NIST SP 800-63C

- Federation and Assertions -

Nov Matake

Nov Matake

- OpenID Foundation Japan
  - 事務局長
  - エバンジェリスト
  - 翻訳 WG リーダー
- #idcon 主催
- OAuth.jp 管理人
- YAuth.jp LLC 代表

800-63-3 より抜粋

Federation Assurance Level (FAL)

- Federation を利用する場合のみ関係してくる Assurance Level
  - Federation における Assertion / Artifact の利用形態に関する要件を示す
- Lv.1
  - Assertion への署名が必須
- Lv.2
  - Lv1 に加えて RP のみが複合可能な形で Assertion の暗号化が必須
- Lv.3
  - Lv.2 に加えて Holder-of-Key Assertion の利用が必須 (Proof-of-Posession)
  - Subscriber が所持する鍵と Assertion が含む鍵の参照の紐付け検証が必須

Terms

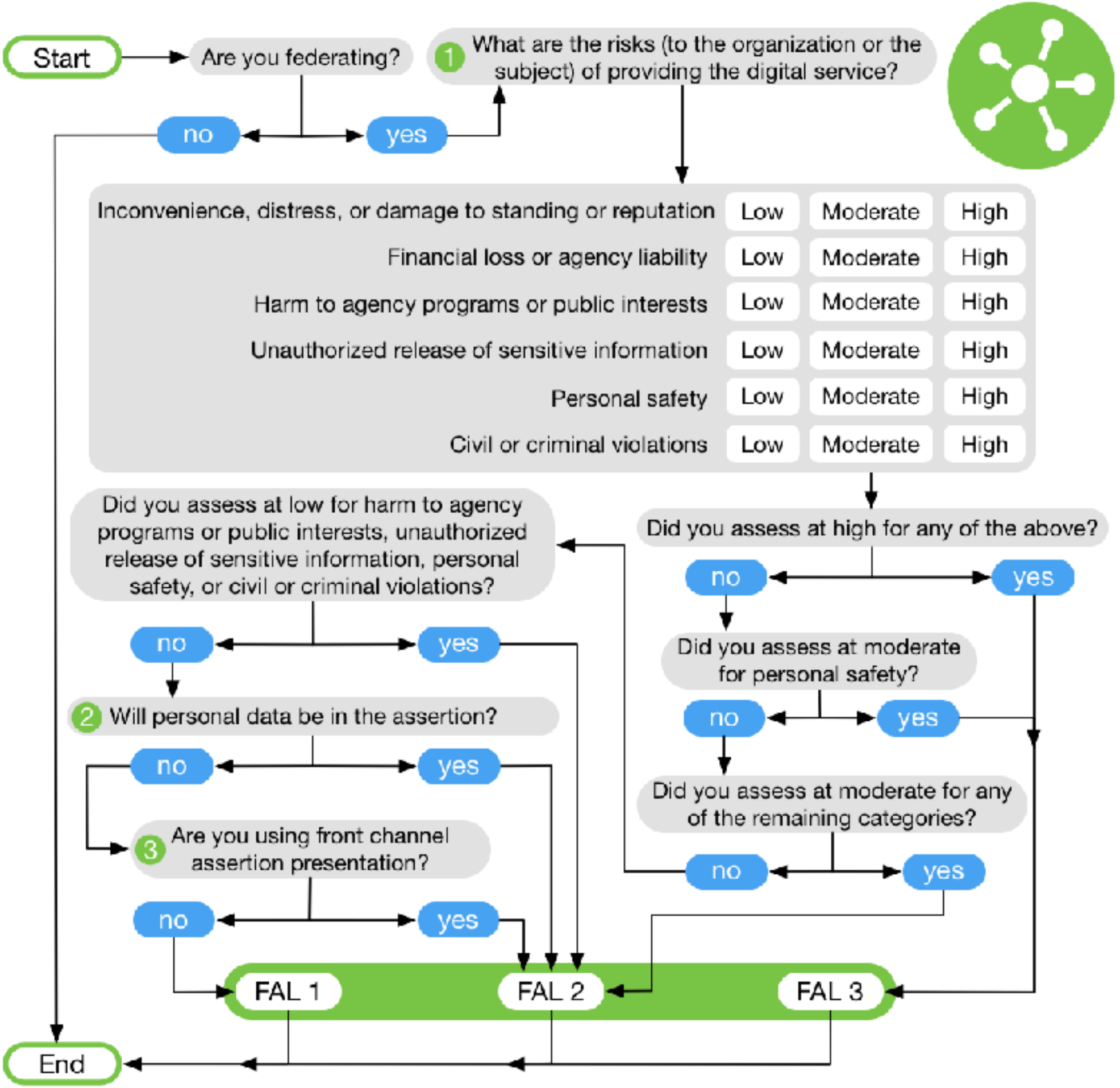
- Approved Cryptography
  - FIPS 承認 or NIST Recommendation 指定/採用
  - Assertion の署名 / 暗号化に用いるアルゴリズムを指定
- Assertion
  - IdP 上での Authentication Event および Subscriber Attribute の情報を含むひとかたまりのデータ
  - e.g., OIDC ID Token / SAML Assertion
- Assertion Reference (Artifact)
  - e.g., Authorization Code / SAML Artifact

ref.) 800-63-3 Appendix A

Terms

- Attribute Value
  - 完全な属性値
  - e.g., 1981.12.13 生まれ
- Attribute Reference (Attribute Claim)
  - ある程度まるめられた (?) 属性値
  - e.g., 18歳以上, 12月生まれ
- Pairwise Pseudonymous Identifier (PPID)
  - IdP-RP ペアごとに固有かつ推測不可能な仮名識別子

ref.) 800-63-3 Appendix A


Start
Are you federating?
no
yes
1 What are the risks (to the organization or the subject) of providing the digital service?
Inconvenience, distress, or damage to standing or reputation
Financial loss or agency liability
Harm to agency programs or public interests
Unauthorized release of sensitive information
Personal safety
Civil or criminal violations
Low
Moderate
High
Did you assess at low for harm to agency programs or public interests, unauthorized release of sensitive information, personal safety, or civil or criminal violations?
Did you assess at high for any of the above?
Did you assess at moderate for personal safety?
Did you assess at moderate for any of the remaining categories?
2 Will personal data be in the assertion?
3 Are you using front channel assertion presentation?
FAL 1
FAL 2
FAL 3
End

800-63-3 を読んだ時点で

すでに FAL は選択済...なはず

800-63C では各 FAL における要件を定義

...はそれほどしてない...

Requirements for FAL 1-3

FAL	Assertion	Signing	Encryption
Lv.1	Bearer	Required	Not Required
Lv.2	Bearer	Required	Required
Lv.3	Holder-of-Key	Required	Required

大部分は代表的実装パターンと
パターンごとの要件をまとめたもの
(FAL とは無関係)

Section Name	Normative/Informative
1. Purpose	Informative
2. Introduction	Informative
3. Definitions and Abbreviations	Informative
4. Federation Assurance Level (FAL)	**Normative**
5. Federation	**Normative**
6. Assertion	**Normative**
7. Assertion Presentation	**Normative**
8. Security	Informative
9. Privacy Considerations	Informative
10. Usability Considerations	Informative
11. Examples	Informative
12. References	Informative

4. FAL

- FAL1 - 3 までの定義
- Key Management
  - IdP の鍵ペアは全 RP 向けに共通でもいい
  - RP と IdP の共通鍵は RP ごとに個別に発行
- Runtime Decisions
  - White List / Black List / Gray List
    - 同意スキップ可能 / RP 利用禁止 / 同意必須
  - 同意の解除機能必須

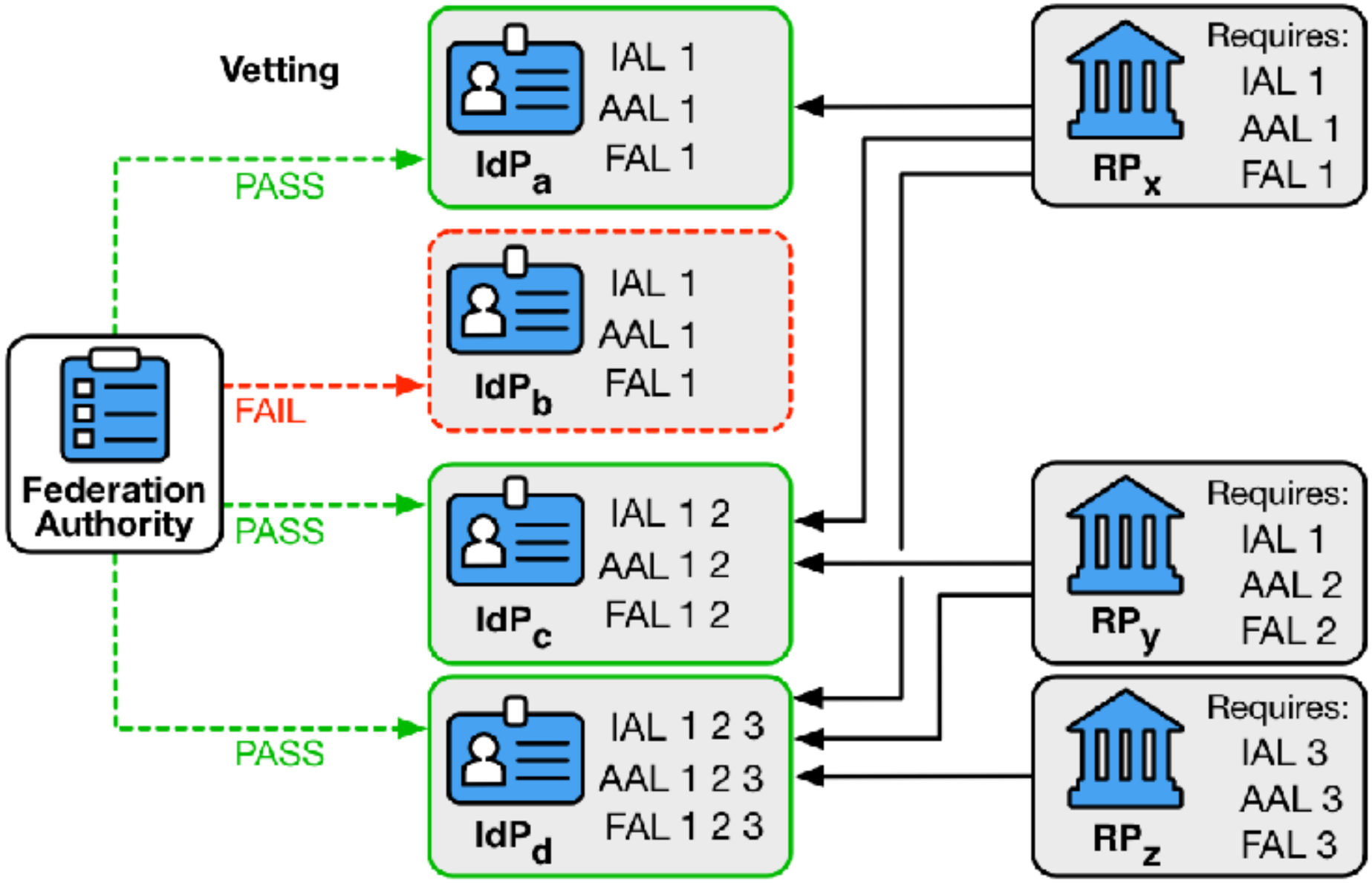
5. Federation

- Manual Registration
- Dynamic Registration
- Federation Authority
  - Trust Framework Provider などの Authority による審査を通過すれば参加可能なモデル
- Proxied Federation
  - IdP と RP の間に Proxy (Broker) が介在するモデル

Manual Reg. v.s. Dynamic Reg.

- Manual Registration
  - White List を運用可能
  - White Listed RP にはユーザー同意をスキップ可能
- Dynamic Registration
  - White List は運用不可
  - 必ずユーザーの同意が必要

Federation Authority



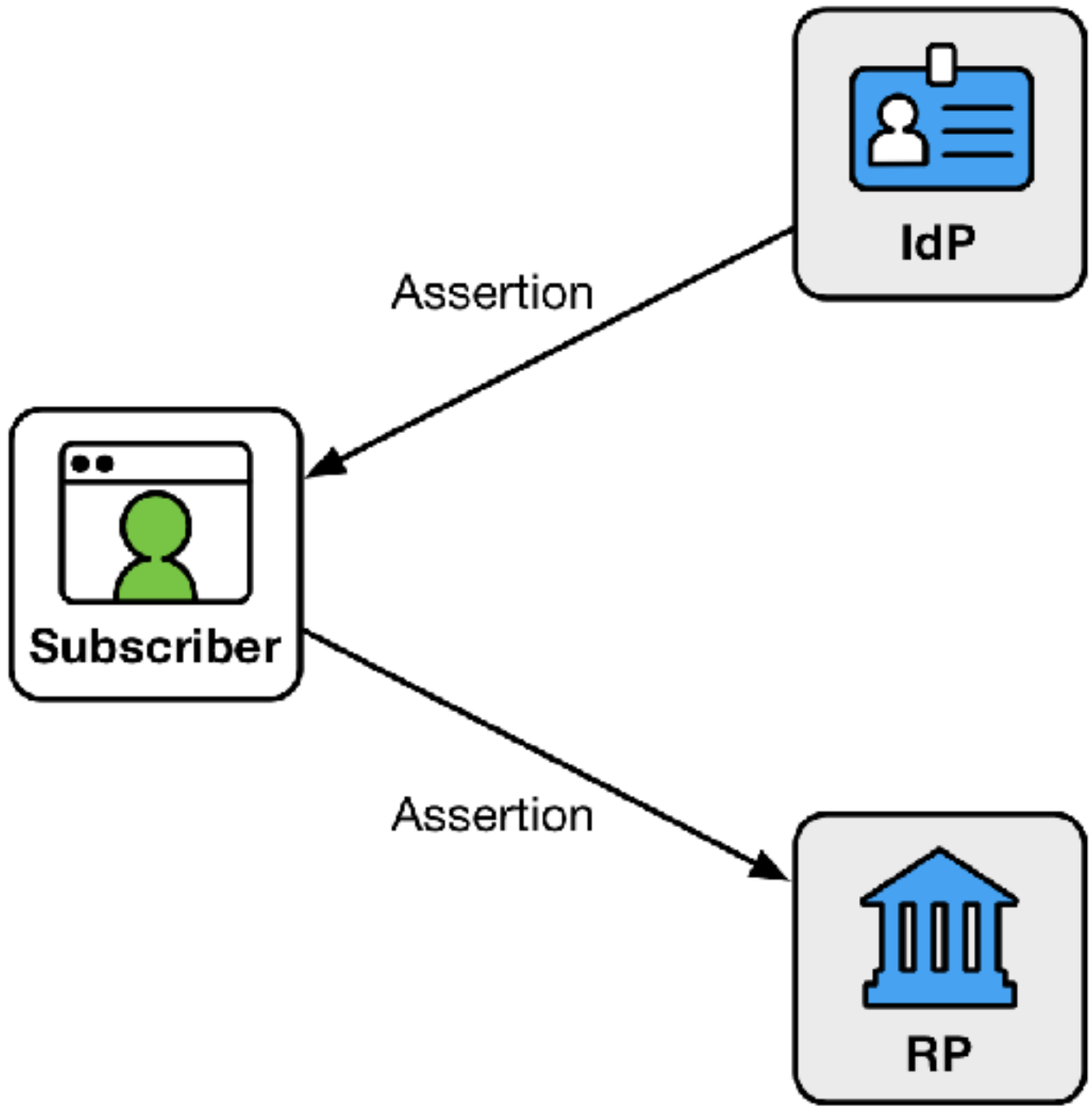
Proxied Federation

- ❖ 末端の IdP と RP がお互いを知らなくてもいい
  - ❖ IdP によるトラッキングを抑止する効果
    - ❖ PPID の生成は難しい
- ❖ Proxy には IdP と RP 両方の働きが求められる
  - ❖ IdP と RP 両方の要件が課される

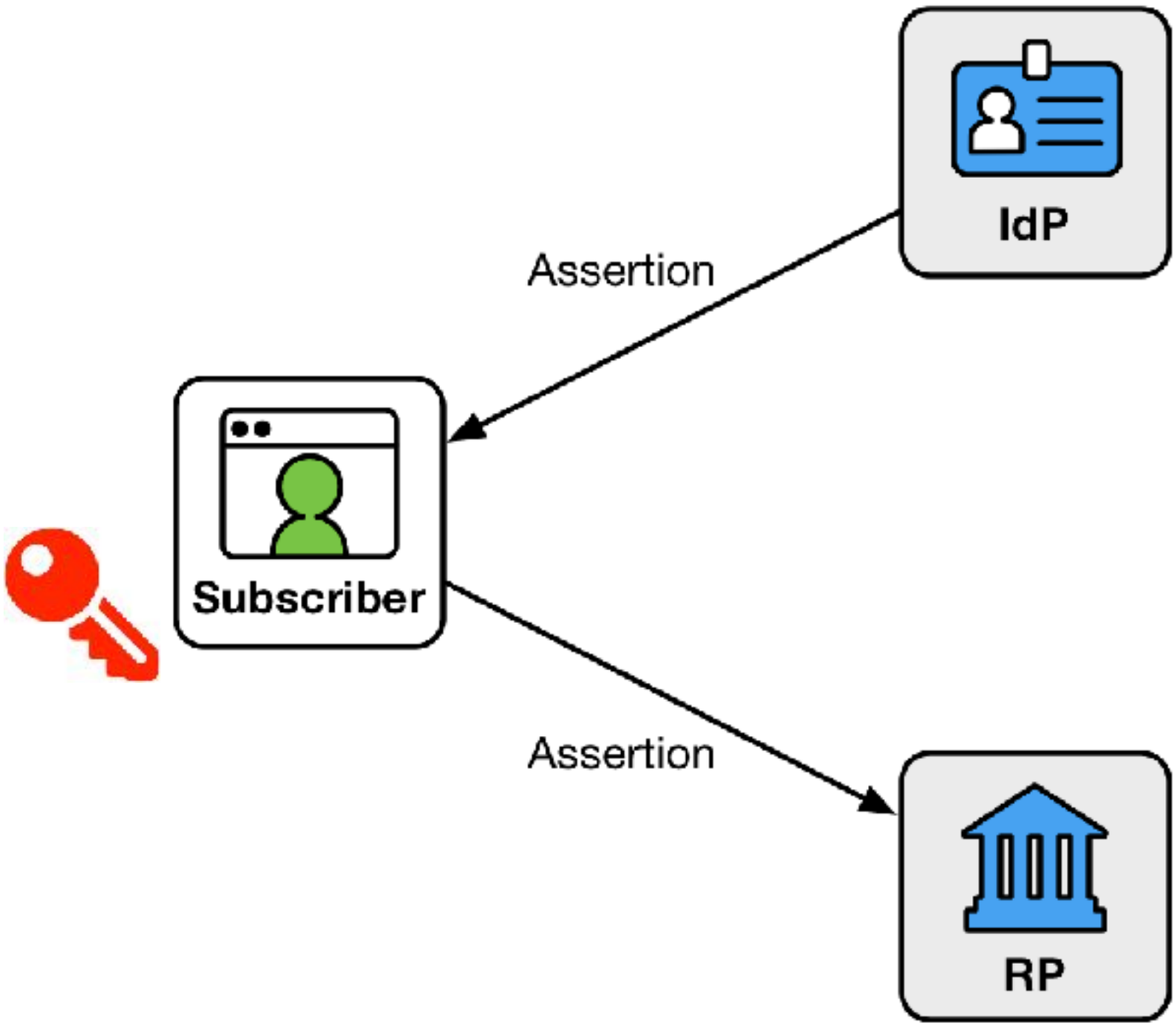
6. Assertion

- Common Metadata
  - Subject, Issuer, Audience, 発行日時, 有効期限, 署名 etc.
  - IAL と AAL も含めることを推奨
- Assertion Bindings
  - Bearer
  - Holder-of-Key (Proof-of-Possession)
- Assertion Protection
  - 署名, 暗号化, Audience Restriction, PPID etc.

Bearer v.s. Holder-of-Key



Bearer v.s. Holder-of-Key



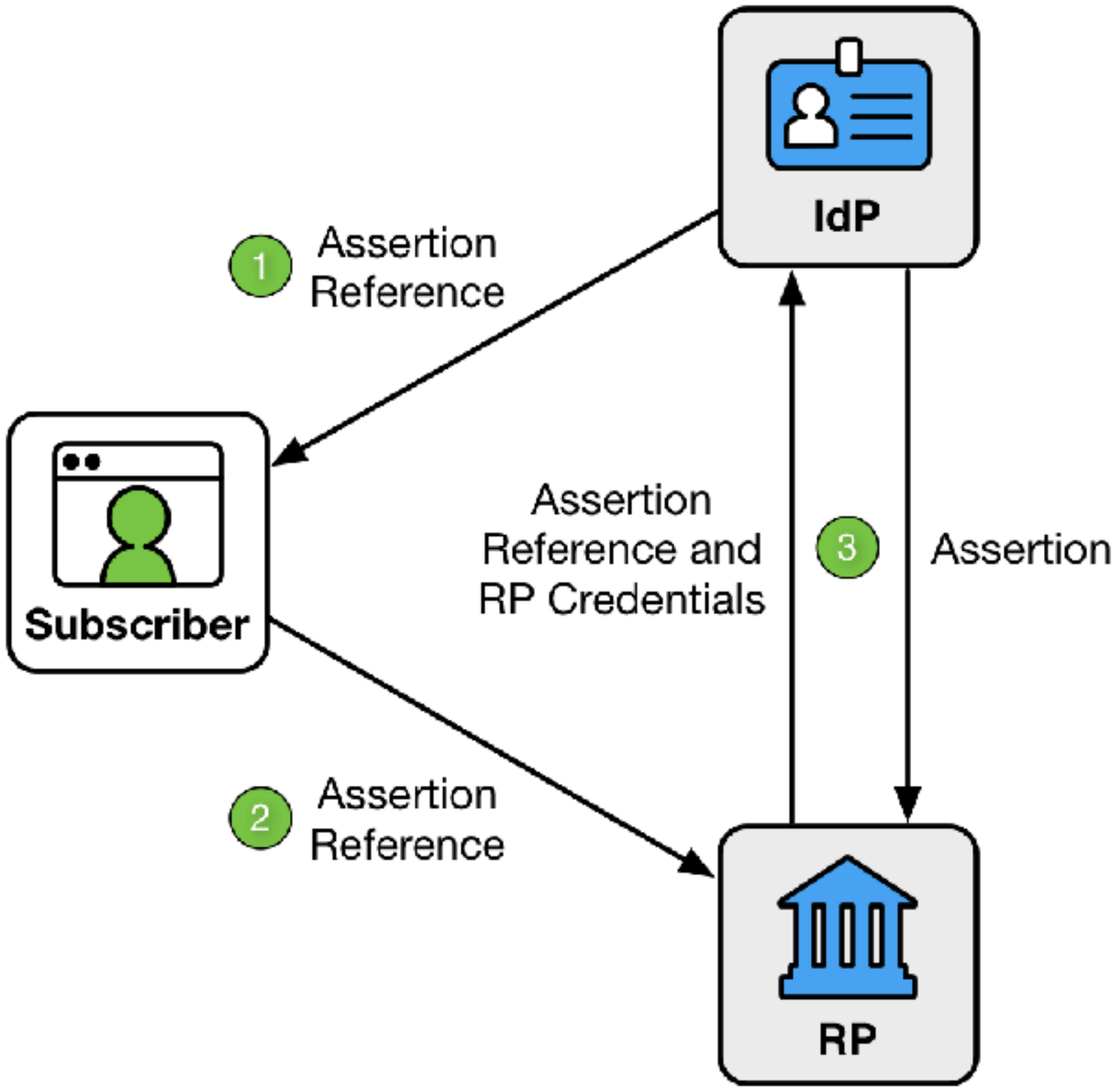
Holder-of-Key

- [RFC 7800] Proof-of-Possession Key Semantics for JWTs
  - https://tools.ietf.org/html/rfc7800
- [draft] OpenID Connect Token Bound Authentication 1.0
  - http://openid.net/specs/openid-connect-token-bound-authentication-1_0.html
- SAML V2.0 Holder-of-Key Web Browser SSO Profile
  - http://docs.oasis-open.org/security/saml/Post2.0/sstc-saml-holder-of-key-browser-sso.html

7. Assertion Presentation

- Back-Channel Presentation
  - ブラウザには Assertion Reference (Artifact) が渡る
  - Back-Channel で Artifact と Assertion を交換
    - e.g.,) OpenID Connect の Code Flow
- Front-Channel Presentation
  - ブラウザーに直接 Assertion が渡る
  - e.g.,) OpenID Connect の Implicit Flow

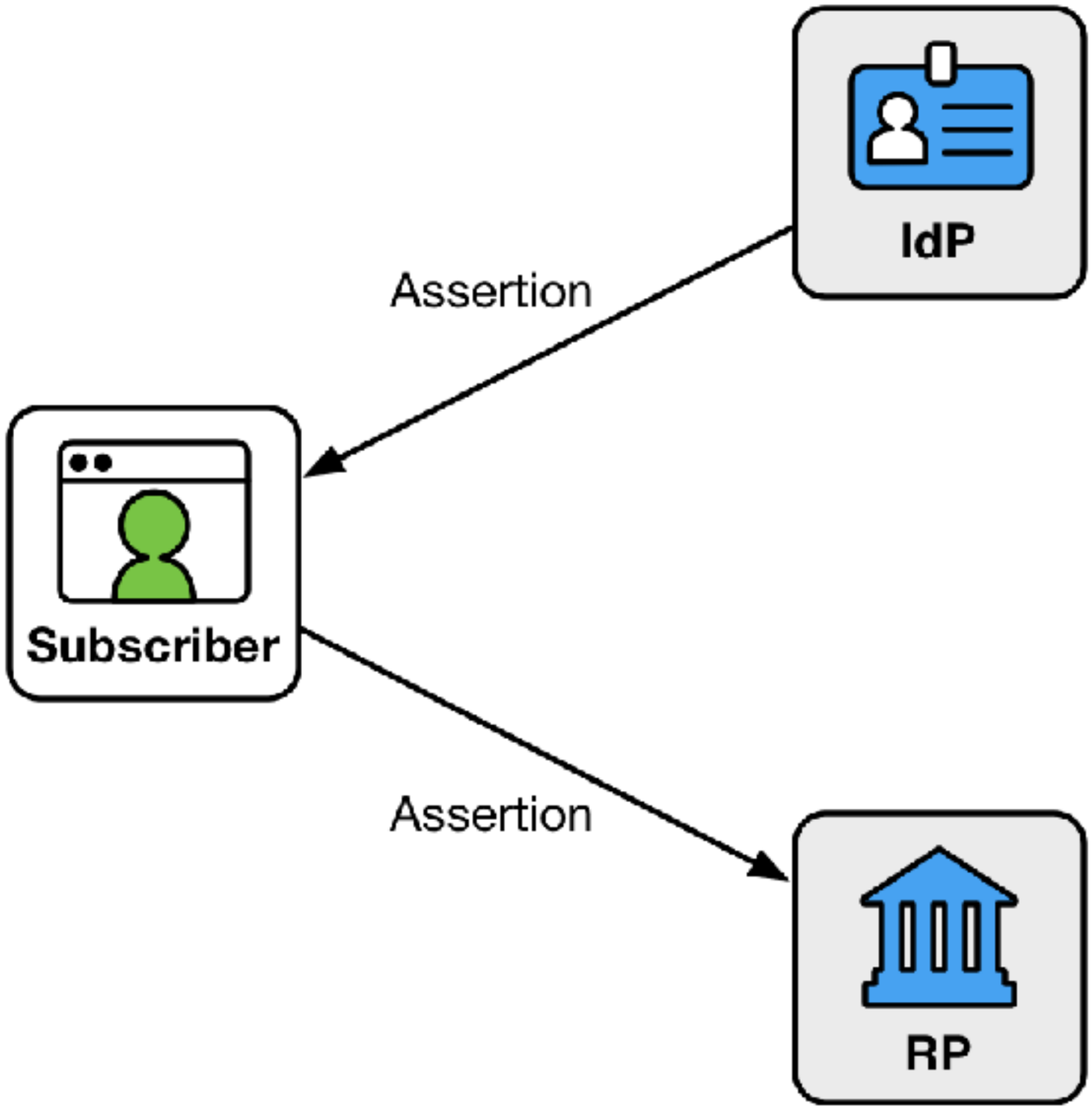
Back-Channel Presentation



Back-Channel Presentation

- Assertion Reference
  - 特定の RP 以外には利用不可な仕組み必須
  - ワンタイム性必須
    - 有効期間は数秒〜数分程度を推奨
    - RP Authentication の実施を推奨
- Channel
  - Authenticated Protected Channel 必須 (e.g., TLS)

Front-Channel Presentation



Front-Channel Presentation

- Assertion
  - 暗号化必須 (= FAL2 以上が必須)
    - “素の” OpenID Connect Implicit Flow は利用不可
- Channel
  - Authenticated Protected Channel 必須 (e.g., TLS)

Protecting Information

- Authenticated Protected Channel (e.g., TLS) 必須
  - IdP <-> RP
  - IdP <-> End-User
  - RP <-> End-User
- API による Attribute へのアクセスの許容
  - UserInfo API 使ってもいいよ
- 可能な限り Attribute Reference を活用すること
  - 「18歳以上」のみでよければ生年月日まで要求するな

素の OpenID Connect / SAML
で対応可能か？

今後 OpenID Connect と SAML
それぞれで Profile 作成が進む？

63C はリクエストへの署名には
言及しないがそれでいいのか？