Newsletter

Edition 07

August 2023

This issue

The 7th issue of our newsletter is entirely about the latest developments and project progress of mGov4EU.

The first thing to report is that an Executive Board / Technical Meeting was arranged in Tartu this June. In addition, mGov4EU successfully completed the Horizon Results Booster Initiative. We also report in on the testing of our pilot project at Tartu University and what results and learnings we have found. The newsletter issue also takes a look at how technology is overtaking legislation and how mGov4EU is helping. A lot has happened at mGov4EU since the last newsletter, which will be briefly presented in this issue.

Executive Board / Technical Meeting in Tartu

The project is relatively in the final phase and the mGov4EU Executive Board Meeting in Tartu marked the beginning of the last six months of the project. On the 20th of June, all partners met in Tartu to report the project progress since the last meeting in Barcelona. In addition to the status update of the individual work packages, the first part of a Technical Integration Workshop was also conducted. The first day of the meeting was rounded off with a subsequent dinner, where the partners were also able to witness the famous „White Nights“ in Estonia. The second day continued with the meeting where administrative things were decided and more workshops were held on our book and on sustainability and co-creation. At the same time the i-voting Pilot of Scytl Election Technologies and Tartu University was tested. After the meeting, our partners University for Continuing Education Krems, Fraunhofer and Tartu University stayed together to prepare for participation at dg.o 2023.

mGov4EU's participation in the HRB initiative

mGov4EU had the honour to participate in the Horizon Results Booster Initiative together with three other projects. Together with ACROSS, inGov and INTERLINK, we are striving to create an open cooperation and innovation platform within our cluster „Innovative Public Services for EU Citizens“. This cluster provides a trusted and secure digital environment where users can share their data and digital identity safely and without any risks. In any case, within the framework of the HRB initiative, we have managed to develop a **policy brief** in which, for example, we have elaborated the political challenges in simplifying the use of public services in the EU, including recommendations to overcome them. Through the initiative and participation in Module A and B, we were able to strengthen our dissemination activities, identify relevant stakeholders, and also earn a certificate in Communication and Dissemination Capacity Building. Check out the common **Twitter** and **LinkedIn** account for more information.

mGov4EU's pilot project in Tartu University

Having reached the last year of the project mGov4EU, we are starting to conduct the pilots to demonstrate the technology that has been implemented during the project. Scytl Election Technologies, as online voting experts, and the University of Tartu in Estonia, are running an online voting pilot. The pilot has been divided into two phases, the first of which has already been conducted. In this article, we will explain the first phase and the lessons learned from it.

The online voting pilot **integrates with several building blocks of the project**. In the first phase we integrated the eID and Wallet authentication building blocks:

1. **eID authentication:** This building block enables a voter to authenticate themselves via **eIDAS** (**electronic identification and trust services**) using only mobile apps and a notified eID scheme. The standard procedure to authenticate with eIDAS is browser-based, thus the user is asked to select their country of origin and is then redirected to the identity provider of the user's home country. Instead, with this building block, an app called eIDAS App pops up just when the authentication process starts and allows the user to select their country of origin. Then the eIDAS App appropriately redirects the user to its local identity provider. At that point, if the identity provider has an app, it also pops up seamlessly for the user.
2. **Wallet authentication:** TThis building block enables the voter to store several pieces of data, such as credentials, inside a virtual wallet implemented as a mobile app. The wallet complements the eID authentication building block; thus, a credential can be stored in advance within the wallet. In this case, the user can directly authenticate without the need to be redirected to the user's local identity provider.

The pilot had some characteristics that we knew in advance and that might pose a challenge to its development. Namely that no real eIDs could be used, only the Android platform was supported, and that it was required to use biometrics. In order to still be able to carry out the testing under as real as possible conditions, we successfully tested with official Austrian test eIDs. Concerning the limitation to only use Android, the reason behind it was that the integrated building blocks were only implemented as Android apps, thus only users with this platform could participate in the pilot. And regarding the biometrics, the apps included certain advanced security features to locally (in the phone) authenticate the user, i.e. the fingerprint reader and a **hardware-backed keystore** (a functionality of the smartphone used to securely store private information, such as credentials or cryptographic keys), that were only available in smartphones manufactured after 2018, approximately. These features required a fingerprint reader and a hardware-backed keystore. This excluded some users that initially wanted to participate in the pilot, despite the fact that they had an Android smartphone. Although the application is only supported on newer phones, it also has the advantage of ensuring that the login process and all data processed in it are secure.

In order to conduct the pilot, the following tasks, from technical to legal, had to be arranged:

- The aforementioned building blocks had to be integrated.
- The i-voting software had to be deployed in the cloud.
- Test users had to be setup (eID authentication) or created (wallet authentication).
- An election, with the questions, answers, dates, etc., had to be set up.
- An electoral roll, which is a list of users authorized to vote in the election, had to be created and uploaded.
- Consent forms for the user's participation in the pilot needed to be written and then signed.
- Data protection agreements were written and signed among the partners that required them.

The first phase of the pilot finally took place in June 2023 at the University of Tartu, where a small election was organized among the university staff to decide on the preferred schedule of a regular departmental meeting. For this phase, the participants used their own personal phones. Some spare phones were also included as a contingency measure in case some of the personal phones did not work. The participants were requested to come on a specific day and at a specific time to one of the university rooms where the pilot took place. The session started by linking test user identities with the actual smartphones of the participants. Two types of authentication were tested, some participants chose the eID-based authentication and others used the Wallet-based authentication. Later, after all the participants were authenticated, they could vote.

In conducting the pilot, we learned several lessons. The most relevant were the following:

- **Not everybody uses smartphone biometrics:** Initially we assumed that everybody would have the biometric features of their smartphones configured, or that the fingerprint of the user was set up to unlock their phone. But this was not a valid assumption. Several people did not have it enabled nor did they know how to use it. Thus, the general public cannot be assumed to have the knowledge of how to use these technologies, despite their usage being quite widespread.
- **Not everybody agreed to use smartphone biometrics:** SSome people did not have biometrics enabled on their phones for privacy reasons. Biometric features are considered personal sensitive data by the **EU GDPR**. Thus, any user who does not want to use biometrics has arguments for their decision. However, it is also necessary to clearly explain to the users how their biometric features are used in these cases so they can make an informed decision. In this particular case, biometric features are only locally used. In other words, they are not stored in any server, just in the user's smartphone for authentication purposes. Thus, despite the fact that they are sensitive personal data, they are never shared with anyone nor exported from the local device.
- **Support had to be provided to the participants:** The procedure to link the test user identities with the smartphones of the participants was not designed for the final user and it required support. This has to be improved or delegated to the staff in charge of doing the setup. In a real setting, this procedure is done by the issuers of the eIDs.

Even though we learned some lessons during the testing, we were able to celebrate numerous achievements:

- The pilot has successfully tested the eID and wallet-building block
- It was shown that the technical approaches and solutions behind the Building Blocks work in practice
- It has been successfully tested with the most widely used smartphone platform (Android)
- It has been successfully tested with a variety of different Android smartphones and users
- A complete voting process was successfully completed
- It was tested with official Austrian test eIDs, i.e. the pilot was connected to the official Austrian test eID infrastructure

In summary, a first phase of the pilot with real users and test credentials was meant to demonstrate the eID and Wallet building blocks developed in the project. Overall, the pilot was successful, but some lessons were got from it and will be considered for the next phase. The second i-voting pilot test will take place in Stuttgart in October.

Mobile identity wallets and 'code is law' – how technology outruns legislation, and how mGov4EU is helping

Almost 25 years ago, Lawrence Lessig, a notable professor of law at Harvard, coined the expression "code is law" in his book **Code and Other Laws of Cyberspace**. Briefly summarized, "code is law" refers to the phenomenon that, in a digital environment, software code can be as effective as legislation – often even more so – in regulating what behaviour is permissible. In simpler terms: if an app only allows you to take a few actions, and you have no alternative to using that app, than the programming of that app might as well be actual law. You're more effectively bound by the software code than you would be by any legal code. If software is your only tool, then coding beats legislation.

What does that have to do with mobile identity wallets and with mGov4EU? The link is actually quite simple: mGov4EU is building and piloting a new generation of mobile identity wallets (and surrounding services) that should be capable of satisfying European legislative requirements. However, those legislative requirements don't exist in their final form yet: while a proposal for legislation around the so-called European Digital Identity Wallet was **published already in June 2021**, the final text still hasn't been adopted yet. Finalisation is rumoured to be a matter of weeks, or a few more months at most; but technically speaking, there are no legal requirements to follow at this time.

One option to respond to that situation could be to wait, and to starting building technical solutions once the legal dust has settled. But, as the recent passing of the second anniversary of the EU legislative proposal shows, legislation is a slow game, and waiting means that precious time is lost. So, the Commission has published its Architecture and Reference Framework in February 2023 – explaining at a high level how the solution that has not yet been legislated should be structured – and a slew of EU funded pilot projects, including mGov4EU, is building wallets that aim to satisfy the objectives of the proposed legislation.

This creates an intriguing situation, where the higher speed of technology can help compensate the lower speed of the law: technical solutions to satisfy the law will likely be nearly done before the law is adopted and published, and the ongoing legislative process can actually still take up the lessons that projects such as mGov4EU are learning.

It's a development that raises interesting questions on a shift of the primacy of the law, to a primacy of technology – or at least on a situation where perhaps code isn't law, but rather code becomes law, through a dialogue between legislators and coders.

And by being among the teams that build the actual code behind identity wallets, even before the law of the land is settled, mGov4EU is helping to drive the discussion forward!

What comes next?

d.go 2023

24th Annual International Conference on Digital Government Research (dg.o 2023) will take place again in Gdańsk, Poland. The focus of the conference this time is on digital governance and solidarity and aims to put the concept of solidarity at the center of the digital government debate. Anyway, some of our mGov4EU partners have submitted papers to the conference and are also participating in it. You will get more insights in the next issue of our newsletter, on our website and social media channels.

Executive Board / General Assembly Meeting in Stuttgart

The next Executive Board / General Assembly Meeting will take place at our partner Fraunhofer IAO in Stuttgart. At the meeting in October, the consortium will prepare among other things, the upcoming project end. We will of course keep you informed about the most important project results.

Symposium on Identity and Mobile Government

Right now, the consortium is in the process of organizing a symposium on Identity and Mobile Government. More information will follow, so don't miss it.

The mGov4EU Consortium

TECHNIKON
Coordinator

Scytl

TARTU ÜLIKOOL
UNIVERSITAS TARTUENSIS
1632

DONAU UNIVERSITÄT KREMS

Scientific Lead

TIMELEX

TU Graz

A-SIT
Technical Lead

esec

Fraunhofer

go.eIDAS

mGov4EU

The mGov4EU project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No. 959072.

Contact

coordination@mgov4eu.eu

www.mgov4.eu

Follow mGov4EU on:

@mGov4EU

Budget

€ 3.9 Million
100% EU-funded

Consortium

10 Partners
5 countries

Duration

36 Months
01/2021 - 12/2023