Bridging eIDAS 2.0 Legal Requirements and Technical Solutions

Giuseppe De Marco[1], Francesco Antonio Marino[2] and Andrea De Maria[2]

[1]*Department for Digital Transformation of the Presidency of the Council of Ministers, Rome, Italy*
[2]*Italian Government Printing Office and Mint, Rome, Italy*

Abstract

In the evolving landscape of digital identity, the Italian Digital Wallet (IT-Wallet) stands out as a pioneering initiative that exemplifies a holistic approach to integrating legal requirements with innovative technical solutions. This paper aims to explore the comprehensive strategy behind the IT-Wallet, focusing on how it meets the legal frameworks provided by the new eIDAS regulation. The eIDAS regulation has been instrumental in establishing trust and security for electronic transactions across the European Union. The IT-Wallet project goes a step further by analyzing these legal requirements and translating them into technical solutions that enhance security and privacy. We will delve into a specific example such as Person Identification Data (PID) Issuance, showcasing the technical implementations that address these legal mandates.

Keywords

eIDAS 2.0, Regulation, IT-Wallet, Digital Identity

1. Introduction

The European Union's revised eIDAS regulation [1], known as eIDAS 2.0, represents a significant advancement in the context of digital identity. This updated framework aims to enhance the security, interoperability, and user-friendliness of electronic identification and trust services across member states. Central to this regulation is the European Digital Identity (EUDI) Wallet, designed to enable EU citizens to securely store and manage their personal identification data. The journey towards eIDAS 2.0 began with the European Commission's announcement in June 2021, followed by a public hearing in February 2022. On November 8, 2023, the Commission, the EU Parliament, and the Council of the European Union reached an agreement on the revised regulation. The formal adoption by the European Parliament took place in February 2024. A noteworthy milestone is set for November 21, 2024, when the European Commission will establish reference criteria and verification procedures for the digital ID wallet. The full rollout of eIDAS 2.0 is expected by 2026.

Compared to eIDAS 1.0, one of the most important innovations introduced by the new regulation is the EUDI Wallet, which allows users to securely store, manage, and present their credentials in both online and offline cross-border use cases, extending identity verification to physical services.

TDI 2024: 2nd International Workshop on Trends in Digital Identity, April 9, 2024, Rome, Italy

gi.demarco@innovazione.gov.it (G. De Marco); fa.marino@ipzs.it (F. A. Marino); a.demaria@ipzs.it (A. De Maria)
0000-0002-0308-0080 (F. A. Marino)

In this paper, we have analyzed the delta of changes that the Parliament legislative resolution made on the eIDAS Regulation, also approved by the European Council considering:

- The European Parliament legislative resolution of 29 February 2024 [2].
- The Regulation of the European Parliament and of the Council amending Regulation (EU) No 910/2014 as regards establishing the European Digital Identity Framework of 13 March 2024 [1].

In Section 2 we provide an analysis of the Legislative text and a methodology to classify the Legal text into requirements. Therefore, in Section 3 we focus on the PID Issuance phase extracting a subset of items that are relevant to PID Issuance. Then, we provide an overview of the Italian PID Issuance Flow in Section 4 highlighting how the Italian implementation profile aligns with the relevant regulatory framework. Finally, in Section 5, we summarize the main results.

2. Analysis and Classification of Legislative text

The new eIDAS 2.0 regulation is composed of three main parts, these are:

Recitals. They provide the background, rationale, and objectives behind the eIDAS Regulation [1]. They explain the context and reasons for the provisions that follow. Recitals are used to interpret and understand the intentions of the legislature and the scope of the normative provisions within the legal act[1]. In particular, we found **one new Recital** at position 67, and **70 updated Recitals** upon 78.

Articles. They outline the obligations, rights, and procedures for Member States, entities, and individuals. We found very important changes (**3 Deleted**, **10 Replaced**, **24 Amended**, and **33 Inserted**) as summarized in Table 1.

Annexes. They include practical details necessary for compliance with the regulation. Delving into the Annexes we found a few changes in the first four annexes and, in addition to these, four new Annexes (see Table 2). In particular:

- "*Annex V*", provides requirements for Qualified Electronic Attestation of Attributes (EAAs).
- "*Annex VI*", contains the list of the required user attributes to be implemented.
- "*Annex VII*", contains requirements for EAAs issued by or on behalf of a Public Body responsible for an Authentic Source.
- "*Annex To The Legislative Resolution*" contains two statements, one containing considerations for web browser vendors and another one about the untraceability of wallet users, that aims to prevent data collection by wallet providers.

[1] The distinction between normative and informative elements in EU legislation, including the role of recitals, is a well-established aspect of EU legal doctrine. This understanding is derived from the jurisprudence of the Court of Justice of the European Union (CJEU) and the practices of legal interpretation within the EU. The CJEU often refers to recitals when interpreting the provisions of EU legislation to understand the intentions of the legislature and the context of the laws.

Table 1
List of Articles status

Status	Articles
Amended	2, 3, 7, 8, 12, 20, 21, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 42, 44, 47.
Replaced	5, 9, 10 (only title), 13, 14, 15, 16, 45, 49, 51.
Inserted	5 from (a) to (f), 11(a), 12(a), 12(b), 19(a), 24(a), 29(a), 32(a), 39(a), 40(a), 45 from (a) to (l), 46 from (a) to (e), 48(a).
Deleted	17, 18, 41.

Table 2
List of Annexes status

Status	Annexes
Replaced	ANNEX I point (i), ANNEX III point (i), ANNEX IV point (c)(ca)(j).
Inserted	ANNEX V, ANNEX VI, ANNEX VII, ANNEX TO THE LEGISLATIVE RESOLUTION.
Deleted	ANNEX II point 3 and 4.

2.1. Classification

After reviewing all the articles and annexes, we categorized them by items and classified each item according to its related subject and scope. Subjects we identified are: *European Commission*, *EUDI Wallets*, *Member States*, and *Relying Parties*. The scopes we defined are: *Governance*, *Issuance*, *Presentation*, and *Wallet Solution*.

In our matrix, we also included additional elements (e.g. requirements currently fulfilled, planned in the roadmap, project constraints, and additional notes) to better manage our national wallet implementation and our national milestones. This work resulted in the analysis of the delta of changes in the eIDAS regulation from an implementation perspective and also a self-assessment matrix that aims to guide us in our developments about the national wallet solution. An extract of this classification matrix is given in Table 3 where for the sake of simplicity we omitted elements related to our national wallet implementation.

2.2. Results

The classification of the items has clarified the distribution of normative elements across the distinct domains of the wallet ecosystem. As depicted in the pie chart in Figure 1, a significant proportion is attributed to the governance of the ecosystem. Within the scope of Governance, we have further delineated sub-categories encompassing general aspects related to certification and accreditation procedures and roles, wallet provisioning, and the security framework, among others. Additionally, we have identified items related to the characteristics of the wallet solution, the issuance of digital credentials, and the presentation of digital credentials.

In Appendix A, Tables 6, 7 and 8, we summarize the relevant requirements extracted by the regulation and related to Issuance, Presentation and Wallet Solution, respectively.

Table 3
Extracted of the classification matrix

Article Name	Article Text	Subject	Scope
Art. 5a(2)	European Digital Identity Wallets shall be provided in one or more of the following ways: (a) directly by a Member State; (b) under a mandate from a Member State; (c) independently of a Member State but recognised by that Member State.	European Digital Identity Wallets	Governance
Art. 5a(6)	Member State shall inform users, without delay, of any security breach that could have entirely or partially compromised their European Digital Identity Wallet or its contents, in particular, if their European Digital Identity Wallet has been suspended or revoked pursuant to Article 5e.	Member State	Wallet Solution
Art. 5a(5)(a)(i)	European Digital Identity Wallets shall, in particular: (a) support common protocols and interfaces: [...] (i) for issuance of person identification data, qualified and non qualified electronic attestations of attributes or qualified and non-qualified certificates to the European Digital Identity Wallet;	European Digital Identity Wallets	Issuance
Art. 5a(5)(a)(ii)	European Digital Identity Wallets shall, in particular: (a) support common protocols and interfaces: [...] (ii) for relying parties to request and validate person identification data and electronic attestations of attributes;	European Digital Identity Wallets	Presentation

3. Understanding the Regulatory Framework for PID Issuance

This section delves into the process of identifying and translating legal requirements into technical specifications for the PID issuance phase. The starting point was a comprehensive analysis of the European Digital Identity Wallet regulation, specifically Article 5(a). From this extensive set of provisions, a subset of items directly relevant to PID issuance was carefully extracted.

The identified legal requirements, outlined in Table 4, form the foundation for the technical development of the Italian PID issuance process. These requirements encompass essential aspects such as:

- Security and Selective Disclosure: Ensuring user control over personal identification data and enabling selective disclosure.
- Protocols and Interfaces: Supporting standardized protocols and interfaces for PID issuance.
- User Onboarding: Facilitating secure user onboarding using electronic identification means.
- User Identification and Association: Guaranteeing the unique representation of the user and linking their identity to the European Digital Identity Wallet.

By focusing on these core elements, the subsequent Sections aimed to develop technical solutions that effectively address the legal mandates while implementing the PID issuance process for Italian citizens.

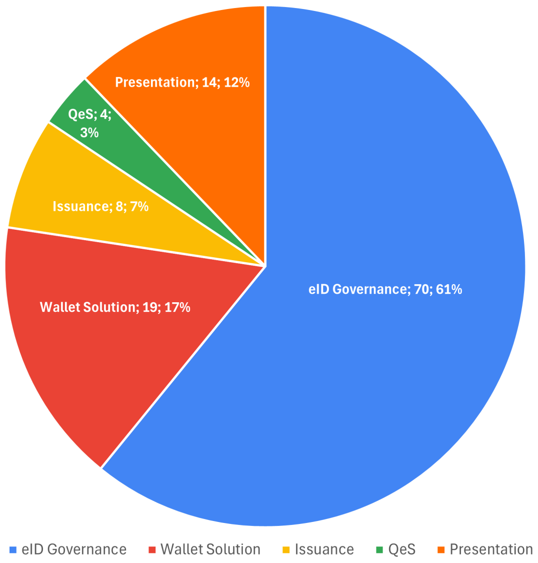

Figure 1: Classification of Legislative Text

4. Overview of the Italian PID Issuance Process

This Section examines how the Italian implementation profile of the Wallet [3] aligns with the relevant regulatory framework, with a particular focus on the issuance phase. By dissecting the process into its constituent sub-phases, this Section aims to provide a comprehensive understanding of the mechanisms employed to ensure user identification, data protection, and security.

4.1. Data Format

Selective Disclosure JWT (SD-JWT) [4] is a specification that introduces conventions to support selective disclosure for JWTs: for an SD-JWT document, a Holder can decide which claims to release (within bounds defined by the Issuer). SD-JWT-based Verifiable Credentials specification (SD-JWT-VC) [5] uses SD-JWT and the well-established JWT content rules and extensibility model as basis for representing Verifiable Credentials with JSON payloads, and it is one of the data format of the Italian Personal Identification (PID) system, designed to meet specific regulatory requirements while ensuring data privacy and security. This section delves into how this format addresses requirements **R1** and **R4**.

Requirement **R1** mandates that European Digital Identity Wallets enable users to securely request, obtain, and control their personal identification data, allowing for selective disclosure. The SD-JWT-VC format directly supports this by:

- **Selective Disclosure**: The data model allows for granular control over which attributes within the PID are revealed in a given presentation. This ensures that only necessary information is released, protecting sensitive data from unnecessary exposure.

Table 4
Extracted Legal Requirements for PID Issuance

ID	Context	Text	Reference
R1	Security and Selective Disclosure	European Digital Identity Wallets shall enable the user, [. . .], to securely request, obtain, [. . .], under the sole control of the user, person identification data [. . .], while ensuring that selective disclosure of data is possible	Art. 5a(4)(a)
R2	Protocols and Interfaces	European Digital Identity Wallets shall support common protocols and interfaces for issuance of person identification data, qualified and non-qualified electronic attestations of attributes or qualified and non-qualified certificates to the European Digital Identity Wallet;	Art. 5a(5)(a)(i)
R3	User Onboarding	European Digital Identity Wallets shall support common protocols and interfaces to securely onboard the user by using an electronic identification means in accordance with Article 5a(24)	Art. 5a(5)(a)(v)
R4	User Identification and Association with EUDIW	European Digital Identity Wallets shall ensure that the person identification data, which is available from the electronic identification scheme under which the European Digital Identity Wallet is provided, uniquely represents the natural person, legal person or the natural person representing the natural or legal person, and is associated with that European Digital Identity Wallet	Art. 5a(5)(c) (f)

- **Cryptographic Key Binding**: Each PID is bound to a specific Wallet Instance through a cryptographic key. This binding mechanism provides a strong guarantee of possession, as it ensures that only the rightful holder of the corresponding private key can present the PID.
- **Data Minimization**: The requirement for a minimum dataset reduces the amount of personal data collected and stored, aligning with data protection principles.

Requirement **R4** stipulates that the PID data uniquely represents the user and is associated with the European Digital Identity Wallet (EUDIW). The SD-JWT-VC format fulfills this requirement through:

- Unique Identification: The data model includes attributes that collectively and uniquely identify the user, ensuring that each individual has a distinct digital identity within the system.
- Association with EUDIW: The cryptographic key binding ties the PID to a specific Wallet Instance, effectively linking the user's identity to their EUDIW. This association is crucial for maintaining data integrity and preventing identity fraud.

In conclusion, the SD-JWT-VC data format for the Italian PID effectively addresses the core aspects of requirements **R1** and **R4**. By providing mechanisms for selective disclosure, cryptographic key binding, and unique user identification, this format contributes to a secure, privacy-preserving, and reliable PID issuance.

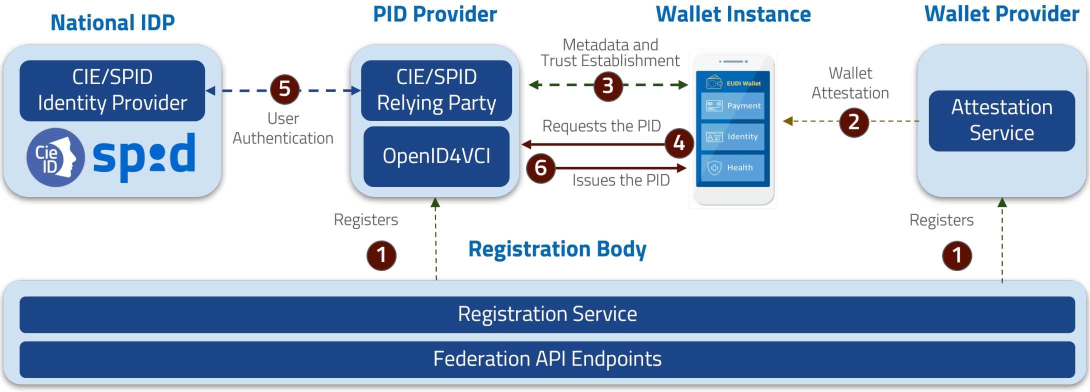

Figure 2: PID Issuance – High Level Flow

4.2. Issuance Flow

Figure 2 illustrates a comprehensive flowchart detailing the process of PID Issuance within the Italian digital identity ecosystem. This process involves multiple entities, including the National Identity Provider (IDP), CIE/SPID, Registration Body, and Wallet Provider. The flow is sequentially numbered from 1 to 6, indicating the steps involved.

1. Registration with Federation API Endpoints [6]: The process begins with the PID Provider, Wallet Provider, and Registration Service registering with the Federation API Endpoints. This step ensures that these entities are evaluable as trustworthy according to the trust framework in use.
2. Attestation Service Registration: Following the initial registration, the Attestation Service provides the Wallet Attestation to the Wallet Instance. This step is crucial for establishing the authenticity and genuineness of the Wallet Instance and the compliance with the security requirements related to both the Hardware and the Software.
3. Metadata Exchange and Trust establishment: This step involves the exchange of metadata to facilitate trust and interoperability between these entities. The PID Provider checks that the Wallet Instance is authentic and valid, and the Wallet Provider is a trusted entity. The Wallet Instance checks that the PID Provider is a trusted entity.
4. User Requests PID: The user initiates the process by requesting a PID.
5. User Authentication: This step ensures that the user's identity is verified through the national digital identity system.
6. PID Issuance: Finally, this step completes the process by providing the Wallet Instance with a valid user's PID.

This flowchart highlights the intricate interactions between various systems to provide a streamlined and secure identity verification process. It underscores the importance of user privacy and data integrity at each stage of authentication and registration.

Focusing on steps 4, 5 and 6, we go into more technical details regarding the protocol used for the issuance of PIDs (see Figure 3). It follows the *OpenID for Verifiable Credential Issuance* specification (OID4VCI) [7], with the following main reference standards/specifications on top:

- *The OAuth 2.0 Authorization Framework* – RFC 6749 [8], recommended in [7, Section 3].
- *Pushed Authorization Requests* (PAR) – RFC 9126 [9], recommended in [7, Section 5].
- *Proof Key for Code Exchange* (PKCE) – RFC 7636 [10], recommended in [7, Section 5].
- *JWT Authorization Requests* (JAR) – RFC 9101 [11].
- *JWT Authorization Response Modes* (JARM) [12].
- *Rich Authorization Requests* (RAR) – RFC 9396 [13].
- *OAuth 2.0 Attestation-Based Client Authentication* [14].
- *OpenID Federation 1.0* [6].

The process is designed to be secure and efficient, ensuring that users can obtain their digital identities with minimal friction. Key steps in the PID issuance process can be summarized as:

- **Authorization Phase**, in which the Wallet sends a Push Authorization Request (PAR) to the PID Provider. It authenticates the client through the Wallet Attestation and establishes trust by building the Federation Trust Chain related to the Wallet Provider. These checks are crucial in preventing fraudulent activities and ensuring the integrity of the digital identity ecosystem. PKCE [10] is also used as a security best current practice in the Authorization Code Flow. The adoption of common and secure protocols and interfaces covers the items we identified with **R1** (the security part of the requirement) and **R2**.
- **User Identification Phase**, where the user is identified by the PID Provider, which now acts as a Relying Party and authenticates the user with the national IdP using one of the available national schemes notified under eIDAS. This covers the item we identified with **R3** about user onboarding and part of **R4** regarding user identification.
- **Credential Request/Issuance Phase**, where the Wallet Instance requests the credential. To do this, it first obtains a DPoP sender-constrained Access Token [15] and uses it on the protected resource (the credential endpoint) by sending a proof JWT containing a public key to which the PID must be bound (Holder Key Binding). This proves that the corresponding private key is under the User's control, ensuring that only the legitimate owner can use the PID during the presentation. This binding is achieved through the use of cryptographic techniques within the JWT. It is worth noting that the Wallet can generate a new fresh key pair with each PID request, improving user privacy (user unlinkability). This again covers the security part of the item **R1** and part of **R4** related to the association with the Wallet.

4.3. Mapping Requirements

The comprehensive mapping of technical solutions to legal requirements, as presented in Table 5, underscores the critical alignment between technological advancements and regulatory frameworks. This alignment is essential for ensuring the security, privacy, and trustworthiness of digital identity systems.

The table highlights several key contexts, such as security and data protection, transparency support, and user onboarding, each associated with specific legal references like the eIDAS Regulation and GDPR. The technical mechanisms demonstrate compliance with these legal requirements, ensuring robust and secure digital identity verification processes.

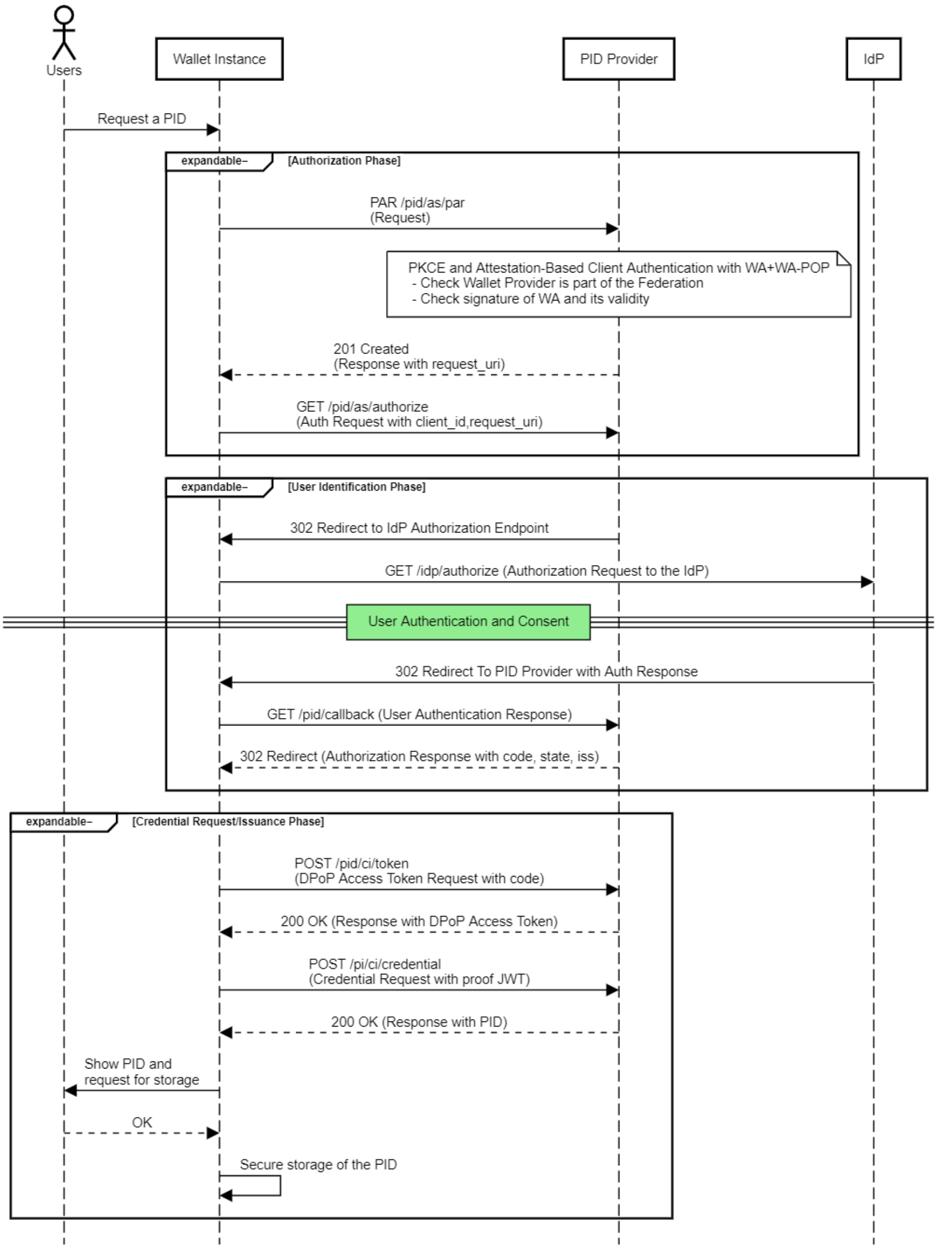
Users
Wallet Instance
PID Provider
IdP
Request a PID
expandable–
[Authorization Phase]
PAR /pid/as/par
(Request)
PKCE and Attestation-Based Client Authentication with WA+WA-POP
- Check Wallet Provider is part of the Federation
- Check signature of WA and its validity
201 Created
(Response with request_uri)
GET /pid/as/authorize
(Auth Request with client_id,request_uri)
expandable–
[User Identification Phase]
302 Redirect to IdP Authorization Endpoint
GET /idp/authorize (Authorization Request to the IdP)
User Authentication and Consent
302 Redirect To PID Provider with Auth Response
GET /pid/callback (User Authentication Response)
302 Redirect (Authorization Response with code, state, iss)
expandable–
[Credential Request/Issuance Phase]
POST /pid/ci/token
(DPoP Access Token Request with code)
200 OK (Response with DPoP Access Token)
POST /pi/ci/credential
(Credential Request with proof JWT)
200 OK (Response with PID)
Show PID and
request for storage
OK
Secure storage of the PID

Figure 3: PID Issuance – Detailed Flow

5. Conclusion

This paper has presented a detailed examination of the Italian Digital Wallet (IT-Wallet) initiative, showcasing how it successfully bridges the gap between the legal requirements set forth by the eIDAS 2.0 regulation and innovative technical solutions. Through a meticulous analysis of the regulatory framework and its implementation, several key findings emerge:

Table 5
Mapping requirements: Technical solutions meet Legal Requirements

ID	References	Context	Technical Mechanism
R1	Art. 5a(4)(a)	Security and Selective Disclosure support	Security, Trust and Privacy • PKCE • Client auth based on Attestation-Based Client Authentication • DPoP Access Token • Proof JWT • Trust Framework based on OpenID Federation 1.0 • SD-JWT / SD-JWT-VC
R2	Art. 5a(5)(a)(i)	Compliance with standards	• OpenID4VCI • OpenID Federation 1.0 • SD-JWT / SD-JWT-VC • Attestation-Based Client Authentication • OAuth2 DPoP
R3	Art. 5a(5)(a)(v)	User Onboarding	• National eID schemes notified eIDAS • Trust Framework based on OpenID Federation 1.0
R4	Art. 5a(5)(c)(f)	User identification and association with EUDIW	• National eID schemes notified eIDAS • Wallet Attestation • Client Auth based on WA-PoP • Cryptographic Holder Binding (HB)

1. **Comprehensive Regulatory Analysis**: The study's classification of legislative text provides valuable insights into the distribution of normative elements across the wallet ecosystem, with a significant proportion attributed to governance. This classification serves as a crucial tool for policymakers and implementers to ensure comprehensive compliance.
2. **Effective Technical Implementation**: The IT-Wallet's approach to Personal Identification Data (PID) issuance demonstrates a robust alignment with key regulatory requirements. The adoption of the SD-JWT-VC data format and the implementation of a secure issuance flow, leveraging protocols such as OpenID for Verifiable Credential Issuance (OID4VCI), showcase how technical solutions can effectively address legal mandates.
3. **Privacy and Security Focus**: The implementation details reveal a strong emphasis on user privacy and data security. Features such as selective disclosure, cryptographic key binding, and user-controlled data management align closely with the eIDAS 2.0 principles of data minimization and user empowerment.
4. **Interoperability and Standardization**: The IT-Wallet's adherence to common protocols and interfaces, as mandated by eIDAS 2.0, contributes to the broader goal of creating an interoperable digital identity ecosystem across the European Union.

The IT-Wallet initiative serves as a prime example of how regulatory compliance can drive innovation in digital identity solutions. By carefully mapping technical mechanisms to legal requirements, the project demonstrates the feasibility of creating a secure, privacy-preserving, and user-friendly digital identity wallet that meets the stringent standards set by eIDAS 2.0.

Future research could explore the practical implications of widespread adoption of such wallets, including user acceptance, cross-border interoperability challenges, and the evolving landscape of digital identity threats. Additionally, comparative studies with other national implementations could provide valuable insights into best practices and areas for further harmonization across the EU.

In conclusion, the Italian Digital Wallet project offers valuable lessons for policymakers, technologists, and identity providers across the EU. It exemplifies how a thoughtful approach to regulatory compliance can result in technical solutions that not only meet legal requirements but also advance the state of the art in digital identity management.

Acknowledgments

This work was conducted within the framework of the IT-Wallet Government Initiative, a project of national significance aimed at advancing digital identity solutions in Italy. The authors would like to express their sincere gratitude to all the stakeholders involved in this ambitious endeavor. Special acknowledgment goes to our collaborators at Fondazione Bruno Kessler (FBK) for their invaluable technical expertise and research contributions. Their insights have significantly enhanced the robustness and efficacy of the IT-Wallet solution. We also wish to thank PagoPA S.p.A. for their crucial role in this project. The synergy between governmental bodies, research institutions, and public-service companies exemplified in this project demonstrates the power of collaborative efforts in addressing complex challenges in digital identity management. This cooperation has been essential in bridging theoretical concepts with practical implementations, ultimately contributing to the advancement of digital services for Italian citizens.

References

[1] European Parliament and Council of the European Union, Regulation (EU) 2024/1183, in: Official Journal of the European Union, 2024. URL: http://data.europa.eu/eli/reg/2024/1183/.

[2] European Parliament and Council of the European Union, European Parliament legislative resolution of 29 February 2024, 2024.

[3] G. De Marco, F. Marino, F. Grauso, et al., The Italian EUDI Wallet Implementation Profile, 2024. URL: https://italia.github.io/eudi-wallet-it-docs/v0.8.0/en/, draft 0.8.

[4] D. Fett, K. Yasuda, B. Campbell, Selective Disclosure for JWTs (SD-JWT), Internet-Draft draft-ietf-oauth-selective-disclosure-jwt-12, IETF, 2024. URL: https://datatracker.ietf.org/doc/draft-ietf-oauth-selective-disclosure-jwt/12/, Work in Progress.

[5] O. Terbu, D. Fett, B. Campbell, SD-JWT-based Verifiable Credentials (SD-JWT VC), Internet-Draft draft-ietf-oauth-sd-jwt-vc-05, IETF, 2024. URL: https://datatracker.ietf.org/doc/draft-ietf-oauth-sd-jwt-vc/05/, Work in Progress.

[6] R. Hedberg, M. Jones, A. Solberg, J. Bradley, G. De Marco, V. Dzhuvinov, OpenID Federation 1.0, 2024. Draft 36.

[7] T. Lodderstedt, K. Yasuda, T. Looker, OpenID for Verifiable Credential Issuance, 2024. Draft 13.

[8] D. Hardt, The OAuth 2.0 Authorization Framework, RFC 6749, 2012. doi:10.17487/RFC6749.

[9] T. Lodderstedt, B. Campbell, N. Sakimura, D. Tonge, F. Skokan, OAuth 2.0 Pushed Authorization Requests, RFC 9126, 2021. doi:10.17487/rfc9126.

[10] N. Sakimura, J. Bradley, N. Agarwal, Proof Key for Code Exchange by OAuth Public Clients, RFC 7636, 2015. doi:10.17487/rfc7636.

[11] N. Sakimura, J. Bradley, M. B. Jones, The OAuth 2.0 Authorization Framework: JWT-Secured Authorization Request (JAR), RFC 9101, 2021. doi:10.17487/rfc9101.

[12] T. Lodderstedt, B. Campbell, JWT Secured Authorization Response Mode for OAuth 2.0 (JARM), 2022. URL: https://openid.net/specs/oauth-v2-jarm.html.

[13] T. Lodderstedt, J. Richer, B. Campbell, OAuth 2.0 Rich Authorization Requests, RFC 9396, 2023. doi:10.17487/RFC9396.

[14] T. Looker, P. Bastian, OAuth 2.0 Attestation-Based Client Authentication, Internet-Draft draft-ietf-oauth-attestation-based-client-auth-03, IETF, 2024. URL: https://datatracker.ietf.org/doc/draft-ietf-oauth-attestation-based-client-auth/03/, Work in Progress.

[15] D. Fett, B. Campbell, J. Bradley, T. Lodderstedt, M. B. Jones, D. Waite, OAuth 2.0 Demonstrating Proof of Possession (DPoP), RFC 9449, 2023. doi:10.17487/RFC9449.

A. Highlighted Articles

Table 6
Highlighted Articles - Credential Issuance

Article Item	Context
Art. 5a(4)(b)	Wallet shall enable the user to generate pseudonyms and store them encrypted and locally within the Wallet
Art. 5a(5)(a)(i)	Issuance of person identification data, qualified and non qualified electronic attestations of attributes or qualified and non-qualified certificates to the European Digital Identity Wallet
Art. 5a(5)(e)	Possibility of implementing electronic attestation of attributes with embedded disclosure policies to be applied when interacting with RPs (the Wallet must support)
Art. 5a(5)(f)	Person Identification Data (PID) uniquely represents the natural person, legal person or the natural person representing the natural or legal person, and is associated with that European Digital Identity Wallet
Art. 5a(16)(a)	PID/EAA Providers are not allowed in tracking user behaviour or knowledge of transactions of the user
Art. 5a(16)(b)	privacy preserving techniques which ensure unlinkability, where the attestation of attributes does not require the identification of the user

Table 7
Highlighted Articles - Credential Presentation

Article Item	Context
Art. 5a(5)(a)(ii)	Support common protocols for Relying Parties to request and validate PID and electronic attestations of attributes
Art. 5a(5)(a)(iii)	Support common protocols and interfaces for the sharing and presentation to relying parties of person identification data, electronic attestation of attributes or of selectively disclosed related data online and, where appropriate, in offline mode
Art. 5a(5)(a)(iv)	Support common protocols and interfaces for the user to allow interaction with the EUDI Wallet and display EUDI Trust Marks
Art. 5a(5)(a)(vii)	Support common protocols and interfaces for authenticating and identifying relying parties by implementing authentication mechanisms in accordance with Article 5b
Art. 5a(5)(a)(viii)	Support common protocols and interfaces for Relying Parties to verify the authenticity and validity of European Digital Identity Wallets
Art. 5a(5(c)	Relying Parties can be authenticated and identified by implementing authentication mechanisms in accordance with Article5b
Art. 5a(8)(b)	Allow Users to verify the authenticity and validity of the identity of Relying Parties registered with free-of-charge validation mechanisms
Art. 5b(8)	Where Relying Parties intend to rely upon European Digital Identity Wallets, they shall identify themselves to the User
Art. 5b(9)	Relying parties shall not refuse the use of pseudonyms, where the identification of the user is not required by Union or national law
Art. 5b(10)	Intermediaries acting on behalf of relying parties shall be deemed to be relying parties and shall not store data about the content of the transaction.
Art. 5f(2)	Private Relying Parties, with the exception of micro enterprises and small enterprises, shall also accept EUDI Wallets
Art. 11a(1)	Relying Parties for cross-border services shall ensure unequivocal identity matching for natural persons

Table 8
Highlighted Articles - Wallet Solution

Article Item	Context
Art. 5a(4)(a)	General features. What the User shall be able to do using the Wallet.
Art. 5a(4)(c)	Wallet to Wallet flow. Data exchange, presentation, between the two Wallets.
Art. 5a(4)(d)	Historical tracking of RPs involved in presentations, with possibility to report to data protection authorities.
Art. 5a(4)(e)	Qualified electronic signatures or Seal by means of Qualified Electronic Seals capabilities.
Art. 5a(4)(g)	Data portability.
Art. 5a(5)(a)(v)	User onboarding using an electronic identification means in accordance with Article 5a(24).
Art. 5a(5)(a)(vi)	Support for common Protocols and Interfaces for interaction between two persons' EUDI Wallets.
Art. 5a(5)(a)(ix)	Support for common Protocols and Interfaces for requesting a Relying Party the erasure of personal data.
Art. 5a(5)(a)(x)	Support for common Protocols and Interfaces for reporting a Relying Party to the competent national authority.
Art. 5a(7)	Optional additional features are possible, including interoperability with existing national electronic identification means.
Art. 5a(8)(a)	Authenticity and validity of European Digital Identity Wallets can be verified with free-of-charge mechanisms.
Art. 5a(9)	Revocation circumstances: user decision, security issue or death of the user or cease of activity of the legal person.
Art. 5a(10)	Users can easily request technical support and report technical problems or any other incidents.
Art. 5a(11)	EUDI Wallet shall be provided under an electronic identification scheme with assurance level high.
Art. 5a(13)	The issuance, use and revocation of the European Digital Identity Wallets shall be free of charge to all natural persons.
Art. 5a(14)	The Wallet Provider shall not collect personal information about the usage of the Wallet by the User.
Art. 5a(21)	Accessible for use, by persons with disabilities.