22-02-2022

The Working Group for Next-Generation Identity Federation

Based on feedback, some wording was revised, and further comments were added.

20-10-2021

The Working Group for Next-Generation Identity Federation

Draft Proposal for Examples of CrP/CrPS

This document provides examples of CrP/CrPS for cases 1.1 and 1.2 in the separate document respectively. In addition, it provides examples of the CrP/CrPS as part of 1.2 in the case where IDaaS conducts identity proofing equivalent to IAL2.

The following is the case where handling only accounts that are directly connected to the Trusted DB.

Credential Policy (CrP)

1. About this document

    This document describes the credential policy of the IdP operated by XX University.

    1.1 The URL of the IdP is XX and issues authentication assertions to the following RPs:

        A. Services within the University

        B. GakuNin

        C. Services operated by Inter-University Research Institute Corporations approved by the University

        D. Other services specifically approved by the University

    1.2 This document does not obtain a Document ID.

2. Scope of this document

    This document provides information for determining the assurance level for identity proofing when providing authentication assertions for service providers participating in 1.1.B and 1.1.C.

3. Accounts subject to this document

    3.1 Accounts

        This document applies to the assurance level for identity proofing for the campus-wide common ID provided by the University.

    3.2 Attributes bound to Accounts

        Among the attributes that are bound to an account as defined in 3.1, the assurance level for the following shall be operated at the same level as the assurance level for identity proofing.

        A. Organization (○○)

B. CommonName

C. eduPersonPrincipalName

D. eduPersonAffiliation (student/staff/faculty)

E. mail

Of the above, it is guaranteed that the eduPersonPrincipalName matches the University's campus-wide common ID.

4. Method of identity proofing for accounts

The IdP generates accounts by obtaining information directly from the University's student information operated by the University's academic affairs system or from the University's faculty/staff information operated by the human resources system.

4.1 Scope of users to whom each method is applicable

A. Among the user accounts, those with the "student" attribute as eduPersonAffiliation are guaranteed to comply with the registration procedures of the academic affairs system.

B. Among the user accounts, those with the "staff" or "faculty" attribute as eduPersonAffiliation are guaranteed to comply with the registration procedures of the human resources system.

Credential Practices Statement (CrPS)

1. About this document

This document sets out specific implementation guidelines for the IdP's CrP.

2. Scope of this document

This document describes specific methods of identity proofing during account generation.

3. Specific method of identity proofing for accounts

A. Registration to the academic affairs system is conducted following the admission process of the University, which begins with the application for admission. In practice, this is done in accordance with the relevant regulations of the University and the guidance of the Ministry of Education, Culture, Sports, Science and Technology (MEXT).

B. Registration to the human resources system is conducted following the University's recruitment procedures for faculty and staff. In practice, this is done in accordance with the relevant regulations of the University.

3.1 Procedures in case of unsuccessful identity proofing

If the identity proofing is not successful and account information cannot be obtained from the academic affairs system or human resources system, the IdP shall not create an account for such person under any circumstances.

4. Consideration for privacy

A. The IdP shall operate in accordance with the principle of minimum in handling personal information.

B. The IdP shall notify the user in advance of how the attributes will be used. In particular, the consent process should be provided to users when attributes are provided to service providers outside the university.

5. Security measures

The IdP shall take all possible measures to ensure security.

6. Procedures at the termination of service

When the IdP terminates services, any personal information retained shall be completely destroyed and disposed of in a manner that prevents access at a later date.

The following is the case where collecting user information, creating accounts and providing services on its own. In cases where an Inter-University Research Institute Corporation operates its own IdP, or IDaaS issues accounts to organisations or individuals that are not part of an existing Trust

Credential Policy (CrP)

1. About this document

   This document describes the credential policy of the IdP for jointly-used services operated by the XX Research Institute.

   1.1 The URL of the IdP is XX and issues authentication assertions to the following RPs:

   A. Services within the Institute

   B. GakuNin

   C. Identity services for the Institute to provide services as an Inter-University Research Institute Corporation

   D. Other services specifically approved by the Institute

   1.2 This document does not obtain a Document ID.

2. Scope of this document

   This document provides information for determining the assurance level for identity proofing when providing authentication assertions for service providers participating in 1.1.C.

3. Accounts subject to this document

   3.1 Accounts

   This document applies to the assurance level for identity proofing for the entire accounts provided by the Institute

   3.2 Attributes bound to Accounts

   Among the attributes that are bound to an account as defined in 3.1, the assurance level for the following shall be operated at the same level as the assurance level for identity proofing.

   A. Organization; except for those given Others as the “OU” attribute

   B. CommonName

   C. eduPersonPrincipalName

   D. eduPersonAffiliation

   E. mail

4. Method of identity proofing for accounts

   The IdP generates accounts by obtaining information directly from the Institute’s student information operated by the Institute’s academic affairs system or from the Institute’s faculty/staff information operated by the human resources system, or by other equivalent means. The IdP may also issue accounts to persons who do not belong to the Institute.

4.1 Scope of users to whom each method is applicable

A. Among the user accounts, those with the “student” attribute as eduPersonAffiliation are guaranteed to be affiliated with the Institute and to comply with the registration procedures of the academic affairs systems of the universities participating in GakuNin.

B. Among the user accounts, those with the “staff” or “faculty” attribute as eduPersonAffiliation are guaranteed to comply with the registration procedures of the human resources system.

C. For accounts issued to persons who do not belong to the Institute, the “member” attribute shall be issued as eduPersonAffiliation. For those who are not registered in the academic affairs system or human resources system of this Institute, the method specified in 5. shall be applied.

5. Issuance of accounts to persons who are not affiliated with the Institute

A. The Institute shall request the submission of evidence as prescribed by the Institute and, if necessary, endorsement documents from staff designated by the Institute.

B. For verification of identity, one of the following shall be performed:

a. In-person interview by a designated staff member

b. Remote interview with adequate communication quality assured. In this case, as necessary, a recording shall be retained as a record of the interview for audit purposes.

c. The verification of identity shall not be conducted by document screening alone without a. and b.

C. Set out and operate procedures for address verification

a. The addresses given in evidence shall be trusted

b. Mobile phone numbers shall be verified via a call over the phone, either in person or via a remote interview

c. Landline phone numbers shall be verified via a call to the representative number of affiliated organisations.

d. E-mail addresses shall not be treated as reliable during the identity proofing process.

D. For JSPS Research Fellows, it is assumed that they have undergone the same identity proofing as the Institute’s employees at the time of their employment at JSPS, and thus the above rules A.-C. shall not be applied.

E. For those who have been granted status at the Institute through the exchange program operated by the Institute, the following shall be performed:

a. Undergo the same identity proofing as the Institute's employees at the time of acceptance.

b. Satisfy the import restrictions, etc. set out by the government.

Credential Practices Statement (CrPS)

1. About this document

This document sets out specific implementation guidelines for the IdP's CrP.

2. Scope of this document

This document describes specific methods of identity proofing during account generation.

3. Specific method of identity proofing for accounts

A. In the case of issuing "student" attribute as eduPersonAffiliation, it is determined, based on the documents provided by the university and GakuNin, that registration to the academic affairs system of the university, which is in partnership with the Institute and is participating in GakuNin, is conducted following the university's admission process, which begins with the application for admission.

B. In the case of issuing a "staff" or "faculty" as edupersonAffiliation, the registration to the human resources system is conducted following the Institute's recruitment procedures for faculty and staff. In practice, this is done in accordance with the relevant regulations of the Institute.

C. For the identity proofing of persons who are not affiliated with the Institute, the following will be conducted.

a. Upon identity proofing, the applicant shall be required to present the following evidence:

1. Two copies of a photo ID issued by a public sector organisation, such as a passport, driver's license, or my number card; or

2. One copy of a photo ID issued by a public sector organisation and two endorsement documents from two or more Institute employees designated by the Institute, respectively; or

3. One copy of the assertion authenticated at AAL2 or higher by a research institution that is participating in GakuNin and accredited as IAL2 or higher. The attribute value that the issuing IdP has certified as IAL2 or higher shall be accepted; or

4. An employee identification card with a photograph issued by the applicant's company may be submitted. In screening for identity proofing, it may be acceptable as having a certain level of evidence.

5. The submitted evidence may be retained for a specified period of time to

ensure the uniqueness of the applicant, and may be used to determine whether the same applicant has applied in the past.

6. The account created following the screening process shall be deactivated after a certain period of time, or when the Institute determines that the person's social status has changed, and an account shall be given to the person again after another screening. The continuity with the deactivated account shall not be guaranteed.

7. The submitted evidence shall be stored in the Institute to ensure the uniqueness of the applicant, with the necessary security measures. If the account in question is deleted, the evidence shall be deleted.

b. The validation of the submitted evidence shall be performed by a designated staff member of the Institute. The position of the staff member shall be disclosed in advance.

c. The verification of evidence shall be conducted through a procedure that includes confirmation of match between the person and the photograph presented in the evidence, either in person or during a remote interview.

3.1 Procedures in case of unsuccessful identity proofing

A. If the identity proofing is not successful for an employee belonging to the Institute or a student of an affiliated university, the IdP shall not create an account for such person under any circumstances.

B. If the identity proofing is not successful for a person not belonging to the Institute, and a complaint is filed with the Institute's designated Complaint Committee within two weeks, the validity of the identity proofing shall be reviewed, and the person concerned shall be notified of the outcome. No complaint shall be accepted more than twice within a consecutive six-month period.

4. Consideration for privacy

A. The IdP shall operate in accordance with the principle of minimum in handling personal information.

B. The IdP shall notify the user in advance of how the attributes will be used. In particular, the consent process should be provided to users when attributes are provided to service providers outside the university.

5. Security measures

The IdP shall take all possible measures to ensure security.

6. Records

All procedures performed for identity proofing shall be recorded and retained until the termination of services, unless otherwise specified.

7. Procedures at the termination of service

When the IdP terminates services, any personal information retained shall be completely destroyed and disposed of in a manner that prevents access at a later date.