

“EUDI WALLET PROTOTYPES”

→ OVERVIEW

WHO IS SPRIND?

SPRIND is the Federal Agency for Disruptive Innovation. SPRIND is a federal company (officially designated a “Gesellschaft des Bundes”) tasked with identifying, financing, and scaling groundbreaking innovations. Inspired by the American DARPA, its main goal is to provide agile and proactive support for people who are creating innovations that will change our lives.

The Challenges and Funken are SPRIND's innovation competitions. They are a tool that SPRIND uses to track down pioneering innovations. In competition with each other, the participating teams demonstrate which solution has what it takes to become a disruptive innovation.

WHAT IS THE TOPIC OF THIS SPRIND FUNKE?

Digital proof of identity is an important basis for the digitalization of our lives. Digital wallets enable users to receive, manage, and present proof of identity and other attributes as part of digital processes. This will make digital wallets an essential part of our society's digital infrastructure. They will enable the complete digitalization of processes and thus allow for completely new approaches to problems, which also makes them the basis for disruptive innovations. Various approaches are currently being discussed for implementing the wallets, but there is not enough implementation experience to make a well-founded decision on the most suitable approach.

The aim of this Funke is to create prototypes with differing wallet implementations for the most trustworthy, user-friendly, and universally applicable European Digital Identity Wallets (EUDIW) for users in Germany. These wallets are also to be compatible with applications in the EU and beyond and should be able to be used by individual people and organizations. This Funke focuses on wallets for individuals.

This innovation competition will allow multiple teams to test and compare their approaches. It is planned that those teams selected for the second and third stages of the competition accompany the EU-wide testing of their wallets as part of the Large Scale Pilots POTENTIAL. The Funke will provide valuable insights for further developing the concept for eIDAS implementation in Germany.

PROJECT CONTENT / PREVIOUS WORK

SPRIND is conducting the architecture and consultation process for the implementation of the eIDAS 2.0 Regulation in Germany on behalf of the Federal Ministry of the Interior and Community (BMI). As part of this project, various architectural proposals have been developed for implementing EUDI wallets in Germany based on the infrastructure that

SPRIND

already exists for the online ID function of the state-issued ID cards. The project website can be found using the [following link](#).

THE GOAL

The Funke aims to develop and test prototypes for EUDI wallets. These prototypes must implement the following functions in a user-friendly and trustworthy manner:

- They must issue and present Person Identification Data (PID) based on the online ID function of the state-issued ID card.
- They must issue and present Electronic Attestations of Attributes (EAAs).
- They must permit pseudonymous login to Relying Parties.
- They must support the authorization of electronic signing and Strong Customer Authentication (SCA).

The interfaces of the wallet prototypes must be compatible with the [Architecture Proposal v2](#). Teams are encouraged to contribute their own creative ideas to the process and to develop and implement suggestions for improving the reference designs.

As part of the Funke, each team will develop at least one wallet app for Android or iOS and make it available for testing. It would be advantageous for the teams to provide a wallet app for both platforms.

The teams must make the wallet app(s) available for installation and use by SPRIND and the LSP POTENTIAL via a suitable distribution mechanism (e.g., TestFlight). If further technical systems are required for the use of the app(s) (e.g., a Cloud HSM), these systems must be operated by the respective team.

In particular, the Funke is intended to address critical challenges in designing an EUDI wallet for users in Germany.

These include:

- A design for issuing and presenting the PID that meets high requirements in terms of security, data protection, usability, and potential user reach.
- A suitable design for issuing and presenting the EAA that supports different types of EAAs in a generic way, ensuring good usability, security, and data privacy while permitting the issuer of each EAA to include their own branding. The EAAs are to be implemented such that they can be used via online channels but also for in-person scenarios.

In general, the prototype must have the potential to scale very well with the number of users and be cost-effective to operate.

We consider a decentralized design for the wallet prototype to be advantageous from the point of view of digital sovereignty, economic efficiency, and usability for in-person scenarios.

When selecting the teams, the jury will ensure that as many PID options as possible from the architecture proposal are covered across the teams.

The exact objectives of the three stages and the evaluation criteria are listed below.

In this context, please refer to the regulations in the participation agreement for the funded track with regard to the exact specifications for the use of a repository for review by SPRIND

and the subsequent publication as open source. Publication as open source must take place on [OpenCoDE](#).

Further details on the rights and use of intellectual property are also regulated in the respective participation agreement.

It is recommended that the teams use existing components for the implementation of the basic functions of the wallets to the extent possible, so that they can focus on the specific challenges of the respective stage during the course of the Funke. A potential basis for this is the [Reference Wallet Application of the European Commission](#).

Note: The Funke serves to explore solutions for EUDI wallets. The result of the Funke will not decide anything in relation to technical designs, technology used, operating models, or providers of one or more future EUDI wallets in Germany. The findings will be used to further develop and refine the concept for the German implementation of the eIDAS Regulation.

STAGE 1 (PID DESIGN EXPLORATION AND EVALUATION)

The aim of this stage is to implement a PID solution. The PID must achieve a level of assurance “high” and it must be interoperable with the EUDI wallets of the other member states. These aspects are given special consideration in the evaluation of each proposal. In addition, for the widespread use of the EUDI, it is absolutely essential that a PID solution has the best chance of achieving a high degree of user reach and acceptance.

In the future, there will be a certification scheme for EUDI wallets and therefore also PIDs. However, its design has not yet been finalized. The following documents will therefore serve as the basis for evaluating the security of the solutions as part of the Funke:

- [Implementing Act 2015/1502](#),
- [Guidance for the application of the levels of assurance which support the eIDAS Regulation](#),
- [BSI TR 03107](#).

The teams can select one or more designs from the PID Reference Designs of the Architecture Proposal and implement them. Teams are encouraged to contribute their own creative ideas to the process and to develop and implement suggestions for improving the reference designs. At the EU level, the PID must achieve a high level of trust. The teams must document what level of trust their design is aiming for and how this can be achieved by the chosen design.

The PID will be presented for online use with OpenID4VP. The PID formats mdoc and SD-JWT VC must be supported.

The BMI will arrange for a reference PID issuer to be made available to the teams, both in the form of a test installation and in the source code. The teams will also be provided with test eID cards for this purpose. The teams can use the reference issuer for development, tests, and demonstrations. However, they are also free to use their own PID issuer. To develop it, they can also access the source code of the reference PID issuer and modify it in a fork.

In addition to the wallet prototype, each team will also implement a test relying party (RP) that can be used to test and demonstrate the prototype.

The team must provide the prototype, including the test RP for demonstration and evaluation of the prototype, to SPRIND’s project team at least one week before the end of the stage and

SPRIND

enable SPRIND to test the prototype. Testability (as part of a test environment) must be guaranteed for at least two weeks after the end of the stage. If the team is selected for the next stage, the testability of stage 1 must be guaranteed for at least two weeks after completion of stage 2.

The project team will support the participating teams by answering questions, e.g., to clarify options from the architecture proposal. All questions and answers will be provided to all participants. The project team will incorporate the answers into the architecture proposal as necessary.

The results of stage 1 must be documented by the teams. In particular, it must be documented how the selected design can achieve the respective security protection goals (security by design) and the privacy goals (privacy by design). The documentation must be made available to the jury at least seven days before the end of the stage.

Evaluation criteria:

- Security (security concept and evaluation according to “security by design”),
- Data protection (compliance with European/German data protection law, privacy by design)
- Interoperability ([Architecture Proposal v2](#) and [EUDIW Architecture and Reference Framework](#)),
- User experience (usability, accessibility, internationalization),
- Potential reach among users,
- Completeness,
- Economic efficiency,
- Software design quality,
- Performance,
- Scalability.

Further details and information can be found in the respective participation agreement.

STAGE 2 (VERSATILE (Q)EAAS WITH GREAT UX)

The aim of this level is to implement generic support for various EAAs in combination with the possibility of non-traceability and very good UX.

In detail, this means:

- Based on this stage, users should be able to have any EAAs issued into their wallet without the wallet software having to be specially adapted for this purpose. This is important in order to achieve a universally usable and non-discriminatory infrastructure for digitalization in Germany, while also ensuring that the infrastructure can be used with applications in the EU and beyond that are interoperable with the EUDI Wallet.
- At the same time, the requirements of the EAA issuers should be met, in particular with regard to the required level of security and the visualization of the EAAs (e.g., issuer branding).
- Efficient implementations for non-traceability (unlikability) in connection with derived EAAs (e.g., eligibility for certain social benefits without identifying data).

SPRIND

The formats mdoc and SD-JWT VC must be supported for EAAs. OpenID4VP must be supported for online use. The in-person presentation of mdoc-based EAAs must also be supported according to ISO 18013-5. Proposals for a presentation of SD-JWT VC for in-person scenarios are welcome.

Besides implementing the functions in the wallet prototype, the teams must also implement at least one of their own EAA issuers and a test RP.

The same evaluation criteria and documentation requirements apply as for stage 1.

In addition to expanding the prototype, the participating teams support the LSP POTENTIAL participants in using their respective wallet prototypes. The teams will also correct errors in the implementation from stage 1 and make minor adjustments based on feedback from the LSP.

The team must provide the prototype, including the test RP and EAA issuer(s) for demonstration and evaluation of the prototype, to the SPRIND project team at least one week before the end of stage 2. Testability must be guaranteed for at least two weeks after the end of stage 2. If the team is selected for the next stage, testability must be guaranteed until the end of the Funke (other versions may be made available after consultation).

Further details and information can be found in the respective participation agreement.

STAGE 3 (LOGIN, QES, AND SCA)

In stage 3, the wallet prototypes will be expanded to include the following functions:

- Pseudonymous logins (Basis: [SIOP v2](#)),
- Qualified electronic signatures, assuming that the signature is triggered in the wallet,
- Strong Customer Authentication (SCA).

The enhancements are implemented and documented by the teams one after the other. Each extension will be made available to LSP POTENTIAL participants for testing after the extension has been completed and reviewed by SPRIND.

In addition to expanding the prototype, the participating teams support the LSP POTENTIAL participants in using their respective wallet prototypes. The teams will also correct errors in the implementation from stages 1 and 2 and make minor adjustments based on feedback from the LSP.

The same evaluation criteria and documentation requirements apply as for stages 1 and 2.

Further details and information can be found in the respective participation agreement.

HOW ARE THE TEAMS SELECTED? SELECTION PROCEDURE FOR PARTICIPATION IN THE FIRST STAGE

SPRIND selects the Funke teams with the support of international experts. The applications undergo a pre-selection process carried out by the team of experts of the EUDI Wallet Infrastructure project and SPRIND. Selected applications are evaluated and invited to a pitch. The applications are evaluated with regard to:

- their potential to become an innovation (approach),
- the effectiveness of the proposed work plan (implementation), and

- the ability of the team to implement this plan (team).

Table 2 shows how these criteria can be assessed.

Table 2: Selection criteria

Approach
Does the proposed concept contain adequate solutions for the challenges described in this call for proposals?
Are the proposed solutions particularly innovative, and can they significantly advance the work on this topic?
Is it foreseeable that the results will meet the requirements for security and data protection as well as the requirements of the eIDAS Regulation?
Is it foreseeable that the results will have very good usability?
Can a large number of users be reached with the proposed approach?
Is the proposed design compatible with the ARF and the Architecture Proposal v2?
Does the proposal contribute to the broadest possible coverage of all PID options from the Architecture Proposal?
Does the proposal include the development and provision of wallet apps for Android and iOS?
Is a largely decentralized approach pursued without unnecessary server components?
Can the proposed solution be operated economically and sustainably in the foreseeable future?
Implementation
Is the calculation of the offer reasonable?
Is the offer within the cost and time frame?
Team
Does the team have the necessary expertise, dynamism, and innovation and implementation strength for the Funke?
Economic efficiency
Are the total costs calculated in proportion to the scope of services offered?

WHAT WILL HAPPEN DURING THE FUNKE? WHAT MUST BE ACHIEVED?

For the first stage, up to six teams will be selected for both the Funded Track and the Non-Funding Track.

After completing the first stage, all teams demonstrate their results to the jury. The jury then decides which teams (max. 4) from the Funded Track and the Non-Funding Track will receive further support in the second stage. The decision is based on the criteria described above.

Accordingly, after completion of the second stage, the two remaining teams from the funded and non-funded tracks will be selected for stage 3.

SPRIND

The schedule shown represents the current planning status. SPRIND reserves the right to make changes during the course of the Funke, see the regulations in the respective participation agreement.

At the end of each stage, the participating team summarizes key elements of the development status in a report. The report should describe whether the objective described in the application has been achieved. In addition, the intellectual property developed (know-how, data, inventions, etc.) should be outlined and, if applicable, a list of publications should be added. The report is required seven days before the end of the respective stage regardless of whether the team applies for the next stage or not.

Further details and information can be found in the respective participation agreement.

The teams can contact the SPRIND Challenge team at any time if they have questions about the development of their solution.

WHO ARE THE WINNERS OF THE FUNKE?

In the end, all future users will be the winners, as the Funke will provide important ideas for developing a concept for user-friendly, secure, and trustworthy EUDI wallets.

The participating teams benefit in many ways: As part of the Funded Track, the participating teams are funded to work on an exciting and innovative topic. Teams from both tracks receive support from SPRIND. They can make their approaches known to a broad public and receive valuable feedback from experts from the jury and the Large Scale Pilot POTENTIAL. And last but not least, their work has an impact, as they provide ideas for designing the future EUDI wallet infrastructure in Germany (and beyond).

CONFIDENTIALITY

SPRIND treats all submissions confidentially. The teams that are qualified for the Funded Track and Non-Funding Track were announced publicly.

WHOM CAN I CONTACT IF I HAVE FURTHER QUESTIONS OR QUERIES?

If you have any questions, please contact us at funke-eudi@sprind.org.