NIST SP 800-63-3

- Digital Identity Guidelines -

Nov Matake

OpenID

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

NIST SP 800-63-3 Draft 版翻訳

- 2016年7月～11月
  - NIST SP 800-63-3 Draft 版の翻訳
- 2016年11月1日
  - #idcon vol.22 - NIST SP 800-63-3 分割、補完関係へ。
  - https://idcon.connpass.com/event/40861/

NIST SP 800-63-3 Final 公開 @ CIS 2017

Digital Identity Guidelines: Now Available

June 22, 2017

The finalized four-volume SP 800-63 *Digital Identity Guidelines* document suite is now available, both in PDF format and online.

The Trusted Identities Group (TIG) thanks all that contributed to the development of these documents.

PDF versions of the documents are available from:

Document	Title	URL
SP 800-63-3	Digital Identity Guidelines	https://doi.org/10.6028/NIST.SP.800-63-3
SP 800-63A	Enrollment and Identity Proofing	https://doi.org/10.6028/NIST.SP.800-63a
SP 800-63B	Authentication and Lifecycle Management	https://doi.org/10.6028/NIST.SP.800-63b
SP 800-63C	Federation and Assertions	https://doi.org/10.6028/NIST.SP.800-63c

Links to the online version of the SP 800-63 suite are below.

SP 800-63-3
Digital Identity Guidelines

SP 800-63A
Enrollment & Identity Proofing

SP 800-63B
Authentication & Lifecycle Management

SP 800-63C
Federation & Assertions

https://pages.nist.gov/800-63-3/

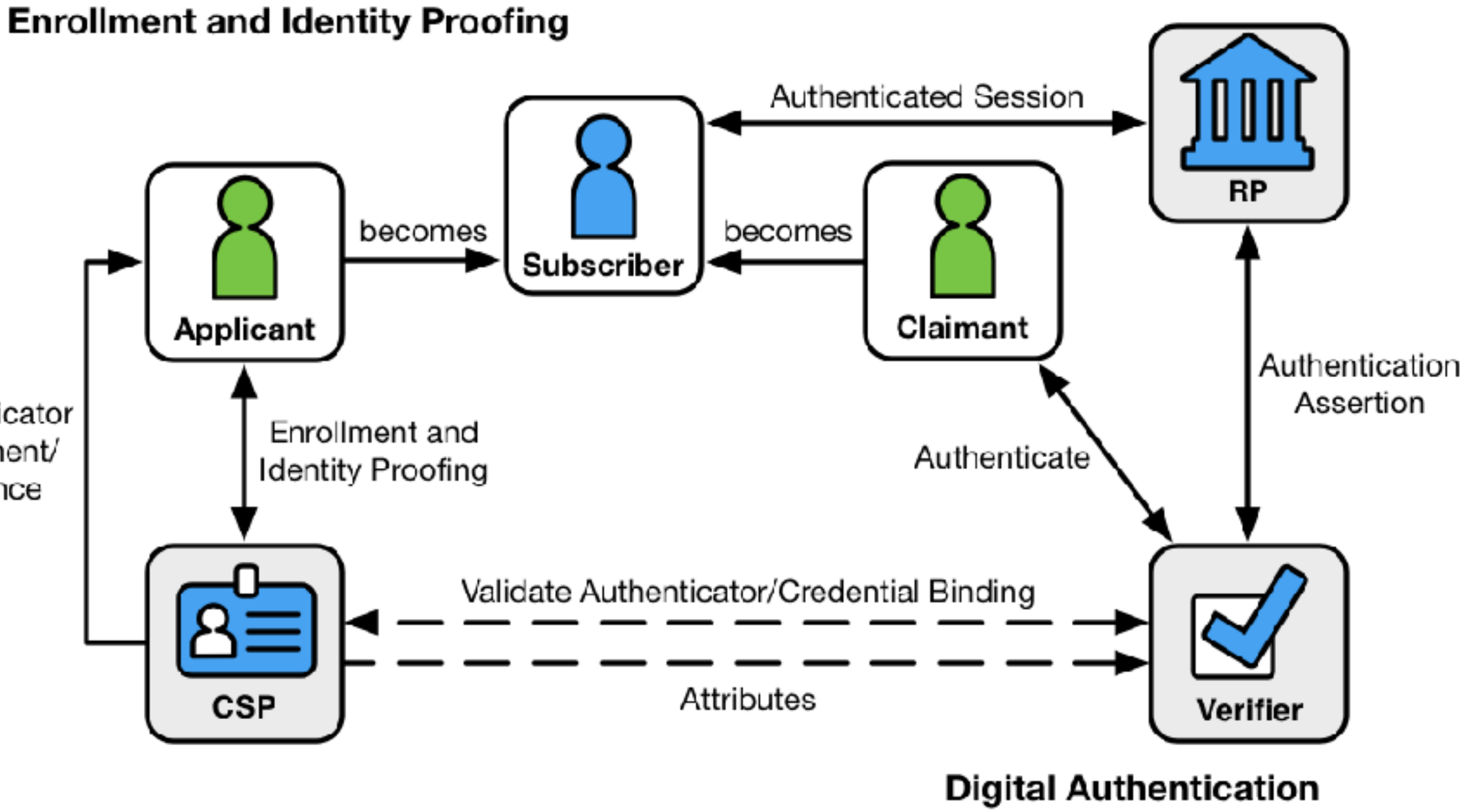
“US 政府機関向けの”
Digital Authentication 実装ガイドライン

US 政府機関以外が参考に “してもよい”

ここに来ているみなさんに向けて
書かれたドキュメントではない

...が、参考になるかもしれない。

Digital Identity Model



SP 800-63-2 までとの違い

- SP 800-63-2
  - Level of Assurance (LOA) を1つのスカラー値として定義
  - LOA 1-4 の各レベルでの要件をカテゴリーごとに列挙
- SP 800-63-3
  - LOA に代わって3つの Assurance Level を定義
  - 各 Assurance Level ごとにサブドキュメント化

3つの Assurance Level

- Identity Assurance Level (IAL)
  - Identity Proofing Process の強度を示す
- Authenticator Assurance Level (AAL)
  - Authentication Process の強度を示す
- Federation Assurance Level (FAL)
  - Federation に用いる Assertion Protocol の強度を示す
- 各 Assurance Level の詳細な要件はサブドキュメント化
  - IAL=63A / AAL=63B / FAL=63C

SP 800-63-3 全体構成

- 4つのドキュメントによって構成される
  - SP 800-63-3 ~ Digital **Identity** Guidelines ~
  - SP 800-63A ~ Enrollment & Identity Proofing ~
  - SP 800-63B ~ Authentication & Lifecycle Management ~
  - SP 800-63C ~ Federation & Assertions ~
- 今後各ドキュメントは **“非同期に”** 改訂される
  - 各ドキュメントの最新版を組み合わせて利用する

LOA は無くなりました

LOA のことは忘れましょう

Why not LOA?

- LOA はスカラー
- Multi-factor Authentication (MFA) を要件とすると...
  - LOA2 以上が必要になり...
    - LOA2 での Identity Proofing が必要！
- Pseudonymity を確保したければ...
  - LOA1 以下が必要になり...
  - MFA を要件にできない！

SP 800-63-2 以前

ヘルスケア情報のトラッキングサービス

↓

ユーザーは Pseudonym な状態のまま

MFA を必須にしたい

↓

Identity Proofing を不要にしたければ LOA1

LOA1 では MFA を必須にできない

SP 800-63-3 以降

ヘルスケア情報のトラッキングサービス

↓

ユーザーは Pseudonym な状態のまま

MFA を必須にしたい

↓

Identity Proofing が不要なので IAL 1

MFA 必須なので AAL 2 を採用

IAL, AAL, FAL の概要

Identity Assurance Level (IAL)

- Identity Proofing Process の強度を示す Assurance Level
- Lv.1
  - Identity Proofing は不要
  - Self-asserted Attribute のみで OK
- Lv.2
  - 識別に用いられる Attribute に関して Remote もしくは対面での Identity Proofing が必要
- Lv.3
  - 識別に用いられる Attribute に関して対面での Identity Proofing が必要
  - Identity Document 検証の担当者は要資格

Authenticator Assurance Level (AAL)

- Authentication Process の強度を示す Assurance Level
  - 各種 Authenticator の強度およびその利用方法を定める
- Lv.1
  - Single Factor Authentication で OK
- Lv.2
  - Two Factor Authentication が必要
  - 2要素目に利用する Authenticator は Software ベースのもので OK
- Lv.3
  - Hardware ベースの Authenticator を用いた Two Factor Authentication が必要

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

各機関ごとに Risk Assessment を行い
最適な IAL, AAL, FAL を選択すること

Start

1 To provide the service, do you need any personal information?

no

yes

2 To complete the transaction, do you need the information to be validated?

no

yes or I don't know

3 What are the risks (to the organization or the subject) of providing the digital service?

Inconvenience, distress, or damage to standing or reputation	Low	Moderate	High
Financial loss or agency liability	Low	Moderate	High
Harm to agency programs or public interests	Low	Moderate	High
Unauthorized release of sensitive information	Low	Moderate	High
Personal safety	Low	Moderate	High
Civil or criminal violations	Low	Moderate	High

Did you assess at high for any of the above?

no

yes

Did you assess at moderate for personal safety?

no

yes

Did you assess at moderate for any of the remaining categories?

no

yes

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?

no

yes

IAL 1

IAL 2

IAL 3

4 Do you need to resolve an identity uniquely?

yes

no

5 Can you accept references?

no

yes

End

6 Use references if you can complete the transaction or offer the service without complete attribute values.

See federation recommendations.

Start

1 What are the risks (to the organization or the subject) of providing the digital service?

Inconvenience, distress, or damage to standing or reputation	Low	Moderate	High
Financial loss or agency liability	Low	Moderate	High
Harm to agency programs or public interests	Low	Moderate	High
Unauthorized release of sensitive information	Low	Moderate	High
Personal safety	Low	Moderate	High
Civil or criminal violations	Low	Moderate	High

Did you assess at high for any of the above?

no → Did you assess at moderate for personal safety?

no → Did you assess at moderate for any of the remaining categories?

no → 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?

no → 2 Are you making personal data accessible?

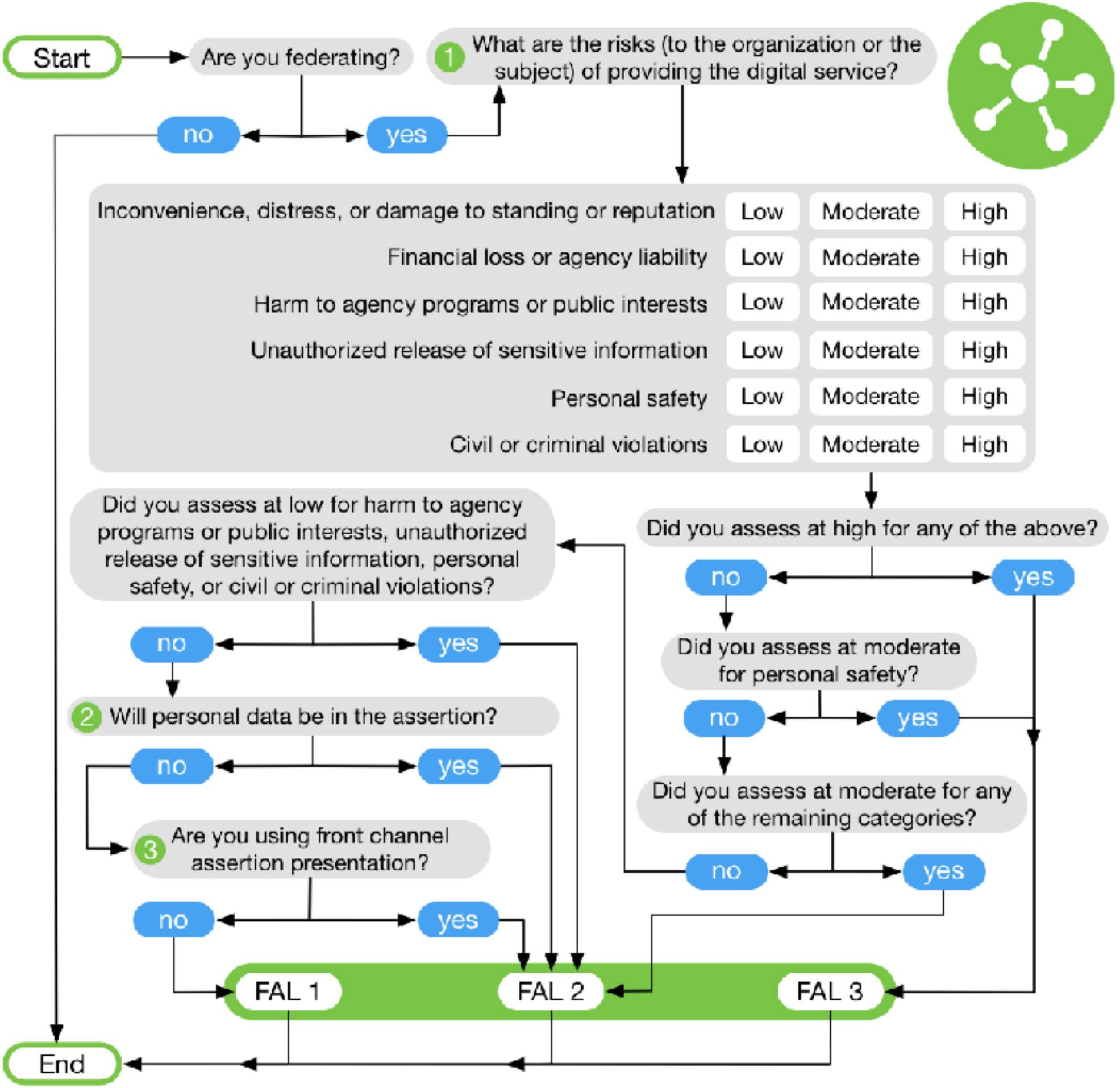
no → AAL 1

yes → AAL 2

yes → AAL 3

End

See federation recommendations.


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

IAL, AAL, FAL の各レベル選定

↓

各 Assurance Level の当該レベルに

対する要件を確認

↓

要件を満たす実装を

“US 政府機関向けの”
Digital Authentication 実装ガイドライン

US 政府機関以外が参考に “してもよい”

まずは Risk Assessment を実施すること

できるのか？