MastodonID

Endbericht | Call 13 | Projekt ID 3888

Inhalt

1. Einleitung

Nutzer:innen des alternativen Social Microblogging Netzwerks Mastodon erhalten mit dieser Erweiterung die Möglichkeit eine dezentrale Identitäts-Referenz (im W3C standardisierten Format einer Decentralized Identity (DID)) ihrem Account hinzufügen und eigenständig zu verwalten.

Damit wird es für die Teilnehmer:innen eines Mastoden-Netzwerks prinzipiell möglich "Seamless" zwischen Instanzen innerhalb eines Mastodon Netzwerkes zu wechseln: denn die bereits aufgebauten Verbindungen - in der Twitter Terminologie ist das die Liste der “Followers” - brechen bei einem Umzug nicht wie üblich ab - sondern können langfristig beibehalten werden.

Denn die Verknüpfungen zwischen den Einträgen im Domain-Name-System (welche von Admins kontrolliert werden) und der “Identität” eines individuellen Mastodon Accounts sind dann nicht mehr entscheidend sind für die Erreichbarkeit innerhalb des Netzes.

Damit wird das Problem der langfristigen Abhängigkeit von einzelnen Server-Instanzen im derzeit erfolgreichsten "Alternative Social Media Network” abgeschwächt. Solche Netzwerke können sich dadurch - auch gegenüber Twitter - als gleichwertige, robuste Alternative beweisen.

In Folge können diese föderal strukturierten Netzwerke - als Gegenvorschlag zu zentralisierten Plattformen - auch außerhalb von kulturellen Nischen an Bedeutung gewinnen.

2. Projektbeschreibung

Wir haben das interne Mastodon Datenbankmodell so erweitert, dass die Möglichkeit besteht einzelne Benutzer des Netzwerks mittels DIDs zu adressieren. Weiters haben wir den DID Universal Resolver - mit Hilfe von Docker Containern – mit geringem Aufwand in eine Mastodon Instanz integrierbar gemacht, um damit jederzeit und vollständig unabhängig DIDs auflösen zu können und damit den gesammelt “sozialen Graphen” auch nach einem Umzug aktuell halten zu können - auch bei sehr schnell steigenden Zuwachszahlen im Netzwerk - die wir wohl in naher Zukunft erwarten dürfen (z.B. nach Änderungen der Moderations-Regeln bei Twitter bei einem Eigentümerwechsel).

Es gibt zu unserem Ansatz eine historische Parallele: die Portabilität von Mobiltelefonnummern! Ursprünglich waren diese Nummern im Eigentum des Mobilfunkbetreibers und wurden an Kunden lediglich “vermietet”. Erst seit der Einführung des “NÜV Standards” können Menschen ihre Nummern mitnehmen, wenn sie den Anbieter wechseln.

Im Zuge des Projekts wurde der Universal Resolver dahingehend weiter entwickelt, dass nun mehr als 30(!) DID Methoden unterstützt werden. Diese Basiskomponenten sind (ähnlich zu BIND für DNS) notwendig, um die verknüpften DID Dokumente auflösen zu können, basierend auf der W3C DID Core Spezifikation (https://www.w3.org/TR/did-core/).

Weiters wurde die Entwicklungs-Pipeline für den Resolver im Laufe des Projektes deutlich verbessert:

https://github.com/decentralized-identity/universal-resolver/blob/main/docs/continuous-integration-and-delivery.md

Und das Main Repository des Resolvers wird zur verbesserten langfristigen Absicherung der offenen Entwicklung der Codebasis seit Juli 2020 von der Decentralized Identity Foundation https://identity.foundation gehostet.

(Die DIF ist eine in den USA registrierte Nonprofit [501(c)(6)] Organisation mit dem Ziel das offene Ökosystem rund um DID/VC Standards zu fördern. Alle DIF Projekte haben eine Apache 2 Lizenz, die Patent-Regeln werden vom W3C übernommen, und jeglicher Content ist CC-BY lizensiert.)

Für die Blockchain- bzw. DID-Communities ergibt sich durch unser Projekt ein wichtiger Mehrwert, da eine prinzipiell Massentaugliche Anwendung auf Basis der DID-Infrastruktur mit direkt erkennbarem Nutzen entstand. Stärken und Schwächen des DID-Konzepts konnten früher erkannt und damit der DID/VC Standardisierungsprozess am W3C unterstützt werden.

Ein zu überwindendes Problem für die breite Etablierung von DID-enabled Networks bestand also “nur” noch darin, dass sich große Teile der internationalen Entwickler-Community im Bereich der alternativen sozialen Netzwerke (Mastodon und viele andere die sich den Überbegriff Fediverse teilen) in den letzten 3 Jahren mehrheitlich dahingehend entwickelt haben, Konzepte *strikt abzulehnen* wo “Token Rewards” (fungible or non-fungible) oder “Proof-of-Work” zum Einsatz kommen.

Es ist also gerade ein Kulturkampf im Gange - wo es aber laut unserer Analyse - im Kern um zwei entgegengesetzte und letztendlich inkohärente Rechts-Philosophische Positionen beim Thema “Regulierung einer öffentlichen Kommunikations-Infrastruktur” (bzw eines public permissionless DLTs) geht:

- PrivilegierteKontrollmöglichkeit über die gemeinsame Datenbank ist ***grundsätzlich abzulehnen, egal in welchem Kontext***, weil sonst Missbrauch dominiert.
- Privilegierte Kontrollmöglichkeit über die gemeinsame Datenbank ist ***grundsätzlich notwendig, egal in welchem Kontext***, weil sonst Missbrauch dominiert.

Wir haben während der Pandemie (2020-2022) eine Verschärfung dieser Entwicklung beobachtet und es wurde immer deutlicher, dass wir die maßgeblichen Haupt-Entwickler:innen des aktuellen Mastodon Main Repositories (ca 90% des Netzes bauen zur Zeit auf dieser gemeinsamen Codebase auf) *nur dann* für eine Kopplung mit einem DID Netzwerk überreden können, wenn dabei eine Methode bzw ein darunter liegendes DLT

Prinzip zur Anwendung kommt, welches zwischen den beiden oben genannten Positionen einen Kompromiss möglich macht.

Nach 2 Jahren intensiver Suche und Analyse aller bekannten Entwürfe steht für uns fest: zu physischen Pseudonym-Parties gibt es keine Alternative wenn es darum geht eine demokratische Teilhabe an der Verwaltung des DLTs zu sichern. Das wird in einem zentralen Paper von Bryan Ford von der EPFL Lausanne überzeugend begründet (https://bford.info/pub/soc/personhood/).

Wir haben uns daher am Ende des Projektes entschieden, ein etwas größenwahnsinnig klingendes Vorhaben zu starten: eine alternative zu Proof-of-Work/Proof-of-Stake zu suchen die zumindest in LOKALEN Kontexten keine Tokens braucht um funktionieren zu können.

Aus diesem Ansatz ist mittlerweile ein gefördertes Dissertations-Projekt entstanden, welches von Paul Fuxjäger an der Fakultät für Informatik der Universität Wien (Forschungsgruppe für Kooperative Systeme https://cosy.cs.univie.ac.at) Anfang 2021 begonnen wurde.

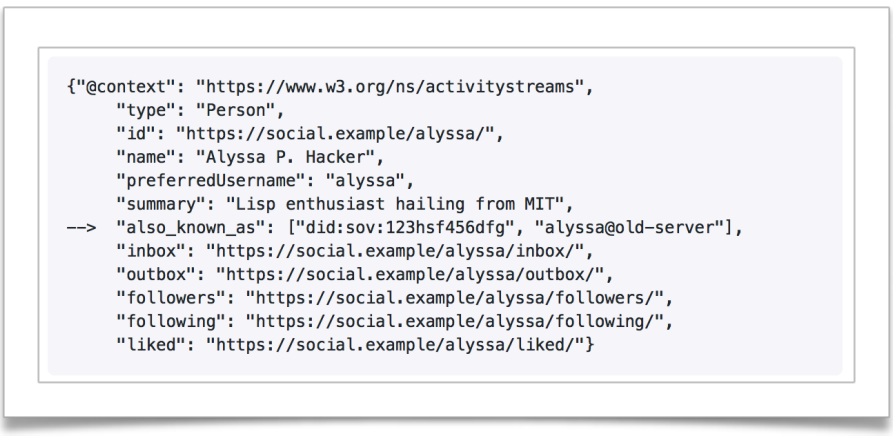
3. Verlauf der Arbeitspakete

3.1.Arbeitspaket 1 - *Detailplanung am Projektstart*

Formales AP am Projektstart. Wird hier nur wegen vorgegebener Nummerierung der Arbeitspakete im Projektplan erwähnt.

3.2.Arbeitspaket 2 - *Requirement Specification*

Basierend auf der v2.8.0 Codebase wurden mehrere virtuelle Test-Netze aufgebaut um einfach nachvollziehen zu können wie die Mastodon-Spezifischen “Actor-Related" ActivityPub Nachrichten im Netzwerk derzeit aussehen. Wir haben dann im ActivityStream Vocabulary ein Element gesucht, welches für die Kommunikation der DIDs zwischen Instanzen im gegenständlichen JSON-LD Kontext am geeignetsten scheint.



Der Vorschlag wurde beim Rebooting-the-Web-of-Trust Meetup im Herbst 2019 zuerst in Wien und dann bei der ersten internationalen ActivityPub Developer Konferenz in Prag präsentiert:

https://github.com/WebOfTrustInfo/rwot9-prague/blob/master/topics-and-advance-readings/fediverse-did-integration.md

Die erfolgreiche Abstimmung dieser Design-Entscheidung mit Mitgliedern der W3C Social Community Group ist hier nachzulesen:

https://github.com/w3c/did-core/pull/389

https://github.com/w3c/did-spec-registries/pull/133

https://twitter.com/fuxjaeger/status/1325755131380588545

3.3.Arbeitspaket 3 - *DID Infrastruktur*

Wir haben Installation und Konfiguration des Universal Resolvers mit Hilfe von Docker Containern signifikant vereinfacht und zahlreiche weitere DID Methoden hinzugefügt.

Hier finden sich die detaillierten Beschreibungen der aktuellen Releases:

https://github.com/decentralized-identity/universal-resolver/releases

Um einen eigenen DID Resolver aufzusetzen reichen diese 4 Schritte:

```
git clone https://github.com/decentralized-identity/universal-resolver
cd universal-resolver/
docker-compose -f docker-compose.yml pull
docker-compose -f docker-compose.yml up
```

Fertige Images sind im Docker Hub verfügbar:

https://hub.docker.com/u/universalresolver

Eine zusätzliche Paketierung, z.B. als Debian Package ist zwar prinzipiell möglich, aber aufgrund der Komplexität im Moment nicht zielführend - denn pro unterstützter DID Methode muss ein passender Treiber inkludiert werden, der dann Abhängigkeiten zu Bibliotheken erzeugt die nicht als .deb Paket verfügbar sind).

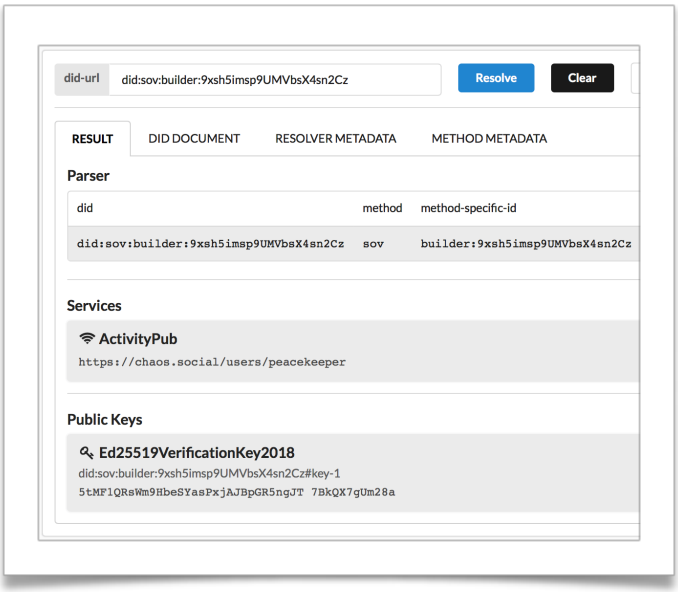
Weitere Details darüber, und über die Entscheidung, die Universal Resolver Codebase im Interesse einer besseren Sichtbarkeit im Github Repository der Decentralized Identity Foundation zu hosten sind in diesem Blogpost nachzulesen:

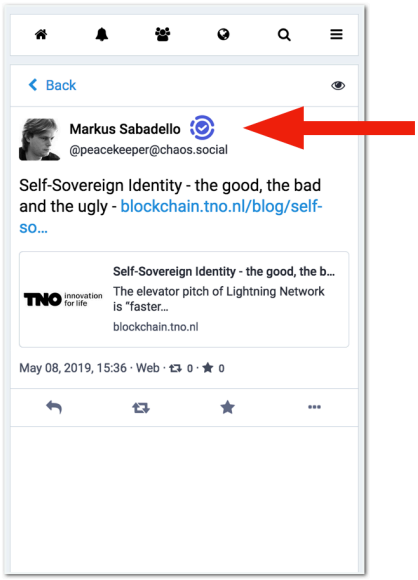
https://medium.com/decentralized-identity/the-universal-resolver-infrastructure-395281d2b540

3.4.Arbeitspaket 4 - *Mastodon Backend Integration*

Nach der Erweiterung des Datenmodells im Mastodon-Backend und der Implementierung der Schnittstelle zum DID Resolvers, liegt nun eine lauffähige Version des Backends vor, in der jedem ActivityPub Actor eine DID zugeordnet werden kann und die in der Lage ist den Service Endpoint im DID Document eines Actors über den Resolver aufzulösen.

Siehe: https://github.com/mastodonid/mastodon



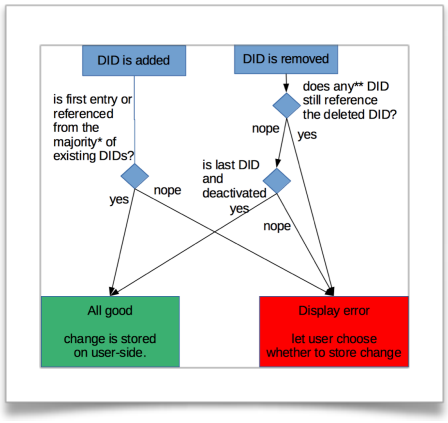


3.5.Arbeitspaket 5 - *Mastodon Frontend Integration*

Damit das Mastodon Web-Frontend mit dieser Erweiterung dazu verwendet werden kann automatisch die Verknüpfungen mit anderen Usern nach einem Server-Wechsel aktuell zu halten, musste noch ein Entscheidungslogik entwickelt werden, welche eine minimale Angriffsfläche gegen Identitäts-Diebstahl hat:

Also haben wir am Empfänger eine Logik implementiert anhand der (im gesamten Netz einheitlich rational) entschieden werden kann, ob eine Re-Follow Anfrage als legitim zu betrachten ist, ODER ob es sich dabei um einen Versuchten Angriff handelt:

Wenn die Anfrage von einem remote Actor kommt, der sich mit der Multi-Source DID “widerspruchsfrei ausweisen” kann, die *davor* von demselben Actor benützt wurde, dann wird die Re-Follow Anfrage als legitim beurteilt und automatisch die neue DNS Adresse im DID Document übernommen. In allen anderen Fällen wird einen Fehlermeldung angezeigt und die Anfrage abgewiesen. Damit ist sichergestellt, dass es maximal aufwendig wird eine Mastodon Identität über eine “gefälschte DID” zu entführen :-D



3.6.Arbeitspaket 6 - *Dokumentation und Formales am Projektende*

Wird hier nur wegen vorgegebener Nummerierung der Arbeitspakete im Projektplan erwähnt. In diesem AP wurde der Endbericht, Dokumentation für Entwickler:innen und abschließende Blogbeiträge verfasst.

Die Disseminations-Aktivitäten während der Projektlaufzeit sind im Kapitel 7 beschrieben.

4. Umsetzung der Förderauflagen

In der Fördervereinbarung für MastodonID wurden keine speziellen Förderauflagen festgelegt.

5. Liste der Projektendergebnisse

1	*Funktionale User-Interface Spezifikation* *Frontend Mockups* *API Spezifikation (DID-Backend, Mastodon-DID)*	*CC-BY-3.0 AT*	*https://www.netidee.at/mastodonid*
2	*Fertig konfigurierte und paketierte Version des "DID Universal Resolver", die in Verbindung mit dem Mastodon-Server eingesetzt werden kann.*	*Apache 2.0*	*https://github.com/decentralized-identity/universal-resolver/*
3	*Lauffähige Version des Backends in der jedem ActivityPub Actor eine DID zugeordnet werden kann und die in der Lage ist den Service Endpoint im DID Document eines Actors über den Resolver aufzulösen. Das Mastodon Web-Frontend kann dazu verwendet werden die Verknüpfungen mit anderen Usern nach einem Server-Wechsel aktuell zu halten.*	*AGPL v3*	*https://github.com/mastodonid*

6. Verwertung der Projektergebnisse in der Praxis

Ergebnisse unserer Arbeit haben bereits in anderen Projekten Eingang gefunden, .z.B. hier wird die Schnittstelle die wir entworfen haben ins Ökosystem von ethereum.org übertragen:

https://codeberg.org/silverpill/mitra

Markus hat 2021, aufbauend auf seine Arbeit am Universal Resolver, ein weiteres Webservice ins Leben gerufen: https://godiddy.com. Dabei handelt es sich um eine gehostete Plattform, die es SSI-Entwicklern und Lösungsanbietern leicht macht, mit DIDs zu experimentieren.

Das World Wide Web Consortium (W3C) hat am 19.Juli 2022 bekannt gegeben, dass Decentralized Identifiers (DIDs) v1.0 nun ein offizieller Webstandard ist.

Markus ist einer der vier Koautor:innen und hat unzählige Stunden (mehrheitlich Ehrenamtlich) in die Ausarbeitung dieser global relevanten Internet-Spezifikation gesteckt, deren Bedeutung in den nächsten Jahren sicherlich noch deutlich zunehmen wird.

Siehe Pressemitteilung: https://www.w3.org/2022/07/pressrelease-did-rec.html.en

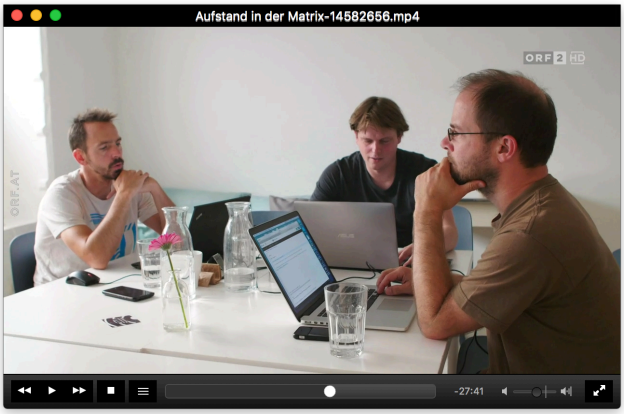
Diesem Schritt ging eine lange Phase der Unsicherheit voraus welche vor allem durch ein wenig nachvollziehbares Veto von Mozilla im Herbst 2021 ausgelöst wurde. Mehr dazu hier:

https://www.evernym.com/blog/w3c-vision-of-decentralization/

7. Öffentlichkeitsarbeit und Vernetzung

Wir wurden für die ORF Dokumentation “Aufstand in der Matrix” zum Thema Dezentrale Identität und Soziale Netzwerke interviewt und einen Nachmittag lang bei unserem Arbeitstreffen im Impacthub und Metalab im Sommer 2019 begleitet:

https://vimeo.com/369258043



Ausgewählte Vorträge von Markus Sabadello zum Thema DIDs und dem Universal Resolver:

sec4dev 2019: Keynote: Decentralized Identifiers (DIDs)

https://www.youtube.com/watch?v=_FNdudes6tA

SSIMeetup Feb 2020: Decentralized identifiers (DIDs) fundamentals and deep dive

https://www.youtube.com/watch?v=SHuRRaOBMz4

DIF F2FJan21: Identifiers and Discovery WG

https://www.youtube.com/watch?v=Tw04ufxNdtQ

DID Conference Korea: Trends in the DID Technology Development and its Status

https://www.youtube.com/watch?v=KmHM6HeQPr4

Ausgewählte Vorträge von Paul zum Thema Mastodon und DID Integration:

Easterhegg 2019 - ActivityPub, the Fediverse, and Everything

https://media.ccc.de/v/eh19-197-activitypub-the-fediverse-and-everything-

PrivacyWeek 2019 - Fediverse Is Here To Stay - The Upcoming Transformation of Online Social Media

https://media.ccc.de/v/pw19-262-fediverse-is-here-to-stay-the-upcoming-transformation-of-online-social-media

Battlemesh 2019 - ActivityPub, the Fediverse and Decentralized IDs

https://media.freifunk.net/v/activitypub-the-fediverse-and-decentralized-ids

Interview in der Radio Ö1 Sendung “Digital Leben” am 3.12.2019

https://soundcloud.com/user88728769/alternativen-zu-facebook-und-twitter-radio-o1-dezember-2019

Netzpolitischer Abend, Mai 2022: „Das Mastodon Netzwerk – ein Projekt für Nerds oder die vielversprechendste Alternative zu Musk-Twitter?“

https://netzpolitischerabend.wordpress.com/2022/05/29/63-netzpolitischer-abend-at-am-2-juni-2022-im-metalab-in-wien/

8. Geplante Aktivitäten nach netidee-Projektende

Das seit Anfang 2021 laufende Dissertations-Projekt von Paul Fuxjäger (an der Universität Wien, Research Group Cooperative Systems) baut direkt auf den Ergebnissen dieses Projekts auf und befasst sich mit der Entwicklung eines DLT Modells (inkl. DID Methode) welches *zumindest in lokalen Kontexten* (z.B. zwischen Mastodon Instanzen mit Orts-Bezug) eingesetzt werden kann ohne dabei gleichzeitig Unmengen an Energie zu verbrauchen und/oder Spekulations-Blasen zu fördern - weil es in diesem Ansatz keinen Token Reward gibt!

Damit wird die zentrale (valide!) Kritik der Mastodon-Hauptentwickler an den derzeit dominierenden DLT Methoden adressiert.

Die erste öffentliche Präsentation fand am 24.06.2022 an der Fakultät für Informatik der Universität Wien statt. Der Plan für das bis 2025 laufende Projekt steht auf der Netidee Projektseite zum Download bereit.

Paul hat gemeinsam mit Erwin Ernst Steinhammer (Politikwissenschafter vom c3w.at) Anfang 2020 eine Arbeitsgruppe gegründet die sich (während die Pandemie-Phase 2020-2021 leider nur unregelmäßig) im Metalab trifft:

https://metalab.at/wiki/Die_Öffentlichkeit_die_wir_uns_wünschen

…mit dem Ziel, Vorschläge für die Kooperation in Fediverse-Verbünden zu erarbeiten, als Weiterentwicklung der ersten Server Konstitution von joinmastodon.org, die Anfang 2020 veröffentlicht wurde: https://joinmastodon.org/covenant

Wir versuchen in dieser Arbeitsgruppe Regelsätze auszuarbeiten, welche in einem Verbund von Mastoden-Instanzen zur friedvollen Auflösung von Konflikten zwischen Moderations-Teams geeignet sind. Ein zentrales Element dabei sind öffentliche Direktmandate um “frei von Einschränkungen der aktuellen Instanz alle Kontakte überall hin im Verbund mitnehmen zu können” - **also genau jene Funktionen, die in einem DID-fähigen Mastodon Netzwerk zur Verfügung stehen.** Teile dieses Konzepts werden in diesen zwei Vorträgen von Erwin erklärt:

ActivityPub Developer Conference 2020 (#APCONF)

Digital public sphere - From gated platforms to the fediverse

https://socialhub.activitypub.rocks/t/digital-public-sphere-from-gated-platforms-to-the-fediverse/945

Remote Chaos Congress 2020 (#RC3)

Die rosarote Brille des Fediverse

https://media.ccc.de/v/rc3-857362-die_rosarote_brille_des_fediverse

9. Anregungen für Weiterentwicklungen durch Dritte

Die Schnittstelle, die wir in diesem Projekt für das Mastodon Netzwerk entwickelt und implementiert haben, kann mit geringem Aufwand in alle weiteren Fediverse Backends integriert werden (https://fediverse.party), die für Server-2-Server Kommunikation die selben JSON-LD basierten ActivityPub/ActivityStream Standards nutzen.