FERI INFORMATION

eIDAS2 発効後の動向と欧州デジタル ID ウォレットのリファレンス・アーキテクチャ

中山　靖司（SBI 金融経済研究所　主任研究員）

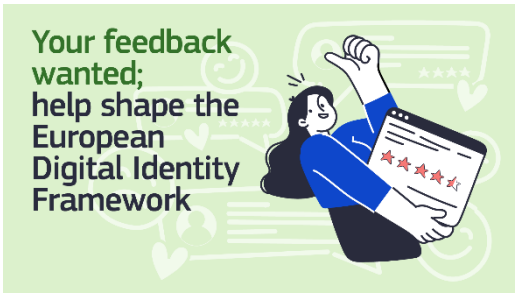
はじめに

本レポートは、当研究所所報第 6 号「『欧州デジタル ID 枠組み規則』制定の経緯と欧州デジタル ID ウォレットの共通仕様」[1]のフォローアップである。同論文では、本年 5 月に発効された同規則（以下「eIDAS2[2]」と呼ぶ）に基づいて EU 市民に提供することが義務付けられた European Digital Identity Wallet（以下「EUDIW」と呼ぶ）の技術仕様等について、「EUDIW Architecture Reference Framework」（以下「EUDIW ARF」）をもとに読み解いた。その際、EUDIW エコシステムのコアとなるコンポーネント等を概説した「リファレンス・アーキテクチャ」や、それらのコンポーネント間で安全なやり取りを可能とするための信頼関係を確立する「トラストモデル」については、紙面の都合により紹介できなかった。

最近になって、EUDIW 関連の実施法案の一部がパブリックコンサルテーションに付され始めているが、実装に関わる内容も多く、改めて「リファレンス・アーキテクチャ」についても言及し、コア・コンポーネント等についても解説しておくことが実施法案の理解を進めるうえで有用であると考えられるため、今回紹介することとした。

eIDAS2 発効後の動向

eIDAS2 では、規則承認後、6～12 カ月で定められた期限までに EUDIW の技術仕様と認証の概要を定めた複数の実施法を整備することが求められている。2024 年 11 月 21 日を期限とする実施法案については、本年 8 月から 9 月にかけて、図表 1 に示す 5 本のパブリックコンサルテーションが行われた。



出所：欧州委員会ホームページ

（図表 1）2024 年第 4Q 成立に向けてパブリックコンサルテーションを行った実施法案

EUDIW – integrity and core functionalities（整合性とコア機能）[3]	相互運用可能で意図するすべての目的に使用できるウォレットを加盟国が確実に提供するためのルールを定めるための施行規則。例えば、ウォレットは、①広範な公共・民間サービスにおける国境を越えた安全なオンライン本人確認、②EA（電子証明書）の共有、③電子署名の発行、を可能にするものでなければならない。
EUDIW – protocols and interfaces to be supported（サポートされるプロトコルとインターフェース）[4]	ウォレットの効果的な運用に不可欠なプロトコルとインターフェースについて、これらの適切な実装を確保するための施行規則。共通のプロトコルとインターフェースをサポートすることで、ウォレットは、①PID（個人識別データ）および EA（電子証明書）の発行および提示、②ウォレットユニット間のデータ共有、③関係者との効率的なコミュニケーションを保証できる。
EUDIW – person identification data and electronic attestations of attributes（個人識別データおよび電子属性証明書）[5]	発行、検証、失効、および停止を網羅する PID（個人識別データ）と EAA（電子属性証明書）の円滑なライフサイクル管理を保証するための施行規則。
EUDIW – trust framework（信頼フレームワーク）[6]	欧州委員会が設置した電子通知システムが、欧州委員会と加盟国間の情報交換のための安全で透明性の高い通信手段として機能するための施行規則。
EUDIW – certification（認証）[7]	EUDIW の適合性認証の要件を定めるための施行規則。

さらに 2025 年 5 月 21 日を期限とする実施法案についても、欧州委員会の公開情報によれば、図表 2 に示す少なくとも 5 本のパブリックコンサルテーションが準備中である。

（図表 2）2025 年第 1Q 成立に向けて準備中の実施法案

EUDIW – registration of relying parties（依拠当事者の登録）[8]	EU 諸国における relying parties（依拠当事者）の登録プロセスに関するルールを定める施行規則。EUDIW にアクセスするための認証に必要な情報、relying parties の連絡先詳細およびウォレットの使用目的（relying parties がユーザーに要求できるデータを含む）に関連するものであり、ウォレットの relying party の登録後に発行されるアクセス証明書の仕様と要件が含まれている。
EUDI Framework – cross-border identity matching（国境を越えた ID 照合）[9]	電子識別手段または EUDIW を使用する際の明確な ID 照合に関するルールを定める施行規則。利用者が国境を越えたオンライン公共サービスにアクセスしようとする場合に、明確な ID 照合を確保するために加盟国が講じるべき措置を定めている。

EUDIW – security breaches（セキュリティ侵害）[10]	ウォレットの信頼性に影響を与えるセキュリティ侵害や一部の情報が漏洩した場合に、EUDIW の一時停止や、場合によっては認証ウォレットリストからの削除を確実に行うためのルールを定める施行規則。
EUDI framework – verification of electronic attestation of attributes（電子属性証明書の検証）[11]	EAA（電子属性証明書）の発行および検証の要件を定めるための実施規則。また、authentic sources（真正情報源）と照合して検証可能でなければならない個人属性のカタログ（個人のアイデンティティを構成する情報）を示しているほか、PuB-EAA（公的電子属性証明）を発行する公的機関が情報を通知・公開する際のルールを定めている。
EUDIW – list of certified wallets（認証ウォレットリスト）[12]	認証済ウォレットのリストとそれに関連する電子的な本人確認スキームに関する情報の届出制度に関する施行規則。EU 諸国が欧州委員会に提出する義務があり、提出書類の授受には欧州委員会が設置する安全な電子システムを使用することになっている。

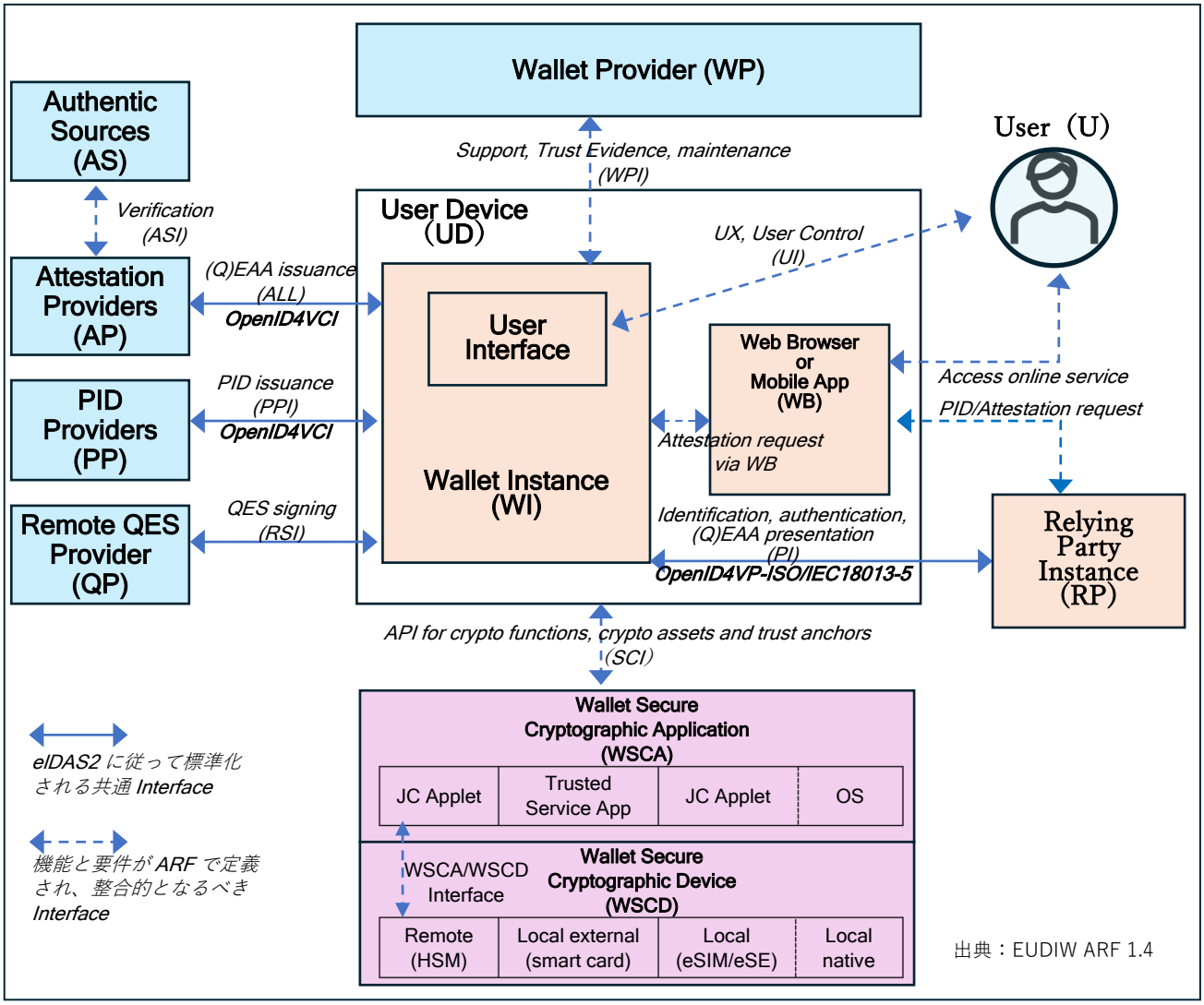
こうした実施法は、技術的な共通仕様や要件を定める「EU デジタル ID ツールボックス」および同ツールボックスの一部を構成する EUDIW ARF と整合することが求められている。今回パブリックコンサルテーションにかけられた実施法案の具体的な文書を見ると、EUDIW を構成するものとして定義されるコア・コンポーネント（後述）や、暗号機能等の高い安全設計にかかわる主要なエンティティを前提に、それらが主要なインターフェースを介してどのように通信するかなど、かなり細かい技術レベルまで含めて規定する内容となっており、EUDIW ARF の記述内容に沿ったものとなっていることがわかる。そこで、所報 6 号では紹介しきれなかった EUDIW ARF の「リファレンス・アーキテクチャ」部分について、本レポートで追加的に解説することとした。

なお、EUDIW ARF は、eIDAS 専門家グループにより適宜更新・作業等が進められているが、その開発作業において筆者が特徴的だと感じた点は、ソフトウェア開発のプラットフォームである GitHub を作成途上文書のバージョン管理や作業コラボレーション支援にも使っているところである。このため、世界中の人々が EUDIW ARF の更新・作業状況およびそれに基づくコンポーネントの開発状況を、同時進行で確認することができるようになっている。ソフトウェア開発などにおいてこうした共有・管理サービスを活用することは既に一般化しているが、日本で規制や行政文書を GitHub で管理運営している先はないのではなかろうか[13]。本稿執筆時の最新版は、EUDIW ARF1.4.1 版であるが、以下では、所報 6 号執筆の際に使用したものと同じ EUDIW ARF1.4 版をもとに、「リファレンス・アーキテクチャ」について解説する。

EUDIW のリファレンス・アーキテクチャについて

図表３は、EUDIW のエコシステムとそのコンポーネントのアーキテクチャの概要を示したものである。なお、技術的内容になるため、正確性を期すため、以下ではコンポーネント名等に関しては英語表記を中心に用いている。

（図表３）EUDIW ソリューションのリファレンス・アーキテクチャ



出所：欧州委員会ホームページ

【コア・コンポーネント】

EUDIW ソリューションのコアとなるコンポーネントとしては、以下のものがある。

User device（UD）：User device は Wallet Instance をホストするためのデバイス。自然人（個人）は通常モバイルデバイスを使うことになるが、法人の場合はクラウドサーバーを使うことも想定される。

Wallet Instance（WI）：User device 上にインストールされたアプリまたはアプリケーション。コアビジネスロジックとインターフェースを実装しており、WSCA/WSCD と直接対話することで、認証の高い保証レベルを確保している。

Wallet Secure Cryptographic Device（WSCD）：WSCD は、暗号鍵等を管理するためのセキュアな環境とストレージを提供するデバイス。改ざん防止および複製防止が対策済みの信頼できるハードウェア。

Wallet Secure Cryptographic Application（WSCA）：WSCA は、WSCD 上で実行されるセキュリティ関連のアプリケーション。一つの WSCA は一つの Wallet Instance に限定して関連付けられ、特定の Wallet Instance のアセット（暗号鍵など）を管理する。

Wallet Provider backend（WP）：WP は、ユーザーに Wallet Instance のサポートを提供し、必要なメンテナンスを行い、Wallet Provider Interface（WPI、後述）を通じて Wallet Trust Evidences と Wallet Instance Attestations を発行する処理システム。

【インターフェースとプロトコル】

図表 3 に示されるインターフェースとそれぞれのプロトコルは、欧州デジタル ID 枠組み規則の第 5 条 a 項第 5 号で定められた仕様に準拠している。主なものとしては下記の仕様がある。

Wallet Provider Interface（WPI）：Wallet Instance が WP と通信するために使用される。Wallet Trust Evidences と Wallet Instance Attestations の発行に用いられる。

The User Interface（UI）：ユーザーと Wallet Instance 間のやり取りが行われる接点である。

Presentation Interface（PI）：Relying Party（依拠当事者）が EUDIW から PID（個人識別データ）や様々な証明書（QEAA、PuB-EAA、EAA など）を安全に要求して受信できるようにするインターフェース。リモートと近接通信の両方に対応する。リモートプレゼンテーションフローのために、Wallet Instance は OpenID for Verifiable Presentation プロトコル（OpenId4VP）を実装する。一方、近接プレゼンテーションフローでは、ISO/IEC 18013-5 標準に準拠する。なお、リモートフローでは、Relying Party がサービスを提供するためにユーザー認証とデータアクセスを必要とする場合、ウェブブラウザまたはモバイルアプリのいずれかを介してプロセスが開始される。

Secure Cryptographic Interface（SCI）：Wallet Instance が WSCA と安全に通信するためのインターフェース。暗号資産の管理と暗号機能の実行のために特別に設計されて

いる。

PID Issuance Interface（PPI）：Wallet Instance が PID Provider と通信するためのインターフェース。OpenID4VCI プロトコルに基づいており、Wallet Instance 内に格納される PID を要求したり受け取ったりするときに使用される。

Attestation Issuance Interfaces (AII)： Wallet Instance が様々な EAA（電子属性証明）を要求する際に使用されるインターフェース。OpenID4VCI プロトコルに基づいている。

Remote Signing Interface (RSI)：Wallet Instance が QES（適格電子署名）リモートサービスプロバイダと通信するためのインターフェース。QES リモート署名の実行に使用される。

【EUDIW と Relying Party の間の通信方法】

EUDIW（Wallet Instance）を Relying Party（依拠当事者）に提示するプレゼンテーションインターフェースの実装では、4 つの異なる通信フローが定義され、用途によって使い分けられる。

近接監視フロー（Proximity Supervised Flow）：EUDIW ユーザーが物理的に Relying Party の近くにいる対面の場合の通信フローであり、Wallet Instance と Relying Party Instance の間で近距離無線通信技術（NFC、Bluetooth 等）を使用して、EAA（電子属性証明）が交換される。この間、Relying Party 側の代表者（人間）がプロセスを監視する。

近接非監視フロー（Proximity Unsupervised Flow）：近接監視フローと似ているが、Relying Party が機械である点が異なる。EUDIW は人間による監視がない中で、Relying Party として機能する機械に対して EAA を提示する。

遠隔デバイス横断フロー（Remote Cross-Device Flow）： このケースでは、EUDIW ユーザーは、EUDIW とは分離されている別のデバイスを使ってサービス情報を閲覧する。EUDIW は安全なセッションを結ぶためにのみ使用される（例：オンラインサービスにアクセスする際に、EUDIW でログインページの QR コードをスキャンする等）。

遠隔同一デバイスフロー（Remote Same-Device Flow）： このケースでは、EUDIW ユーザーは、オンライン接続におけるセッションのセキュリティ保護と、情報交換を含むデジタルサービスの利用の両方で、EUDIW デバイスを使用する。

Relying Party がサービスを提供するためにユーザー認証といくつかのデータを必要とする場合、サービスのプロセスはウェブブラウザまたはモバイルアプリのいずれかで開始される。特に遠隔同一デバイスフローでは、サービスプロバイダが EAA（電子属性証明）やデータを必要とする時はいつでも、ユーザーのブラウザやアプリは EUDIW にリクエストをリダイレクトする。

これとは対照的に、遠隔デバイス横断フローと近接監視フローおよび近接非監視フローでは、ウェブブラウザとのやり取りを必要としない NFC タップまたは QR コードのスキャンに

よって Wallet Instance をアクティブ化することからサービスプロセスが始まる。

【WSCD の実装方法別アーキテクチャ】

暗号機能等の高い安全設計に基づく EUDIW ソリューションは、WSCD（Wallet Secure Cryptographic Device）の実装方法によって、少なくとも 4 つの異なるタイプのアーキテクチャに分けられる。

リモート WSCD： HSM (Hardware security module)を使用して Wallet Provider によって実装された機能を使用するアーキテクチャで利用されるデバイス。WSCD はユーザーのデバイスとは別の遠隔地に設置されている。

ローカル外部 WSCD：デバイスにセキュアエレメントのような十分安全なハードウェアがない場合、セキュリティを強化するための外部機器が必要になる。例えば、ユーザーのデバイスに接続して暗号化機能を提供する外部 WSCD（ハードウェアトークンやスマートカードなど）が使われる。

ローカル WSCD：ユーザーのデバイス内に WSCD が直接統合されているアーキテクチャで利用されるデバイス。これには、eSIM/eUICC や eSE （内蔵セキュリティエレメント）などのソリューションが使われる。WSCA（例えば Java カードアプレット）は Wallet Provider によって配置される。

ハイブリッド・アーキテクチャ：前の 3 つのアプローチのうち 2 つ以上を組み合わせたもの。

最後に

本レポートでは、EUDIW の eIDAS2 発効後の動向を紹介するとともに、EUDIW のリファレンス・アーキテクチャの概要について解説した。EUDIW では、「ウォレットは多種多様であっても、仕様はヨーロッパ共通（One European set of specifications. Many different wallets.）」と謳われている。EU 全域で国境を越えてシームレスに機能するウォレット構築に向け、共通の標準仕様を定めるとともに、これを実施法で参照することで実効性を確保しており、すべての EU 加盟国のすべてのウォレットの仕様に反映される仕組みとなっている。各加盟国は、eIDAS2 発効に基づき、2026 年までに、国民、居住者、企業に向けて少なくとも 1 つの EUDIW を提供[14]することが義務付けられている。今のところ、スケジュールは守られており、EUDIW はリリースに向けて着実に進捗しているように見受けられる。

以　上

1 中山靖司「欧州デジタル ID ウォレットの共通仕様」、SBI 金融経済研究所所報第 6 号、2024 年 8 月（https://sbiferi.co.jp/assets/pdf/review/review_vol06_04_202408.pdf）

2 eIDAS2: electronic identification, authentication and trust services 2.0

3 https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/14341-European-Digital-Identity-Wallets-integrity-and-core-functionalities_en

4 https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/14339-European-Digital-Identity-Wallets-protocols-and-interfaces-to-be-supported_en

5 https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/14340-European-Digital-Identity-Wallets-person-identification-data-and-electronic-attestations-of-attributes_en

6 https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/14338-European-Digital-Identity-Wallets-trust-framework_en

7 https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/14337-European-Digital-Identity-Wallets-certification_en

8 https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/14399-European-Digital-Identity-Wallets-registration-of-relying-parties_en

9 https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/14400-European-Digital-Identity-Framework-cross-border-identity-matching_en

10 https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/14401-European-Digital-Identity-Wallets-security-breaches_en

11 https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/14402-European-digital-identity-framework-verification-of-electronic-attestation-of-attributes_en

12 https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/14403-European-Digital-Identity-Wallets-list-of-certified-wallets_en

13 行政文書ではないが、ツールやデータに関しては、日本の省庁でも GitHub を活用した事例はある。例えば、住所の表記揺らぎに対応した住所ベースレジストリの提供（デジタル庁）、AI 技術や新素材に関連する契約書の見本「モデル契約書」の改訂における意見募集（経済産業省と特許庁）、政府統計ポータルサイト e-Stat の API 機能を使ったアプリの公開（総務省）等の例がある。

14 EUDIW は、「デジタル権利と原則に関する EU 宣言（2022 年 12 月 15 日）」（https://digital-strategy.ec.europa.eu/en/policies/digital-principles）に概説されている原則に準拠しており、 2030 年までに EU 市民の 100%がデジタル ID にアクセスできるようにするという「デジタル 10 年政策プログラム」（https://eur-lex.europa.eu/eli/dec/2022/2481/oj）の目標達成に貢献するとしている。