“EUDI WALLET PROTOTYPES”

→ OVERVIEW

WER IST DIE SPRIND?

SPRIND ist die Bundesagentur für Sprunginnovationen. SPRIND ist eine Gesellschaft des Bundes und hat die Aufgabe, bahnbrechende Innovationen zu identifizieren, zu finanzieren und zu skalieren. Inspiriert von der amerikanische DARPA ist ihr Hauptziel, agile und proaktive Unterstützung zu leisten, um Innovationen hervorzubringen, die unser Leben verändern.

Die Challenges und Funken sind die Innovationswettbewerbe der SPRIND. Sie sind ein Instrument, mit dem die SPRIND bahnbrechende Innovationen aufspürt. Im Wettbewerb miteinander demonstrieren die teilnehmenden Teams, welche Lösung das Zeug zur Sprunginnovation hat.

WORUM GEHT ES IM SPRIND FUNKE?

Digitale Identitätsnachweise sind eine bedeutende Grundlage für die Digitalisierung unseres Lebens. Digitale Brieftaschen, sogenannte Wallets, ermöglichen es Nutzenden, im Rahmen von digitalen Prozessen Identitäts- und andere Nachweise zu empfangen, zu verwalten und vorzuweisen. Damit werden Wallets ein essentieller Bestandteil der digitalen Infrastruktur unserer Gesellschaft sein. Sie ermöglichen eine vollständige Digitalisierung von Prozessen und damit auch völlig neue Herangehensweisen an Probleme, was sie auch zur Basis von Sprunginnovationen macht. Derzeit werden unterschiedliche Ansätze für die Implementierung von Wallets diskutiert, es gibt aber zu wenig Implementierungserfahrung, um eine fundierte Entscheidung über den bestgeeigneten Ansatz zu treffen.

Ziel des Funke ist es, Prototypen unterschiedlichster Implementierungen von Wallets für die vertrauenswürdigsten, nutzerfreundlichsten und universell einsetzbarsten European Digital Identity Wallets (EUDIW) für Nutzer:innen in Deutschland zu entwickeln und zu erproben. Diese Wallets sollen auch mit Anwendungen in der EU und darüber hinaus kompatibel sein und sowohl für natürliche Personen als auch Organisationen nutzbar sein. Der Funke fokussiert auf Wallets für natürliche Personen.

Auf dem Wege eines Innovationswettbewerbs können verschiedene Teams ihre Ansätze testen und miteinander vergleichen. Es ist geplant, dass diejenigen Teams, die für die zweite und dritte Stufe des Wettbewerbs ausgewählt werden, die EU-weite Erprobung ihrer Wallets im Rahmen des Large Scale Pilots POTENTIAL begleiten. Der Funke liefert damit wertvolle Erkenntnisse für die weitere Ausgestaltung des Konzepts für die eIDAS-Umsetzung in Deutschland.

PROJEKTINHALT / VORARBEITEN

SPRIND führt im Auftrag des Bundesministeriums des Inneren und für Heimat (BMI) den Architektur- und Konsultationsprozesses für die Umsetzung der eIDAS-2.0-Verordnung in

Deutschland durch. Im Rahmen dieses Projektes wurden bisher verschiedene Architekturvorschläge für die Implementierung von EUDI Wallets in Deutschland auf Basis der existierenden Infrastrukur der Onlineausweisfunktion des Personalausweises entwickelt. Die Projektwebseite befindet sich unter folgendem Link.

DAS ZIEL

Das Ziel des Funkes ist die Entwicklung und Erprobung von Prototypen für EUDI Wallets, mit dem Ziel der Evaluation der verschiedenen Architekturoptionen. Diese Prototypen müssen folgende Funktionen nutzer:innenfreundlich und vertrauenswürdig implementieren:

- Die Ausstellung und Präsentation von sogenannten Person Identification Data (PID) auf Basis der Onlineausweisfunktion des Personalausweises.
- Die Ausstellung und Präsentation von sogenannten Electronic Attestations of Attributes (EAAs).
- Das pseudonyme Login zu Relying Parties.
- Die Autorisierung von Elektronischen Signaturen und Strong Customer Authentication (SCA).

Die Schnittstellen Wallet-Prototypen müssen mit dem Architecture Proposal v2 kompatibel sein, damit sie mit den Wallet(-Prototypen) anderer Mitgliedsstaaten interoperable sind und im Large Scale Pilot (LSP) POTENTIAL gemeinsam getestet werden können. Es ist erwünscht, dass Teams eigene kreative Ideen in den Prozess einbringen und Vorschläge für Verbesserungen der Referenzdesigns entwickeln und implementieren.

Im Rahmen des Funkes soll je Team jeweils mindestens eine Wallet App für Android oder iOS entwickelt und für Tests zur Verfügung gestellt werden. Die Bereitstellung einer Wallet-App für beide Plattformen durch das jeweilige Team an die SPRIND wäre vorteilhaft.

Die Teams müssen die Wallet-App(s) über einen geeigneten Verteilmechanismus (z. B. TestFlight) für die Installation und Nutzung durch SPRIND und den LSP POTENTIAL zur Verfügung stellen. Sollten für die Nutzung der App(s) weitere technische Systeme erforderlich sein (z. B. ein Cloud HSM), sind diese Systeme durch das jeweilige Team zu betreiben.

Im Funke sollen insbesondere kritische Herausforderungen beim Design eines EUDI Wallets für Nutzer:innen in Deutschland adressiert werden.

Dazu gehören:

- Ein Design für die PID-Ausstellung und -Präsentation, das hohe Anforderungen in Bezug auf Sicherheit, Datenschutz, Nutzbarkeit und erreichbare Nutzer:innen-Reichweite erfüllt.
- Ein geeignetes Design für EAA-Ausstellung und -Präsentation, das verschiedenste Arten von EAAs auf generische Art und Weise unterstützt, wobei eine gute Nutzbarkeit, das Branding des Ausstellers des jeweiligen EAAs sowie Sicherheit und Datenschutz gewährleistet sind. Hierbei ist eine Nutzung der EAAs über den Online-Kanal aber auch für "in-person" Szenarien umzusetzen.

Generell muss der Prototyp das Potenzial haben, sehr gut mit der Anzahl der Nutzer:innen zu skalieren und kostengünstig betreibbar zu sein.

Ein dezentrales Design des Wallet-Prototyps wird aus Sicht der Digitalen Souveränität, Wirtschaftlichkeit und der Nutzbarkeit in „in-person“ Szenarien als vorteilhaft angesehen.

Die Jury wird bei der Auswahl der Teams darauf achten, dass über die Teams hinweg möglichst alle PID-Optionen aus dem Architecture Proposal abgedeckt werden.

Genaue Ziele der drei Stufen und der Bewertungskriterien sind unten aufgeführt.

In diesem Zusammenhang ist hinsichtlich der genauen Vorgaben zur Nutzung eines Repository zur Prüfung durch die SPRIND sowie die spätere Veröffentlichung als Open Source auf die Regelungen in der Teilnahmevereinbarung für den Funded Track zu verweisen. Die Veröffentlichung als Open Source hat auf OpenCoDE zu erfolgen.

Weitere Details zu den Rechten und der Nutzung des geistigen Eigentums sind ebenfalls in der jeweiligen Teilnahmevereinbarung geregelt.

Es wird empfohlen, dass die Teams soweit wie möglich auf existierende Komponenten für die Implementierung der Basisfunktionen der Wallets zurückgreifen, so dass sie sich im Verlauf des Funkes auf die konkreten Herausforderungen der jeweiligen Stufe konzentrieren können. Als potenzielle Basis sei hier insbesondere die Reference Wallet Application der Europäischen Kommission erwähnt.

Hinweis: Der Funke dient der Exploration des Lösungsraums für EUDI Wallets. Das Ergebnis des Funkes stellt keinen Vorgriff auf Entscheidungen zu technischen Designs, verwendeter Technologie, Betriebsmodelle oder Anbieter eines oder der zukünftigen EUDI Wallets in Deutschland dar. Die gewonnen Erkenntnisse werden der weiteren Entwicklung und Verfeinerung des Konzepts für die deutsche Umsetzung der eIDAS Verordnung dienen.

STUFE 1 (PID DESIGN EXPLORATION AND EVALUATION)

Das Ziel dieser Stufe ist die Implementierung einer PID-Lösung. Die PID muss ein hohes Vertrauensniveau erreichen und sie muss mit den EUDI Wallets der anderen Mitgliedsstaaten interoperabel sein. Diese Aspekte werden bei der Bewertung des jeweiligen Vorschlags besonders gewürdigt. Darüber hinaus ist es erfolgskritisch für die Verbreitung der EUDI Wallets, dass eine PID-Lösung die besten Chancen für eine hohe Nutzer:innen-Reichweite und -Akzeptanz hat.

Es wird in Zukunft ein Zertifizierungsschema für EUDI Wallets und damit auch PIDs geben. Dessen Ausgestaltung ist aber noch nicht abgeschlossen. Daher dienen im Rahmen des Funkes die folgenden Dokumente als Basis der Bewertung der Sicherheit der Lösungen:

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

Die Teams können aus den PID Reference Designs des Architecture Proposals ein oder mehrere Designs auswählen und diese implementieren. Es ist erwünscht, dass Teams eigene kreative Ideen in den Prozess einbringen und Vorschläge für Verbesserungen der Referenzdesigns entwickeln und implementieren. Auf EU-Ebene muss die PID ein hohes Vertrauensniveau erreichen. Die Teams müssen dokumentieren, auf welches Vertrauensniveau ihr Design abzielt und wie dieses durch das gewählte Design erreicht werden kann.

Die Präsentation der PID erfolgt online unter Nutzung von OpenID4VP. Als PID-Formate müssen mdoc und SD-JWT VC unterstützt werden.

Das BMI wird die Bereitstellung eines Referenz-PID-Issuers für die Teams veranlassen, sowohl in Form einer Test-Installation als auch im Source Code. In diesem Kontext werden den Teams auch Test-Karten zur Verfügung gestellt. Die Teams können für die Entwicklung, Tests und Demonstrationen den Referenz-Issuer nutzen. Es steht ihnen aber frei, einen eigenen PID-Issuer zu benutzen. Zu dessen Entwicklung können sie auch auf den Source Code des Referenz-PID-Issuers zurückgreifen und diesen in einem Fork modifizieren.

Jedes Team implementiert neben dem Wallet-Prototyp auch eine Test-Relying Party (RP), die zum Testen und Demonstrieren des Prototyps verwendet werden kann.

Das Team muss den Prototyp inklusive Test-RP für Demonstration und Bewertung des Prototypens spätestens eine Woche vor Ende der Stufe dem Projektteam von SPRIND zur Verfügung stellen und SPRIND die Testbarkeit ermöglichen. Die Testbarkeit (im Wege einer Testumgebung) muss mindestens bis zwei Wochen nach Ablauf der Stufe gewährleistet werden. Sollte das Team für die nächste Stufe ausgewählt werden, muss die Testbarkeit von Stufe 1 für mindestens zwei Wochen nach Abschluss der Stufe 2 gewährleistet werden.

Das Projektteam unterstützt die Teams durch die Beantwortung von Fragen z. B. zur Klarstellung von Optionen aus dem Architecture Proposal. Alle Antworten werden für alle Teilnehmer:innen bereitgestellt. Das Projektteam wird die Antworten bei Bedarf in das Architecture Proposal einarbeiten.

Die Ergebnisse der Stufe 1 sind durch die Teams zu dokumentieren. Insbesondere muss dokumentiert werden, wie das gewählte Design die jeweiligen Sicherheitsschutzziele (im Sinne von Security by Design) und die Datenschutzziele (im Sinne von Privacy by Design) erreichen kann. Die Dokumentation muss der Jury spätestens sieben Tage vor dem Abschluss der Stufe zur Verfügung gestellt werden.

Bewertungskriterien:

- Sicherheit (Sicherheitskonzept und Bewertung nach "security-by-design"),
- Datenschutz (Konformität mit europäischem/ deutschem Datenschutzrecht, Privacy by Design),
- Interoperabilität (Architecture Proposal v2 und EUDIW Architecture and Reference Framework),
- Nutzer:innen-Erfahrung (Nutzbarkeit, Accessibility, Internationalisierung),
- potenzielle Reichweite bei Nutzer:innen,
- Vollständigkeit,
- Wirtschaftlichkeit,
- Software Design Qualität,
- Performanz,
- Skalierbarkeit.

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

Das Ziel dieser Stufe ist die Implementierung der generischen Unterstützung von verschiedensten EAAs in Kombination mit der Möglichkeit zur Nicht-Verfolgbarkeit und sehr guter UX.

Im Einzelnen bedeutet das:

- Auf Basis dieser Stufe soll es Nutzer:innen ermöglicht werden, beliebige EAAs in ihr Wallet ausstellen zu lassen, ohne dass die Wallet Software dafür speziell angepasst werden muss. Das ist wichtig, um zu einer universell verwendbaren und diskriminierungsfreien Infrastruktur für die Digitalisierung in Deutschland zu kommen, die auch mit Anwendungen in der EU und darüber hinaus, die mit der EUDI Wallet interoperabel sind, verwendet werden kann.
- Gleichzeitig sollen die Anforderungen der Aussteller der EAAs, insbesondere in Bezug auf das erforderliche Sicherheitsniveau und die Visualisierung der EAAs (z. B. Issuer Branding), erfüllt werden.
- Effiziente Implementierungen für Nicht-Verfolgbarkeit (Unlikability) im Zusammenhang mit abgeleiteten EAAs (z. B. Berechtigung für bestimmte Sozialleistungen ohne identifizierende Daten).

Als Formate für EAAs müssen mdoc und SD-JWT VC unterstützt werden. Für die Online-Präsentation muss OpenID4VP unterstützt werden. Darüber hinaus muss die in-person Präsentation von mdoc-basierten EAAs über ISO 18013-5 unterstützt werden. Vorschläge für eine Präsentation von SD-JWT VC in in-person-Szenarien sind willkommen.

Die Teams müssen neben der Implementierung der Funktionen im Wallet-Prototyp auch mindestens einen eigenen EAA-Issuer und eine Test RP implementieren.

Es gelten dieselben Bewertungskriterien und die Anforderungen an die Dokumentation entsprechend wie bei Stufe 1.

Über die Erweiterung des Prototypen hinaus unterstützen die teilnehmenden Teams die Teilnehmer:innen des LSP POTENTIAL bei der Nutzung ihrer jeweiligen Wallet Prototypen. Des Weiteren werden die Teams Fehler in der Implementierung aus Stufe 1 beheben und kleinere Anpassungen auf Basis des Feedbacks aus dem LSP vornehmen.

Das Team muss den Prototyp inklusive Test-RP und EAA-Issuer für Demonstration und Bewertung des Prototypens spätestens eine Woche vor Ende der Stufe 2 dem Projektteam zur Verfügung stellen. Die Testbarkeit muss für mindestens zwei Wochen nach Ablauf der Stufe 2 gewährleistet sein. Sollte das Team für die nächste Stufe ausgewählt werden, muss die Testbarkeit bis zum Ende des Funke sichergestellt werden (ggf. werden in Absprache andere Versionen zur Verfügung gestellt).

STUFE 3 (LOGIN, QES, AND SCA)

In Stufe 3 sollen die Wallet-Prototypen um die folgenden Funktionen erweitert werden:

- Pseudonymes Login (Basis: SIOP v2),
- Qualifizierte Elektronische Signaturen, unter der Annahme, dass die Auslösung der Signatur im Wallet durchgeführt wird,
- Strong Customer Authentication (SCA).

Die Erweiterungen werden durch die Teams nacheinander umgesetzt und dokumentiert. Jede Erweiterung wird den Teilnehmer:innen des LSP POTENTIAL nach Fertigstellung und Prüfung durch SPRIND zum Test zur Verfügung gestellt.

Über die Erweiterung des Prototypen hinaus unterstützen die teilnehmenden Teams die Teilnehmer:innen des LSP POTENTIAL bei der Nutzung ihrer jeweiligen Wallet Prototypen. Des Weiteren werden die Teams Fehler in der Implementierung aus den Stufen 1 und 2 beheben und kleinere Anpassungen auf Basis des Feedbacks aus dem LSP vornehmen.

Es gelten dieselben Bewertungskriterien und die Anforderungen an die Dokumentation entsprechend wie bei den Stufen 1 und 2.

AUSWAHLVERFAHREN FÜR DIE TEILNAHME AN DER ERSTEN PHASE

Die SPRIND wählt mit Unterstützung internationaler Expert:innen die Funke-Teams aus. Die Bewerbungen durchlaufen eine Vorauswahl innerhalb des Teams der Expert:innen des EUDI Wallet Infrastruktur Projektes und der SPRIND. Ausgewählte Bewerbungen werden bewertet und zu einem Pitch eingeladen. Die Bewerbungen werden hinsichtlich

- ihres Potenzials eine Innovation zu werden (Ansatz),
- der Effektivität des vorgeschlagenen Arbeitsplans (Umsetzung) und
- der Fähigkeit des Teams, diesen Plan umzusetzen (Team)

bewertet.

Tabelle 2 zeigt, wie diese Kriterien beurteilt werden können.

Tabelle 2: Auswahlkriterien

Ansatz
Beinhaltet das vorgeschlagene Konzept adäquate Lösungen für die in dieser Ausschreibung beschriebenen Herausforderungen?
Sind die vorgeschlagenen Lösungen besonders innovativ und können das Thema signifikant voranbringen?
Ist absehbar, dass die Ergebnisse die Anforderungen an Sicherheit und Datenschutz sowie die Anforderungen der eIDAS-Verordnung erfüllen?
Ist absehbar, dass die Ergebnisse eine sehr gute Nutzbarkeit haben werden?
Kann mit dem vorgeschlagenen Ansatz eine große Anzahl von Nutzer:innen erreicht werden?
Ist das vorgeschlagene Design mit dem ARF und dem Architecture Proposal v2 kompatibel?
Trägt der Vorschlag zu einer möglichst breiten Abdeckung aller PID-Optionen aus dem Architecture Proposal bei?
Beinhaltet der Vorschlag die Entwicklung und Bereitstellung von Wallet-Apps für Android und iOS?
Wird ein weitestgehend dezentraler Ansatz ohne unnötige Serverkomponenten verfolgt?
Ist die vorgeschlagene Lösung absehbar wirtschaftlich und nachhaltig betreibbar?
Umsetzung
Ist die Kalkulation des Angebots schlüssig?

Ist das Angebot im Kosten- und zeitlichen Rahmen?
Team
Hat das Team die erforderliche Expertise, Dynamik, Innovationsstärke und Umsetzungsstärke für den Funke?
Wirtschaftlichkeit
Stehen die angebotenen Gesamtkosten im Verhältnis zum angebotenen Leistungsumfang?

WAS WIRD WÄHREND DES FUNKE PASSIEREN? WAS MUSS ERREICHT WERDEN?

Für die erste Stufe werden jeweils für den Funded Track und für den Non-Funding Track bis zu sechs Teams ausgewählt.

Nach Abschluss der ersten Stufe demonstrieren alle Teams ihre erreichten Ergebnisse gegenüber der Jury. Die Jury entscheidet dann darüber, welche Teams (max. vier) jeweils des Funded Tracks und des Non-Funding Tracks in der zweiten Stufe weiter unterstützt werden. Die Entscheidung basiert auf den oben genannten Kriterien.

Entsprechend soll nach Abschluss der zweiten Stufe eine Auswahl der zwei verbleibenden Teams jeweils des Funded Tracks und des Non-Funding Tracks für Stufe 3 erfolgen.

Der dargestellte Ablauf stellt den aktuellen Planungsstand dar. SPRIND behält sich vor, im Verlauf des Funkes Änderungen vorzunehmen, vgl. dazu die Regelungen in der jeweiligen Teilnahmevereinbarung.

Am Ende der jeweiligen Stufe fasst das teilnehmende Team wesentliche Elemente des Entwicklungsstands in einem Bericht zusammen. Der Bericht soll beschreiben, ob das in der Bewerbung beschriebene Ziel erreicht wurde. Darüber hinaus soll das entwickelte geistige Eigentum (Know-how, Daten, Erfindungen etc.) skizziert und ggf. eine Liste der Veröffentlichungen ergänzt werden. Der Bericht ist sieben Tage vor Ende der jeweiligen Stufe einzureichen und unabhängig davon erforderlich, ob sich das Team für die nächste Stufe bewirbt oder nicht.

Die Teams können sich bei Fragen zur Entwicklung ihres Lösungsansatzes jederzeit an das SPRIND Challenge-Team wenden.

WER SIND DIE GEWINNER DES FUNKES?

Am Ende gewinnen alle zukünftigen Nutzer:innen, denn der Funke wird wichtige Impulse für die Entwicklung eines Konzepts für nutzerfreundliche, sichere und vertrauenswürdige EUDI Wallets liefern.

Die teilnehmenden Teams gewinnen auf vielfältige Weise: Im Rahmen des Funded Tracks werden die teilnehmenden Teams für die Arbeit an einem spannenden und innovativen Thema finanziert. Teams beider Tracks erhalten Unterstützung durch die SPRIND. So können sie ihre Ansätze einer breiten Öffentlichkeit bekannt machen und erhalten wertvolles Feedback von Expert:innen aus der Jury und dem Large Scale Pilot POTENTIAL. Nicht zuletzt haben ihre Arbeiten einen Impact, denn sie geben Impulse für die Ausgestaltung der zukünftige EUDI Wallet Infrastruktur in Deutschland (und darüber hinaus).

VERTRAULICHKEIT

SPRIND behandelt alle Einreichungen vertraulich. Die Teams, welche sich für den Funded Track und den Non-Funding Track qualifiziert haben, wurden öffentlich bekannt gegeben.

AN WEN KANN ICH MICH BEI WEITEREN FRAGEN UND RÜCKFRAGEN WENDEN?

Bei Fragen zum Funke wenden Sie sich an funke-eudi@sprind.org.