數位皮夾設計規劃

Taiwan Digital Identity

Decentralized Identity Public Service for Authentication and Authorization

Version: 0.9.9.b
Date: 2024.1.12
Ministry of Digital Affairs, Taiwan

Disclaimer: This content is a working draft and does not represent the official opinion of a specific agency. This document has been translated into English using machine translation. The original document was written in Traditional Chinese. If there are any errors, please do not hesitate to inform us by letter.

Contact person: mashbean Huang (Department of Democracy Network)
Contact email: mashbean@moda.gov.tw
Contact number: 886-2-23800334

Table of Contents

Objective

This project aims to establish the "**Digital Wallet**" (officially known as the **Decentralized Digital Identity Authentication and Authorization System**, referred to in English as Taiwan Digital Identity Wallet, TW-DIW) as a fundamental public service for Taiwanese users by the year of 2027. Users will be able to exercise their "Self-sovereign Identity (SSI)" through the process of authorization and authentication of digital identity. This service will be effectively integrated with various mobile devices, browsers, identity issuers, digital service providers, and web3 developers, and become a cornerstone of digital services and embedded within specific services. On the one hand, it will accelerate the digital transformation of government agency credentials and, on the other hand, assist private identity issuers in adopting more secure and interoperable identity interface services. The public can use this service to interact with different digital identities through various channels such as government websites, cross-border platforms, international affairs, and e-commerce, and complete identity authentication and authorization functions in simple, secure, and convenient manners. Additionally, as this project is open source, we expect it to become one of the packages that could be used in other digital infrastructure in more countries by 2027.

These are the three core objectives of this project:

1. To create a signature and authentication mechanism that balances privacy and convenience, thereby fundamentally **preventing deep fakes and digital fraud**.
2. To **provide a secure and convenient digital transformation solution** for government agencies' credentials, accelerating the realization of the goal of “smart nation”.
3. To construct an identity interoperability agreement **for cross-border recognition**, enhancing the convenience of overseas or digital living for citizens..

Description

"Digital Wallet" is a decentralized identity system for digital life daily, and is in line with modern digital human rights. Its core functions are **authentication (AuthN) and authorization (AuthZ)**. This project does not issue a centralized digital national identity. Instead, it constructs the de facto identity of citizens using various types of documents issued by Taiwan's public and private sectors, thus providing essential digital identity services and aims to achieve the goal of "autonomy in personal identity and data authorization." This service is part of Taiwan's Digital Innovation Key Infrastructure Plan, marking Taiwan's digital public infrastructure project, with the work item being called as "Cross-Border Data Authentication and Authorization Control System."

Just as in real life, where people can put their ID cards, employee badges, credit cards, and loyalty cards in a wallet, digital life also requires a wallet for purposes like "proving who you are" and "authorizing others." Public and private sectors, as well as individuals, can place issued credentials in the wallet. These credentials can be official documents like ID cards, email accounts, academic certificates, as well as leisure-related vouchers like membership cards or entry tickets.

For issuers of credentials or identities, the "Digital Wallet" is a software development toolkit (SDK) and interface. It helps any identity issuer, such as government digital certificates, corporate financial certificates, or individuals, to integrate already issued digital credentials. These are automatically converted into "cards" that comply with Decentralized Identifiers (DIDs) and Verifiable Credentials (VCs) standards, stored in the user's (Holder's) "Digital Wallet." This process is known as authentication (AuthN). For users, the "Digital Wallet" is an operational interface, an application, or web service, allowing users to authenticate any identity.

Users can decide whether to activate these identities' authorization features, applying them to external services such as government signatures, corporate activities, or general entertainment purposes. This process is known as authorization (AuthZ). The authorization process adheres to privacy-preserving principles and undergoes layered authorization to minimize the risk of revealing too much identity

information. This includes the use of Zero-Knowledge Proofs (ZKP) or other cryptographic algorithms. Users personally manage the related authorization functions and can cancel the authorization service at any time. This model is therefore known as the "authorization switch." The technical specifications behind the user's authorization switch should be able to interface with any service that meets interoperability standards, such as the default wallet provided by mobile operating systems, blockchain wallet services, or digital identity wallets from other countries. Regardless of whether the authorized party is a government agency, corporate service, or individual, all can become verifiers to authenticate the user's identity.

Furthermore, just as a person can have more than one wallet in real life, in the digital world, users can also have multiple "Digital Wallets" to segregate different types of identity credentials. Users can revoke and create these credentials at any time without worrying about their digital footprint and identity being tracked by malicious actors.

To effectively construct a "composable, cross-border, non-exclusive" cooperative model, the aforementioned decentralized identity-related credentials can be stored in public blockchains or decentralized storage systems. This allows these privacy-protected credentials to be in an interoperable state and available for notarization by non-exclusive third parties, thereby facilitating cross-border use cases, such as mutual recognition of digital passports, international driver's license usage, and more. This project is committed to creating a Digital Wallet that is suitable for developers around the world to fork, especially enabling integration with mobile device services, browser developers, and government services of various countries, and effective use of SDKs and APIs, allowing the Digital Wallet developed by Taiwan to be applied cross-border.

The "Digital Wallet" incorporates the spirit of the Web of Trust from the PGP (Pretty Good Privacy) asymmetric encryption protocol, aligns with the next-generation decentralized identifiers and verifiable credentials data model standards (W3C Decentralised Identifier, Verifiable Certificate Data Model), the European Union's digital identity wallet (EUDIW) under eIDAS 2.0 (electronic Identification,

Authentication and Trust Services), and various web3 digital identity services such as Gitcoin Passport, Polygon ID, World ID, etc. It will become the next generation of reliable digital infrastructure for citizens' identity linkage and extended services. This is further detailed in Appendix 5.

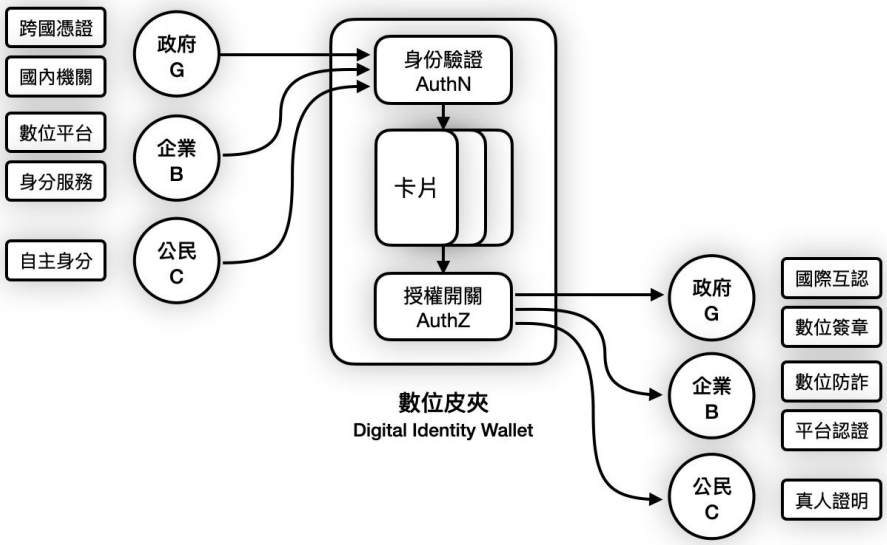


Figure 1, Functional Diagram

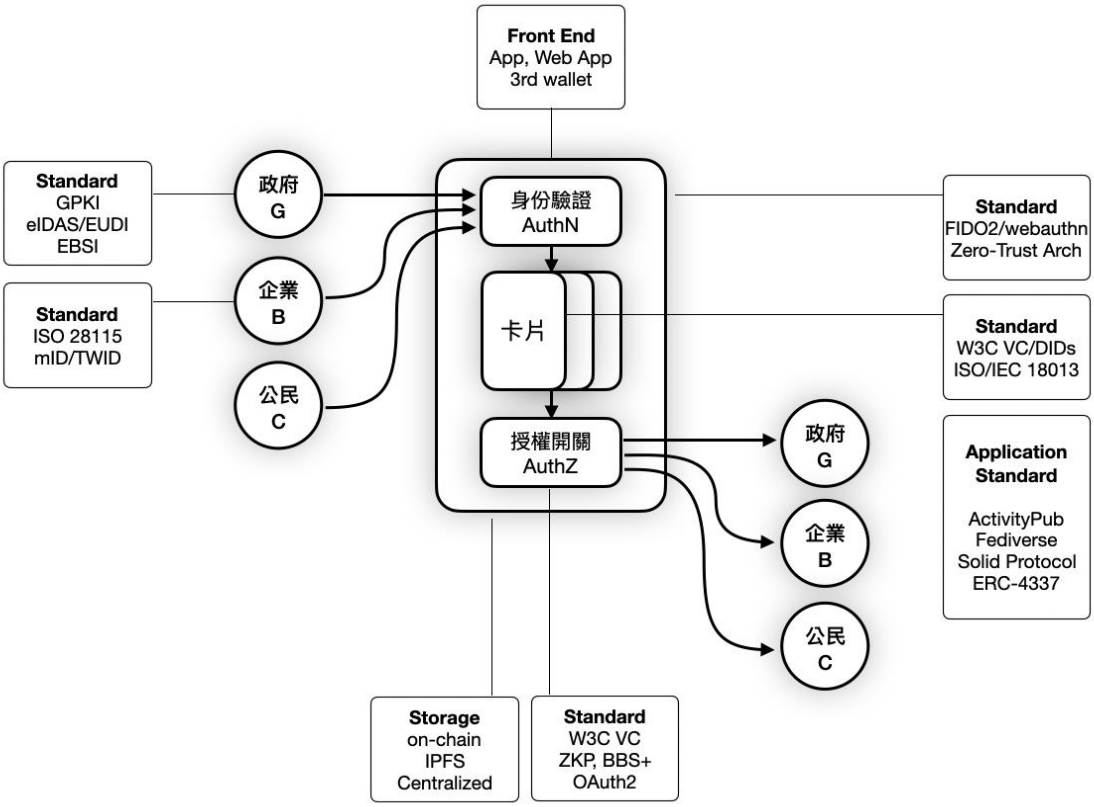


Figure 2, Schematic Diagram of Relevant Specifications Inventory

Features

The "Digital Wallet" (Decentralized Digital Identity Authentication and Authorization System) has the following features:

1. **De facto Identity:** It represents factual identity, as opposed to a centralized single legal identity.
2. **Self-Sovereign Identity (SSI)**: Users can cancel or close the interfaced identity at any time, known as the "master switch" design.
3. **Composable & Programmable Social Relationship:** Social relationships are modular and programmable.
4. **Permissionless and Open Source:** Everyone can develop, adopt, and interface without government permission.
5. **Compatible with Cross-Border & Future Digital Needs (e.g., web3):** The related storage credentials are stored in public blockchains or decentralized storage services.
6. **Passwordless:** Utilizes biometric recognition or hardware keys, and complies with FIDO standards or similar.
7. **Secure & Privacy Preserving:** Adheres to the principle of minimal disclosure and public key infrastructure methods, achieving the goal of "authentication required for each login" and "protection for each authorization."
8. **Functional Equivalence:** Complies with national and international laws and agreements.
9. **Resilience & Social Recovery:** The entire system avoids the risk of single server failure. Even if the holder's device is stolen or the server room is destroyed, the holder can still quickly re-establish their identity.

The "Digital Wallet" **will not**:

1. Issue new identities.
2. Store unnecessary personal data.
3. Store biometric data and private keys on government servers; such data is only stored on user devices.

4. Act as a decentralized identity with an object as the subject, such as trade objects, digital transaction objects, etc., although future compatibility is not ruled out.

Stakeholders

This chapter describes the scenarios in which various stakeholders use this service.

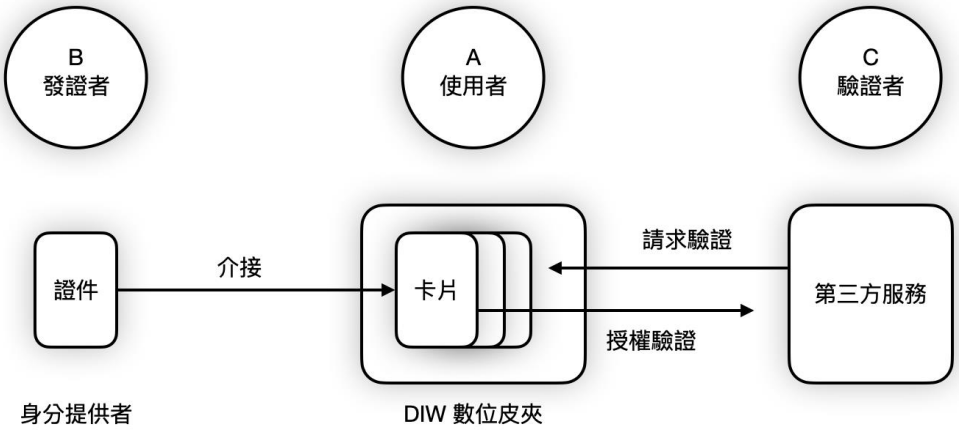


Figure 3, Service Requirement Illustration

A. User (or Credential Holder)

1. Users can be natural persons, legal entities, or non-legal entities.
2. Users hold a Decentralized Identifier (DID) as the wallet address to receive "cards."
3. The Digital Wallet is a public service; users can use it for free and without the need to create a new account.
4. Users can freely log in to various service accounts and store them in the form of "cards."
5. When facing new demands, users can agree to the link requests of various "cards" with one click, but the system will provide warnings.
6. The linking status of each "card" will be displayed in card format, listing the service providers with linking requests for easy user management.
7. Users can cancel the identity or linking status of a "card" at any time (opt-out).
8. Except for the verifier, others cannot know who holds a "card."
9. Obtaining a "card" is free and can be done within seconds.
10. Users can log in using biometric recognition or a hardware key without needing to remember a password.

11. When users undergo repeated identity service verification, the previous "card" will automatically become invalid (replacement principle).
12. Each authorization in the Digital Wallet requires biometric recognition or a hardware key, or the activation of Multi-Factor Authentication (MFA) services based on the trust level.

B. Issuer

1. Issuers can be government agencies, commercial legal entities, foreign agencies, or individual natural persons, such as:
    a. Telecom service providers, like SIM card identity or mobileID.
    b. Digital service identity providers, like Google ID, Line ID, TWID.
    c. Government-related credential issuing agencies, like TW FidO.
2. Credential issuance levels are based on the Digital Signature Act and electronic signature regulations.
3. Natural persons can issue "cards" to other natural persons or legal entities.
4. Issuers can provide new "cards" to users through their services (such as existing identity providers).
5. Each "card" corresponds to only one account.
6. Every "card" has a life cycle and requires periodic linking.
7. Issuers can cancel the "cards" they have issued at any time.
8. Issuers can decide whether to issue "cards" for the entire account list at once or let users decide whether to join (opt-in).
9. Issuing "cards" is free of charge.
10. Before issuing, issuers must fill out a standardized form, letting other verifiers know when and where there is a need for mutual connection.
11. Issuers can offer to transfer existing identities (IC or non-IC digital identities) or issue new identity services.
12. Each identity issuer has the right to delete "cards."

C. Verifier

1. Verifiers can develop authentication features that are interoperable with this service at any time.
2. Verifiers can request user authorization for "card" authentication, but the system will automatically maintain the principle of minimal disclosure.

3. Verifiers have a list of different levels of authentication recommendations and grades for reference.
4. There will be a lightweight user interface for verifiers with counter authentication needs.

D. Administrator

1. The Ministry of Digital Affairs (Taiwan) is responsible for system maintenance and upgrades, managing the official version of the Digital Wallet according to the criteria set, and releasing the source code under the open-source license.
2. The Ministry of Digital Affairs (Taiwan), based on relevant international standards, establishes a list of Authenticator Assurance Level (AAL) recommendations and sets up a list of certified issuers with corresponding application methods.
3. The Ministry of Digital Affairs (Taiwan), along with relevant cybersecurity authorities, provides response plans against threats.

Service Requirement Explanation

This section describes the definitions and requirements of each service component.

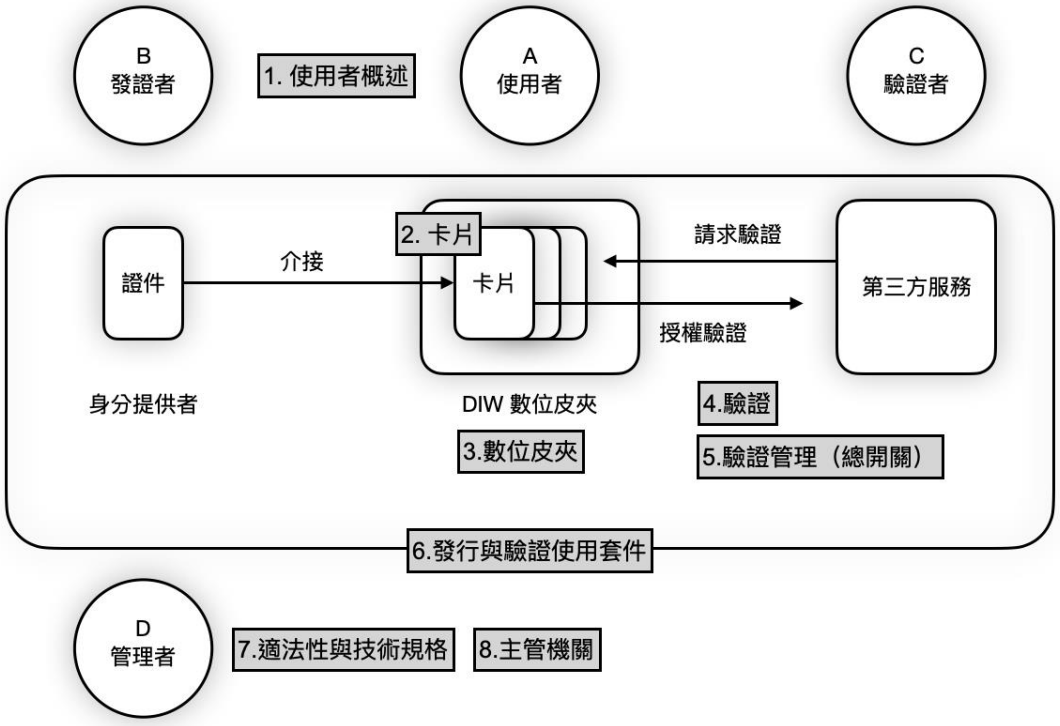


Figure 4, Service Requirement Explanation Diagram

0. Definitions

1. Authentication (AuthN): The process of confirming that a user has a certain identity or owns a certain asset through specific means.
2. Authorization (AuthZ): The process where a user (holder) gives permission to a verifier to perform specific tasks. In this context, it usually represents the holder linking certain credentials to the verifier, enabling or disabling certain services.
3. User, or Holder: An individual or organization that applies for credentials in the Digital Wallet and uses the Digital Wallet. (See the User section)

4. Issuer: An individual or institution that opens applications for credentials. The application process may record the applicant's personal information. (See the Issuer section)
5. Verifier: An individual or organization that determines whether the holder meets the qualifications based on the digital signature presented by the holder. (See the Verifier section)
6. "Card": A verifiable credential stored in a Decentralized Identifier (DID) format that can be verified by non-specific third parties. Its specifications comply with standards set by the World Wide Web Consortium (W3C) and other relevant standards.
7. Arbitration and Supervisory Authority: According to the laws of the Republic of China, an authority that can independently influence the effective status, activation status, and interfacing status of the "card," separate from the holder and issuer.
8. Multi-Factor Authentication (MFA): A method of confirming identity based on three attributes: 'Something You Know' (e.g., passwords), 'Something You Have' (e.g., cards and mobile phones), and 'Something You Are' (e.g., biometric characteristics). For medium trustworthiness (AAL2) and above verifications where errors can cause significant loss, at least two types of factors must be verified simultaneously.

1. User Overview

This section provides an overview of the overall functionality of the Digital Wallet and describes the conditions required to become an issuer, verifier, or holder, as well as the respective responsibilities they need to bear. These three roles correspond to the three sections of the descriptive requirements inventory.

1. The Digital Wallet (DIW) provides easy identity linking, enabling holders to pass various checks in work and life simply by presenting "cards" from their Digital Wallet.

1.1. **Cards:** Credentials for verification through DIW, originating from verifiable digital credentials and Decentralized Identifiers (DID). "Cards" are recorded in DIW through specific interoperable protocols or standards.

1.2. **Holders:** Both domestic and foreign individuals or groups can become holders.

1.2.1. No application is required to become a holder. Once any "card" is interfaced with DIW, one becomes a de facto holder. (See User section)

1.2.2. Holders are responsible for the custody of their DIW.

1.3.**Issuers:** Subject to legal limitations, both domestic and foreign central and local government departments, private companies, non-profit organizations, non-legal entities, and individuals can issue "cards" and become issuers. (See Issuer section)

1.3.1. No application is required to become an issuer.

1.3.2. Issuing "cards" is free of charge.

1.3.3. Issuers must publicly present the conditions and regulations for applying for "cards," and specify what data and proofs need to be provided. (For example, applying for a digital driver's license requires in-person processing and authentication; Google accounts and corresponding credentials must be verified by Gmail verification codes; mobile natural person credentials and corresponding Digital Wallet credentials only need TW FidO authentication, etc.)

1.3.4. The data specifications of the "cards" issued by issuers must comply with the standards set by DIW, including W3C DID 1.0 or VCDM 1.1 Recommendation, eIDAS2.0, ISO/IEC 18013-5, ISO29115, NIST-SP800-63, etc. (See Appendix 5, Digital Wallet Standards Inventory)

1.3.5. The issuance level of "cards" must comply with the digital signature specifications of the Electronic Signature Act.

1.3.6. Issuers are responsible for the inspection data and proofs during issuance.

1.3.7. Issuers are responsible for the custody of the key pair used to issue "cards".

1.3.7.1. When conducting business with smart IC cards, government agencies, financial institutions, and other licensed organizations must comply with

existing national regulations on electronic key custody, following the government's public key infrastructure (GPKI) framework.

1.3.8. Issuers are responsible for the custody of data provided by holders when applying for "cards". Issuers must adhere to the principle of minimal disclosure and not reveal unnecessary holder attributes to third parties.

1.3.9. Each jurisdiction has its own verification and authorization regulations and technical standards. If "cards" are to be used internationally, standards for "card" and data custody, and compliance with corresponding legal responsibilities in the relevant jurisdiction, are the responsibility of the issuer. (For example, the EU's GDPR grants users the "right to be forgotten". If issuers want the "card" to be usable in the EU, they must ensure that the "card" and database can be made permanently inaccessible through certain operations.)

1.4. **Verifiers:** Subject to legal limitations, both domestic and foreign individuals or groups can become verifiers. (See Verifier section)

1.4.1. No application is required to become a verifier.

1.4.2. Verification with "cards" or requesting holder authorization of "cards" is free of charge.

1.4.3. Verifiers can list approved "cards" based on the attributes they wish holders to possess, such as educational background, property, activity records, etc.

1.4.4. Verifiers can request holders to authorize single or multiple "cards", verifying whether holders meet the requirements based on the logical relationships between different "cards".

1.4.5. Verifiers can open or close corresponding digital services based on the authorization of "cards". (For example, a social media platform determines that account A is linked to B's natural person credential and thus grants account A a blue checkmark.)

1.4.6. Verifiers are responsible for the effects of the verification level settings (such as AAL1, AAL2, AAL3).

1.4.7. Verifiers must comply with national laws and restrict or terminate the verification of corresponding "cards" and holders according to the latest

list issued by supervisory and arbitration authorities. Verifiers bear the responsibility for non-compliance with relevant laws.

1.5. **Duality:** The issuer of the same "card" can also be a verifier. (For example, membership cards, social platforms that manage identity systems and also provide digital services.)

2. "Card"

This section describes the file nature of "cards," the data they can record, and the attributes or tags they must have. It mainly corresponds to the descriptive requirements inventory section for "issuers."

2. **Definition:** A "card" is a digital credential stored in the Digital Wallet, verifiable by non-specific third parties, stored in the format of Verifiable Credential (VC) and Decentralized Identifier (DID). It is issued by the issuer, interfaced on DIW, and then authorized to the verifier.

2.1. **Attributes:** The attributes of each "card" that can be verified are determined by the issuer. For example, some "cards" can prove that the applicant is a natural person, some can prove ownership of certain property, some can prove passing a particular exam, some can prove joining an organization or website, some can prove the applicant has purchased drinks at a location, and some simply prove access to a specific security level area.

2.2. **Attribute Format:** The data specification of "cards" must cover all verification needs in work and life, including but not limited to: identity documents, proof of property, service credentials like health insurance cards, membership cards, website login credentials like username and password, admission tickets, proof of purchase, notices, letters of intent, declarations, etc. These verification needs must be met by a single "card" and by the logical relationships between multiple "cards."

2.3. **Necessary Attributes:** "Cards" must include the following necessary attributes, and the attribute content must not be empty:

- Issuer
- Applicant
- Issuance Time
- Expiry Date
- Sensitivity of Data Attached at Issuance

2.4. **Issuer Uniqueness:** The data format of the "card" must ensure the uniqueness of the issuer's identity.

2.5. **Optional Attributes:** "Cards" may include the following non-essential tags:

- Verifiable values, strings

2.6. **Validity Period:** "Cards" must automatically expire at the end of their validity period (life cycle management).

2.6.1. "Cards" must notify the holder to reapply before the expiry date, via DIW, SMS, Email, etc., according to the agreement between the issuer and the holder.

2.6.2. "Cards" must have a default auto-disable function. If a holder's "card" is not interfaced with DIW or not authorized to a verifier within a certain period, it will automatically be disabled and require the holder to reactivate it.

2.7. **Application Fee:** Applying for "cards" is free of charge.

2.8. **Application Time:** The operation time from the issuer accepting the application to the holder receiving the "card" must be shorter than or equal to the most efficient application operation time in current digital business (e.g., general SMS or Email notification).

2.9. **Non-Repudiation:** After issuance, "cards" must remain accessible to the applicant. Officially certified issuers must have an interface allowing applicants to always check which "cards" they have applied for, even if some have expired or

been revoked, unless the user deletes this requirement themselves. This feature makes each "card" and the necessary attributes listed in 2.3 unchangeable, or modifiable only after written agreement by both parties.

2.10. **Access Control:** Under normal circumstances, only the issuer and holder can change the status of a card, such as issuing, updating, revoking, etc. Others cannot alter the content.

2.10.1. **Exceptional Circumstances:** When the issuer or holder violates the laws of the Republic of China, or the use of the "card" violates the laws of the Republic of China, the statutory authority can, according to the corresponding legal procedures, list related "cards" that should not pass verification for verifiers to follow. See sections 5 and 7 for related items.

3. Digital Wallet (DIW)

This section describes the product requirements of DIW, the role of its users, how it is used, and how to operate "cards" with DIW. It mainly corresponds to the descriptive requirements inventory section for "users."

3. **Definition:** DIW is an operational interface for the credential holder, including mobile applications, web pages, or other methods.

3.1. **Permissionless Use:** DIW can be activated immediately upon download or on a web page. The activation process does not require any application for permission and does not verify any data. This applies to issuers, holders, and verifiers.

3.2. **Passwordless:** DIW adopts a no account-password (ID-Password) management model and must comply with technical standards such as FIDO2/webauthn, including biometric recognition, mobile device password generators, hardware keys, etc. It can use services like multi-device credentials or Passkeys.

3.2.1. **Multi-Factor Authentication (MFA):** DIW must have "multi-factor authentication" functionality. Interfacing, activating, pausing, and disconnecting each "card" must trigger multi-factor authentication. Authentication standards must meet the corresponding Authenticator Assurance Level (AAL).

3.2.1.1. DIW can activate each "card" through private keys generated by biometric recognition, hardware keys, or password generators.

3.2.2. **Private Key Autonomy:** The private keys and biometric data of DIW must comply with corresponding cybersecurity standards and be stored only on the holder's personal device (not stored anywhere else). For different devices of the same person, such as mobile devices, web pages, and plugins, connectivity can be achieved through third-party Passkeys or other OpenID Connect (OIDC) standards.

3.3. **Blockchain Attestation:** DIW can read and write "card" statuses on the public blockchain, such as application, cancellation, identity linking, suspension of use, reactivation, etc.

3.3.1. 3.3.1. The way DIW operates the status of "cards" should consider the "right to be forgotten" for service providers with relevant situational needs. Officially certified issuers must include a cancellation function, allowing holders to cancel the link between the specified "card" and their original identity.

3.4. **Multiple Holdings:** Natural persons, legal entities, or groups can simultaneously hold multiple DIWs.

3.5. **Custodial Responsibility:** DIW is not reissued if lost, nor is it necessary. Users can recreate a wallet and relink each "card." Related "cards" are stored on the user's end. Lost "cards" will expire on the due date or automatically become invalid when the same "card" is re-applied. If the device is lost and users suspect that the private key for biometric recognition or hardware key has been compromised, they can contact the issuer of each "card" for revocation.

3.6.1. If a device using DIW is lost or deleted, and service restart is required, the holder will relink and bind identity documents.

3.6. **Replacement Principle:** By default, once a "card" corresponding to a particular individual is interfaced with a new DIW, it is automatically disconnected from all other DIWs (i.e., the "card" in the old DIW becomes invalid or is deleted).

3.7.1. **Exceptional Cases:** In some exceptional cases, a "card" can be interfaced by multiple DIWs. For example, a parent can interface a child's health insurance "card." Such exceptions are determined by the issuer.

3.7. **Interoperability:** DIW must be able to interface with all "cards" issued according to corresponding specifications and mark itself as currently holding these "cards."

3.8. **Accessibility and Access Control:** DIW must have a clear visual way for the holder to activate, temporarily close, and disconnect the identity link of each "card."

3.9.1. DIW must display the necessary tags for each "card," with the list of necessary tags mentioned in 2.3.

3.9. **Principle of Minimal Disclosure:** Non-essential tags for each "card" are by default hidden in the DIW interface.

3.10.1. DIW must include a UI function to display tags, allowing users to reveal non-essential tags of a "card" through flipping over, additional clicking, etc.

3.10. **Privacy Protection Principle:** Information sent out by DIW must not enable any party other than the holder to identify who is currently interfacing with each "card" inside DIW, and must comply with the principle of minimal disclosure in 3.10.

4. Authentication

This section describes the method of authentication using DIW, mainly corresponding to the descriptive requirements inventory sections for "users" and "verifiers."

4. **Definition:** The authentication that each DIW can pass is entirely determined by the "cards" that are interfaced and activated in DIW.

4.0.1. **Neutrality:** DIW is not a credential and does not integrate any credential data. It has no ability to influence the outcome of any authentication.

4.0.2. **Decentralized:** The authentication process of DIW does not require any external service, only recognition of the issuer by the verifier. Thus, any authentication that can be completed with current electronic verification methods can also be completed by DIW.

4.1.**Items to be Verified:** Each item to be verified is a symbolic logic equation.

4.1.1. The item to be verified must be composed entirely of AND, OR, NOT, EQV (equal to), > (greater than), < (less than), and codes of each "card." (For example, to distribute subsidies, the requirements might be "ID card or natural person credential" and "any financial account," represented by the symbolic logic sentence ((id0001 or id0002) and (fin0001 or fin0002 or …)).

4.1.1.1. **Programmable:** Verifiers can freely combine the desired attributes of the holder using the above symbolic logic equations, making the process of issuing and verifying credentials freely combinable, programmable, and more decentralized than the current state, allowing third-party users to be creative and combine more potential verification scenarios, achieving programmable social relationships.

(Example 1: Verifying "natural person credential" and "social media account" to obtain a real person verification badge, like a blue checkmark.)

(Example 2: With user consent, voluntarily disclose some health data for research purposes and obtain other platform identity benefits, achieving the goal of data collection.)

4.1.1.2. **Composable:** Composability can avoid problems encountered by current centralized credentials. Each attribute of the holder can be combined from different credentials, without needing to be centralized in a single institution, thus reducing the possibility of a single point of failure and achieving a composable state of social relationships.

(For example, credentials proving the holder is a natural person can be separate from those proving their assets; credentials proving the holder is a legal driver can be separate from those proving their residence.)

4.2. **Issuing Verification Requests:** When verifiers perform verification, they send out a symbolic logic equation of the "cards" to be verified and request a response from DIW.

4.3. **Holder Authorization:** Upon receiving the request, DIW must visually display each part of the request, indicating which "cards" can satisfy each part, allowing the holder to choose in sequence.

4.3.1. If at least one part of the "card" conditions requested by the verifier cannot be satisfied by the "cards" currently interfaced in DIW, DIW must indicate what type of "card" is missing to pass the verification.

4.3.2. If more than one of the currently interfaced "cards" in DIW can meet the verification requirements but have not been activated, the DIW interface must allow the holder to decide whether to activate that "card."

4.3.3. If the verifier's requested symbolic logic equation of "cards" would reveal too much personal information of the holder, DIW must issue a warning.

(For example, when logging into an online shopping site, DIW might ask, "Do you want to link your ID card or natural person credential?" then ask, "Do you want to link your account with Bank A, Bank B, or the Post Office?")

If the verifier is not a registered financial institution, supervisory authority, etc., DIW must pop up a window saying, "This verification will let the other

party know you are a natural person and have applied for more than 3 credit cards. Are you sure you want to continue with the verification?"

4.4. **Responding to Verification Requests:** Based on the holder's selection, DIW will send the corresponding "cards" for the verifier to check, without transmitting any other information, including the contents of the "cards" or the list of other "cards" interfaced in DIW, like the Verifiable Credentials Data Model v1.1 (VCDM) standard of W3C's Verifiable Presentation (VP).[1]

4.4.1. In the process of checking "cards," the method must comply with the principles of minimal disclosure and public key infrastructure, such as using Zero-Knowledge Proof (ZKP) or BBS Cryptosuite, in accordance with the principle of minimal disclosure in 3.10.

4.5. **Linking "Cards":** After the verifier checks the list of "cards" sent by DIW, they will link the selected "cards" to the verifier.

4.6. **Passing Verification:** The kit or application provided by DIW must allow the verifier to easily complete the authorization verification process.

5. Verification Management

This section describes "Verification Management," which involves access control rights and the lifecycle of a "Verifiable Presentation," enabling the holder to independently control the "authorization status" of the card, known as the "Master Authorization Switch."

5. **Definition:** A verifiable presentation is an encrypted display that allows verifiers to trust the original data source without seeing the original credential.

5.0.1. Each instance of verification using a "card" constitutes a verifiable presentation.

5.1. **Validity Period:** Every "verifiable presentation" has a validity period.

[1] Verifiable Credentials Data Model v1.1: https://www.w3.org/TR/vc-data-model/#dfn-verifiable-presentations

5.1.1. **Lifecycle Management:** Verifiers must set up a timing system to synchronize the validity period of each "card's" verifiable presentation with the issuer.
5.1.2. The digital wallet system must provide a display interface for the holder to view the validity period of the "verifiable presentation" after authorization has been verified.

5.2. **Access Control (Master Switch):** When a holder uses the digital wallet to pause or stop the activation status of a "card," or disconnects the identity link, the "card" cannot be included in the next "verifiable presentation." If all similar "cards" within the digital wallet are closed or disconnected, the next verification will fail.

5.3. **Informed Consent and Autonomous Decision:** When a holder changes the activation status of a "card," the digital wallet must allow the holder to confirm whether to continue receiving authorization requests for that "card." Holders must also be able to change this decision, reactivate the "card," and authorize verification.

6. Issuing and Verification Toolkit

This section describes the toolkit that needs to be developed for DIW products to facilitate the verification process of DIW and for issuers and verifiers to develop software to interact with DIW. It mainly corresponds to the descriptive requirements inventory sections for "issuers" and "verifiers."

6. **Definition:** DIW must include one or more toolkits (SDKs) and interfacing user interfaces for issuers and verifiers.

6.1. **Issuer Functionality Requirements:** The toolkit must enable issuers to issue "cards" in accordance with relevant standards, for interfacing and operation by DIW.
6.1.1. **Opt-in:** The toolkit must allow issuers to issue multiple "cards" at once based on current data, or issue them one by one upon receiving applications.
6.1.2. **Revoke:** The toolkit must enable issuers to temporarily suspend and revoke the "cards" they have issued.
6.1.3. **Storage and Transfer:** The toolkit must be compatible with future data transfer needs and possibilities, enabling issuers to establish transfer

procedures based on existing blockchain, online, or offline databases to issue, store, or transfer "cards."

6.1.4. **On-Demand Update:** The toolkit must allow issuers to batch update the status of "cards" based on the latest public and private sector credentials data, such as household registration, medical, legal information, etc. (For example, when a holder loses capacity or dies, they must be able to promptly revoke. When a holder's assets are seized, asset-related "cards" must be temporarily disabled.)

6.2. **Verifier Functionality Requirements:** The toolkit must enable verifiers to develop software and interfaces, compliant with relevant protocols, to check the conditions of "cards," link "cards," and issue verification requests to DIW, and approve the results, including automated verification processes or counter staff.

6.2.1. **Trust Requirements:** The toolkit must include a personal data disclosure level table and trust level recommendations for verifiers to review the "cards" that need to be checked and whether checking these "cards" may lead to excessive acquisition of personal data.

6.2.2. **Compliance Requirements:** To handle issues like fraud, warrants, and malicious bankruptcy, the toolkit must include features enabling verifiers and their supervisory authorities to list a ban/restricted use list based on legal procedures, automatically suspending or terminating the verification of corresponding "cards." The ban/restricted use list may include issuers, "cards," and holders.

7. Legality and Technical Specifications

This section describes the standards and specifications, legal standards, and cybersecurity standards that DIW and "cards" must comply with. It also discusses the legal status of "cards."

7.1. **Compatibility with Cross-Border and Web3 Requirements:** DIW, "cards", and the entire verification system must be compatible with corresponding Web3 standards, as well as the EU eIDAS2.0 and EUDIW standards, ensuring that

users can freely combine various functions programmatically, expanding a variety of usage scenarios.

7.1.1. Therefore, the entire system must operate through independent algorithms that are censorship-resistant, resilient, and decentralized.

7.2. **Independence:** DIW, "cards", and the entire verification system must not depend on any specific software or hardware architecture in terms of specifications.

7.3. **Legal Equivalence:** According to the "Electronic Signature Law," the legal status of all levels of "cards" is equivalent to the digital signature issued by the same issuer under the same registration requirements.

7.4. **Cybersecurity Standards:** DIW, "cards", and the entire verification system must comply with corresponding cybersecurity standards.

8. Regulatory Authorities

This section describes the regulatory authorities for DIW and "cards", and the authorities that can independently operate "cards" between issuers and holders. Corresponds to the section on "Administrators."

8. **Open Source:** DIW and "cards" are open-source services. The related source codes are made publicly available for everyone to access and use upon release.

8.1. **Maintenance Unit:** The specifications and versions of DIW and "cards" are maintained and upgraded by the Ministry of Digital Affairs.

8.2. **Regulatory Authority for Issuer Violations:** If the functionality of "cards" must be suspended due to an issuer violating the laws of the Republic of China, the corresponding "cards" list and the verifications that must be suspended for each "card" will be handled by the regulatory authorities as specified by law.

8.3. **Regulatory Authority for Holder Violations:** If the use of "cards" must be suspended due to a holder violating the laws of the Republic of China, the list of holders will be managed by the regulatory authorities as specified by law.

Conclusion

The "Digital Wallet" leverages next-generation technology standards to provide an "identity" infrastructure for authentication and authorization. This system allows various individuals, organizations, and groups with relevant needs to independently issue various types of credentials and decide what services to provide based on these credentials. This approach enables a shift away from the current centralized credential system mentality, returning to a state where each credential can prove specific attributes, establishing a decentralized verification ecosystem through a composable, programmable process.

Currently, all online verifications, online registrations, physical document verifications, and most physical verifications can be achieved through this verification ecosystem.

Furthermore, given the diversity of credential types and verification conditions in this ecosystem, it can create verification scenarios that are currently difficult to achieve.

Most importantly, the specification design of the Digital Wallet minimizes the exposure of personal data during the verification process, adhering to the "Principle of Minimal Disclosure." It also reduces the need for usernames and passwords during login, aligning with the cybersecurity trend of "Passwordless Authentication." Additionally, it programmatically facilitates the necessary verification for authorization and creates "composable" authorization conditions. Society will no longer need to entrust sensitive personal data to any one organization for issuing any authoritative credential, significantly reducing the risk of single database breaches or misuse.

The composable, programmable nature effectively mitigates threats of digital surveillance, data leaks, and data misuse, better safeguarding information security and digital human rights than existing verification methods. On the other hand, this verification system also reduces the centralization of identity documents, implementing the autonomy and resilience of identity. This enhances public trust in government governance and reduces the risk of centralized database breaches, lowering the possibility of a single point of failure.

Organizations like EU Digital Identity (EUDI) Wallet, Polygon ID, Microsoft Entra, and others are actively promoting, experimenting with, and implementing this objective. As a leading nation in digital technology and digital democracy, our country should maintain the forefront in technical specifications, ecosystem development, and promotion levels, ensuring the development potential and international attractiveness of related technology industries. At the same time, it is crucial to ensure that our country's future identity verification methods are as interoperable as possible with public and private organizations in other international democratic societies, achieving a People-first Public Private Partnership.

Appendix 1: Issues for Discussion

1. **Centralization Risk of FIDO Servers:** The FIDO architecture has a single point of failure issue because its concept is based on "something you have." It relies on specific tokens to pass multiple authentications, and the server is maintained by authorities like TW FidO managed by the Ministry of Interior's Information Service Division, Taiwan Financial FIDO managed by relevant organizations. This concept makes the "something you have" a prime target for attacks, and regardless of how data is distributed, methods like man-in-the-middle, impersonation, fake revocation, etc., can compromise it. The question is, how to design a decentralized FIDO and key management mechanism?

2. **Communication Needs Between Issuers and Verifiers:** How should changes to verification standards be managed? Should it be notified uniformly by public key infrastructure like DIW to the issuers, or should verifiers individually notify each issuer?

3. **Multi-Factor Authentication and Third-Party Services:** Does DIW need its own password generator, or should it link to the issuer's password generator? What level of cybersecurity strength is required for the password generator? Or what about SMS password verification service or Email authentication?

4. **Cybersecurity Standards:** What data and cybersecurity standards should exist for transferring existing identities (like IC card or non-IC card digital identities)?

5. **Issuer Development Toolkit:** Should the SDK include a full set of features for future issuing needs, allowing existing identity managers to issue corresponding "cards"?

6. **Regulatory Authority Determination:** Who should be the regulatory authorities for the entire infrastructure and its components?

7. **Terminology Definition:** Is there a better term for "cards"? The most intuitive is "credential," but it needs a prefix to avoid confusion with general credentials (like vouchers, talismans, cards); should the Tag of a "card" be translated as "label" or "attribute"?

8. **Functionality Settings:** Should the DIW interface display a free comment field? There's a concern about potential misuse.

9. **Functionality Settings for Lower Trust Levels:** For credentials with a low trust level, i.e., where errors have minor impacts, should the default approach for dealing with holder death, incapacity, or asset seizure be the same as for other credentials?

10. **Functionality Settings for Exceptional Cases:** In the exceptional cases of 3.7.1, should children be aware that their health insurance "card" is interfaced by their parents?

11. **Right to be Forgotten and Blockchain Storage:** How can the requirements of the "right to be forgotten" in 3.3.1 be compatible with blockchain storage? This seems to be a fundamental issue discussed since the emergence of blockchain storage.

12. **DID Credential Management:** How many DIDs should each user end of the system be allowed to hold? Just one or any number? We believe that allowing any number offers greater flexibility. According to access control principles, every user end can fully operate the status of DID and "cards" (which does not mean every user end has complete control over DID and "cards"). Such complete control would cause conflicts and increase disputes. The impact of DID and "cards" can be fully attributed to user end behavior. Whether the user end is a natural or legal person, they can bear responsibility based on their actions.

13. **Private Key Management System:** How many private keys should each user end of the system manage? We believe that integrating public and private key

management capabilities into DIW personal devices offers greater flexibility. Each "card" and DID has a public key address. As long as the DIW personal device can operate the control relationship between public and private keys, it allows:

A. One private key to manage multiple public keys and multiple private keys.

B. Specific private keys to manage specific public keys.

14. **Accountability:** When there is an issue with a "card," the ultimate request for disposition must be made to the issuer, such as in cases of forged driver's licenses or impersonation using health insurance cards, which are handled by the competent authority. Digital credentials should also be designed this way to reduce centralization risks. If the "card" is an EOA (External-owned Account), the attribution of actions and related responsibilities revert to the EOA user. DIW itself has no blockchain address and no related influence, and should not bear related responsibilities. In special needs, supervisory and arbitration agencies can list names for verifiers to stop verification.

15. **Electronic Signature:** How should users select a specific credential for signing when they have multiple "card" credentials, as the effectiveness and functionality will vary. For instance, if Alice wants to buy a game on an electronic platform, after granting permission on the platform, she can choose from her electronic platform account, natural person credential, centralized third-party login service, or even cryptocurrency account in DIW. This part requires sophisticated UX and a "default mode" to train users in the concept of SSI. A capacity can be reserved in the DIW frontend framework for future API integration with other website data, displaying the potential and impact of various credentials, thus allowing holders to choose. For example, the entire system can set up a price comparison website feature, showing the current sale price for purchasing with each "card" and indicating whether there are concerns of personal data infringement for each "card."

Appendix 2: Usage Scenarios

This appendix lists the usage scenarios for the digital wallet, corresponding user interfaces, and the demonstration project sequence.

Table 1: Inventory of Digital Wallet Usage Scenarios

		Government	Business	Citizens
web2	Nation-wide	**Digital Signatures** Cross-Platform Login Personal Data Authorization Eligibility for Subsidies	**Platform Authentication** **Identity** Anti-Fraud Membership Cards and Loyalty Programs Financial Services Non-Personal Data Login	**Autonomous Organizations** Community Initiatives
	Cross-border	**International Recognition** International Driver's Licenses Digital Passports	**Platform Authentication** Work Credentials	**Identity Verification** Message Traceability Educational Certificates
web3	Cross-border	-	**User Verification** Decentralized Finance Preventing Conspiracy Attacks	**Identity Verification** Digital Democracy Access Control Qualifications

Table 2: Inventory of Digital Wallet User Interfaces

		Issuer API/SDK		
		Government	Business	Citizens
Verifier API/SDK	G	Personal Data Authorization Subsidy Eligibility International Driver's License Digital Passport	-	-
	B	Identity Fraud Prevention Digital Signatures	Membership Cards, Loyalty Programs Financial Services Anti-Collusion Measures Decentralized Finance Work Credentials	Educational Certificates Message Tracing Digital Democracy Gate-controlled Qualifications
	C	-	-	Initiate Communities

The following scenarios are prioritized in order to demonstrate the project's importance:

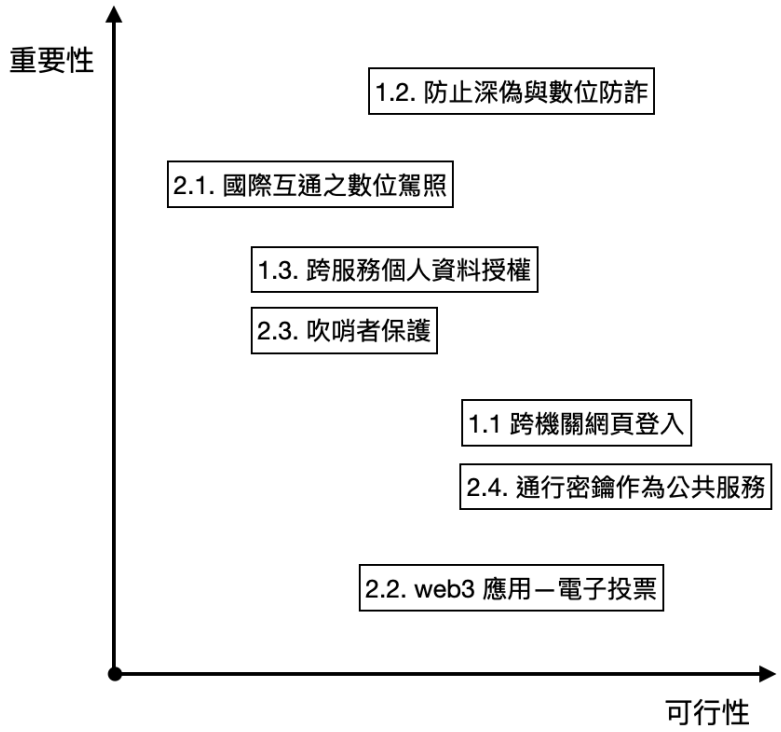


Figure 5: Inventory of Scenario Importance and Feasibility

The importance mentioned in Figure 5 refers to the infrastructure and corresponding scenarios required to create a transformation in the existing identity ecosystem. The higher the importance of the use case, the more it enables manufacturers or end-users to discover new login or authentication possibilities, open up new authentication options, and develop new login tools. This can change the current state of centralized login or reduce the risk of personal data leakage.

Importance and functional completeness are independent of each other. Even for important use cases, it may not be necessary to create a complete set of features by the first half of 2024-2025. Demonstrative functionality is sufficient during this period. The extension and ideation of features can be left for future development competitions, open-source communities, or the free market to explore.

1. Important Demonstration Scenario

This scenario has a high level of importance and feasibility. It is worth implementing as a demonstration case due to the public infrastructure requirements.

1.1 Cross-Agency Web Login (Single Sign-On, SSO)

1.1.1. Background: Currently, different government agencies in the Republic of China (Taiwan) use different login interfaces. For example, the Public Construction Commission's procurement website uses username and password, the Directorate-General of Budget, Accounting and Statistics' expense reporting system uses a natural person certificate (requires a card reader and HiCOS software), and the Ministry of Digital Development's zero-trust portal uses a mobile natural person certificate (TW FidO, requires scanning a QR code on a mobile phone). As Taiwan progresses towards becoming a smart nation, various government agencies are at different stages of digital transformation. When colleagues perform different tasks, they encounter different login methods. The Digital Wallet aims to consolidate various certificates required for different operations into "cards" and standardize the authorization method to achieve the goal of "Single Sign-On" (SSO) and "Multi-Factor Authentication" (MFA).

1.1.2. Description: Users use the DIW service to apply for the integration of certificates issued by various agencies (issuers) into the Digital Wallet, forming cards in the form of VC with DID identity. For example, if TW FidO authentication is used, the wallet obtains the "Mobile Natural Person Certificate Card," which is signed using a card reader and certificate software. After performing operations on the official Digital Wallet service webpage, users obtain the "Natural Person Certificate Card" or "Organization and Group Certificate (XCA) Card." Through the recognition of issuing agencies, the card has the same effect as the physical smart card itself and must be re-bound to the physical card within a certain period to effectively manage the lifecycle of the card. After obtaining the card, government employees (users) can log in to web service interfaces that support the Digital Wallet. They can use the Digital Wallet app to scan a QR code to log in to the website. The login process is similar to the OpenID Connect and FIDO standards' WebAuthn. The login process does not require entering a password but activates the key stored on the device through biometric authentication or hardware keys for login to the service website using the "card."

1.1.3. Challenges: Both public agencies, whether issuers or verifiers, need to agree and successfully interface or verify the services of the Digital Wallet, whether through APIs, SDKs, or applications. Additionally, government personnel need to undergo education and training.

1.1.4. Features: Reduces the inconvenience of government employees using multiple channels to log in. As it is a web service, it ensures that older systems can be accessed across platforms, reducing the problem of operating system monopolization. It can be used on Windows, MacOS, iOS, and Android platforms.

1.2. Preventing Deepfakes and Digital Fraud (Verifiable Presentation)

1.2.1. Background: Whether it's on social platforms or e-commerce platforms, there is a constant risk of fake accounts, fraudulent accounts, spam accounts, and phishing accounts. In a state of insufficient cybersecurity awareness, users are vulnerable to both personal and financial losses. However, requiring users to provide personal information can raise concerns about digital surveillance, tracking digital footprints, or enabling advertising abuse. In this dilemma, it is challenging for platforms to balance user privacy and security. Combining multiple identity credentials and minimizing the disclosure of identity status can help address these concerns.

1.2.2. Description: Users must interface with at least two cards: one for their account on a social platform or e-commerce platform and another that can be traced back to a government-issued certificate in Taiwan (such as a national ID card or documents that require an ID or national ID to apply, such as a driver's license or personal bank account, etc., referred to as "derivatives of natural person certificates"). During the interface process, users gain a "platform card" (VC/DID) through one-time password (OTP) authentication on the platform, which is the Authentication (AuthN) process. Similarly, through "derivatives of natural person certificates" login, users also obtain a platform card.

The second stage is the Authorization (AuthZ) stage, where the platform provides a QR code and sends a request to the user. Using encryption principles, the user sends a Verifiable Presentation (VP), with the message being "Platform-specific user ID and Is it a Taiwanese natural person? (Yes)." This allows the user to obtain a "real person badge" on the platform, similar to the blue checkmarks on platforms like Facebook or Twitter. If users want to revoke the "link" between the two, they can do so on the digital wallet page.

Once introduced in e-commerce or major social platforms, this service could even gradually become a widely used anti-fraud tool. Regardless of how the criminals communicate or what opportunities they claim to provide or which organization they claim to represent, they can use this tool to request proof of "natural person," "representing an organization," or "owning property," and receive an

automatic alert when verification fails. Common problems such as phantom households or zombie companies can be significantly mitigated by filtering based on factors such as "number of daily verifications for this card" and "application date for this card."

1.2.3. Challenges: Social or e-commerce platforms must play the roles of issuers and verifiers, providing relevant certification and verification services, and specially marking their pages. Users must simultaneously link government-issued certificates and platform identities. A widely-used anti-fraud tool requires cooperation from regulatory agencies and law enforcement agencies or modifications to relevant laws to allow third-party companies to verify the data.

1.2.4. Features: Linking dual identities to showcase the advantages of the "fact identity." Solves the problem of platforms being unable to determine whether users are real people, based on users' voluntary willingness.

1.3. Cross-Service Personal Data Authorization (Digital Signatures)

1.3.1. Background: When third-party services (such as financial service providers) need to use personal data from a specific platform (such as the Ministry of Digital Development's MyData platform), users often have to download the data themselves and then transfer it to the third-party service provider. A "digital wallet" can issue temporary credentials to third-party services, allowing them to download specified data.

1.3.2. Description: After users bind and obtain a natural person certificate and a "card" for a third-party service, the specific platform acts as the verifier and requests a VP from the user, such as "specific natural person and specific service user ID." After verification, the third-party service can download specific data allowed by the user.

1.3.3. Challenges: MyData needs to allow third parties to interface with personal data and support "digital wallet" services.

1.3.4. Features: Users authorize third parties to download specific platform personal data for a specific period.

2. Technical and Standard-Compatible Future Scenarios

2.1. International Interoperable Digital Driver's Licenses

2.1.1. Background: Currently, Taiwanese driver's licenses and other documents are not recognized by foreign governments. However, with amendments to the Electronic Signature Act and further international cooperation and trade negotiations, in the field of digital certificates, there is a higher chance and faster pace of mutual recognition of bilateral documents if the technical aspects are aligned.

2.1.2. Description: After users obtain a digital driver's license at a motor vehicle office, it can be automatically converted into an international driver's license, which is recognized as equivalent to a driver's license of that country.

2.1.3. Challenges: Both at the technical level (eIDAS, EUDIW, ISO 18013 mDL) and at the political level, this involves multiple stakeholders' alignment and recognition. Additionally, Taiwanese driver's licenses currently do not have IC card certificates, and the issuance process of digital certificates requires a procedure similar to in-person issuance. This relies on the motor vehicle authority and counter staff to provide issuance-side services using the "digital wallet." If the verifying party is a foreign institution and they use digital verification methods rather than just looking at the photo on the driver's license to verify authenticity, they must know how to use the "digital wallet" for verification. If there are regulations for digital wallets in that region, both sides must be able to communicate.

2.1.4. Features: Digitization of paper-based documents, mutual recognition of bilateral documents through DID.

2.2. web3 Applications - Digital Democracy (Real Identity Verification)

2.2.1. Background: Preventing collusion or preventing bots has always been a challenging issue in the cryptocurrency and blockchain space.

2.2.2. Description: When a user binds a blockchain wallet (such as an Ethereum wallet using did:ether) and obtains an address card, they can also obtain a natural person certificate card. Third-party web3 services, such as Gitcoin Passport, make requests. After the user issues a VP and is verified as a real person, Gitcoin Passport increases their real person score, which can be used for weighting donation amounts in quadratic funding, or when a centralized exchange exports funds, it can identify that the account is at least associated with a real person.

2.2.3. Challenges: Natural person certificates are not universally held, and web3 users may not necessarily want to expose their social identity, even if the "digital wallet" follows the minimum disclosure principle.

2.2.4. Features: Using domestically issued certificates to verify real identity in cross-border web3 services.

2.3. Whistleblower Protection (Real Identity Verification and Minimum Disclosure Principle)

2.3.1. Background: Many public policies, as well as law enforcement actions, rely on a significant amount of sensitive whistleblower information before they are formulated and during their implementation. Citizens who possess such sensitive information often work or live in the same environment as the subjects of their reports and are in a position of significant vulnerability. At such times, citizens may be reluctant to provide accurate whistleblower evidence due to fears of retaliation if their personal information is exposed. Similar challenges arise in cases involving violations of labor laws, factory management guidance, waste disposal regulations, workplace harassment prevention laws, and the true conditions of rental agreements and prices.

2.3.2. Description: After the user interfaces with the "derivatives of natural person credentials," a "card" (VC/DID) specifically for the whistleblower report is generated for that instance. Users use this card to access the whistleblower platform. If the authenticity of the report is highly related to the real-time and location data, the conditions for generating the "card" can be increased to include relevant sensitive personal information credentials. The platform provides fields for all the evidence required for the whistleblower report and describes the conditions for satisfying effective evidence, as well as guidelines for anonymous reporting. Once the relevant authorities review the whistleblower report, whether or not enforcement is carried out based on the evidence, the "card" becomes invalid. The platform must timely announce the number of whistleblower reports and the quantity of various types of evidence submitted but should not disclose any evidence content or processing details.

2.3.3. Challenges: To prevent collusion between the subjects of the report and responsible personnel in the relevant authorities and to prevent the subjects from identifying the user based on the timing of the evidence, this system cannot prevent frivolous reports, and it must be up to the relevant authorities to determine the effectiveness of the evidence. All anonymous reports face similar challenges, and

the inclusion of evidence can be determined by the relevant authorities based on their evidentiary requirements.

2.3.4. Features: This system may significantly increase the quantity of important evidence and the number of anonymous whistleblowers. It is less likely to be questioned by the regulated parties.

2.4. Passkey as a Public Service

2.4.1. Background: Many websites or platforms require user registration without involving sensitive personal information. The login process often relies on single-factor authentication or two-factor authentication (2FA) using "phone + password." Remembering numerous passwords is not secure, and "phone + password" 2FA can be susceptible to man-in-the-middle attacks. On the other hand, smart card certificates are inconvenient and are being downgraded in trust level (AAL2) by international standards organizations. While there are various services for single sign-on or password management, they require storing credentials in centralized online databases, which raises security concerns for some users. High-security level services typically come at a cost. Dedicated hardware devices for authentication, while secure, are often impractical. As for current passkey standards (such as FIDO2/W3C Webauthn Level 2), they do not effectively address cross-device logins (planned in W3C webauthn level 3 draft), and there is currently a lack of effective decentralized identity integration solutions in the industry.

2.4.2. Description: Service websites or platforms incorporate digital wallets into the login process and include it as one of the possible solutions for "forgot password" scenarios. The user login process with a digital wallet is briefly described as follows:

- The user receives a notification from the trusted service provider's official interface to download the digital wallet, or if the digital wallet is already downloaded, an authorization request is sent along with a near-field communication (NFC) request.
- The user consents to the request and applies to create a new key pair (public key - new device private key) using biometrics as part of the new device's private key. The service provider creates a new "card" to link the old and new devices. At this point, the user becomes the holder, and the service provider becomes the issuer.
- The user authorizes the service provider to connect the card using biometrics. The service provider becomes the verifier.
- The user consents to the NFC functionality. The mobile device becomes a new device, binding to the same key pair.

- After this, the user can log in using the mobile device without a password. The user can also configure automatic login to the service provider when the mobile device and computer are in close proximity, bypassing the username and password interface.

  The same process can be integrated into the "forgot password" handling. The service provider simply adds an "Login with Digital Wallet" option. When the user clicks on the corresponding link in their email, a new key pair is created, and the service provider requests the creation of a new "card" (VC/DID) for that account. The user is prompted to use the digital wallet for integration, eliminating the need for the user to input a new username and password on the original platform. Afterward, the user can log in to the website or platform using the digital wallet. The digital wallet can achieve cross-device synchronization through the current webauthn level 3 standard.

2.4.3. Challenges: This competes directly with single sign-on or password management services and requires precise identification of websites or platforms that are easily adaptable to this solution. Additionally, relevant standards are not yet mature.

2.4.4. Features: Digital wallets are more convenient than one-time passwords (OTP) and have a trust level (AAL) that is higher than most website or platform login requirements. As long as the convenience is higher than existing username and password methods, it can attract transitions and has high scalability.

Appendix 3: Inventory of Development Kit Requirements

Table 3: List of Development Kits and Usage Interfaces

<table>
<tr><th colspan="2"></th><th>Issuer</th><th>Verifier</th><th>Holder</th></tr>
<tr><td rowspan="2">Simple Service</td><td>Mobile-app</td><td colspan="2">Mild Business and Civic Services</td><td rowspan="2">User Interface</td></tr>
<tr><td>Web-app</td><td colspan="2">Government Counter Verification
(Un-digitized documents)
Financial and Business Services</td></tr>
<tr><td>Self-develop</td><td>SDK</td><td colspan="2">TW FidO Integration
(Digitized, no IC card)
Smart Card Integration
(Digitized, with IC card)</td><td>Third-Party Service Integration
(such as web3 wallets)
(such as EUDI wallet)</td></tr>
</table>

Appendix 4: Inventory of Decentralized Identity Principles and Requirements

This section is compiled from the Use Cases and Requirements for Decentralized Identifiers by the World Wide Web Consortium (W3C) [2] and compared with the design principles of the "Digital Wallet" white paper in our country. This document is in draft note status. First, the document lists 22 requirements as follows:

1. **Authentication/proof of control:** It is possible to prove that the entity claiming control over the identifier is indeed its controller
2. **Decentralized/self issued:** These identifiers are created and managed by the controller of the identifier, who may also be its subject. They are not assigned, given, sold, or rented to the individual using them. The party relying on the identifier for identification, authentication, and authorization, does not need to manage the creation, update, and recovery of these identifiers.
3. **Guaranteed unique identifier:** Identifiers are globally unique with no possibility of duplication, however unlikely that may be.
4. **No call home:** When using these identifiers, there is no need to contact the issuer of the identifier to verify it. Verification and authentication can occur without further communication with the issuer.
5. **Associated cryptographic material:** The identifier is tightly coupled with cryptographic material that can be used to prove control over that identifier.
6. **Streamlined key rotation:** When authentication materials need to be updated, these identifiers can update without direct intervention with requesting parties and with minimal individual interaction.
7. **Service endpoint discovery:** These identifiers allow requesting parties to look up available service endpoints for interacting with the subject of the identifier.
8. **Privacy preserving:** Use of the identifier does not, of itself, reveal any information about the subject
9. **Delegation of control:** The controller of the identifier is able to delegate that control to a third party.

[2] https://www.w3.org/TR/did-use-cases/#requirements

10. **Inter-jurisdictional:** Inter-jurisdictional identifiers do not depend on the legal jurisdiction in which they are issued. They are valid for uses anywhere without loss of fidelity or reliability. No jurisdiction is directly able to prevent their use.
11. **Can't be administratively denied:** These identifiers can't be denied or taken away by administrative function. This prevents shifting politics and bad actors from interfering.
12. **Minimized rents:** These identifiers don't incur ongoing expenses if unused nor on a per transaction basis. Fees based on updates—which incurs network and computational costs to verify—are considered "minimal".
13. **No vendor lock in:** These identifiers are not dependent on any given vendor. Vendor-specific identifiers restrict usage to that which is acceptable to the vendor and may allow vendors to extract disproportionate rents for usage.
14. **Preempt/limit trackable data trails:** As cookies and other session/state-tracking mechanisms were gradually turned into scaffolding for unwanted or collusive tracking in the evolution of the web stack, so too might any new data exchange or communication systems unwittingly facilitate unwanted tracking based on new data trails. Resistance to these kinds of surveillance exploits need to be designed into new systems.
15. **Cryptographic future proof:** These identifiers are capable of being updated as technology evolves. Current cryptography techniques are known to be susceptible to quantum computational attacks. Future-proofed identifiers provide a means to continue using the same identifier with updated, advanced authentication and authorization technologies.
16. **Survives issuing organization mortality:** These identifiers survive the demise of the organization that issued them. They usefulness of these identifiers survive organizations going out of business, being purchased (and potentially losing domain names or root credentials), and even the internal decay of an organization that no longer has the ability to verify the authenticity of records they once issued.
17. **Survives deployment end-of-life:** These identifiers are usable even after the systems deployed by requesting parties move past their useful lifetime. They are robust against technology fads and can seamlessly work with both legacy and next-generation systems.

18. **Survives relationship with service provider:** These identifiers are not dependent on the tenure of the relationship with a service provider. This contrasts with identifiers like service-centric emails, e.g. joe@example.com, which, when used as identifiers in other systems, can cause problems when individuals no longer use the service provider.
19. **Cryptographic authentication and communication:** These identifiers enable cryptographic techniques to authenticate individuals and to secure communications with the subject of the identifier, typically using public-private key pairs.
20. **Registry agnostic:** These identifiers are free to reside on any registry implementing a compatible interface. They are not beholden to any particular technology or vendor.
21. **Legally-enabled identity:** These identifiers can be used as a basis for credentials and transactions that can be recognized as legally valid under one or more jurisdictions.
22. **Human-centered interoperability:** Decentralized identifiers need to be easy to use by people with no technical expertise or specialist knowledge.

Table 4: Inventory of DID Principles and Requirements

	1 De facto Identity	2 Self-Sovereign Identity (SSI)	3 Composable & Programmable Social Relationship	4 Permissionless and Open Source	5 Compatible with Cross-Border & Future Digital Needs (e.g., web3)	6 Passwordless	7 Secure & Privacy Preserving	8 Functional Equivalence	9 Resilience & Social Recovery
1		◎				⊙	◎	⊙	⊙
2		◉	◉		⊙	⊙			⊙
3					⊙	⊙	⊙		
4	◎		◉						
5					⊙		⊙		
6	◉		◉						
7	◉		◉	⊙					
8	⊙	⊙	◎			⊙			
9	X	X	X	X	X	X	X	X	X
10			◎	◎	⊙			⊙	
11	◎	◎	◎	◎	⊙			⊙	◎
12	-	-	-	-	-	-	-	-	-
13	⊙			◎	⊙	◎			
14	⊙	⊙	⊙			⊙	⊙		
15	-	-	-	-	-	-	-	-	-
16	⊙		◎	⊙	⊙	◎			◎
17	⊙	⊙	◎		⊙				⊙
18		⊙	◎			◎			◎
19					◎	◎	◎		
20	◎		⊙	⊙					⊙

21	⊙							◎	◎
22		◎		⊙		⊙			
Legend explanation: ◉ Highly compatible; ◎ Moderately compatible; ⊙ Compatible; X Mutually exclusive; - Not included									

Appendix 5: Inventory of Digital Wallet Standards

1. European Union Digital Identity Wallet Architecture Reference Framework

This section is compiled from the European Union Agency for Cybersecurity (ENISA) publication "Digital Identity Standards" and the first version of the "Architecture and Reference Framework (ARF)" for the European Digital Identity Wallet (EUDIW). It serves as a standard reference and future comparison point for our country's "Digital Wallet" white paper, with the aim of ensuring compatibility with cross-border requirements and expanding various usage scenarios.

The European Union Digital Identity Wallet categorizes its standard requirements into two types. This section primarily focuses on the specifications related to Type 1: Type 1 focuses on personal identification data (PID) to meet the use case of ISO 29115 "Digital Identity Verification Level" LoA3 high trust level for cross-border identification.

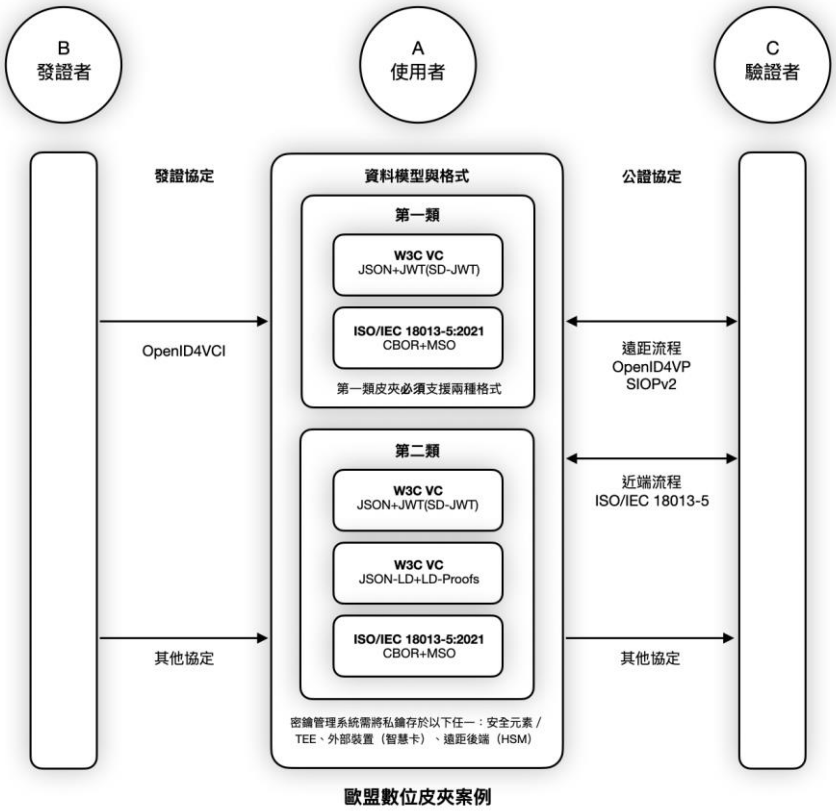


Figure Six: European Union Digital Wallet Standard Use Cases (Revised)

The specifications that **MUST** be met include, but are not limited to, the following:

1. **Cryptographic Keys Management System:**
   - EUDIW solutions must rely on one of the following components to store and manage cryptographic keys:
     - Embedded secure elements or trusted execution environments (TEEs, applicable to mobile devices).
     - External devices (security elements/IC cards).
     - Backend (remote hardware security modules).
   - The choice of hardware security and support depends on each EUDI Wallet solution.
   - EUDIW solutions must implement security measures to prevent cryptographic leakage risks.

2. **Attestation Exchange:**
   - EUDIW solutions must support OpenID4VP as the attestation exchange protocol for remote operation flows.
   - When anonymous identity verification is required, request parameters should be specified according to the OpenID SIOPv2 protocol.
   - EUDIW solutions must support the protocols detailed in ISO/IEC 18013-5:2021 for proximity operation flows.
   - EUDIW solutions must be capable of performing proof of possession.
   - EUDIW solutions must support selective disclosure of attributes as specified in ISO/IEC 18013-5:2021.
   - EUDIW solutions must support attribute-selective disclosure as specified in the SD-JWT standard.

3. **Issuance Protocol:**
   - EUDIW solutions must support OpenID4VCI as the issuance protocol. Member states are free to include additional issuance protocol options in their national solutions.

4. **Data Model:**
   - EUDIW solutions must support proofs issued according to the data model specified in ISO/IEC 18013-5:2021.
   - EUDIW solutions must support proofs issued according to the data model specified in the W3C Verifiable Credentials Data Model 1.1.

5. **PID and (Q)EAA Formats:**
   - EUDIW solutions must support proofs in JWT and SD-JWT formats.
   - EUDIW solutions must support proofs in CBOR format.

6. **Signature Formats:**
   - EUDIW solutions must support signature and encryption formats that comply with the JOSE (JWT) specification.

- EUDIW solutions must support signature and encryption formats that comply with the COSE specification.

7. **Cryptographic Suites and Mechanisms:**
   - EUDIW solutions must support cryptographic suites and mechanisms with detailed attributes specified in SOG-IS Consent Version 1.2.

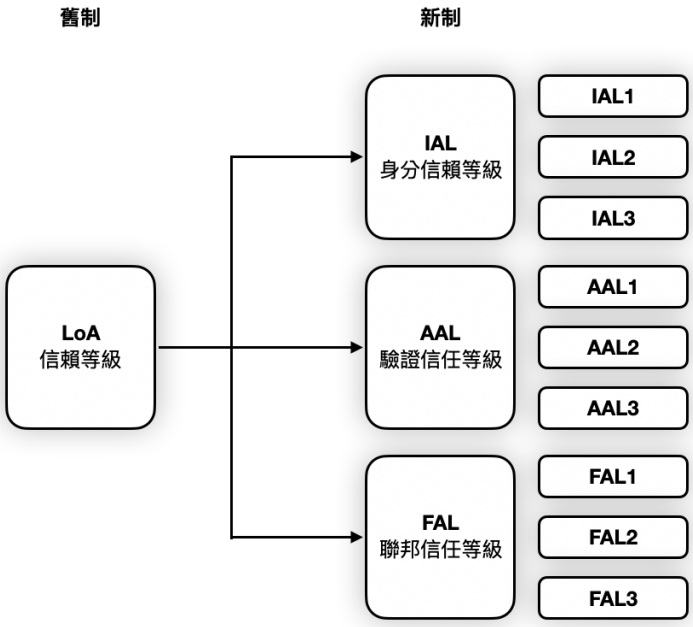
These specifications and requirements ensure the robustness and security of EUDIW solutions.

2. Level of Assurance (LOA) and XAL[3]

The National Institute of Standards and Technology (NIST) in the United States has established technical requirements for digital identity services provided to federal agencies. NIST 800-63-3, "Digital Identity Guidelines," expands on the concept of Levels of Assurance (LOA) for digital identity electronic authentication, initially specified in the Office of Management and Budget (OMB) Memorandum M-04-04 and ISO/IEC 29115. It addresses how to assess the credibility of identity verification and electronic authentication and assigns relevant levels. Each level is defined with corresponding assessment criteria and potential impacts.

1. LOA1: Low Assurance Level - Little or no confidence in the claimed or asserted individual.
2. LOA2: Medium Assurance Level - Some degree of confidence in the claimed or asserted individual.
3. LOA3: High Assurance Level - High confidence in the claimed or asserted individual.
4. LOA4: Highest Assurance Level - Very high confidence in the claimed or asserted individual.

NIST 800-63-3 further divides LOA into three processes: Identity Proofing, Authentication, and Federation Identity Management. It optimizes and refines the concerns originally left undefined in LOA 2-3 and integrates them into a set of XAL standards.



[3] Paul A. Grassi, Michael E. Garcia, James L. Fenton (2017/06), Digital Identity Guidelines，來源：https://doi.org/10.6028/NIST.SP.800-63-3

Figure 7: Correspondence between LOA and XAL (NIST 800-63-3) Specifications (Revised)

IAL (Identity Assurance Level): Specifies the rigor of the identity proofing process for establishing an individual's identity. The choice of IAL aims to mitigate potential identity proofing errors.

- IAL1: At this level, attributes are self-asserted (if provided) or should be treated as self-asserted; no verification process is required.
- IAL2: In addition to meeting IAL1 requirements, it introduces remote or in-person identity proofing requirements. At least one of the procedures provided in SP 800-63A for remote or in-person identity verification must be used.
- IAL3: In addition to meeting IAL2 requirements, in-person identity proofing is required, such as face-to-face or supervised remote identity verification. Verification of identity attributes must involve the examination of physical documents, as described in SP 800-63A.

AAL (Authentication Assurance Level): Ensures the rigor of the authentication process and the binding of the authenticator to a specific personal identifier. Choosing AAL aims to mitigate potential authentication errors (e.g., unauthorized applicants using credentials not belonging to them).

- AAL1: Provides some assurance that the applicant controls the authenticator registered to the user. AAL1 requires single-factor authentication using various available authentication technologies. Successful authentication requires the applicant to prove ownership and control of the authenticator through a secure authentication protocol.
- AAL2: Provides high confidence that the applicant controls the authenticator registered to the user. For authentication at AAL2, the applicant must prove possession and control of two distinct authentication factors through approved encryption techniques.
- AAL3: Provides very high confidence that the applicant controls the authenticator registered to the user. AAL3 certification is based on proving ownership of keys through an approved encryption protocol. AAL3 is similar to AAL2 but requires resistance to impersonation for the authenticator.

FAL (Federation Assurance Level): Specifies the rigor of using federation assertion protocols. FAL is not mandatory, as not all digital identity systems utilize federated identity architectures. Choosing FAL aims to mitigate potential federation-related identity errors.

- FAL1: Allows the relying party to receive a holder assertion from the identity provider. The identity provider must sign the assertion using approved encryption methods.

- FAL2: Adds a requirement that assertions must be encrypted using approved encryption techniques so that the relying party is the only party able to decrypt them.
- FAL3: Requires the user to provide proof of possession of the encryption key reference and the assertion itself. The assertion must be signed using approved encryption methods and encrypted for the relying party using approved encryption methods.

3. Digital Identity Verification Standards Relevant to eIDAS 2.0 Specifications[4]

Table 5: References to Digital Identity Verification Standards (Revised)

	eMRTD (ISO 7501 – ICAO 9303)	eIDAS Token (TR-03110-2)	mDL (ISO/IEC 18013-5)	mID (ISO/IEC 23220)	X509 PKI certificates (ISO/IEC 9594-8)	SAML eIDAS (ITU-T	**OpenID Connect**	**OpenID Connect with SIOP**	**FIDO2** (ITU-T X.1277 & X.1278)	**SSI**
正式標準	O 國際	O 歐盟	O 國際	規劃中	O	O	X	X	O	X
個人身分識別資料 (PID) 格式	LDS1 eMTRD	LDS2 eMRTD/ Specific ASN.1 definition	mdoc mDL CBOR/ mdoc mDL signed JWT	mdoc CBOR, mdoc signed JWT (planned support for VC)	X.509 ASN.1 definitions	SAML assertion in XML format, according to an XSD definition	ID Token signed JWT	ID Token signed JWT (planned support for VC)	N/A	VC according to JWT, JSON-LDAnoncreds …
（合格）電子屬性證明格式	N/A	LDS2 eMRTD/ Specific ASN.1 definition	N/A	mdoc CBOR, mdoc signed JWT (planned support for VC)	X.509 and X520 ASN.1 definitions	SAML assertion in XML format, according to an XSD definition	ID Token signed JWT	ID Token signed JWT (planned support for VC)	N/A	VC according to JWT, JSON-LD, Anoncreds …
主體的離線認證	O	O	O	O	X	X	X	X	O	X
主體的線上認證 (LoA)	X	O	O	O	O	O	O	O	O	O
依賴方的離線認證	O	O	O	O	X	X	X	X	X	X
依賴方的線上認證	X	O	O	O	O	O	O	O	O	O
裝置綁定（例如智慧型手機）	X	選擇性	X	選擇性	選擇性	N/A	N/A	N/A	O	選擇性
使用安全元件（信賴程度）	X	O	X	X	選擇性	N/A	N/A	N/A	選擇性	選擇性
使用者單獨控制	X	O	X	O	選擇性	X	X	X	O	O
最初為執法機關設計	O	X	O	X	X	X	X	X	X	X
需要集中式身份提供者	X	O 需額外	O 只有伺服器相容	O 只有伺服器相容	X	O	O	O	N/A	X

[4] ENISA (2023/07), DIGITAL IDENTITY STANDARDS，來源：https://www.enisa.europa.eu/publications/digital-identity-standards

選擇性披露	X	O	O	O	X	O	O	O	O	O
不可追蹤性/不可連結性	X	O	X	X	X	X	X	X	O	O
支援身份管理生命週期	發行/驗證/撤銷	發行/驗證/屬性共享/撤銷	發行/驗證/屬性共享/撤銷	發行/驗證/屬性共享/撤銷	發行/吊銷/撤銷/更新	驗證/屬性共享	驗證/屬性共享	驗證/屬性共享	驗證	發行/驗證/吊銷/撤回/更新
信任模型	聯邦式	聯邦式	聯邦式	聯邦式	企業/聯邦	企業/聯邦	企業/聯邦	聯邦式/去中心	中心化，可去中心但視驗證器決定	去中心化
標準的成熟度	高	高	中	低	高	高	高	中/低	高	中/低