Creation Date: 2022/02/20
Update: 2022/02/21

Necessity of Validated Attribute Expressions in Academic Accreditation and Draft Technical Specifications

ITOCHU Techno-Solutions Corporation
OpenID Foundation eKYC-IDA WG
OpenID Foundation Japan
Naohiro Fujie

The following is a draft specification of a validated attribute expression to be issued by the Identity Provider of the next generation of academic accreditation participants.

1. The Need for Validated Attribute Representation in the Academic Trust Framework
   The necessity of adding a state of verification regarding identity information that is passed across institutions to constitute an accreditation trust framework is discussed in light of the current status of the accreditation trust framework and the state of trust in other domains.

   (ア) Current status of entities and trust related to academic accreditation
   Organize relevant entities/terms based on the definitions in ISO/IEC 24760-1:2019.
   Table Organization of related entities/terms (ISO/IEC 24760-1:2019)

Entity/Terminology	Description.	Examples of entities in the context of academic accreditation
IIA: Identity Information Authority	Provide assurance of authenticity and accuracy of attributes Entity related to a particular domain that can make provable statements on the validity and/or correctness of one or more attribute values in an identity.	Student affairs/human resources departments at universities and institutions
IIP/IdP: Identity	Provide identity information (often the same entity as the IIA).	Accreditation infrastructure for

Information Provider/ Identity Provider	Entity that makes available identity information.	universities and institutions
Credential	Identity used for authentication Representation of identity for use in authentication.	Student ID, password, etc.
Verifier	An entity that performs Verification, the process of establishing that the identity information associated with a particular entity is accurate Entity that performs verification.	Accreditation infrastructure for universities and institutions
Relying party/RP	Entities that rely on Verification of identity information about a particular entity Entity that relies on the verification of identity information for a particular entity.	Accreditation infrastructure for universities and institutions /Applications

The related entities are shown in the figure below when applied to accreditation-related institutions (e.g., universities/institutions).

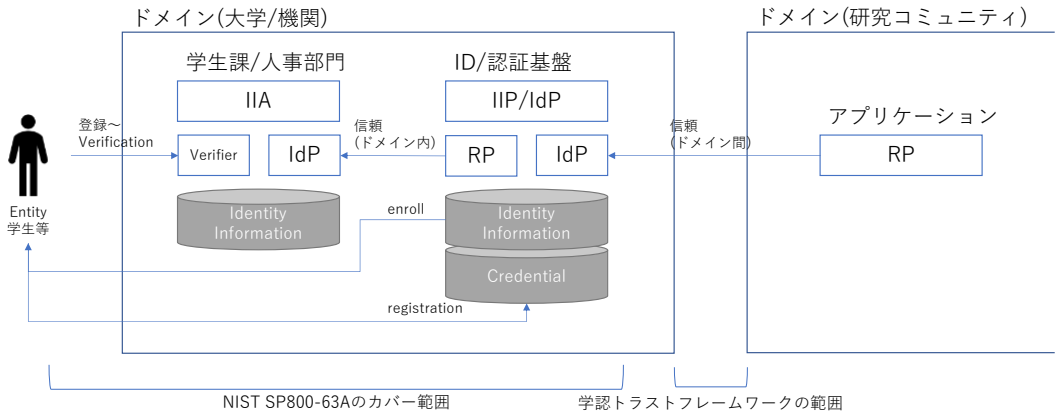


Figure Entity Relationships in Accreditation-Related Organizations

（イ）Scope of the Academic Accreditation Trust Framework

Scope is the trust relationship between RP-IIP/IdP across domains.

However, in order to trust the IIP/IdP beyond the domain, the RP needs to explicitly ask the IIP/IdP what kind of In order for RPs to trust the IIP/IdP, they need to explicitly ask

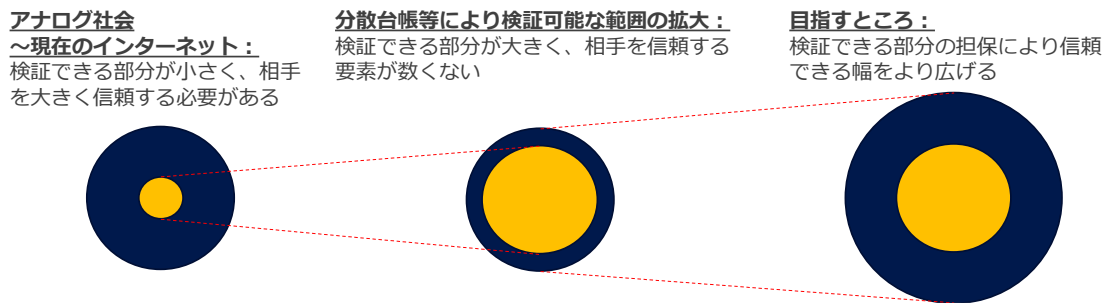
the IIP/IdP what Identity Information provided by the IIP/IdP was registered through the Verification process by the IIA.

（ウ）Change in trust model

In the traditional trust framework, by placing comprehensive trust in the trust framework, RPs have implicitly placed their trust[1] in the participating (accredited) institutions of the framework without conducting their own verification.

However, in conventional academic accreditation, it has been difficult to respond to individual requirements of RPs in order to achieve scalability, and only a broad and shallow level of requirements has been realized. As a result, each research community had to individually obtain information from IIA and perform Verify.

In order for the research community to collaborate not only with accreditation participating organizations but also with private companies in the future, in addition to the implicit trust in the existing trust framework, it is necessary to enable RPs to obtain information on the verification process performed by the IIA when registering the Identity Information provided by the IIP/IdP, and to verify it themselves. In addition to the implicit trust in the existing trust framework, it is necessary to enable RPs to obtain information on the verification process performed by the IIA at the time of registration of Identity Information provided by the IIP/IdP and to perform verification themselves.



Extension of trust by expanding the verifiable range (Additions made to the Trusted Web Promotion Council, Cabinet Secretariat document)

2. Attribute expressions for expressing trustworthiness in conventional SAML

---

[1] Degree of belief that the other party will behave as expected without confirmation of facts (from the definition by the Cabinet Secretariat/Trusted Web Promotion Council).

AuthnContextClassRef[2] is a specification for representing the authentication context in SAML Assertion.
The SAML IdP can request support for the authentication strength specified to the SAML IdP by the SAML IdP.
e.g.) Request authentication from SAML SP using at least Password

```
< AuthnRequest ...>
  < RequestedAuthnContext Comparison="minimum" ...>
    < AuthnContextClassRef [omitted] >
      urn:oasis:names:tc:SAML:2.0:ac:classes:PasswordProtectedTransport
    </AuthnContextClassRef>
  </RequestedAuthnContext>
</AuthnRequest>
```

However, the following problems exist in the use of AuthnContextClassRef.

- It can only define information on authentication methods, and cannot express the Identity Proofing strength level (SP800-63A) and authentication strength level (SP800-63B) defined in NIST SP800-63 in a three-dimensional manner.
- Many existing SAML SP implementations accept a fixed PasswordTransport, and setting other values could result in disruptive changes to existing systems.

Therefore, this document proposes an attribute representation to express identity assurance level and authentication strength by extending the schema of SAML Assertion. As for the level of identity assurance, one or more of the items (a) through (c) in Section 3 of this document can be included in the Assertion and sent. This is compatible with the method of expression of Verified Claims/Authority Claims in the prior example, OpenID Connect for Identity Assurance[3], to enable smooth replacement of the Verified Claims/Authority Claims when IdPs of each organization respond to OpenID Connect in the future. This will enable smooth replacement of the Verified Claims/Authority Claims when each organization's IdPs support OpenID Connect. In consideration of the fact that there may be use cases where verified and unverified attributes are mixed, "Verified_" will be added as a prefix to verified attributes.
In addition, it is possible to include one or more of (a) through (b) described later in Section 4 of this document regarding authentication strength in the Assertion.

---

[2] http://docs.oasis-open.org/security/saml/v2.0/saml-authn-context-2.0-os.pdf

[3] https://openid.net/specs/openid-connect-4-identity-assurance-1_0-ID3.html

(Attribute Value is a serialized JSON to be represented as a SAML Assertion)

3. Proposed attribute expressions for expressing trustworthiness regarding identity assurance

（ア）Representation of identity assurance level with trust framework

Represents the level of trustworthiness defined by a particular trust framework.

Since eduPersonAssurance[4] is used in academic certification as an attribute to express the level of assurance, the relationship with this expression should be discussed.

Example) Example of expressing IAL: 2 in the Acceptable Trust Framework (Value is expressed as JSON for notational clarity, but is actually Stringify)

```
< Attribute Name="AssuranceDefinitions">
  < AttributeValue>.
  {
    "trust_framework": "nii_gakunin_ial_2022",
    "assurance_level": "2"
  }
  </AttributeValue>
< /Attribute>
<Attribute Name="Verified_displayName">
  < AttributeValue>.
    licensed scholar
  </AttributeValue>
< /Attribute>
```

（イ）Representation of attribute information about the Verification process

Expresses the details of Verification (Identity Proofing) performed by Verifier.

- Laws, regulations and rules applied
- Evidence used
- Evidence Validation
- Means of Verification of the identity of the evidence and the presenting entity (Applicant)
- Date and time each process was executed
- entity that executed each process

[4] https://meatwiki.nii.ac.jp/confluence/display/GakuNinShibInstall/eduPersonAssurance

Example) An example of expressing the fact that face-to-face identity verification was conducted using a driver's license in accordance with Gakusho standards (Value is expressed as JSON for notational clarity, but in reality it is a String)

```
< Attribute Name="AssuranceDefinitions">
  < AttributeValue>.
  {
    "trust_framework": "nii_gakunin_ial_2022",
    "assurance_level": "2",
    "evidence": [
      {
        "type": "document",
        "validation_method": {
          {
            "type": "pipp",
            "time": "2022-02-22T00:00:00Z",
            "entity": "school office"
          }
        },
        "verification_method": {
          {
            "type": "pipp",
            "time": "2022-02-22T00:00:00Z",
            "entity": "school office"
          }
        },
        "document_details": {
          "type": "driving_permit",
          "document_number": "0000000000000000",
          "date_of_issuance": "2021-01-01",
          "date_of_expiry": "2025-12-31",
          "issuer": {
            "name": "Minato Police Office",
            "country": "Japan"
          }
        }
      }
```

```
    ]
  }
  </AttributeValue>
< /Attribute>
<Attribute Name="Verified_displayName">
  < AttributeValue>.
    licensed scholar
  </AttributeValue>
< /Attribute>
```

(ウ) Expression of attribute information regarding affiliation with the institution in question

Whereas (a) expresses about identification, the following attributes are used to express affiliation with an institution.

- Name of Institution
- Corporate ID number of the organization you belong to
- Role of the entity in the organization to which the entity belongs
- Role Duration
- Entity to which the role is assigned and how it is assigned

Example) An example of expressing that the individual in question belongs to a university in accordance with the criteria for academic recognition (Value is expressed as JSON for notational clarity, but is actually a String).

```
< Attribute Name="AssuranceDefinitions">
  < AttributeValue>.
  {
    "trust_framework": "nii_gakunin_ial_2022",
    "assurance_level": "2",
    "authority": [{
      "applies_to": {
        "organization_name": "Kyoto-University",
        "organization_number": "9999999"
      },
      "permission": [{
        "role": "Student",
        "validity": [{
          "start": "2021-04-01T00:00:00Z"
```

```
          }]
        }],
        "granted_by": {
          "method": "examination",
          "granting_body": "admission_office",
          "reason": "pass the exam"
        }
      }]
  }
  </AttributeValue>
< /Attribute>
<Attribute Name="Verified_displayName">
  < AttributeValue>.
    licensed scholar
  </AttributeValue>
< /Attribute>
```

The detailed specification (draft) for attribute expressions for expressing reliability is as follows

Table) List of Attribute Expressions

category	Claim Name	meaning
framework	Trust_framework	Applicable laws and rules (trust framework)
confidence level	Assurance_level	Trust Levels in the Trust_framework
Evidence at the time of identification	Evidence	Information on evidence used
	Type	Type of evidence
	Validation_method	Information on authenticity verification of evidence
	Type	Methods used for authenticity verification (e.g.) pipp: face-to-face confirmation/physical in person proofing
	Time	Date and time of

		verification
	Entity	Verified Entities
	Verification_method	Information on evidence and bearer identity verification
	Type	Methods used for identity verification (e.g.) pipp: face-to-face confirmation/physical in person proofing
	Time	Date and time of verification
	Entity	Verified Entities
	Document_details	Information about the details of the evidence document
	Type	Type of evidence
	Document_number	Document number of evidence
	Date_of_issuance	Date of Evidence Issued
	Date_of_expiry	Evidence Expiration Date
	Issuer	Information related to the issuer of the evidence
	Name	Name of Evidence Publisher
	Country	Evidence issuing country
Institutional Affiliation	Authority	Authority Information
	Applies_to	Information on Applicable Customers
	Organization_name	organization name
	Organization_number	Organization number (corporate number, etc.)
	Permission	Information on roles within the organization
	role	Role within the

		organization
	Validity	Information on role expiration dates
	Start/End	Start/End Date
	Granted_by	Information sensitized to the entity to which the role is assigned
	Method	method of grant
	Granting_body	Granted Entity
	reason	Reason for granting

4. Proposal of attribute expressions to express confidence regarding authentication strength

(ア) Trust framework representation of authentication strength

Represents the level of trustworthiness defined by a particular trust framework.

Example) Example of expressing AAL: 2 of the Academic Authorization and Trust Framework (Value is expressed as JSON for notational clarity, but is actually Stringify)

```
< Attribute Name="AssuranceDefinitions">
  < AttributeValue>.
  {
    "trust_framework": "nii_gakunin_aal_2022",
    "assurance_level": "2"
  }
  </AttributeValue>
< /Attribute>
```

(イ) Expression of information about the authentication method actually used

Expresses details of the method of entity authentication in IIP/IdP.

- Authenticator used (arrayed to represent multi-factor authentication)

Example) Example of authentication using a hardware token in addition to a password (Value is represented as JSON for clarity in notation, but is actually a String)

```
< Attribute Name="AssuranceDefinitions">
  < AttributeValue>.
  {
    "trust_framework": "nii_gakunin_aal_2022",
```

```
    "assurance_level": "2",
    "authenticators": [
      {
        "type": "password",
        "level": "2",
        "enroll_date": "2020-04-01T00:00:00Z"
      },
      {
        "type": "hardware_token",
        "level": "2",
        "enroll_date": "2021-10-01T00:00:00Z"
      }
    ]
  }
  </AttributeValue>
< /Attribute>
```

The detailed specification (draft) for attribute expressions for expressing reliability is as follows

Table) List of Attribute Expressions

category	Claim Name	meaning
framework	Trust_framework	Applicable laws and rules (trust framework)
confidence level	Assurance_level	Trust Levels in the Trust_framework
authentication device	Authentication	Information about certifiers
	Type	Type of certifier
	Level	Certifier strength
	Enroll_date	Enrolled date and time

5. Correspondence between each assurance level and detailed attribute expressions in the Academic Trust Framework

The correspondence between each assurance level in the Academic Accreditation Trust Framework and the attribute expressions shown in Sections 3-4 shall be as follows

Table) Correspondence between each assurance level and attribute expression

category	level	attribute	value

		representation		
ID assurance level	1	Evidence	Type	student card **employee ID card** driver's license personal identification number card
			date	within the validity period
			Issuer	Organization issuing authority
		Validation method	Type	remote
			Time	Within 3 months
			Entity	Certified Administrator
		Verification method	Type	remote
			Time	Within 3 months
			Entity	Certified Administrator
		Authority	Applies_to	Accredited Institutions
			Permission	within the validity period
			Granted_by	N/A
	2	Evidence	Type	student card **employee ID card** driver's license personal identification number card GBIZ ID
			date	within the validity period
			Issuer	Organization issuing authority
		Validation method	Type	remote

			Time	Within 3 months
			Entity	Certified Administrator
		Verification method	Type	remote
			Time	Within 3 months
			Entity	Certified Administrator
		Authority	Applies_to	Accredited Institutions
			Permission	within the validity period
			Granted_by	N/A
	3	Evidence	Type	student card **employee ID card** driver's license personal identification number card GBIZ ID
			date	within the validity period
			Issuer	Institution issuing authority
		Validation method	Type	remote
			Time	Within 3 months
			Entity	Certified Administrator
		Verification method	Type	remote
			Time	Within 3 months
			Entity	Certified Administrator
		Authority	Applies_to	Accredited Institutions
			Permission	within the validity period

			Granted_by	N/A
Authentication Strength	1	Authenticator	Type	Password
			Level	1 (no complexity requirement)
			Enroll_date	N/A
			Number of array elements	1
	2	Authenticator	Type	Password SW Token
			Level	2 (with complexity requirement)
			Enroll_date	N/A
			Number of array elements	2 or more
	3	Authenticator	Type	Password HW Token
			Level	2 (with complexity requirement)
			Enroll_date	Within 6 months
			Number of array elements	2 or more

6. Proposal for implementation model

   Since there may be cases where it is difficult for IIP/IdPs in each institution to actually implement the attribute expressions proposed in this document, we propose the following two methods as implementation models.

   1. Method in which IIP/IdP directly performs attribute representation

      The IIP/IdP of each organization sends the attribute expressions regarding the assurance level proposed in this document directly to the RP as a SAML Assertion.

   2. A method in which an authentication proxy such as Orthros works with the IIA to represent attributes on behalf of the IIA.

      By placing an Authentication Proxy system between the IIP/IdP of each organization and the RP, the Authentication Proxy sends attribute expressions related to the

assurance level on behalf of the IIP/IdP of each organization. In this case, it is assumed that an implicit trust relationship is established between the Authentication Proxy and the IIP/IdP of each organization.

Table) Comparison of methods in cases where RPs can receive detailed attribute expressions

	Method 1	Method 2
Sender of detailed attributes	IIP/IdP for each institution	Authentication Proxy
Trust relationship between RP-IIP/IdP	Directly trust (Verifiable trust relationship)	Establish an implicit trust relationship between the Authentication Proxy and each agency's IIP/IdP

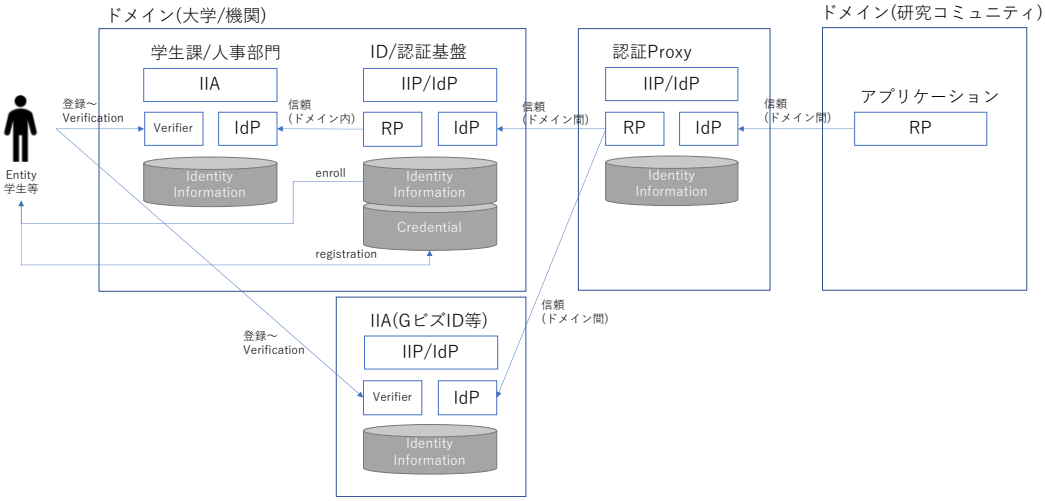


Figure) Image of the implementation model

In addition to cases where the IIP/IdP side of each institution is difficult to implement, there may also be cases where it is difficult for the RP side to implement the detailed attribute expressions for interpretation and verification. In such cases, the above two implementation methods can also solve the problem.

1. Method in which IIP/IdP directly performs attribute representation
   Each RP interprets the detailed attribute expressions sent out by each agency and verifies that they match the required level of assurance.
2. A method in which an authentication proxy such as Orthros works with the IIA to represent attributes on behalf of the IIA.

The authentication proxy system verifies the ID assurance level and authentication strength on behalf of the RPs based on information obtained from each IIP/IdP or separately from the IIA, and sends only a normal SAML Assertion to the RPs. In this case, it is assumed that an implicit trust relationship has been established between each RP and the authentication proxy.

Table) Comparison of methods in cases where RPs cannot receive detailed attribute expressions

	Method 1	Method 2
Interpretation and verification of detailed attributes	each RP	Authentication Proxy
Trust relationship between RP-IIP/IdP	Directly trust (Verifiable trust relationship)	Establish an implicit trust relationship between the RP and the Authentication Proxy