資料2

令和5年度
本人確認ガイドラインの改定に向けた有識者会議
論点協議資料（第5回分）

令和6年2月　　トラストタスクフォース

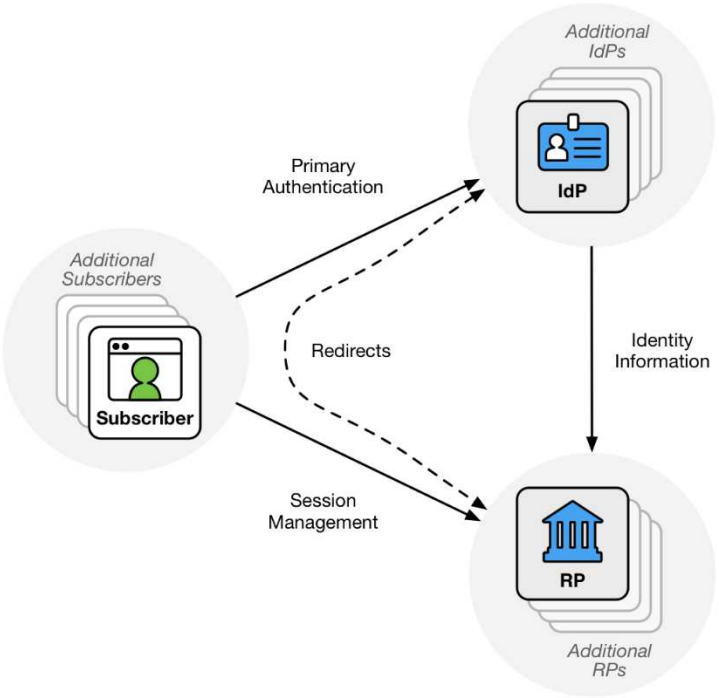
デジタル庁
Digital Agency

論点概要：フェデレーションについて

- 次期本人確認ガイドラインではFederationの概念を取り込む予定であるが、NIST SP 800-63C-4の記載内容は多岐にわたっており、我が国の行政手続では当面関係しないと思われる内容も見受けられる、
- そのため、本人確認ガイドラインへの取り込みにあたっては、NIST SP 800-63C-4の内容の調整や取捨選択が必要。

論点	ご意見をいただきたい観点
NISTのガイドラインの内容を どのように調整・取捨選択すべきか	NIST SP 800-63C-4のモデルやFALに関して • そのまま取り込むべき部分はどこか？ • 追加／修正／削除すべき部分はどこか？

議論の前提：NISTにおけるFederationのプロセス



1	まず, IdP と RP が **Trust Agreement の締結に合意**する. これは二者間合意でも良いし, オーソリティの要請による多者間合意や信頼できる当事者を通じた委任によるものでもよい. このステップは2つのシステムが接続するための最初の許可となる. リクエストおよび開示できるパラメータはこのステップで確立される. どの Attribute が所与の RP および Subscriber について開示されるかの詳細についての決定は, 以降のステージに遅延されることもある.
2	次に, IdP と RP は**プロトコルレベルで信頼関係を確立するため Registration** を行う. これにより当事者間で情報がセキュアに交換可能となる. 最初のステップでは接続許可を示すポリシー決定が行われるが, このステップでは IdP と RP を示す Credential および識別子の確立が行われる. これにより Federation Protocol を通じてコミュニケーションが可能となる. このステージは Subscriber が RP にログインしようとする前に実施することもあるし, Subscriber が RP に対して IdP を利用するよう試行した結果として実施されることもある.
3	次に, IdP と RP は Subscriber を Authenticate するため **Federation Transaction を実施することを決定**する. この一環として, IdP と RP は当該 Transaction において **Subscriber に関するどの Attribute が IdP から RP に渡されるかを決定**する. このステップにおける決定は, 最初のステップで確立された Trust Agreement と, 2つめのステップで確立された RP および IdP の Identity に基づいて行われる.
4	最後に, Subscriber は IdP に対して Authenticate し, その **Authentication イベントの結果がネットワークを介して RP に Assertion として提示**される. RP は IdP から提示されたこの Assertion を処理し, Subscriber との間に Authenticated Session を確立する.

出典：NIST SP 800-63 Digital Identity Guidelines (翻訳版) (openid-foundation-japan.github.io)

議論の前提： NIST FALのRequirements

Requirements	FAL3	FAL2	FAL1
Cryptographic Verifiability Federation Protocol において提示された Assertion が, それを発行した特定の IdP を追跡可能であり, その関係性を Digital Signature や MAC などの暗号論的メカニズムにより検証可能であること. また RP によって当該 Assertion が改変されたり偽造されていないことを検証できること.	Required	Required	Required
Audience Restriction Federation Protocol において提示された Assertion が, 特定の RP に向けたものであり, 当該 RP が当該 Assertion の Audience を検証可能であること.	Required	Required	Required
Injection Protection Attacker が当該 Federation Transaction リクエスト外で得た Assertion を提示してくるような Attack に対して, RP が強固な保護策を持つこと.	Required	Required	Recommended
Trust Agreement IdP と RP が, 双方ともに, 当該 Subscriber を当該 RP にログインさせるために当該 Federation Transaction に参加することに合意すること. これは両パーティー間の事前の静的な合意によることもあるし, 当該接続を持って暗黙的に合意したとみなされることもある.	Static	Static	Dynamic or Static
Registration IdP と RP が相互に自身の識別子とキーマテリアルを交換し, それ以降の Federation Transaction 内で Assertion や Artifact の Verification に用いることができるようにすること.	Static	Dynamic or Static	Dynamic or Static
Presentation Assertion がそれ単体で RP に (Bearer Assertion として) 提示されたり, Subscriber が提示する Authenticator と紐づけた形で提示されたりすること.	Assertion and Bound Authenticator	Bearer Assertion	Bearer Assertion

出典： NIST SP 800-63 Digital Identity Guidelines (翻訳版) (openid-foundation-japan.github.io)

参考：NIST FAL1の要件

Requirements
FAL1 では, IdP が生成する Assertion は Sec. 6 のコアとなる要件を満たさねばならない (**SHALL**). これらの要件には, IdP が Approved Cryptography を用いて Assertion の内容に署名を施すことによる, Attacker からの Assertion 改変および偽造に対する保護策が含まれる. RP は, Sec. 6 にあるように, Assertion を受け取った際はその起源や Integrity (完全性) を検証し, それが期待した出所を起源としたものであることを保証せねばならない (**SHALL**).
FAL1 における Assertion は全て, 特定の RP (群) に対する Audience Restriction が施されなければならず (**SHALL**), RP が当該 Assertion の Audience に自身が含まれていることを確認せねばならない (**SHALL**). IdP は, Approved Cryptography による署名及び鍵を用いて当該 Assertion を保護し, 当該 RP を含む全ての Assertion 所有者が IdP になりすますことができないようにせねばならない (**SHALL**). Assertion が Asymmetric Key を用いた Digital Signature により保護されている場合は, IdP は同じ Public & Private Key ペアを用いて複数の RP に向けて Assertion に署名を行っても良い (**MAY**). IdP は, HTTPS で保護された well-known location を用いるなど, 検証可能な形で自身の Public Key を公開してもよい (**MAY**). Assertion が Shared Secret を用いた鍵付き Message Authentication Code (MAC) により保護されている場合は, IdP は RP 毎に異なる Shared Secret を用いなければならない (**SHALL**).
FAL1 では IdP-RP 間の Trust Agreement は完全に Dynamic に確立しうる (**MAY**). 例えば, Subscriber が RP に対して動的に IdP を選択・指定し, RP は IdP のパラメータを Discovery により取得し自身を IdP に登録することも可能である. IdP は Subscriber に対してどの Attribute を何の目的で RP に提示するかを選択させる. こういった例では, IdP-RP 間の信頼関係は完全に Subscriber の要求および行動により主導される. なお FAL1 でも Static な Trust Agreement および Registration が可能であることは留意.
既存の Federation Protocol では, FAL1 は OpenID Connect Implicit Client プロファイル [OIDC-Implicit], OpenID Connect Hybrid Client プロファイル [OIDC], 追加機能なしの SAML Web SSO プロファイル [SAML-WebSSO] などにより実装可能である. これらのプロファイルでは, Assertion は IdP により署名され, RP は署名された Assertion の内容により指定される.

出典：NIST SP 800-63 Digital Identity Guidelines (翻訳版) (openid-foundation-japan.github.io)

参考：NIST FAL2の要件

Requirements
FAL1 に対する要件は, ここでより明確ないし厳密にオーバーライトされない限り全て FAL2 でも求められる.
FAL2 では Assertion は Attacker による Injection Attack から強固に保護される必要がある (**SHALL**). この要件を満たすためには, Assertion は Sec. 7.1 にあるように, OpenID Connect Basic Client プロファイル [OIDC-Basic] などを用いて, Back-Channel で提示されるべきである (**SHOULD**). この提示方法では, RP はワンタイムな Assertion Reference を用いて IdP から直接 Assertion を取得する. 従って Attacker は外部アクセスポイントを通じて Assertion を Inject することはできない. Sec. 7.2 のような Front-Channel による提示では, RP は追加の Injection Protection を実装しなければならない (**SHALL**). Assertion の提示方法の如何を問わず, Injection Attack は Federation Transaction を常に IdP からではなく RP から開始することで防ぐこともできる. これにより, RP は取得される Assertion をある Session 内において Subscriber が開始した特定のリクエストと紐づけることができる.
FAL2 では, IdP-RP 間の Trust Agreement は Static に確立されなければならない (**SHALL**). これには RP に提示可能な Attribute 及びその利用目的の制限の確立も含む. Trust Agreement は IdP-RP の二者間 (Bilateral) で確立することもできるし (**MAY**), 多者間 (Multilateral) での Federation パートナーシップを介して確立することもできる (MAY). RPと IdP が実行時に確立済の Trust Agreement を証明可能であれば, Registration は Dynamic でもよい (**MAY**). そのような証明方法は Federation Protocol により多様であるが, Software Attestation の提示や Trusted Domain 上の URL の管理権限を証明することなどが例として挙げられる.
政府が運営する IdP のうち FAL2 での Authentication を提供する IdP は, Assertion の署名及び暗号化に用いる鍵を [FIPS140] Level 1 およびそれ以上の手法により保護しなければならない (**SHALL**).

出典：NIST SP 800-63 Digital Identity Guidelines (翻訳版) (openid-foundation-japan.github.io)

参考：NIST FAL3の要件

Requirements
FAL1 および FAL2 に対する要件は, ここでより明確ないし厳密にオーバーライトされない限り全て FAL3 でも求められる.
FAL3 では Subscriber は Assertion に加えて Authenticator を Direct に RP に提示することで Authenticate せねばならない (**SHALL**). ここで用いられる Authenticator は Bound Authenticator とも呼ばれ, Sec. 6.1.2 に後述される. 例えば Subscriber が IdP と RP の間で Federation によるログインプロセスを実施する場合, RP は Subscriber に RP Subscriber Account に紐づく Bound Authenticator の提示を促す. FAL3 で提示される Bound Authenticator は Subscriber が IdP に Authenticate する際に用いられる Authenticator と同一である必要はない. Assertion は RP が Subscriber を識別する際に用いられるが, その際に Bound Authenticator はログインしようとしている当事者が Assertion により識別される Subscriber であるという高い確度を与える. なお, Subscriber が Bound Authenticator を用いて Authenticate し, RP が当該 Authenticator が正しく当該 Assertion が示す RP Subscriber Account に紐づいていることを検証するまで, FAL3 が達成されることはない.
FAL3 では, IdP-RP 間の Trust Agreement および Registration は Static に確立されなければならない (**SHALL**). 全当事者にとって, 識別に用いられるキーマテリアルおよび Federation パラメータ (RP に送信される Attribute リストを含む) は, Federation による Authentication プロセス実施前に固定されていなければならない (**SHALL**). Federation による Authentication プロセスの中で送信する項目をさらに制限する場合には, 動的に決定がなされてもよい (**MAY**). (e.g., Trust Agreement で合意されたパラメータには含まれているものの Email Address を開示したくない場合など)
FAL3 での Authentication を提供する IdP は, Assertion の署名及び暗号化に用いる鍵を [FIPS140] Level 1 およびそれ以上の手法により保護しなければならない (**SHALL**).

出典：NIST SP 800-63 Digital Identity Guidelines (翻訳版) (openid-foundation-japan.github.io)

参考：Assertionに含めるAttributeの要件

#	Requirements
1	全ての Assertion には以下の Attribute を含めるものとする (**SHALL**). • **Subject Identifier:** Assertion が指し示す当事者 (i.e., Subscriber) の識別子 • **Issuer Identifier:** Assertion 発行者 (i.e., IdP) の識別子 • **Audience Identifier:** Assertion を利用することが想定された当事者 (i.e., RP) の識別子 • **Issuance Time:** IdP が Assertion を発行した時刻を示すタイムスタンプ • **Validity Time Window:** その期間を超えて RP が Subscriber を Authentication する目的で Assertion を有効なものとして受け入れることのない (SHALL NOT) よう示す期間. これは通常 Assertion の有効期限タイムスタンプという形で Issuance タイムスタンプとともに伝えられる. • **Assertion Identifier:** 当該 Assertion を一意に識別する値で, 攻撃者が以前の Assertion を Replay することを防止する目的で利用される. • **Signature:** Digital Signature ないしは Message Authentication Code (MAC). IdP に紐づいた鍵の識別子や Public Key を含み, Assertion 全体をカバーするもの. • **Authentication Time:** IdP が最後に (可能であれば) 直接 Authentication イベントを通じて Subscriber の存在確認を行った時刻を示すタイムスタンプ. • **IAL:** Assertion が指し示す Subscriber Account の IAL を示す値, ないしはいかなる IAL も明言されないことを示す値. • **AAL:** IdP が Subscriber を Authenticate した際の AAL を示す値, ないしはいかなる AAL も明言されないことを示す値. • **FAL:** Assertion が指し示す Federation プロセスにおいて IdP が意図する FAL を示す値.
2	Sec. 6.1.2 に後述のように Assertion が FAL3 で Bound Authenticator とともに用いられる場合, Assertion は以下を含むものとする (**SHALL**). • **Authenticator Binding:** Public Key, 鍵の識別子, その他の Subscriber が保持する Bound Authenticator (IdP が管理するもの) の識別子, ないしは RP が管理する Bound Authenticator が Assertion 検証に要求されることを示す値.

出典：NIST SP 800-63 Digital Identity Guidelines (翻訳版) (openid-foundation-japan.github.io)

ご意見をいただきたい論点

NIST SP 800-63C-4 目次		ご意見をいただきたい論点
4 Federation Assurance Level (FAL)	4.1. Federation Assurance Level 1 (FAL1) 4.2. Federation Assurance Level 2 (FAL2) 4.3. Federation Assurance Level 3 (FAL3) 4.4. Requesting and Processing xALs	NIST FALの基準を本人確認ガイドラインにそのまま取り込めるのか。修正・見直すべき点はどこか （以下の論点❶～❸により詳細を議論）
5 Federation	5.1. Trust Agreements 5.2. Registration 5.3. Authentication and Attribute Disclosure 5.4. RP Subscriber Accounts 5.5. Privacy Requirements 5.6. Reauthentication and Session Requirements in Federated Environments 5.7. Shared Signaling	❶政府の本人確認ガイドラインとして、Dynamic Trust Agreement／Dynamic Registrationは必要なのか ❷政府の本人確認ガイドラインとして、Shared Signalingの実装は必要なのか、強制力はどう設定すべきか
6 Assertion	6.1. Assertion Binding 6.2. Assertion Protection 6.3. Identity APIs	❸NIST FAL3で求められるBound Authenticatorは、政府の本人確認ではどのようなケースで必要になるか
7 Assertion Presentation	7.1. Back-Channel Presentation 7.2. Front-Channel Presentation 7.3. Protecting Information	
その他全般		❹その他、本人確認ガイドラインへの取り込みにあたって、どのような点を追加検討すべきか

❶政府の本人確認ガイドラインとして
Dynamic Trust Agreement／Dynamic Registrationは必要なのか

- 政府のIdPが事前合意なしにRPとの連携を開始するケースは想定されないのではないか。
- 本人確認ガイドラインに取り込む際には、Trust AgreementもRegistrationもStaticを前提とすべきではないか。

Requirements	FAL3	FAL2	FAL1
Trust Agreement IdP と RP が, 双方ともに, 当該 Subscriber を当該 RP にログインさせるために当該 Federation Transaction に参加することに合意すること. これは両パーティー間の事前の静的な合意によることもあるし, 当該接続を持って暗黙的に合意したとみなされることもある.	Static	Static	Dynamic or Static
Registration IdP と RP が相互に自身の識別子とキーマテリアルを交換し, それ以降の Federation Transaction 内で Assertion や Artifact の Verification に用いることができるようにすること.	Static	Dynamic or Static	Dynamic or Static

出典：NIST SP 800-63 Digital Identity Guidelines (翻訳版) (openid-foundation-japan.github.io)

参考：Trust Agreementについて

5.1. Trust Agreements より一部抜粋

Trust Agreement では, 以下のパラメータを確立することとする (**SHALL**).

- IdP が RP に対して開示できる Attribute のリスト
- IdP が Assertion を生成できる Subscriber Account の母集団
- RP がリクエストする Attribute のリスト (IdP が RP に対して開示できるリストのサブセット)
- RP がリクエストする各 Attribute についてその利用目的
- Subscriber Attribute の開示にかかる意思決定の責務を負うAuthorized Party
- Subscriber が RP に開示される Attribute について知る手段
- IdP が提供しうる xAL
- RP が必要とする xAL

Trust Agreement は Static に確立されることもあれば Dynamic に確立されることもある. Static Trust Agreement の確立においては, 双方に期待される挙動, 権利および要件について, 法的ないしは契約に基づいた合意がなされる. Static Trust Agreement のパラメータは, 当該合意に参加する全当事者 (IdP や RP のオペレーターや影響する Subscriber を含む) に開示されなければならない (**SHALL**).

出典：NIST SP 800-63 Digital Identity Guidelines (翻訳版) (openid-foundation-japan.github.io)

参考：Registrationについて

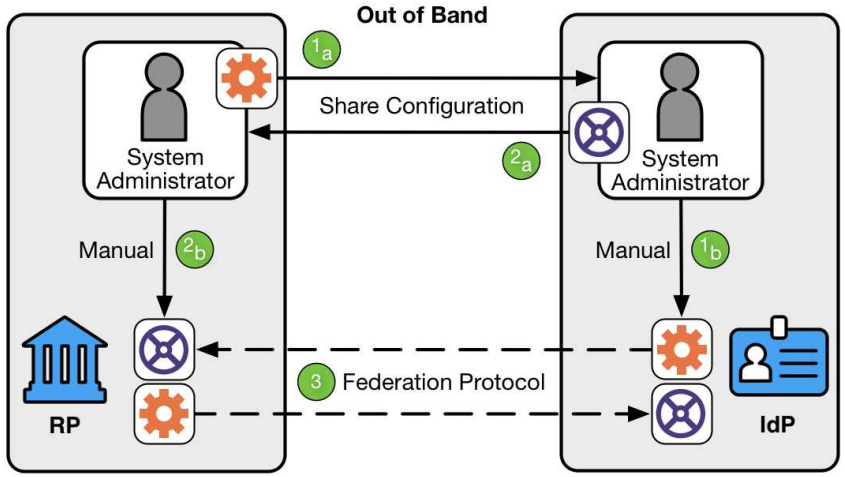
5.2.1. Manual Registration

Manual Registration モデルでは, Subscriber が関与する前に, IdP と RP のオペレータが手動で相互運用が期待される当事者に関する設定情報を Provisioning する.

（中略）

Federation 関係確立においては, 期待され許容可能な IAL, AAL に関するパラメータを確立しなければならない (**SHALL**).

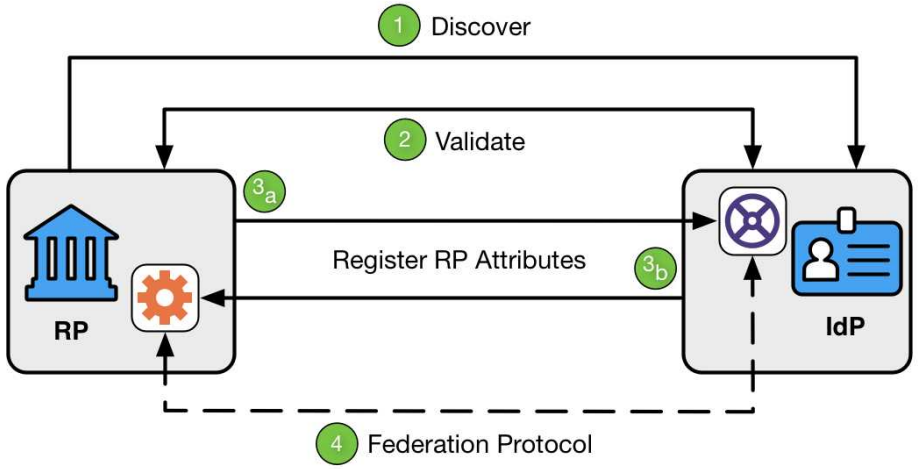
Figure 4. Manual Registration



5.2.2. Dynamic Registration

Federation の Dynamic Registration モデルでは, Transaction 実行時に Federation メンバー間の関係取り決めが行われることもある. このプロセスのおかげで, IdP と RP は Manual Registration (See Sec. 5.2.1) により手動で関係を構築することなく相互接続することも可能である. Dynamic Registration をサポートする IdP は自身の設定情報 (Dynamic Registration Endpoint 等) 可能な限りシステム管理者の関与を必要としない形で公開すること (**SHALL**).

Figure 5. Dynamic Registration



出典：NIST SP 800-63 Digital Identity Guidelines (翻訳版) (openid-foundation-japan.github.io)

❷政府の本人確認ガイドラインとして、Shared Signalingの実装は必要なのか、強制力はどう設定すべきか

- 政府の行政手続向けのガイドラインとして、Shared Signalingの要求を取り込むべきか？強制力はどうすべきか？
- 来年度の検討のため、Shared Signalingを採用すべき理由（メリットや必要性）、見送るべき理由（デメリット、懸念事項）のそれぞれについて、ご意見をいただきたい。

IdP は Subscriber Account に以下のような変更が生じた際, シグナルを送ることができる (**MAY**).

- Account が Terminate された.
- Account が侵害された恐れがある.
- Federated Identifier 以外の識別子 (Email Address, Certificate CN 等) をはじめとする Account の Attribute に変更が生じた.
- Account に適用されうる IAL, AAL ないしは FAL の範囲に変更が生じた.

RP は RP Subscriber Account に以下のような変更が生じた際, シグナルを送ることができる (**MAY**).

- Account が Terminate された.
- Account が侵害された恐れがある.
- RP が管理する Bound Authenticator が追加された.
- RP が管理する Bound Authenticator が削除された

出典：NIST SP 800-63 Digital Identity Guidelines (翻訳版) (openid-foundation-japan.github.io)

参考：Shared Signalingに関する要求

Section	Requirements
5.4.2. Attribute Synchronization	IdP は RP に提供した Subscriber Account の Attribute に更新があった場合, RP にシグナルを送るべきである (**SHOULD**). これは, Sec. 5.7 の Shared Signaling や Sec. 5.4.3 の Provisioning API を利用したり, Assertion にシグナルを含めて提供する (関連する Attribute の最終更新日時を含めたり, RP に自身のキャッシュが期限切れだと判断する手段を提供したり) などの方法で実現可能である. IdP は Subscriber Account が Terminate されたり Subscriber Account が持つ RP への Access が無効化された場合, RP にシグナルを送るべきである (**SHOULD**). これは, Sec. 5.7 の Shared Signaling や Sec. 5.4.3 の Provisioning API などの方法で実現可能である. このシグナルを受け取った場合, RP は RP Subscriber Account を Terminate させ, RP Subscriber Account に関連する全ての personal information を削除せねばならない (**SHALL**). ただし監査やセキュリティ目的で必要とされる場合を除く.
5.5. Privacy Requirements	IdP は, Sec. 5.7 にある Shared Signaling を用いて, Subscriber Account の Terminate シグナルを当該 Subscriber Account に紐づいた Federated Identifier の Provisioning を受けた RP に送るべきである (**SHOULD**). IdP からこのシグナルを受け取った RP は RP Subscriber Account を Terminate し, 当該 RP Subscriber Account に関連する全ての Personal Information を削除しなければならない (**SHALL**). ただし監査やセキュリティ目的で必要とされる場合を除く.
6.1.2.2. RP-Managed Bound Authenticators	RP は, 以下のようなイベントが発生した際は, Out-of-band な手段で Subscriber に通知し (**SHALL**), IdP にも Shared Signaling システム (Sec. 5.7 参照) を通じて通知を行うべきである (**SHOULD**). • 新たな Authenticator が RP Subscriber Account に紐づけられた. • 既存の Bound Authenticator が RP Subscriber Account から紐付け解除された.

出典：NIST SP 800-63 Digital Identity Guidelines (翻訳版) (openid-foundation-japan.github.io)

❸NIST FAL3で求められるBound Authenticatorは、政府の本人確認ではどのようなケースで必要になるか

- Bound Authenticatorは、政府の行政手続において具体的にどのような脅威を想定して採用する必要があるか。

Requirements	FAL3	FAL2	FAL1
Presentation Assertion がそれ単体で RP に (Bearer Assertion として) 提示されたり, Subscriber が提示する Authenticator と紐づけた形で提示されたりすること.	Assertion and Bound Authenticator	Bearer Assertion	Bearer Assertion

6.1.2. Bound Authenticators

Bound Authenticator とは Subscriber が Assertion とともに RP に提示する Authenticator である. RP に Bound Authenticator を保持していることを証明するため, Subscriber は Assertion の正当な Subject であるということを一定の確度を持って証明する. これにより, Attacker は Assertion に加え Bound Authenticator も詐取・提示することが必要になるため, Attacker が Subscriber 向けに発行された Assertion を詐取して利用することはより困難になる. さらに Bound Authenticator は独立した Authentication により RP を不正もしくは侵害された IdP から保護する.

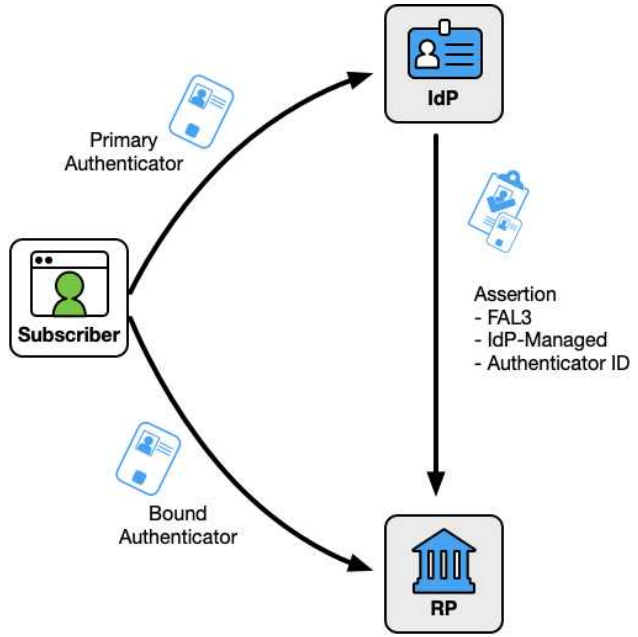


Figure 9. IdP-Managed Bound Authenticators

出典：NIST SP 800-63 Digital Identity Guidelines (翻訳版) (openid-foundation-japan.github.io)

デジタル庁
Digital Agency