A DID-Based Framework for Secure Digital Identity and Inter-Institutional Communication in Government Services

Andreea DINU, Paul-Cristian VASILE , Alexandru GEORGESCU
National Institute for Research and Development in Informatics – ICI Bucharest, Bucharest, Romania
andreea.dinu@ici.ro, paul.vasile@ici.ro, alexandru.georgescu@ici.ro

Abstract: The digital transformation of government services requires secure, interoperable, and privacy-preserving mechanisms for managing digital identities and exchanging information between citizens and public institutions. This paper explores the application of Decentralized Identifiers (DIDs) and Verifiable Credentials (VCs) in governmental environments, focusing on their potential to support trusted digital interactions while reducing dependence on centralized identity management systems. The proposed approach combines decentralized identity mechanisms, distributed ledger technologies, and secure peer-to-peer communication to support authentication, verification, traceability, and controlled disclosure of identity information.
Three complementary governmental scenarios are presented: citizen enrolment and issuance of verifiable credentials, access to digital government services through selective presentation of identity attributes, and secure inter-institutional communication using DID-based channels. The scenarios illustrate how decentralized identity technologies can support more secure and transparent digital public services while promoting data minimization, user control, interoperability, and auditability. The paper also discusses the main security, privacy, and trust considerations associated with the proposed approach and its potential for further integration into digital government ecosystems.
Keywords: Decentralized Identifiers (DID), Self-Sovereign Identity (SSI), Verifiable Credentials, Digital Identity, Digital Government, Blockchain, Secure Communication, Interoperability, Data Privacy.

INTRODUCTION

The continuous digitalization of public administration has significantly changed the way citizens interact with governmental institutions. Public services that traditionally required physical presence are increasingly delivered through online platforms, making reliable digital identification and authentication fundamental components of modern e-government ecosystems. However, the expansion of digital public services

https://doi.org/10.54851/v8i2y202602

also increases the amount of personal and identity-related information processed by governmental systems and raises important concerns regarding privacy, security, interoperability and trust. In the Romanian context, Petcu and Barbu (2022) highlight the importance of ensuring the availability, integrity and resilience of information systems alongside the protection of personal data.

Traditional digital identity management systems generally rely on centralized or federated architectures in which identity providers are responsible for storing, managing, and validating users' identity information. While these approaches have enabled the development of electronic services on a scale, their dependence on centralized identity providers and repositories introduces several limitations, including concentration of sensitive information, limited user control over personal data, interoperability challenges and potential single points of failure. Soltani et al. (2021) identified, in their survey of Self-Sovereign Identity (SSI) ecosystems, the increasing complexity and fragmentation of conventional digital identity practices as important drivers for the development of decentralized identity models. Similar limitations of traditional electronic identity systems, particularly their reliance on central entities and the limited control provided to users over their identity data, have been highlighted in the context of e-government services by Pöhn et al. (2021).

These challenges become particularly relevant in the governmental sector, where digital interactions may involve sensitive personal information and multiple public authorities. A citizen may be required to repeatedly provide identity information or supporting documents to different institutions, while institutions need mechanisms for determining whether identity information, credentials, and their issuers can be trusted. Moreover, public-sector digital identity infrastructures must support not only citizen-to-government interactions but also secure and interoperable exchanges between governmental organizations.

Recent research on national digital identity systems confirms that technological architecture alone is insufficient for addressing these requirements. Legal frameworks, data protection requirements, governance mechanisms, and interoperability between participating organizations are also important factors in the successful implementation of national digital identity infrastructures (Naghmouchi et al., 2025).

Self-Sovereign Identity has emerged as an alternative identity management paradigm in which individuals can exercise greater control over their digital identities and the disclosure of their personal information. Its technical ecosystem is commonly built around Decentralized Identifiers (DIDs), Verifiable Credentials (VCs), digital wallets, cryptographic mechanisms and distributed trust infrastructures (Soltani et al., 2021). In this model, trusted issuers can provide digitally signed credentials containing specific identity attributes, which are stored and managed by the holder and subsequently presented to a verifier when required. Such an approach can enable users to disclose only the information necessary for a particular interaction instead of systematically transferring complete identity records. Research on SSI and digital wallets highlights this issuer-holder-verifier model as a fundamental mechanism through which verifiable claims can be exchanged and validated (Babel et al., 2025).

The application of SSI to governmental services has consequently received increasing research attention. Pöhn et al. (2021) investigated the relationship between electronic identities and SSI and analysed existing initiatives to identify lessons and challenges associated with introducing SSI into governmental environments. Weigl et al. (2023) subsequently demonstrated that the implementation of SSI cannot be considered exclusively as a technological problem, as institutional characteristics and different interpretations of technology influence its design and adoption.

From a governance perspective, Gans et al. (2022) examined blockchain-based SSI and highlighted the implications of shifting control over identity data toward individuals, while also emphasizing that the introduction of such infrastructures creates new governance considerations for public authorities. More recent research by Feulner et al. (2025) specifically examined SSI innovation in the public sector through a case study involving tax registration for online marketplaces. Their findings suggest that the value of SSI in public organizations depends not only on technical capabilities but also on how those capabilities fit organizational, cultural, regulatory, and political contexts.

Interoperability remains another significant issue. Decentralized identity ecosystems may involve credentials issued by different organizations and used across different administrative domains. Research on cross-domain decentralized identity has therefore investigated trust architectures capable of supporting the verification of credentials issued by different entities and has identified trust registries and common verification mechanisms as important elements for broader SSI adoption (Johnson et al., 2025)

Although previous studies have extensively discussed the principles, architecture, governance requirements and adoption challenges associated with SSI, an important research direction concerns the translation of these concepts into concrete and interconnected governmental workflows. Public-sector applications require mechanisms that cover the complete identity lifecycle, from credential issuance to service access and trusted communication between institutions.

Therefore, this paper investigates how DID-based identities and Verifiable Credentials can be integrated into operational scenarios for digital government services, through the national project "Resilient and Interoperable Communication Systems Based on Distributed Technologies and Self-Sovereign Digital Identity – RODID". Rather than considering identity verification as an isolated process, the proposed approach combines decentralized identity management, credential verification, distributed trust mechanisms, and secure peer-to-peer communication within a common framework.

The main contribution of this work is the definition and analysis of three complementary governmental scenarios:

- Citizen enrolment and Verifiable Credential issuance, where a trusted governmental entity verifies the citizen and issues digitally signed credentials associated with a decentralized identity;
- Access to digital government services, where citizens use their credentials to provide the specific identity attributes required by a public service while limiting unnecessary disclosure of personal information;
- Secure inter-institutional communication, where governmental entities establish trusted DID-based communication channels for exchanging requests, confirmations, credentials, and other relevant information.

Together, these scenarios represent an end-to-end approach in which the same decentralized trust ecosystem supports identity issuance, identity verification, digital service access and government-to-government communication. This structure directly reflects the operational workflows proposed for the RoDID governmental pilot, which combines DID, Verifiable Credentials, a digital issuer registry, blockchain-based integrity and traceability mechanisms, and secure peer-to-peer communication.

The paper aims to evaluate the applicability of such an approach to governmental environments and to discuss its potential contribution to data minimization, interoperability, security, auditability, and trust in digital public services.

DECENTRALIZED DIGITAL IDENTITY AND SECURE COMMUNICATION

The implementation of decentralized identity in digital government relies on several complementary technologies that together provide mechanisms for identification, authentication, trust establishment, and secure information exchange. Within the proposed approach, the main technological components are Decentralized Identifiers (DIDs), Verifiable Credentials (VCs), blockchain technology, and secure peer-to-peer (P2P) communication. Their integration provides the technological foundation for the governmental scenarios presented in this paper. For deployment in Romanian public services, RoDID would need to align with the European Digital Identity Framework established by Regulation (EU) 2024/1183 (eIDAS 2.0), particularly its requirements for wallet interoperability, trusted attribute issuance and selective disclosure, with regulatory compliance remaining subject to further validation (European Parliament and Council, 2024).

Decentralized Identifiers (DIDs) represent a new type of identifier designed to enable verifiable and decentralized digital identities. A DID is associated with a DID Document containing the information required to authenticate an entity and establish trusted interactions, such as public cryptographic keys and verification mechanisms. Unlike conventional identifiers that depend on a centralized identity provider, DIDs can support identity models in which individuals and organizations have greater control over their digital identities (W3C,2022). In the RoDID approach, DIDs represent the foundation for identifying both citizens and institutional actors and for establishing trusted digital interactions.

Verifiable Credentials (VCs) complement DIDs by enabling trusted entities to issue digitally verifiable claims about an individual or organization. A credential may contain attributes such as identity information, residence, fiscal status, eligibility for a public benefit, or the legal capacity to represent an organization. Within the governmental scenarios considered in this work, credentials are issued by authorized entities and stored by citizens in their digital wallets. They can subsequently be presented to a public institution when accessing a service. This model also enables the disclosure of only the attributes required for a specific interaction, supporting the principle of data minimization (W3C,2025).

Blockchain technology provides the distributed trust and traceability layer of the proposed ecosystem. Rather than storing complete identity information directly on the blockchain, the RoDID approach uses the distributed infrastructure to support credential integrity, issuer validation, revocation status, timestamps and audit-related information. The immutable and chronological nature of blockchain records can therefore provide a verifiable history of relevant operations while supporting interactions between multiple participating entities. In the proposed workflows, for example, credential hashes or anchors and revocation information can be published to the blockchain, while a dedicated digital registry is used to validate credential issuers (Yaga et al., 2018).

Finally, secure peer-to-peer communication enables authenticated and confidential information exchange between entities identified through DIDs. This component is particularly relevant for government environments, where communication may involve citizens, service providers, and multiple public institutions. Instead of relying exclusively on conventional communication channels, DID-based P2P communication can establish trusted channels through which requests, proofs, credentials, confirmations and other information can be exchanged. In the inter-institutional scenario, for example, two institutions establish a DID-to-DID channel and exchange signed information through an authenticated and confidential communication

mechanism, while relevant interactions can be recorded for auditing purposes.

Together, these technologies form an integrated framework in which DIDs provide decentralized identification, Verifiable Credentials provide trustworthy digital attestations, blockchain supports trust and traceability, and P2P communication enables secure exchanges between identified entities. This technological foundation supports the three governmental scenarios analyzed in the following sections: citizen enrolment and credential issuance, access to digital government services, and secure inter-institutional communication.

PROPOSED FRAMEWORK FOR GOVERNMENT SERVICES

The proposed framework integrates decentralized identity management and secure communication mechanisms to support trusted interactions between citizens and public institutions. Its architecture follows the principles of the RoDID ecosystem, combining Decentralized Identifiers (DIDs), Verifiable Credentials (VCs), a digital registry of trusted credential issuers, blockchain infrastructure, digital wallets, and secure peer-to-peer communication. The objective is to establish a common trust environment in which identity information can be issued, presented, verified, and exchanged without requiring repeated transfer or centralized storage of complete identity records.

The architecture involves three main categories of actors: the Holder, the Issuer, and the Verifier. The Holder, typically a citizen, controls a digital wallet containing the DID and the credentials issued to them. The Issuer is a trusted public authority responsible for validating identity information and issuing cryptographically signed credentials. The Verifier represents a public institution or digital government service that requests and verifies specific identity attributes before granting access to a service. This model is consistent with the identity interaction model described within the project, which distinguishes between the identity owner, the entity requesting identity information and the trusted entity responsible for validating it.

An additional role is played by the trust infrastructure, consisting of the blockchain network and the digital registry of credential issuers. The issuer registry enables participating entities to determine whether a credential originates from a recognized issuer, while the blockchain layer can support integrity verification, credential status, timestamps and traceability. In the proposed pilot workflow, for example, the credential is cryptographically signed by the issuer, the issuer is validated through the digital registry and the credential hash or anchor, and revocation status can be recorded on the blockchain. Importantly, personal identity information does not need to be stored directly on the blockchain; the distributed ledger primarily provides a trust and audit layer for the ecosystem.

The communication layer connects these identity components and enables secure interactions between the actors. When accessing a governmental service, the Verifier sends a request for the identity attributes required for that specific service. The citizen's wallet selects the corresponding information from the available credentials and communicates the required proof through the DID-based P2P protocol. The Verifier can then validate the credential signature, verify the issuing authority through the issuer registry, and check relevant credential status information before granting access to the service.

The same communication model can be extended to institution-to-institution interactions. Public authorities can establish DID-to-DID communication channels through which requests, confirmations, or credentials are exchanged in an authenticated and confidential manner. Relevant interactions can additionally be recorded or anchored for auditing and traceability purposes.

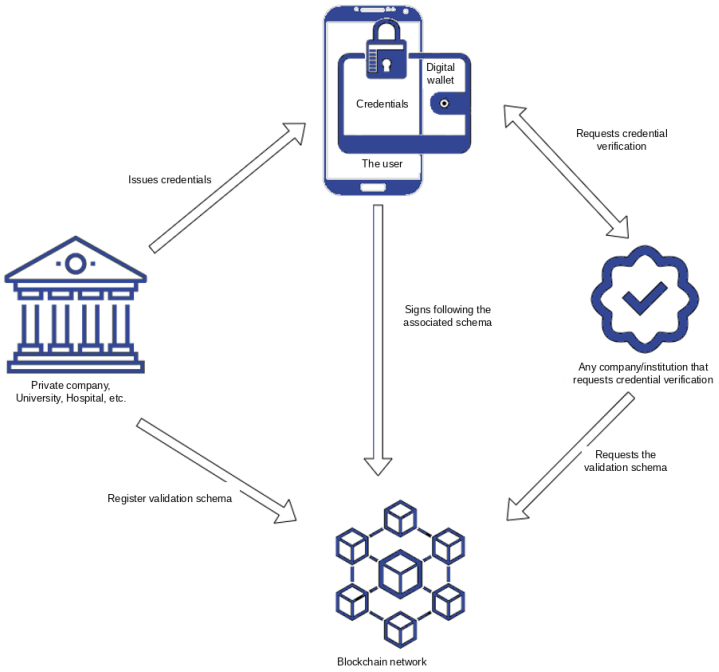


Figure 1. *Workflow schema for issuing, verifying and using DIDs and credentials*

Therefore, the proposed architecture can be viewed as the interaction of three interconnected layers: an identity layer, based on DIDs, wallets, and Verifiable Credentials; a trust and verification layer, supported by the issuer registry and blockchain infrastructure; and a communication layer, based on secure DID-enabled P2P exchanges. Together, these components provide the technological foundation for the governmental scenarios presented in the following section.

DID-BASED GOVERNMENTAL SCENARIOS

To demonstrate the applicability of the proposed framework in the public sector, three complementary governmental scenarios are considered. The scenarios cover the main stages of a decentralized digital identity lifecycle: identity enrolment and credential issuance, credential-based access to public services, and secure communication between governmental institutions. Together, they illustrate how DIDs, Verifiable Credentials, blockchain-based trust mechanisms, and secure peer-to-peer communication can support interactions between citizens and public authorities.

Scenario 1 – Citizen Enrolment and Verifiable Credential Issuance

The first scenario addresses the creation of a decentralized identity and the issuance of trusted digital credentials to a citizen. The process begins when the citizen creates a DID through a digital wallet. A public authority acting as an Issuer performs the initial identity verification using the information and procedures required for the respective governmental context.

Following successful verification, the institution issues a cryptographically signed Verifiable Credential, which is transferred to the citizen's wallet. The issuing institution is validated through the digital registry of trusted issuers, while relevant information regarding credential integrity and revocation status can be anchored in the blockchain infrastructure.

Depending on the governmental service, the issued credentials may represent different attributes or statuses, including basic identity information, residence, fiscal

status, eligibility for a public benefit, or the legal capacity to represent an organization. The resulting credential can subsequently be reused in interactions with authorized public services without requiring the citizen to repeatedly submit conventional copies of identity documents.

A concrete application of this scenario in the Romanian public sector could involve ANAF issuing a fiscal-status credential to a citizen. Following identity authentication and verification of the relevant tax records, ANAF could issue a cryptographically signed Verifiable Credential confirming that, at the time of issuance, the citizen has no outstanding fiscal obligations.

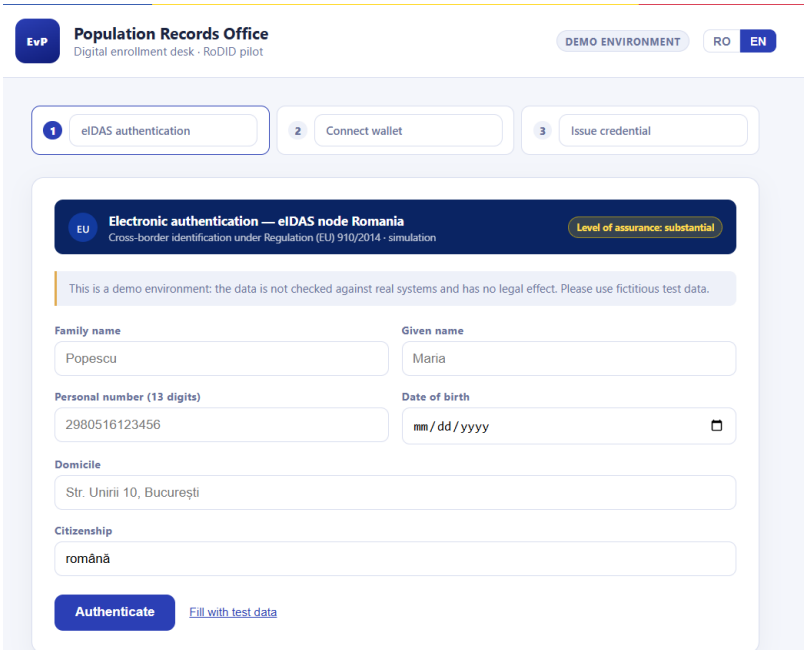


Figure 2. *Enrolment dashboard*

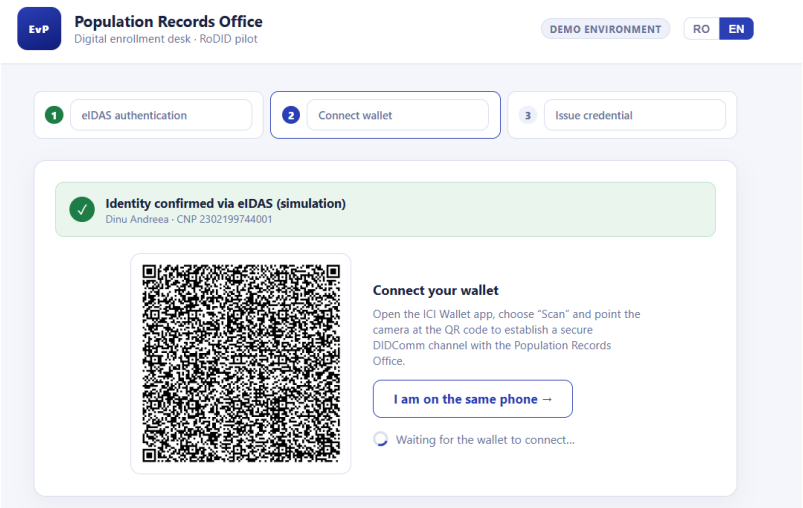


Figure 3. *Communication channel establishment page*

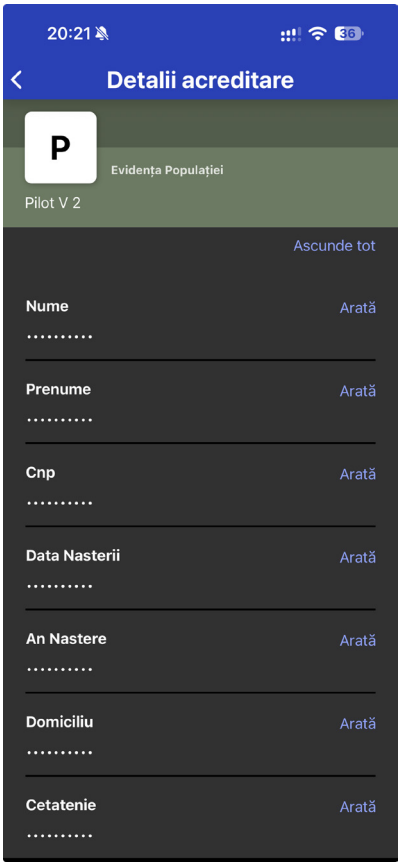


Figure 4. *Credential details*

Scenario 2 – Access to Digital Government Services

The second scenario demonstrates how previously issued credentials can be used to access a digital public service. A citizen initiates an interaction with a governmental portal, such as when submitting an administrative request, requesting a document, accessing a benefit, or authenticating to an institutional service.

Instead of requesting the complete identity dataset, the institution sends a proof request specifying the information required for the service. For example, the citizen may be asked to demonstrate identity, residence, and that a particular age requirement is satisfied. The citizen's wallet identifies the relevant credentials and provides the required attributes through the DID-based communication mechanism.

The governmental system then verifies the credential's cryptographic signature, validates the Issuer against the trusted issuer registry, and checks relevant blockchain information, including integrity, revocation status, and timestamps. If these checks are successfully completed, access to the requested service can be granted. A corresponding audit event may also be recorded or anchored in the blockchain infrastructure.

This scenario is particularly relevant from a privacy perspective because it supports data minimization: the interaction can be designed around the information required for a particular administrative process rather than the systematic exchange of complete identity records. The workflow can also reduce repeated document submission and facilitate automated verification and traceability.

Building on the example presented in Scenario 1, when the citizen subsequently accesses a service provided by a Romanian local authority that requires proof of fiscal status, the wallet presents the previously issued credential, the wallet presents the

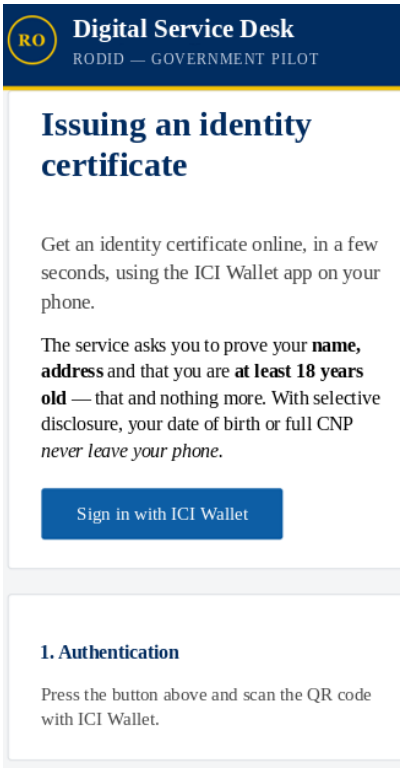


Figure 5. *General digital service service use case page*



Figure 6. *Request for digital credential proof*

credential rather than requiring the citizen to obtain and upload a new fiscal certificate. The local authority verifies the credential's issuer, signature, validity and revocation status through the decentralized trust infrastructure. Where the service does not require the complete fiscal record, the citizen could disclose only the necessary statement or attribute, reducing unnecessary exchange of personal data.

Scenario 3 – Secure Inter-Institutional Communication

The third scenario extends the use of decentralized identities from citizen-to-government interactions to government-to-government communication. Public institutions frequently need to exchange confirmations, requests, documents, or other information when processing administrative procedures. The proposed scenario uses institutional DIDs and secure P2P communication to establish authenticated communication channels between participating authorities.

An institution initiates a DID-to-DID communication channel with another institution and sends a request for confirmation or additional information through the secure P2P protocol. The receiving institution responds through the authenticated and confidential channel and digitally signs the response. Where required, the response may also contain a Verifiable Credential or another digitally signed confirmation whose cryptographic proof may be anchored to the blockchain. Relevant interactions can subsequently be logged to provide an auditable record of the communication process.

A relevant application of the proposed government-to-government communication model could involve the National Trade Register Office (ONRC) and the National Agency for Fiscal Administration (ANAF) in an administrative procedure concerning a Romanian company. When processing a request that requires fiscal information or confirmation of specific company-related data, ONRC could initiate a secure DID-to-DID communication channel with ANAF instead of requiring the company's representative to obtain and submit supporting documents separately. Both institutions would be represented by institutional DIDs registered within the trusted governmental ecosystem.

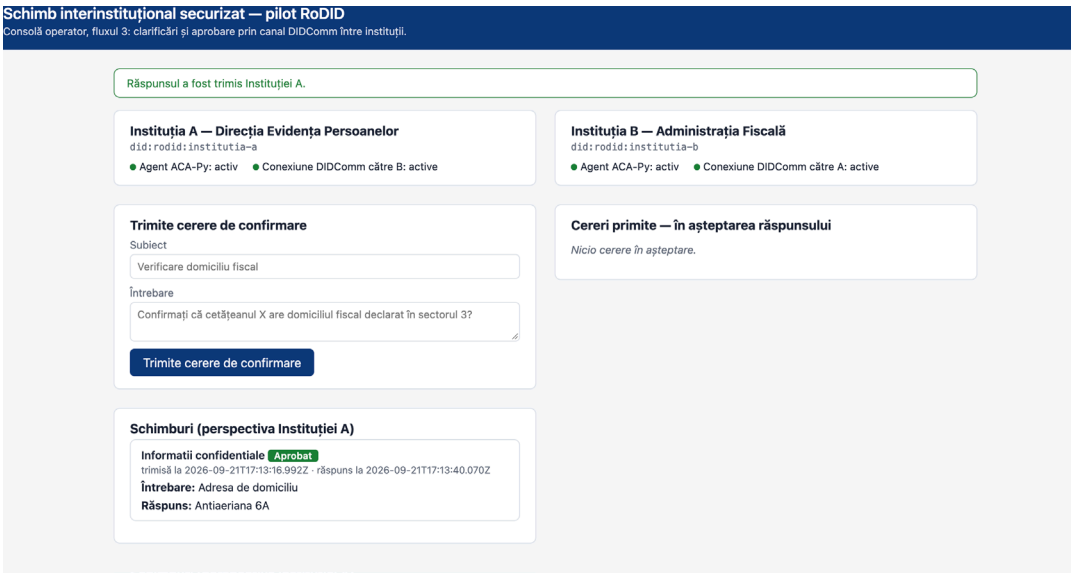


Figure 7. *Inter-institutional communication dashboard*

ONRC would send a digitally signed request specifying the company and the information required for the administrative procedure. ANAF would authenticate ONRC, verify its authorization to request the information, retrieve the relevant data from its authoritative systems, and return a digitally signed response through the encrypted P2P channel. Where appropriate, the response could take the form of a Verifiable Credential, for example confirming a specific fiscal status or attribute of the legal entity. The receiving institution could automatically verify the issuer, signature, validity, and credential status before using the information in its administrative workflow. To support accountability and auditability, cryptographic proofs, timestamps, and transaction references could be anchored to the blockchain, while the actual fiscal or company-sensitive information would remain off-chain. In this way, decentralized identity provides a trusted communication layer between public institutions, reducing repeated document requests, limiting the role of companies as intermediaries in administrative data exchange, and enabling verifiable cross-agency workflows.

Collectively, these scenarios illustrate the RoDID ecosystem as an integrated trust framework supporting citizen-to-government and government-to-government interactions. By combining decentralized identities, Verifiable Credentials, blockchain-based trust mechanisms, and secure P2P communication, RoDID enables identity verification, trusted data exchange, and inter-institutional interoperability within a common technological framework. This approach provides a foundation for secure, privacy-preserving and interoperable digital public services.

SECURITY, PRIVACY AND TRUST CONSIDERATIONS

The adoption of decentralized identity technologies in governmental services requires particular attention to security, privacy, and trust, as the proposed scenarios involve sensitive identity information and interactions between citizens and public institutions. Within the proposed framework, these aspects are addressed through a combination of cryptographic mechanisms, Verifiable Credentials, decentralized identifiers, trusted issuer validation, blockchain-based traceability, and secure communication channels.

From a security perspective, DIDs and Verifiable Credentials provide mechanisms for authenticating participating entities and verifying the integrity and authenticity of digital credentials. Credentials are cryptographically signed by their issuers, allowing a verifier to determine whether the presented information originates from an authorized entity and whether it has been modified. In the proposed governmental scenarios, this verification is complemented by checking the issuer against the digital registry and validating relevant credential status information, including revocation and integrity information. Secure DID-based peer-to-peer communication further supports confidentiality and authenticity when sensitive information is exchanged between governmental institutions.

Privacy represents another important requirement, particularly because governmental services may process extensive amounts of personally identifiable information. The proposed approach follows the principle of data minimization, allowing citizens to provide the attributes required for a specific service rather than systematically disclosing their complete identity information. For example, a service could request proof of identity, residence, or fulfilment of an age requirement, while the wallet selects the relevant attributes from the available credentials. This approach is consistent with the SSI principles considered in RoDID, including user control, consent, minimization, and protection of identity information.

An important privacy consideration is the separation between personal identity data and information recorded on the blockchain. Sensitive personal information should not be directly stored on an immutable distributed ledger. Within the proposed scenarios, blockchain is instead used as a supporting trust and traceability mechanism, for example by storing or anchoring credential hashes, revocation information, timestamps, or audit-related events. The actual credential remains under the control of the holder through the digital wallet. This separation reduces unnecessary exposure of personal information while maintaining the possibility of verifying credential integrity and status.

Trust is established through the interaction of multiple components rather than through a single centralized authority. The digital registry of credential issuers provides a mechanism for determining whether an organization is authorized to issue a particular credential, while cryptographic verification establishes the authenticity and integrity of the credential itself. Blockchain-based records can additionally support traceability and auditing of relevant operations. The RoDID project specifically envisages a digital registry of Verifiable Credential issuers to automate the verification of decentralized identities and facilitate interoperability between public institutions.

However, decentralized identity does not eliminate the need for governance and institutional trust. Public authorities still need clearly defined responsibilities concerning credential issuance, verification, revocation, wallet management, access control, and the recognition of trusted issuers. Technical trust mechanisms therefore need to operate together with appropriate organizational and governance rules, particularly when credentials are exchanged across different governmental institutions.

Overall, the proposed framework combines cryptographic trust, controlled disclosure of identity information, issuer validation, secure communication, and auditability. These mechanisms provide the security and privacy foundation required for the governmental scenarios while maintaining the traceability necessary for public-sector processes. At the same time, their practical deployment requires an appropriate balance between decentralization, user control, institutional accountability, and regulatory requirements.

DISCUSSION AND FUTURE PERSPECTIVES

The governmental scenarios presented in this paper demonstrate how decentralized identity technologies can be integrated into different stages of digital public service delivery. Rather than addressing digital identity only as an authentication mechanism, the proposed approach connects credential issuance, identity verification, service access, secure communication, and auditability within a common trust framework. This is consistent with the broader objective of RoDID to support secure digital services for citizens while improving interoperability between public institutions.

One of the main advantages of the proposed approach is the possibility of reducing repeated exchange and storage of personal information. Verifiable Credentials allow citizens to reuse trusted digital evidence issued by authorized institutions, while selective presentation mechanisms can limit the information disclosed according to the requirements of a particular service. From an institutional perspective, automated verification of credential authenticity, issuer status, and revocation could simplify administrative processes and reduce reliance on manually verified documents.

Another relevant aspect is inter-institutional interoperability. Government services frequently involve more than one public authority, requiring information or confirmations to move between different organizations. The use of institutional DIDs, trusted issuer registries, and secure P2P

communication could provide a common mechanism for establishing the identity of participating organizations and exchanging authenticated information. This is particularly relevant for processes involving sensitive information, where confidentiality and auditability are essential.

Nevertheless, the transition from experimental scenarios to operational governmental services introduces several challenges. Technical interoperability must be complemented by common governance rules defining which institutions can issue credentials, how trusted issuers are registered, how credentials are revoked, and how responsibilities are distributed among ecosystem participants. Furthermore, integration with existing public-sector information systems, digital identity infrastructures, and administrative processes represents an important consideration for real-world deployment.

Future work should therefore focus on the implementation and evaluation of the proposed scenarios in a governmental pilot environment. Attention should be given to evaluating technical performance, security, usability, interoperability, and the practical interaction between citizens, credential issuers, and governmental service providers. Future work could also explore domain reputation assessment as a complementary security measure for governmental portals, drawing on the machine-learning-based approach proposed by Rotuna et al. (2025) for identifying potentially malicious .ro domains.

Further research could also investigate the extension of the framework toward cross-institutional and cross-border digital identity ecosystems, where credentials issued by one trusted authority could be recognized by other organizations according to common technical and governance rules. Such developments could provide a pathway from isolated DID-based applications toward interoperable ecosystems in which decentralized identity and secure communication mechanisms support a broader range of digital public services.

CONCLUSIONS

This paper presented a DID-based approach for supporting digital identity management and secure communication in governmental services. The proposed framework integrates Decentralized Identifiers, Verifiable Credentials, blockchain-based trust mechanisms, trusted issuer registries, digital wallets, and secure peer-to-peer communication, reflecting the technological components considered within the RoDID project.

Three complementary scenarios were analyzed: citizen enrolment and Verifiable Credential issuance, access to digital government services using verifiable identity information, and secure inter-institutional communication. Together, these scenarios cover interactions between citizens and public authorities as well as exchanges between governmental institutions, illustrating how decentralized identity can be incorporated into different stages of digital public-service delivery.

The proposed approach highlights several potential benefits, including data minimization, reduced duplication of identity information, automated credential verification, improved traceability, and secure information exchange. At the same time, the analysis shows that successful implementation depends not only on the underlying technologies but also on interoperability, governance, trusted issuer management, credential lifecycle management, privacy protection, and integration with existing governmental infrastructures.

Future work will focus on the practical implementation and evaluation of the proposed scenarios within a governmental pilot environment, allowing the framework to be assessed from technical, security, interoperability, and usability perspectives. Such validation represents an important step toward determining how DID-based identity and secure communication mechanisms can contribute to more interoperable, privacy-preserving, and trustworthy digital government ecosystems.

ACKNOWLEDGEMENTS

This work was supported by the RoDID project, "Resilient and Interoperable Communication Systems Based on Distributed Technologies and Self-Sovereign Digital Identity" (Project Code PN 23 38 01 01), under Contract No. 13N/2023, within the National Core Programme FUTURE TECH, carried out by the National Institute for Research and Development in Informatics – ICI Bucharest.

REFERENCE LIST

Babel, M., Willburger, L., Lautenschlager, J. *et al.* (2025) Self-sovereign identity and digital wallets. *Electron Markets,* 35, article 28, doi: 10.1007/s12525-025-00772-0

European Parliament and Council (2024) 'Regulation (EU) 2024/1183 of 11 April 2024 amending Regulation (EU) No 910/2014 as regards establishing the European Digital Identity Framework', *Official Journal of the European Union*, L, 2024/1183, 30 April. Available at: https://data.europa.eu/eli/reg/2024/1183/oj.

Feulner, S., Guggenberger, T., Lautenschlager, J., Urbach, N. and Völter, F. (2025) 'Self-sovereign identity in the public sector: Affordances, experimentation, and actualization', *Government Information Quarterly*, 42(3), article 102052. doi: 10.1016/j.giq.2025.102052

Gans, R.B., Ubacht, J. and Janssen, M. (2022) 'Governance and societal impact of blockchain-based self-sovereign identities', *Policy and Society*, 41(3), pp. 402–413. doi:10.1093/polsoc/puac018

Johnson Jeyakumar, I.H. and Kubach, M. (2025) 'A trust implementation model for cross-domain decentralized identity ecosystems: Architecture, use case, and implementation', Procedia Computer Science, 254, pp. 10–19. doi:10.1016/j.procs.2025.02.059.

Naghmouchi, M., Laurent, M., Levallois-Barth, C. and Kaaniche, N. (2025) 'Perspectives on national digital identity systems', Blockchain: Research and Applications, article 100429, ISSN 2096-7209, doi:10.1016/j.bcra.2025.100429.

Petcu, I. and Barbu, D.-C. (2022) 'The New Challenges of Romania's Cyber Security Policy', *Romanian Cyber Security Journal*, 4(1), pp. 57–67. doi: 10.54851/v4i1y202207.

Pöhn, D., Grabatin, M. and Hommel, W. (2021) 'eID and self-sovereign identity usage: An overview', *Electronics*, 10(22), Article 2811. doi:10.3390/electronics10222811.

Rotuna, C.I., Sacala, I.Ș. and Alexandru, A. (2025) 'Towards Proactive Domain Name Security: An Adaptive System for .ro domains Reputation Analysis', *Future Internet*, 17(10), article 478. doi: 10.3390/fi17100478.

Soltani, R., Nguyen, U.T. and An, A. (2021), 'A survey of self-sovereign identity ecosystem', *Security and Communication Networks*, 2021(1), Article 8873429. doi:10.1155/2021/8873429

W3C (2022). *Decentralized Identifiers (DIDs) v1.0: Core Architecture, Data Model, and Representations.* W3C Recommendation, URL: https://www.w3.org/TR/did/, Accessed: 20 September 2026

W3C (2025). *Verifiable Credentials Data Model v2.0.* W3C Recommendation, URL: https://www.w3.org/TR/vc-data-model-2.0/, Accessed: 20 September 2026

Weigl, L., Barbereau, T. and Fridgen, G. (2023) 'The construction of self-sovereign identity: Extending the interpretive flexibility of technology towards institutions', *Government Information Quarterly*, 40(4), Article 101873. doi:10.1016/j.giq.2023.101873

Yaga, D., Mell, P., Roby, N. and Scarfone, K. (2018). *Blockchain Technology Overview.* NISTIR 8202. National Institute of Standards and Technology. doi: 10.6028/NIST.IR.8202.



This is an open access article distributed under the terms and conditions of the
Creative Commons Attribution-NonCommercial-ShareAlike 4.0 International License.