Vorteile von Open Source bei Identity & Access Management

Peter Gietz, DAASI International

Forum E, it-sa 2023
Nürnberg

DAASI International

Agenda

- Open Source (OS)
- OS und Digitale Souveränität
- OS für Identity und Access Management

Über DAASI International

Gründung 2000

- in Tübingen mit 4 Mitarbeiter*innen
- Spin-Off des ZDV der Universität
- Tübingen aus DFN-Projekten zu
- X.500/LDAP heraus

Stand 2023

- 26 Mitarbeiter*innen
- > 17 FTE
- > 2 Millionen Jahresumsatz

DAASI International ist ein erfolgreicher PoC für ein nicht skalierendes aber nachhaltiges Businessmodell auf Open-Source-Grundlage

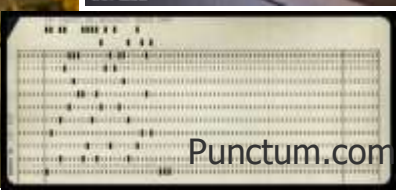
DAASI International steht für digitale Souveränität

- Open Source für Flexibilität und digitale Souveränität
- Datenschutz für informationelle Selbstbestimmung und digitale Souveränität
- Offene Standards für Interoperabilität und Kombinationsmöglichkeiten, was ebenfalls digitale Souveränität fördert

Am Anfang war Open Source

Hochschulen betrieben Großrechner

- z. B. Zuse Z22, 1957 mit Trommelspeicher und Lochkartenlocher
- Hardware wurde mit Betriebssystem und Compiler geliefert (ohne Zusatzkosten)
- **Software wurde ausschließlich von den Nutzer*innen geschrieben und im Code geteilt**
  - „distributed under the principles of openness and cooperation long established in the fields of academia“[2]
  - „Such communal behavior later became a central element of the so-called hacking culture“ [2]
- **SHARE** ist erste (1955) User Group für IBM Mainframes
  - **„Its not an acronym, it’s what we do“** [3]



*„46 Benutzer*innen aus 16 Instituten nutzen die Z22 in 1964 für ca. 65 Aufgabenstellungen. Die Nutzung erfolgt zu mehr als 90 % durch Programme im Freiburger Code*, der Rest ist in Algol.“ [1]*

* Eine Art Assembler

Open-Source-Definition von OSI

- Open Source Initiative
  - sieht sich primär als Verwalter Ihrer OS-Definition als Grundlage des OSS-Ökosystems
  - listet mit der Definition kompatible OS-Lizenzen
- Die OS-Definition hat 10 Merkmale [5]:
  1. Software wird **frei zur Verfügun**g gestellt *(free redistribution)*
  2. **Source Code** wird mitverteilt *(must include source code)*
  3. Lizenz muss **Modifikationen des Codes** erlauben *(derived works)*
  4. Solche Änderungen müssen zu einem neuen Namen oder einer neuen Versionsnummer der Software führen, um **Autorenschaft zu dokumentieren** *(Integrity of The Author's Source Code)*
  5. Nutzung **darf nicht auf bestimmte Gruppen eingeschränk**t **werden** *(no discrimination against persons or groups)*
  6. Nutzung **darf nicht auf bestimmte Domänen eingeschränkt werden** *(no discrimination against fields of endeavor)*
  7. **Gleiche Lizenz für alle** *(Distribution of License)*
  8. **Produktunabhängig**: Rechte dürfen nicht von einer Distro etc. abhängig gemacht sein *(license must not be specific to a product)*
  9. **Softwareunabhängig**: darf man nicht verlangen, dass die SW nur zusammen mit anderer SW verbreitet werden *(license must not restrict other software)*
  10. **Technologieneutrale** Verteilung über beliebige Medien *(license must be technology-neutral)*

Vorteile von Open Source

- kein Vendor-Lock-in
  - Kunde hat stärkere Position gegenüber den Herstellern und kann die Roadmap wesentlich besser beeinflussen
  - Wer den Code besitzt, hat die Macht
- maximale Flexibilität und Unabhängigkeit
  - erweiterbar und anpassbar bei neuen Anforderungen, durch Hersteller, dem Kunden selbst, oder einem dritten Dienstleister
- Standardkonformität
  - In der Regel bedient OSS offene internationale Standards
- hohes Innovationspotenzial
  - Auch für neue Standards und Technologien gibt es in der Regel OSS
- Hohe Sicherheit durch Transparenz
  - Sicherheitslücken und Backdoors werden schneller entdeckt bzw. gar nicht erst eingebaut
- Lizenzkostenfrei
  - Nutzung an sich ist kostenlos

DAASI International

Open Source im Business-Kontext

Offener Quellcode schafft maximale Transparenz und bietet höchste Flexibilität durch Anpassungs- und Gestaltungsmöglichkeiten. Dadurch bilden sich auch Kooperationsräume, durch die wertvolles Wissen mit enormem Innovationspotenzial entsteht. Diese Eigenschaften machen Open Source zu einer unverzichtbaren Basis nachhaltiger Wertschöpfung – nicht nur im Bereich Software. Die Vernetzung verschiedener Anwendungen, Cloud Computing, IoT und die Anbindung der Zukunft an das Heute, also ein Miteinander von etablierten und neuen Lösungen, all dies erfordert Interoperabilität, wie sie vorwiegend durch Open Source gewährleistet wird.
(Open Source Business Alliance [6])

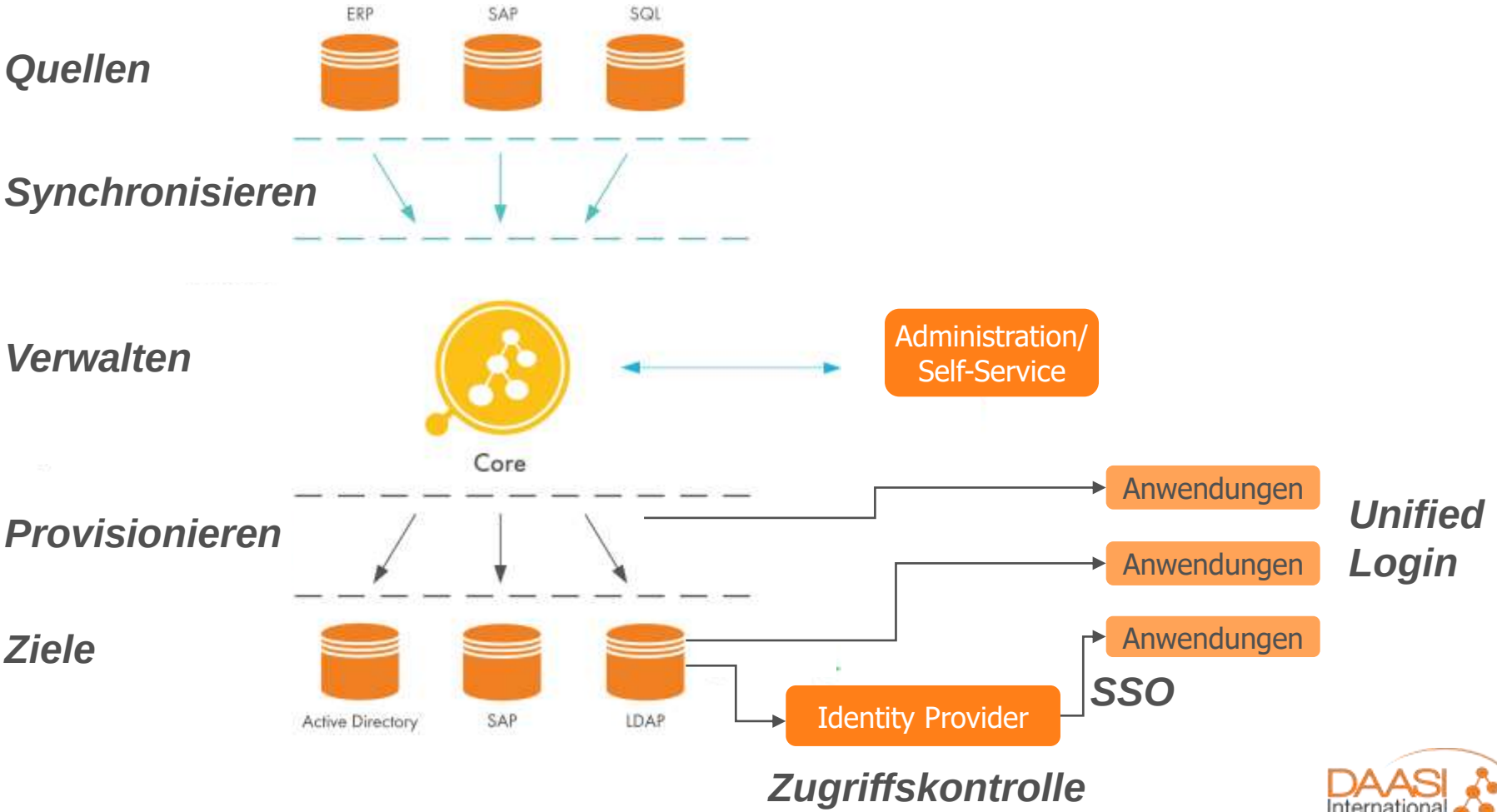
DAASI International

Open Source und IAM

- **Identity & Access Management:**
  - ermöglicht die zentrale Verwaltung von Identitätsdaten (Mitarbeiter*innen, Kunden, Lieferanten) und deren organisatorische Verortung (Organigramm), sowie deren Rechte und Rollen
  - bezieht Stammdaten aus Quelldatenbanken (HR-System, CRM etc.)
  - versorgt beliebige Zielanwendungen mit Identitätsinformationen
  - ermöglicht zentrale Verwaltung von Rollen und Rechten
- **Identity & Access Management hilft:**
  - Verwaltungsaufwand sowie Kosten zu reduzieren und somit Effizienz zu steigern
  - konsistente Datenstämme und -strukturen zu etablieren sowie Sicherheit und Datenschutz zu erhöhen
  - Zufriedenheit zu steigern (verbesserte User Experience durch Vereinfachung)
  - den Aufwand zu verringern (weniger Calls am Helpdesk, z. B. Passwort Recovery)
  - Risiken durch unbefugte Zugriffe zu minimieren

DAASI International

IAM unser Verständnis



Open Source und IAM

Gerade bei IAM sind die Anforderungen sehr heterogen:

- Jede IT-Landschaft ist anders:
  - viele verschiedenen Quellen und Ziele
- Jede organisatorische Prozesslandschaft ist anders:
  - Onboarding, Offboarding, Rollen und Rechtevergabe etc.
- Auch Compliance-Anforderungen werden unterschiedlich umgesetzt
- Aus Sicherheitsgründen muss die Corporate Identity abgebildet werden

Standardlösungen können diese Heterogenität oft nicht abbilden

DAASI International

Open Source und IAM

- **Open Source:**
  - Ermöglicht es, beliebige Quellen und Ziele anzuschließen, wenn nicht über Standards, die von OS-Bibliotheken in der Regel unterstützt werden, dann über Implementierung proprietärer Protokolle
  - Ermöglicht es flexibel alle organisatorischen Prozesse abzubilden
  - Nicht die Prozesse an die Software anpassen, sondern die Software an die Prozesse!
  - Reports können individuell erstellt und layoutet werden
  - Sehr kundenspezifischer Code kann von dem Rest der Software gekapselt werden
    - Auch solcher Code kann nachgenutzt werden, wenn er nicht Betriebsgeheimnisse enthält (z. B.: Algorithmus zur Bildung des Login-Namens oder E-Mail-Adresse)
  - Wegen der Standardkonformität können OS-Produkte gut miteinander kombiniert werden

DAASI International

Open Source und IAM

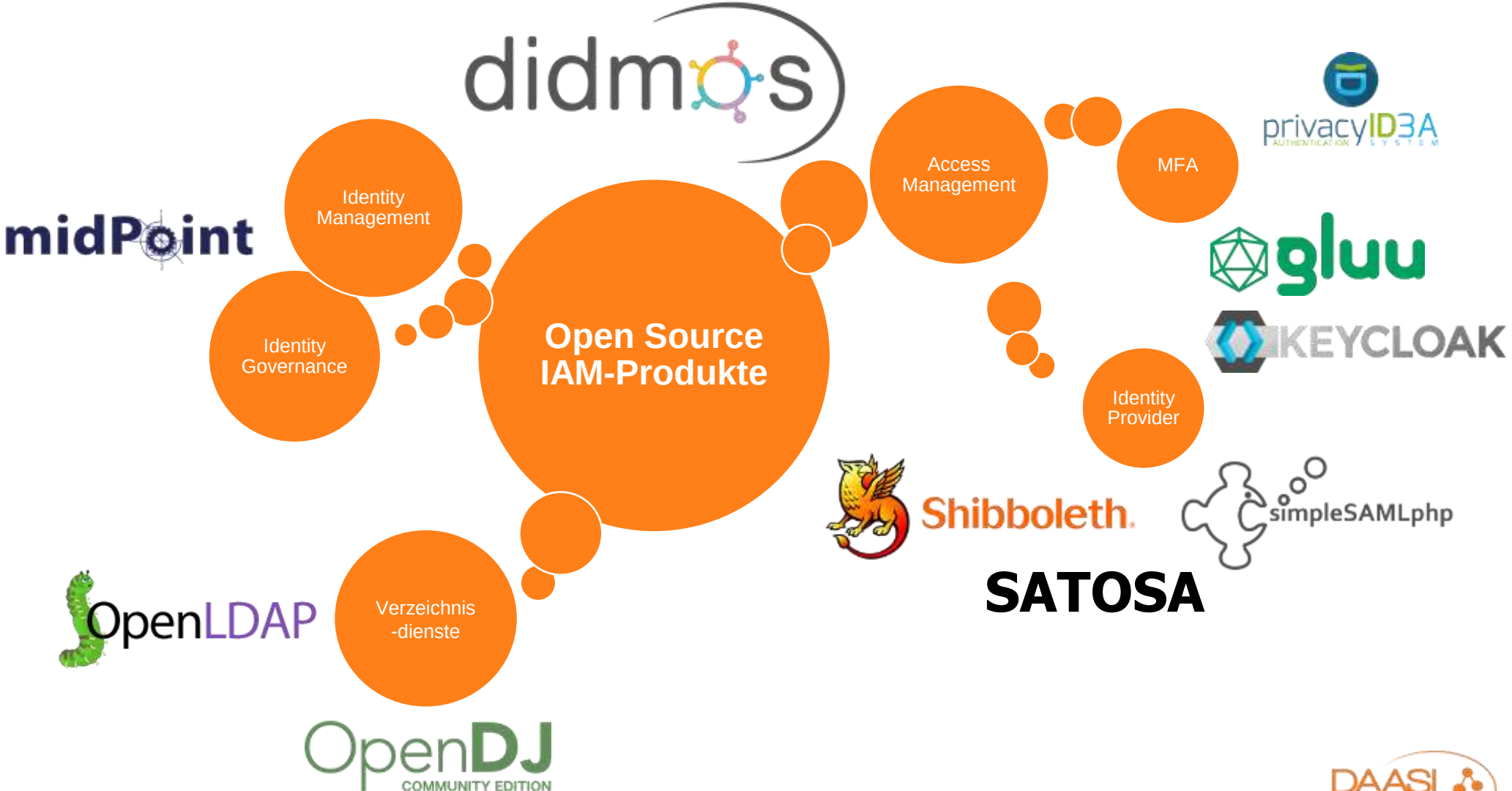
- Potentielle Nachteile von Open Source:
  - Wie kann ich wissen, dass es sich um gut geschriebenen Code handelt?
  - Wer übernimmt Verantwortung für Bugs und daraus entstehenden Schaden
  - Wie ist die nachhaltige Pflege gesichert?
  - Wer bietet überhaupt Schulungen an?
  - Wie intensiv müssen Mitarbeiter*innen auf Open Source geschult werden
- Alles lösbare Probleme: Open-Source-Unternehmen
  - Sie verpflichten sich vertraglich Open-Source-Code zu pflegen
  - Sie machen Qualitätskontrolle und übernehmen Verantwortung
  - Sie garantieren nachhaltige Pflege
  - Sie bieten Schulungen an
  - Umgewöhnen muss man sich immer, ob OS- oder proprietäre Software
    - bei jedem Wechsel der Software oder auch nur der Softwareversion

DAASI International

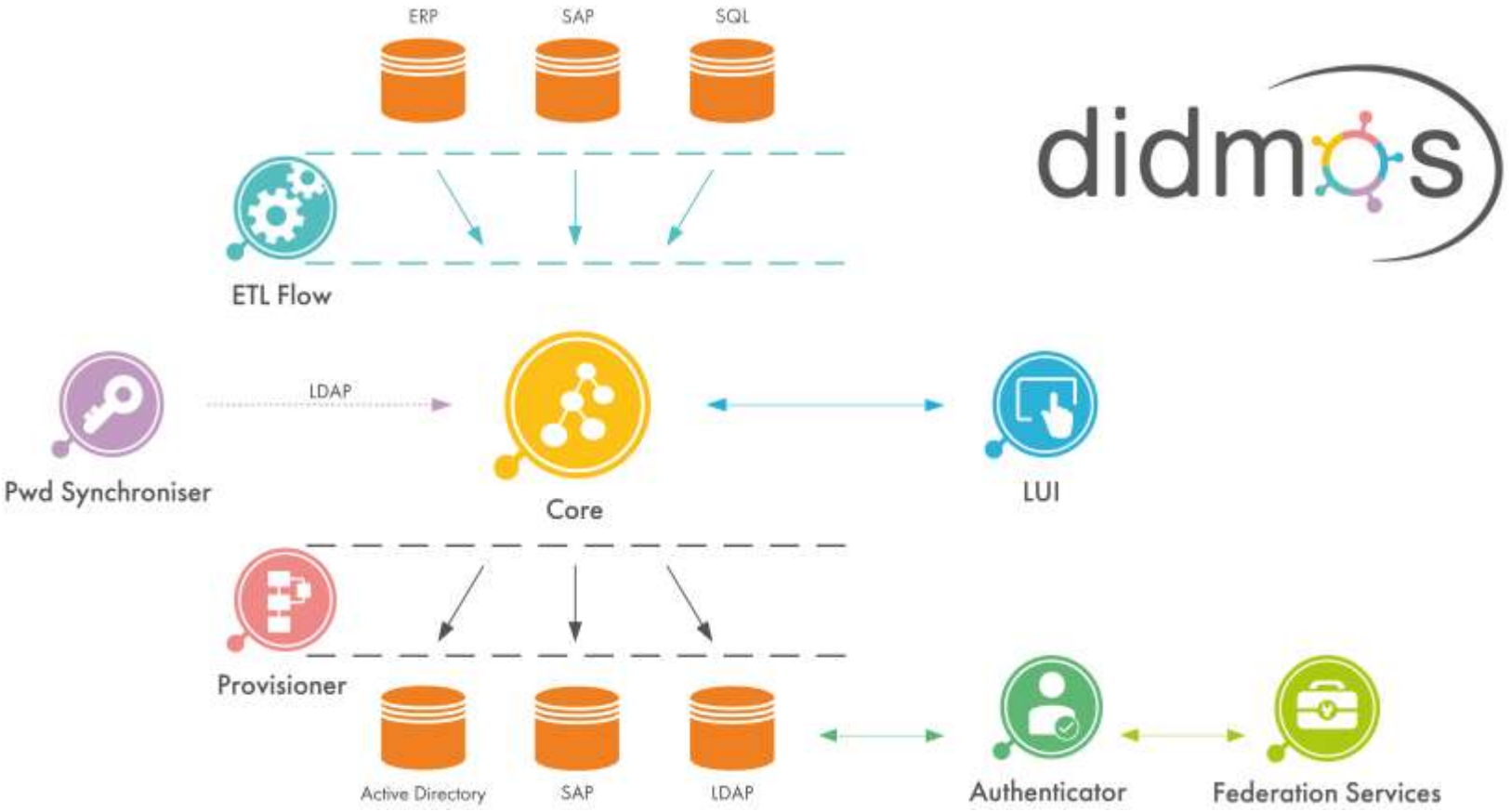
Es gibt viele solcher Firmen

Open Source Business Alliance
Bundesverband für digitale Souveränität e.V. [7]

- 2011 als Zusammenschluss der Linux Solutions Group e.V. und dem LIVE Linux-Verband e.V. gegründet
- vertritt die Interessen von Open-Source-Firmen und damit von Open Source
- > 200 Mitgliedsunternehmen mit Jahresumsatz von insg. 126,8 Milliarden Euro
- tritt dafür ein, Open Source als Standard in der öffentlichen Beschaffung und bei der Forschungs- und Wirtschaftsförderung zu etablieren
- steht Unternehmen, Privatpersonen, Medien und der Politik für Expertisen und als Ansprechpartner zur Verfügung


didmos
privacyIDEA
midPoint
Identity Management
Identity Governance
Open Source IAM-Produkte
Access Management
MFA
gluu
KEYCLOAK
Identity Provider
Shibboleth
simpleSAMLphp
SATOSA
OpenLDAP
Verzeichnis -dienste
OpenDJ
COMMUNITY EDITION

didmos: eine flexible ganzheitliche Lösung



didmos Module

Core
Metadirectory mit
REST-Interface

LUI
Weboberflächen für Self-Service
und Administrationsinterface

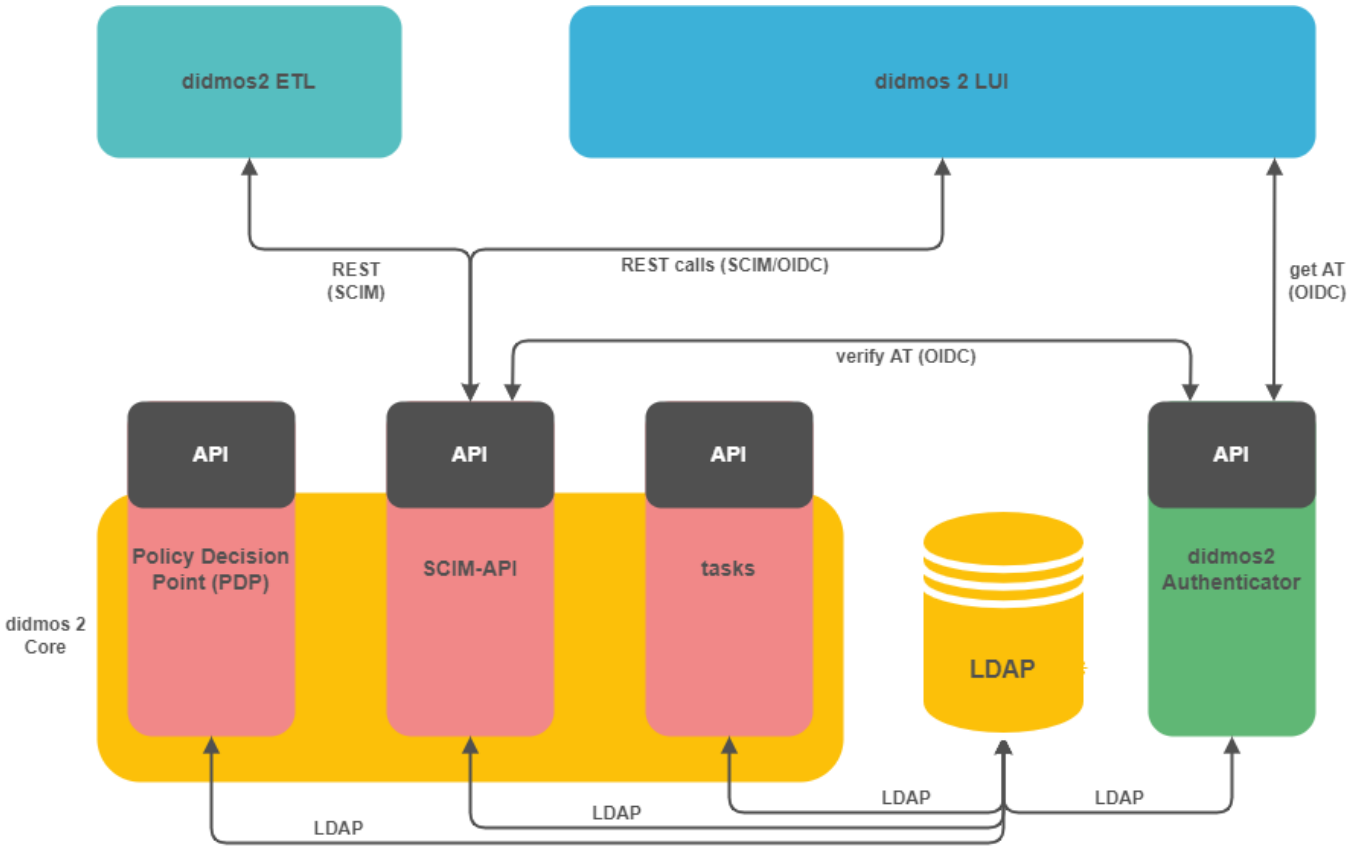
ETL Flow
Modulbasiertes Workflow-
System zur Synchronisierung

Provisioner
Queue-basiertes System zur
Provisionierung der Ziele

Authenticator
Identity-Provider
(SAML und OIDC)

Pwd Synchroniser
Synchronisierung von
Active Directory Passwörter

didmos Core und Standards



didmos Core LDAP Datenmodell

- **Multi Tenancy**
  - Root-Tenant kann auch allein für einfachere (bzw. Single-Tenant) Anwendungsfälle genutzt werden
- **Interne und externe Benutzerkonten**
  - ou=people für in didmos verwaltete Benutzer*innen
  - ou=social-people für sog. „Shadow Accounts“, die von didmos Authenticator bei Registrierung erzeugt werden
- **HA-fähig**
  - LDAP als Multi-Master-Setup
  - Jede Backend-Instanz nutzt ein dediziertes LDAP

Vorteile von didmos

- Modularisierung erlaubt Kombinationsmöglichkeiten mit anderen OS-Produkten
- Flexibel konfigurierbar
- Flexibel erweiterbar
- Kapselung von kundenspezifischem Code
- REST-basierte Architektur
- Standardbasiert (LDAP, OIDC, SCIM, SAML, SPML, XSLT)
- Keine Subskriptionsgebühren

DAASI International

midPoint – die Open-Source-Standardlösung

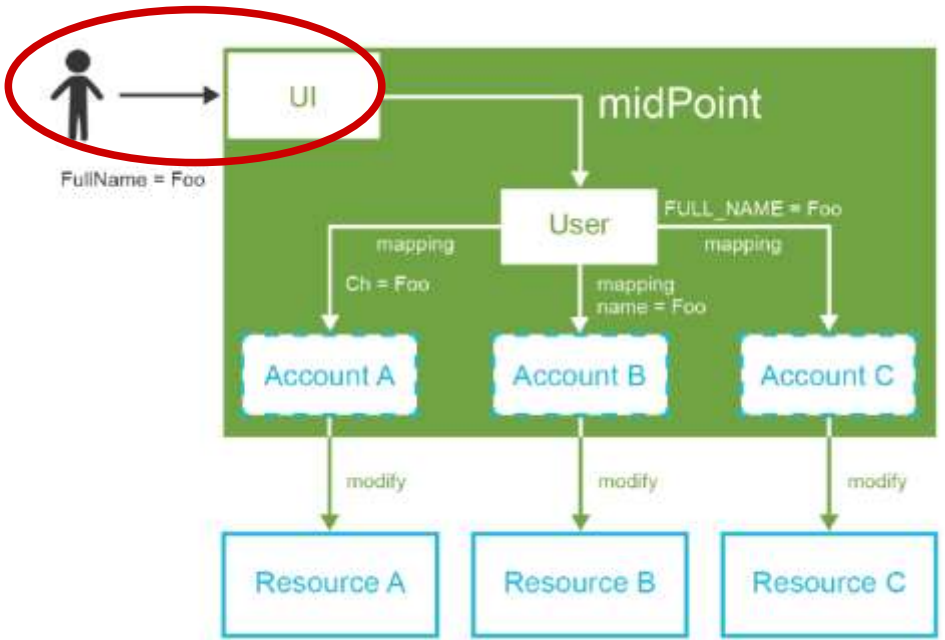
- Open-Source-Software von Evolveum
- Komplettlösung für Identity Governance und Provisioniereung
- Identity Governance
- Auditing
- Organisationsstruktur
- Credential Management
- Entitlement Management

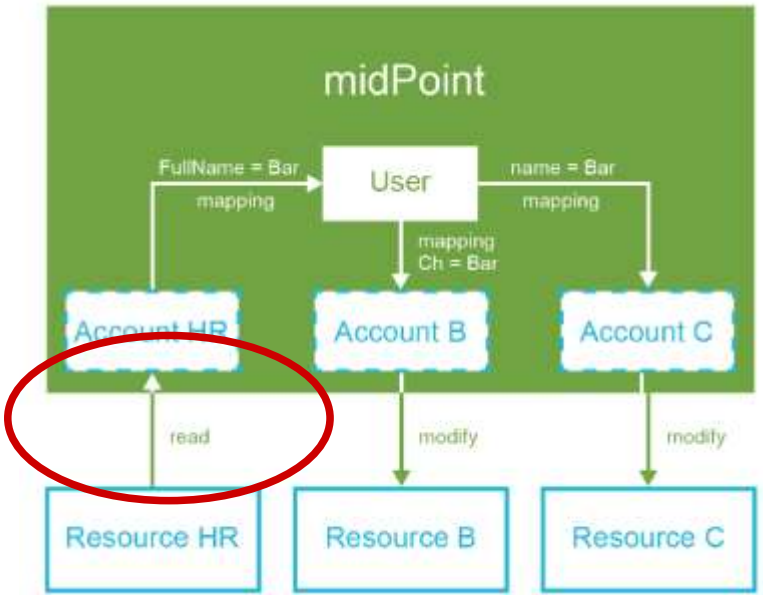
Wir empfehlen midPoint,

- insbesondere, wenn ein Standardprodukt gewünscht ist oder wenn es um eine Migration eines midPoint-nahen Produkts wie OpenIdM oder Forgerock geht.

IdM mit midPoint

Quelle: entweder Benutzeroberfläche oder über Konnektor





Vielen Dank für Ihre Aufmerksamkeit!

Sie möchten mehr erfahren? Besuchen Sie uns!

Stand 7A-521

Kontakt, weitere Informationen und zitierte Quelle

eMail: info@daasi.de
Web: www.daasi.de

[1] https://www.uni-marburg.de/de/hrz/ueber-uns/profil/geschichte/1963-1983-die-grossrechner-aera
[2] https://en.wikipedia.org/wiki/History_of_free_and_open-source_software#Free_software_before_the_1980s
[3] https://www.share.org/Portals/0/Docs/SHARE_1571014_Timeline.pdf
[4] https://de.wikipedia.org/wiki/Open_Source
[5] https://opensource.org/osd/
[6] https://osb-alliance.de/ueber-uns/leitlinien-der-osb-alliance-2022
[7] https://osb-alliance.de bzw. https://osb-alliance.de/ueber-uns/was-ist-die-osb-alliance