

ONCE

Online einfach anmelden

Programm / Ausschreibung	IKT der Zukunft, IKT der Zukunft, IKT der Zukunft - bilateral	Status	abgeschlossen
Projektstart	15.07.2021	Projektende	31.12.2023
Zeitraum	2021 - 2023	Projektlaufzeit	30 Monate
Keywords	digitale Identitäten; Privatsphäreschutz; Sicherheit mobiler Geräte		

Projektbeschreibung

Das Rahmenprojekt ONCE beschäftigt sich mit dezentralen, benutzerzentrischen, offenen ID-Wallets, die verschiedene digitale Identitäten vereinen und z.B. zur gesicherten Anmeldung an Webservices dienen (Self-Sovereign-Identities, SSI). Dabei sind vertrauenswürdige ausstellende Behörden im Fokus, wobei eine digitale Identität vom Benutzer selbstbestimmt aus beliebigen Quellen (auch mit unterschiedlichem Vertrauensniveau) zusammenstellbar ist und das entstehende ID-Ökosystem allen möglichen Ausstellern und Akzeptanzstellen digitaler Identitäten offensteht. Das CDL Digidow beschäftigt sich mit der Verwendung solcher bereits ausgestellten Identitäten in der physischen Welt, also z.B. zum Öffnen von Türen oder der Benützung von Verkehrsmitteln. ONCE und Digidow teilen viele der Ziele z.B. im Bereich Privatsphärenschutz durch einen bewussten, selbstbestimmten Umgang mit der eigenen digitalen Identität und durch den Ausschluss massiver zentraler Datensammlung bereits auf der technischen Ebene, sind aber orthogonal in Bezug auf den konkreten Forschungsfokus.

Ziel ist eine Verbindung beider Projekte, um bestmögliche Synergien für die künftige Nutzung digitaler Identitäten in der breiten Gesellschaft zu erzielen.

Angestrebgt wird einerseits, die verteilten, dezentralen „Personal Identity Agents“ aus dem CDL Digidow als ID-Wallets bzw. IdPs in ONCE nutzbar zu machen und damit die Ziele und Nutzbarkeit beider Projekte zu verbinden. Dieser Projektantrag soll genau diese Brücke ermöglichen. Neben der prinzipiellen Herausforderung, zwei neuartige Mobile-ID-Ansätze mit divergierendem Anforderungsprofil wechselseitig interoperabel zu verbinden, ergibt sich die wesentliche offene Forschungsfrage, wie digitale Identitäten sicher auf aktuellen Smartphone-Plattformen gespeichert und verwendet werden können, wenn dabei nicht kategorisch nur die Schutzziele des höchsten, im gesamten ID-Ökosystem vorkommenden Vertrauensniveaus beachtet werden sollen.

Andererseits ergibt sich daraus die Notwendigkeit, Sicherheitsmerkmale von (Android-) Smartphones quantitativ zu erfassen und auszuwerten, um eine Eignung zum Betrieb dieser verbindenden ID-Wallets/Agents adaptiv an den Schutzbedarf konkreter Anwendungsfälle zu bestimmen. Gleichzeitig ergibt sich aus solchen Metriken auch die Basis für eine transparente, longitudinale Darstellung der Sicherheit von Smartphones und der Pflege dieser Sicherheit durch den Hersteller (z.B. in Form von Updates). Diese neuartige Möglichkeit zur transparenten Bewertung und zum direkten Vergleich von Smartphones kann somit eine Anreizwirkung zu nachhaltiger Pflege und Umgang mit dem Produkt „Smartphone“

schaffen. Dieses Projekt wird daher für die öffentliche, für Endnutzer verständliche Aufbereitung dieser Daten in Form einer öffentlich zugänglichen Transparenzdatenbank sorgen.

Abstract

The BMWi project ONCE aims to build decentralized, human-centric, open ID wallets to unify and manage multiple different digital identities of an individual. While the use of digital services with identities issued by trusted governmental entities is the main focus, the evolving ecosystem should remain open to other (potentially less trusted) issuers and users/verifies of such identities (also called relying parties) in the sense of self-sovereign identity (SSI). The CDL Digidow primarily focuses on the use of digital identities in the physical world, e.g. to open doors or travel on public transport. While ONCE and Digidow share all of the most important core principles – particularly an explicit, self-sovereign, data minimization driven approach to digital identity without massive, centralized instances of data collection – and put privacy and individual control in their focus, they are orthogonal in their respective research focus areas.

Our main goal is to bridge these two projects to enable optimal and obvious synergies in the creation, management, and use of digital identities for a broad population.

First, we will enable the distributed, decentralized “Personal Identity Agents” developed within the scope of Digidow to act as decentralized ID-Wallets (or IdPs) in ONCE, combining the usefulness of both projects for a significantly wider range of application scenarios. The present project proposal aims to create this specific bridge. In addition to the challenge of making two novel approaches towards digital identity interoperable, this raises a new open research question: how to securely store and use digital identities on existing smartphone platforms without necessarily enforcing the highest possible security level on all participants, independently of their device capabilities or use case requirements.

Second, to answer this new research question, we will quantitatively measure and analyze security attributes of (Android) smartphones to evaluate their applicability towards hosting ID-Wallets/Agents adapted to the respective use cases. A transparent, longitudinal analysis and publication of such security metrics also forms the basis for comparing smartphones by different manufacturers, e.g. based on their historic update behavior or available security features over time. This in turn creates incentives towards more sustainable maintenance and use of the product “smartphone”. Our proposed project therefore goes well beyond the primary goal of bridging the digital identity approaches of ONCE and Digidow and will enable the publication of a public transparency database targeting end users to aid their responsible purchase and use of smartphones, impacting a wide range of security and privacy critical smartphone applications.

Projektpartner

- Universität Linz