Summary

Carsten Schmidt, Thomas J. Lampoltshammer, and Vincent Homburg

Abstract The preceding chapters present lessons from 3 years of work in the mGov4EU project. This chapter summarises and synthesises the key findings and takeaways based on experiences gathered in 3 years of working with pilots in the mGov4EU project. Concerning the mGov4EU reference architecture, it is concluded that technical challenges could be addressed with a dedicated eID app to allow for app-to-app interaction, tighter integration between mobile applications and service provider applications and alternative wallet-based authentication protocols. Studies of mobile government users identified users' lack of awareness and reluctance to use biometric functionalities in mobile devices, highlighting the critical role of a well-designed user interface. It was also found that identity wallets come with accessibility risks and data protection concerns, for which solutions are proposed. Overall, it is concluded that mGov4EU's results are reusable and sustainable.

Keywords Once-only principle · Single digital gateway · SDGR · Digital single market · mGov4EU · Building blocks · OOTS · eID · eIDAS · Co-creation

1 What Can We Learn from 3 Years of Transdisciplinary Research in the mGov4EU Project?

In the preceding chapters, mGov4EU participants have presented the findings of 3 years of practice-oriented transdisciplinary research in the mGov4EU project. In this chapter, the findings are summarised, and key takeaways are synthesised. As one of the key motivations of mGov4EU was to study practical implementations

C. Schmidt · V. Homburg (✉)
University of Tartu, Tartu, Estonia
e-mail: carsten.schmidt@ut.ee; vincent.homburg@ut.ee

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

V. Homburg et al. (eds.), *From Electronic to Mobile Government*,
https://doi.org/10.1007/978-3-031-64471-9_13

of the ongoing eIDAS regulation and SDGR once-only principle by developing and testing mobile cross-border services, we will first present takeaways from using eIDAS and SDGR layers in mobile government applications and reflect on how eIDAS and SDGR principles relate to mobile government architectures and business models. In the subsequent section, we will present lessons learned from studying users' experiences and reflect on how studying user journeys and focusing on user experiences can help elevate mobile government applications. Then, Sect. 4 will synthesise key takeaways on how to deal with safety, ethics and privacy considerations. In Sect. 5, we will present relevant insights for future research endeavours and European digital government policy initiatives and, more generally, reflect on the sustainability of the mGov4EU deliverables. We end this chapter with a short epilogue.

2 Takeaways from Using SDGR and eIDAS Layers in Pilots

Throughout the various project phases and during the development, implementation and validation of the internet voting, mobile signing and smart mobility pilots, a cohesive mGov4EU reference architecture was developed with which challenges of 'mobile-first', secure user identification across borders and efficient cross-border data exchange could be addressed in the various pilots. The mGov4EU reference architecture aligns reasonably well with eIDAS nodes, and it was concluded that the architecture allows for cross-border authentication, cross-border data exchange and document/evidence retrieval. Challenges that had to be dealt with were that eIDAS nodes use Security Assertion Markup Language (SAML) protocols that were incompatible with many native mobile applications. In order to resolve these compatibility challenges, two solutions were developed. The first was to develop dedicated eID apps to allow for app-to-app communication, and the second was to develop a mobile app software development kit (SDK) for tighter integration between mobile applications and service provider applications. OpenID Connect (OIDC) and OAuth open authentication protocols were implemented as alternatives to the SAML protocols.

Another lesson learned was that the EUDIW standards proved difficult to work with, and throughout the project, a specific wallet solution was developed as a transitional bridge between the current and upcoming eIDAS Regulation iterations. Wallet-based authentication was realised using Verifiable Credentials and Self-Issued Open ID Provider v2-to-Open ID Connect translation.

In conclusion, especially the 'mobile-first' principle central to the mGov4EU project made it necessary to implement alternative technical solutions for identification and wallet-based authentication. With these modifications, the mGov4EU project resulted in a comprehensive solution for mobile-first, digital identity and cross-border evidence retrieval within the eIDAS and SDGR frameworks, and these solutions demonstrate the potential of mobile-first public service delivery in a European context.

3 Findings Derived from Mobile Government Users' Experiences

Studies of mobile government users revealed that especially smartphones' biometric functionalities pose challenges. Partly this is so because some users are unaware of identification by fingerprint, and partly this is because some users are reluctant to use biometric solutions. These findings underline the importance of accommodating diverse user preferences in the design of mobile government applications. Furthermore, it was found that well-designed, inclusive user interfaces and seamless user experience reduce the need for user training and are generally conducive to adoption of mobile government adoption across various types of users.

4 Security, Ethics and Privacy

Continuous reflection on the pilots' experiences and ongoing political development revealed that the EU Digital Identity Wallets trigger general accessibility and digital divide concerns. Furthermore, it was concluded that security is a critical concern in collaborative research projects like mGov4EU, and in order to remedy these concerns, a five-step method is proposed and tested in the mGov4EU project. Application of the method in the mGov4EU showed its strength in identifying security risks and integrating security measures into work packages. The proposed method, with its generic nature, holds the potential for broader applicability across various collaborative research projects.

5 Sustainability Beyond the Project

mGov4EU is a project and, by definition, has an end date. An important ambition, however, was to produce relevant insights and deliverables for cross-border mobile government services beyond the pilots central to the project. A vital goal for mGov4EU was to develop sustainable results. Reflection on the development process, testing and validation and lessons learned resulted in the identification of four crucial insights that allow for sustainability beyond the project's end date.

First, from a technical point of view, it can be stated that decoupling the eID interoperability system, the Digital Wallet system, the SDG interoperability system, the eSignature system and the architecture allows for maximum reusability of the deliverables beyond the project itself. This resulted in reusable and extensible technical building blocks.

Second, policymakers and developers of future cross-border mobile government services may also use the five-step security risk assessment method that is generic in its ability to detect and remedy risks in other initiatives as well.

Third, the usage of co-creation in the project was valuable for its outcomes; it has resulted in an analysis of business model dynamics within the context of the mGov4EU project, enabling future policymakers and mobile government developers to create innovative mobile government initiatives. The earlier and stronger co-creation elements are incorporated into the process, the more beneficial they are.

Fourth, from a non-technical point of view, on the one side, the mGov4EU project has taught us in detail that achieving semantic operability is both a key challenge and a critical factor for any future European mobile government initiative. On the other side, it has used the GOFA (Governance, Operational, Finance and Architecture) model to develop a sustainability plan. Furthermore, the project has showcased that the GOFA model itself is sustainable and extensible; it can be used for large-scale projects and projects on a smaller scale and beyond.

6 Epilogue: Some Famous Last Words

With the summary of findings and identification of lessons learnt throughout the mGov4EU project, this chapter marks the end of a project that has not only brought together scholars and practitioners from ten participating organisations and five countries but has also invited participants with backgrounds in computer science, law, political science and public administration to embark on a transdisciplinary journey. The pilots in internet voting, smart mobility and mobile signing provided engineering challenges and opportunities to record users' experiences and also allowed for ethical reflection and, above all, for lessons learned and concrete deliverables that are most likely relevant, valid and usable, beyond the end date of the project. We are quite confident that policymakers and developers in future European mobile government initiatives can make fruitful use of the insights reported in the various chapters of this book, and we would like to wish them gute Reise, turvalist reisi, buen viaje, *safe travels*.