SovereignID

Endbericht | Call 12 | Projekt ID 2186

1. Einleitung 3

2. Projektbeschreibung 3

Personal XDI Server 3

Backup/Restore Funktionen für das Freedombox OS 4

XDI-Core Libraries + Android UI 4

3. Verlauf der Arbeitspakete 5

3.1.Arbeitspaket 1 - Erstellung der Debian Pakete 5

3.2.Arbeitspaket 2 – Integration des XDI Moduls 5

3.3.Arbeitspaket 3 – Erweiterung der WebUI 5

3.4.Arbeitspaket 4 – Erweiterung der Android-App 6

3.5.Arbeitspaket 5 – Erstellung eines Backup-Moduls 6

3.6.Arbeitspaket 6 – Externkommunikation 7

4. Liste Projektendergebnisse 8

5. Verwertung der Projektergebnisse in der Praxis 8

Allgemeine Hinweise zum Betrieb einer Freedombox 8

6. Öffentlichkeitsarbeit/ Vernetzung 9

7. Geplante Aktivitäten nach netidee-Projektende 11

8. Anregungen für Weiterentwicklungen durch Dritte 11

1. Einleitung

Es ist mittlerweile hinlänglich bekannt, dass personenbezogene Daten von Konzernen und staatlichen Akteuren als eine Art Rohstoff ("das neue Öl") betrachtet werden. Alle bisherigen Konzepte einer digitalen Identität, vom Facebook-Account bis zur Bürgerkarte, basieren auf der zentralen Speicherung und Kontrolle solcher Daten.

Seit einigen Jahren etablieren sich jedoch immer stärker dezentrale Modelle und die Idee der "souveränen Identität", das bedeutet dass nur ein Individuum selbst seine digitale Identität erstellen, verwenden, und auch wieder zerstören kann. Moderne Technologien wie die "Sovrin" Blockchain und das "XDI" Datenprotokoll erlauben es diese Vision zu realisieren, allerdings sind diese für die meisten Personen nur schwer zugänglich.

Wir sind seit einigen Jahren an der Entwicklung der FreedomBox beteiligt. Wir arbeiten außerdem aktiv an der Sovrin Blockchain sowie am XDI Protokoll mit, und nehmen regelmäßig an Veranstaltungen im In- und Ausland Teil, um die Idee der souveränen Identität sowie die Technologien zu verbreiten.

Im Gegensatz zu anderen Blockchain-basierten Identitätslösungen (siehe Liste http://bit.ly/2ue1uxi) wurden Sovrin und XDI speziell für diesen Anwendungsfall entwickelt. Die FreedomBox ist als langfristiges, stabiles und sicheres open-source Projekt eine ideale Basis für digitale Identäten.

2. Projektbeschreibung

Wir haben in diesem Projekt eines der bekanntesten Betriebssysteme für Personal Homeserver Applications - das Freedombox OS (https://freedombox.org) - um mehrere Funktionen erweitert:

Personal XDI Server

Alle Nutzer:innen der Freedombox Software sind nun in der Lage sogenannte "Self Sovereign Identities" (SSI) direkt von ihrem persönlichen Heimserver aus zu hosten und völlig unabhängig von einem zentralen Identitäts-Provider (also ohne "Facebook/Google/Amazon/Apple Login") zu verwalten.

Dabei kommen in diesem Projekt die derzeit ausgereiftesten Technologien für die Verwaltung von SSIs zum Einsatz:

1) Decentralized IDs - kurz DIDs - entwickelt vom World Wide Web Consortium - W3C (https://w3c-ccg.github.io/did-spec/).

2) XDI - ein Protokoll zur Kommunikation von "Distributed Semantic Data Graphs" basierend auf DIDs. (https://xdi2.org)

XDI wurde vom OASIS Konsortium innerhalb des XDI Technical Committees entwickelt und zählt zu den derzeit umfangreichsten Protokollen zur Verwaltung von SSI Informationen (https://www.oasis-open.org/committees/tc_home.php?wg_abbrev=xdi).

Anwendungsfälle:

- Hosting von öffentliche Schlüsselinformationen für Public-Key-Based-Login und E2E Encryption

- digitale Beglaubigungen, sogenannte Verifiable Claims

Damit können Funktionen die im Moment nur von zentralen Diensten (zB https://keybase.com) angeboten werden auch selbst gehostet und verwaltet werden.

Backup/Restore Funktionen für das Freedombox OS

1. Freedombox Core backup support functionality

2. Remote Storage Options + SSHFS mount

3. UP/DOWN Streaming (large files support)

[4. XDI home directory backup/restore]

Die letzte Funktionalität ist vorbereitet aber nicht im UI verfügbar gemacht - denn sie hat aufgrund der Paket-Abhängigkeiten keine Chance auf Aufnahme in "Out of the Box" Experience von Freedombox - d.h. sie wäre nur technisch sehr versierten Nutzern zugänglich. Das hat uns dazu bewogen die Implementierung der Arbeit an allgemeinen Backup Funktionen (1-3) dem Punkt 4 vorzuziehen.

XDI-Core Libraries + Android UI

Diese Bibliotheken ermöglichen den entfernen Zugriff auf die Sovrin/XDI Funktionalität der FreedomBox von einer JAVA-basierten Platform aus. Sie erlauben es einzelnen Personen, ihre “souveräne” digitale Identität zB auch vom Smartphone aus zu verwalten.

3. Verlauf der Arbeitspakete

3.1.Arbeitspaket 1 - Erstellung der Debian Pakete

Hauptätigkeit: Programmierung von Debian-Paketen für Sovrin; Programmierung von Debian- Paketen für XDI.

Es wurde ein Debian-Paket für XDI programmiert, dieses ist in Github verfügbar:

https://github.com/peacekeeper/debian-xdi2-selfhosted/tree/debian

Dieses Debian-Paket wird von einem Build-Server automatisch gebaut:

http://debian-dev.freedombox.at:8080/

Der Build-Server kann als Repository in die FreedomBox eingebunden werden, siehe hier für technische Informationen:
http://debian-dev.freedombox.at/

Ein Debian-Paket für Sovrin (genauer: Hyperledger Indy-SDK, das ist der Open-Source Code von Sovrin) ist ebenfalls verfügbar:

https://github.com/hyperledger/indy-sdk/tree/master/libindy/debian

Es gab keine nennenswerten Probleme bzw. große Abweichungen vom Plan.

3.2.Arbeitspaket 2 – Integration des XDI Moduls

Hauptätigkeit: Integration der Debian-Pakete für Sovrin/XDI in die FreedomBox-Architektur und die FreedomBox WebUI

Wie geplant wurde das XDI Debian-Paket in die 'Plinth' Weboberfläche integriert.
Das Installieren, starten und stoppen von XDI ist somit einfach über die Weboberfläche per Mausklick möglich.

Link: https://salsa.debian.org/fonfon-guest/plinth/tree/xdi
Es gab keine nennenswerten Probleme bzw. große Abweichungen vom Plan.

3.3.Arbeitspaket 3 – Erweiterung der WebUI

Hauptätigkeit: Erweiterung des Moduls für die FreedomBox WebUI (“Plinth”) zur Verwaltung von Sovrin/XDI Identitäten.

Entgegen dem ursprünglichen Plan haben wir beschlossen, die Verwaltung von Identitäten und Identitätsdaten nicht direkt in Plinth zu integrieren.

Stattdessen implementieren wir in Plinth die entsprechenden Schnittstellen — die eigentliche Verwaltung erfolgt dann per Smartphone App.

Diese Schnittstellen sind nun implementiert und funktionstüchtig.

3.4.Arbeitspaket 4 – Erweiterung der Android-App

Hauptätigkeit: Erweiterung einer bereits existierenden (FreedomBox-) Android-App, um die Sovrin/ XDI Funktionalität per Smartphone nutzen zu können.

Die Evaluierung der aktuellen Android-App (https://github.com/freedombox/android-app) führte zur Erkenntnis dass es kaum nennenswerte Synergie-Effekte haben würde dieses Repository als Basis zu verwenden. Wir haben uns daher entschlossen ein Template zu bauen welches für die Implementierung der XDI-Funktionen besser geeignet ist.

Folgende grundsätzliche Problematik ergab sich bei der Entwicklung des Android UIs:

Wir gehen davon aus dass “DID Master-Keys” zu Beginn (zumindest kurzzeitig) immer auf dem mobilen Computing Device vorliegen müssen (bzw den elektronischen Hilfsmitteln die zur “DID Creation” notwendig sind).

Dieser Master Key sollte laut DKMS Design Doc V4 (https://github.com/hyperledger/aries-rfcs/tree/master/concepts/0051-dkms) aber immer folgendermaßen behandelt werden:

“saved offline” in secure offline storage, or a highly secure encrypted vault, such as a secure element, TPM, or TEE. “sharded” using a technique such as Shamir secret sharing or derived from secure multiparty computation.

Beide Optionen sind im geplanten Kontext (Nutzung auf Android) nicht durchführbar OHNE dabei durch "offline saving" einen deutlich höheren Sicherheits-Technischen Aufwand zu generieren, oder bei "sharded" von einem bereits existierenden Netzwerk für Vertrauliche Kommunikation abhängig zu sein.

Um die XDI Funktionen des Servers von einem Smartphone aus "sicher und einfach" benutzen zu können wird empfohlen die im Projekt entwickelten Bibliothek in ein bereits bestehendes OpenSource Identity-Wallet-Framework zu integrieren. Die uns bekannte beste Option dafür ist im Moment connect.me von Evernym https://github.com/sovrin-foundation/connector-app welche vor kurzem veröffentlicht wurde.

3.5.Arbeitspaket 5 – Erstellung eines Backup-Moduls

Hauptätigkeit: Erstellung eines Moduls für die FreedomBox-WebUI (“Plinth”), das das Absichern und Wiederherstellen von Sovrin/XDI Identitätsdaten ermöglicht.

Dieses Backup-Modul geht nun über die von uns geplante Funktionalität hinaus: Es kann sowohl Dateisystem-Snapshots zur Absicherung und Wiederherstellung eines laufenden Systems machen, als auch eine Import/Export-Funktionalität für die Daten einzelner FredomBox-Apps bieten.

Es wurden zahlreiche, lokale Backup Funktionen (local FS mount, USB Sticks, etc) implementiert. Auch Backups auf anderen Servern (via SSHFS) sind nun möglich mit jeder Standard-Installation einer Freedombox. Yay!!!

Für dezentrale, selbst verwaltete Backups sind sogenannte "cooperative storage clouds" eine naheliegende Lösung. Die meisten Software-Projekte in diesem Bereich sind noch im Alpha-Stadium, und es sind noch einige offene Fragen zur Administration und Koordination solcher Backup-Lösungen zu klären - die Integration eines dezentralen Backups wird also im Rahmen dieses Netidee-Projekts nicht mehr möglich sein (und war auch nicht Teil des ursprünglichen Plans).

3.6.Arbeitspaket 6 – Externkommunikation

Wir sind in mehrere relevante Communities eingebunden, die sich mit digitaler Identität bzw. verwandten Themen wie persönliche Daten und Privatsphäre beschäftigen, und wir haben an mehreren Konferenzen und sonstigen Veranstaltungen teilgenommen, um die Ideen und Technologien dahinter zu verbreiten bzw. Austausch vorzunehmen.

Im März 2018 hat Markus beim diesjährigen Elevate Festival die Grundidee hinter dem SovereignID Projekt vorgestellt.

Link: https://elevate.at/diskursprogramm/e18riotmatrix/
Weiters haben wir am 3. Blockchain Community Treffen der Stadt Wien (30. Juli 2018) zwei kurze Vorträge gehalten. Ebenfalls vertreten waren wir bei der MyData Konferenz in Helsinki im August 2018 und beim ISPA Blockchain Summit am 12. September 2018

Markus Sabadello hat an zahlreichen internationalen Konferenzen zum Thema teilgenommen und dort das Projekt international sichtbar gemacht/präsentiert:

- Internet Identity Workshop (https://internetidentityworkshop.com/past-workshops/)
- Rebooting Web-of-Trust (https://www.weboftrust.info)
- MyData 2018 (https://mydata2018.org)

4. Liste Projektendergebnisse

1	Debian-Pakete für Sovrin und XDI	AGPL	http://debian-dev.freedombox.at/debian/release/sid/
2	Modul für FreedomBox WebUI (“Plinth”) für Sovrin/XDI	AGPL	https://salsa.debian.org/fonfon-guest/plinth/tree/xdi
3	Modul für FreedomBox WebUI (“Plinth”) für Backup-Funktion	AGPL	https://salsa.debian.org/fonfon-guest/plinth/tree/package-version
4	XDI-App	GPLv3	https://github.com/paulfuxjaeger/SovereignID-Android

5. Verwertung der Projektergebnisse in der Praxis

Die FreedomBox ist ein langfristiges Software-Projekt das von einer internationalen Community getragen wird. Durch die Bereitstellung der Software über Debian ist die Installationsmöglichkeit über Jahre hinweg gewährleistet. Die Entwicklung der Sovrin-Blockchain wird von der Linux Foundation (Hyperledger) unterstützt. Die Knoten der Blockchain werden weltweit verteilt von großen, stabilen Institutionen wie Banken, Universitäten, Staaten, und internationalen Organisation betrieben (Prinzip von "Diffuse Trust”).

Falls das Sovrin Projekt trotz seiner langfristigen Ausrichtung scheitert kann auch jede andere, öffentliche Blockchain verwendet werden. Es ist zu erwarten, dass die Idee der souveränen Identität massiv an Bedeutung gewinnen wird, und dass sich durch Partnerschaften und ein internationales Ökosystem viele Möglichkeiten ergeben, auf unserem Projektergebnis aufzubauen und unsere Arbeit nachhaltig zu finanzieren und auszubauen.

Allgemeine Hinweise zum Betrieb einer Freedombox

Solch ein Server kann ohne Probleme im eigenen Wohnbereich betrieben werden. Dafür reicht ein kleiner Single-board Computer (https://wiki.debian.org/FreedomBox/Hardware) der mit sehr geringen Anschaffungs- und Betriebskosten verbunden ist, bzw auch direkt vorkonfiguriert um ca 80 Euro von der Freedomboxfoundation gekauft werden kann:

https://freedomboxfoundation.org/buy/

6. Öffentlichkeitsarbeit/ Vernetzung

Wir schätzen die Bedeutung von Öffentlichkeitsarbeit in diesem Projekt sehr hoch ein, denn:

Das Konzept der “Souveränen Digitalen Identität” unterscheidet sich grundlegend von den Ansätzen die bisher in diesem Bereich verwendet werden. Dieser große **strukturelle Unterschied** macht es schwierig das Konzept in 2min einfach verständlich zu erklären.

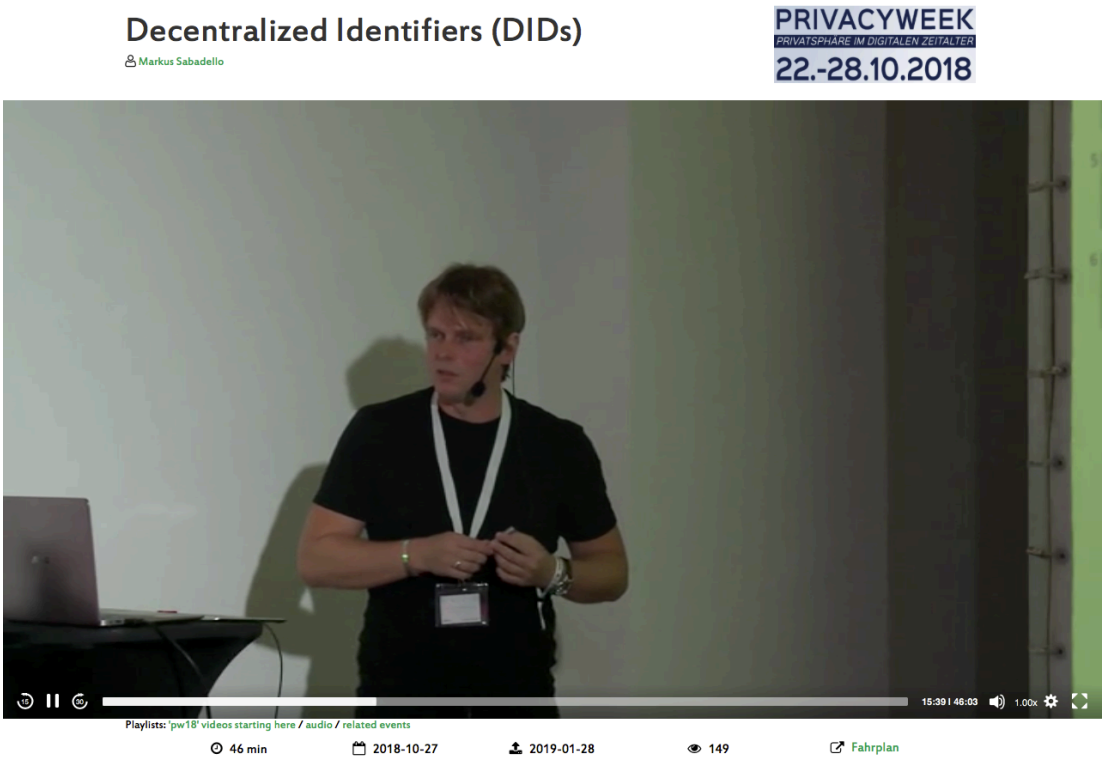
Das Konzept funktioniert nur wenn Netzwerk Effekte genutzt werden können und erfordert deswegen eine **breite Unterstützung in der Early Adopter Community** im Bereich der dezentralen Internet Infrastruktur. Solche Menschen finden und ansprechen, darum ging es uns:

Vortrag beim “Netzpolitischen Abend” - Grundkonzepte von DIDs und Self Sovereign Identity - 04.10.2018

https://www.youtube.com/watch?v=gt9nxdfvX8k&feature=youtu.be&t=4001

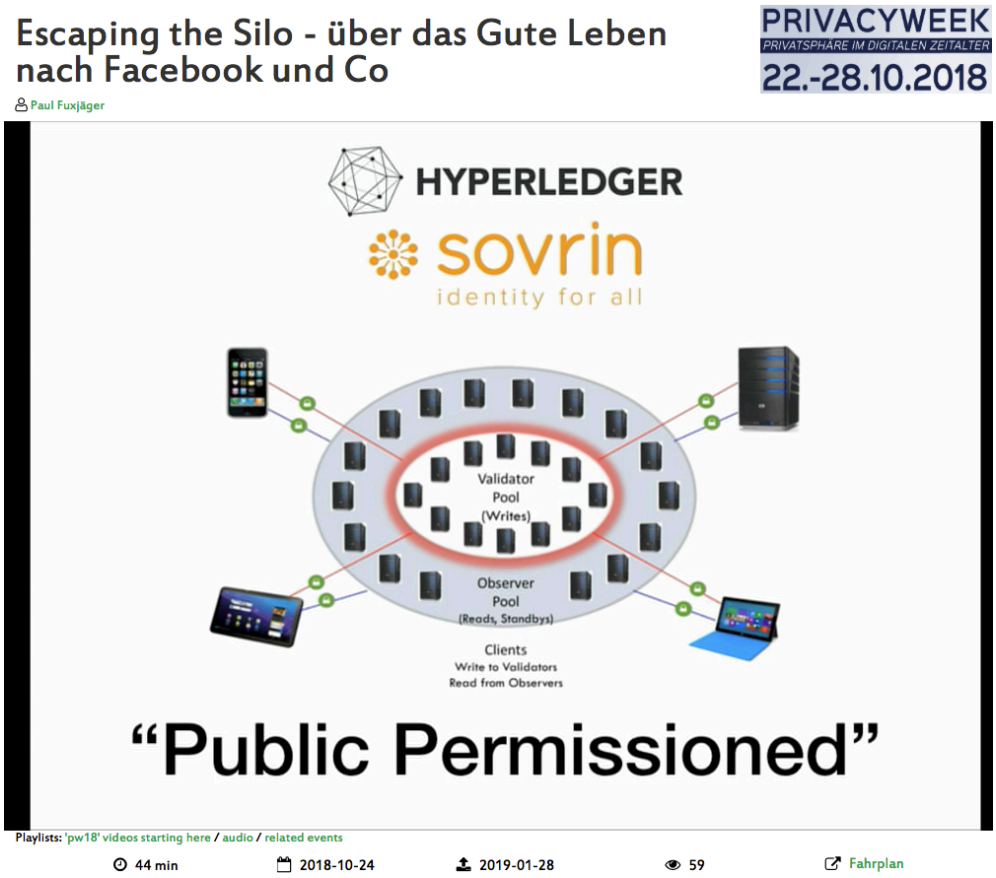
Vortrag auf der PrivacyWeek - Decentralized Identifiers (DIDs) - 27.10.2018

https://media.ccc.de/v/pw18-25-decentralized-identifiers-dids-



Vortrag auf der PrivacyWeek - Escaping the Silo - über das Gute Leben nach Facebook und Co - 24.10.2018

https://media.ccc.de/v/pw18-101-escaping-the-silo-ber-das-gute-leben-nach-facebook-und-co



Interview auf Radiosender FM4 - Sendung: Homebase

https://soundcloud.com/burstup/decentralized-identifier-interview-mit-paul-fuxjager-c3w-privacy-week-fm4mp3

Vortrag auf der TU WIEN - Auf Einladung haben wir das Konzept in der LVA "Privacy Enhancing Technologies - PET" vorgestellt - 29.11.2018

https://tiss.tuwien.ac.at/course/courseDetails.xhtml?dswid=2478&dsrid=680&courseNr=188982

Vortrag beim Hyperledger Meetup Vienna - Meetup #6: Identity for All - 16.10.2018

https://www.meetup.com/Hyperledger-Vienna/events/255191300/

7. Geplante Aktivitäten nach netidee-Projektende

Die Ergebnisse dieses Projekts (alle DID-relevanten Erkenntnisse und Funktionen) kommen direkt zur Anwendung im Projekt MastodonID (https://netidee.at/mastodonid). Dort statten wir das derzeit größte verteilte Soziale Netzwerk mit den DID Schnittstellen aus die wir in SovereignID entwickelt haben.

Wenn die Integration in den Mastodon Stack gelingt wird der bisher größte Nachteil von verteilten Sozialen Netzwerk Systemen - die langfristige Abhängigkeit von einzelnen Server-Instanzen - erstmals vollständig auflösbar. Das Netzwerk wird dadurch deutlich robuster gegenüber den bereits aufflammenden SPAM/Harassment Attacken.

8. Anregungen für Weiterentwicklungen durch Dritte

Um die XDI Funktionen des Servers von einem Smartphone auch **mit ausreichender Sicherheit** benutzen zu können sollten die XDI Bibliotheken in ein modernes Open-Source Identity-Wallet-Framework integriert werden. Dadurch ist sichergestellt dass die notwendigen Sicherheitsmaßnahmen auf der Mobilen Plattform eingehalten werden können (siehe https://github.com/hyperledger/aries-rfcs/blob/master/concepts/0051-dkms/dkms-v4.md Kapitel 7 und 8).

Besonders geeignet dafür ist das connect.me Framework welches speziell für Sovrin/ HyperledgerIndy entwickelt wird und vor kurzem auch als erweiterbare Android App veröffentlicht wurde: https://github.com/sovrin-foundation/connector-app