Future Outlook and Research Ideas

Thomas J. Lampoltshammer, Herbert Leitold, Carsten Schmidt, and Thomas Zefferer

Abstract This chapter uses the lessons learned from technical work and piloting of the mGov4EU project, as well as experience made so far in developing the Single Digital Gateway (SDG) Once-Only Technical System (OOTS) and the European Digital Identity Wallet (EUDIW). These are our basis, and we dare to look into the future. The two European flagship policy initiatives OOTS and EUDIW are meant to facilitate citizens' journey through European public services but also are meant as tools to navigate private services in the Digital Single Market. It, however, would be naïve to assume that setting such complex systems into production is the end of an endeavour. We might only learn through first experience where pitfalls lie but in particular what opportunities are given that haven't been seen before. We, therefore, give authors' views on where this road might lead us and what research might be essential to get there. The chapter, thus, aims at anticipating what might be needed to reap the benefits of OOTS and EUDIW in a mobile world from a governance perspective, a privacy and data protection perspective, a services perspective and a mobile technologies perspective. Therefore, each section first sets the scene by outlining the status. This is followed by addressing some challenges and gives an outlook by indicating how research might address these challenges.

T. J. Lampoltshammer
University for Continuing Education Krems, Krems an der Donau, Austria
e-mail: thomas.lampoltshammer@donau-uni.ac.at

H. Leitold (✉)
Secure Information Technology Center - Austria A-SIT, Graz, Austria
e-mail: Herbert.Leitold@a-sit.at

C. Schmidt
University of Tartu, Tartu, Estonia
e-mail: carsten.schmidt@ut.ee

T. Zefferer
A-SIT Plus GmbH, Wien, Austria
e-mail: thomas.zefferer@a-sit.at

V. Homburg et al. (eds.), *From Electronic to Mobile Government*,
https://doi.org/10.1007/978-3-031-64471-9_12

Keywords eIDAS · SDG · EUDI Wallet · OOTS · AI · Blockchain · Once-Only

1 The Basis: eIDAS, SDG and Synergies Between These

The two EU Regulations SDG [1] and eIDAS [2], the ongoing eIDAS revision [3], respectively, address citizen and business needs in the Digital Single Market with a particular focus on cross-border services. SDG and electronic identity provisions of the original eIDAS Regulations are primarily directed to the public sector. This is due to Member State (MS) obligations to integrate in their services. The eIDAS revision enhances such mandatory support to the private sector, in particular for the European Digital Identity (EUDI) framework—commonly referred to as the EUDI Wallet or EUDIW [4]—in case such private sector services legally or contractually require strong authentication.

The SDG OOTS [5] and the EUDI Wallet have in common that the provision of citizen or business data shall be facilitated. Such citizen or business data are referred to as evidence in SDG and as electronic attestations of attributes (EAA) or qualified electronic attestations of attributes (QEAA) in eIDAS, respectively. For simplicity, we refer to both evidence and EAA as "attributes". While the common goal of providing attributes is shared by both regulations, its implementation follows quite different paradigms: OOTS aims to relieve a citizen or business from providing needed attributes whatsoever, as with OOTS, a system is established where (public) service providers can, based on citizen consent, request attributes (i.e. evidence in SDG-terminology) from the competent authority that is authoritative for such data, usually some form of register. The eIDAS Revision, however, puts the citizen or business into the centre of data provision, as the EUDI Wallet is meant to be a mobile tool that can hold and provide attributes (EAA or QEAA in eIDAS terminology), and thus, the citizen is somehow a carrier of her data and in control of it.

These two paradigms are conceptually different: With OOTS, evidence is requested at the very moment it is needed by a service. Provided the citizen consents to do so, the evidence requester needs to learn which competent authority is holding and is authoritative for such attributes. This needs quite some core platform services like directories or semantic mappings of different evidence MS hold to a service's information needs and requires common protocols and interfaces—this is what OOTS essentially is about and what has been enshrined in an Implementing Act [5] and accompanying technical specifications. The OOTS infrastructure comes with relieving the citizen or businesses from taking care of who can provide which information about them but is currently limited to public sector services and public sector attribute providers. With the EUDI Wallet, on the other hand, the service requests information it requires directly from the citizen or business as EAA or QEAA through the Wallet. Thus, less core services are involved in the very moment when the citizen or business wants to get service but comes with the need to anticipate what the actual information demand of this service is and has to get these

attributes as EAA or QEAA with the EUDI Wallet in advance. Note, that therefore some MS aim to provide EAA also synchronously by the EUDI Wallet, retrieving attributes from authentic sources only when required. However, for the general case of an EUDI Wallet storing data asynchronously in advance, one could argue that the EUDI Wallet is better suited for attributes that are frequently needed and that are not too dynamic, as outdated information is of little use when asynchronously stored ahead. Address and age being somehow atomic attributes are simple examples, but the Wallet is also meant to hold complex EAA like a mobile driving licence. OOTS seems superior, in particular with complex processes where citizens may not know what the service's actual information need is, where information needs are not static but dependent on context or simply where citizens do not want to manage their data on their own. Examples of SDG evidence would be register excerpts like a professional qualification certificate. These are, however, just examples where OOTS and the Wallet might be seen serving different situations and needs, and a clear-cut borderline is not given—to the contrary, OOTS and the EUDI Wallet may both serve a particular service on the same information need; hence, the objectives are similar despite conceptual differences.

Taking such conceptional differences aside, there are dependencies between SDG and eIDAS, as well as obvious similarities. On the one hand, service access via OOTS requires authentication, which eIDAS provides. On the other hand, for providing EAA to the EUDI Wallet, some common interfaces for retrieving data are needed, which OOTS is developing. Further synergies exist, and in an attempt to exploit these, the European Commission has established an OOTS-EUDI Contact Group of MS experts so that investments in OOTS and EUDI can cross-fertilise and lead to even better user experience.

Being directed to public services a communality is that mobile government (mGovernment) is still in its infancy. Governments have of course not overlooked the trend of using mobile phones and, in particular, smartphones to access the Internet and services. Those MS that already have a mobile first strategy are ahead and provide various mGovernment apps. Still, eGovernment services are long-term investments and procedural rules that have grown from traditional ways of interacting with government-defined service needs. Mobile services, however, often follow different paradigms like being transaction-based rather than conventional session-based services with browsers. A main difference is of course the devices' form factor, where filling forms or attaching documents in many conventional eGovernment processes give questionable user experience. This is where both OOTS and EUDIW can make a difference in no longer bothering users with filling data, provided that services make intensive use of it aiming at a user experience as convenient as the many commercial apps have that we all use daily, where ordering goods or booking travels is at one's fingertip.

The remainder of this chapter addresses exactly these challenges, namely, how synergies between the SDG OOTS and the eIDAS EUDIW can be best exploited and how these basic infrastructures are best to prepare for seamless mobile user experience. The focus is on giving an outlook and identifying research challenges that are to be addressed to make that happen. We therefore structure this chapter

into sections viewing current challenges from a governance angle, a privacy and data protection perspective, a services view and from mobile technology constraints. Each of these sections first sketches the current state in relation to SDG and eIDAS, then highlights challenges or potential pain points and finally elaborates on research questions that might be worthwhile solving to overcome these. The chapter takes the findings of the mGov4EU project into account, complemented by the authors' own experiences and views. Such personal views in excess of common project findings are justified, taking into account that research by its heart is a creative process where excellent results can be driven by a consensual view on a challenge but often even more by individual ideas.

2 Governance Outlook

At the time of writing this chapter, the legislative process on the eIDAS revision has not yet been completed, as well as the launch of OOTS in December 2023 being close ahead. Still, the political agreement reached in the trilogue and the status of the EUDIW toolbox process [4] gives a first glance of what lies ahead for eIDAS. Moreover, the public OOTS launch in December 2023 was a few days ahead when these lines where written, so practical experience with SDG was limited to a few Connectathon events where the European Commission and Member States got together for interoperability events and did their first practical tests with the OOTS components.

With the legal basis of the SDG Regulation [1], the existing eIDAS Regulation [2] and its revision [3], the top-level governance structure is defined. An SDG Coordination Group governs OOTS, and a similar role is taken by the eIDAS Coordination Network and its successor, European Digital Identity Cooperation Group (EDICG), under the eIDAS revision, respectively. In these governance groups, the European Commission works together with Member States to shape OOTS and the EUDI Wallet, respectively. This includes preparing the comitology of the Implementing Acts as secondary legislation.

With SDG primarily directed to the public sector— it binds public services in requesting evidence from public sector competent authorities cross-border—the public sector-led SDG Cooperation Group seems suitable in governing OOTS. At first sight, the same holds for EDICG in relation to the EUDI Wallet, as obligations are directed to Member States like to issue a Wallet, to provide person identification data (PID) and to provide interfaces to competent authorities so EAA and QEAA can get issued to the EUDI Wallet. Thus, the public sector-led EDICG is a suitable vehicle to represent public sector interest.

However, when taking a closer look at the eIDAS revision, the stakeholder landscape is much broader. Private sector services have a right to integrate with the EUDI Wallet. Some sectors even have an obligation to do so. The latter include sectors as important as banking and financial services, telecommunications, health or social security, as well as gatekeepers under the Digital Markets Act

(DMA) [6]. In September 2023, the European Commission announced the six big companies as first gatekeepers under DMA: Alphabet (Google), Amazon, Apple, ByteDance (TikTok), Meta (Facebook) and Microsoft. Aside from these sectors and organisations that will act as relying parties making use of the Wallet, further stakeholders exist like qualified trust service providers (QTSP) that will offer citizens provision of QEAA, the software industry that might want to provide integration components for the EUDI Wallet or develop Wallets on their own, qualified consumer protection organisations or privacy advocates.

It is not realistic and would be naïve to assume that EDICG, which likely will be recruited from Member State electronic identity and trust services experts, can alone cover requirements of such a diverse stakeholder grouping or can represent their interest. Drivers, barriers and opportunities of policy initiatives are to be considered for cross-border governance [7].

We argue that stakeholder engagement needs to be broadened to best reap the benefits of OOTS and EUDI Wallet and the synergies between them. Policy-led initiatives like the EUDI-OOTS Contact Group are a good first step but at most scratch the surface on what these infrastructures can deliver. Public consultation on the outcomes should be a step to get the various interests heard but shall be further intensified by community building to have stakeholders engage themselves.

3 Privacy and Data Protection Outlook

OOTS and the EUDI Wallet process personal data in order to facilitate citizens' service needs and, thus, with the purpose to serve citizens. Still, trust needs to be earned so that citizens feel that their data stays protected and does not get misused. Both eIDAS and SDG have data protection at their core. The implementation of the SDGR is set to streamline and simplify the provision of cross-border digital services within the European Union. This regulation aims to create a unified digital environment, making it easier for citizens and businesses to access and utilise public services across borders. Mobile solutions will play a crucial role in realising the objectives of the SDGR, enabling users to seamlessly interact with government services through their smartphones. The harmonisation of digital processes under the SDGR will reduce bureaucratic barriers, enhancing the efficiency of cross-border transactions and fostering a more interconnected European digital landscape. A complementing key aspect shaping the future landscape of cross-border mGovernment services is the emphasis on data privacy and security, with the General Data Protection Regulation (GDPR) [8] playing a pivotal role. Member State governments are obliged to ensure that cross-border services adhere to stringent data protection standards, safeguarding the personal information of individuals. The GDPR acts as a cornerstone, fostering trust among users and encouraging the adoption of mGovernment services by addressing concerns related to privacy and data security.

The main measures taken by OOTS are that citizen consent is required before a service can issue an evidence request and data preview must be seen by the citizen before such evidence actually gets delivered. The EUDI Wallet has a couple of privacy measures as well. First and upfront, users have to consent to the release of their attributes and, through selective disclosure provisions, can de-select data they do not want to release. This is complemented with the fact that relying parties need to register and declare their information needs. Moreover, the EUDI Wallet shall provide unobservability of the user so citizens cannot be tracked.

While these measures provide basic privacy protection, there are a number of challenges that ask for future research. Firstly, the class of services the Wallet is meant for requires unique identification. This, for instance, holds true for public services or for banking services under "know your customer" (KYC) and anti-money laundering rules. Unique identification shall be supported by eIDAS provisions on identity matching where Member States shall assist in matching to user accounts. However, the provision for unique and persistent person identifiers that the original European Commission proposal [3] and the Council's general approach have foreseen for this class of services has been turned down in the trilogue—the interinstitutional negotiations of the co-legislators Parliament, Commission and Council. While the lack of persistent identifiers can be seen as privacy enhancing, when in combination with the identity matching requirement it essentially means that the latter may need a bigger set of attributes than when supported by unique identifiers. Further research may be needed on how identity matching can best be implemented under data minimisation principles.

A further source of future research related to the EUDI Wallet relates to the use of pseudonyms versus their recovery. The eIDAS revision foresees pseudonymous identifiers as a privacy measure, and one approach commonly followed is to have these pseudonyms device-bound and device-generated, i.e. to have the Wallet create pseudonyms. A user requirement, however, will be that these pseudonyms can get recovered, if the Wallet device that created it gets lost or is defunct. This allows for the user to continue to use accounts that these pseudonyms are linked to, like a social media service. The Wallet foresees backup functions for user data, which can also be seen as questionable. On the one hand, it renders the user in charge to manage their data, which creates efforts or at least needs awareness that such data management is needed. On the other hand, smartphones use hardware-backed secure elements to protect sensitive data. This gives challenges when pseudonyms shall get protected at this level, as they can no longer easily get backed up. Research may be needed on how to best assist citizens in managing their Wallet data like their pseudonyms.

Finally, further work is suggested on how the stringent privacy measures of both OOTS and the EUDI Wallet, such as user consent and selective disclosure, match with usability goals. Authentication and attribute provision as provided by eIDAS and SDG are no goal in themselves but are needed to fulfil the service the citizen is seeking for. Each additional step may be seen as a hurdle in getting these services. This asks for research on how to best align privacy measures with usability.

4 Electronic Services Outlook

Citizens and businesses expect a seamless integration experience when using OOTS and their EUDI Wallet when requesting a service. Public services are, however, still document-based in asking particular evidence like a birth certificate. SDG OOTS does the first step to dematerialise a service's information need from a particular document, in mapping a certain information need to various evidence attributes. To give a simple example, age could either be proven by a birth certificate as well as by a proof of citizenship as OOTS evidence but also by the minimum data set of an eIDAS authentication or an age claim of the EUDI Wallet. Using OOTS and the Wallet seamlessly to provide attributes is also one of the synergies identified by the OOTS-EUDI Contact Group.

Taxonomies of public service requirements could, however, go far further in describing the actual information need rather than evidence or documents. To achieve this, it would need further research on how typically rule-based public services that are tailored to information available in the same state can best handle other states' data. The Wallet poses a particular challenge in that context, as EAA and QEAA need to be provided in advance, unless synchronously retrieved from authentic sources.

We also envision that the sole availability of OOTS and the EUDI Wallet will influence future service design. The current limitation of OOTS to public services and competent authorities does not mean that its concepts cannot be transformed to or be taken up by other sectors. Consider, for instance, a short weekend vacation where the air carrier asks the user for identity card data in its booking app, as the travel will be outside the Schengen area. The car rental app needs driving license data and information about the insurance policy that the user claims providing additional waivers. Finally, the hotel advance room check-in asks for the client's home address and—again—identity card data. These are just some data that may be requested already before the vacation starts. Users currently may employ browser form filler extensions to get these tasks facilitated. This has the downside that the user needs to trust the browser vendor in storing their personal data, as sensitive as the home address. Imagine how the same use case can be carried out when using the home address and identity card data held and safeguarded by the user's EUDI Wallet and where data from the insurance company can be provided by services similar to what OOTS does. Such an approach, however, would need research on how OOTS could get transposed to private sector services in a trustworthy way so that private data providers do not learn user traits. Combine these with advanced cryptographic methods like zero knowledge proofs and the various actors like in our simple example of an air carrier, a car rental company and a hotel can get information they need in a privacy-enhanced manner and without the user having to fetch the data or to entrust other services on managing these.

Public services can be complex and may involve various authorities. With the advent of the EUDI Wallet promising authentication that is supposed to work cross border and with introducing identity matching to serve all public services,

research on service redesign is advisable so that citizens' life situations can get better addressed without having them to approach various authorities. The concept of a single point of contact (SPOC) in cross-border public services where a SPOC is meant as a hub orchestrating the process with several authorities was introduced as early as 2006 with the EU Services Directive [9]. With unique high-quality authentication the EUDI Wallet provides, it can be used further beyond businesses that provide services. An example for citizens is the Digital Babypoint that has been introduced as a mobile service in Austria: making massive use of once-only principles and of public registers, the various administrative procedures after birth, such as registering at the parent's home and getting official documents delivered, can be done in one step. The unique identification of a parent in an eGovernment app and the civil status register proving custodianship serve as key to trigger the processes at the various authorities. Several such examples exist nationally, where the public register ecosystem and administrative culture is homogeneous. It however soon grows complex cross border. Research is advisable how life situations involving many competent authorities and different processes can be orchestrated in a service design that works across the EU and get best facilitated by OOTS.

5 Mobile Technologies Outlook

A shift to mobile devices and services is clearly seen but already showing a trend of being "conservative" in the sense of assuming a tablet or smartphone as the primary user device. Personal computing environments are increasingly amended by wearables with less user interaction capabilities but more sensors, as well as edge and cloud services, smart vehicles, etc. with unprecedented computing capabilities. Thus, complementing traditional service offerings by a user's life situation in a privacy-friendly manner can benefit the user with personalised service offerings, as long as their control and privacy are well protected.

Delivering public services electronically has, however, grown from traditional procedural laws and often started from simply transforming these to an electronic replica of the very same process, i.e. have the user fill an application form, enclose the documents needed to prove claims and have the application signed. Carrying out such a process on the smartphone already gives challenges, where just using responsive design alone to match the form factor does not do the job: filling out large forms on a mobile phone, while possible, is cumbersome, and we hardly ever carry electronic copies of official documents like birth certificates with us on the mobile device. That is where the EUDI Wallet and OOTS come into play and can benefit mobile service design: data usually collected through forms and accompanying evidence can be provided as QEAA through the Wallet, which at the same time are already an authentic representation of facts, and making use of OOTS allows one to not bother the user about collecting documents at all. OOTS is meant to have the service take care of this, and based on the consent given by the user, the service can take care of collecting the information needed from the various

competent authorities. Thus, constraints given to mobile devices ask for a service design that makes massive use of information provisioning through OOTS and the Wallet.

Also when using OOTS with mobile devices, they can suffer constraints. OOTS foresees the preview of evidence before these are being delivered. Preview seems easy with simple documents or atomic attributes. For complex documents, however, the display form factor can be a challenge. Research is advisable on how information provided by SDG evidence providers can be transformed from paper-inspired documents to a structured representation where rather the actual facts, which the evidence requester needs, gets asserted, not a lengthy document. For example, services granting building permits may only need to know that the applicant is a master builder and prefer that as structured information over a full diploma with nice visual seals.

The EUDI Wallet, while meant to be in production in only a few years—indicatively end of 2026 to early 2027—will require extensive research. A pain point is that the high information security and data protection requirements would ask for support by hardware security elements to operate the Wallet self-contained on the mobile device. Such hardware elements exist on modern smartphones with secure enclaves or trusted execution environments (TEE), but requirements of the Wallet may well exceed their standard functions, like their needed resistance against attacks or the strength of function or the support of novel cryptographic primitives. Mobile devices and their operating systems, however, rarely originate from within the EU, and it remains to be seen how the market will support such needs. Even if the eIDAS Revision will ask gatekeepers under the Digital Market Act [6] to grant Wallet issuers access to the operating system, hardware or software features, some of the desired features may simply not exist on some devices. Think, for instance, of a Wallet issuer that plans to implement zero-knowledge proofs for advanced privacy features and would hope for hardware support of cryptographic primitives for better protection of the processing. Research may be needed how to make the EUDI Wallet broadly available based on technology provided on the market—and some variants are already enshrined in recitals of the eIDAS Revision like making use of external secure elements or remote hardware security modules (HSM)—and gradually advanced as more advanced technology appears.

The EUDI Wallet is mainly thought from technology available and broadly used today, i.e. smartphones. This is pretty limiting for two main reasons:

1. On one hand, services for citizens need to be inclusive and accessible. It should also serve citizens who do not want to or cannot use a smartphone—for whatever the reason may be. Think, for instance, of persons with special needs like visually impaired or persons who need financial aid and cannot afford an expensive phone to file for such subsidy.
2. On the other hand, technology evolves quickly, and we may not yet know the devices we will have in only 5 years, which is when the EUDI Wallet will be set into production. Consider how fast traditional PCs were complemented by tablet computers with different physical interfaces and introducing apps as

a paradigm different to office software, not to mention the smartphone wave and cloud computing. This asks for research on how to complement smartphone Wallets already now so we are ready for such technological progress.

Finally, the EUDI Wallet—while pretty innovative—still can be seen as just an evolution of electronic identity to be used with services as we know them now. With the user holding an electronic identity device that has various other sensors and is already connected to other computing components either in the cloud or in close proximity, we can think further. The very same physical device that holds the Wallet is playing music via the car's entertainment systems and knows my exact location and even the route I will be using through the navigation app. Why should my surrounding full of various computing not mesh and the smart car suggest to me the best road-toll package when approaching the first toll station in another country so I can use the fast lane? The car registration certificate stored as QEAA in my Wallet anyhow can fill the application; OOTS might need to deliver the license number and maximum weight of the boat trailer, and that needs an extra toll; and finally, the payment can be made through the upcoming Digital Euro that I authorise through the EUDI Wallet. It seems obvious that such a scenario needs loads of research and engineering to fill the gaps before such a scenario can become a reality in a secure, privacy-friendly, usable and, in a particularly not distracting way, hands-free via voice biometry while one drives safely. But that is what this chapter was about, to identify future research to advance OOTS and EUDIW. Such research may also well be challenging.

A paradigm shift towards efficiency, security and user-centricity marks the future outlook of cross-border mGovernment services. This is fuelled by innovative approaches such as the OOTS and the EUDIW, in conjunction with disruptive technologies like blockchain and artificial intelligence (AI). OOTS represents a key enabler for the seamless provision of cross-border government e-services. This principle ensures that citizens only need to provide their information once to the government, and this information is then securely shared across various public administrations. OOTS streamlines bureaucratic processes, reduces data redundancy and enhances the overall user experience for citizens and companies engaging in cross-border services. Implementing OOTS in mobile applications can significantly reduce administrative burdens, allowing citizens to access government services effortlessly, regardless of their location.

The EUDIW is another pivotal element shaping the future of cross-border government services. EUDIW aims to provide citizens with a secure and interoperable digital identity that can be used across EU Member States. This digital identity wallet ensures reliable means of authentication, enabling them to access government services seamlessly. The integration of EUDIW with mobile applications enhances the convenience of cross-border transactions, offering citizens a unified and secure platform for interacting with various government agencies. Complementing these advancements, disruptive technologies like blockchain and AI play crucial roles in fortifying the future of mobile cross-border government services.

With its decentralised and tamper-resistant nature, blockchain technology ensures the integrity of cross-border transactions. Implementing blockchain in mobile applications can enhance the security and transparency of data exchange, providing a robust foundation for cross-border collaboration. Additionally, blockchain can facilitate smart contracts, automating and executing predefined conditions in a trustful manner and further streamlining cross-border processes.

AI contributes to the evolution of cross-border government services by enabling advanced data analytics, natural language processing and automation. AI-powered chatbots can enhance user interactions, providing users with instant assistance in multiple languages. Machine learning algorithms can analyse vast datasets to identify trends, supporting decision-making processes for government agencies involved in cross-border initiatives. The combination of AI and mobile cross-border services creates a dynamic and responsive ecosystem that adapts to citizens', companies', and governments' diverse needs.

6 Conclusions

The Single Digital Gateway Regulation (SDG) that defines the Once-Only Technical System (OOTS) and the revision of the eIDAS Regulation introducing the European Digital Identity Wallet (EUDI Wallet) are European flagship policy initiatives that address the Digital Single Market, and both aim to facilitate providing information that citizens and businesses need to deliver when accessing public sector or private services. The paradigms are different. The EUDI Wallet can be seen as an identification means and as an information storage under the user's control, while OOTS frees the user from the hassle of collecting such information whatsoever. Still, the overall purpose is argued targeting similar goals.

The European Commission-funded mGov4EU project was meant to get these concepts together in making SDG and eIDAS fit for the mobile computing environment we meanwhile live in. It complements policy initiatives like the OOTS-EUDI Contact Group that addresses synergies in a dialogue between the European Commission and Member State experts. mGov4EU was meant to carry out research on how to best implement such synergies. Such research and the successful completion of the project, through proofing its concepts in its three pilots i-voting, smart mobility and e-signatures, are, however, not to be seen as the end of a journey but rather an opening to even further research questions.

We gave an outlook on what SDG and the eIDAS Wallet might bring and discussed research potential we see. This covered various dimensions: In the governance dimension, we argue that an environment as complex as and involving as many stakeholders as SDG and the EUDI Wallet cannot just be governed by expert groups defined in the policy basis. It needs community building and stakeholder engagement to cover various interests, diverse service requirements and user needs. The privacy dimension we discussed acknowledges that data protection is at the heart of both SDG and eIDAS. Still, some future research is suggested

like how the objective of citizen unobservability when using the Wallet can cope with the services' need of identity matching that both eIDAS and OOTS have. In the electronic services dimension, we argue that with the new paradigms OOTS and EUDI Wallet introduced, research on new service designs is needed so as to best make services fit for the mobile environment. Finally, we discussed the mobile computing dimension where constraints of mobile devices or dependency on the non-European market players providing smartphones and mobile operating systems ask for research on how the EUDI Wallet can be broadly deployed with the technology we currently have without getting in compromises on security and privacy. We also argue that research is needed on how to implement with alternatives to smartphones, particularly for accessibility and inclusiveness considerations but also to prepare for future devices we now even cannot imagine.

Mobile cross-border government services are characterised by a convergence of innovative frameworks like OOTS and EUDIW, possibly aligned with the transformative power of blockchain and AI. These advancements on the one side promise a future where citizens and companies can seamlessly access government services across borders, fostering greater collaboration and efficiency in the globalised digital landscape. On the other side, some challenges and considerations must be addressed and continuously monitored. Issues related to data privacy, security and international regulatory frameworks need careful attention to ensure the responsible implementation of these technologies. Governments must collaborate on standards for cross-border data exchange and establish trust frameworks to build confidence in using disruptive technologies.

References

1. Regulation (EU) 2018/1724 of the European Parliament and of the Council of 2 October 2018 establishing a single digital gateway to provide access to information, to procedures and to assistance and problem-solving services and amending Regulation (EU) No 1024/2012.
2. Regulation (EU) 2018/1724 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.
3. European Commission 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.
4. European Commission Recommendation of 3.6.2021 on a common Union Toolbox for a coordinated approach towards a European Digital Identity Framework.
5. European Commission Implementing Regulation of 5 August 2022 setting out technical and operational specifications of the technical system for the cross-border automated exchange of evidence and application of the 'once-only' principle in accordance with Regulation (EU) 2018/1724 of the European Parliament and of the Council.
6. Regulation (EU) 2022/1925 of the European Parliament and of the Council of 14 September 2022 on contestable and fair markets in the digital sector and amending Directives (EU) 2019/1937 and (EU) 2020/1828 (Digital Markets Act).

7. Krimmer, R., Dedovic, S., Schmidt, C., Corici, A.-A.: Developing cross-border E-governance: exploring interoperability and cross-border integration. In Electronic participation. Springer International Publishing (2021)
8. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)
9. Directive 2006/123/EU (EU) 2018/1724 of the European Parliament and of the Council of 12 December 2006 on services in the internal market