eduPersonAssurance attribute

22.10.23

Pegasi Knowledge
https://ghost.pegasi.fi/wiki/

Table of Contents

eduPersonAssurance attribute

Overview

Attribute “eduPersonAssurance” is used in federated SAML2 authentication to manage risk that is involved in allowing access to a service provider. Using this attribute the service provider can limit access by the reliability of the identity provider and user account. This article gives a simple explanation and usage example with Shibboleth IDP identity provider.

Roughly put this attribute describes the following properties of the requesting user:

- How certain we are that this login represents this real world user, identifier uniqueness
- How certain we are that this user is who he/she claims to be, identity authenticity
- How certain we are that the attributes of the user are correct and up to date, certainty of attribute data

We also have two named assurance profile attribute values that define all of the above in two different levels: Cappuccino and Espresso. Example follows later.

To assert the values defined in this profile to the RPs the CSPs will use URIs which have the following prefix: $PREFIX$=https://refeds.org/assurance

General criteria

These requirements must be met in all of the cases below. Organization is not allowed to provide assurance data without meeting the requirements stated below.

Refeds requirements according to Refeds Assurance Framework

- The Identity Provider is operated with organizational-level authority
- The Identity Provider is trusted enough that it is (or it could be) used to access the organization’s own systems
- Generally-accepted security practices are applied to the Identity Provider
- Federation metadata is accurate, complete, and includes at least one of the following: support, technical, admin, or security contacts

IGTF general requirements

- Long term commitment on identity providing
- Secure credential processing
- IT systems security
- Credential strength
- Site security

- Auditing
- Privacy and confidentiality

Identifier uniqueness

This describes how certain we are that this login represents this a single natural person.

Uniqueness statements

For uniqueness we have four statements that are used to define the level of uniqueness

- Unique-1 : This login represents a single natural person
- Unique-2 : The identity provider is able to contact this natural person if necessary (phone, email, home address etc)
- Unique-3 : This login is never re-assigned to another party, this login belongs to this person permanently
- Unique-4 : This user has a unique identifier that can be one of the following
    - eduPersonUniqueId
    - SAML 2.0 persistent name identifier (OASIS SAML)
    - Subject-id or pairwise-id (OASIS SIA)
    - OpenID Connect sub: public or pairwise

In addition to the identifiers mentioned in Unique-4, eduPersonPrincipalName (ePPN, [eduPerson]) is a human-readable user identifier whose re-assignment practice is undefined by its specification. To support Relying Parties' use of ePPN, the following extra values are defined to describe a CSP's ePPN practices.

Levels of uniqueness

We have three levels of uniqueness which are defined using the statements above as follows

- $PREFIX$/ID/unique
    - All of the statements from Unique-1 to Unique-4 are fullfilled
    - This login is unique permanently, no other instances of this user from this organization are expected
    - This login is identified by an unique identifier such as national id, persistent id or other similar means
- $PREFIX$/ID/eppn-unique-no-reassign
    - Statements from Unique-1 to Unique-3 are fullfilled for eduPersonPrincipalName value
    - This login is unique permanently, no other instances of this user from this organization are expected
- $PREFIX$/ID/eppn-unique-reassign-1y
    - Statements from Unique-1 to Unique-2 are fullfilled for eduPersonPrincipalName value

    - This login may be reassigned to another natural person after one year of user expiration
    - This login should be removed from service provider system after one year of inactivity
    The expected Relying Party behaviour for observing ePPN re-assignment
- If the CSP asserts eppn-unique-no-reassign, the Relying Party knows that when it observes a given ePPN value it will always belong to the same individual.
- If the CSP asserts eppn-unique-reassign-1y, the Relying Party knows that if an ePPN holder doesn't show up for one year, the ePPN holder may have been changed. A safe practice for the Relying Party is to close a user account or remove the ePPN value associated to it if the user hasn't logged in for one year. The Relying Party can also use some out-of-band mechanism to verify whether the user is still the same person.
- If the CSP asserts neither eppn-unique-no-reassign nor eppn-unique-reassign-1y, the Relying Party cannot rely on ePPN as a unique user identifier but should use it only in combination with another identifier identified in the definition of Unique-4.

Identity authenticity

This describes how certain we are that this user is who he/she claims to be.

Identity authentity statements

- Identity proofing : How well is the user identified by the identity provider
- Credential issuance : How sure we are that the login is given to the right natural person, how mature is the process of producing the login data to the user
- Renewal : How mature is the user login renewal process
- Replacement : How user can get new login to replaced the old / revoked one

Identity authenticity levels

These encapsulate the level of authentity of a user. Please look IGTF and Kantara descriptions below. These values constitute an ordered set of levels with increasing requirements. The CSP asserting a value high MUST also assert (and comply with) the value medium and low for a given user. The CSP asserting a value medium MUST also assert (and comply with) the value low for a given user.

Low

$PREFIX$/IAP/low

- sections 5.1.2-5.1.2.9 and section 5.1.3 of Kantara assurance level 1
    - IGTF level DOGWOOD
    - IGTF level ASPEN

  Examples:

- Self registered login with verified e-mail address, no photo ID nor face check

Medium

$PREFIX$/IAP/medium

- sections 5.2.2-5.2.2.9, section 5.2.2.12 and section 5.2.3 of Kantara assurance level 2
- IGTF level BIRCH
- IGTF level CEDAR
- section 2.1.2, section 2.2.2 and section 2.2.4 of eIDAS assurance level low

Examples:

- Copy of photo ID presented to identity provider organisation with additional remote video conversation

High

$PREFIX$/IAP/high

- section 5.3.2-5.3.2.9, section 5.3.2.12 and 5.3.3 of Kantara assurance level 3
- section 2.1.2, section 2.2.2 and section 2.2.4 of eIDAS assurance level substantial

Examples:

- Face to face conversation, verified genuine photo ID with all possible means to minimize the risk of stolen or invalid document

Local assurances

Organisation may assert following value independent of values above

$PREFIX$/IAP/local-enterprise

Home Organisations may have several internal systems with varying assurance level requirements. It is assumed that the Home Organisation has made a risk based decision on what exactly are the assurance level requirements for those accounts. It is assumed that the Home Organisation's internal systems referred to here could be:

- The ones that deal with money (for instance, travel expense management systems or invoice circulation systems)
- The ones that deal with some employment-related personal data (for instance, employee self-service interfaces provided by the Human Resources systems)
- The ones that deal with student information (for instance, administrative access to the student information system)

Freshness

To assure the freshness of the eduPersonAffiliation, eduPersonScopedAffiliation and eduPersonPrimaryAffiliation attributes the following statements can be used. The freshness of the attribute is further limited to the following attribute values: faculty, student and member. Other values and attributes are out of scope. The values are hierarchical. A CSP which asserts $PREFIX$/ATP/ePA-1d MUST assert also $PREFIX$/ATP/ePA-1m for a given user.

- $PREFIX$/ATP/ePA-1m : attributes are refreshed within 31 days time
- $PREFIX$/ATP/ePA-1d : attributes are refreshed within 1 days time
  This specification imposes no particular requirements on the organisational business practices regarding when the departure takes place. This value is intended to indicate only the maximum latency for the CSP's identity management system to reflect the departure in the user's attributes. Notice also that this section does not require that the departing user's account must be closed; only that the affiliation attribute value as observed by the RPs is updated.

Assurance profiles

There exists two assurance profiles that encapsulate the requirements above into a simple common name. Both individual assurance assertions and all assurance profiles which they qualify should be populated.

Cappuccino

Assurance profile Cappuccino (attribute value $PREFIX$/profile/cappuccino) must contain minimum following assurance attribute values:

- $PREFIX$
- Uniqueness level:$PREFIX$/ID/unique OR $PREFIX$/ID/eppn-unique-no-reassign
- Identity authenticity level: $PREFIX$/IAP/low AND $PREFIX$/IAP/medium
- Attribute quality and freshness level: minimum ePA-1m (Required only if eduPersonAffiliation-attributes are populated and released)

Espresso

Assurance profile Cappuccino (attribute value $PREFIX$/profile/cappuccino) must contain following assurance attribute values:

- $PREFIX$
- Uniqueness level: $PREFIX$/ID/unique OR $PREFIX$/ID/eppn-unique-no-reassign
- Identity authenticity level: $PREFIX$/IAP/low AND $PREFIX$/IAP/medium AND $PREFIX$/IAP/high
- Attribute quality and freshness level: minimum $PREFIX$/ATP/ePA-1m (Required only if

eduPersonAffiliation-attributes are populated and released)

References and examples

eIDAS Assurance levels

Please look at the original article for details

eIDAS Low

1. The person can be assumed to be in possession of evidence recognised by the Member State in which the application for the electronic identity means is being made and representing the claimed identity.
2. The evidence can be assumed to be genuine, or to exist according to an authoritative source and the evidence appears to be valid.
3. It is known by an authoritative source that the claimed identity exists and it may be assumed that the person claiming the identity is one and the same.

eIDAS Substantial

Level low, plus one of the alternatives listed in points 1 to 4 has to be met:

1. The person has been verified to be in possession of evidence recognised by the Member State in which the application for the electronic identity means is being made and representing the claimed identity

   and
   the evidence is checked to determine that it is genuine; or, according to an authoritative source, it is known to exist and relates to a real person
   and
   steps have been taken to minimise the risk that the person's identity is not the claimed identity, taking into account for instance the risk of lost, stolen, suspended, revoked or expired evidence;

   or

2. An identity document is presented during a registration process in the Member State where the document was issued and the document appears to relate to the person presenting it and
   steps have been taken to minimise the risk that the person's identity is not the claimed identity, taking into account for instance the risk of lost, stolen, suspended, revoked or expired documents;
   or
3. Where procedures used previously by a public or private entity in the same Member State for a purpose other than the issuance of electronic identification means provide for an equivalent

assurance to those set out in section 2.1.2 for the assurance level substantial, then the entity responsible for registration need not to repeat those earlier procedures, provided that such equivalent assurance is confirmed by a conformity assessment body referred to in Article 2(13) of Regulation (EC) No 765/2008 of the European Parliament and of the Council (1) or by an equivalent body;

or

4. Where electronic identification means are issued on the basis of a valid notified electronic identification means having the assurance level substantial or high, and taking into account the risks of a change in the person identification data, it is not required to repeat the identity proofing and verification processes. Where the electronic identification means serving as the basis has not been notified, the assurance level substantial or high must be confirmed by a conformity assessment body referred to in Article 2(13) of Regulation (EC) No 765/2008 or by an equivalent body.

eIDAS High

Requirements of either point 1 or 2 have to be met:

1. Level substantial, plus one of the alternatives listed in points (a) to © has to be met: (a) Where the person has been verified to be in possession of photo or biometric identification evidence recognised by the Member State in which the application for the electronic identity means is being made and that evidence represents the claimed identity, the evidence is checked to determine that it is valid according to an authoritative source; and the applicant is identified as the claimed identity through comparison of one or more physical characteristic of the person with an authoritative source; or (b) Where procedures used previously by a public or private entity in the same Member State for a purpose other than the issuance of electronic identification means provide for an equivalent assurance to those set out in section 2.1.2 for the assurance level high, then the entity responsible for registration need not to repeat those earlier procedures, provided that such equivalent assurance is confirmed by a conformity assessment body referred to in Article 2(13) of Regulation (EC) No 765/2008 or by an equivalent body and steps are taken to demonstrate that the results of the earlier procedures remain valid; or © Where electronic identification means are issued on the basis of a valid notified electronic identification means having the assurance level high, and taking into account the risks of a change in the person identification data, it is not required to repeat the identity proofing and verification processes. Where the electronic identification means serving as the basis has not been notified, the assurance level high must be confirmed by a conformity assessment body referred to in Article 2(13) of Regulation (EC) No 765/2008 or by an equivalent body and steps are taken to demonstrate that the results of this previous issuance procedure of a notified electronic identification means remain valid. OR
2. Where the applicant does not present any recognised photo or biometric identification evidence, the very same procedures used at the national level in the Member State of the entity responsible for registration to obtain such recognised photo or biometric identification evidence are applied.

IGTF levels

IGTF levels cut thru organisation to provide requirements for multiple aspects of the identity provider organisation.

Please look at the original article for details.

Base requirements

Base requirements comply with the common sense practises of IT administration and include

- Long term commitment on identity providing
- Secure credential processing
- IT systems security
- Credential strength
- Site security
- Auditing
- Privacy and confidentiality

Aspen

- The natural person behind the login must be recorded and backtraceable up to one year after login expiration
    - For non-person logins the person in charge must be backtraceable by secure means
    - For host or service entries the FQDN must be associated with an owner person who is authorised to register this login
    - Login must be revoked if backtraceability is lost
- Identity provider organisation must have a documented process of identity provisioning and validation
- Login must have a permanent identifier representing the login, such as eppn
    - For non-human accounts the owner permanent identifier must be available
- Password or credential lifetime maximum of one year
- Site security
    - Must not knowingly rely on inaccurate or false data providing third parties involved in identity operations
    - Recommended to use third parties with insident response capability
- Auditing
    - Must have auditable evidence (logs) on retaining the same identity over time
    - Must perform operational audits of the staff and systems involved once a year to verify the compliance to organisation rules
    - Must maintain a list of personnel critical to identity processes
    - Recommended that connected systems (including IDM) self audit regularly with auditable logs

Birch

- The natural person behind the login must be recorded and backtraceable up to one year after login expiration
    - For non-person logins the person in charge must be backtraceable by secure means
    - For host or service entries the FQDN must be associated with an owner person who is authorised to register this login
    - Login must be revoked if backtraceability is lost
    - All issued credentials must be revoked if backtraceability is lost
- The first time identity check should include face-to-face meeting and valid, reliable photo identification documents such as passport id ID card
- Further identifying should be done with one of the following means
    - In person with a trusted agent and reliable photo ID
    - Existing credentials such as username-password, shared secret, TOTP
- Login must have a permanent identifier representing the login, such as eppn
    - For non-human accounts the owner permanent identifier must be available
- Password or credential lifetime
    - Maximum of 400 days if stored in a file protected with a single authentication
    - Without expiration with renewal times of 400 days if using two factor authentication of which one is hardware / biometric based
    - 1200 days without renewal for network and service entities with domain name ownership validated
- Site security
    - Must not knowingly rely on inaccurate or false data providing third parties involved in identity operations
    - Recommended to use third parties with insident response capability
- Auditing
    - Must have auditable evidence (logs) on retaining the same identity over time
    - Must perform operational audits of the staff and systems involved once a year to verify the compliance to organisation rules
    - Must maintain a list of personnel critical to identity processes
    - Recommended that connected systems (including IDM) self audit regularly with auditable logs

Cedar

- The natural person behind the login must be recorded and backtraceable up to one year after login expiration
    - For non-person logins the person in charge must be backtraceable by secure means
    - For host or service entries the FQDN must be associated with an owner person who is authorised to register this login
    - Login must be revoked if backtraceability is lost
    - All issued credentials must be revoked if backtraceability is lost
- The first time identity check should include face-to-face meeting and valid, reliable photo identification documents such as passport id ID card
- Further identifying should be done with one of the following means

    - In person with a trusted agent and reliable photo ID
    - Existing credentials such as username-password, shared secret, TOTP
- Identity provider organisation must keep user initial identifation records for a minimum of two years after login expiration
- Login must have a permanent identifier representing the login, such as eppn
    - For non-human accounts the owner permanent identifier must be available
- Password or credential lifetime
    - Maximum of 400 days if stored in a file protected with a single authentication
    - Without expiration with renewal times of 400 days if using two factor authentication of which one is hardware / biometric based
    - 1200 days without renewal for network and service entities with domain name ownership validated
- Auditing
    - Must have auditable evidence (logs) on retaining the same identity over time
    - Must perform operational audits of the staff and systems involved once a year to verify the compliance to organisation rules
    - Must maintain a list of personnel critical to identity processes
    - Recommended that connected systems (including IDM) self audit regularly with auditable logs

Dogwood

- User login must be unique, it must not be re-allocated to another natural person later
- Permanent, non-public association to natural user
- Backtracing to natural person only with IDP organisation co-operation
    - Login must be revoked if backtraceability is lost
- Recommended to be used with additional stronger (SP based) authentication to proof identity
- Login must have a unique identifier which identifies the source organisation and is backtraceable to the natural person by the issuing organisation
- Password or credential lifetime maximum of 400 days
- Site security
    - Must not knowingly rely on inaccurate or false data providing third parties involved in identity operations
    - Recommended to use third parties with insident response capability
- Auditing
    - Must perform operational audits of the staff and systems involved once a year to verify the compliance to organisation rules
    - Must maintain a list of personnel critical to identity processes

Certainty of attribute data

Kantara used to provided means to measure attribute data reliability but now also includes measurements for other assurance views.

Please also look at the Kantara service assessment documents for details.

Kantara assurance levels

Kantara gives us multiple levels of attribute assurance.

- Level 1 : Little or no confidence in the attribute data
- Level 2 : Some confidence in the attribute data
- Level 3 : High confidence in the attribute data
- Level 4 : Very high confidence in the attribute data

Level One

Minimal confidence on attribute correctness. The attribute data is given by an individual without release of data is given back. Examples: payment transactions, web forms, self registered ID based operations.

No cryptographic methods required. Use this level if faulty data does not result in negative outcome.

5.1.1 Credential Operating Environment

- Password entropy minimum of 14 bits
- Repeated authentication attempts must be handled with a temporary login disable, timeout or similar
- Consider and assess potential security threats
- Organization must prepare for following threats
    - Malicious code injects
    - Human security threats, revealed / paper written passwords or similar
    - Out of band attacks
    - Password spoofing trojans or similar
- Limiting access to stored administrational passwords
    - Only active administration people
    - Encrypted storage such as Keepass
    - No plaintext passwords sent over unsecured or public networks

5.1.2 Credential issuing

- Identity must be proofed on credential delivery and evidence must exist of this
- Identity must be verified with
    - In-person proofing using valid photo ID
    - Remote identity verification using telephone number or email
- Further use with organization credentials
- On suspicious activities the organization must do additional verification of identity and halt completion while verification not finished
- Keep records of identity proofing
- Provide means for user to update user-definable attribute data, such as personal email address
- Create credentials only when user identity is proofed
- Login must be unique and may be selectable by user

- Provide this unique login information to service providers
- AUthentication must be used from one of the following methods
    - If password is used, the entropy must be minimum of 14 bits
    - If challenge-response questions are use they must be created by user, answers must not be null
    - If challenge-response questions are not created by user they must be selected from a list of at least five questions, answers must not be null

5.1.3 Credential renewal

- Password change must be allowed using old password or other authentication to proof their identity

5.1.4 Credential revocation

- Credential revocation must be done over a secured communication

5.1.5 Credential status management

- Organization must have valid status information of logins
- Status information availability must be 95%

5.1.6 Credential verification / authentication

- Identity provider must service service providers with authentication and identity assertion which is protected from hacking
- Each identity assertion must be signed and unique to a single transaction
- Identity provider must deny revoked logins
- Identity provider must limit failed authentication a
- Limit failed authentication attempts to maximum of 100 in any 30 day period
- Expire assertions
    - In 12 hours for users coming from address that is within same internet domain
    - In 5 minutes for users coming from address that is outside internet domain
- Assurance attribute describes the initial authentication of the user
- Identity assertion requirement is one of the following
    - Assertion is signed
    - Assertion is encrypted using a shared secret key
    - Assertion has min 64 bits entropy
    - Assertion is sent over a protected, mutually authenticated session

Level Two

Some confidence on attribute correctness. Some risk involved with faulty data.

Single factor authentication is recommended. Gotchas or similar are required to prevent spamming / guessing.

5.2.1 Credential Operating Environment

- Password entropy minimum of 14 bits
- Repeated authentication attempts must be handled with a temporary login disable, timeout or similar
- Consider and assess potential security threats
- Organization must prepare for following threats
    - Malicious code injects
    - Human security threats, revealed / paper written passwords or similar
    - Out of band attacks
    - Password spoofing trojans or similar
- Limiting access to stored administrational passwords
    - Only active administration people
    - Encrypted storage such as Keepass
    - No plaintext passwords sent over unsecured or public networks

5.2.2 Credential issuing

- Identity must be proofed on credential delivery and evidence must exist of this
- Identity must be verified with
    - In-person proofing using valid photo ID
    - Remote identity verification using telephone number or email
- Further use with organization credentials
- On suspicious activities the organization must do additional verification of identity and halt completion while verification not finished
- Keep records of identity proofing
- Provide means for user to update user-definable attribute data, such as personal email address
- Create credentials only when user identity is proofed
- Login must be unique and may be selectable by user
- Provide this unique login information to service providers
- AUthentication must be used from one of the following methods
    - If password is used, the entropy must be minimum of 14 bits
    - If challenge-response questions are use they must be created by user, answers must not be null
    - If challenge-response questions are not created by user they must be selected from a list of at least five questions, answers must not be null

5.2.3 Credential renewal

- Password change must be allowed using old password or other authentication to proof their identity

5.2.4 Credential revocation

- Credential revocation must be done over a secured communication

5.2.5 Credential status management

- Organization must have valid status information of logins
- Status information availability must be 95%

5.2.6 Credential verification / authentication

- Identity provider must service service providers with authentication and identity assertion which is protected from hacking
- Each identity assertion must be signed and unique to a single transaction
- Identity provider must deny revoked logins
- Identity provider must limit failed authentication a
- Limit failed authentication attempts to maximum of 100 in any 30 day period
- Expire assertions
    - In 12 hours for users coming from address that is within same internet domain
    - In 5 minutes for users coming from address that is outside internet domain
- Assurance attribute describes the initial authentication of the user
- Identity assertion requirement is one of the following
    - Assertion is signed
    - Assertion is encrypted using a shared secret key
    - Assertion has min 64 bits entropy
    - Assertion is sent over a protected, mutually authenticated session

Level Three

High confidence on attribute correctness. Substantial risk involved with faulty data.

Multi factor authentication is required. Identity proofing require photographic ID / passport / similar verification. Authentication must be based on a password or a key though a cryptographic protocol. Usage of soft-, hard- or OTP device tokens.

Level Four

Very high confidence on attribute correctness. Critical risk involved with faulty data.

Multi factor authentication is required. Identity proofing require photographic ID / passport / similar verification. Authentication must be based on a password or a key though a cryptographic protocol using hardware device tokens. High levels of cryptographic assurance required for all elements of credential and token management.

Shibboleth IDP V4 static example

A medium level university example added to attribute-resolver.xml (source HAKA federation).

```
<AttributeDefinition xsi:type="Simple" id="eduPersonAssurance">
    <InputDataConnector ref="staticAttributes" allAttributes="true" />
```

```
</AttributeDefinition>


<DataConnector id="staticAttributes" xsi:type="Static">
    <Attribute id="eduPersonAssurance">
<Value>https://refeds.org/assurance/ID/eppn-unique-no-reassign</Value>
        <Value>https://refeds.org/assurance/ATP/ePA-1m</Value>
        <Value>https://refeds.org/assurance/IAP/medium</Value>
        <Value>https://refeds.org/assurance/IAP/low</Value>
        <Value>https://refeds.org/assurance</Value>
        <Value>https://refeds.org/assurance/profile/cappuccino</Value>
    </Attribute>
</DataConnector>
```

Comments

All comments and corrections are welcome.