Meeting Minutes of The Working Group for Next-Generation Identity Federation

Meeting on GakuNin, Thursday, 24 December 2020

- We discussed the structure for conducting R&D on authentication, and it was decided that the Trust Working Group will be expanded and implemented, and that the members, objectives, etc. will be finalised by the end of the year, and that the activities of the Trust Working Group will be actively promoted.

Meeting for Exchanging Opinions on GakuNin, Friday, 19 February 2021

- GakuNin was launched in 2009 as an academic access management federation in collaboration with universities and other institutions in Japan and the NII. It has been operated as a stable service under the Committee for Academic Authentication as a project of the NII since 14 January 2014; however, there have been little research and developmental activities. In the meanwhile, it has been suggested that a new trust framework may be necessary for research data management and authentication level required there, the collaboration with industry and academia, and the authentication in the next HPCI. Therefore, it was concluded that it would be appropriate to establish a new working group to deal with these issues through volunteers exchanging opinions on these issues and the future goals.
- The mission of the new working group is to discuss and develop trust technologies for open and secure research and education data distribution in the academic field, to discuss how to promote and work toward its operation, and to take charge of other necessary matters related to the trust framework in the future.

Meeting for Exchanging Opinions on GakuNin, Thursday, 11 March 2021

The attendees from universities, research projects, and the private sector explained the current status and issues in the authentication infrastructure from their perspective. The main issues are as follows:

- GakuNin's institutional accreditation process is a big hurdle (i.e., to expand the participation of small-scale institutions)
- It is complicated for institutions to operate and manage IdPs (i.e., development of a system like a proxy IdP service)
- A mechanism to define the middle ground between "institutions" and "individuals" (i.e., management function such as a "project" that can be freely combined and recombined)
- A mechanism for individual users to move from one institution to another
- Promotion of the use of GakuNin by raising users' awareness to use it proactively
- Multi-factor authentication
- Attribute information and attribute verification to address security issues
- New authentication infrastructure that is less of a burden for both users and operators

FY2021 The First Meeting of The Working Group for Next-Generation Identity Federation, Friday, 23 April 2021

1. Regarding the structure of the new trust framework, there was an explanation about the proposed form of providing IDaaS to universities that cannot operate TrustedDB or TrustedDB as IdP for collaborative research. After this, the following comments were made:

- The NII's services have been subscribed to institutions. In the case of research data, however, the

information held by users has more importance; therefore, it will become important how to transfer the information held by individual researchers when they change jobs.

- Although the main subscribing entity of IDaaS has been institutions, a model is emerging in which the research community subscribes. It is likely to become a problem that the difference in the roles played by IDaaS will become greater.
- While trusting TrustedDB for basic attributes, could the project side manage the information related to the project?
- When an institution conducts identity proofing, it is important to link the identity of the person to the institution.

2. After an overview of mAPCore, its challenges, and future plans were given, the following comments were made:
   - A plan to develop API to enable group management directly from SPs (or IdPs) participating in GakuNin, and to provide more detailed roles for members by providing only the minimum API for group management (create, update, add/delete members) from external SPs.
   - The mAP acts as the issuer to prove that a person belongs to a group or project.
   - Regarding the framework of institutions and individuals, if we were to focus on the individuals, it may become easier to create a model to tackle issues such as Orphan IDs and individuals who receive identity guarantees from multiple groups.
3. After a review of UPKI services and an explanation was given on the changes in the situation with certificates, the following comments were made:
   - Difficulties in agility due to emphasis on diversity is not only a problem for UPKI but also for the global community as a whole. While agility can be ensured by unifying with IDaaS, etc., it is necessary to consider how to ensure diversity and R&D at universities.
   - In relation to the next-generation authentication infrastructure, it is necessary to consider the balance between ensuring diversity, risk control, expanding scale, and agility.

Published Documents:

- Meeting for Exchanging Opinions on GakuNin: Opinions from IDaaS providers
- What is mAP Core?

FY2021 The Second Meeting of The Working Group for Next-Generation Identity Federation, Thursday, 27 May 2021

1. There was a presentation on survey report on authentication management at international joint research project (1 case), accreditation management at universities (2 cases), identity assurance, and the standards for eKYC, followed by a Q&A session. After these, the following comments were made:
   - The universities are operating in a manner similar to IAL2, although there are some differences in procedures.
   - It seems to be a problem that the distinction is not well defined between user confirmation upon registration and that upon continuance. A further report will be published by the OpenID Foundation Japan soon on how to handle the continuing user confirmation.
   - It is also important to consider how to reconfirm the status when personnel are transferred.

Published Documents:

- Examples of authentication management for international joint research projects
- Identity Assurance and eKYC Criteria

FY2021 The Third Meeting of The Working Group for Next-Generation Identity Federation, Wednesday, 30 June 2021

1. After the survey report was presented on the IALs and attribute sets required on the platform side (4 cases) followed by a Q&A session, the following comments were made:
    - We would like to create a mechanism to maintain the IAL and AAL in order to raise the level of authentication to ensure that accounts at the university and IDaaS are adequately trusted so that the sources held by the research community can be used conveniently.
    - It would be convenient for both parties if the framework were to approve institutions that meet certain criteria rather than institutions approving the users; for this purpose, it is desirable that the latest user affiliation always be reflected.
    - The Group ID is intended to cover a wide range, so what is specified by IAL are different in terms of level.
    - The importance is in "equivalent" to IAL2. It is dangerous to link identity proofing and issuing of IDs too directly.
    - The attributes required by SPs have not yet been determined and instead of using a non-definitive phrase such as "IAL2 equivalent", we need to define Japanese IAL2.
    - There is room for discussion on the importance of research data to be stored and what should be required in terms of authentication from a software perspective.
2. After an explanation was given to the requirements for the new authentication infrastructure and the requests for trust framework providers, the following comments were made:
    - The hurdle needs to be raised when accommodating corporate researchers in academic authentication collaborations.
    - If ID issuance is defined, not only companies but also universities and other institutions that cannot conduct identity proofing will come to IDaaS.
    - The focus should be on how to authorise services to the research community, and we need to consider what the research community requires in terms of identity proofing, identity management, and authentication policies. The research community should stay out and GakuNin should take the lead in taking care of what to do with identity proofing.
    - We need to discuss again what kind of role the research community should play to make it efficient and secure.
    - We need to establish a service that issues IDs for orphan researchers whose identities cannot be verified by university IdPs as soon as possible, so that the service can be provided through GakuNin.
    - As there is no IDaaS-like service in GakuNin, it could be a shortcut to achieve this if we work together with academic societies and others.
3. We discussed about the structure such as presentation, panel discussion, etc. for the Authentication Track (the theme is "New Trust: Trust technologies for open and secure research data distribution in academic fields") at the Open Forum 2021 (Thursday, 8 July 2021).
   Published Documents:
    - Requirements for New Authentication Infrastructure and Requests for Trust Framework Providers

FY2021 The Fourth Meeting of The Working Group for Next-Generation Identity Federation, Monday, 26 July 2021

1. It was reported that the contacts were made to IGTF, eduGAIN, and Kantara regarding co-existence and compatibility collaboration, and awaiting responses from them.

2. After an introduction to the FIDO authentication and its support for AAL, the following comments were made:
   - The final goal is to provide robust authentication so that the services provided by the research community can be used; so, the use of FIDO seems realistic.

3. After an explanation was given on the support for AAL2 and higher at GakuNin, the following comments were made:
   - Regarding FIDO accreditation of developing software, Japan has the largest number of FIDO accreditation and has guidelines; therefore, it would be good if GakuNin is accredited .

4. After an explanation was given on the results of the survey on Kantara Criteria, the following comments were made:
   - We would like to consider the IAL accreditation procedure for universities and research communities based on Kantara Criteria.
   - We would like to use this as a basis for discussing whether Kantara's procedures are applicable to Japan and how to apply them; however, we would like to hear opinions on Kantara's procedures from universities and the research community, as it will be chaotic without the consent of the universities and institutions operating IdP and the research community providing the service.

   Published Documents:
   - Investigation of Kantara Criteria
   - Proposals based on the installation of biometrics in smartphones and insights gained through a summary of FIDO authentication
   - Toward a Balance between High Level of Security and Usability in Authentication with Private Sector IDs Utilising the Functions of My Number Card
   - AAL2 at GakuNin

FY2021 The Fifth Meeting of The Working Group for Next-Generation Identity Federation, Friday, 10 September 2021

1. There was an explanation on Microsoft's support for AAL2 and higher, TPM2.0 (which has become mandatory in Windows 11) and its usage, the biometric authentication function of Windows Hello, PIN authentication, and multi-factor authentication for Azure AD, followed by a Q&A session.

2. After an introduction to the FIDO authentication and its support for AAL, the following comments were made:
   - There is a concern that the number of inquiries and response time may increase if a problem occurs when the service authenticates the ID after the university has authenticated the ID and password.

3. After the Kantara IAL2 Criteria was explained and the points raised by the IdPs (2 universities and 3 research communities) were introduced, the following comments were made:
   - The idea of CSP is that the person in charge of administration performs the identity proofing and the person in charge of information system registers IDs according to a single rule. The important thing is the evidence for issuing IDs; it will be strong evidence if the ID cards issued by the university can be verified.
   - Since the Kantara Criteria does not have any kind of template for the document structure to be created, the Japanese version of the template must be created by GakuNin.
   - The translation of the Kantara Criteria should be made easier for university personnel to understand

by making the evidence more generic, with specific examples of evidence, etc., so as to facilitate deeper discussion of interpretations from the research community and other IdPs.

- The HPCI is currently operating almost all at IAL2, but this cannot be continued. It is planned to begin organising IAL requirements for the HPCI in conjunction with the design and construction of the next authentication infrastructure.
- Regarding the approach to multi-factor authentication in GakuNin RDM, it is possible to use GakuNin RDM for second-stage authentication; however, this would conflict with the Kantara Criteria as the second-stage authentication and service authentication would be the same, and there is a concern that the cost of supporting authentication would increase. Therefore, this should be carefully considered.
- The CrP/CrPS template needs to be properly considered.

Published Documents:

- Support for AAL2 and Higher at Microsoft
- Investigation of Kantara Criteria (Revised)
- Kantara IAL2 Japanese Translation
- A Study for Multi-factor Authentication in GakuNin RDM

FY2021 The Sixth Meeting of The Working Group for Next-Generation Identity Federation, Friday, 15 October 2021

1. It was explained that the goals for this year's discussion would be to discuss from the perspective of "IAL, AAL, international cooperation, implementation in GakuNin, and consideration of new services", and to get the results of the working group out to the public, leading to a strategy for acquiring budgets. After this, the following comments were then made:

    - As the budget request will take a long period of time, we would like to start with a discussion of building a prototype. The NII is engaged in a variety of projects, so it would be possible if we can get their understanding.
    - We would like the NII to consider expanding the framework of its projects; we will discuss the results of the current fiscal year and the goals for the next fiscal year by spreading seeds for how the research community, including research data and open science, can benefit from it and building prototypes, etc. so as to take a little shape in the next two to three months.
    - The Data Society Alliance has expressed concern that companies are having trouble with authentication and so wishes to create a system that allows them to use data by not only authenticating individuals but also organisations. We felt that it would be better to include not only the research community but also the industrial community that utilises data as a target audience.

2. After an explanation was given on "Draft for the Operation of IAL2 in the New GakuNin" and "Draft Proposal for Examples of CrP/CrPS", it was stated that the next step would be to confirm whether it is operational at universities, whether universities are recognized as having a high level of assurance by the research community, and whether IDaaS operators can turn around the IDaaS business. After this, the following comments were then made:

    - There is a study meeting on authentication on 22 October and we would like to get opinions on these points as an informal proposal at the meeting. We would also like to hear other opinions on how much assurance would be sufficient, so we would like it to be read from that perspective as well.

3. An explanations was given on the technology layers being standardised by the OpenID Foundation and DIF, and on the data format initiatives currently being considered for standardisation by the Digital Credential Forum, led by MIT.
4. After an explanation was given on the risk assessment methods of the various eKYC methods based on the IAL assessment sheet, the following comments were made:
    - The situation where eKYC is used is where there is no direct connection between the source and the IdP, which is why the role of IDaaS comes into play. The reason why IDaaS is necessary for the research community is to accommodate the IDs of corporate researchers and others who are not directly connected. So, it would be appreciated if the standards for IdPs, IALs, and AALs would emerge and be accredited.
    - It is desired to collect various cases of the eKYC assessment methods depending on the usage.
5. The Open-IDP is starting to consider the implementation of a mechanism to support data access and portability in the event of personnel transfers; it was decided that this will be reported in the next meeting.
6. Based on the hearing with FIDO and Microsoft regarding AAL, an explanation was given of the perceptions so far, such as the need for AAL2, which is not an easy task because of the need to evaluate both the authenticator's providers and the university's operation. After this, the following comments were exchanged on how to proceed with the discussion:
    - We would like to expand the survey questions in the IdP Operational Status Survey and so would like the NII to create questions that reflect the discussion.
7. It was announced that the activities of the Working Group for Next-Generation Identity Federation were introduced at the OpenID Foundation Japan eKYC-WG held on 8 October.

Published Documents:

- Opinion on the Operation of IAL2 in the New GakuNin (20210918)
- Draft Proposal for Examples of CrP/CrPS (20210918)
- DID and Related Technologies, Trends in Its Standardisation, and Examples of Its Applications
- IAL Evaluation Sheet
- Creation of New Trust in Academic Authentication Infrastructure: Activities of The Working Group for Next-Generation Identity Federation

FY2021 The Seventh Meeting of The Working Group for Next-Generation Identity Federation, Friday, 12 November 2021

1. An explanation was given on IAL2 and eKYC, and it was decided to further expand on the risk assessment of eKYC. In addition, the following comments were made:
    - It would be great to have comments on eKYC risk assessment and suggestions for eKYC from the perspective of NIMS and other organisations that have to support researchers in the private sector.
    - The community of research collaborators needs to distinguish between authentication and verification of attributes of authorisation, both of which would be done by the CSP.
2. IdP Operational Status Survey: It was announced that the survey on AAL2 -related questions for SPs that handle sensitive information will be launched to IdPs and GakuNin Information Exchange MLs during the week of 15 November. After this, the results of the Japanese translation of the Kantara AAL2 Criteria were explained, and the following comments were made:

- AAL has many different types of authenticators and different operational situations, so it would be interesting to see and summarise the results of the AAL survey.

3. After an explanation was given on the status of the Orthros project regarding the mechanism to support data access and portability in the event of personnel transfers, the following comments were made:

- I heard at the Open Science Cloud two years ago that there was an awareness of the problems with OrphanID and inter-organisational transfers. (I also heard that) eduID is providing a persistent identifier.
- Is it possible to guarantee the level of IAL assurance when IDs are transferred? If we simply copy the European precedents, we may be able to achieve the current level of GakuNin, but we may not be able to do what we want to do in the next generation authentication that we have been discussing.
    - Although it would be good for universities to become IAL2, it is concerned that if something like Japanese Public Key Infrastructure cannot be used to link IAL2 at University A and IAL2 at University B as being the same, it will be very difficult to prepare a new mechanism, etc. It may not be possible in all cases, but to the extent that it is possible, it seems that it would be more efficient to use Japanese Public Key Infrastructure
- The Digital Agency has asked to hear about the recent status of GakuNin, and we hope to collaborate well with them. We are also discussing the possibility of providing a service at the NII to link the authentication proxy that was introduced previously, if we can link it well and combine it with the My Number Card. We hope to create Orthros with such functions in the future and to lead the way in this initiative.
- This fiscal year, we are hoping to develop a basic authentication proxy service and are in the process of showing how private companies can access GakuNin RDM via Orthros in an open forum as a practical demonstration of industry-academia collaboration.

4. Others

- It was reported that a comment was received from Kantara questioning over the neutrality of GakuNin if it was to grant IAL2 and AAL2 to its participating institutions; however, we will defend it to all intents and purposes because it would lose its significance as a trust framework.
- We are aware of the need to establish a joint study group to provide a forum for young researchers to provide information.
- Regarding the release of the "Request for Document Evaluation from the Perspective of Criteria Development and Deployment for the Construction of the Next-Generation Authentication Infrastructure", it was announced that the request for evaluation was released on the GakuNin website.
- Discussing a framework for next-generation authentication is an important but time-consuming effort. On the other hand, there is a need to adopt the discussed framework proactively, and so, a proposal was made to start discussion and consideration of a pilot initiative with a small start with some organisations that are willing to support it. It was decided to establish a sub-working group and report its progress as needed to the working group.

Published Documents:

- AAL2 - Investigation of Kantara Criteria
- KIAF-1440 SP 800-63B SAC & SoCA v4.0_Japanese translation
- Challenges in Authentication Approval in Inter-Organisational Transfers

FY2021 The Eighth Meeting of The Working Group for Next-Generation Identity Federation, Thursday, 23 December 2021

The activities of the newly established Sub-Working Group on Short-Term Initiatives was shared as a progress report of the meeting to examine the leading initiatives in the Next-Generation Identity Federation.

1. After EXGEN NETWORKS and Microsoft explained the status of AAL2 support for IDaaS, the following comments were made:

    - Although GakuNin should consider the applicable qualifications, it became clear that it is the current technology. It is particularly encouraging that it is supported by IDaaS.

After this, a report was given on the progress of the interim statistics of the questionnaire "Factors Available for Multi-Factor/Multi-Step Authentication", and the following comments were made:

- We feel that it is important to have some business models drawn up at an early stage, such as how high-end authentication can spill over to the long tail, so these discussions are necessary in the future.
- This survey asked about multi-factor authentication for authentication systems used on campus, including those outside of GakuNin. The IdP survey that was limited to GakuNin was conducted separately, and the results showed that only a single digit number of institutions have introduced multi-factor authentication. It should be understood that this response was obtained because this survey was conducted for multi-factor authentication outside of GakuNin.
- While the survey results seem to indicate that many are concerned about operational costs, it would be good to know how many people are likely to be able to immediately adopt it, as free multi-factor authentication such as Office 365 Education A1 is available. After that, the next phase would be to find out how to get these people to use it.
- We have to start by increasing the presence of our activities and making people feel that it is important to be involved in this. We should be more aware that this is a problem for us.

2. A report was given on the status of IAL feedback, and it was highlighted that the future discussion should consider the handling of researchers who are not directly employed by universities.

Then, after information was shared on the trends in e-seal and corporate KYC, the following comments were made:

- We requested some information to be shared with the intention to see if this could be done in relation to IDaaS as compensation for those who only belong to a company or academic society and wish to claim their identity in IAL2.
- We are developing a system that allows users to use GakuNin RDM after conducting identity proofing via gBizID, with the goal to demonstrate it at the Open Forum in 2022 as a verification experiment.

Then, an explanation was given on the added and revised contents of the document following the comments made at the previous working group meeting regarding the IAL Evaluation Sheet. After a Q&A session, it was decided that the issue should be discussed again.

Published Documents:

- Draft Opinion on the Operation of AAL2 in the New GakuNin (20211207)
- Authenticator registry_MSAuthenticator
- e-Seal and Corporate KYC: With respect to identity proofing of members in an organisation
- IAL Evaluation Sheet (6th_update)
- Review Procedures for the "GakuNin LoA1 Accreditation Program"

FY2021 The Nineth Meeting of The Working Group for Next-Generation Identity Federation, Tuesday, 18 January 2022

1. We continued the discussion on IALs, starting with the explanations from two research projects on how KYC is operated when granting accounts to external researchers. Then, following the previous discussion, an explanation was given on IAL Evaluation Sheet. The following comments were exchanged:

    - It will probably lead to writing the CrP/CrPS properly as Kantara requires, but it would be necessary to guide those who involved appropriately as it will be a challenge.

Then, an introduction was given on the development status of authentication cooperation between OpenIDP and other authentication. After this, the following comments were made:

- It is necessary to consider whether Orthros' IdPs will be subject to accreditation in the future.

Then, an explanation was given on the four comments made on the IAL by the end of December. The following comments were made:

- We would like to reflect the feedback on the ambiguity of the wording and modifications to match the actual situation and begin discussions on the drafting of specific criteria for the future.
- Although IAL would be manageable for universities, we need to request gBizID participation in IDaaS or Orthros to accommodate overseas and corporate users.

2. In the discussion on the AAL, an explanation was given on the results of the survey on the burden of operating an authenticator registry. The following comments were made:

    - It may be necessary to operate not only the initial accreditation of the authenticator itself, but also its maintenance and management from a lifecycle perspective.
    - We also need to get the IPA and major vendors together and ask for their cooperation.
        - We understand that the operation of the authenticator registry is burdensome; we will collect and report on the sense of burden through a trial run of the Sub-Working Group on Short-Term Initiatives.

3. After an explanation was given on the review procedures in the "GakuNin LoA1 Accreditation Program", the following comments were made:

    - There are two topics to reflect in the assertion to be accredited; for accreditation, Kantara's LOA1 accreditation program is running and has not been accredited since Kantara started. It would take quite a long negotiation to seek accreditation from Kantara this time, so we are thinking of proceeding in the form of accreditation by GakuNin.

Published Documents:

- IAL Evaluation Sheet (6th_update, rediscussed)
- Authentication Proxy Service Orthros
- Draft for the Operation of IAL2 in the New GakuNin (20211020)
- Draft Opinion on the Operation of AAL2 in the New GakuNin (20211207)
- Consideration for the Operation of Authenticator Registry
- Authenticator registry_MSAuthenticator
- Review Procedures for the "GakuNin LoA1 Accreditation Program"

FY2021 The Tenth Meeting of The Working Group for Next-Generation Identity Federation, Tuesday, 22 February 2022

1. We continued the discussion on the IAL, and there was an additional explanation on the revised draft of the operation. After this, the following comments were made:

    - Once academic and corporate users are able to use external IDs, it may be the right scenario to concentrate on authorisation control.
    - The MOU must be provided by GakuNin.
    - The intent of the proposal is not to apply to all, but to create a step-by-step process. It would be that most of the SPs can apply this by expressing the GakuNin IAL2 or trusting it since it is the GakuNin IdP; however, there may be cases where rigorous confirmation is required. So, it would be better to use the proposal in such cases. From this point forward, it is a matter of authorisation, and in addition to creating an account, it would be better to consider the control over what to do with access privileges in a step-by-step manner.
    - It is important to confirm affiliation; it is necessary for GakuNin to state that the employee's ID, etc., which serves as evidence, is to be trusted.

Then, an explanation was given on the revised sections of Ver. 2 of the "Draft for the Operation of IAL2 in the New GakuNin" which reflects the feedback received, etc. It was announced that it will be released after reviewing it on Slack, and the confirmation with IdPs and SPs for no problem will be made at the end of the fiscal year or at the beginning of the fiscal year.

2. With regard to AAL, a report was given on the status of the discussion on operating an authenticator registry. The following comments were made:

    - There is a great deal of variation in certificate operations among universities, so it is necessary to consider the cost and other factors to determine whether it is necessary to use a public certification authority.
    - Even for private authentication, CP and CPS must be written, but the review process could be troublesome. → For academic institutions, it would be better but not necessary as a trust framework can be established without it. However, if companies are included, it is necessary to prepare CP and CPS and be ready to present them.
    - After working on the topic of AAL, we would like to discuss the proposal for certificate authentication.
    - As for the authenticator itself, it would be quite a lot of work if we include operational parameter control; so, we would like to start small and ask for help from those who can conduct experiments.

    Published Documents:

    - Draft for the Operation of IAL2 in the New GakuNin (20220225)
    - Draft Opinion on the Operation of AAL2 in the New GakuNin (20211207)
    - Draft Proposal for Examples of CrP/CrPS (20220222)
    - Necessity of Verified Attribute Expression in GakuNin and Technical Specifications (Draft) (20220221)

FY2021 The Eleventh Meeting of The Working Group for Next-Generation Identity Federation, Wednesday, 23 March 2022

Prior to the discussion, it was announced that the "The Operation of IAL2 in the New GakuNin (Ver. 2)" had been released on the Web, and that opinions had been exchanged with university officials who had

provided comments regarding the document. It was confirmed that the criteria for accreditation should be documented and presented to institutions, and that it is necessary to establish a system for the work.

Then, it was reported that there was basically no problem with the result of the SP side's examination on the acceptability of "The Operation of IAL2 in the New GakuNin (Ver. 2)". After this, the following comments were then made:

- Regarding whether GakuNin's IAL2 is recognised by international standards, we are planning to discuss its overall operability with Kantara and the IGTF and will try to ensure that GakuNin's IAL2 is recognised as compatible with international standards.
- It was confirmed that it should be explicitly stated that GakuNin's IAL2, like international standards, changes with social situations.
- Although there will be a gap depending on the time of accreditation, it may be acceptable overall to make those accredited in accordance with the criteria at the time of IAL2 accreditation valid until the end of the criteria expiration date. It is necessary, however, to clarify whether these rules can be determined by us or whether there are international rules that need to be followed.
- Kantara's accreditation period is renewed annually. Currently, an IdP federation does not require as severe a response as server certificates; it is, however, necessary to prepare for the future.
- It was also proposed and approved that the "Draft Opinion on the Operation of AAL2 in the New GakuNin" should be made public to solicit a wide range of opinions.

The following agenda items were then explained and discussed:

1. Regarding the evidence to rescue orphan IDs and the operation of IDaaS, an explanation was given on the IDaaS model for collaborative research services (a mechanism to enable collaborative research with company-affiliated researchers) and how to express identity assurance (a proposal for a minimal implementation). The following comments were made:

   - I would like the working group to develop a common IDaaS service for company-affiliated researchers and university researchers, since the research infrastructure in Japan will not progress if this is not done.
   - The IAL2 with a strong affiliation to an institution will lose its eligibility at the moment a researcher transfers to a new institution; therefore, there should be a need for a common IDaaS in order to continue research smoothly.
   - The IAL2 and AAL2 has become a commodity; so, the approach should be that they are not doing anything special.
   - We would like to separate out the KYC criteria as an annex to IAL2; so, we will continue to consider this including a whitelist.

2. After an explanation was given on the progress of the authentication proxy service Orthros, the following comments were made:

   - Orthros manages who can authenticate to which SP on the basis of which institution the user is from. When creating a user on Orthros, the user can link themselves to other accounts as a means of authentication. Then, the administrator of the institution can set which SPs the user can log in to and with what status for each SP. It was also explained that SPs can also specify which level they allow access to.
   - It was suggested that Orthros be connected to the ongoing experiment conducted by the sub-working group to connect SP and IdP, and it was decided to consider this idea.

3. A status report was given on the experimental initiatives, including timelines, undertaken by the Sub-Working Group on Short-Term Initiatives.

Published Documents:

- IDaaS Model for Collaborative Research Services (A mechanism to enable collaborative research with company-affiliated researchers)
- How to Express Identity Assurance (A proposal for a minimal implementation)
- Authentication Proxy Service Orthros: A progress report (2022/03/23)
- Request for Document Re-Evaluation from the Perspective of Criteria Development and Deployment for the Construction of the Next-Generation Authentication Infrastructure (20220311)
- Draft for the Operation of IAL2 in the New GakuNin (20220225)

AAL (Authenticator Assurance Level)

This indicates the strength of the authentication process (single-factor or multi-factor authentication, authentication method) when a registered user logs in.

Lv.1 Single-factor authentication is acceptable

Lv.2 Two-factor authentication is required; software-based authentication method for the second factor is acceptable

Lv.3 Two-factor authentication is required, and the second factor of the authentication method must be hardware-based (e.g., hardware token)

CrP/CrPS (Credential Policy / Credential Practices Statement)

Operational policy and implementation procedures for handling credential information

CSP (Credential Service Provider)

This is what was previously referred to as an IdP in the NIST and KIAF documentation models, and regulates services that issue credentials, such as passwords and certificates, to users.

eduGAIN

An international federated service that interconnects research and education identity federation.

eKYC (electronic Know Your Customer)

Identity proofing procedures for service providers

FIDO (Fast IDentity Online)

One of the authentication technologies that is expected to replace traditional passwords. It is expected to become an industry standard.

IAL (Identity Assurance Level)

This indicates the rigor and strength of the identity proofing performed by the CSP (Credential Service Provider) when a user registers for a new account.

Lv.1 No identity proofing required; self-reported registration is sufficient

Lv.2 Depending on the content of the service, attributes used for identification must be verified either remotely or in person.

Lv.3 Attributes used for identification must be verified in person, and the person in charge of verifying documents must be qualified.

IDaaS (Identity as a Service)

Cloud services that manage identity

Identity assurance

Assurance of attributes

IdP (Identity Provider)

Identity management system for authentication systems

IGTF（Interoperable Global Trust Federation）

The IGTF is a body to establish common policies and guidelines that help establish interoperable, global trust relations between providers of e-Infrastructures and cyber-infrastructures, identity providers, and other qualified relying parties.

Kantara (Kantara Initiative)

An industry organisation established in the U.S. on 17 June 2009 to promote the interoperability of identity management technologies related to OpenID, SAML (security assertion markup language), and Information Card.

mAP Core (member Attribute Provider Core)

A group management function for the authentication system in the GakuNin Cloud Gateway

NIST SP 800-63

The guidelines for electronic authentication published by the U.S. National Institute of Standards and Technology (NIST) (currently in its third edition 63-3). Although it is intended for use as security measures by the U.S. government, Kantara has also updated its authentication scheme to comply with the new standard.

OpenID Connect

A protocol for linking user identity information, including authentication results

OrphanID

IDs that do not have a managing organisation or identity guarantee, such as non-GakuNin participating universities or corporate researchers.

SP (Service Provider)

The application (service) side of an authentication system

UPKI (University Public Key Infrastructure)

A nationwide joint electronic authentication infrastructure for inter-university collaboration