eIDAS Constructed Attributes Specification for the Swedish eID Framework

ELN-0611-v1.0  
Version 1.0

2016-08-29

1 Introduction 3

1.1 Requirement key words 3

2 Provisional Identifier 3

2.1 Provisional identifier (prid) attribute 3

2.2 Provisional Identifier Persistence Indicator (pridPersistence) attribute 4

2.3 Algorithms 6

2.4 Algorithm selection and resulting pridPersistence value 6

3 References 8

# Introduction

This document extends “Attribute Specification for the Swedish eID Framework”, [EidAttributes] providing specifications for constructed attributes.

The concept of constructed attributes is introduced in Swedish national authentication nodes (proxy nodes) delivering identity assertions to Swedish Service Providers based on user authentication with a foreign eID.

A constructed attribute is an attribute that was not delivered by the foreign Identity Provider service, but was constructed in the Swedish authentication node by applying defined rules and algorithms to the authenticated user (subject) received from the foreign Identity Provider service (typically an eIDAS node).

## Requirement key words

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

These keywords are capitalized when used to unambiguously specify requirements over protocol features and behavior that affect the interoperability and security of implementations. When these words are not capitalized, they are meant in their natural-language sense.

# Provisional Identifier

The Attribute Specification for the Swedish eID Framework defines the attributes prid and pridPersistence.

The prid attribute holds a unique identifier for a person derived from attributes provided from another country. The purpose of this attribute is to provide a common unique attribute for an authenticated user independently of the attribute set or the characteristics of these attributes provided by the authentication service in the other country.

The pridPersistence attribute provides an indicator of the expected persistence of the prid identifier over time. The value in this attribute is determined by assessing the persistence of underlying foreign attributes from a particular source used in a particular prid generation algorithm.

This document defines a set of prid algorithms, when to use each algorithm and the resulting pridPersistence value.

## Provisional Identifier (prid) Attribute

The provisional identifier (prid) attribute is a SAML attribute identified by the SAML attribute name urn:oid:1.2.752.201.3.4.

The prid attribute holds a string value containing the following data:

**{2 letter ISO 3166 country code of citizen country}** + **”:“** + **{10..30 character identifier}**

Syntactically, provisional ID is defined by the following regular expression:

**^[A-Z]{2}:[0-9a-z][0-9a-z-]{8,28}[0-9a-z]$**

Explanation:

^ assert position at start of the string

[A-Z]{2} **match exactly 2 characters present in the list below**

A-Z a single character in the range between A and Z (case sensitive)

: matches the character “:“ literally

[0-9a-z] **match a single character present in the list below**

0-9 a single character in the range between 0 and 9, or

a-z a single character in the range between a and z (case sensitive)

[0-9a-z-]{8,28} **match between 8 and 28 characters present in the list below**

0-9 a single character in the range between 0 and 9, or

a-z a single character in the range between a and z (case sensitive), or

- the literal character “-“

[0-9a-z] **match a single character present in the list below**

0-9 a single character in the range between 0 and 9, or

a-z a single character in the range between a and z (case sensitive)

$ assert position at end of the string

Examples:

NO:29078534891

DK:09208-2002-2-194967071622

The 2 letter country code is the 2 letter ISO 3166 country code expressed in upper case letters. E.g. “SE” for Sweden and “NO” for Norway. This identifies the country that issued the eID used to authenticate the user (i.e. provided the infrastructure to identify the person). This is not necessarily the person’s actual citizenship or country of residence.

The identifier component holds a minimum of 10 and a maximum of 30 characters. The characters in the identifier component are restricted to the numeric characters 0-9, the letters a-z and the hyphen character “-“ (0x2D). Letters “a-z” MUST be lower case. Should a provisional ID ever be presented with upper case letters then such letter should be matched using case insensitive matching (e.g. “a” is equivalent to “A”). The identifier component MUST NOT start or end with a hyphen character.

## Provisional Identifier Persistence Indicator (pridPersistence) Attribute

The provisional identifier (pridPersistence) attribute is a SAML attribute identified by the SAML attribute name urn:oid:1.2.752.201.3.5.

The pridPersistence attribute holds a string value containing the following data:

**{1 letter Identifier (A, B or C)}**

Syntactically, provisional ID persistence indicator is defined by the following regular expression:

**^[A|B|C]$**

Explanation:

^ assert position at start of the string

[A|B|C] **match a single character present in the list below**

A|B|C a single character in the list A, B or C literally (case sensitive)

$ assert position at end of the string

Examples:

A

B

C

Value definitions:

|  |  |
| --- | --- |
| Value | Defined meaning |
| A | Persistence over time is expected to be comparable or better than a Swedish national ID number (personnummer). This means that the identifier typically is stable throughout the lifetime of the subject and is typically preserved even if the subject changes address, name or civil status. |
| B | Persistence over time is expected to be relatively stable, but lower than a Swedish national ID number (personnummer). This means that the identifier typically remains unchanged as long as the person does not change address, name or civil status. Such or similar event may cause the identifier to change but the identifier will not change just because the subject gets a new eID (electronic identification means) or changes eID provider. |
| C | No expectations regarding persistence over time. The identifier may change if the subject changes eID or eID provider. |

A Service Provider accepting a user with a pridPersistence value “C” SHOULD inform the user about the risk of losing access to the user account if the identifier changes over time and how to regain access to the account, should this happen[[1]](#footnote-1).

## Algorithms

This section defines algorithms for generating the identifier component of prid attribute values. The identifier component make up the characters following the “:” (colon) character in the prid.

The following prid generation algorithms are defined:

|  |  |
| --- | --- |
| **Name** | **Identifier component algorithm** |
| **default-eIDAS** | Input values:  eidasID = The identifier string value from the eIDAS PersonIdentifier attribute from the attribute source (identified by the attribute name http://eidas.europa.eu/attributes/naturalperson/PersonIdentifier).  Calculated values:  strippedID = eidasID after removing the 6 leading characters matching the regular expression ^[A-Za-z]{2}[\/](SE|se)[\/]$ (e.g, ”NO/SE/”).  normalizedID = strippedID converted according to the following steps:   1. Removing any white space and non-printable characters 2. Converting all upper case letters [A-Z] to lower case 3. Replacing with a single “-“ character, all sequences of characters of length (1…n) that does not contain [0-9] or [a-z]. 4. Remove any leading or trailing “-“ characters.   Result:  **If length of normalizedID < 10 characters:**  Return normalizedID padded with leading “0” (zero) characters until length = 10 characters.  **If length of normalizedID 10 - 30 characters:**  Return normalizedID  **If length of normalizedID > 30 characters:**  Return the string representation of the first 30 hexadecimal digits of the SHA256 hash of the UTF-8 encoded bytes of strippedID.  Exceptions:  If the following conditions occur in the process, prid generation fails:   1. Leading 6 characters of PersonIdentifier does not match regexp ^[A-Za-z]{2}[\/](SE|se)[\/]$ 2. normalizedID < 8 characters (not counting “-“ (hyphen) characters).   Examples (PersonIdentifier 🡪 prid identifier component):  NO/SE/05068907693 🡪 05068907693  DK/SE/09208-2002-2-194967071622 🡪 09208-2002-2-194967071622  XX/DK/1234567890 🡪 NULL (Failed: target country is not SE)  XX/SE/#12345-3456//ABC 🡪 12345-3456-abc  XX/SE/aErf#(EAd9) 🡪 0aerf-ead9  XX/SE/aErf#(EAd) 🡪 NULL (Failed: Less than 8 ID characters)  XX/SE/(1952 12 14-1122) 🡪 19521214-1122  19521214-1122 🡪 NULL (Failed: Leading 6 character format error) |

## Algorithm Selection and Resulting pridPersistence Value

This section defines the current algorithm selection rules and the resulting pridPersistence value. These rules are processed in the presented order. The first rule where the present conditions matches all the matching rules is selected.

If the present conditions do not match any of the listed rules, then prid generation fails.

**Rule 1**

|  |  |
| --- | --- |
| Matching rule 1 | Authenticated attributes are provided by an eIDAS node (proxy service). |
| Matching rule 2 | Authenticated subject is a person and has a PersonIdentifier attribute. |
| Matching rule 3 | Attributes provided by any of the countries SE, NO or DK |
| Selected algorithm | default-eIDAS |
| pridPersistence value | A |

**Rule 2**

|  |  |
| --- | --- |
| Matching rule 1 | Authenticated attributes are provided by an eIDAS node (proxy service). |
| Matching rule 2 | Authenticated subject is a person and has a PersonIdentifier attribute. |
| Selected algorithm | default-eIDAS |
| pridPersistence value | C |

# References

[RFC2119]

[Bradner, S., Key words for use in RFCs to Indicate Requirement Levels, March 1997.](http://www.ietf.org/rfc/rfc2119.txt)

[SAML2Core]

[OASIS Standard, Assertions and Protocols for the OASIS Security Assertion Markup Language (SAML) V2.0, March 2005.](http://docs.oasis-open.org/security/saml/v2.0/saml-core-2.0-os.pdf)

[SAML-XSD]

S. Cantor et al., SAML assertions schema. OASIS SSTC, March 2005. Document ID saml-schema-assertion-2.0. See <http://www.oasisopen.org/committees/security/>.

[XML-Schema]

XML Schema Part 2: Datatypes Second Edition, W3C Recommendation, 28 October 2004. See <http://www.w3.org/TR/xmlschema-2/>.

[EidAttributes]

Attribute Specification for the Swedish eID Framework.

[eIDAS\_Attr]

[eIDAS SAML Attribute Profile](https://joinup.ec.europa.eu/sites/default/files/eidas_saml_attribute_profile_v1.0_2.pdf), 22 June 2015.

1. One way to accomplish this is to provide the user with a secret account key that can be used to regain access to the account in the future. Another option is to register an e-mail address to which a restore key will be e-mailed upon request. [↑](#footnote-ref-1)