UPKI 認証連携基盤　運用ポリシー（案）

Japanese Identity Federation (UPKI-Fed) Policies and Rules of Membership (Draft1)

Introduction

The Japanese Identity Federation (UPKI-Fed) framework provides a set of rules within which Members of the Federation can exchange user information and controlled resources. The policy document ensures that all Members properly safeguard protected content and user data. An accompanying document sets forth the technical requirements for transactions.

The agreement is made and entered into by the National Institute of Informatics, responsible for operation and management of the Federation, and the Member, _____, (collectively, the Federation and Member are referred to as "parties"). This Agreement is effective as of the date signed by a duly authorized representative of Member as defined herein.

PARTICIPANT BY EXECUTING THIS AGREEMENT ACKNOWLEDGES AND AGREES THAT PARTICIPANT HAS CAREFULLY READ AND ACCEPTS THE TERMS AND CONDITIONS OF THIS AGREEMENT, AND FURTHER ACKNOWLEDGES THAT PARTICIPANT WILL BE BOUND LEGALLY BY ITS TERMS AND CONDITIONS.

1. Definitions

2. Japanese Identity Federation

In these Rules:
Attribute means End User data required by the Service Provider for access control decisions;
Data means Attributes and Metadata;
End User means any user of a Service Provider's resources or services made available under the framework of the Federation;
Identity Provider means any Member who is responsible for the Attributes or authentication provided for End Users; the System that issues those Attributes to the Federation may be operated by a third party identity provider acting as agent of the Identity Provider;
Federation means the Japanese Identity Federation;
Federation Operator means the National Institute of Informatics (NII);
Member means any organisation, institution or individual who has enrolled in the Federation;
Metadata means technical and administrative data related to the Member as described in the Technical Specifications;
Policy Board means the Policy Board for the Japanese Identity

Federation, made up of representatives of Japanese government, education and industry;
Rules means these rules as updated from time to time by the Federation
Operator pursuant to Section 11;
Service Provider means any Member who grants access to End Users to services or resources made available by that Member;
System means the Member's hardware, software and any other IT asset which is used to process the Data;
Technical Specifications means the "Technical Recommendations for Members" document located at http://wwwUPKI-Fed.or.jp/technical-recommendations.pdf as may be updated by the Federation Operator from time to time.

3. Inconsistency. In the event of any conflict or inconsistency between this document and the Technical Specifications, then this document will prevail.

4. Membership. Membership of the Federation is available to any corporation or organization legally incorporated in Japan. There is no participation fee charged at present.

5. Rules Applying to All Members. The following requirements apply for all participants in the Federation.

5.1. The Member warrants and undertakes that:

5.1.1. all and any Data, when provided to the Federation Operator or another Member (as the case may be), are accurate and up-to-date, including Metadata it may provide to the Federation;
5.1.2. it will use its reasonable endeavors to comply with the Technical Specifications;
5.1.3. it will observe good practices in relation to the configuration, operation and security of the System, particularly the management of DNS names, digital certificates and private keys;
5.1.4. it will supply the Federation with an Administrative Contact and a Technical Contact that are able to act as liaisons to the Federation and other Members.
5.1.5. in the event that Metadata must be updated, it will be done in a timely fashion and with appropriate notification of the Federation Operator.

5.2. The Member will not act in any manner which damages or is likely to damage or otherwise adversely affect the reputation of the Federation.

5.3. The Member grants the Federation Operator the right:

5.3.1. to publish and otherwise use and hold the Metadata for the purpose of administering the operation of the Federation;
5.3.2. to publish the Member's name for the purpose of promoting the Federation.

5.4. The Member must give reasonable assistance to any other Member investigating misuse. In particular, if the Member uses outsourced identity providers, it must cooperate with the identity provider to investigate and take action in respect of such misuse.

6. Rules Applying to Service Providers. The following requirements apply to any member while acting in the role of a Service Provider.

6.1. The Service Provider will only use the Attributes for the following purposes:
6.1.1. making service access control or presentation decisions and only in respect of the service for which the Attributes have been provided;
6.1.2. maintenance of a persistent local account for the End User for use by the service for which the Attributes have been provided;
6.1.3. generating aggregated anonymized usage statistics for service development and/or for other purposes agreed in writing from time to time with the Identity Provider;

6.2. The Service Provider must not disclose to third parties any Attributes supplied by Identity Providers other than to any data processor of the Service Provider or where the relevant End User has given its prior informed consent to such disclosure.

6.3. The Service Provider acknowledges that it is responsible for management of access rights to its services or resources and the Federation Operator will have no liability in respect thereof.

7. Rules for Identity Providers. The following requirements apply to any member while acting in the role of an Identity Provider.

7.1. The Identity Provider must ensure that accurate information is provided about such End Users. In particular:
7.1.1. credentials of End Users who are no longer members of the organization will be revoked promptly, or at least no Attributes asserted for such End Users to the Federation;
7.1.2. all Authentication supplied about the End User is sufficiently well performed for the reasonable requirements of a requested Service;
7.1.2.1. passwords used for authentication of End Users to Service Providers are never passed in cleartext;
7.1.3. all Attributes of the End User are sufficiently accurate for the reasonable requirements of a requested Service.
7.2. The Identity Provider acknowledges its responsibility to manage and safeguard the release of information about its End Users.
7.3. The Identity Provider should make available reliable and trustworthy information about identity management systems managed by their organization as requested by Members or the

Federation.

7.4. When using services or resources provided by Service Providers, the Identity Provider must ensure that End Users abide by the licenses or other agreements in relation to those services or resources, as well as rules and policies set by their own organization, by any Identity Provider that makes statements about them (if different from the End User's own organization), and by the network(s) they use to access those services or resources. If an End User is subject to conflicting policies then the more restrictive policy will apply.

8. Rules for Federation Operator. Federation Operator agrees to act in abidance with the following requirements.

8.1. Federation Operator will use reasonable efforts to provide periodically to Members composite metadata describing all Systems that have been registered with the Federation.

8.2. Federation Operator will make a good faith effort to confirm that all registrants are proper representatives of their organization.

8.3. Federation Operator will operate a common Discovery Service to allow End Users to identify their home organization. There is no requirement for any Service Provider to use the Discovery Service.

8.4. The Federation may rely on Certificate Authorities enumerated in the Technical Specifications and their intermediaries to identify servers through the issuance of public key material. Representatives of any Member may also provide public key material, such as an X.509 Certificate, and vouch themselves that it is representative of their System.

8.5. Agreements may be negotiated with other Federations by the Federation Operator to allow users and services in different Federations to transact within this framework. Federation Operator will inspect the policies of any and all peers and provide guidance to all Members when any such agreement is reached.

9. Data Protection & Privacy.

9.1 Any transaction between Members that involves an exchange of sensitive data, such as End User Attributes or controlled content, will involve reasonable protection as set forth in the Technical Guidelines to prevent attackers and eavesdroppers from intercepting this information.

9.2 The End User is given the right to refuse the release of any Attribute to any Service Provider, with the understanding that such refusal may also make access to the Service impossible. At all times, the Identity Provider shall make every effort to reveal as few Attributes as possible to grant access to resources.

10. Abuse. Identity Provider operators will educate their End Users about proper use of resources and respect for intellectual property.

In the event that an End User acts in violation of policies and agreements between the

organizations, the Service Provider will promptly notify the Identity Provider. The Identity Provider will investigate any alleged abuse and restrict Attributes or authentication for that user to prevent further inappropriate access and, if required, supply additional information about the End User and the transactions to the Service Provider.

11. Dispute Resolution.

In the event of any dispute or disagreement between two or more Federation Members ("Disputing Members") arising out of or pertaining to their participation in the Federation, the parties agree to make every reasonable attempt to resolve the dispute between or among themselves. In the case that such a dispute cannot be so resolved, the
Disputing Members may choose to submit the dispute to the Federation Policy Board. If the dispute is between a Federation Member and Federation and arises out of or pertains to the participation in the Federation, or the dispute is between or among Federation Members and affects the Federation, the Federation Member(s) shall submit the dispute to the Federation Policy Board. The Federation Policy Board shall resolve the dispute in the best interests of the Federation.
Member agrees that all decisions by the Federation Policy Board concerning disputes between Federation and Member shall be final.

12. Liability

12.1. ANY SERVICE PROVIDED FOR HEREIN BY THE FEDERATION, THE FEDERATION PARTICIPANTS OR ANY OF THE FEDERATION'S THIRD PARTY SERVICE PROVIDERS IS PROVIDED ON AN AS IS, AS AVAILABLE BASIS, WITHOUT WARRANTIES OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NON-INFRINGEMENT. THE FEDERATION EXPRESSLY DISCLAIMS ANY REPRESENTATION OR WARRANTY THAT ANY SERVICE WILL BE ERROR-FREE, SECURE, OR UNINTERRUPTED. NO STATEMENT, ORAL OR WRITTEN, GIVEN BY THE FEDERATION, ANY OF ITS EMPLOYEES, OR ANY OTHER PERSON WILL CREATE A WARRANTY, NOR MAY ANY PARTICIPANT OR OTHER PERSON RELY ON ANY SUCH STATEMENT FOR ANY PURPOSE. FURTHERMORE, NOTWITHSTANDING ANY CONTRARY
PROVISION SET FORTH IN THIS AGREEMENT, PARTICIPANT EXPRESSLY AGREES THAT IN NO EVENT SHALL THE FEDERATION'S ENTIRE LIABILITY FOR ANY LIABILITIES, LOSSES, CLAIMS, JUDGMENTS, DAMAGES (WHETHER DIRECT, INDIRECT, CONSEQUENTIAL, INCIDENTAL, SPECIAL OR OTHERWISE), EXPENSES OR COSTS (INCLUDING REASONABLE FEES AND EXPENSES OF COUNSEL) ARISING OUT OF THIS AGREEMENT, WHETHER IN CONTRACT, TORT OR OTHERWISE, EXCEPT FOR DIRECT DAMAGES RESULTING SOLELY FROM THE FEDERATION'S INTENTIONAL AND WILLFUL ACTIONS, EXCEED AN AMOUNT EQUAL TO 100,000 YEN.

12.2. The Federation, its third party services providers, and the Federation Members reserve the right to interrupt, suspend or reduce the provision of any service to Member, or any other person, including the Member's end users, when such action is necessary in the Federation's sole judgment. The Federation will endeavor where reasonably possible, but does not promise, to provide advance notice to Member of any such interruption, suspension, or reduction. As soon as possible following the interruption, suspension or reduction the Federation will contact the Member and any participants in an attempt to resolve any problems and restore service.

NOTWITHSTANDING ANY OTHER PROVISION HEREIN, THE FEDERATION, THE FEDERATION PARTICIPANTS, AND THE FEDERATION THIRD PARTY SERVICE PROVIDERS OR THEIR DESIGNEES SHALL NOT BE LIABLE TO PARTICIPANT OR OTHER PERSON FOR ANY ERROR IN TRANSMISSION OR LACK THEREOF OR FOR ANY INTERRUPTION OR TERMINATION OF PARTICIPATION, EITHER PARTIAL OR TOTAL, EITHER INTENTIONAL OR ACCIDENTAL (INCLUDING ANY ERROR, INTERRUPTION OR TERMINATION DUE TO THE DELIBERATE MISCONDUCT OR NEGLIGENCE OF ANY PERSON), WHETHER OR NOT PRIOR NOTICE OF ANY SUCH INTERRUPTION OR TERMINATION HAS BEEN GIVEN.

12.3. The Federation shall not be liable to any Member (or its end-users) for claims or damages caused in whole or part by (i) the fault or negligence of the Federation Members or by the failure of the Federation Members to perform their responsibilities; (ii) third party claims against the Federation Members, except to the extent that such
claims arise solely from the intentional and willful actions of the Federation; or (iii) any act or omission of any other party furnishing products or services to the Federation or the Federation Members. Furthermore, the Federation shall not be liable, either in contract, in tort or otherwise, for unauthorized access to Member's transmission
facilities, its equipment, or unauthorized access to or alteration, delay, theft or destruction of Member's (or its end users') data files, programs, procedures or other information, except for direct damages arising solely from the intentional and willful actions of the Federation.

12.4. Member is and shall be solely responsible for any or all use of any service or resource obtained as a result of participating in the Federation, including but not limited to audio, video, text, data or other communications originating or transmitted from any site owned or operated by Member, including any third party content or materials, routed to, passed through and/or stored on or otherwise transmitted or
routed to any other the Federation Member or user ("Member Content"). The Federation does not intend to review the Member Content, and Member assumes all responsibility for use of such Member Content. Member shall make no claim against the Federation regarding said Member Content. The Policy Board of the Federation or its designees, in their sole discretion, may from time to time and at any time make determinations that particular uses are not consistent with the

purposes of the federation, which determinations will be binding on Member.

12.5. Member acknowledges that the Federation does not conduct its own review or due diligence concerning the qualifications of prospective participants in the Federation, but instead relies on the promises made by the Federation Members that they will observe and abide by all operating, intellectual property, and other requirements imposed by
the Federation or the Federation Members in connection with their participation in the Federation.

13. Insurance required?
14. Termination.

14.1. This Agreement may be terminated for cause by either party for failure of the other party to comply with or to perform any term, condition, representation or covenant contained in this Agreement and such failure continues for ten (10) days after written notice from the other party thereof. Furthermore, Member's participation in the Federation may be terminated with just cause by Federation Operator or the majority vote of a quorum of the Federation Policy Board.

14.2. The Federation Operator may dissolve the Federation with no less than 3 months' notice to all Members if the Federation Operator has insufficient funding to continue operation of the Federation.

15. Rule Changes. The Federation may modify the terms of this Agreement with all Members at any time and from time to time by giving 30 days notice to any Member. The Federation will give this notice by announcing any changes to this Agreement both in email to the Member's Executive Contact and on The Federation's Web page, http://www.UPKI-Fed.or.jp/
. Each Member's participation in the Federation after the change takes effect will constitute its continuing agreement to this Agreement as so modified. Each Member has the right to terminate its participation if this Agreement is modified in any way that is not acceptable to the Member.

16. Governing Law. This Agreement shall be governed by and interpreted in accordance with the laws of Japan, and exclusive venue for any and all disputes under law or jurisprudence hereunder shall lie in the courts of Japan.

17. Notices

All notices and other communications hereunder may be delivered to Member or Federation by postal mail, email, or facsimile to the following respective addresses, unless or until otherwise notified by Member or Federation in writing to the other party:

Member Communication Administrative Contact Information

Name
Postal Address
Email Address
Telephone
Fax

Federation Contact Information
Japanese Identity Federation
c/o National Institute of Informatics

Email address: UPKI-Fed-admin@nii.ac.jp
Telephone:
Fax:

18. Execution of this Agreement

This Agreement becomes effective when signed by an officer of each party empowered to enter into legally binding contracts on behalf of their respective organizations.

Agreed to on behalf of Member by:

Signature
Date
Print Name
Title

Accepted on behalf of Federation by:

Signature
Date
Print Name
Title