Z" Destination="https://login.lc.test/saml/sp/acs" Version="2.0">
        <saml:Issuer>urn:nl-eid-
gdi:1.0:RD:00000004000000149000:entities:9002</saml:Issuer>
        <samlp:Status>
            <samlp:StatusCode
Value="urn:oasis:names:tc:SAML:2.0:status:Responder">
                <samlp:StatusCode
Value="urn:oasis:names:tc:SAML:2.0:status:AuthnFailed"/>
            </samlp:StatusCode>
            <samlp:StatusMessage>Authentication
cancelled</samlp:StatusMessage>
        </samlp:Status>
    </samlp:Response>
</samlp:ArtifactResponse>
```

Code Block 9 RD-LC ArtifactResponse cancel

7.9.4 LogoutRequest examples

```
<samlp:LogoutRequest xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol"
                     xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion"
                     ID="_1fb026f12803a5e193ca2458c949f2e1e3cfde6e2d"
                     Version="2.0"
                     IssueInstant="2020-08-17T14:09:35Z"

Destination="https://pp2.toegang.overheid.nl/kvs/rd/request_logout"
                     >
    <saml:Issuer>urn:nl-eid-
gdi:1.0:DV:00000004000000010000:entities:9002</saml:Issuer>
    <ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
        <ds:SignedInfo>
            <ds:CanonicalizationMethod
Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#" />
            <ds:SignatureMethod
Algorithm="http://www.w3.org/2001/04/xmldsig-more#rsa-sha256" />
            <ds:Reference
URI="#_1fb026f12803a5e193ca2458c949f2e1e3cfde6e2d">
                <ds:Transforms>
                    <ds:Transform
Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature" />
                    <ds:Transform Algorithm="http://www.w3.org/2001/10/xml-
exc-c14n#" />
                </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:X509Data>
                <ds:X509Certificate>...</ds:X509Certificate>
            </ds:X509Data>
        </ds:KeyInfo>
    </ds:Signature>
    <saml:NameID>ef904537461642eeb923ffda73110cb1</saml:NameID>
</samlp:LogoutRequest>
```

Code Block 10 DV-RD LogoutRequest

```
<samlp:LogoutRequest xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol"
                     xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion"
                     ID="_1fb026f12803a5e193ca2458c949f2e1e3cfde6e2d"
                     Version="2.0"
                     IssueInstant="2020-08-17T14:09:35Z"

Destination="https://pp2.toegang.overheid.nl/kvs/rd/request_logout"
                     >
    <saml:Issuer>urn:nl-eid-
gdi:1.0:LC:00000008000000020000:entities:9011</saml:Issuer>
    <ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
        <ds:SignedInfo>
            <ds:CanonicalizationMethod
Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#" />
            <ds:SignatureMethod
Algorithm="http://www.w3.org/2001/04/xmldsig-more#rsa-sha256" />
            <ds:Reference
URI="#_1fb026f12803a5e193ca2458c949f2e1e3cfde6e2d">
                <ds:Transforms>
                    <ds:Transform
Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature" />
                    <ds:Transform Algorithm="http://www.w3.org/2001/10/xml-
exc-c14n#" />
                </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:X509Data>
                <ds:X509Certificate>...</ds:X509Certificate>
            </ds:X509Data>
        </ds:KeyInfo>
    </ds:Signature>
    <saml:NameID>ef904537461642eeb923ffda73110cb1</saml:NameID>
</samlp:LogoutRequest>
```

Code Block 11 LC-RD LogoutRequest

7.9.5 LogoutResponse examples

```
<samlp:LogoutResponse xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion"
                      xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol"
                      Destination="https://login.dv.test/saml/sp/logout"
                      ID="_a69e4de1d6344deaae521ac96290edb5"

InResponseTo="_1fb026f12803a5e193ca2458c949f2e1e3cfde6e2d"
                      IssueInstant="2020-08-17T14:09:36Z"
                      Version="2.0"
                      >
    <saml:Issuer>urn:nl-eid-
gdi:1.0:RD:00000004000000149000:entities:9002</saml:Issuer>
    <dsig:Signature xmlns:dsig="http://www.w3.org/2000/09/xmldsig#" Id="Id-
0001597673376485-ffffffffe506c0aa-1">
        <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="#_a69e4de1d6344deaae521ac96290edb5">
                <dsig:Transforms>
                    <dsig:Transform
Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature" />
                    <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="Id-
0001597673376485-ffffffffe506c0aa-2">

<dsig:KeyName>07c3d08bc6c3303a85c5e0c9547dfd91047f7c58</dsig:KeyName>
        </dsig:KeyInfo>
    </dsig:Signature>
    <samlp:Status>
        <samlp:StatusCode
Value="urn:oasis:names:tc:SAML:2.0:status:Success" />
    </samlp:Status>
</samlp:LogoutResponse>
```

Code Block 12 RD-DV LogoutResponse

```
<samlp:LogoutResponse xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion"
                      xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol"
                      Destination="https://login.lc.test/saml/sp/logout"
                      ID="_a69e4de1d6344deaae521ac96290edb5"

InResponseTo="_1fb026f12803a5e193ca2458c949f2e1e3cfde6e2d"
                      IssueInstant="2020-08-17T14:09:36Z"
                      Version="2.0"
                      >
    <saml:Issuer>urn:nl-eid-
gdi:1.0:RD:00000004000000149000:entities:9002</saml:Issuer>
    <dsig:Signature xmlns:dsig="http://www.w3.org/2000/09/xmldsig#" Id="Id-
0001597673376485-ffffffffe506c0aa-1">
        <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="#_a69e4de1d6344deaae521ac96290edb5">
                <dsig:Transforms>
                    <dsig:Transform
Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature" />
                    <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="Id-
0001597673376485-ffffffffe506c0aa-2">

<dsig:KeyName>07c3d08bc6c3303a85c5e0c9547dfd91047f7c58</dsig:KeyName>
        </dsig:KeyInfo>
    </dsig:Signature>
    <samlp:Status>
        <samlp:StatusCode
Value="urn:oasis:names:tc:SAML:2.0:status:Success" />
    </samlp:Status>
</samlp:LogoutResponse>
```

Code Block 13 RD-LC LogoutResponse

8 SAML 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 TLS certificates in metadata

TLS certificates MUST be included in the LC metadata as a signing certificate (@use=signing). Difference with normal signing certificates can be made via extended key usage. See SAML Version 2.0 Errata 05, E62 (https://docs.oasis-open.org/security/saml/v2.0/errata05/os/saml-v2.0-errata05-os.html#__RefHeading__8148_1983180497)

8.2 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

8.3 DV metadata

Published by	Consumed by
DV that connect to RD directly	RD

Example of DV metadata.

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

Element/@Attribute	0..n	Description
EntityDescriptor	1	The metadata MUST contain one <EntityDescriptor> with one <SPPSSODescriptor> 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.

Element/@Attribute	0..n	Description
		Either validUntil or cacheDuration MUST be present. (following OASIS specification https://docs.oasis-open.org/security/saml/v2.0/saml-metadata-2.0-os.pdf)
-@cacheDuration	0..1	MAY contain cacheduration. RD is advised to check for new metadata after the given period. Either validUntil or cacheDuration MUST be present. (following OASIS specification https://docs.oasis-open.org/security/saml/v2.0/saml-metadata-2.0-os.pdf)
-Signature	1	Contains the Digital signature of the DV for the enveloped message (Algoritm="http://www.w3.org/2000/09/xmldsig#enveloped-signature"). MUST contain a <KeyInfo> element with a <KeyName> or <X509Certificate> element.
-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 TLS. 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 two seperate certificates. 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 SAML Version 2.0 Errata 05, E62 (https://docs.oasis-open.org/security/saml/v2.0/errata05/os/saml-v2.0-errata05-os.html#__RefHeading__8148_1983180497). 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. All certificates must be PKIoverheid certificates.
---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 user out of its current session if participating in a SSO sesssion.

Element/@Attribute	0..n	Description
---@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: http://docs.oasis-open.org/security/saml/v2.0/saml-bindings-2.0-os.pdf. 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 user will be redirected after authentication. If more than one is included one MUST contain the attribute @isDefault with value "true".
--AttributeConsumingService	0..n	Condtional: MUST be used if the DV does not support Extensions in the AuthnRequest. When used MUST contain 1 or more elements that describe the service requested using a pointer to a service definition registered with the AD.
---@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 AuthnRequest. It is adviced to Always include an AttributeConsumingServiceIndex in the AuthnRequest.
---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 the RV service catalogue (DC).

8.4 LC SAML SP metadata

Published by	Consumed by
LC	RD

Example of LC SAML SP metadata.

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 behind 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 the SAML 2.0 Metadata specification (see https://docs.oasis-open.org/security/saml/v2.0/saml-schema-metadata-2.0.xsd).

8.4.1 LC SP metadata

Element/@Attribute	0..n	Description
EntitiesDescriptor	1	Required element to start Metadata containing mutiple 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 https://docs.oasis-open.org/security/saml/v2.0/saml-metadata-2.0-os.pdf)
-@cacheDuration	0..1	MAY contain cacheduration. RD is advised to check for new metadata after the given period. Either validUntil or cacheDuration MUST be present. (following OASIS specification https://docs.oasis-open.org/security/saml/v2.0/saml-metadata-2.0-os.pdf)
-Signature	1	MUST contain the Digital signature of the LC for the enveloped message (Algoritm="http://www.w3.org/2000/09/xmldsig#enveloped-signature"). MUST contain a <KeyInfo> element with a <KeyName> or <X509Certificate> element. MUST be included to verify the integrity of the metadata. 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 LC EntityDescriptor.
-EntityDescriptor	1..n	MUST contain the EntityDescriptor of the LC (see "LC EntityDescriptor within LC metadata"). MUST contain the EntityDescriptors of all DV's the LC supports (see "DV EntityDescriptor within LC metadata").

8.4.2 LC EntityDescriptor within LC metadata

Element/@Attribute	0..n	Description
EntityDescriptor	1	Required element to start Metadata.
-@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.

Element/@Attribute	0..n	Description
		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 LC 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 TLS. This can be achieved by inclusion of 2 KeyDescriptor element with @use="signing". One MUST be used to sign the SAML messages, the other one MUST be used for TLS. 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 two separate certificates. TLS certificates for client authentication MUST be included as a signing certificate in the LC saml metadata. Difference with normal signing certificate can be made via extended key usage. See SAML Version 2.0 Errata 05, E62 (https://docs.oasis-open.org/security/saml/v2.0/errata05/os/saml-v2.0-errata05-os.html#__RefHeading__8148_1983180497). All certificates must be PKIoverheid certificates containing the OIN as refered to in this EntityDescriptor's entityID.
---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 LC supports SSO. Describes the endpoint used to log the user out of its current session if participating in a SSO sesssion.

Element/@Attribute	0..n	Description
---@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: http://docs.oasis-open.org/security/saml/v2.0/saml-bindings-2.0-os.pdf. 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 user will be redirected after authentication.
---@Binding	1	The binding parameter denotes the type of binding used. This is an urn relating to: http://docs.oasis-open.org/security/saml/v2.0/saml-bindings-2.0-os.pdf. At least one AssertionConcumerService 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 entries are included, one of these entries MUST be flagged as default by setting the isDefault XML attribute with value "true".

8.4.3 DV EntityDescriptor within LC metadata

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

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. 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.

Element/@Attribute	0..n	Description
-@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".
--KeyDescriptor	1..2	MUST contain at least 1 KeyDescriptor element with @use="encryption". A second <KeyDescriptor> MAY be present to support certificate rollover. All certificates must be PKIoverheid certificates containing the OIN as refered to in this EntityDescriptor's entityID.
---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 user 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 ingnored as the <AssertionConsumingService> definitions in the LC EntityDescriptor MUST be used.

8.5 RD SAML IdP Metadata

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

Example of RD SAML IdP metadata.

RD publishes metadata in accordance with urn: oasis: names: tc: SAML: 2.0: metadata with one EntityDescriptor element. The metadata is signed in accordance with the SAML signature.

The metadata published by RD is in accordance with the table below:

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 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 https://docs.oasis-open.org/security/saml/v2.0/saml-metadata-2.0-os.pdf)
-@cacheDuration	0..1	MAY contain cacheduration. DV or LC is advised to check for new metadata after the given period. Either validUntil or cacheDuration MUST be present. (following OASIS specification https://docs.oasis-open.org/security/saml/v2.0/saml-metadata-2.0-os.pdf)
-Signature	1	Contains the Digital signature of RD for the enveloped message (Algoritm="http://www.w3.org/2000/09/xmldsig#enveloped-signature"). MUST contain a <KeyInfo> element with a <KeyName> element.
-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.
--ArtifactResolutionService	1..n	The ArtifactResolutionService MUST be implemented at least once per service.

Element/@Attribute	0..n	Description
---@Binding	1	The binding parameter denotes the type of binding used. In theArtifactResolutionService this is the SAML-SOAP binding only. The value of this attribute is an urn relating to: http://docs.oasis-open.org/security/saml/v2.0/saml-bindings-2.0-os.pdf
---@Location	1	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 [SAMLProf].
---@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: http://docs.oasis-open.org/security/saml/v2.0/saml-bindings-2.0-os.pdf
---@Location	1	The URL of the SAML SingleSignOnService endpoint
--SingleLogoutService	1..n	Describes the endpoint used to log the user 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

8.6 Example Metadata

8.6.1 Example RD SAML IdP metadata

This is an example of the metadata the RD publishes in the role of SAML IdP.

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

```
<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="Id-
0001597663996617-fffffffff8db1b55-1">
        <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-signature"/>
                    <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="Id-
0001597663996617-fffffffff8db1b55-2">

<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_artifact"
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>
```

Code Block 14 RD SAML IdP metadata

8.6.2 Example DV SAML SP metadata

This is an example of the metadata the DV publishes in the role of SAML SP.

Published by	Consumed by
DV that connect to RD directly	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-signature" />
                    <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>
```

Code Block 15 DV SAML SP metadata

8.6.3 Example LC SAML SP Metadata

In this example the LC (entityID="urn:nl-eid-gdi:1.0:LC:00000008000000020000:entities:9011") services two DV's (entityID="urn:nl-eid-gdi:1.0:DV:00000004000000010000:entities:9002" and ityID="urn:nl-eid-gdi:1.0:DV:00000004000000020000:entities:9003").

Published by	Consumed by
LC	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-signature" />
                    <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:9011"
                         validUntil="2021-03-03T10:00:00Z"
                         >
        <md:SPSSODescriptor AuthnRequestsSigned="true" WantAssertionsSigned="true"
protocolSupportEnumeration="urn:oasis:names:tc:SAML:2.0:protocol">
            <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="true"/>
        </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:9002"
                         validUntil="2021-03-03T10:00:00Z"
                         >
        <md:SPSSODescriptor AuthnRequestsSigned="true" WantAssertionsSigned="true"
protocolSupportEnumeration="urn:oasis:names:tc:SAML:2.0:protocol">
            <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="true"/>
        </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:9003"
                         validUntil="2021-03-03T10:00:00Z"
                         >
        <md:SPSSODescriptor AuthnRequestsSigned="true" WantAssertionsSigned="true"
protocolSupportEnumeration="urn:oasis:names:tc:SAML:2.0:protocol">
            <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="true"/>
        </md:SPSSODescriptor>
    </md:EntityDescriptor>
</md:EntitiesDescriptor>
```

Code Block 16 LC SAML SP metadata

9 Technical requirements and recommendations

In this chapter additional instructions and requirements are given for message handling by the participants.

9.1 Signing, encryption algorithms and hash functions

eID SAML 4.x no longer supports 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	namespace
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: http://www.w3.org/TR/xmldsig-core/#sec-AlgID)

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

Digest

algorithm	namespace
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: http://www.w3.org/TR/xmldsig-core/#sec-AlgID)

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 in accordance with the SAML standard.

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 http://www.w3.org/TR/xml-exc-c14n/)
- 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.
- Participants MUST sign messages and metadata with a PKIoverheid certificate with a key length of at least 2048 bits, and which contains the OIN (organisatie-identificatie nummer) of the participant. The (extended) key usage of the used 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 SAML2.0 core (§5.4) and SAML 2.0 Metadata (§3.1).

9.2 Signature

Each <Signature> element in SAML messages generated by a DV or LC and in the DV or LC SAML SPmetadata MUST contain either a <KeyInfo> element with a <X509Certificate> element OR a <KeyName> element containing a keyname. The use of <KeyName> is preferred as this limits the amount of data exchanged.

Each <Signature> element in SAML messages generated by a RD and in the RD SAML IdP metadata MUST contain a <KeyInfo> element with a <KeyName> element containing a keyname that corresponds to a <KeyName> in a <KeyDescriptor> element in the RD's metadata.

Certificates used to verify a <Signature> MUST be retrieved from the party's verified metadata. The <X509Certificate> or <KeyName> in the <KeyInfo> of the Signature MUST only be used to retrieve the corresponding certificate from the verified metadata.

9.3 Encryption

Encryption is used to guarantee confidentiality. Encryption in combination with SAML is achieved via XML-encryption. 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	namespace
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 SHOULD NOT be used (http://www.w3.org/2009/xmlenc11#mgf1sha1).

9.4 TLS transport

The 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.

When connecting directly between the RD and the LC or DV (back channel), both parties must use a PKIoverheid certificate and mutual authentication is mandatory. This is also called two-sided or mutual TLS.

9.5 NotBefore en NotOnOrAfter

LCs and DVs 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 that are supported in the interface are listed here.

9.7 Local session

The DV is responsible for keeping track of the local End User session. This session MUST be terminated after at most 30 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.

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

9.8 RelayState

DVs may provide a RelayState for their own session monitoring. The 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.

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

9.9 User interaction

When a web service forwards an end user to an RD, an AD or a BVD, this must be done in such a way that it is clear to the user on which website he is and that he can actually check this. That is why the following requirements apply:

1. The end user must be redirected to the AD in the same screen that the user clicked on "Log in to <AD>".
2. The end user must see a browser window with the full address bar. This allows a user to see on which website he is entering his data. The user can check this by inspecting the certificate (green lock).

3. It is not allowed to invoke an RD, AD or BVD website in a frame or iframe, or to embed these websites in another way in a page of the web service.

The DV or a LC on behalf of the web service must decide on the basis of the assertion(s) whether a user can gain access to the web 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 user does not have the required level of assurance (AuthnContext in Assertion) then:

1. The DV or LC is obliged to immediately end the current session on its web service.
2. Should show an appropriate message (see section 5.13 Error messages and statuses).

10 Type definitions

This page and underlying pages describe identifier types which are used both at the DigiD SAML-CA and the DigiD OIDC interfaces with the goal to create consistency between these interfaces.

- Attribute Identifier types
- entityID
- Levels of Assurance

10.1 Attribute Identifier types

eID SAML 4.4 describes the following Attribute Identifier Types

Attribute	Identification-code	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 https://wiki.bsn-koppelregister.nl/display/DC/Encrypted+structures)
Pseudonym	`urn:nl-eid-gdi:1.0:id:Pseudonym`	Encrypted Pseudonym (see https://wiki.bsn-koppelregister.nl/display/DC/Encrypted+structures)

The following attributes may be supplied additionaly, only through eTD (see https://afsprakenstelsel.etoegang.nl/display/as/Identificerende+kenmerken)

10.2 entityID

The format of the entityID element is: **urn:nl-eid-gdi:1.0:<ROLE>:<OIN>:entities:<index>**

Attribute	Value	Remarks
<OIN>	The OIN of the organisation.	
<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 or the service provider to define different endpoints (in the metadata). Numbers between 9000 and 9999 are reserved for test systems.	

10.3 Levels of Assurance

The table shows the SAML eID Levels of Assurance and their corresponding levels with DigiD, eTD and eIDAS. The <Assertion> created by the RD wil contain the eID LoA. IdP assertions included in the <Advice> element of the RD <Assertion> will contain the LoA definition from the scheme used by the IdP or BVD.

DigiD 3.3	DigiD	eTD	eIDAS	eID
-	-	1	-	
urn:oasis:names:tc:SAML:2.0:ac:classes:PasswordProtectedTransport	Basis	2	Low	http://eID.logius.nl/LoA/basic
urn:oasis:names:tc:SAML:2.0:ac:classes:MobileTwoFactorContract	Midden	2+	Low	http://eidas.europa.eu/LoA/low
urn:oasis:names:tc:SAML:2.0:ac:classes:Smartcard	Substantieel	3	Substantial	http://eidas.europa.eu/LoA/substantial
urn:oasis:names:tc:SAML:2.0:ac:classes:SmartcardPKI	Hoog	4	High	http://eidas.europa.eu/LoA/high