Openkex onepager netidee

Projektziele

openKex ist eine offene, dezentral kontrollierte Infrastruktur für digitale Identitäten, mit der Menschen sich eine dauerhafte, „digitale Existenz“ schaffen können, die durch ein eigenes Hardware Modul abgesichert werden kann. (Volks-HSM). Damit können bestehende digitale Identitäten (Social Media Identitäten, Zertifikate, ...) datensparsam unter zweckgebundenen Identitäten verlinkt werden. Verbindungen zu Kontakten können für sicheren Datenaustausch hergestellt werden, ohne dass Kontakt-Daten von Plattformen abgezogen und verwertet werden.

Vertrauensdienste, Intermediäre oder zentrale Plattformen haben keine vorgegebene Rolle bei openKex, denn die Teilnehmer entscheiden selbst darüber, ob und durch welche Nachweise Vertrauen entsteht und welche Dienste und Vermittler sie dafür brauchen. In unserer zunehmend digitalisierten globalen Welt, in der es immer schwieriger wird, Anbieter auszutauschen, denen nicht mehr vertraut wird, bietet openKex eine wichtige Brückentechnologie mit der Menschen ihre digitale Existenz und damit auch ihre Daten nachhaltig absichern können.

Erreichte Projektendergebnisse

Lizenz: GNU General Public License, Version 3.0 (GPLv3)
Repositories: https://github.com/openKex/netidee

- E1: Schlüsselmanagement Client (kex App): Design Studie, API
- E2: Referenzimplementierung einer Applikation mit Kontaktbuch-Integration: Design Studie
- E3: **Kryptospeicher Paket** (VolksHSM): Library, API
- E4: Infrastruktur Paket und Referenzimplementierung für Knoten: API, Whitepaper
- E5. Security Review: Bericht
- E6. User Test: Bericht

künftige Erweiterungsmöglichkeiten bzw. Nutzung für andere Einsatzbereiche durch Dritte

Digitale Anwendungen mit denen Daten verschlüsselt gespeichert oder ausgetauscht werden sollen, gewinnen mit openKex eine nutzerzentrierte, datensparsame Sicherheitsebene für das dazu erforderliche Kontakt- und Identitätsmanagement.

Von der Integration mit openKex profitieren Entwickler von Diensten, wenn sie Datensparsamkeit und Sicherheit beweisen und Einstiegsbarrieren minimieren wollen. Weil Nutzer damit Dienste direkt mit ihren selbstverwalteten Identitäten und Kontakten verwenden können, ist es schon „per Design“ technisch ausgeschlossen, dass ein System oder eine Anwendung ohne Wissen und Zustimmung des Nutzers Zugriff auf dessen Schlüssel, Daten oder Kontakte hat.