19-04-2022

The Working Group for Next-Generation Identity Federation

Draft for the Operation of IAL2 in the New GakuNin

This version of the document reflects comments received in response to the “Draft for the Operation of IAL2 in the New GakuNin”, which was published on 20 October 2021 and on which feedback was collected from various sources. No changes were made to the Preface. No changes were made to the text of the rules. Examples, however, were added to increase transparency of the accreditation process, and these sections were used to reflect the comments. These are intended to be used as guidelines.

The Working Group for Next-Generation Identity Federation aims to build and operate a large-scale trust framework by creating standards for authentication strength and inviting universities and research institutions and research communities to participate in the authentication collaboration so that it can support authentication for access to services that handle information that requires careful handling both inside and outside the university and access to services for which strong security is a prerequisite such as information and computational resources held by various research communities in Japan and abroad. In order to achieve this, it is essential to establish and implement standards for the Identity Assurance Level (IAL), an assurance level for identity proofing, and the Authentication Assurance Level (AAL), an assurance level for authentication. The Working Group is to develop standards that are operable by participating institutions and that can be agreed upon internationally.

In the authentication industry, the U.S. NIST standards and Kantara, one of its operating organisations, are always mentioned as the baseline for this type of discussions. GakuNin has been operating with a basic level of assurance by developing and implementing Operating Policies and System Administration Standards. In fact, GakuNin has made the accreditation of LoA1, the basic assurance level, operational within GakuNin by participating in Kantara.

In response to the needs to implement the higher standards of IAL2 and AAL2, this document provides the following observations and proposed policies related to the development of standards for the operation of IAL2 in the new GakuNin, specifically in accordance with NIST SP800-63 and Kantara KIAF1430. The contents are as follows:

1. Universities' internal definition of CSP and the subsequent replacement policy for re-interpreting NIST/KIAF
2. Differentiating what is defined within the operational scope of the CSP from what is related to higher-level university administration
3. General provisions for CSP operations
4. General security
5. Templates for CrP/CrPS
6. Standards for identity proofing to achieve IAL2
7. Accreditation, operation and auditing system by the GakuNin Trust WG
8. Contact details for comments and inquiries regarding this document

We are preparing a survey of the current situation as we begin the process of establishing the AAL2. We would appreciate your cooperation in this regard as well.

1. Universities' internal definition of CSP and the subsequent replacement policy for re-interpreting NIST/KIAF

In the model of the NIST and KIAF documents, what was previously called an IdP is called a Credential Service Provider (CSP), and its rules cover services that issue credentials such as passwords and client certificates to users. In their model, the Verifier is responsible for verifying the credentials and issuing assertions to the RP (SP). IdPs, as in our case, generally have the combined functions of Verifier (in terms of verifying credentials) and some of the functions of CSPs (in terms of issuing credentials). In the case of a university or research institute, the user registration function of the CSP would be under the responsibility of the departments in charge of academic affairs and human resources. As CSPs and IdPs operate not completely separated in terms of the NIST model, it is likely to cause ambiguity, for example, whether the implementing entity of IAL2 within this document would be the IdP (as we call it) or the CSP.

In this document, we would like to begin by first clarifying this potentially misleading situation.

1.1 In the case of a university or research institute where academic affairs or human resources is registering users as a CSP

The operation of unified accounts is now commonly observed in many universities. For example, instead of accounts being issued by information infrastructure centres, they are provisioned directly from a database of academic affairs and human resources that is trusted by the organisation (hereafter referred to as Trusted DB). Even if the operation of the IdP is outsourced (IDaaS), it applies to this if it is based on a Trusted DB.

In such cases, identity proofing by CSPs, as specified by NIST, is conducted as part of the admissions and hiring process and the maintenance of a Trusted DB that reflects this process. In such cases, the department operating the IdP does not need to be responsible for many of the IAL maintenance actions specified by NIST. **It is sufficient to assess the maturity of the organisation (i.e., that admissions and recruitment are running smoothly and without incident).** It is sufficient for the IdP to define the account creation process and its policies by referring to higher-level regulations.

1.2 In case the IdP is operating accounts as an IdP for jointly-used services operated within the organisation

For example, this applies to a university department or research institute that operates a jointly-used system and issues accounts to users outside the organisation. In such cases, a full set of the following provisions apply. If, however, a university or research institute's accounts are sufficiently trustworthy, the cost of IAL screening can be greatly reduced by using them for creating accounts. In this sense, IALs (and AALs) at home institutions are also important.

2 Differentiating what is defined within the operational scope of the CSP from what is related to higher-level university administration

Based on the above observations, the following sections will discuss the NIST/KIAF documents by categorizing the rules into Types 1 and 2 and define the actions to be taken by the IdPs participating in the new GakuNin.

Type 1) General provisions for CSP operation (as specified by NIST/KIAF in General Requirements, CrP/CrPS, Security Control, Trusted Referee Proofing)
Type 2) Provisions for identity proofing (as specified in the resolution, evidence collection, validation, verification, presence, and address confirmation)

Rule 0 defines whether an institution operating an IdP is classified as Type 1 or Type 2.

Rule 0.1 For the IAL on accounts served by an IdP that are provisioned directly from the institution's Trusted DB, the rules related to Type 1 shall be applied. For the IAL on other accounts, the rules related to Type 1 and Type 2 shall be applied.

Note: It is often the case that the types of "Trusted DB" are not only simple, nor are their operations. For example, the system can be designed to provision from Trusted DB 1 to DB2 and to assign new attributes with DB2 as the starting point of trust, and furthermore, it is expected that such attributes have operations that are trusted by other services. In this document, they are collectively referred to as Trusted DB; the complexity of the configuration of Trusted DB is not subject to evaluation in this document as long as it is consciously controlled and operated within an organisation.

Rule 0.2 In 0.1, the accreditation body (i.e., GakuNin) shall accredit whether the audited institution's accounts are provisioned directly from its Trusted DB and determine which items to be applied.

Note: "Whether provisioned directly" shall be determined based on the following criteria:

1. The system architecture of provisioning is sufficiently automated, etc., and thus able to sufficiently deter arbitrary operations by the organisation (e.g., creation of accounts by processes other than the said provisioning)
2. The operations of provisioning are sufficiently controlled in terms of system security and

authorisation management

Note: In Rule 0.1, it is stated that the complexity of the Trusted DB configuration is not subject to this evaluation. Even if the system is complex, as long as the operation is appropriate, it is considered that this rule is satisfied.

Rule 0.3 In the case where it is accredited that provisioning is done directly from a Trusted DB in 0.2, it shall accredit whether or not the said Trusted DB implements identity proofing of a strength equivalent to IAL2.

Note: Japanese universities and research institutes are regulated by the Ministry of Education, Culture, Sports, Science and Technology (MEXT) and other organisations with respect to the administration of entrance examinations and admission procedures for students and the recruitment of faculty and staff. If it is determined that the institution is in compliance with those regulations, the accreditation may be granted by applying those regulatory items accordingly. In general, it is expected that the strength of IAL2 is met if it is operated within a Japanese institution. It is possible, however, that universities and other institutions whose procedures are completed online may be conducting identity proofing under more relaxed standards than the conventional ones. In such cases, the accreditation may be granted by taking into consideration of “maturity of the organisation” and “past incident history” comprehensively.

Note: Depending on the university or institution, there may be cases where a JSPS Research Fellow, an exchange student from a partner university, or a researcher from a company is registered in the Trusted DB without going through the normal admission or recruitment process or is given an account as equivalent as such. If the university/institution has established rules for acceptance and confirms that the same level of identity proofing is in place as in normal circumstances, then the accounts and provisioning are considered to be adequately controlled by the university/institution.

Note: There are universities and research institutions that have issues related to research ethics and problems with poor conduct by students and faculty members. These are of serious concern to the RPs that provide services. The new GakuNin does not necessarily examine the circumstances of individual RPs in this regard; however, it is also possible to include elements of such issues in these organisations in the evaluation of the “maturity of the organisation”.

3 General provisions for CSP operations

This section defines the general provisions for CSP operation. It is required to establish operational rule documents and so-called “venous system” services such as risk assessment, auditing, and complaint handling.

Provisions related to privacy

Rule 1.1 Personal information held by CSPs shall be based on the principle of minimum. Privacy considerations shall be taken into account in the collection and retention of such information.
Note: In cases where Trusted DBs, etc. are provisioned externally, the referenced items shall be kept to the minimum required for operation.
Rule 1.2 When the CSP collects and retains attributes, it shall clarify the purpose of use, limit usage scenarios, disclose them within the CrP, and operate based on the principle of minimum.
2. When collecting attributes, it shall establish privacy rules, indicate them to users, and obtain their consent.
Note: Privacy rules include a description of whether the attributes to be collected are required or optional and the disadvantages of not consenting to attribute collection.
Rule 1.3 When additional attributes are collected and operated for purposes other than identity-related services, it must not be to the detriment of users who do not consent to the collection. When collecting, an assessment of effectiveness shall be made and documented, along with an associated privacy risk assessment.
Note: “Other than identity-related services” includes security measures and legal requirements.

3.1 Matters related to the handling of complaints

Rule 1.4 The procedures for handling complaints regarding user registration procedures and the contents of registration shall be defined and operated.
2. The complaint handling procedure shall be evaluated at least once a year to assess its effectiveness.

3.2 Creation and implementation of CrP/CrPS

It is required to establish a policy and operating rules (CrP/CrPS) for the credential. Templates are provided in a separate document.

Rule 1.5 The identity proofing and registration policy shall be published in advance as a Credential Policy (CrP).
2. The CrP must specify the following:
A. The types of identity proofing methods to be applied and the source of evidence to be

used for each

B. The methods of identity proofing to be applied/not applied depending on the type of user

Rule 1.6 The Credential Practice Statement (CrPS) to implement the CrP must specify the following:

A. Specific implementation methods and procedures for the identity proofing methods set out in the CrP

B. Methods of handling cases where identity proofing is not successful for each of the implementation methods.

Rule 1.7 With regard to the implementation of the CrP/CrPS, privacy and security risk management shall be conducted regularly, at least once every six months, or whenever major changes occur in the CrP, and the results shall be documented. The specific details of risk management shall include the following:

A. If identity proofing is to be performed beyond the mandatory requirements in the CrPS, the procedures to be followed

B. A list of personal information to be collected and retained as part of the identity proofing procedures set out in the CrP

C. Schedule for retention and disposal of records as required by law, internal regulations, etc.

D. If fraud prevention measures are to be taken, the measures to prevent

Rule 1.8 Logs shall be kept of the implementation of the identity proofing and for auditing purposes. In particular, it shall include the method of identity proofing, the evidence to be collected, records of inquiries to the source of the evidence, all procedures for validation of the evidence, and all procedures for verification of the evidence, the results of each implementation and the conclusions of the identity proofing.

3.3 Security measures

Rule 1.9 Any personal information collected during the identity proofing process shall be protected by information security.

Rule 1.10 The entire procedure of identity proofing must be performed using security-protected communications.

3.4 Termination of services

Rule 1.11 If the CSP terminates its services, it shall specify how it disposes of, destroys, and protects against unauthorized access to personal information it collected up to that point.

4 General security

Rule 1.12 Systems that operate CSPs shall implement adequate security measures in accordance with general security standards.

Note: It could be unified government standards for security policy, or it could be a university security policy if it refers to them. For the time being, it is important to establish a policy or standards that everyone can agree on, and to show that it is being operated in accordance with that policy or standards.

5 Templates for CrP/CrPS

⇒ In a separate document

6 Standards for identity proofing to achieve IAL2

The following clauses apply to Type 1.2 (operating a nationwide jointly-used IdP). In such cases, it must set out the procedures for assessing and issuing accounts.

For the Type 1.1, which refers to a university IdP that is provisioned by connecting directly to a Trusted DB, the discussion here does not apply, as it follows the previous discussion.

For example, in the case where a university account is used to register with a nationwide jointly-used IdP, the balance between both types must be considered. If the university account meets the assurance levels of IAL (≧2) and AAL (≧2), then the assertion of login there can be claimed as STRONG evidence (see below).

6.1 Document resolution

Rule 2.1 The collection of personal information when using collected data as evidence of the identity of a particular person shall be kept to a minimum socially acceptable level.

6.2 Evidence collection

Rule 2.2 The CSP shall collect one piece of STRONG or higher evidence from the user (see below). Provided, however, that the CSP can directly confirm that the source of the evidence has collected two or more pieces of evidence before issuing the evidence.

2. If the CSP is unable to confirm the above, it shall collect two pieces of evidence that are STRONG or higher.

3. If this is not possible, one piece of STRONG evidence and two pieces of FAIR evidence may be used to substitute.

Rule 2.3 The reasons for determining the level of evidence shall be documented in writing.

e.g.: A. A student or staff ID card with a photograph issued by a Japanese university may be treated as STRONG.

B. An employee ID card issued by a general company must be treated as FAIR.

C. A passport and driver's license are STRONG. If, however, the biometric data stored inside can be accessed, they may be treated as SUPERIOR.

D. Provided that the authentication assertion issued by a university IdP remotely (within some trust) is IAL2 and AAL2, it may be treated as STRONG evidence that can be directly confirmed by the CSP, as long as the assurance level of the name (CommonName) is 2.

6.3 Validation of evidence

Rule 2.4 The evidence collected shall be validated based on its strength with a validation level equal to or higher than that described below.

Rule 2.5 The reasons for determining the level of validation shall be documented.

2. The policies, guidelines, and requirements for training personnel who determine validity shall be documented.

6.4 Verification of evidence

Rule2.6 The evidence shall be verified with a strength of STRONG or higher. In particular, knowledge-based verification shall not be performed.

Rule 2.7 The reasons for determining that verification was conducted at STRONG or higher shall be recorded.

6.5 Verification of identity

Rule 2.8 The verification of identity shall be conducted by at least one type of in-person or remotely supervised or remotely unsupervised. The procedure shall be described in the CrP.

6.6 Verification of address

Rule 2.9 The address of a user must be identified only from the issuing source of the evidence, and self-reporting must not be accepted.

Rule 2.10 If the identity verification is conducted under surveillance, the registration code may be sent to the user's address or hand-delivered in person. The validity period of the registration code must not exceed 7 days.

2. If the identity verification is conducted in an unsupervised environment, the registration code must be sent to the user's address. In this case, the identity verification shall be completed by making the user produce the registration code that was sent. The validity period of the registration code must not exceed 7 days.

Rule 2.11 If a registration code is used as an authentication factor, the factor must be deactivated at the first time it is used as an authentication factor. The validity period must not exceed 10 days for postal mail, 10 minutes for telephone, and 24 hours for e-mail.

Rule 2.12 The registration code and the results of the identity proofing must not be sent to the same address.

Note: The address referred here shall be either a physical mailing address, a mobile phone, a landline phone, or an e-mail address.

6.7 Standards and examples of evidence, validation, and verification for Fair/Strong/Superior

6.7.1 Requirements for evidence with the strength of STRONG:

A. The issuing policy is reasonably set out for living persons and issued to them. In addition, the policy is documented and adequately supervised by regulatory authorities

B. Reference numbers are uniquely assigned

C. The listed name is the officially recognized one. Only full names are acceptable, not abbreviations

D. It is either accompanied by a photograph or contains biometric data. Or it is an assertion with an assurance level of IAL2, AAL2

E. Of the above information, digital information is protected by encryption

F. If it contains physical features (such as information on a card), it is difficult to be copied and reproduced

G. It is confirmed to be within the expiration date.

Example: 1. A photographic identification card issued by a public sector organisation. Passport, driver's license, radio operator's certificate, etc. Those issued by universities under the supervision of the Ministry of Education, Culture, Sports, Science and Technology may also be treated as such, provided they are properly operated.

2. In order for an assertion issued by a university IdP to be considered STRONG, it is necessary to grant assurances of IAL2 for the uid (uniquely defined) and CommonName.

Note that the rules regarding evidence with the strength of FAIR are omitted here.

6.7.2 Requirements for validation with the strength of STRONG:

A. The evidence can be confirmed by appropriate means (including human confirmation) that it has not been tampered with, either on the face of the card or in the digital information it contains

B. The personal information in the evidence can be confirmed as legitimate by checking it against the information provided by the issuer

Note: Passports and licenses can be carefully checked for irregularities. For these, forgery is punishable by law (forgery of official documents), hence it can be considered a social deterrent.

Note: As for assertions, if they were sent via protected communication, they can be considered STRONG.

6.7.3 Requirements for verification with the strength of STRONG

A. The verification of identity match by comparing a photograph with the individual in person or by comparing biometric data. In the case of in-person, the quality of communication, screen quality, etc. must be kept sufficiently high to maintain adequate verification quality. As a strict rule, technical verification is required to assure the quality indicated in NIST/KIAF.

Note: Matching the photo in evidence with the person him/herself. The same accuracy is required as when registered biometric data is used (such as that used in immigration control). In the case of in-person screening by humans, it is trusted; in the case of remote screening, however, it is required to assure the quality of communication and images that enable the same level as in-person screening.

Note: In the case of assertion, it is acceptable to examine the content.

7 Accreditation, operation and auditing system by the GakuNin Trust WG

Currently, GakuNin provides a framework for LoA1 (equivalent to Level 1 in NIST SP800-63-1) accreditation to participating institutions. The Trust WG is handling the actual work. For IAL2 and the subsequent AAL2, it will be Kantara to determine if this document meets Kantara's criteria; if it does, the GakuNin Trust WG may be able to undertake the Kantara accreditation process (at least) in Japan. There will be a difference depending on whether the IAL2 is of Kantara or the GakuNin's own. The difference will not be an issue in Japan; however, it will require negotiation to deal with service providers, such as eduGain, that contribute to international research cooperation.

In any case, the GakuNin Trust WG is responsible for IAL2 accreditation within the GakuNin. It will authorise accredited IdPs to send out attribute values related to the assurance. For example, attribute values such as gakunin-IAL2 would be distributed at least in Japan. The Trust WG will also be in charge of auditing these operations.

In addition, the Trust WG will be actively engaged in advising institutions participating in GakuNin to obtain IAL2 accreditation. In this case, a different individual would be responsible for advising than the one doing the accreditation.

8 Contact details for comments and inquiries regarding this document

For comments or inquiries regarding this document, please contact us below.

https://www.gakunin.jp/contact