



Bundesamt
für Sicherheit in der
Informationstechnik

Deutschland
Digital•Sicher•BSI

Neues aus der Expert Group

OmniSecure, Berlin 22.05.2023

Gliederung

Funktion und Aufgabe der
Expert Group

Stand 2023: ARF und Referenz
Wallet

Weiteres Vorgehen



eIDAS Expert Group

Aufgaben, Funktion und Organisation



Rolle der Expert Group

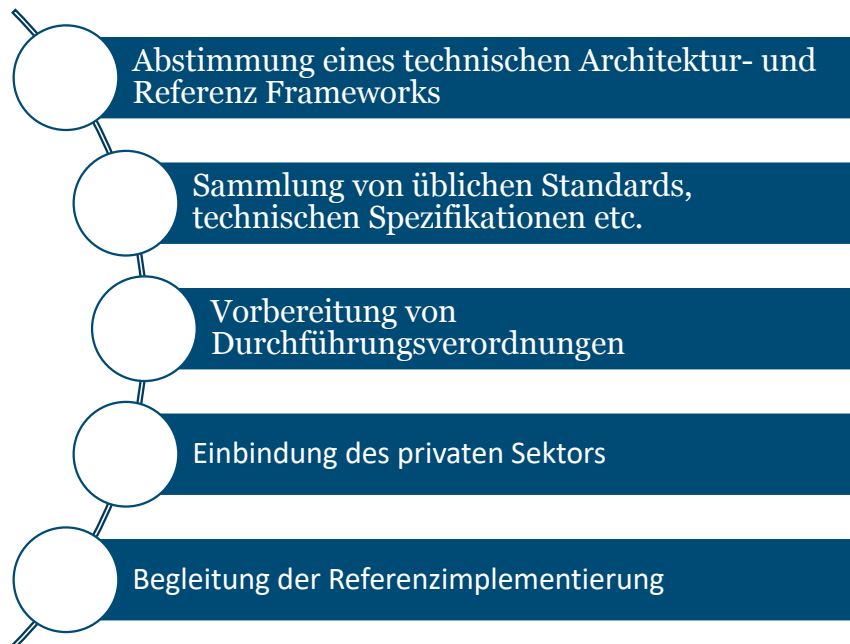
- Rechtsakt Artikel 6a (11):

Innerhalb von 6 Monaten nach Inkrafttreten dieser Verordnung legt die Kommission technische und betriebliche Spezifikationen und Bezugsnormen für die Anforderungen der Absätze 3, 4, 5 und 7a im Wege eines Durchführungsrechtsakts zur Umsetzung der EUID-Brieftasche fest. Dieser Durchführungsrechtsakt wird gemäß dem in Artikel 48 Absatz 2 genannten Prüfverfahren erlassen

- Entwicklung von Durchführungsakt durch Kommission
 - Technologien und Rahmenbedingungen für EUDI Wallet Entwicklung und Interoperabilität
- Gründung einer Expert Group zur Unterstützung und Beratung
 - Jeder Mitgliedstaat entsendet Experten
 - DE Vertreten durch BSI und BNetzA
 - Meinungen werden durch Konsens oder Mehrheitsvotum angenommen

Ein Staat, eine
Stimme

Ziele der eIDAS Expert Group



Soll den legislativen Prozess nicht vorwegnehmen oder stören.
Informationsfluss soll aber bestehen.

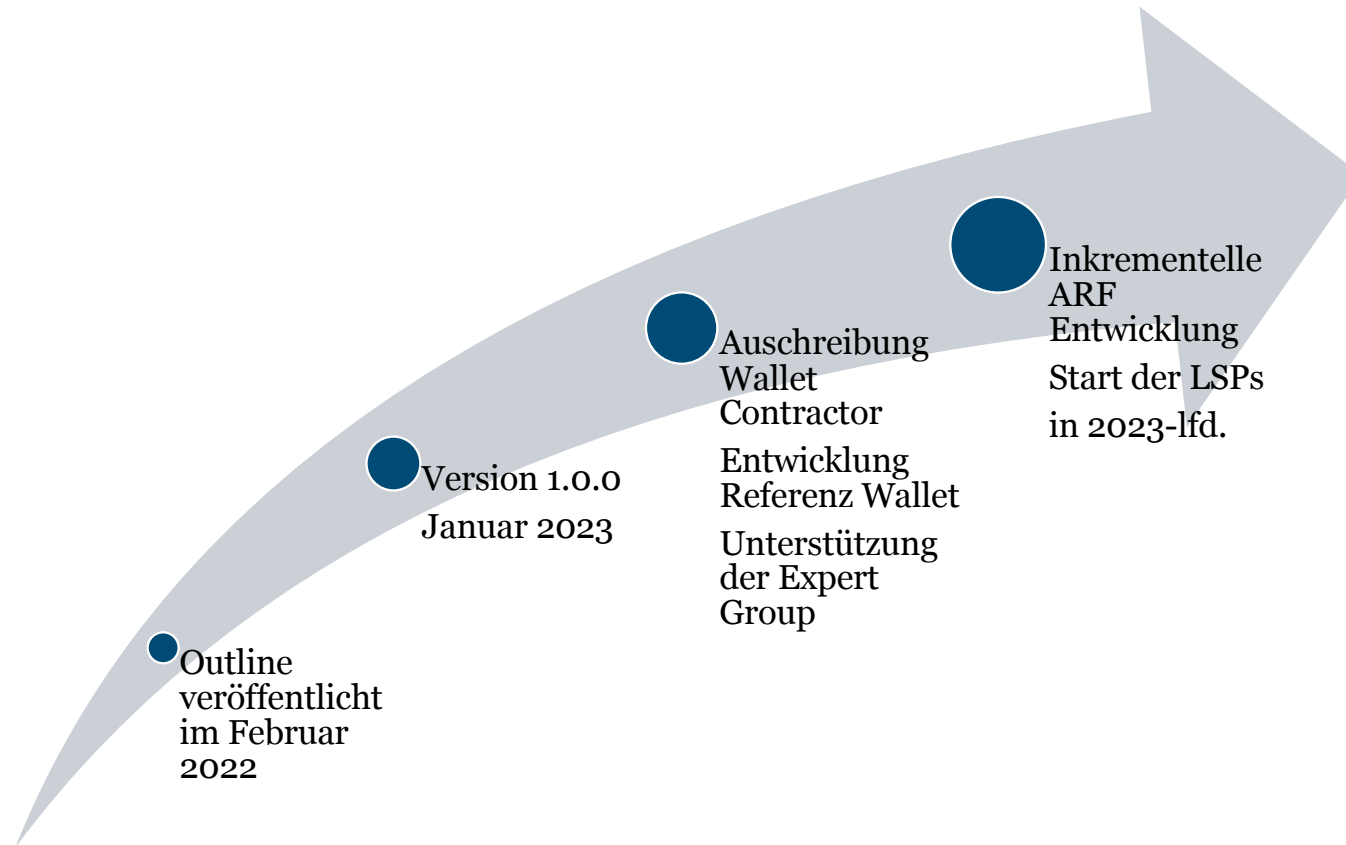
Stand 2023

ARF und Referenzimplementierung



Stand 2023

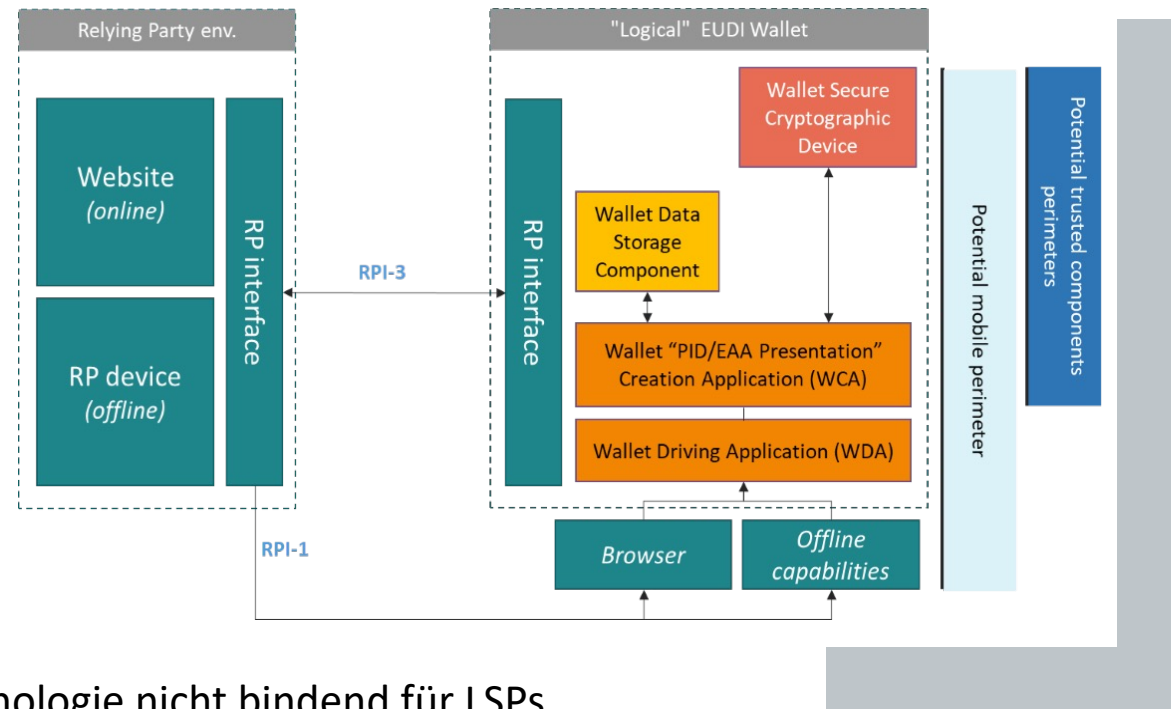
Aktueller Stand der Arbeiten



Stand ARF

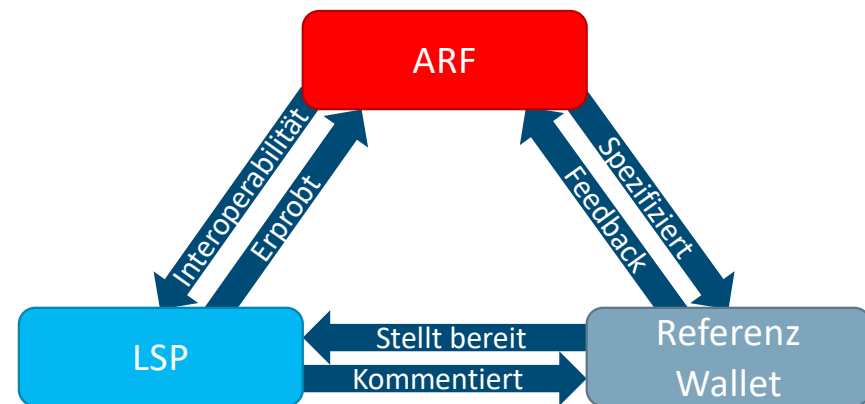
- ARF definiert Allgemeine Architektur
 - Unterteilung in mehrere Logisch (und z.T. physisch) abgetrennte Module
 - Z.B. Kryptographie auf SmartCard
- Etablierung von Profilen für Attestations
 - Verschiedene Anforderungen je nach Rahmenbedingungen
 - Potentiell verschiedene Technologiestacks
- Protokollvorgaben für Schnittstellen
 - ISO mDoc und OpenID4VP

➡ Fokus auf Referenzimplementierung: Technologie nicht bindend für LSPs



ARF, LSP und Referenzimplementierung

- ARF Spezifiziert Referenzwallet
 - Direktes Feedback zur umsetzbarkeit
 - ARF gibt Interoperabilitätsvorgaben für LSPs
 - Durch Spezifizierung von minimalen Technologieanforderungen
 - LSP erprobt (neue) Technologien
 - Erfahrungen fließen in ARF Technologien ein
 - LSP nutzt Referenzwallet
 - Erprobung der Referenz im Einsatz
- ➡ Die Stränge formen einen Symbiotischen Kreis
- Was in einem passiert beeinflusst die anderen



Weiteres Vorgehen

Weiterentwicklung ARF und Referenzwallet



Weiterentwicklung ARF

- ARF ist noch nicht Ausreichend
 - ARF beschreibt erst grobe Architektur und Schnittstellen
 - Z.B. Fehlen Sicherheitsvorgaben, Authentisierungsmechanismen, Vertrauensmodelle, etc.
- Inkrementelle Weiterentwicklung
 - Fehlende Themen in Backlog
 - Inkrementelle Updates zum ARF nach jedem abgearbeiteten Backlog Punkt
 - Updates alle 3-6 Wochen
- ARF Online Verfügbar auf GitHub
 - Kommentierung durch Externe Möglich (über Issues)

Unter Zulieferung
von Referenzwallet
Entwicklers

Backlog

EUDI Wallet User Journeys (eID, mDL)

EUDI Wallet rulebook authentication (PID, mDL)

EUDI Wallet Design Guide

Relying Party authentication

PID and mDL rulebooks – validity confirmation / revocation

EUDI Wallet Design Guide – Design Solutions on Data disclosure scenarios

EUDI Wallet attestation rulebook

Issuing a (Q)EAA to the EUDI Wallet

Pseudonym attestation

Presenting a (Q)EAA from the EUDI Wallet

Developing an EUDI Wallet Architecture (eSE, HSM, SmartCard)

Signing documents with EUDI Wallet



Vielen Dank für Ihre Aufmerksamkeit!

Kontakt

Frederic Kehrein
Referent DI 12

frederic.kehrein@bsi.bund.de

Tel. +49 (0) 228 9582 5051

Mobil +49 (0) 160 9814 2888

Bundesamt für Sicherheit in der Informationstechnik (BSI)
Godesberger Allee 185-189
53175 Bonn

www.bsi.bund.de



Bundesamt
für Sicherheit in der
Informationstechnik

Deutschland
Digital•Sicher•BSI

Das BSI als die Cyber-Sicherheitsbehörde des Bundes gestaltet Informationssicherheit in der Digitalisierung durch Prävention, Detektion und Reaktion für Staat, Wirtschaft und Gesellschaft.

Deutschland
Digital•Sicher•BSI