28-03-2022

The Working Group for Next-generation Identity Federation

Draft for the Operation of AAL2 in the New GakuNin

This document is to establish the policy for the operation of AAL2 in the new GakuNin, following the separate document “Draft for the Operation of IAL2 in the New GakuNin”. **The control target is IdPs.**

The goal of the The Working Group for Next-generation Identity Federation is to help IdPs provide strong authentication and to establish an environment in which various services such as supercomputers and research infrastructures, whose provision has been discouraged from a security perspective or done individually with complicated authentication, are made available through an authentication by IdPs. It was concluded that it would be appropriate to request IdPs who wish to participate to operate IAL2 and AAL2, which are one-step stronger standards for identify proofing and authentication necessary for this purpose, and for GakuNin to take responsibility for accreditation and operation. For the AAL2 standards, we have decided to set the standards based on NIST SP800-63 and Kantara KIAF1440 specifically. The following are our views on its operation and the proposed policy for the development of the rules. The contents consist of the following:

1. Basic policy for AAL2 operation
2. Development of GakuNin authenticator registry for evaluation of individual authenticators
3. Control of password operations
4. Control of authenticator operation (including policies on interpretation of smartphone unlocking and use of biometric data)
5. Control of authenticator life cycle
6. Relationship between CSP operational controls and user controls
7. General provisions for AAL2 operation

1. Basic policy for AAL2 operation

In KIAF 1440, the following requirements are set out for authenticators for the operation/accreditation of the AAL2.

> “A single multi-factor authenticator or a combination of password authentication with a possession-based authenticator.”

Today, there is a wide variety of authenticators released by various vendors. In terms of evaluating authenticators from a security perspective, there are those that obtain various accreditations (e.g., FIPS 140-1), those that are certified by consortia (e.g., FIDO), and those that obtain de-facto standards and take a strategy to make the adopters have no choice but to take them on board. It is difficult to evaluate every one of these operations, including operational parameters, and it would be like putting a fifth wheel on a coach to re-evaluate those that meet industry standards. In addition, if GakuNin were to establish its own standards, any discrepancy in standards should be avoided during international collaboration.

Therefore, it is efficient to focus on operational issues while actively referring to external accreditations, including industry standards, for technical issues. The operational issues include initial binding of the authenticator and user, life cycle management including expiration, and session management as part of CSP operations. It is also important to set out the controls for password authentication, which is also an important part of AAL2.

2. Development of GakuNin authenticator registry for evaluation of individual authenticators

What can be used for AAL2 is: “a single multi-factor authenticator or a combination of password authentication with a possession-based authenticator”. Many authenticators are being released and operated in the world. It is not rational to accredit the adoption of these authenticators at each participating institution. Therefore, it is desirable to investigate and accredit representative authenticators in advance. Or, if an authenticator were to be accredited at the request of a participating institution, a framework should be established to apply the results to other institutions as well.

GakuNin Authenticator Registry: GakuNin will investigate the performance of authenticators and prepare a registry of whether they can be used for AAL2 accreditation. When an authenticator is audited and accredited at the request of a participating institution, the results are registered and updated periodically for use by other institutions for accreditation.

It is appropriate that the accreditation be performed in accordance with the applicable technical standards of KIAF 1440.

When registering an authenticator with the Registry, if the authenticator in question has already been accredited by an external body, a trusted consortium, etc., the external accreditation can (and should) be actively used to speed up the accreditation process.

The strength of an authenticator depends on not only the performance of the hardware/software, but also on operational parameters, initial binding, and life cycle management including expiration. Only the results of the evaluation of hardware and software performance should be registered in the

Registry, and the remainder should be evaluated by each institution requesting accreditation. The following rules are requirements for GakuNin and not for participating institutions requesting accreditation, and are therefore treated separately from other rules.

Rule 0.1 The single-factor authenticator or single-factor authenticators that are accredited by GakuNin as suitable for use in authentication equivalent to AAL2 shall be registered in the GakuNin Authenticator Registry and to be used for AAL2 accreditation of participating institutions.
Note: Listed below are candidates for requesting information and corporation for accreditation: MS, Google, FIDO Consortium. For multi-factor authentication provided by IDaaS, it is necessary to request cooperation including accreditation under the Rule 3.x group.

The following is a list of authenticators other than passwords that are currently subject to accreditation by KIAF:
Look-Up secret/ out-of-band authenticator/ authentication using public lines/ single-factor OneTimePassword/ multi-factor OneTimePassword/ single-factor cryptographic software (Authenticator, key pair, etc.) / single-factor cryptographic device/ multi-factor cryptographic software / multi-factor cryptographic device (key pairs stored in IC cards, etc.)/

The examples of registered items for KIAF-compliant authenticators are given in a separate document.

3. Control of password operations

The password is the required authenticator to be used when AAL2 is achieved by a combination of two single-factor authenticators. The password control is essential. Therefore, special rules are set out here. The following rules comply with KIAF 1440.

Rule 1.1 When a password is used as one of the authenticators for multi-factor authentication, the following must be satisfied.

a. Password requirements:

Passwords must be at least 8 characters in the case it is set by the user, and at least 6 characters in the case it is set randomly by the system. Passwords that the system prohibits (e.g., those registered on a blacklist, etc.) must not be set.

b. Requirements for the password verification side:

The following shall be the accreditation criteria:

1. Verify the set password without restricting the length limit

2. In the case it is set by the system randomly, the randomness requirement must be satisfied.
3. No hints are given when entering passwords
4. Do not allow users to register passwords that are deemed inappropriate. When rejecting a password, the system must provide a reason for the rejection
5. Throttling must be implemented
6. If it is considered that the password has been compromised, it should be able to enforce a password change in a secure manner
7. If storing passwords, they must be "properly" cryptographically processed with respect to hashing and salt.

In KIAF 1440 (and NIST SP800-63), which forms the basis of this document, password-only authentication is prohibited when dealing with personally identifiable information (PII). In other words, it clearly states its standpoint that important information is to be protected by multi-factor authentication. Therefore, the strength required for password authentication alone cannot necessarily be considered high. It is important to correctly understand this standpoint; given that many Japanese institutions are using password authentication only, and that they are processing information containing PII, it should be emphasized that the standards set out here are not intended to prevent participating institutions setting up stronger password policies.

Note: For example, the Ministry of Internal Affairs and Communications provides a general policy on passwords below.
https://www.soumu.go.jp/main_sosiki/joho_tsusin/security/business/staff/01.html
This standard can be used as a specific standard when evaluating (b).4 above.

4. Control of authenticator operation (including policies on interpretation of smartphone unlocking and use of biometric data)

This section defines rules that include controls for the user's side operation of smartphones, which are now one of the leading devices for multi-factor authentication.

Rule 2.1 The CSP must provide instructions in advance on procedures to be followed in the event of theft or loss of the device containing the authenticator and must establish and document procedures for prompt cancellation or suspension of the authenticator in the event that such an incident should occur.
Rule 2.2 The CSP must establish a method of protection against online guessing attacks. If the authenticator has no particular mechanism, the CSP must limit the number of consecutive

authentication failures to no more than 100.

The following are the rules for communication with the verifier during the authentication process.
Rule 2.3 In the case the CSP signs the result of the authentication verification, it must use a digital signature with a strength greater than or equal to that specified in NIST SP800-131A.
Rule 2.4 In the case the CSP and the verifier are independent, communications between them must be done through mutually authenticated communication channels using approved cryptography.
Rule 2.5 In the case the CSP uses the verifier's key, the key must use an approved encryption or hash algorithms and must have a strength greater than that specified in NIST SP800-131A.

In addition, it shall be specified that PINs and biometrics for unlocking, which are typically used for smartphones and other devices, should not be considered as authentication factors. This is because the verifier cannot confirm whether or not the device has been unlocked.

Rule 2.6 In the case a physical device is used as part of the authentication, the unlocking factor of that device, in particular the PIN or biometrics for this purpose, must not be used as an authentication factor.

There are certain restrictions on the use of biometric data for authentication as defined by NIST and KIAF. Specifically, the use of biometric data is only approved as part of multi-factor authentication, and not as one of the factors in a combination of single-factor authentication. Considering that multi-factor authentication using biometric data has nevertheless become common (e.g., FIDO's biometric enrolment and its use), proof of compliance with the appropriate technical standards should be required if this is adopted. The "appropriate technical standards" refers to the U.S. standards in NIST and KIAF; if, however, a level equal to or higher than those is established in Japan, it should be followed. Currently, use of biometric data for authentication is only approved as part of a multi-factor authenticator: therefore, it is appropriate to treat it as part of the registry items for each authenticator in the accreditation of authenticators in the Authenticator Registry defined in **Rule 0.1**.

5. Control of authenticator life cycle

Authenticators require management (i.e., life cycle management) from distribution to users through renewal and expiration. This section defines the rules for this aspect and evaluates and accredits the operation of the IdP.

Rule 3.1 (Binding authenticators to users) The CSP must either distribute an authenticator to the user

at the time of user registration, or register an authenticator that has been presented by the user and approved by the CSP.
2 In the case it is done at the time of user registration, after successfully completing identity proofing, a password or at least one biometric data can be bonded online with the authenticator possessed by the user. When doing so, the CSP must verify that the authenticator is AAL2 or higher. In addition, personal information must not be disclosed to the user before AAL2 authentication has been completed.
3 In the case user registration and binding are not completed in a single physical or protected electronic session, the CSP must verify the identity of the applicant in a subsequent process by conducting the followings:

a. In the case it is done remotely, verify by issuing confidential information to a telephone number, e-mail, or postal address that has been verified in advance as belonging to the individual and with established trust as being a reliable mean to reach the individual. In this case, secret information can be issued to the authenticator only within a protected session.
b. In the case of in-person, verify using the same secret information as in a. above or the biometric data recorded in previous sessions. This shall be used only once. The secret information shall be issued to the authenticator only when the authenticator is issued in-person or distributed in a way that the applicant's address can be verified.
4 In the case of binding a new authenticator to a user or registering a new authenticator to an authenticator presented by a user, the CSP must first authenticate the user with AAL2.
5 In the case of a multi-factor authenticator, if a registrant loses all authenticators for a single factor of authentication before completing multi-factor authentication, the following must be provided as a replacement:
a. Require registrants to personally conduct identity proofing in accordance with the standards in the corresponding IAL documents in this document.
b. In the case the CSP retains evidence of the registrant's registration, it must require the registrant to authenticate to an existing account using the remaining authentication factors, if available.
c. In the case the CSP re-conducts the identity proofing by binding the password to the registrant using two physical authenticators, a confirmation code shall be issued as secret information. The issued code must be a string of at least 6 characters and digits using an approved random number generator. The code shall be valid for 7 days if posted to the registrant's registered address, and for 10 minutes otherwise.
Note: It is common for various authenticators on smartphones and PCs to be bound to smartphones by self-reporting. In order to control this operation, it is necessary to set out a process to allow initial binding and then for the IdP to verify it, and to evaluate the risk of such a process. In addition, some authenticators allow duplication of keys by users, so it is an issue how to ensure the control

(prohibition) of such duplication.

Rule 3.2 (Binding authenticators to users) The CSP must preserve all records of the authenticator bound to the account and of all important details regarding its maintenance for the duration of the life cycle of the authenticator for the duration of the defined record retention period.

Rule 3.3 (Binding authenticators to users) The CSP must maintain information on the throttling of the usage approval, if necessary.

Rule 3.4 (Binding authenticators to users) The CSP must determine the type of available user-provided authenticators and provide this information to the verifier for the decision of the AAL2.

Rule 3.5 (Binding authenticators to users) The CSP must preserve records of the authenticator bound to the account and its maintenance records for the duration of the life cycle of the authenticator for the duration of the defined record retention period.

Note: 3.2-3.5 are rules relevant to the storage of related logs.

Rule 3.6 (Binding authenticators to users) When binding a new authenticator to a user, the CSP must confirm the security level of the protocol to be bound and of the protocol providing the key.

Rule 3.7 (Binding authenticators to users) In the case of binding a multi-factor authenticator, it must be done after identity proofing has been completed, or after multi-factor authentication has already been completed.

Rule 3.8 (Lost, stolen, damaged, or unauthorised duplication) In the case where the CSP has a backup or a method of authenticating the subject using alternative authenticators, the method is confined to passwords or possession-based authenticators.

2 In the case where the CSP reserves a suspension when an authenticator compromise is reported, it must reinstate the suspension if the user is able to authenticate by other, stronger means, and furthermore, requests reactivation of the suspended authenticator.

Note: It is the standpoint of NIST and KIAF that the prohibition of “unauthorised reproduction” should not be specified in this section, but rather in the accreditation of each authenticator (Rule 0.1). Considering the actual operation, it may be necessary to set out some operational controls, especially for soft tokens.

Rule 3.9 (Revocation) In the event of the expiration of an authenticator, the CSP must not accept a request for authentication using the expired authenticator.

2 In the event of the expiration of an authenticator, the CSP must require the user to surrender or prove destruction or deletion of the physical authenticators (including any attribute certificates signed by the CSP) as soon as practical upon receipt of a new authenticator, or notice of revocation or termination.

Rule 3.10 The CSP must promptly revoke the binding of the account and authenticator and notify the user in the event of any of the following:

a. The account ceased to exist

b. The user requests revocation

c. The CSP determines that the user no longer meets the eligibility requirements

d. The CSP is obligated to do so in response to a legal instrument

2 In the event of the revocation of an authenticator, the CSP must require the user to surrender or prove the destruction of the physical authenticators (including any attribute certificates signed by the CSP) as soon as practical after the revocation or termination occurs.

6. Relationship between CSP operational controls and user controls

This section defines rules related to re-authentication.

Rule 4.1 The CSP must request re-authentication when the user's inactivity reaches 30 minutes or 12 hours after the last successful authentication regardless of status, and must terminate the session if it is not successful.

Rule 4.2 When the CSP receives a request for re-authentication from the RP, it must comply and start a new session.

Note: An RP requesting AAL2 would request re-authentication when the session inactivity period reaches 30 minutes or 12 hours after the last successful authentication regardless of activity.

Rule 4.3 The CSP must not extend the session key beyond the end of the session.

Rule 4.4 When a session is terminated due to inactivity, the CSP must require the user to enter a password or biometric data.

7. General provisions for AAL2 operation

This section defines rules related to general security and privacy protection.

Rule 5.1 Systems operating CSPs shall have adequate security measures in accordance with prevailing security standards. For example, security measures shall be at the medium level of ISMAP or FedRAMP, from which it is derived.

Note: It can be uniform government standards for security policy, or it can be the university's security policy if it refers to them. For the time being, it is important to set a policy or standards that everyone can agree on, and to show that it is being operated in accordance with them. This is the same intent as Rule 1.12 of IAL2.

Rule 5.2 The CSP shall specify the storage of various types of data to meet the requirements of various laws and regulations, and shall disclose this information to users in advance.

Rule 5.3 The CSP shall operate in accordance with laws and regulations regarding the protection of

personal information, as well as various technical standards.

Rule 5.4 The CSP shall obtain explicit user consent when using users' personal information for purposes other than authentication, fraud mitigation related to authentication, and compliance with relevant laws and regulations.

2 The CSP must not disadvantage users who do not agree with the above.