Programma eID
Afsprakenstelsel

Interface specifications

eID Scheme

Version: 1.0

Date: 21 January 2014

Status: Definitief

Colophon

eID Program

eID SCHEME project

Visitor Address:

Herman Gorterstraat 5

Utrecht

Version	1.0
Principal	Steering group eID
Annex(es)	
Number of pages	34
Copy number	

Introduction

This document is part of the eID SCHEME and describes the interface specifications for the eID SCHEME NETWORK. The specifications detail the connection, security and messaging protocols for the interaction between the different roles in the eID SCHEME.

The eID SCHEME intends to be independent of technology where possible. These specifications are the main point where technology independence is not a goal. Instead it is a goal to standardise as much as possible in order to guarantee interoperability throughout the eID SCHEME NETWORK.

The following topics have not been included in these specifications and should be added in a future version.

- Single Sign On / Sign Out
- Sessions
- SOAP
- WS-security
- Metadata
- Example messages
- Language preference
- Processing rules per role
- Authentication of an expected subject

Notational conventions

Reserved terms are indicated like this: RESERVED TERM.

References to SAML XML elements are indicated like this: <*SAMLelement*>.

References to SAML XML attributes are indicated like this: *@SAMLattribute*.

References to the name of Attributes specified by this specification (to be included in SAML Attribute Statements) are indicated like this: `AttributeName`.

Table of contents

Colophon—2

Introduction—3

Notational conventions—4

Table of contents—5

1 General specifications—9

1.1 Terminology—9

1.2 SAML—9

1.2.1 SAML for DECLARATIONS—9

1.2.2 SAML profiles—9

1.2.3 SAML binding—9

1.2.4 SAML version—9

1.3 Web Services—10

1.3.1 SOAP—10

1.3.2 WS-Security—10

1.3.3 DECLARATION OF ASSOCIATION—10

1.4 Transport layer security—10

1.4.1 SSL/TLS—10

1.4.2 SSL/TLS certificates—10

1.5 Message security—10

1.5.1 Signing of messages—10

1.5.2 Signing of <Assertion> elements—10

1.5.3 Signing certificates—10

1.5.4 Signing algorithm—11

1.5.5 Hashing algorithm—11

1.5.6 Canonicalization method—11

1.5.7 Validating signatures—11

1.6 Masking 'personal' information—11

1.7 SAML specific security—11

1.7.1 XML Signature specifications for SAML—11

1.7.2 Linking of DECLARATIONS—12

1.8 Other—13

1.8.1 Character sets and encoding—13

1.8.2 Optional elements and attributes—13

1.8.3 Time—13

2 Data dictionary—14

2.1 Core data elements—14

2.2 Sector identifiers—16

2.3 Attribute catalogue—16

2.4 Subject identifiers—16

2.5 Service Catalogue—17

3 Generic SAML message constructs—18

3.1 AttributeQuery—18

3.2 Extensions in request—19

3.3 SAML Response—19

3.4 SAML Assertion—20

3.5 Generic eID attribute statement—21

4 K1: Interface eID Broker – Identity Provider—23

4.1 Request—23

4.2 Response—24

4.2.1 Authentication Statement—24

4.2.2 Attribute Statement for Declaration of Identity—24

5 K2: Interface eID Broker – Authorisation Information Provider—26

5.1 Request—26

5.2 Response—26

5.2.1 Attribute Statement for Declaration of Authorisation—26

6 K8: Interface eID Broker – Attribute Provider—27

6.1 Request—27

6.2 Response—27

7 K5: Interface eID Broker – SectorID Provider—28

7.1 Request—28

7.2 Response—28

7.2.1 Attribute Statement for Declaration of Attribute—28

8 K3: Interface Service Provider – eID Broker—29

8.1 Request—29

8.2 Response—30

8.2.1 Alternative 1: providing all Declarations as separate <Assertion> elements—30

8.2.2 Alternative 2: embedding all Declarations in one <Assertion>—30

9 K4: Interface SERVICE INTERMEDIARY – SERVICE PROVIDER—31

10 K7: Interface IDENTITY PROVIDER / AUTHORISATION INFORMATION PROVIDER – SCHEME AUTHORITY—32

Appendix A: XML Schema for Extensions element—33

1 General specifications

This chapter describes general specifications that apply to several or all interfaces. Applicability is indicated per specification.

1.1 Terminology

See Section 5: "Begrippenlijst".

1.2 SAML

This paragraph describes how the interface specifications described in this document use/are built on the SAML specifications.

1.2.1 SAML for DECLARATIONS

The following DECLARATIONS are modelled as a SAML assertion:

- DECLARATION OF IDENTITY;
- DECLARATION OF AUTHORISATION;
- DECLARATION OF ATTRIBUTE;

In this document the terms DECLARATION and assertion are exchangeable.

1.2.2 SAML profiles

Since the EID SCHEME aims to lower implementation barriers where possible, these specifications aim for full conformance with common SAML profiles. These profiles are:

- Web Browser SSO profile;
- Attributes profile.

1.2.3 SAML binding

Since the EID SCHEME aims to lower implementation barriers where possible and strives to be conformant to existing profiles like the Kantara eGov profile, these specifications specify one binding that is able to transport all required information still meeting the security requirements.

All SAML messages between EID PARTICIPANTS should be exchanged over an HTTP artifact binding.

EID BROKERS may offer additional bindings to their customers.

In order to avoid caching of security information, for every HTTP request the following headers must be set:

- Cache-Control = "no-cache, no-store"
- Pragma = "no-cache"

N.B. the SAML <*AttributeQuery*> does not bind to any asynchronous binding according to the SAML specifications. However, to meet user consent requirements at the source of the information it is really necessary to have the USER redirected to that source through an asynchronous binding. Therefore this specification *does* require the <*AttributeQuery*> to be used with a HTTP artifact binding.

N.B. for machine-to-machine communication purposes also a SOAP binding for the interface with the AUTHORISATION INFORMATION PROVIDER and the SCHEME AUTHORITY will be specified. This will be part of a future version of this document.

1.2.4 SAML version

Only SAML version 2.0, errata 5 (1 May 2012) shall be used.

1.3 Web Services

Place holder for future version.

1.3.1 SOAP

1.3.2 WS-Security

1.3.3 DECLARATION OF ASSOCIATION

1.4 Transport layer security

This paragraph describes the general transport layer security requirements.

1.4.1 SSL/TLS

All connections must be secured with SSL 3.0 or higher or TLS. The WS-I basic security profile[1] mentions cipher suites that are discouraged. The cipher suites shall not be used.

1.4.2 SSL/TLS certificates

All participants and public SERVICE PROVIDERS must use PKIoverheid G2 SSL certificates for securing connections.

Private SERVICE PROVIDERS must use either

- PKIoverheid G2 SSL certificates, or
- Another SHA256 based Extended Validation SSL certificate, recognized by all common browsers

for securing connections.

All certificates must have a key length of minimal 2048 bits.

The (extended) key usage field of a certificate must allow use for SSL/TLS.

1.5 Message security

This paragraph describes the general message security requirements.

1.5.1 Signing of messages

All messages (request and response, SAML and SOAP) must be signed by the sender of that message with an XML Signature.

1.5.2 Signing of <Assertion> elements

All <*Assertion*> elements must be signed by the <*Issuer*> of that <*Assertion*> with an enveloped XML Signature.

1.5.3 Signing certificates

All EID PARTICIPANTS and SERVICE PROVIDERS must use their SCHEME CERTIFICATE for signing purposes.

All certificates must have a key length of minimal 2048 bits.

The (extended) key usage field of a certificate must allow use for message signing.

[1] http://www.ws-i.org/Profiles/BasicSecurityProfile-1.0.html

1.5.4 Signing algorithm

For all signing the RSA-SHA256 algorithm must be used.

1.5.5 Hashing algorithm

For all hashing of message data (e.g. creating message digests) the SHA256 algorithm must be used.

1.5.6 Canonicalization method

For all canonicalization purposes, both in creating digests and creating the signature value, Exclusive XML Canonicalization must be used.

1.5.7 Validating signatures

The signature of every message and every <*ASSERTION*> should be verified, prior to further processing the message/Assertion. Unsigned information shall not be processed.

1.6 Masking 'personal' information

All SAML attributes that contain sensitive subject information (regardless whether the subject is a natural or legal person) are masked during transport, so that only intended recipients can unmask the information. The procedure of masking exists of the following steps.

1. The value of the attribute is padded with the "#" symbol and a timestamp. This guarantees that not intended audience sees a different value for every message even if the actual value is the same, preventing pattern recognition.
2. The attribute is encrypted according SAML specifications.
3. The symmetric key for the SAML attribute is encrypted with the public key of the SCHEME CERTIFICATE of every intended recipient.

The SAML Attributes that are not encrypted are gathered in a generic attribute statement (see Paragraph 3.5). Values belonging to the SAML core specifications are not encrypted.

1.7 SAML specific security

1.7.1 XML Signature specifications for SAML

This paragraph describes the specification for an XML <*Signature*> as used in SAML messages and <*ASSERTION*>s.

Element/@Attribute	**0..n**	**Description**
<*Signature*>	1	
@Id	0..1	May be used. No EID SCHEME requirements.
<*SignedInfo*>	1	
@Id	0..1	May be used. No EID SCHEME requirements.
<*CanonicalizationMethod*>	1	
@Algorithm	1	Must indicate Exclusive XML Canonicalization.
<*SignatureMethod*>	1	
@Algorithm	1	Must indicate RSA-SHA256 (note that here also Exclusive XML Canonicalization must be used).
<*Reference*>	1	
@Id	0..1	May be used. No EID SCHEME requirements.

@URI	1	Must refer to root of message/Assertion.
@Type	0..1	May be used. No EID SCHEME requirements.
<Transforms>	1	
<Transform>	2	
<Algorithm> (1st)	1	Must indicate Exclusive XML Canonicalization.
<Algorithm> (2nd)	1	Must indicate an enveloped signature.
<DigestMethod>	1	
<Algorithm>	1	Must indicate SHA-256
<DigestValue>	1	Must contain digest value.
<SignatureValue>	1	Must contain signature value.
<KeyInfo>	1	
<KeyName>	0	Shall not be used.
<KeyValue>	0	Shall not be used.
<RetrievalMethod>	0	Shall not be used.
<X509Data>	1	
<X509IssuerSerial>	0	Shall not be used.
<X509SKI>	0	Shall not be used.
<X509SubjectName>	0	Shall not be used.
<X509Certificate>	1	Must contain the SCHEME CERTIFICATE that can be used to verify the signature.
<X509CRL>	0	Shall not be used.
<PGPData>	0	Shall not be used.
<SPKIData>	0	Shall not be used.
<MgmtData>	0	Shall not be used.
<Object>	0	Shall not be used.

1.7.2 Linking of DECLARATIONS

It is intended that every DECLARATION that is based on another DECLARATION can be linked to that DECLARATION in an unbreakable manner. The only mechanism provided by SAML off the shelve, is including (nesting) an *<Assertion>*, which does not allow for enough flexibility while constructing an AUTHORISATION CHAIN with belonging DECLARATIONS OF ATTRIBUTE. Therefore additional measures, proprietary to these specifications have been taken.

For linking DECLARATIONS the following measures must be taken.

Referring to the DECLARATION
An ID to the referred DECLARATION is included in the *<Assertion>* in the *<Advice>* element in an *<AssertionIDRef>* element. This allows for standard assessment of the referred DECLARATION (e.g. is it present, is it conform SAML specs).

- Unbreakable link
  In order to provide an unbreakable link to the referred DECLARATION the *<SignatureValue>* of

that DECLARATION is included in the new DECLARATION as an attribute *LinkedAssertionSignatureValue*.

N.B. A DECLARATION can be linked to only one referred DECLARATION.

1.8 Other

1.8.1 Character sets and encoding

Systems must support the MES-2 character set.

Characters must be UTF-8 encoded.

1.8.2 Optional elements and attributes

Optional elements and optional attributes may be included in messages. If an empty optional element or empty optional attribute is included, it is treated as though the element or attribute was not present.

1.8.3 Time

All time must be indicated in Coordinated Universal Time (UTC), formatted as yyyy-mm-ddThh:mm:ssZ.

All EID PARTICIPANTS and SERVICE PROVIDERS must synchronise with a stratum 2 or 3 NTP time server.

2 Data dictionary

This chapter describes all data elements used in the SAML messages

2.1 Core data elements

All data elements that belong to the core of these specifications are prefixed with nl:eid-scheme:core: These data elements are included in SAML Attribute Statements as a SAML <*Attribute*>.

SAML <*Attribute*> name	**Description**	**Format**
ActingOnBehalfOf	Indicates whether a DECLARATION OF IDENTITY is used for acting on one's own behalf or to represent another person. Note that with the proper user consent, a DECLARATION OF IDENTITY may be issued for dual use: to act on one's own behalf and to represent another person (value "both").	Valid values are "Self", "Other", "Both"
ActingSubjectID	Identifies the ACTING SUBJECT. If the AUTHORISATION CHAIN is complete and does not contain a DECLARATION OF AUTHORISATION, the *ActingSubjectID* in the DECLARATION OF IDENTITY also describes the LEGAL SUBJECT.	See Paragraph 2.4.
ActingSubjectIDType	Identifies the type of the *ActingSubjectID*	See Paragraph 2.4.
AuthorisationChainComplete	If the <*Assertion*> is either a DECLARATION OF IDENTITY or a DECLARATION OF AUTHORISATION (thus part of an AUTHORISATION CHAIN) this field indicates if the AUTHORISATION CHAIN is complete.	Boolean 0/1/no/yes/false/true
DeclarationType	Identifies the type of DECLARATION in a SAML <*Assertion*>.	Valid values are "DeclarationOfIdentity", "DeclarationOfAuthorisationInformation", "DeclarationOfAttribute".
DeprecatedActingSubjectID	Former ID of the ACTING SUBJECT, used for migration purposes only.	See Paragraph 2.4.
DeprecatedActingSubjectIDType	Identifies the type of the *DepricatedActingSubjectID*	See Paragraph 2.4.

SAML <*Attribute*> name	**Description**	**Format**
DeprecatedLegalSubjectID	Former ID of the LEGAL SUBJECT, used for migration purposes only.	See Paragraph 2.4.
DeprecatedLegalSubjectIDType	Identifies the type of the *DepricatedLegalSubjectID*	See Paragraph 2.4.
DepricatedSectorID	Former *SectorID* of a subject, used for migration purposes only.	See Paragraph 2.2.
DepricatedSectorIDType	Identifies the type of *DepricatedSectorID*.	See Paragraph 2.2.
eIDSchemeVersion	Version of the EID SCHEME	1.0
EntityID	ID of an entity active in the EID SCHEME.	OIN based on KvK-nummer. N.B. for foreign entities similar national identifiers shall be used.
Evidence	Contains the <*Assertion*> elements that are provided as evidence with the request.	One or more <*Assertion*> elements. See Appendix A.
IntendedAudience	Identifies all parties that are intended to process the content of the requested assertion(s)	SCHEME CERTIFICATE, issued by the EID SCHEME governance body, for each party.
LegalSubjectID	Identifies the LEGAL SUBJECT.	See Paragraph 2.4.
LegalSubjectIDType	Identifies the type of the *LegalSubjectID*.	See Paragraph 2.4.
LevelOfAssurance	Indicates the LEVEL OF ASSURANCE in four levels, one for lowest, four for highest. For a request it is the required LEVEL OF ASSURANCE. For a response it is the LEVEL OF ASSURANCE of the 'weakest link' in the process. Processes must be assessed by an external auditor.	Valid values are "LoA1", "LoA2", "LoA3" or "LoA4" N.B. LEVELS OF ASSURANCE may differ per type of DECLARATION. The exact number of levels and their meaning will be specified in a separate document.
LinkedDeclarationSignatureValue	Contains the <*SignatureValue*> of the linked DECLARATION.	Base64
ProvidedAttributes	Contains names of the attributes that are provided by the <*Issuer*> of <*Assertion*>.	String max 1024. Names are separated by a "|".
RequestedAttributes	Contains the names of the attributes that are requested from the recipient of the request.	One or more requested attributes. See Appendix A.

SAML <*Attribute*> name	Description	Format
RequestType	Indicates in what is the purpose of a request.	Valid values are • "RequestForDoI" to an IDENTITY PROVIDER • "RequestForDoAU" to an AUTHORISATION INFORMATION PROVIDER • "RequestForDoAT" to an ATTRIBUTE PROVIDER • "RequestForDoSI" to a SECTORID PROVIDER • "RequestForDECLARATIONS" to an EID BROKER.
SectorID	Identifies a subject in a certain sector.	See Paragraph 2.2.
SectorIDType	Identifies the type of *SectorID*.	See Paragraph 2.2.
ServiceID	Identifies a service in the SERVICE CATALOGUE.	See Paragraph 2.5.

2.2 Sector identifiers

All sector identifiers are prefixed with nl:eid-scheme:sectorid:

Sector Identifier	Description	Format
BSN	Dutch citizen service number. Issued and maintained by the Dutch government.	9 digit number

2.3 Attribute catalogue

All attributes describing subjects are prefixed with nl:eid-scheme:attribute:

Attribute	Description	Format
FirstName		String max 70
Initials		String max 35
LastName		String max 140
Date of Birth		yyyy-mm-dd
Place of Birth		String max 70
Gender		"M", "F", "U"

2.4 Subject identifiers

All SECTORID'S (see Paragraph 2.2) can be used to identify a subject. In addition the following subject identifiers can be used.

All subject identifiers are prefixed with nl:eid-scheme:subjectid:

Subject Identifier	Description	Format
PSEUDOID	Pseudonym identifying a natural person.	See document "Werking van het Stelsel".
KvK-nummer	Number of entity registered with the Dutch Chamber of Commerce.	8 digit number
Vestigingsnummer	Number of a location related to an entity registered with the Dutch Chamber of Commerce.	12 digit number
RSIN	ID of a legal entity	9 digit number

N.B. Values for PSEUDOID are audience specific. Therefore a PSEUDOID per audience is included in an <*Assertion*>. For the other Subject Identifiers this is not necessary.

2.5 Service Catalogue

In the SERVICE CATALOGUE services are registered. Every SERVICE PROVIDER is owner of its own services.

For each service the following information must be present:

- ID
- Name
- Description
- LEVEL OF ASSURANCE
- Optional: SECTORID(s) required
- Optional: Attribute(s) required

To be detailed in a future version.

3 Generic SAML message constructs

This chapter describes several parts of SAML messages/assertions that occur several times. In order to avoid redundancy these parts are included in a separate chapter.

3.1 AttributeQuery

This paragraph describes the general SAML AttributeQuery that is used to request a DECLARATION OF AUTHORISATION, and a DECLARATION OF ATTRIBUTE.

Element/@Attribute	0..n	Description
@ID	1	Must identify the message uniquely within the scope of the sender and receiver for a period of at least 12 months.
@Version	1	Must be "2.0".
@IssueInstant	1	Time of issuing of the request.
@Destination	1	URL of the recipient where the request is sent.
@Consent	1	Must indicate implicit consent. N.B. Since we aim for consent at the source of the information, there's nothing to be gained through explicit consent at the side of the requestor.
<Issuer>	1	Must contain EntityID of the EID BROKER.
@NameQualifier	0	Shall not be used.
@SPNameQualifier	0	Shall not be used.
@Format	0	Shall not be used.
@SPProviderID	0	Shall not be used.
<Signature>	1	See Paragraph 1.7.1.
<Extensions>	1	See Paragraph 3.2.
<Subject>	1	
<BaseID>	0	Shall not be used.
<NameID>	1	Contains a transient identifier. For a request for a DECLARATION OF AUTHORISATION it must be a new transient identifier not related to any other transient identifier used in the AUTHORISATION CHAIN. For a request for a DECLARATION OF ATTRIBUTE it must be the same as the one contained in one of the *<Assertion>* element(s) that is/are provided as `Evidence`. It refers to the identity for which the attributes or SECTORID are requested.
@NameQualifier	0	Shall not be used.
@SPNameQualifier	0	Shall not be used.
@Format	1	Must indicate a transient identifier.
@SPProviderID	0	Shall not be used.
<EncryptedID>	0	Shall not be used.

Element/@Attribute	0..n	Description
<*SubjectConfirmation*>	0	Shall not be used. N.B. for all exchange through SAML bindings the Bearer confirmation method is assumed. SOAP exchange to be defined.
<*Attribute*>	0..n	Contains all names of attributes (or SECTORID) that the recipient is requested to provide. One for every attribute.

3.2 Extensions in request

This paragraph describes the contents of the <*Extensions*> element that is used in request messages. Requests from EID BROKER to other EID PARTICIPANTS must contain these extensions. Requests from the SERVICE PROVIDER to the EID BROKER may contain these extensions.

See also Appendix A.

Element/@Attribute	0..n	Description
<*eIDSchemeVersion*>	1	See Paragraph 2.1.
<*RequestType*>	1	See Paragraph 2.1.
<*LevelOfAssurance*>	1	See Paragraph 2.1. Contains the LEVEL OF ASSURANCE that is required for the requested DECLARATIONS.
<*ServiceID*>	1	See Paragraph 2.1. Identifies the service for which an authorisation is required.
<*IntendedAudience*>	1	See Paragraph 2.1.
<*AudienceCertificate*>	1..n	One entry for every party that is intended to receive and process the requested <*Assertion*>.
<*X509Certificate*>	1	Contains the SCHEME CERTIFICATE of a party.
<*RequestedAttributes*>	0..1	See Paragraph 2.1. Contains all names of attributes that the recipient is requested to provide. Shall only be used in SAML AuthnRequest. For SAML AttributeQuery the standard way of asking for attributes shall be used.
<*RequestedAttribute*>	1..n	One for every attribute.
<*Evidence*>	0..1	See Paragraph 2.1.
<*Assertion*>	1..n	One for every <*Assertion*> that is provided as evidence with the request.

3.3 SAML Response

This paragraph describes the response message that contains one or more <Assertion> elements.

Element/@Attribute	0..n	Description
@ID	1	Must identify the message uniquely within the scope of the sender and receiver for a period of at least 12 months.
@InResponseTo	1	Must contain the @*ID* of the request message to which this message is a response.

Element/@Attribute	0..n	Description
@Version	1	Must be "2.0".
@IssueInstant	1	Time of issuing of the response.
@Destination	1	URL of the receiver where the response is sent.
@Consent	1	Must indicate implicit consent.
<Issuer>	1	Must contain ID of the sender of the response.
@NameQualifier	0	Shall not be used.
@SPNameQualifier	0	Shall not be used.
@Format	0	Shall not be used.
@SPProviderID	0	Shall not be used.
<Signature>	1	See Paragraph 1.7.1.
<Extensions>	0	Shall not be used.
<Status>	1	
<StatusCode>	1	
@Value	1	If not "success" additional information should be provided. To be detailed.
<StatusCode>	0..1	Only present if top-level StatusCode is not "success"
@Value	1	
<StatusMessage>	0..1	Only present if top-level StatusCode is not "success"
<StatusDetail>	0..1	Only present if top-level StatusCode is not "success"
<Assertion>	0..n	Contains the *<Assertion>*(s) that are delivered in the response.
<EncryptedAssertion>	0	Shall not be used.

3.4 SAML Assertion

This paragraph describes an *<Assertion>*.

Element/@Attribute	0..n	Description
@ID	1	Must identify the *<Assertion>* uniquely within the scope of the *<Issuer>* for a period of at least 12 months.
@Version	1	Must be "2.0".
@IssueInstant	1	Time of issuing of the Assertion.
<Issuer>	1	Must contain ID of the *<Issuer>* of the *<Assertion>*.
@NameQualifier	0	Shall not be used.
@SPNameQualifier	0	Shall not be used.
@Format	0	Shall not be used.
@SPProviderID	0	Shall not be used.

Element/@Attribute	0..n	Description
<*Signature*>	1	See Paragraph 1.7.1.
<*Subject*>	1	
<*BaseID*>	0	Shall not be used.
<*NameID*>	1	Contains the transient identifier. Two <*Assertion*> elements that describe the same entity must have the same transient identifier. <*Assertion*> elements in the same AUTHORISATION CHAIN must have different transient identifiers.
@NameQualifier	0	Shall not be used.
@SPNameQualifier	0	Shall not be used.
@Format	1	Must indicate a transient identifier.
@SPProviderID	0	Shall not be used.
<*EncryptedID*>	0	Shall not be used.
<*SubjectConfirmation*>	0	Shall not be used.
<*Conditions*>	1	
@NotBefore	1	
@NotOnOrAfter	0..1	
<*Condition*>	0	Shall not be used.
<*AudienceRestriction*>	1	Identifies every party that is intended to receive and process the <*Assertion*>.
<*Audience*>	1..n	Contains the EntityID for a party.
<*OneTimeUse*>	0..1	If present must be false.
<*ProxyRestriction*>	0	Shall not be used.
<*Advice*>	0..1	Used to reference a linked <*Assertion*>.
<*AssertionIDRef*>	1	Contains the ID of a linked <*Assertion*>.
<*AssertionURIRef*>	0	Shall not be used.
<*Assertion*>	0	Shall not be used.
<*EncryptedAssertion*>	0	Shall not be used.

3.5 Generic eID attribute statement

This paragraph describes a generic attribute statement that is present in every SAML <*Assertion*>. The attribute statement contains the following attributes.

N.B. These attributes are delivered in a non-encrypted manner.

SAML Attribute	0..n	Description
DeclarationType	1	See Paragraph 2.1. Contains the type of the DECLARATION.
eIDSchemeVersion	1	See Paragraph 2.1.
LevelOfAssurance	1	See Paragraph 2.1.

SAML Attribute	0..n	Description
ProvidedAttributes	0..1	See Paragraph 2.1.
ActingOnBehalfOf	0..1	See Paragraph 2.1. Must be present for DECLARATION OF IDENTITY. Shall not be present for other DECLARATIONS.
AuthorisationChainComplete	0..1	See Paragraph 2.1. Must be present for DECLARATION OF IDENTITY and DECLARATION OF AUTHORISATION. Shall not be present for other DECLARATIONS. If for a DECLARATION OF IDENTITY the *ActingOnBehalf* attribute is set to "Self" the *AuthorisationChainComplete* must be set to true.
LinkedDeclarationSignatureValue	0..1	See Paragraph 2.1.

4 K1: Interface eID Broker – Identity Provider

This chapter specifies the interface between eID Broker and Identity Provider in which a Declaration of Identity is requested and provided.

4.1 Request

This request is implemented as a SAML AuthnRequest.

Element/@Attribute	0..n	Description
@ID	1	Must identify the message uniquely within the scope of the sender and receiver for a period of at least 12 months.
@Version	1	Must be "2.0".
@IssueInstant	1	Time of issuing of the request.
@Destination	1	URL of the Identity Provider where the request is sent.
@Consent	1	Must indicate implicit consent.
@ForceAuthn	0..1	If not present or false, SSO may be executed. If present and true, a new authentication is enforced.
@IsPassive	0..1	If present must be false.
@ProtocolBinding	0..1	Must indicate HTTP artifact binding.
@AssertionConsumerServiceIndex	0..1	If present must refer by index to an endpoint entry in SAML metadata. Shall not be present if *@AssertionConsumerServiceURL* is present. If neither *@AssertionConsumerServiceIndex* or *@AssertionConsumerServiceURL* is present, default endpoint from metadata must be used.
@AssertionConsumerServiceURL	0..1	If present, URL must point to a SAML endpoint. Shall not be present if *@AssertionConsumerServiceIndex* is present.
@AttributeConsumingServiceIndex	0	Shall not be used.
@ProviderName	0	May be used. No eID Scheme requirements.
<Issuer>	1	Must contain EntityID of the eID Broker.
@NameQualifier	0	Shall not be used.
@SPNameQualifier	0	Shall not be used.
@Format	0	Shall not be used.
@SPProviderID	0	Shall not be used.
<Signature>	1	See Paragraph 1.7.1.
<Extensions>	1	See Paragraph 3.1.
<Subject>	0	Shall not be used.
<NameIDPolicy>	0	Shall not be used.

Element/@Attribute	0..n	Description
<Conditions>	0	Shall not be used.
<RequestedAuthnContext>	0	Shall not be used.
<Scoping>	0	Shall not be used.

4.2 Response

This response, containing a DECLARATION OF IDENTITY, is implemented as a SAML response (see Paragraph 3.3) containing one SAML *<Assertion>* (see Paragraph 3.4) containing (in this order) one authentication statement, the generic eID attribute statement (see Paragraph 3.5), optionally one attribute statement specific to the DECLARATION OF IDENTITY and optionally one attribute statement containing other requested attributes.

All attributes provided outside of the generic eID attribute statement must be encrypted.

4.2.1 Authentication Statement

Element/@Attribute	0..n	Description
@AuthnInstant	1	Time of authentication
@SessionIndex	0..1	May be used. No EID SCHEME requirements.
@SessionNotOnOrAfter	0..1	May be used. No EID SCHEME requirements.
<SubjectLocality>	0	Shall not be used.
<AuthnContext>	0..1	May be used. No EID SCHEME requirements.
<AuthnContextClassRef>	0..1	May be used. No EID SCHEME requirements.
<AuthnContextDecl>	0..1	May be used. No EID SCHEME requirements.
<AuthnContextDeclRef>	0..1	May be used. No EID SCHEME requirements.
<AuthenticatingAuthority>	0..n	May be used. No EID SCHEME requirements.

4.2.2 Attribute Statement for DECLARATION OF IDENTITY

This optional attribute statement contains the following encrypted attributes.

SAML Attribute	0..n	Description
ActingSubjectID	1..n	See Paragraph 2.1. If type is PSEUDOID one for every recipient. If no PSEUDOID is provided for the SERVICE PROVIDER either additional information through a DECLARATION OF AUTHORISATION or DECLARATION OF ATTRIBUTE, or an additional attribute statement containing other requested attributes must be present. Otherwise no meaningful information is provided to the SERVICE PROVIDER.
ActingSubjectIDType	1	See Paragraph 2.1.
DeprecatedActingSubjectID	0..n	See Paragraph 2.1. Used only during migration of identifiers. If type is PSEUDOID one for every recipient.
DeprecatedActingSubjectIDType	0..1	See Paragraph 2.1. Used only during migration of identifiers.

If this attribute statement is not present an additional attribute statement containing other requested attributes must be present. Otherwise no meaningful information is provided to the recipient.

5 K2: Interface eID Broker – Authorisation Information Provider

This chapter specifies the interface between eID Broker and Authorisation Information Provider in which a Declaration of Authorisation is requested and provided.

N.B. An interface for requesting a Declaration of Authorisation for machine-to-machine interaction will be specified in a future version.

5.1 Request

This request is implemented as a SAML AttributeQuery. See Paragraph 3.1.

5.2 Response

This response, containing a Declaration of Authorisation, is implemented as a SAML response (see Paragraph 3.3) containing one SAML <*Assertion*> (see Paragraph 3.4) containing (in this order) the generic eID attribute statement (see Paragraph 3.5), one attribute statement specific to the Declaration of Authorisation and optionally one attribute statement containing other requested attributes.

All attributes provided outside of the generic eID attribute statement must be encrypted.

N.B. the transient identifier in the <*Subject*> of the Declaration must be different from the <*Subject*> of any other Declaration in the Authorisation Chain.

5.2.1 Attribute Statement for Declaration of Authorisation

The attribute statement contains the following encrypted attributes.

SAML Attribute	0..n	Description
LegalSubjectID	1..n	See Paragraph 2.1. If this Declaration is not the last in the Authorisation Chain this actually identifies an intermediary. If type is PseudoID one for every recipient.
LegalSubjectIDType	1	See Paragraph 2.1.
DeprecatedLegalSubjectID	0..n	See Paragraph 2.1. Used only during migration of identifiers. If type is PseudoID one for every recipient.
DeprecatedLegalSubjectIDType	0..n	See Paragraph 2.1. Used only during migration of identifiers.
ActingSubjectID	1..n	See Paragraph 2.1. If this Declaration is not the first in the Declaration of Authorisation in the Authorisation Chain this actually identifies an intermediary. If type is PseudoID one for every recipient.
ActingSubjectIDType	1	See Paragraph 2.1.

6 K8: Interface eID Broker – Attribute Provider

This chapter specifies the interface between eID Broker and Attribute Provider in which a Declaration of Attribute is requested and provided.

6.1 Request

This request is implemented as a SAML AttributeQuery. See Paragraph 3.1.

6.2 Response

This response, containing a Declaration of Attribute, is implemented as a SAML response (see Paragraph 3.3) containing one SAML Assertion (see Paragraph 3.4) containing (in this order) the generic eID attribute statement (see Paragraph 3.5) and optionally one attribute statement containing any of the requested attributes.

All attributes provided outside of the generic eID attribute statement must be encrypted.

N.B. the transient identifier in the <*Subject*> of the Declaration must be the same as the <*Subject*> of the Declaration (either a Declaration of Identity or a Declaration of Authorisation) describing the identity of the actor that is described by this Declaration of Attribute.

7 K5: Interface eID Broker – SectorID Provider

This chapter specifies the interface between eID Broker and SectorID Provider in which a Declaration of Attribute is requested and provided.

7.1 Request

This request is implemented as a SAML AttributeQuery. See Paragraph 3.1.

7.2 Response

This response, containing a Declaration of Attribute, is implemented as a SAML response (see Paragraph 4.2) containing one SAML Assertion (see Paragraph 4.3) containing (in this order) the generic eID attribute statement (see Paragraph 3.5) and one attribute statement specific to the Declaration of Attribute.

All attributes provided outside of the generic eID attribute statement must be encrypted.

N.B. the transient identifier in the <*Subject*> of the Declaration must be the same as the <*Subject*> of the Declaration (either a Declaration of Identity or a Declaration of Authorisation) describing the identity of the actor that is described by this Declaration of Attribute.

7.2.1 Attribute Statement for Declaration of Attribute

The attribute statement contains the following encrypted attributes.

SAML Attribute	0..n	Description
SectorID	1	See Paragraph 2.1.
SectorIDType	1	See Paragraph 2.1.
DepricatedSectorID	1	See Paragraph 2.1.
DepricatedSectorIDType	1	See Paragraph 2.1.

8 K3: Interface SERVICE PROVIDER – EID BROKER

This chapter specifies the interface between SERVICE PROVIDER and EID BROKER in which all required DECLARATIONS are requested and provided. The interface tries to be as compliant with the WebSSO profile, but also allows for more advanced features for more demanding SERVICE PROVIDERS.

N.B. an interface for gathering additional DECLARATIONS for an already authenticated subject will be specified in a future version.

8.1 Request

This request is implemented as a SAML AuthnRequest.

Element/@Attribute	0..n	Description
@ID	1	Must identify the message uniquely within the scope of the sender and receiver for a period of at least 12 months.
@Version	1	Must be "2.0".
@IssueInstant	1	Time of issuing of the request.
@Destination	1	URL of the EID BROKER where the request is sent.
@Consent	1	Must indicate implicit consent.
@ForceAuthn	0..1	If not present or false, SSO may be executed. If present and true, a new authentication is enforced.
@IsPassive	0..1	If present must be false.
@ProtocolBinding	0..1	
@AssertionConsumerServiceIndex	0..1	If present must refer by index to an endpoint entry in SAML metadata. Shall not be present if *@AssertionConsumerServiceURL* is present. If neither *@AssertionConsumerServiceIndex* or *@AssertionConsumerServiceURL* is present, default endpoint from metadata must be used.
@AssertionConsumerServiceURL	0..1	If present, URL must point to a SAML endpoint. Shall not be present if *@AssertionConsumerServiceIndex* is present.
@AttributeConsumingServiceIndex	0..1	If present, must refer to an entry in the SERVICE CATALOGUE. Either this or *<Extensions>* must be present. Not both.
@ProviderName	0	May be used. No EID SCHEME requirements.
<Issuer>	1	Must contain EntityID of the EID BROKER.
@NameQualifier	0	Shall not be used.
@SPNameQualifier	0	Shall not be used.
@Format	0	Shall not be used.
@SPProviderID	0	Shall not be used.
<Signature>	1	See Paragraph 1.7.1.

Element/@Attribute	0..n	Description
<*Extensions*>	0..1	See Paragraph 3.1. Either this or *@AttributeConsumingServiceIndex* must be present. Not both.
<*Subject*>	0	Shall not be used.
<*NameIDPolicy*>	0	Shall not be used.
<*Conditions*>	0	Shall not be used.
<*RequestedAuthnContext*>	0	Shall not be used.
<*Scoping*>	0	Shall not be used.

8.2 Response

The response is specified in two ways. During a proof of technology it must be proven which of these is the best.

8.2.1 Alternative 1: providing all DECLARATIONS as separate <Assertion> elements

The response is implemented as a SAML response containing all SAML <*Assertion*> elements, obtained by the EID BROKER.

8.2.2 Alternative 2: embedding all DECLARATIONS in one <Assertion>

The response is implemented as a SAML response containing one SAML <*Assertion*> containing no Statements. The SAML <*Assertion*> contains all original <*Assertion*> elements, obtained by the EID BROKER.

The original <*Assertion*> elements are included in the <*Advice*> element, in an <*Assertion*> element.

9 K4: Interface SERVICE INTERMEDIARY – SERVICE PROVIDER

Placeholder for future version.

10 K7: Interface IDENTITY PROVIDER / AUTHORISATION INFORMATION PROVIDER – SCHEME AUTHORITY

Placeholder for future version.

Appendix A: XML Schema for Extensions element

This appendix lists the XML Schema for the extensions element. See Paragraph 3.2.

```
<?xml version="1.0" encoding="UTF-8"?>
<!-- edited with XMLSpy v2012 sp1 (http://www.altova.com) by Vincent Jansen (Innopay) -->
<xs:schema xmlns:eid="urn:nl:eid-scheme:1.0" xmlns:xs="http://www.w3.org/2001/XMLSchema"
xmlns:md="urn:oasis:names:tc:SAML:2.0:metadata"
xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion" xmlns:ds="http://www.w3.org/2000/09/xmldsig#"
targetNamespace="urn:nl:eid-scheme:1.0" elementFormDefault="qualified" at-
tributeFormDefault="qualified" version="1.0">
  <xs:import namespace="urn:oasis:names:tc:SAML:2.0:metadata" schemaLocation="saml-schema-
metadata-2.0.xsd"/>
  <xs:import namespace="urn:oasis:names:tc:SAML:2.0:assertion" schemaLocation="saml-schema-
assertion-2.0.xsd"/>
  <xs:import namespace="http://www.w3.org/2000/09/xmldsig#" schemaLoca-
tion="http://www.w3.org/TR/2002/REC-xmldsig-core-20020212/xmldsig-core-schema.xsd"/>
  <xs:element name="eIDSchemeVersion" type="xs:string"/>
  <xs:element name="RequestType">
    <xs:simpleType>
      <xs:restriction base="xs:string">
        <xs:enumeration value="DeclarationOfAttribute"/>
        <xs:enumeration value="DeclarationOfIdentity"/>
        <xs:enumeration value="DeclarationOfAuthorisation"/>
      </xs:restriction>
    </xs:simpleType>
  </xs:element>
  <xs:element name="LevelOfAssurance">
    <xs:simpleType>
      <xs:restriction base="xs:string">
        <xs:enumeration value="LoA1"/>
        <xs:enumeration value="LoA2"/>
        <xs:enumeration value="LoA3"/>
        <xs:enumeration value="LoA4"/>
      </xs:restriction>
    </xs:simpleType>
  </xs:element>
  <xs:element name="ServiceID" type="xs:anyURI"/>
  <xs:element name="IntendedAudience">
    <xs:complexType>
      <xs:sequence>
        <xs:element name="AudienceCertificate" maxOccurs="unbounded">
          <xs:complexType>
            <xs:complexContent>
              <xs:extension base="ds:X509DataType"/>
            </xs:complexContent>
          </xs:complexType>
        </xs:element>
      </xs:sequence>
    </xs:complexType>
  </xs:element>
  <xs:element name="RequestedAttributes">
    <xs:complexType>
      <xs:sequence>
        <xs:element ref="md:RequestedAttribute" maxOccurs="unbounded"/>
      </xs:sequence>
    </xs:complexType>
```

```
  </xs:element>
  <xs:element name="Evidence" type="saml:EvidenceType"/>
</xs:schema>
```