Privacy and Security - Related Challenges of the Future EU Digital Identity

Andreea Florina RADU
Babes Bolyai University, Cluj-Napoca
andreea.radu@mai.gov.ro

Ioana PETCU
National Institute for Research & Development in Informatics - ICI Bucharest
ioana.petcu@ici.ro

Dragoş-Cătălin BARBU
Bucharest University of Economic Studies
National Institute for Research & Development in Informatics - ICI Bucharest
dragos.barbu@ici.ro

Abstract: The present article comprises a brief analysis of the concept, features and value of the future EU Digital Identity, while its main purpose is to X-ray the present technical infrastructure, the legislative framework and the cyber security challenges of the future EU e-Wallet.
The articles demonstrate that the implementation of future digital identities will pave the way to a greater range of e-government services, more efficient, a need that could be easily identified in the context of the COVID-19 pandemic. Nevertheless, in this context, it also highlights the role of cyber security in the context of the ongoing digital transformation, under the conditions where it becomes more and more obvious that the benefits of the European digital economy and society can only be fully accomplished under the premise of cyber security, as cornerstone of digital transformation. In addition, the article also addresses some privacy and security-related issues of personal data transfers and storage linked to the future e-Wallets. The conclusion aims to underline the role of secure identification services in the context of building a trusted and secure Digital Identity for all European citizens.
Keywords: Cybersecurity, e-Governance, ICT, EU Digital Identity, e-Wallet, EU-DIW, Privacy & security.

A BRIEF INTRODUCTION TO THE SUBJECT

The new industrial revolution, the development of new digital technologies and the new knowledge society, (Petcu, 2020) over which the Covid-19 pandemic overlapped, made the digital transformation gain an alert pace, forcing both governments and organizations to reevaluate their approach in terms of identity management, access to public data and implicitly access to electronic public services for its citizens/companies.

The transversal impact of digitization is felt with small but sure steps in all areas of the economy, administration and society, as a whole.

https://doi.org/10.54851/v4i2y202205

Moreover, indisputable proof of the unprecedented technological revolution (Radu, Petcu, 2021) is the fact that about 20 years ago, mobile phones were used only for a limited range of operations such as phone calls, sending text messages, performing quick calculations, alarm settings. Once, their connection to the Internet (data services) was completed, these devices have acquired additional use, becoming real mobile mini-computers, which provide electronic mail services, data sharing through a variety of applications, navigation through online/satellite maps, banking applications and mobile/digital wallets intended for storing cards, virtual currencies/cryptocurrencies with transaction possibilities, identity and travel documents.

IDENTIFYING THE NEED

At present, in order to access different platforms and services, we need to log in with an email address or a user associated to an email address or a phone number and thus gives full control to such service providers, who can revoke those services at any time. Additionally, there is no universal accepted standards for expressing, exchanging or validating digital credentials across national boundaries. There are already some successful implemented mobile e-IDs in Austria, Belgium, Denmark, Estonia, Latvia, Portugal, with similar patterns on take-up, but different approaches based on the national specifics. In this regard, there is a justified need for emerged standards based on digital verifiable and decentralized identifiers that individuals can own independently, such as e-Wallets. In this respect, *Digital Identity* is the user's key to safe, efficient and in real-time digital services.

THE FUTURE EU DIGITAL IDENTITY WALLET IN THE CONTEXT OF THE DIGITAL TRANSFORMATION

Lato sensu, Digital Identity represents all the information existing in the online environment about a certain person or entity (whereas, entity can be represented by a private company/business agency or government/public institution) or correlated with that person/entity (posts on media platforms, interactions, actions, possible articles and publications, affiliations to various educational institutions, organizations). The digital identity brings together offline information of the person/entity (name, physical address) and online existing data related to that person/entity or created by its online activity.

Stricto sensu, the EU Digital Identity was proposed by the European Commission as a response to the general concern related to personal data management on different accessed web platforms. Each and every time one shares its personal data on a web platform, no control over the data can be granted. So, COM's proposal aims a secured and trustable European e-Identity, which can be used, in a user-controlled manner, to access a variety of services, such as travelling, paying taxes, concluding bank transactions, enrolling in a national or European institution/agency, applying for a job or a scholarship, sharing personal identification, travelling or education documents, purchasing medications, renting a car.

The framework for the future EU Digital Identity was gradually introduced, through a series of European initiatives, Commission's recommendations and important conclusions on the matter expressed by the EU Council as guidance, as shown in Figure 1.

Complementing the previous actions and based on the need for enactment, in June 2021, the European Commission launched a proposal for a Regulation establishing the future European Digital Identity (the so-called EU-ID Regulation, also known as e-IDAS 2) in order to tackle and overcome the shortcomings of the current legislative framework, respectively the e-IDAS Regulation on electronic identification and trust services (EUR – Lex., 2014).

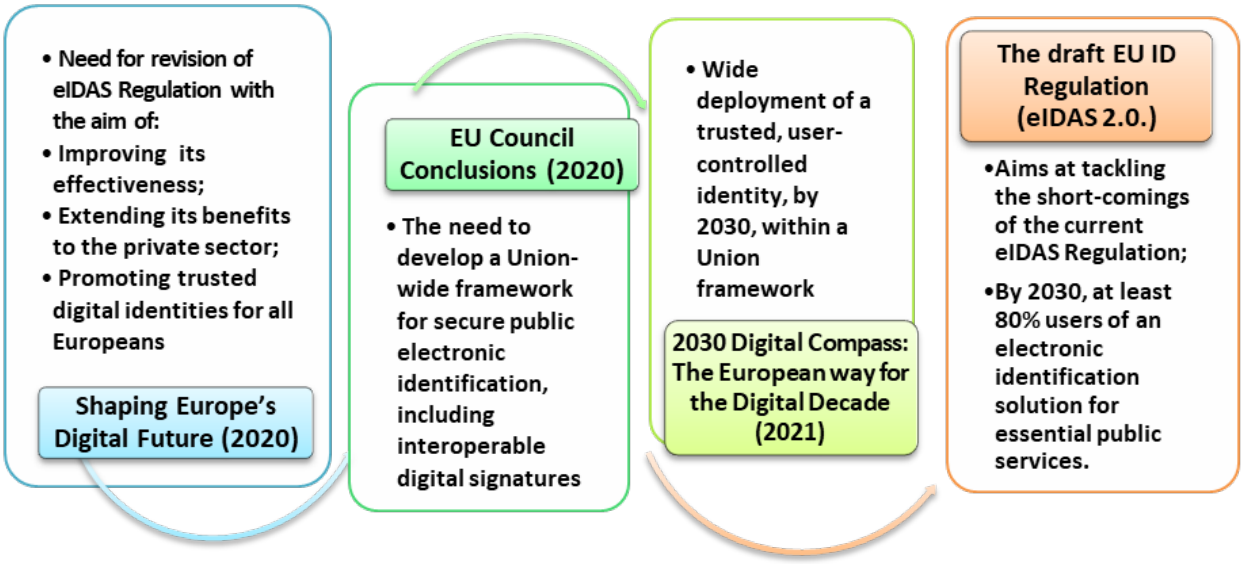

Fig. 1: *EU Digital Identity framework. Gradual initiatives*
Source: adapted by authors

The importance of this proposal, which is currently the subject of negotiations between the EU member states and the COM, resides in the establishment of precise rights and obligations for the future actors involved, as well as features of its main innovation, namely, the digital identity wallet (see Figure 2).

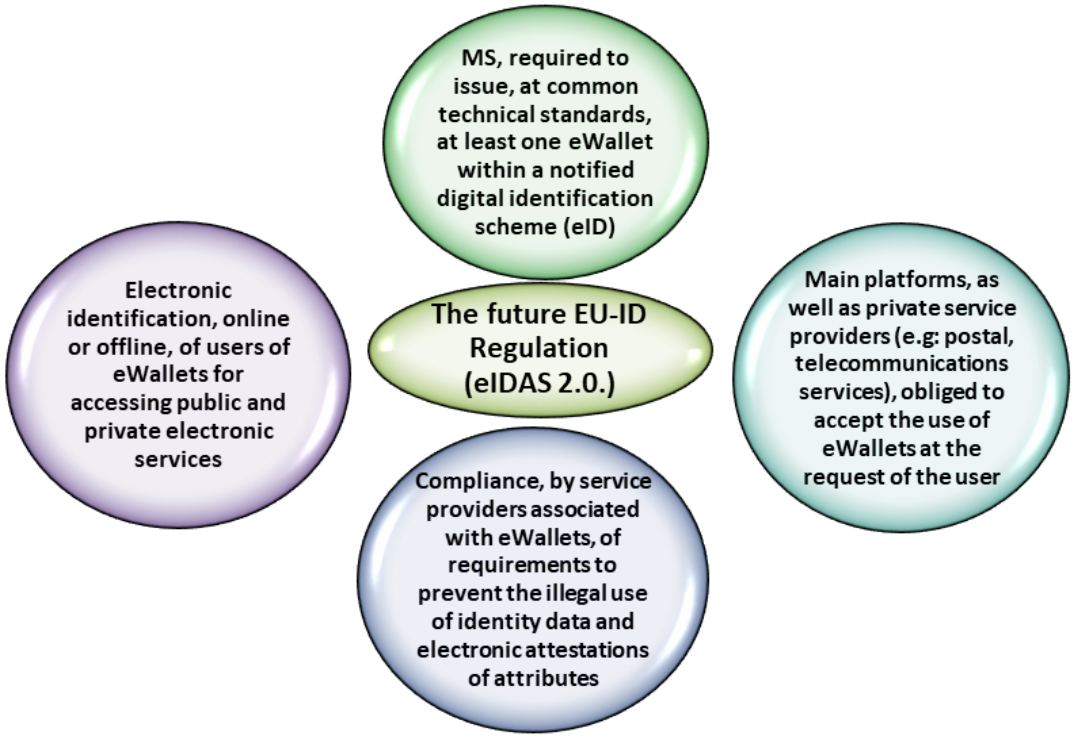

Fig. 2: *The future EU-ID Regulation and its main provisions*
Source: adapted by authors based on the text of the proposal for EU-ID Regulation

De facto, the future framework of European digital identity will be based on a set of clear and common rules regarding the accessibility, the format of the shared data and their security, so that the national digital identity solutions can be replaced by a single solution of electronic attestations of attributes, common to all EU Member States.

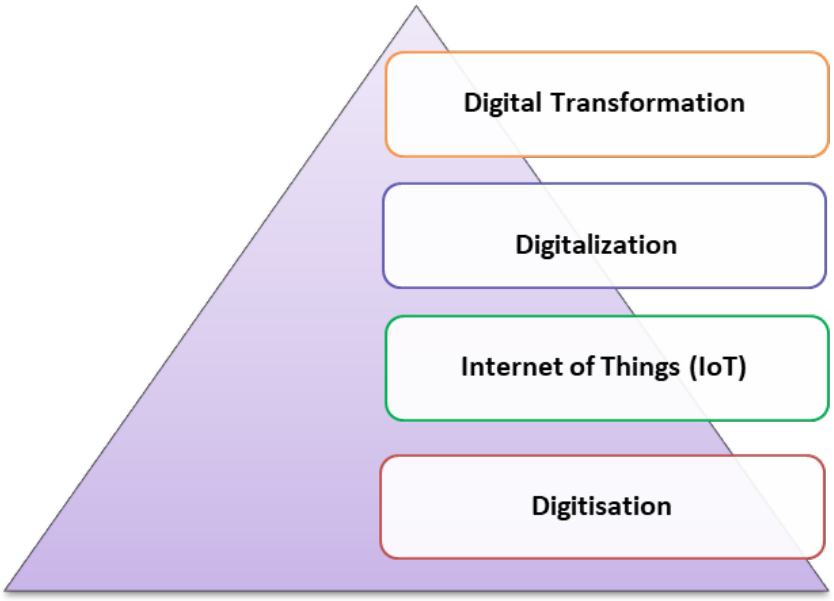

Fig. 3: *From Digitization to Digital Transformation*
Source: adapted by authors

Whereas, Digitization means converting something from analogue to digital. An example is scanning a printed document and thus turning it into a digital format document (e-doc); Internet of things (IoT) means the use of communications and software to connect a digitized item to the internet, meaning that the scanned document transformed into a .pdf document is uploaded to the internet (e.g.: sent to an email address, uploaded to a webpage); Digital Transformation equals to re-designing the working process within the public administration, leveraging digital technologies according to the new technological paradigm and thus creating more efficiency and adding more value to the final beneficiaries (citizens/ companies).

In this regard, it is important to understand that the COM initiative regarding the creation of a European Digital Identity came against the background of the need for a unified approach to digital governance strategies, one that it is no longer left to the will of contextual factors such as culture and institutional heritage, political mandate etc.

The foundation of the new European digital identity is based on 3 pillars, namely:

1. *Strengthening the national e-IDs system under e-IDAS* (by delivering: Security and trust, Improved supply, e-ID mutual recognition procedure at EU level, Extended identity data, Linking Identity and Credentials),
2. *Delivering a European secure and trusted "digital wallet"* (by delivering: improved user control, data control and portability, no tracking) and
3. *Providing identity-linked services by the private sector* (through legislative framework and common standards for private & public attributes, credentials and attestations providers and delivering improved rules applicable for qualified trust services).

Qualified Certificates for Website Authentication (QWACs), addressed in the proposal for an Eu-ID Regulation, represent an important technical tool for establishing the European Digital Single Market. Of course, there is also criticism of the revisions proposed by the Commission. Thus, intense negotiations took place between the COM and the representatives of major browsers such as Chrome, Firefox, Mozilla, Safari regarding the QWAC recognition and use. Those representatives complained in the sense that the technical solutions proposed by the COM would endanger the privacy of end users and create security risks, such as and that it would undermine technical neutrality and interoperability. They also argued on the requirement to incorporate a list of trusted service providers (TSP), agreed by national authorities, to provide new forms of guaranteeing the authenticity of websites, as well as to display QWACs issued by TCPs in a user-friendly manner.

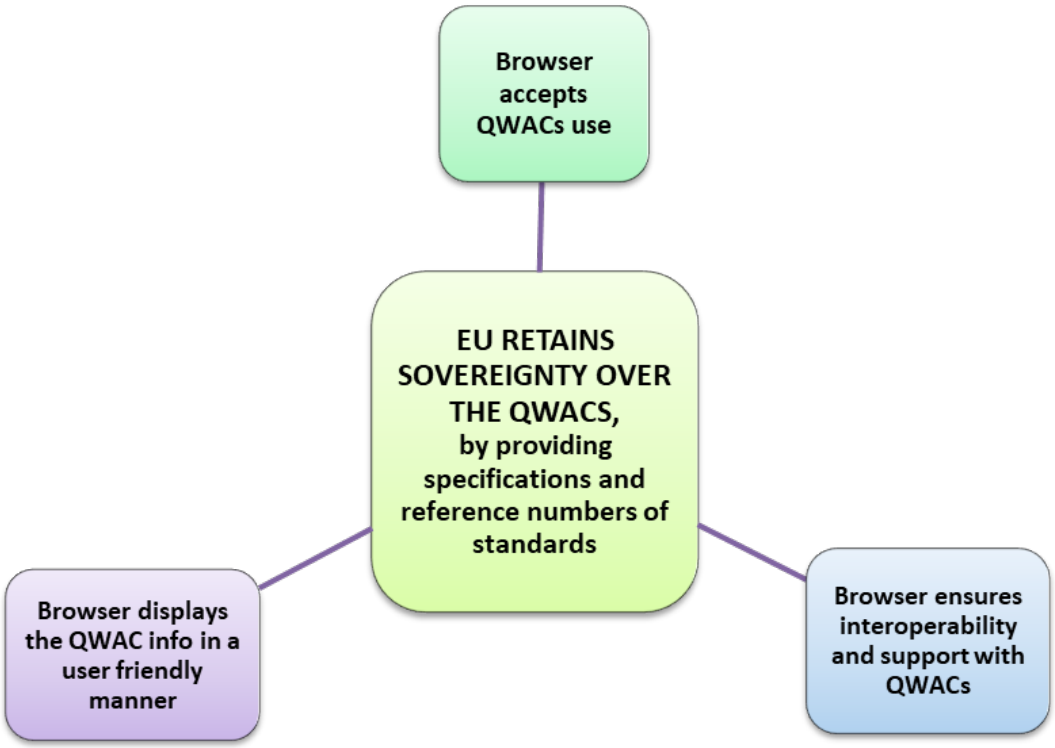

Fig. 4: *The goal of the proposal for an EU-ID Regulation regarding the Qualified Certificates for Website Authentication (QWACs)*
Source: adapted by authors based on the text of the proposal for EU-ID Regulation

MILESTONES AT NATIONAL LEVEL

In terms of the steps undertaken by the Romanian Government on its way to digital transformation, important progresses were done in recent years in all major areas such as the relevant Legislation, Governance and Infrastructure. The most important step was the creation of the Authority for the Digitalization of Romania in 2020, responsible for realizing and coordinating the implementation of strategies and public policies in the field of digital transformation and the information society.

As the DESI index shows, Romania is among the EU member states with the lowest level of e-governance transformation (see Figure 5).

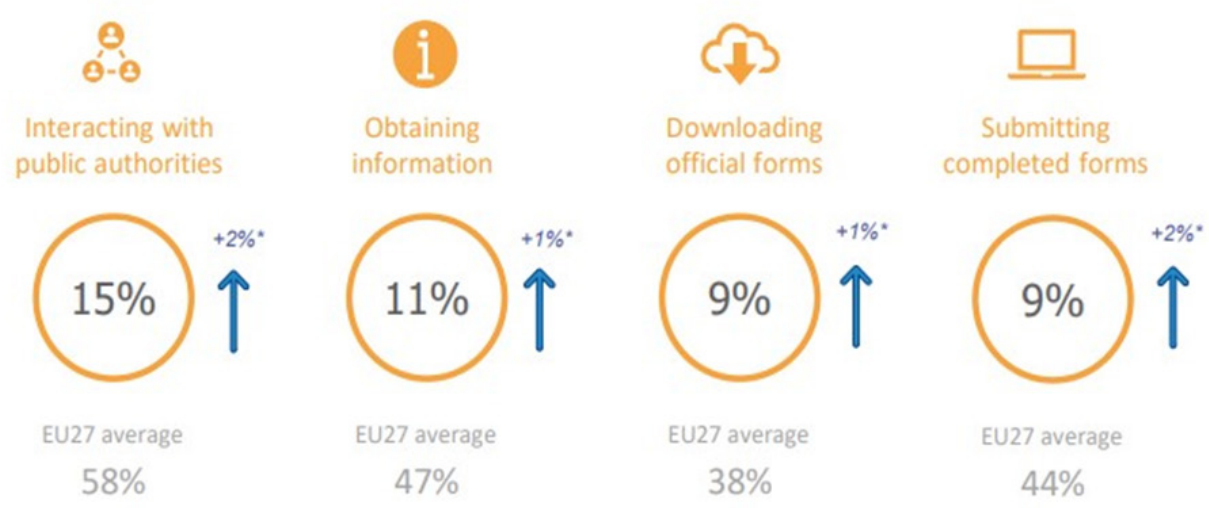

Fig. 5: *Digital Public Administration indicators (% of individuals using the Internet)*
Source: Digital Strategy (2022)

In this regard, the reform for digitization of Romania means the transition to a new paradigm - technological, informational and social.

As the so far steps towards the digital public administration infrastructure development, we can list several milestones, such as:

- main National Portals (eGovernment Portal, Electronic Point of Single Contact - edirect.e-guvernare.ro, Open Data Portal - data.gov.ro);
- main Networks: Local Communities Electronic Networks (LCENs), Trans European Services for Telematics between Administrations (TESTA);
- data exchange tools: The National System of Interoperability (SNI) - will connect the databases of Romania's public administrations;
- e-Procurement and e-Invoicing Platforms - simplify procedures for both suppliers and purchasing agencies.
- e-Payment platform – the National Electronic Payment System for Taxes, with more than 1.2 Mill. users (citizens and businesses) and 1000 public institutions.
- One-Stop-Shop (OSS) system (2021): is a Cross-border platform, which allows businesses to benefit from e-Services for VAT registration and reporting across EU Member States.

Moreover, among the most relevant projects in the implementation/ completion phase, we can name:

- Information system for health registers - RegIntermed;
- The Centralized Software Platform for Digital Identification - PSCID, which aims to establish the National Electronic Register of Electronic Identities of all consumers of electronic eGovernment services and interconnect with the unified and secure access portal to electronic eGovernment services and enroll citizens in the desired services;
- e-ID and TrustServices - The project for the realization of the technological interoperability system with the EU member states – SITUE, which aims to make the eIDAS node operational for Romania and its interconnection with the

eIDAS nodes of the other member states and with the providers of identity and electronic services in Romania;
- Creating the strategic framework for the adoption and use of innovative technologies in public administration 2021 – 2027;
- Integrated Information System for the Issuance of Civil Status Acts - SIIEASC (the objectives include reducing the time required to process civil status information transactions and the costs of storing information for local and central administrations for services related to life events such as: birth, marriage, divorce, death).

In order to effectively start embracing digital government, governments had to start guarantee certain staged rights in online communication with citizens (such as: personal data protection, cybersecurity, digital signature), upgrading those rights as emerging technologies evolve, as shown in Figure 6 (the so-called 2nd or 3rd generation rights, e.g.: digital identity, one-stop-shop, open data, AI information and opt-out).

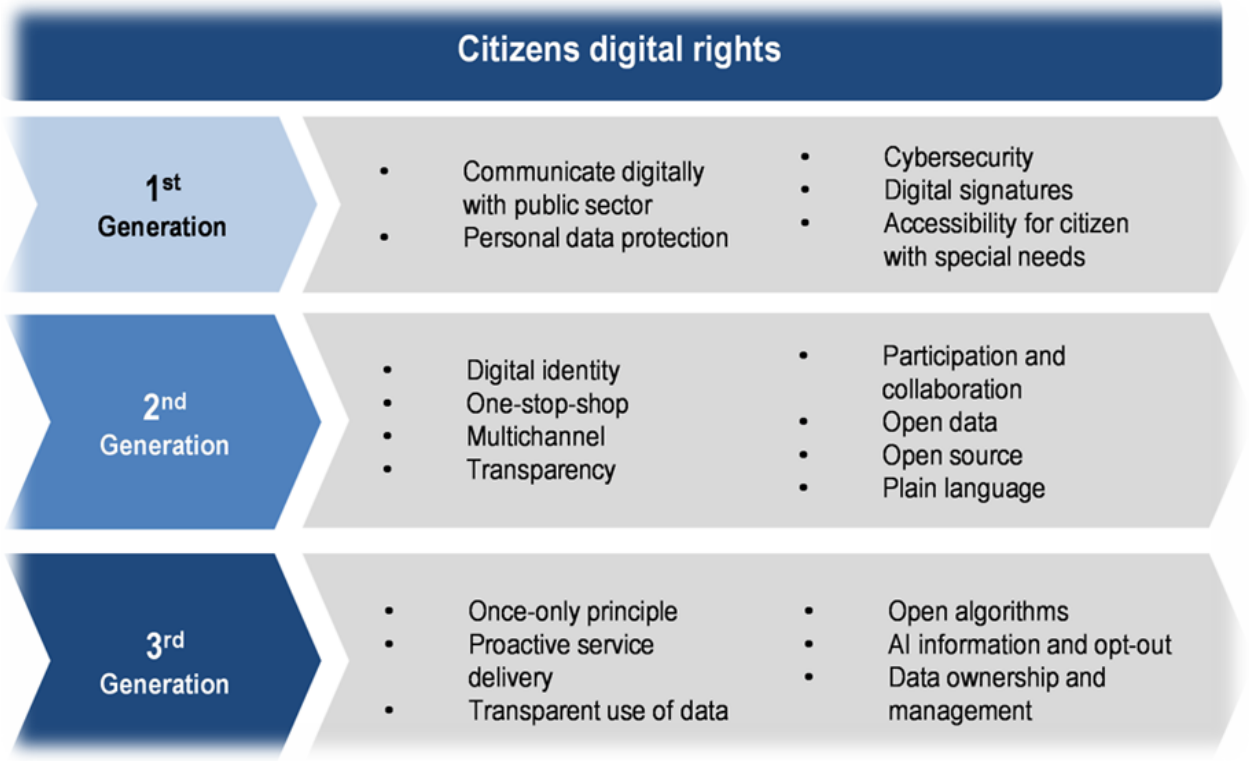

Fig. 6: *Digital rights – Towards a citizen-driven Digital Transformation*
Source: (OECD, 2019)

Thus, from what has been mentioned above it becomes obvious that one's Digital Identity is managed using European Digital Identity Wallets (EU-DIW). And this is how it works (see Figure 7): The user is provided with confidential-based credentials by the empowered authority. When the user presents its credentials, the DIW generates a unique identifier and signs it using a private key, secured by a biometric proof or a pin known only by the user, which connects to a uniquely paired public key, which grants access to certain products/services, just like the user would present a physical ID or a member card.

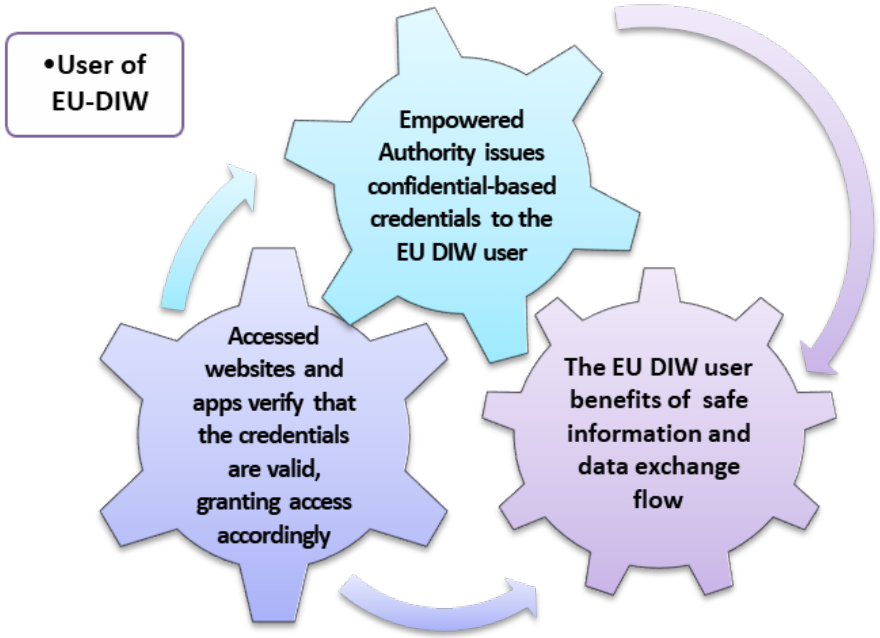

Fig. 7: *EU Digital Identity Wallet – Functioning*
Source: adapted by authors

Additionally, due to the PKI technology, users can use their mobile ID to sign documents with just a few clicks. So, the main gain of verifiable credentials is that the user can easily access and control its shared data and unlock a more trustworthy internet.

One recent example of the usefulness of instant access to e-health documents directly from the personal mobile phone is the case of the Covid-19 Green Certificate. So, mobile e-Wallets will contribute to saving personal medical records, thus relieving the citizens of the inconvenience of physically carrying the documents.

CHALLENGES TO THE CROSS-BORDER USE OF NATIONAL E-IDS

Among the challenges of cross-border use of national e-IDs, we identified: coverage, acceptance, usage, user friendliness. So, according to the available data, at EU level, less than 1/4 of the most important public service providers enable users to establish their identity online, without using a password via the use of an e-Identity system, with some improvements shown in the recent 2 years in the context of the Covid-19 pandemic. Therefore, the success rate of cross-border authentication is rather low, since only 60% of the EU citizens from 14 Member States are able to use their national e-ID in another Member State, as there is no obligation to notify e-ID schemes under the eIDAS Regulation. Moreover, in recent years, only up to 30000 successful cross-border authentications/ year were registered compared to hundred thousand or even millions at internal level.

Taking this into consideration, the COM is quite determined to ensure the success of the future EU DIW, therefore it is willing to allocate €74m Euros to at least 4 pilot projects (tackling use cases of driver license, diploma, payment authentication, eHealth, digital travel credentials and social security), as part of the Digital Europe Programme (DIGITAL), to identify the infrastructure needs for the implementation of a digital wallet at the EU level. However, we ask ourselves if this determination also guarantees the success of this brave project. The answer is uncertain. In any case, we have identified certain potential risks, which we will present in the following.

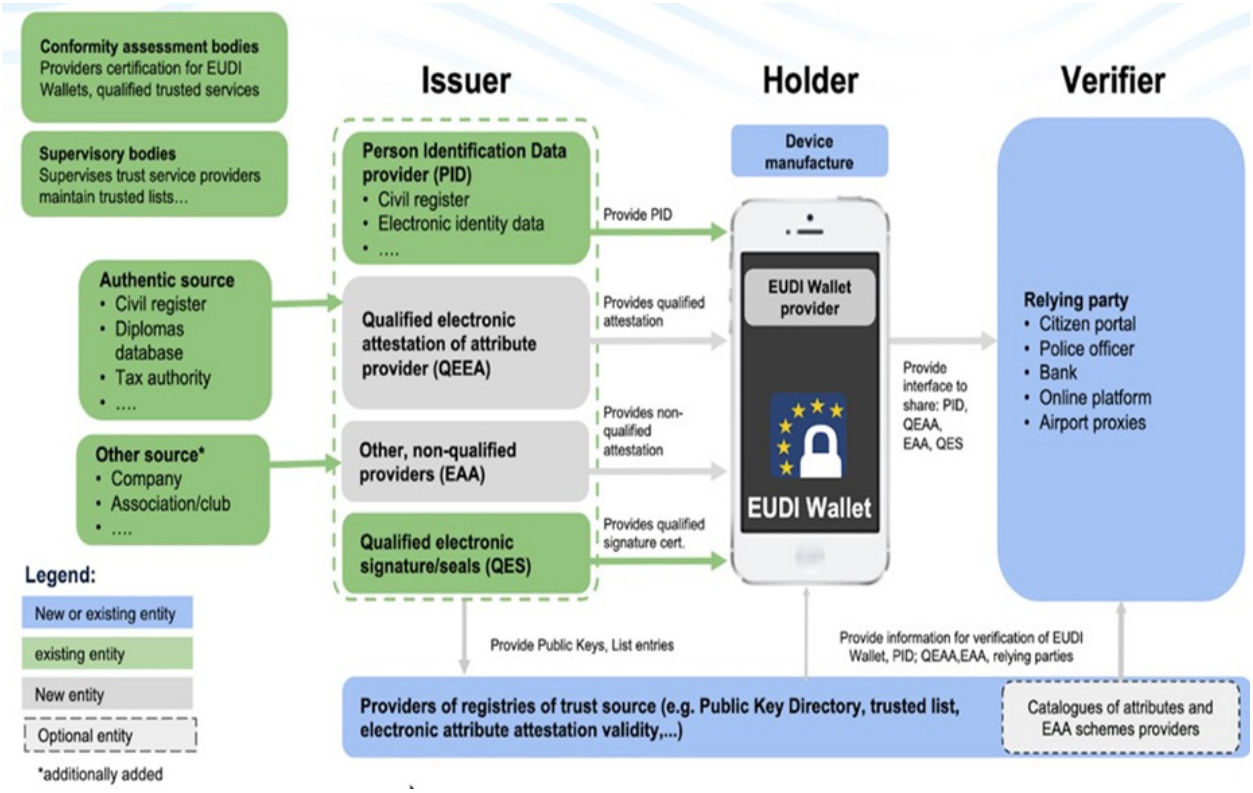

Fig. 8: *Roles interacting with the EU-DIW (mapped into SSI architecture)*
Source: Lissi (2022)

Regarding the timeline envisaged by the COM until issuing of the EU DIW, it is obvious that there is a certain acceleration in the evolution of things, for reasons related to the Covid-19 pandemic, but also in the context of the ongoing digital revolution. Thus, by October 2022, the eIDAS 2.0. Toolbox should be published and the technical architecture finalized. Furthermore, in the Q1 2023, the eIDAS 2.0. should have been adopted, so that starting Q1 2024, Member States would be able to implement it and already issue the EU DIWs.

MAIN BENEFITS OF USING EU DIGITAL IDENTITY WALLETS

With the help of the EU DIW, which will be recognized across borders, throughout Europe, EU citizens and companies will be able to prove their identity, sign and share electronic documents, access online services, with just one click on the button of their phone. Moreover, governments and organizations would also see EU DIW as a tool to identify users' online and offline activities.

As the Regulation itself provides "Wallets can also serve the institutional needs of public administrations, international organizations and the Union's institutions, bodies, offices and agencies", meaning that interaction between citizens/companies and relevant entities (public administration, health sector) is done exclusively in a virtual way, controlled and secured, whereas the danger of bribery and corruption no longer exists. Moreover, from a logistical and financial point of view, digital identity brings a high-level of return on investment to the government, since the EU DIW translates into reduced administrative costs and expenses associated with simplified, more efficient and time saving public services provided by the public administration.

THE FUTURE EU DIGITAL IDENTITY WALLET – A SECURE AND TRUSTABLE TOOL?

The future wallet is intended to store various identity and travel documents, driving licenses, educational and professional diplomas, tax records, health records, bank accounts etc., all in digital format. Even though the future EU DIW comes as an answer to many snags and moreover will also comprise one's whole identity in a digital solution, which simplifies citizens and businesses life, it is also linked to privacy and security-related issues that one must address.

As for the ethical aspect regarding the access, use and reuse of one's personal data, Belgium, Estonia, Netherlands and Spain, for instance, allow citizens to be informed that their data are used by public authorities through different online platforms. This example should be treated as matter of good practice.

Since the EU-DIW shall contain a lot of personal data, it is highly important for the potential users – either citizens or businesses – to perceive it as secure, in order to be trusted, accepted and effectively used for all its purposes. This is the attribute of the European commission and of the bodies that support it in its efforts to operationalize the EU e-ID, as well as of the national authorities to instill confidence in European citizens for this bold project.

Fig. 9: *The history and future of Identification and Authentication*
Source: Lissi (2022)

As for the ethical aspect regarding the access, use and reuse of one's personal data, Belgium, Estonia, Netherlands and Spain, for instance, allow citizens to be informed that their data are used by public authorities through different online platforms. This example should be treated as matter of good practice.

Since the EU-DIW shall contain a lot of personal data, it is highly important for the potential users – either citizens or businesses – to perceive it as secure, in order to be trusted, accepted and effectively used for all its purposes. This is the attribute of the European commission and of the bodies that support it in its efforts

to operationalize the EU e-ID, as well as of the national authorities to instill confidence in European citizens for this bold project.

So, why should we worry, since one of the main benefits of the wallet, highlighted by the European Commission, is the full control of the data the user is using and sharing? Moreover, since the wallets are:

- *issued exclusively by competent, authorized authorities (under a notified scheme);*
- *developed according to European harmonized standards (e.g.: in line with Regulation (EU) 2016/679) and common technical framework, certification and conformity assessment;*
- *based on two key concepts: improved identification and authentication (see Figure 9)), which should obviously protect the user from any possible cyber-attacks;*
- *signed by means of qualified electronic signatures,*

then why is the security-related concern still high on public debates?

Cybersecurity is, in essence, the cornerstone of digital transformation, an aspect with intrinsic values on several levels of activity. Paradoxically, the technological evolution is the one raising new security challenges, although it is also the one that most often provides the solutions for these problems. Thus, the frequency and complexity of cyber-attacks increase exponentially with the use of ICT infrastructures and technologies by citizens, businesses, organizations, industries.

In order to support the cyber security measures of the future European national identity framework, under the EU Cyber security Act of 2019, the EU Agency for Cybersecurity was granted extended mandate to explore the area of electronic identification, thus supporting the European Commission by delivering specific security related expertise and recommendations as regards trust services and technical and regulatory requirements.

OUR FINDINGS AND RECOMMENDATIONS

Below we have exposed some of the identified challenges and opportunities of EU-e-ID implementation, as well as the privacy and security associated risks and some solutions to reduce the risk of cyber-attacks on mobile phones and, implicitly, on digital wallets, as it can be seen in Table 1.

Table 1: *Challenges and opportunities of EU-e-ID implementation*

CHALLENGES of EU-DIW	OPPORTUNITIES of EU-DIW
• No interoperability with other e-ID solutions at the moment and potential overlapping problems (Service providers will have to deal with supporting several e-IDs, including the EU DIW)	• One's whole identity in a digital solution, which simplifies citizens' and businesses' life
• Potential incompatibility and overlapping with existing legislation (e.g.: incompatibility with the European Data Protection Regulation (EU) 2016/679 and overlapping of e-IDAS 2.0. with the Single Digital Gateway Regulation, both aiming to solve similar problems but by different approaches)	• Simplified, more efficient and time saving public services provided by the public administration

• The complexity of the e-Wallet (the technology and infrastructure are not yet prepared to implement the EUeID in such a short time – early 2024)	• Reduced administrative costs and expenses
• Not feasible timeframe for the e-Wallet standards to be ready for deployment in early 2024 as proposed, due to the lack of standardization bodies/organizations formally recognized by the European Union: ETSI, CEN and CENELEC in Europe and ISO and ITU, at international level)	• Reducing the risks of corruption close to zero, by cutting the physical interaction civil servant-citizen
• Not properly covering private sector needs	• European e-ID as opportunity for enforcing Digital Services Acts
• Technologic monopolies of the gatekeepers	• Digital identity brings a high-level of return on investment to the government
• Insufficient user demand for the EU-DIW, due to lack of trust	
• Insufficient buy-in for government service provider	

Privacy and security associated RISKS	Potential cyber-security SOLUTIONS
• Higher risks associated with the use of EU DIW by people with low digital literacy/ poor technological knowledge, due to the fact that they need to give their explicit consent while aren't fully aware of what personal data transfers involve.	Imposing strict requirements for data protection and privacy for the issuer of the EU DIW and for qualified providers of attestations of attributes, including compliance with GDPR requirements.
• Since digital identity wallet is dependent on mobile devices/wearables, though convenient for many above mentioned reasons, this can also represent a hazard and the challenge is that the device could run out of battery, or face network connection issues.	A certification of conformity issued by Member States' competent authorities in accordance with the relevant European cybersecurity certification standards would provide a higher level of trust and interoperability
• Higher risk of mobile devices/wearables interception while connect to wireless networks. This increases the risk of cyber-attacks on the wallets, since information (one's personal data) travels across an uncontrolled wireless network.	Integrating secure connections to infrastructure and software based secure storage for passwords and IDs

There are still some open questions and topics for debate, mainly related to the relationships between existing infrastructures, legislation and their interconnectedness, but also in terms of defining the assets needed to be protected in the EU DIW, guaranteeing the conformity of the source of attributes with the European values, ensuring proper coordination with the European Data Protection Regulation (GDPR), NIS2, the Digital Services Act, Digital Markets Act. Taking into the consideration all that has been mentioned above, it becomes more and more obvious that the timeframe planned by the European Commission for the operationalization of the EU e-wallet is not exactly feasible.

REFERENCE LIST

Ailioaie, S., Hera, O., & Kertesz, S. (2001). *Ghidul de e-Democrație și Guvernare Electronică* (Guide made for the Parliament of Romania). ASER Bucharest.

Anghel, M., & Neagoe, A. (2015). Nivelul de Digitalizare al guvernării electronice din România. *Revista Română de Informatică şi Automatică, 25*(4), 19-26.

Cristescu, A. (2005). Dimensiuni practice ale conceptului de e-Guvernare în România şi Japonia. *International Conference - Administrația publică la începutul celui de-al III-lea mileniu. Diseminarea celor mai bune practici japoneze în România*. National University of Political Studies and Public Administration (SNSPA), Bucharest, Romania.

EU Monitor. (2021). *COM (2021)118 – Communication. 2030 Digital Compass: the European way for the Digital Decade*. Retrieved from https://www.eumonitor.eu/9353000/1/j9vvik7m1c3gyxp/vlgzpb7ivmr4

EUR – Lex. (2014). *Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC*. Retrieved from https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv%3AOJ.L_.2014.257.01.0073.01.ENG

EUR – Lex. (2016). *Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data entered into force on 25 May 2018*. Retrieved from https://eur-lex.europa.eu/eli/reg/2016/679/oj

EUR – Lex. (2020). *European Commission, Communication from The Commission to The European Parliament, The Council, The European Economic and Social Committee and The Committee of The Regions Shaping Europe's Digital Future, Brussels, 19.2.2020, COM 2020/ 67 Final.* Retrieved from https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX%3A52020DC0067

EUR – Lex. (2021). *Proposal for a Regulation of the European Parliament and of the Council amending Regulation (EU) No 910/2014 as regards establishing a framework for a European Digital Identity.* Retrieved from https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52021PC0281

European Commission. (2022). *Digital Public Administration factsheet 2022 Romania*. Retrieved from https://joinup.ec.europa.eu/collection/nifo-national-interoperability-framework-observatory/digital-public-administration-factsheets-2022

European Commission. (2022). *Digital Economy and Society Index (DESI) 2022 Romania*. Retrieved from https://digital-strategy.ec.europa.eu/en/library/digital-economy-and-society-index-desi-2022

European Commission. (2019). *E-Government factsheets. Anniversary report.* Retrieved from https://joinup.ec.europa.eu/sites/default/files/custom-page/attachment/2019-03/10egov_anniv_report.pdf

European Council. (2020). *EUCO 13/20, Special meeting of the European Council (1 and 2 October 2020) – Conclusions*. Retrieved from https://www.consilium.europa.eu/en/press/press-releases/2020/10/02/european-council-conclusions-1-2-october-2020/

Lissi. (2022). *e-IDAS and the European Digital Identity Wallet: Context, status quo and why it will change the world.* Retrieved from https://lissi-id.medium.com/eidas-and-the-european-digital-identity-wallet-context-status-quo-and-why-it-will-change-the-2a7527f863b3

The Organization for Economic Co-operation and Development (OECD). (2019). *Digital Government Review of Panama: Enhancing the Digital Transformation of the Public Sector*. Retrieved from https://www.oecd-ilibrary.org/sites/5edbea0b-en/index.html?itemId=/content/component/5edbea0b-en

Nixon, G. P., & Koutrakou, N. V. (Eds.). (2007). *E-Government in Europe. Re-booting the state.* Routlage.

Petcu, I., Barbu, D. C., Anghel, M., Golea, G. D., & Radu, A. (2020). Shaping the future: between opportunities and challenges of the ongoing 4th and forthcoming 5th industrial revolution. *16th International Scientific Conference eLSE 2020, 3*, 91-97.

Radu, A. F., & Petcu, I. (2021). Intrinsic aspects of e-Government consolidation across the European Union. Case study: Romania. *Romanian Journal of Information Technology and Automatic Control, 31*(4), 83-96.

United Nations Department of Economic and Social Affairs. (2020). *United Nations E-Government Survey (2020).* Retrieved from https://publicadministration.un.org/egovkb/en-us/Reports/UN-E-Government-Survey-2020