UPKI 認証連携基盤 システム定義（案）

1. Introduction and References

SAML 2 Core
SAML 2 Profiles
SAML 2 Metadata

1. SAML 標準

利用する SAML 標準は下記とする。

SAML 2 Core
SAML 2 Profiles
SAML 2 Metadata

---

2. Protocol

The UPKI Federation (UPKI-Fed) supports protocols that are in wide use by its constituency and the applications they want to access with federated identity. Only protocols that are broadly supported are listed, to maximize choice of software and protocol interoperability for all members. Multiple protocols and profiles may be used. An identity providing organization should support all protocols, but a service provider need only support at least one protocol of its choice.

2. プロトコル

UPKI 認証連携基盤（仮称：UPKI-Fed）はフェデレーティッド・アイデンティティによるアクセスを利用する参加機関やアプリケーションが利用する多くのプロトコルをサポートする。全ての参加機関に連携するソフトウェアとプロトコルの選択肢を最大限とするため，広く利用されているプロトコルのみを一覧として示す。また，複数のプロトコルとプロファイルを利用可能とする。IdP 組織は全てのプロトコルをサポートするべきであり，しかし、SP は自身の選択による最低１つのプロトコルをサポートする必要がある。

3.1 Security Assertion Markup Language (SAML) V2.0

SAML V2.0 is a standard for federated identity assertions and protocols created by OASIS. The primary profile used is the Web Browser SSO Profile. The Holder-of-Key Web Browser SSO Profile is available as an alternative for client PKI authenticated transactions.

3.1 Security Assertion Markup Language (SAML) V2.0

SAML V2.0 は OASIS により策定された federated identity のアサーションとプロトコルの標準仕様である。主要なプロファイルは Web Browser SSO Profile である。 Holder-of-Key Web Browser SSO Profile は、クライアント PKI 認証のトランザクションの１つとして利用可能である。

3.1.1 Authentication Request

HTTP-bound SAML protocol AuthnRequest messages should be sent in conformance with the requirements in section 4.1.3 and 4.1.4 of the Web Browser SSO Profile.

3.1.1 認証要求

HTTP-bound SAML プロトコルの AuthnRequest メッセージは、 Web Browser SSO Profile の 4.1.3、および、4.1.4 の仕様を満足する形で送信する必要がある。

3.1.2 Authentication Response

HTTP-bound SAML protocol Response messages carrying a SAML assertion should be sent in conformance with the requirements in section 4.1.3 and 4.1.4 of the Web Browser SSO Profile. Multiple statements should be included in a single assertion when possible, and no more than one authentication statement should be present.
The response should be signed and encrypted.

3.1.2 認証応答

SAML アサーションを含む, HTTP にバインドした SAML プロトコルの応答メッセージは, Web Browser SSO Profile の 4.1.3 と 4.1.4 の仕様を満足する形で送信する必要がある。可能であれば、１つのアサーションに複数のステートメントを挿入する, ただし, 認証ステートメントは２つ以上挿入するべきではない。
応答は署名、暗号化を行うべきである。

3.1.3 Attributes

UPKI-Fed makes extensive use of attributes and considers them the primary unit of

identity. Attributes should be used by all applications as primary determinants of access.

All attributes should have unique URI names. Existing attributes that meet the semantic requirements for a deployment should always be used when possible. If no attribute is issued by other organizations should always be preferred for the same attribute. Otherwise, all participants may create new attribute names and values in URI spaces they control. Use of a URL backed by a description of the attribute is recommended.

Object classes describe sets of attributes to exchange. UPKI-Fed imposes no specific requirements for the implementation of any object classes. However, it is recommended that all participants support the x.520 person, orgPerson, and inetOrgPerson object classes, and the EDUCAUSE/Internet2 eduPerson object class. These object classes may be stored or generated in any fashion, but when sent in a SAML assertion, should be named in accordance with the MACE-Dir SAML attribute profile.

http://middleware.internet2.edu/dir/docs/draft-internet2-mace-dir-saml-attributes-latest.pdf

Some attributes may not be freely expressed, but instead restrict the set of authorities that may state them. For example, an identity provider at the University of A may not be permitted to assert that someone is a student at the University of B. UPKI-Fed may provide advice on which attributes may be asserted by providers both by restricting the scopes available to IdP's and distributing Shibboleth 2.0 policy filters. This is only guidance. SP's are responsible for verifying that all attributes they receive are issued by authorities they trust, and IdP's are responsible for not expressing attributes for which they have no authority.

Whenever possible, the user's identity should be concealed through use of transient identifiers. Persistent identifiers are used when the user must be uniquely identified across sessions, but actual identity is not necessary. Only when the user's specific real identity must be known should true identifiers be used.

3.1.3 属性

UPKI-Fed では，属性をアイデンティティの主な構成要素と考え，これを有効に利用する。属性は,全てのアプリケーションにてアクセスの主な認可判断要素として利用されるべきである。

全ての属性はユニークな URI 名を持つべきである。内容的に利用可能な既存の属性は可能な限り利用するべきである。他の組織から属性が発行されない場合は、常に同じ属性が利用されるべきである。そうでないならば、全ての参加組織は自ら管理する URI 空間内の新たな属性名､値を作成してもよい｡属性の記述により裏打ちされた URL の利用が推奨される。オブジェクトクラスは交換する属性のセットを記述する｡UPKI-Fed は特定のオブジェクト

クラスを導入する要求は行わない。しかし、全ての参加組織は x.520 の person、orgPerson、inetOrgPerson, および, EDUCAUSE/Internet2 の eduPerson オブジェクトクラスを利用することを推奨する。これらのオブジェクトクラスは任意に蓄積、生成される、しかし、SAML アサーションにより送付される時には、MACE-Dir SAML 属性プロファイルに準拠した名前を付けるべきである。

http://middleware.internet2.edu/dir/docs/draft-internet2-mace-dir-saml-attributes-latest.pdf

いくつかの属性は自由な記述はできず，特定の管理者のみが記述できるようになっている。例えば、A 大学の IdP は、ある学生が B 大学の学生であることを証明することは許可されていない。プロバイダーがどの属性を保証して良いかについて，UPKI-Fed は IdP で利用可能なスコープによる制限や，Shibboleth2.0 のポリシーフィルターを配布することでアドバイスを行う。これは単なるガイドである。SP は受信する全ての属性が信頼するオーソリティから発行されたものであることを検証する責任を持つ。また、IdP は権限を持たない属性を示さない責任を持つ。可能な場合は常に、ユーザのアイデンティティは Transient（一時的） ID を利用するべきである。Persistent（永続的）ID はユーザが複数セッションに渡りユニークに識別される必要がある場合に利用される。ただし、これは実際の ID である必要は無い。唯一、ユーザの特定な実際の識別が必要な場合のみ、本当の ID が利用されるべきである。

3.1.4 Metadata

All members of UPKI-Fed are responsible for supplying to UPKI-Fed either the metadata for all their providers or sufficient information so that UPKI-Fed is able to compile metadata on their behalf. Initially, UPKI-Fed will aggregate and host this metadata on behalf of providers. In the future, this metadata may be hosted by providers themselves and signed with certificates issued by an authority that is certified by UPKI-Fed for this purpose.

3.1.4 メタデータ

UPKI-Fed に加入する全ての参加機関は，自らが管理するメタデータ，または，メタデータ生成のために必要な情報をフェデレーションに対して提供する。
はじめはフェデレーション側で提供されたメタデータを集中して収集・管理することとなるが，その後，（フェデレーションが）信頼する認証局から発行された証明書によって署名を行ったメタデータを各エンティティ（IdP,SP）側で管理する。

3.1.4.1 URL

UPKI-Fed's metadata is available from *****.

3.1.4.1 メタデータの格納場所

UPKI-Fed のメタデータは，下記サイトからダウンロード可能とする。

3.1.5 Discovery

SP's are encouraged to perform discovery in the way that is most appropriate for their user base. UPKI-Fed provides metadata describing all IdP's in UPKI-Fed to assist SP's in this process. UPKI-Fed will also operate a SAML 2.0 compliant discovery service (DS) that can also generate Shibboleth 1.3 authentication requests when necessary. Any SP may freely use this service so long as they requested permission to do so with their metadata submission.

3.1.5 Discovery サービス

UPKI-Fed では，フェデレーションに存在する全ての IdP が記載されているメタデータをフェデレーション内で参照可能な状態にすることで，SP は最適な方法で利用者の（所属する機関の）IdP を確認することが可能となる。

また，UPKI-Fed では，必要であれば，Shibboleth1.3 認証と互換性を持った，SAML2.0 準拠の Discovery Service（以下「DS」という）として動作させることが可能である。

SP 側では，（DS に対して）メタデータの送付とともに，利用申請を行うことで，DS を自由に利用することが可能である。

---

4. Software Support

Any member may choose to use any combination of software products that fully support the protocol recommendations in Section 1. UPKI-Fed is able to provide direct technical support for any members that will install and use Shibboleth. Support for commercial products should be available from the vendor.

4.ソフトウェアサポート

参加機関は，第 1 章で推奨するプロトコルを完全にサポートするソフトウェア製品を任意の組み合わせで利用することが可能である。

なお，UPKI-Fed では，各参加機関が Shibboleth（IdP や SP）の構築・運用に関する技術サポートを提供するが，商用製品に対するサポートは提供しない。（ベンダサポートを利用するようにしてください。）

4.1. Provider Certificates

All implementations should be capable of mutual TLS authentication or XML signature for direct SOAP calls. The certificate used for TLS authentication and XML signature and encryption must be provided to UPKI-Fed, which will place it in the publicly available metadata. It can either be issued by a root certificate authority in the list below, or be independently issued with a voucher for its security given by the member itself.

4.1. サービス提供者の認証について

サービス提供者側（のアプリケーション）では，ダイレクト SOAP 接続要求に XML 署名や TLS 相互認証を実装しなくてはならない。また，TLS 相互認証，XML 署名及び暗号化に利用する証明書は，メタデータ内に記述して公開するため，UPKI-Fed に提供する必要がある。
なお，（XML 署名や TLS 相互認証を行うための）証明書は，以下のリストに掲げるルート認証局，あるいは，UPKI-Fed が信頼する認証局から発行された証明書を利用しなければならない。

4.1.1. Trusted Provider CA's

UPKI Open-Domain Certificate Authority

4.1.1. 信頼する認証局

UPKI オープンドメイン認証局

4.2. Distributed Metadata Signature Certificates

UPKI-Fed may also separately support the signature of metadata by members themselves. The certificate used to compute the signature of the metadata itself, as opposed to the certificate within the metadata, must be issued by a narrower set of certificate authorities.

4.2. メタデータへの署名証明書

UPKI-Fed では，フェデレーションの参加機関が自己署名したメタデータについても取り扱うことが可能である。しかし，メタデータ自身に署名するために利用する証明書については，逆に，限られた（信頼された）認証局から発行された証明書を利用しなくてはならない。

4.2.1. Trusted Metadata CA's

UPKI Open-Domain Certificate Authority

4.2.1 メタデータの署名に利用する認証局

UPKI オープンドメイン認証局

4.2.2. UPKI-Fed's Signing Certificate URL

The certificate used to sign the metadata is available from
https://xxx.xxx.ac.jp/metadata/UPKI-Fed-signing.pem

4.2.2. UPKI-Fed 署名用証明書の URL

UPKI-Fed が利用する署名用の証明書は，次の URL からダウンロード可能とする。
https://xxx.xxx.ac.jp/metadata/UPKI-Fed-signing.pem

4.2.3. UPKI-Fed's Signing Certificate Fingerprint

The MD5/SHA-1 fingerprint of the certificate used by UPKI-Fed for signing is AA:AA:AA:AA:AA:AA:AA:AA:AA:AA.

4.2.3. UPKI-Fed 署名用証明書フィンガープリント

UPKI-Fed で利用される署名用証明書の MD5 または SHA-1 は以下とする。
【M D 5】AA:AA:AA:AA:AA:AA:AA:AA
【SHA-1】AA:AA:AA:AA:AA:AA:AA:AA

4.3. Compromise of Private Key

In the event that there is a compromise of the private key used for signing of metadata, the accompanying certificate will be revoked and a new key and certificate will be acquired. All members will be promptly notified at both their administrative and technical contacts and this document will be updated.

4.3. 秘密鍵の危殆化

メタデータに利用する署名用の証明書の秘密鍵が危殆化した場合には，関連する証明書を全て無効化するとともに，（新しい鍵ペアにより）証明書を再発行する。
その旨は，直ちにフェデレーション管理者及び技術担当者の両方に通知するとともに，必要なドキュメントについて更新を行う必要がある。

---

5. Identifier Recycling & Lifetime

When a user is no longer associated with an assigned identifier at an IdP, the IdP should make every effort to inform all SP's that may have persisted accounts using

that identifier. Once an identifier is no longer in use, it must not be reallocated within 24 months of this final use. Persistent identifiers should never be reallocated. They may be either programmatically assigned and stored in a database, or generated using an algorithm sufficiently unlikely to result in any collision.

5. ID 管理のライフサイクル

利用者に割り当てた ID の有効期間が切れた場合（利用者側で ID を利用しなくなった場合）には，当該 IdP では，その ID を課金管理等に利用しているかもしれない他の IdP に対して，その旨を通知できるような仕組みになっていなくてはならない。
また，（利用しなくなった）当該 ID については，最終利用時から 24 ヶ月（2 年）間は再利用を禁止する。また，“ Persistent ID ”については，決して再利用されないように注意する必要がある。。例えば，プログラム上で（誤って）割り当ててデータベースに格納してしまったり，コリジョンが起こりそうもないアルゴリズムを利用して生成されてしまったりすることもある（ため注意が必要である）。

---

6. Rules for Services

Any entity that operates within UPKI-Fed as a service should follow these guidelines to ensure that private and sensitive user data is not abused or lost.

6.サービスのルール

UPKI-Fed で，サービスを提供する全てのエンティティは，本ガイドラインに従い，利用者の（取扱注意データを含む）個人情報の不正利用や紛失等に注意するべきである。

6.1. Minimum Profile Support

Any implementation of software used by services should support one or more of the profiles described in section 3.

6.1. 最小限サポートするプロファイル

サービス提供者側（のアプリケーション）では，第 3 章に掲載されたプロファイルについて，最低でも 1 つ以上のプロファイルについてサポートするべきである。

6.1.1. Attribute Requirements

All services need to submit their attribute requirements to UPKI-Fed. A service may describe an attribute as required, desired, or optional. UPKI-Fed will aggregate these attribute requirements and make them publicly available to assist identity providers in determining release policies.

6.1.1. 要求される属性

（全てのサービス提供側は）各サービスを利用する際に，必要となる属性及び当該属性の“必須”，“推奨”，“任意”の種別について（フェデレーションに）情報提供すること。UPKI-Fedでは，IdP側で情報公開ポリシーを決定できるように，サービスと要求される属性情報のマトリクスを参照可能としておくこととする。

6.1.2. Maintenance of User Information

User information should not be stored unless necessary for the provision of services, in which case the minimum required should be retained. This maximizes privacy and the freshness of attributes, while minimizing the risk of accidental exposure.

6.1.2. 利用者情報の維持管理

（各サービス提供側では）利用者情報について，個人情報の保護及び情報の最新性を担保するとともに情報漏えいのリスクを最小化するため，サービスのプロビジョニング等，必要最小限の場合を除き保持しないこととする。

6.1.3. Log Retention

Services must maintain log information on access to their services for a minimum of three months in accordance with Japanese law.

6.1.3. ログの保管

サービスへのアクセスログは最低でも3ケ月間保管しなければならない。
（国内の法律に従った検討が必要。）

6.2. Rules for End User Organizations

End user organizations must always bear in mind that they hold great responsibility in a federated identity system. They are obligated to protect user information from improper disclosure, and services depend on them for accurate information to make informed access control decisions. Technical implementation choices allow end user organizations to meet this responsibility.

6.2. 利用者組織の規程

UPKI-Fedの参加機関は，各々が協力して認証連携を実現していくのである（IdPの認証連携に対して責任を持たなければならない）ということを常に認識していなければならない。例えば，利用者情報を不適切な公開から保護するとともに，（IdPとの認証連携に依存する）各

サービスが正確にアクセス制御の判断が可能なように取り計らわなければならない。
実装の際には特にこの点に注意することが必要である。（実装の自由度と責任）

6.2.1. Minimum Profile Support

Any implementation of software used by end user organizations should support all of the profiles described in section 3.

6.2.1. サポートされるべきプロファイル

利用者が利用するアプリケーションにおいては，セクション 3 に記載する全てのプロファイルをサポートするべきである。

6.2.2. Log Retention

Logs that record all transactions with all services must be maintained by any end user organization. These logs should be maintained for at least one year. The logs should include:

1) A timestamp recording the date and time of the transaction;
2) The principal about which attributes are asserted;
3) All attributes asserted.

6.2.2. ログの保管

各利用機関では，エンドユーザが利用する全てのサービスに対して，以下の項目を含むトランザクションログを取得するとともに，少なくとも 1 年間は保管すべきこととする。

1) 処理の発生した日時を示すタイムスタンプ
2) 認証認可された主体
3) 認証認可に利用された属性

以上