参考資料1

デジタルクレデンシャル
利用用途に応じた管理要件

2025/3/10

一般社団法人 OpenID ファウンデーション・ジャパン/代表理事
米国OpenID Foundation/共同議長 eKYC&IDA WG
富士榮 尚寛（ふじえ なおひろ）

OpenID Japan

デジタルクレデンシャルの利用用途に応じた管理要件に関する考察

Discussion Paper: Management Requirements for Different Uses of Digital Credentials

version 1.0（2025/01/24）

慶應義塾大学SFC研究所データ・アーキテクチャ・ラボ
伊藤忠テクノソリューションズ株式会社

富士榮　尚寛
伊藤忠テクノソリューションズ株式会社みらい研究所 所長
一般社団法人OpenIDファウンデーションジャパン 代表理事
鈴木　茂哉
慶應義塾大学大学院政策・メディア研究科 特任教授
阿部　涼介
慶應義塾大学大学院政策・メディア研究科 特任助教
貞弘　崇行
伊藤忠テクノソリューションズ株式会社みらい研究所

エグゼクティブ・サマリー

スマホに搭載される運転免許証をはじめ、学生証や学修歴、スキル証明、国民IDなど公的機関や民間組織が発行する各種証明書類（クレデンシャル）のデジタル化に向けた検討が活発に進められている。クレデンシャルのデジタル化は、我が国のみならず、世界で同様に各種ベンダによるソリューションの開発〜提供が始まっており、今後拡大していく市場としての期待を集めている。 そのような状況において特定のベンダやプラットフォーム提供者に依存するのではなく、かつ、クレデンシャルの用途に応じたセキュリティやプライバシーを含む管理要件や相互運用性に関して検討し、その結果を相互運用可能な標準活動をへて世界で利用されることこそがクレデンシャルのデジタル化の持続可能性のための重要な戦略となる。 そのために、本書においてはクレデンシャル（身分証明書）をデジタル化する上で必要となる管理要件を整理した。具体的には、1)正しい主体に対して発行されているクレデンシャルであるかどうかを当人認証の強度を判断可能な状態であること、2)利用するウォレットの特定と発行済みのクレデンシャルの管理（取り消しなど）を発行機関側で可能な状態であること、3)検証者が本人確認書類として当該クレデンシャルを利用できること、のための論点を整理する。今後、この論点をもとに政府や学術機関において具体的なアーキテクチャを定義し、各構成要素に求められる実装・管理要件およびガバナンスルールを定義し、より良い社会実装に向けて検討が進むことを期待するものである。

導入

国民IDや運転免許証のスマホ搭載やデジタルアイデンティティウォレットの大規模展開など、デジタルクレデンシャルの発行と利活用に関する検討がグローバルで進んでいる。しかしながらデジタルクレデンシャルの用途によっては発行先や状態を厳格に管理することが必要となるケースも想定される。特に本人確認書類としての利用が想定されるケースにおいては物理的な書類における「原本」と「コピー」に相当する考え方をどのようにデジタルに持ち込むことが妥当なのか、真正性検証が可能でありデジタルクレデンシャルの主体とクレデンシャルのホルダーが一致していることが一定程度確認されれば問題ないのかについては十分に検討を行う必要がある。本ディスカッションペーパーではデジタルクレデンシャルの種別・利用用途に応じた管理の必要性と考えられる手法について論点を整理する。また、先行して実証・実装が進む欧州の事例を踏まえて概説する。なお、本書の想定読者は所謂IHV（Issuer-Holder-Verifier）モデルに関する基本的な点について理解していることを前提としており、モデルそのものや基本的なアクターに関する解説は省略する。必要に応じて「Decentralized Identifiers (DID) とVerifiable Credentials (VC) の現況 [1] 」などの先行論文を参照されたい。

https://dal.sfc.keio.ac.jp/ja/TR/management-requirements-for-digital-credentials/

文章の構成

- 原本と複製に関する課題
- 本人確認プロセスの分解とデジタルクレデンシャル利用時の要件
- クレデンシャル管理とウォレットの信頼性に関する要件
- クレデンシャル管理に関して考慮すべきシナリオ
- 実装方式に関する議論
- 現在の標準技術仕様で解決できない残存課題
- プライバシーに関する考慮事項
- 他国の動向
- デジタルクレデンシャル導入時に検討すべきこと

ディスカッションペーパーで語られることのサマリー

- **クレデンシャルをデジタル化する上での懸念事項**
  - デジタル化が目的となってしまい、利用シーンに関する考慮不足による安全性やプライバシーへの配慮を欠く実装が蔓延ること
  - さらに、その実装が特定ベンダやプラットフォーマーによるロックイン（デファクト・スタンダード化）され、相互運用性が欠如し国際的においていかれること
- **デジタルクレデンシャルの管理要件を以下の論点で整理**
  - 1)正しい主体に対して発行されているクレデンシャルであるかどうかを当人認証の強度を判断可能な状態であること
  - 2)利用するウォレットの特定と発行済みのクレデンシャルの管理（取り消しなど）を発行機関側で可能な状態であること
  - 3)検証者が本人確認書類として当該クレデンシャルを利用できること
- この論点をもとに政府や学術機関において具体的なアーキテクチャを定義し、各構成要素に求められる実装・管理要件およびガバナンスルールを定義し、より良い社会実装に向けて検討が進むことを期待

主要な話

1. クレデンシャルの用途の話
   - 身元確認書類として使うもの、資格証明書や属性証明として使うもの
2. 発行するクレデンシャル自体の話
   - デジタル資格証明はどう扱う？原本・複製・派生の違いは？
3. 身元確認でのクレデンシャルの使い方の話
   - 身元確認のプロセスとデジタルクレデンシャルの使い方
4. 発行者によるクレデンシャル管理の話
   - 誰がどう責任を負うのか
   - 管理するためにはどのような工夫が必要となるか

クレデンシャルの用途について

クレデンシャルをデジタル化する前に

- 何に使うクレデンシャルなのかを明確化することが重要
  - 身元確認書類として本人確認に利用
  - 資格証明や属性証明に利用
- クレデンシャルを行使する主体の違いを認識する
  - 基本的に身元確認書類は本人が利用する暗黙の前提あり
  - 資格証明、属性証明は本人以外の主体が利用する可能性あり

  ※委任や代理人シナリオは一旦おいておく
- ポイントはVerifierの目線で考えること
  - Verifierが当該のクレデンシャルを何の目的で使うことを想定して発行するか？
  - 目的外利用されない工夫も必要（ex. 成績証明で身元確認？）

発行するクレデンシャル自体について

原本と複製に関する課題

- 各種クレデンシャルの原本と複製の使い分けの課題
- 現実世界では原本と複製の差は歴然
  - パスポート原本でないと出入国審査は通過できない
  - パスポートのコピーでも旅行保険への加入はできる
- ではデジタル世界における原本と複製は？
  - 原本（Original）：デジタル署名＋タイムスタンプ？
  - 複製（Duplicate）：全く同じビット配列のファイルは原本？複製？
  - 派生（Derived）：マイナンバーカードで本人確認済みの証明書の扱いは？

クレデンシャルの段階の例

現実世界	デジタル世界
発行者が直接発行したもの（例：パスポート）	電子署名とタイプスタンプを組み合わせて作成以後改ざんされていないことが証明できるもの
発行者が直接発行したもの（発行者が複数発行することが可能なもの。原本として扱うことができるもの）	原本を電子的に複製したもの（原本と明確な差異はない）
コピー機等で複写されたもの（例：パスポートのコピー）	原本の発行者以外の第三者が原本を元に別途発行したもの
原本の発行者以外の第三者が原本を元に別途発行したもの（例：「本人確認済み」のスタンプが押された書類）	

クレデンシャルの段階の例

現実世界	デジタル世界
発行者が直接発行したもの（例：パスポート）	電子署名とタイプスタンプを組み合わせて作成の後改ざんされていないことが証明できるもの
発行者が直接発行したもの（発行者が複数発行することが可能なもの。原本として扱うことができるもの）	原本を電子的に複製したもの（原本と明確な差異はない）
コピー機等で複写されたもの（例：パスポートのコピー）	原本の発行者以外の第三者が原本を元に別途発行したもの
原本の発行者以外の第三者が原本を元に別途発行したもの（例：「本人確認済み」のスタンプが押された書類）	

原本（Original）

複製（Duplicate）

派生（Derived）

原本と派生クレデンシャルの問題

- 技術的には明確な違いがある
  - 署名者が異なる
  - 当然ビット配列も異なる
  - 完全に別のもの
- 利用者やVerifierの解釈が“混ざる”ことがある
  - マイナンバーカードで本人確認を行なったデジタル証明書
  - マイナンバーカードをデジタル化した証明書（カード代替電磁的記録）
- ビジネスの視点？
  - あえて混乱させた方が“売れる”かも？

身元確認でのでのクレデンシャルの使い方について

本人確認と身元確認

本人確認は身元確認と当人認証より構成される

本人確認と身元確認・当人認証と主な特徴

本人確認

	身元確認	当人認証
確認の内容の例	● 提示された本人確認書類が偽造されていないことを確認 ● 提示された本人確認書類と申告内容を照合し、申請者に関するものであることを確認	● 取得されたパスワードや生体情報を、あらかじめ登録されているものと照合し、同一人物であることを確認
確認できること	実在性*2	当人性
実施シーンの事例	● ユーザー登録*3 ● 銀行口座の開設 ● 携帯電話の契約 ● クレジットカードの申込み	● ログイン ● スマートフォンのロック解除 ● サービス問い合わせ時の電話等での本人確認

出典）民間事業者向けの業界横断的なデジタル本人確認のガイドライン/OpenIDファウンデーションジャパン、2023年

https://www.openid.or.jp/news/2023/03/kycwg.html

デジタルクレデンシャルとの関係性は？

主にデジタルクレデンシャルが関係するのは身元確認

本人確認と身元確認・当人認証と主な特徴

本人確認

	身元確認	当人認証
確認の内容の例	• 提示された本人確認書類が偽造されていないことを確認 • 提示された本人確認書類と申告内容を照合し、申請者に関するものであることを確認	• 取得されたパスワードや生体情報を、あらかじめ登録されているものと照合し、同一人物であることを確認
確認できること	実在性*2	当人性
実施シーンの事例	• ユーザー登録*3 • 銀行口座の開設 • 携帯電話の契約 • クレジットカードの申込み	• ログイン • スマートフォンのロック解除 • サービス問い合わせ時の電話等での本人確認

出典）民間事業者向けの業界横断的なデジタル本人確認のガイドライン/OpenIDファウンデーションジャパン、2023年
https://www.openid.or.jp/news/2023/03/kycwg.html

身元確認プロセスの分解とデジタルクレデンシャル

主にResolutionとValidation（NIST定義）で利用される

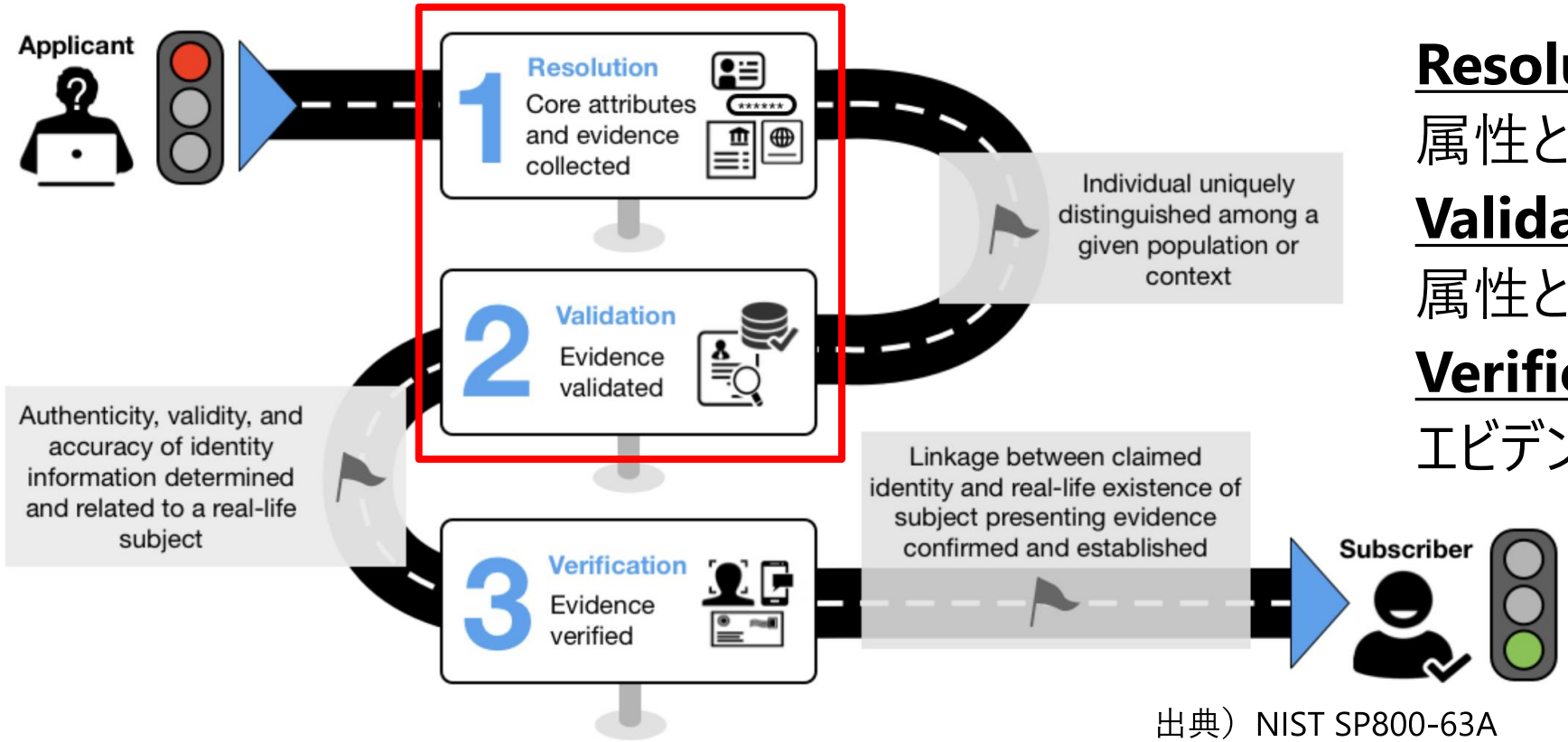


Figure 4-1 The Identity Proofing User Journey

Resolution
属性とエビデンス収集

Validation
属性とエビデンスの真正性確認

Verification
エビデンスと提示者の同一性確認

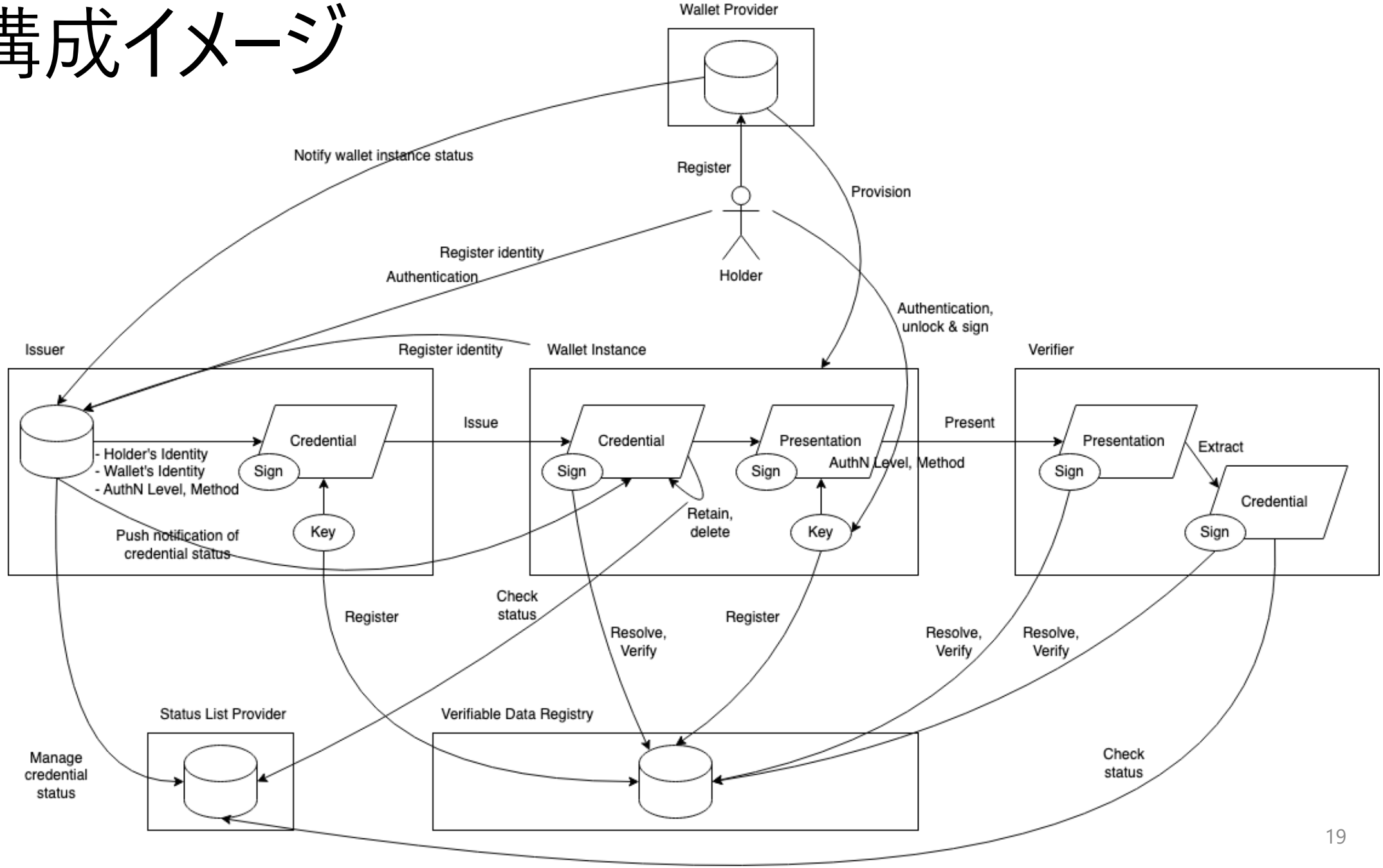
出典）NIST SP800-63A
https://pages.nist.gov/800-63-3/sp800-63a.html

発行者による証明書管理について

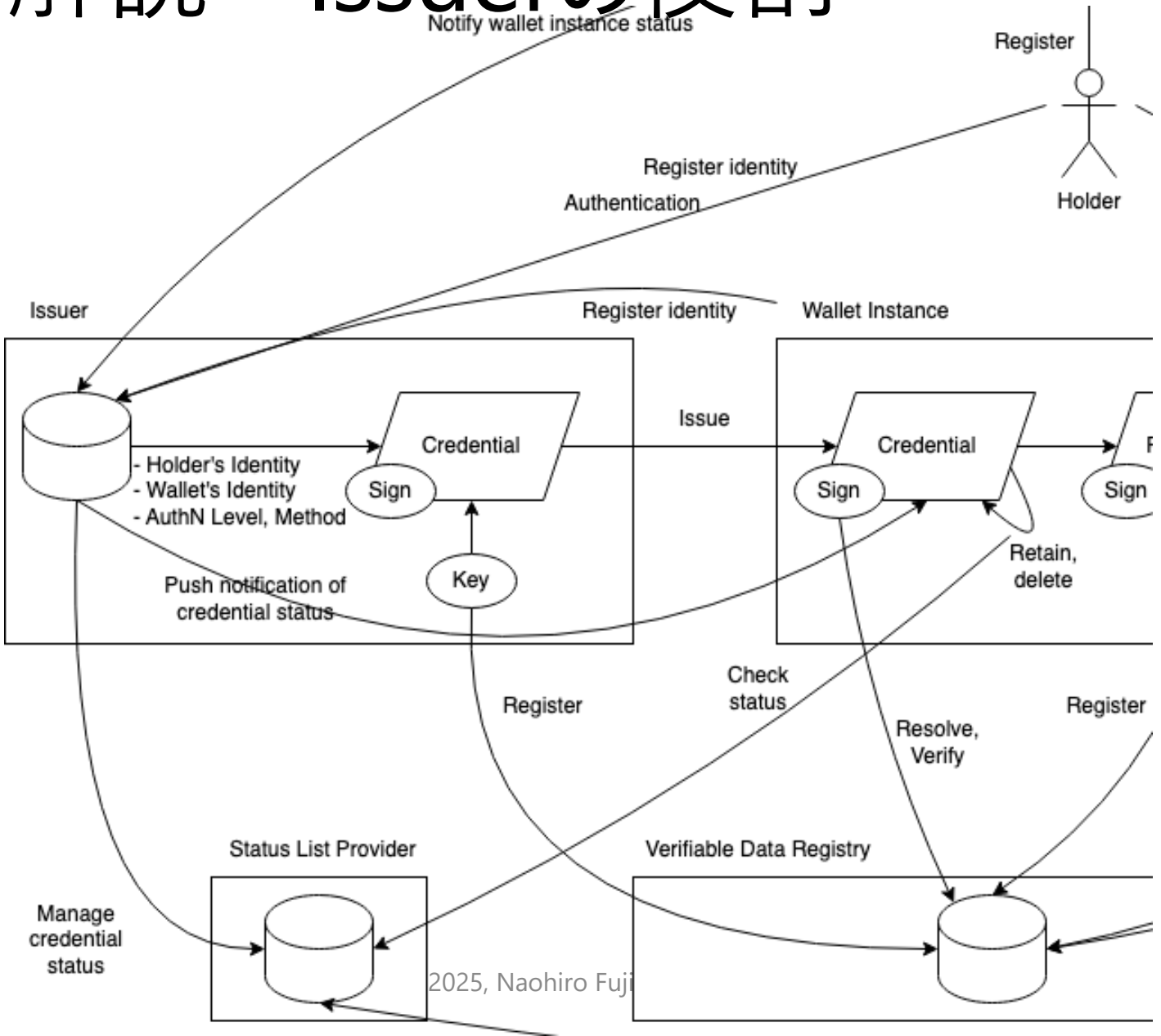
クレデンシャルの状態管理の必要性

- 身元確認書類として使う場合は特に重要
  - Verifierが当該クレデンシャルが確かに提示者となるHolderに対して発行されたことを判別・判定できること
  - みだりに大量発行されていないこと（同時に発行できる枚数の制限など）
  - 証明書のライフサイクル全般にわたってステータスの管理（取り消しなど）ができること
- 実装に向けた要件の例
  - Holder・クレデンシャル・Walletインスタンスがそれぞれバインディングできること
  - Issuer起点でクレデンシャルの発行状態を保持・管理すること
  - Issuer起点で発行済みクレデンシャルを特定して取り消しできること

全体構成イメージ


Wallet Provider
Notify wallet instance status
Register
Provision
Register identity
Authentication
Holder
Authentication,
unlock & sign
Issuer
Register identity
Wallet Instance
Verifier
Issue
Present
Credential
Credential
Presentation
Presentation
Extract
- Holder's Identity
- Wallet's Identity
- AuthN Level, Method
Sign
Sign
Sign
AuthN Level, Method
Sign
Credential
Key
Retain,
delete
Key
Push notification of
credential status
Register
Check
status
Resolve,
Verify
Register
Resolve,
Verify
Resolve,
Verify
Status List Provider
Verifiable Data Registry
Manage
credential
status
Check
status

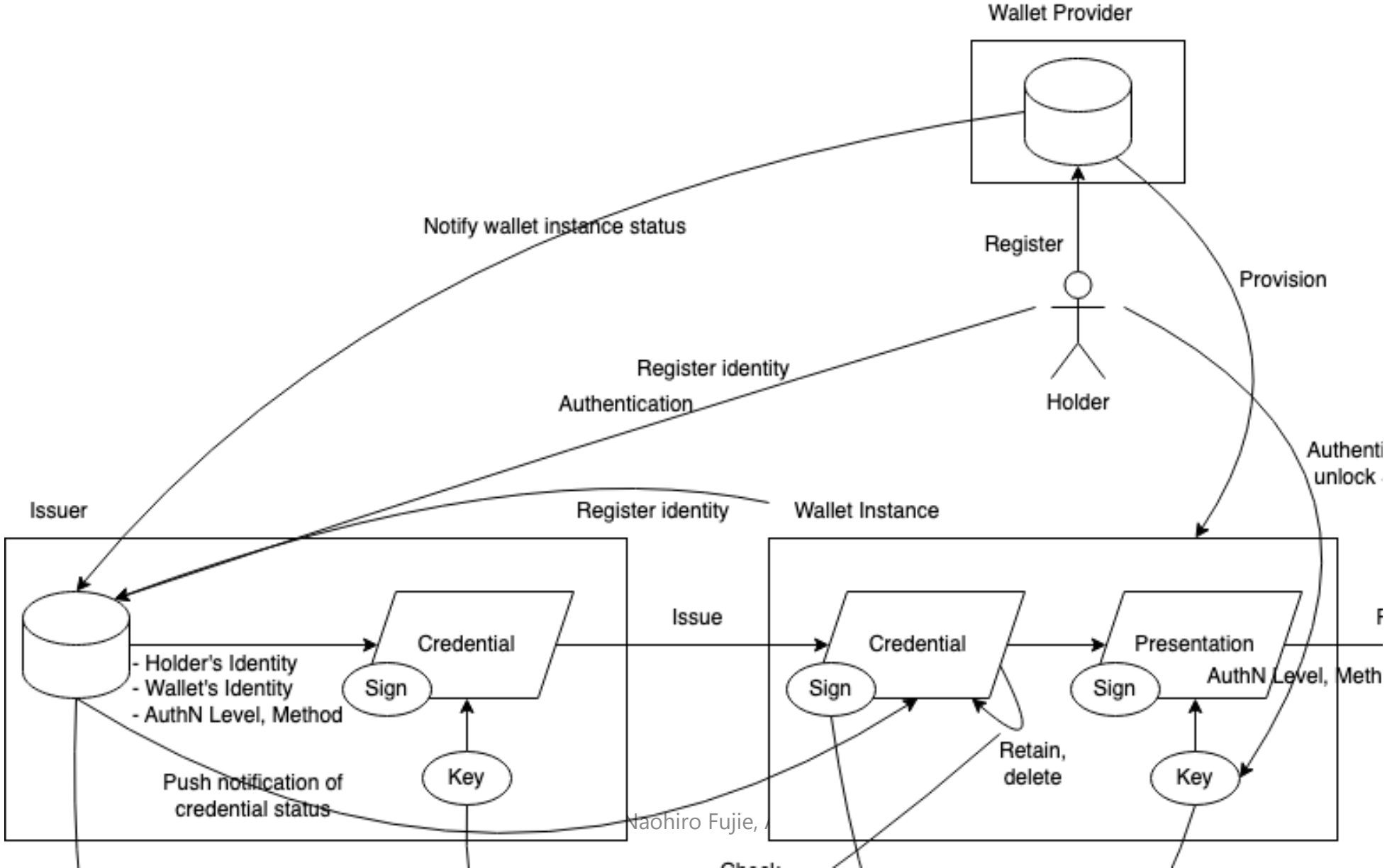
構成要素解説：Issuerの役割



構成要素解説：Issuerの役割

- 以下の要件を満たすクレデンシャルを発行する
  - クレデンシャルとHolderのバインディングができること
  - クレデンシャルとWalletインスタンスのバインディングができること
  - 発行先のWalletインスタンスを特定できること（後から特定して取り消すため）
- クレデンシャルに以下の情報を包含し署名する
  - Issuerに登録されたHolderのIdentity
  - Holderの当人認証を一定の強度で実施したこと
  - 発行先となるWalletインスタンスの情報
- 発行したクレデンシャルの状態を管理・取り消しを行う
  - Status Listとの連携（後述）、WalletへのPush通知など

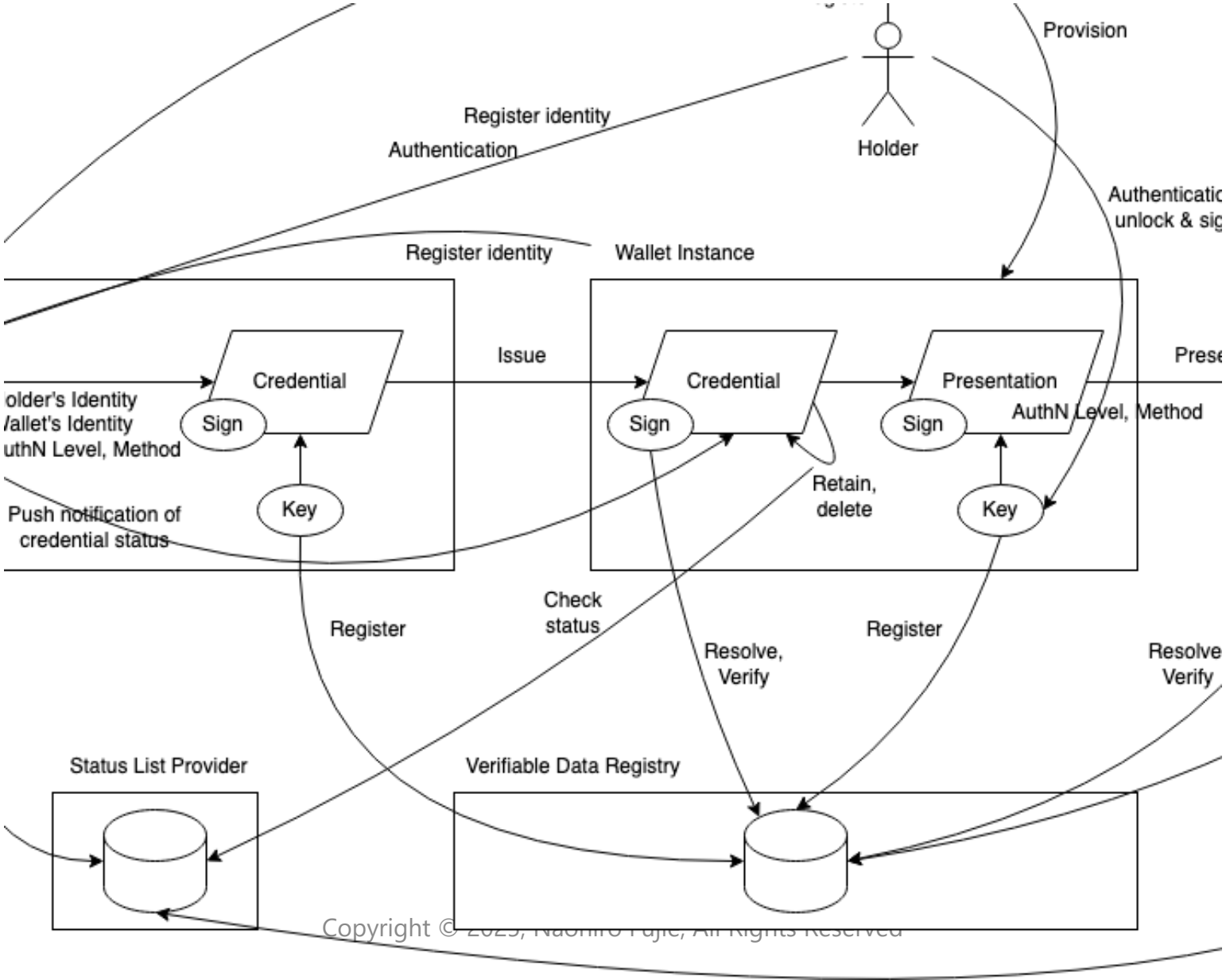
構成要素解説：Wallet Providerの役割



構成要素解説：Wallet Providerの役割

- Holderが利用するWalletを配布・管理する
  - 特定のバージョンのWalletにバグがあった場合や、署名アルゴリズムの危殆化が判明した場合などIssuerに対して通知する
- 管理する上で必要な要件
  - 配布とアクティベーションの管理。どのVersionのWalletインスタンスが利用されているか管理する（Holder情報の登録やインスタンス情報の登録）
  - Issuerへの情報公開（通知など）

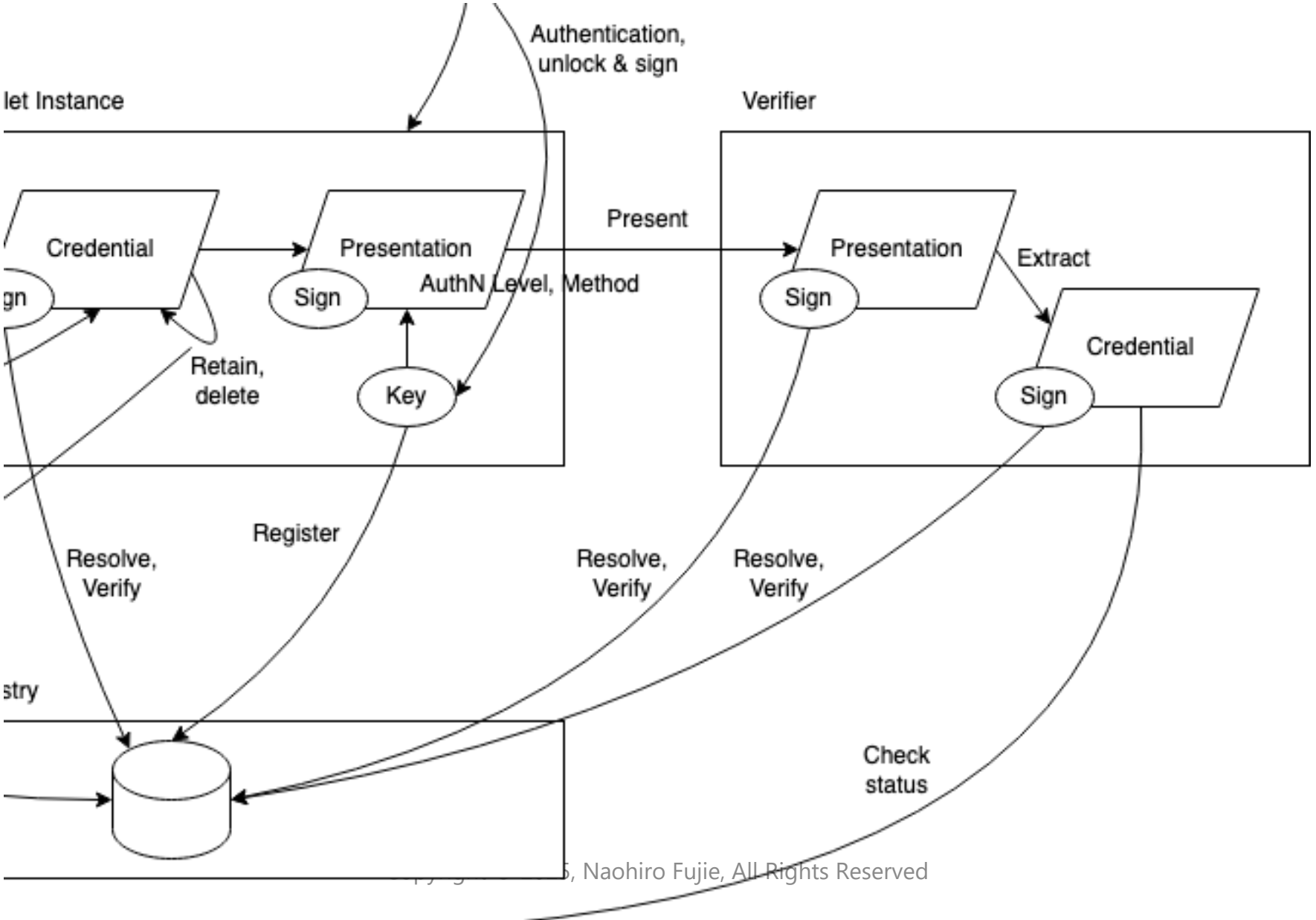
構成要素解説：Walletインスタンスの役割



構成要素解説：Walletインスタンスの役割

- 発行されたクレデンシャルを保存、Verifierからのリクエストに応じて提示する役割
- 保存しているクレデンシャルの状態の把握
  - Status Listの確認、Issuerからの通知の確認
  - どのくらいの期間保存すべきかも検討が必要
- Holderとのバインディングを強化する取り組みは必要
  - クレデンシャル発行時のQRコードの横取り：Issuerが表示するPINの入力など
  - デバイスの盗難や貸し借りへの対応：Wallet起動時、提示時の一定強度での当人認証、強度レベルのVerifierへの提示（Presentationへの包含）など

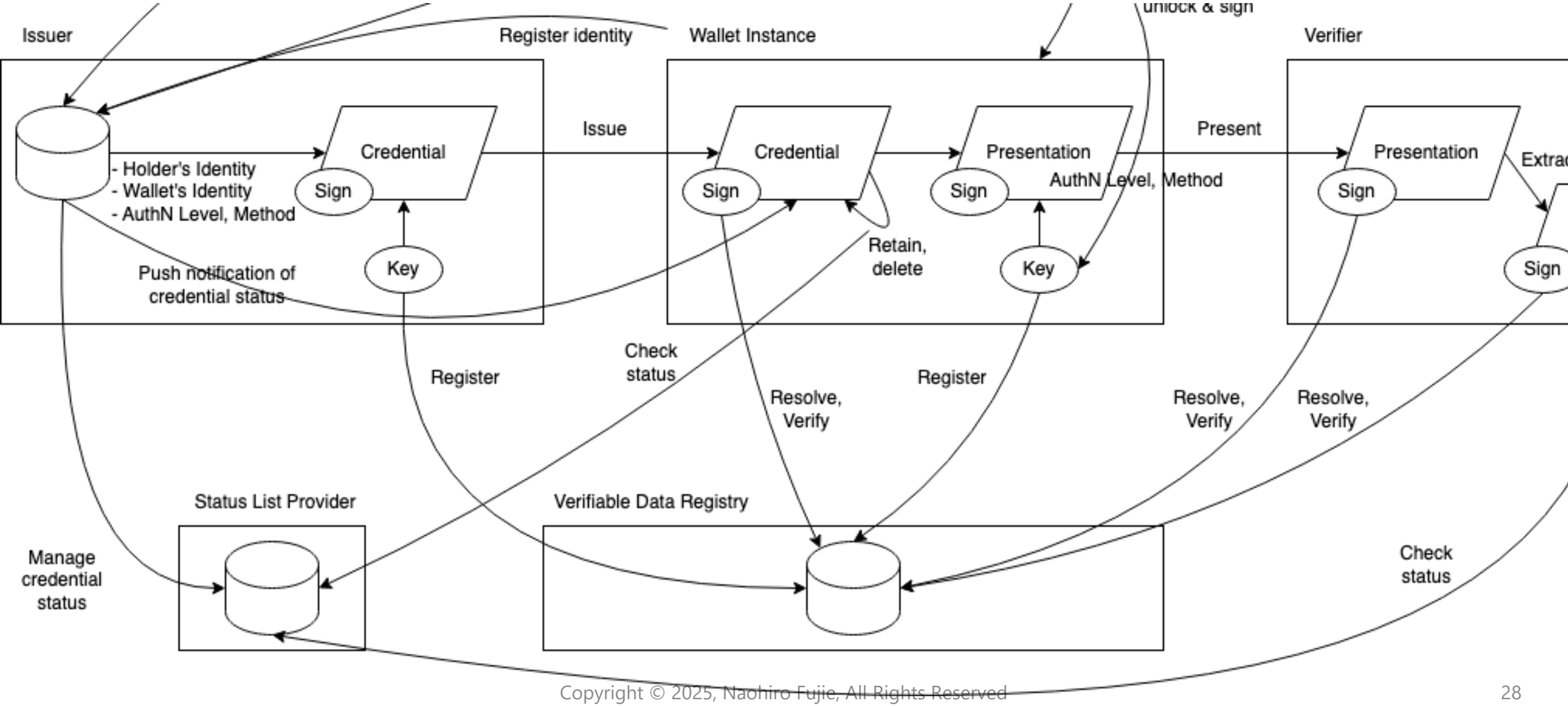
構成要素解説：Verifierの役割



構成要素解説：Verifierの役割

- Holderから提示されたPresentationと包含されるクレデンシャルの検証を行う
  - 署名検証
  - ステータス検証
  - 中身の属性等の検証（有効期限確認、属性値による認可なども）

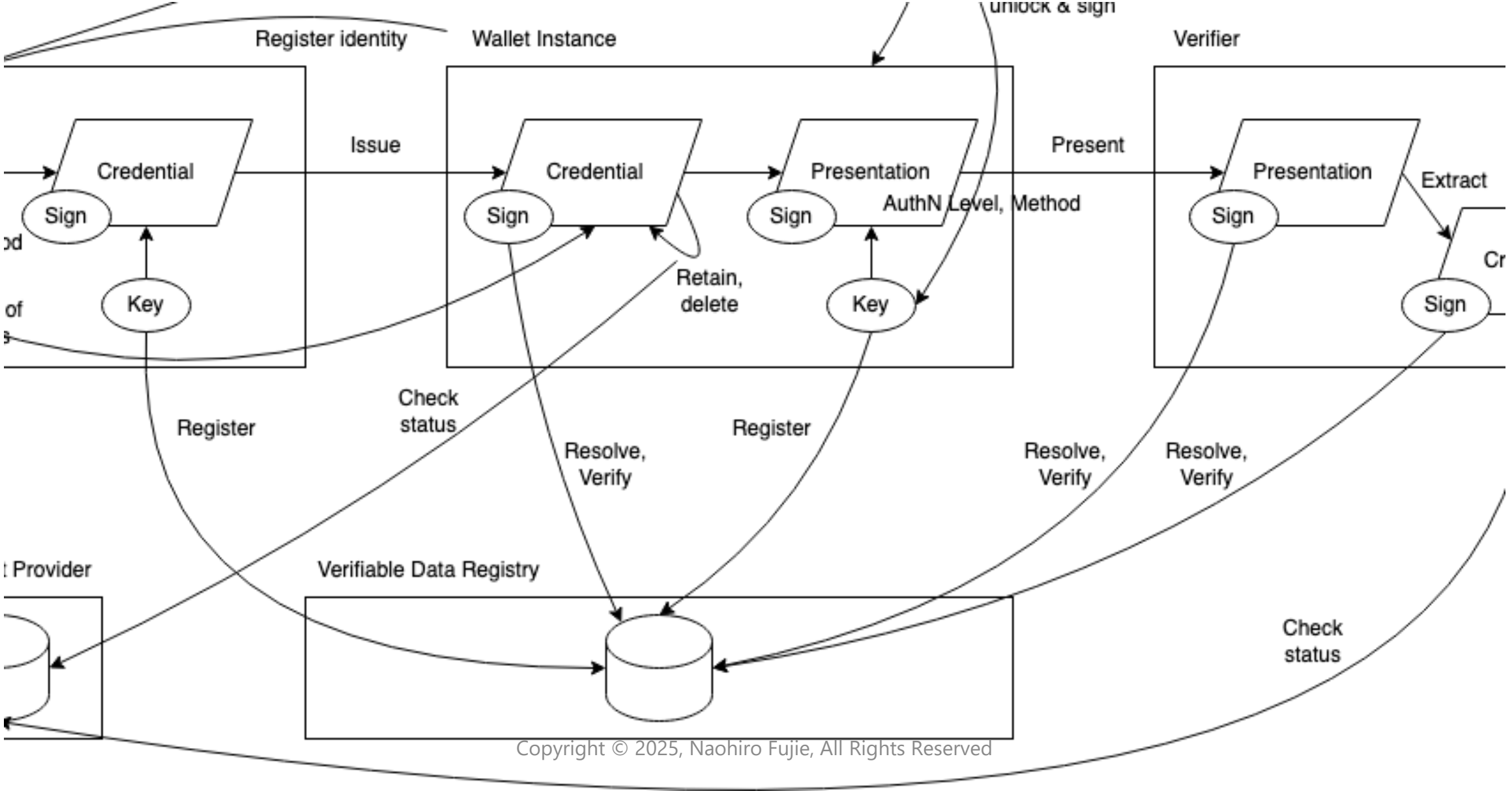
構成要素解説：Status List Providerの役割



構成要素解説：Status List Providerの役割

- Issuerが発行する各クレデンシャルの状態を管理する
- HolderやVerifierからの問い合わせに対して状態を返却する
- 誰が実装するのかはプライバシーの観点、ビジネスモデルの観点から検討を十分に行う必要がある
  - HolderやVerifierからの問い合わせを受けるので誰が、どこにクレデンシャルを提示したのか、などの情報が集約されてしまう
  - IssuerがStatus Listを保持するとIHVモデルの良さである、発行と提示の分離ができなくなる（Federationで良いのでは？という話になる）

構成要素解説：Verifiable Data Registryの役割



構成要素解説：Verifiable Data Registryの役割

- 独立したVerifiable Data Registryが必要かどうかは検討が必要
  - 単一のバケツである必要もなく、Issuer、Wallet Providerがそれぞれ運営しても良い
- 主な役割は以下の通り
  - Issuerが発行したクレデンシャルの検証に必要な公開鍵やStatus Listの場所を公開する
  - Walletが発行したPresentationの検証に必要な公開鍵を公開する

考慮すべきシナリオの例

様々なシナリオが存在することを考慮する

- 単一の利用者が複数のデバイスを保持しているケース
- 複数の利用者がクレデンシャルを共有利用するケース
- 代理人のケース（親が子供のクレデンシャルを利用して修学補助金の申請をするケースなど）

その他考慮事項の例

- プライバシーへの考慮
  - Issuer/Verifier、Verifier/Verifierの結託による名寄せと意図しない属性の提供
  - Pairwise識別子やゼロ知識証明なども検討が進むがまだまだ実用フェーズには至っていない

技術標準の現在地

まだ検討が十分でないことも多数存在

- 複数ウォレットに入ったクレデンシャルのバインディング
- ウォレットでの当人認証結果の表現
- 鍵管理の話（バックアップ・リカバリ、同期など）
- 各主体の信頼性（トラストフレームワーク、Trust Listなど）
- クレデンシャルの利用用途を確認する方法

他国の動向

他国も同様に様々な検討を進めている

- 関連する活動の例
  - 欧州連合/EU Digital Identity Wallet
  - 米国/AAMVA Mobile Driver's License Implementation Guidelines
- 重要なのは、各域・各国で閉じて検討を進めすぎずに、議論する場を作ること
  - 例）欧州連合はInternet Identity WorkshopやOAuth Security Workshopなどのアンカンファレンスへの課題と検討状況を持ち込んで業界プロフェッショナルを巻き込んだ議論をしている