netidee PROJEKTE

fairkom

Gesellschaft zur Förderung medialer Kommunikation und immaterieller Gemeingüter

Badgasse 3 | 6850 Dornbirn
+43 50 80 20
info@fairkom.eu
www.fairkom.eu

fairlogin

Federated Sinle-Sign-On für die Zivilgesellschaft

Endbericht | Call 11 | Projekt ID 1909

Inhalt

1 Einleitung

Single-Sign-On für typische Cloud-Dienste wird derzeit nur von großen Anbietern angeboten. NutzerInnen insbesondere aus der Zivilgesellschaft und in NGOs würden gerne selbst betriebene Cloud Lösungen mit Single-Sign-On realisieren. Jedoch sind deren Mitglieder aufgrund des fehlenden Komforts bei einer einheitlichen Authentifizierung und Autorisierung stets versucht, auf die Dienste der großen Anbieter wie Google, iCloud, Sharepoint & Co auszuweichen.

Bei fairlogin geht es um die Etablierung einer dienste- und provider-übergreifenden Authentifizierung und Autorisierung für Open Source basierte Cloud Dienste. NutzerInnen, speziell im NGO - und Nachhaltigkeitsumfeld, wollen Open Source Cloud Lösungen gerne nutzen, haben aber oft für jeden Dienst und bei jedem Provider ein anderes Login.

Auch sollen Zugangsrechte für Gruppen zB für die Verwaltung von Dateien in ownCloud/nextcloud oder Dokumente in einem Wiki nicht in jedem Dienst separat verwaltet werden müssen.

Mit fairlogin haben wir 2017 eine Lösung für die Überwindung dieser Herausforderungen geschaffen und 2018 mit diversen Partnern getestet. Dieses Dokument berichtet über die technischen Herangehensweisen bei der Anbindung von Open Source basierten Webdiensten Diensten an Single-Sign-On, Anwendungsbeispiele und Erfahrungen bei der Föderierung mit anderen Identity Providern.

2 Projektbeschreibung

Projektziel war die Etablierung eines Single-Sign-On Serviceangebotes und die Dokumentation, wie man einen solchen aufbaut. fairlogin verwendet LDAP als User Store und einen Identity Provider, der über OAuth2, SAML2 oder kerberos den SSO-Dienst zur Authentifizierung von NutzerInnen und die Verwaltung von Gruppenrechten anbietet.

Wir haben nach der Entwicklung von Use Cases zunächst einen Satz gängiger Open Source Cloud-Dienste, welche von NGOs, die von der fairkom betreut werden genutzt werden, an fairlogin angebunden. Diese hatten unterschiedliche Authentifizierungsprotokolle, wie OpenLDAP bzw. OAuth2 und OpenID Connect. Dazu wurde die Authentifizieurngsmaske von keycloak angepasst und in einem Wiki die Technik beschrieben.

Unser Identity Provider kann ebenso andere ID Provider einbinden, womit NGOs untereinander Vertrauensverhältnisse aufbauen können und die NutzerInnen es vermeiden können, bei jeder NGO ein Passwort hinterlegen zu müssen. Damit

haben wir den Grundstein für eine Föderierung von Identity Diensten sowohl für die Zivilgesellschaft, aber auch für andere Sektoren geliefert.

3 Verlauf der Arbeitspakete

3.1 Arbeitspaket 1 - *Use-Case Evaluierung – Marktuntersuchung*

Kurzbeschreibung der Haupttätigkeiten

- Bestandsaufnahme
- Erörterung Usecases & User Anforderungen
- Evaluierung vorhandener Technologien (SAML, LDAP, OpenID/Connect, Midpoint, Fusiondiretory, FreeIPA)
- Markt-Test

Besondere Erfolge/ Probleme

Keine

Gab es große Abweichungen zum Plan? Warum?

Keine

Erkenntnisse zur Vorgangsweise

Am Anfang stand eine Befragung einiger Communities nach deren Cloud Bedürfnis, sowie die Ausarbeitung eines Persona Modells für prototypische NutzerInnen.

Mit diesem Hintergrund wurden ein Plan in Form von Diagrammen in Workshops erstellt und damit Struktur und Abläufe wesentlicher fairlogin Funktionen erarbeitet. Dabei wurden die Anforderungen und Nutzungsprofile nach unterschiedliche Zielgruppen kategorisiert. Diese dienten als Grundlage der Spezifikation für die Auswahl einer geeigneten Identity Provider Technologie. Auch die ersten Gedanken einer nachhaltigen Finanzierung durch potentielle Geschäftsmodelle wurden festgehalten.

Es wurden drei Identity Provider Technologien evaluiert: OpenAM, MidPoint und WSO2.1 Nach einer Evaluierung nach Kriterien wie Single-Sign-On Unterstützung und Benutzer- und Gruppenverwaltungsfunktionen war es letztendlich die Anzahl der unterstützten Authentifizierungsprotokolle und Federation-API die den Fokus auf WSO2 gelegt haben. Typischerweise unterstützen diese LDAP, einige auch schon modernere SSO Protokolle wie

SAML2, OAuth2. Interessanter waren die, die auch schon aktuelle Protokolle wie OpenID bzw. OpenID Connect verwenden. WSO2 unterstützte darüber hinaus zusätzliche Schnittstellen zu großen Identity Providern sowie ein paar ausgefallene Protokolle.

Später sind wir durch die Vernetzung mit dem OpenFabNet2 auf KeyCloak aufmerksam gemacht worden, welches der von RedHat in Entwicklung befindlicher Identity Provider ist. Nachdem wir sichergestellt haben, dass alle wichtigen Protokolle auch von KeyCloak unterstützt werden, haben wir uns entschieden auf diesen umzustellen, weil das Open Source Pendant KeyCloak leichter als WSO2 wartbar erschien.

FreeIPA, die Oberfläche zur Verwaltung von Usern und Gruppen für Linux/Unix Umgebungen von Redhat, dem Herausgeber vom KeyCloak, unterstützt leider nicht die User und Gruppen Verwaltungskonzepte von KeyCloak. Dabei hat ein User eine Hauptgruppe, kann jedoch weiteren Gruppen angehören. Den Gruppen untereinander können jedoch keine weiteren Zugehörigkeiten bzw. Hierarchien zugeordnet werden. Somit haben wir ohne FreeIPA den Identity Provider auf Basis von keycloak aufgebaut.

3.2 Arbeitspaket 2 – *Dashboard – LDAP Identity Provider Setup*

Kurzbeschreibung der Haupttätigkeiten

- Dashboard & LDAP Setup
- Erstellung LDAP Schema
- Test-Case: Anbindung erster Apps und Usertest; Einbindung des ersten Nachhaltigkeitsnetzwerks

Besondere Erfolge/ Probleme

Keine

Gab es große Abweichungen zum Plan? Warum?

Keine

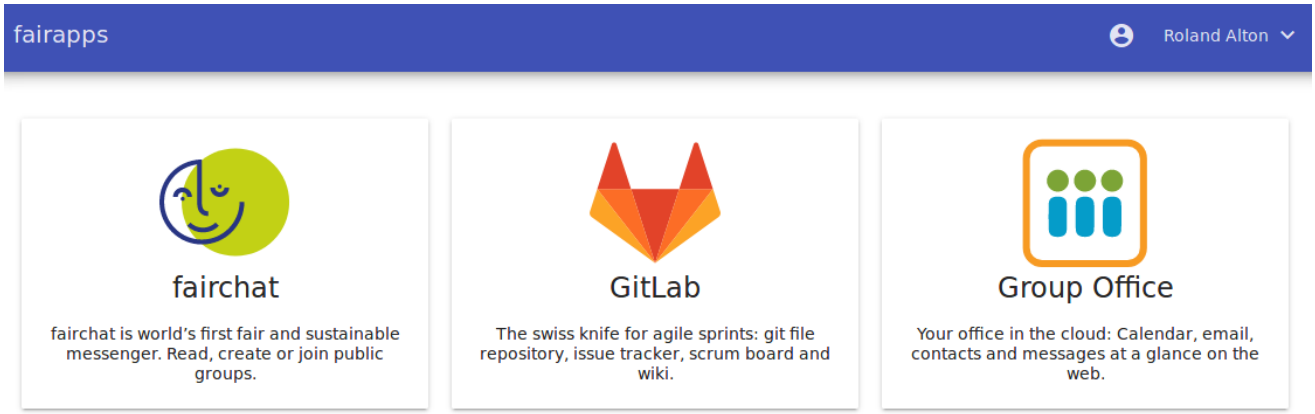
Erkenntnisse zur Vorgangsweise

Mit einem OpenLDAP Backend haben wir den ersten Prototypen schon mit WSO2 gebaut und die Daten von etwa 600 NutzerInnen aus unserem Leitsystem GroupOffice über ein Script mit dem SCIM Protokoll in das OpenLDAP Backend übertragen. Durch das Umsatteln auf KeyCloak musste der Import über SCIM leicht angepasst werden, da KeyCloak diesen Standard derzeit noch nicht

unterstützt. Jedoch war die API recht vergleichbar und konnte daher relativ schnell umgestellt werden.

Nun ging es darum einerseits das Dashboard, also die Einstiegsoberfläche für die AnwenderInnen zu den Diensten und später auch für die AdministratorInnen, welches ebenfalls erst für WSO2 als Prototyp gebaut wurde, auf KeyCloak zu migrieren.

Parallel dazu haben wir ein Dashboard entwickelt, welches im November 2017 als Identity-Provider-Initiated Plattform in den Beta-Test ging.



3.3 Arbeitspaket 3 – *LDAP / SAML / OIDC Integration*

Kurzbeschreibung der Haupttätigkeiten

- GroupOffice / ISPConfig LDAP Integration
- Modul-Neuentwicklung
- Account Migration
- Design

Besondere Erfolge/ Probleme

Vereinzelte Schwierigkeiten bei der Übernahme insbesondere von schwachen Passwörtern aus dem GroupOffice.

Gab es große Abweichungen zum Plan? Warum?

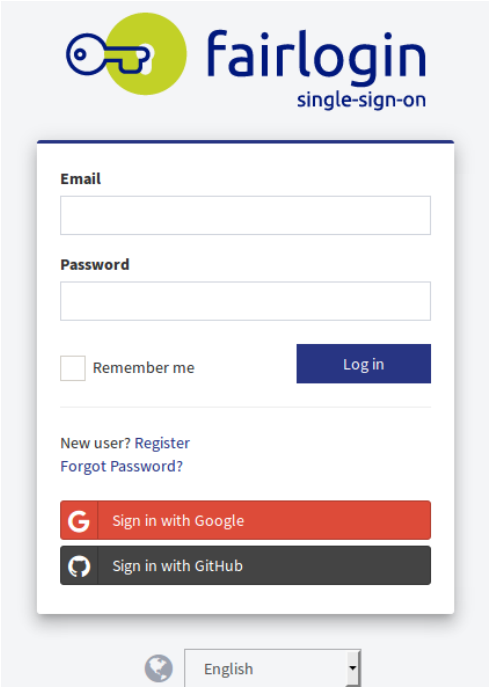
Keine

Erkenntnisse zur Vorgangsweise

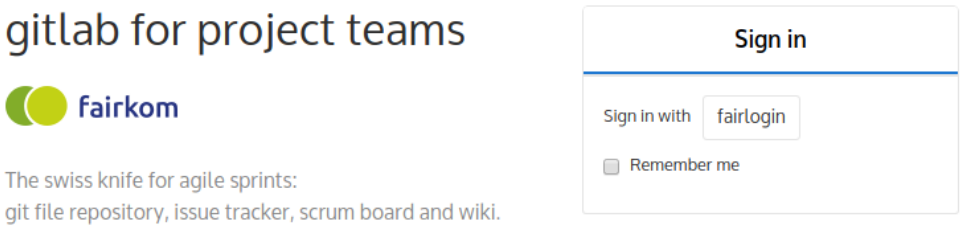
Als erster Dienst wurde fairchat.net basierend auf Rocket.Chat mit dem Identity Provider Integriert. Zunächst sollte diese Integration per OpenID bzw. OpenID

Connect geschehen. Jedoch war das dazugehörige Plugin für RocketChat nicht genügend ausgereift womit wir dann die Integration mit SAML2 durchgeführt haben. Da wir schnell echte Erfahrungen sammeln wollten, haben wir diese Integration gleich mit dem Produktiv-System von fairchat vorgenommen. Damit waren die migrierten User gleich produktive Identitäten. Mittlerweile wurde eine Verbesserung des oAuth Handlers durch uns in Rocket:Chat integriert[1].

Seit Juli 2017 können BenutzerInnen sich eine fairlogin ID unter folgender URL einrichten: https://id.fairkom.net/auth/realms/fairlogin/account/

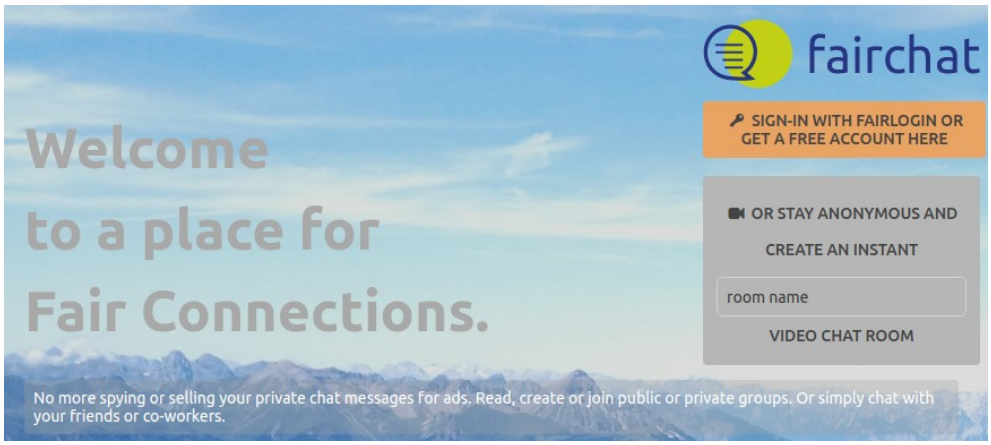


Typischerweise wird die Login- bzw. Registrierungsseite von einem Service aus aufgerufen. Hier zwei Beispiele mit „fairlogin“ Button, die im August 2017 realisiert worden sind: git.fairkom.net und fairchat.net:



Um die Identity – Provider Federation zu demonstrieren, bieten wir ebenso ein Sign-In mit einem Google oder GitHub Konto an.

1 https://github.com/arminfelder/Rocket.Chat/pull/1



Bei der Übernahme der Konten gab es anfangs ein paar Schwierigkeiten insbesondere von schwachen Passwörtern aus dem GroupOffice, die nicht gleich aufgefallen sind. Daher hatten wir einerseits einige produktive User, die noch nicht sauber über das KeyCloak im LDAP vollständig angelegt wurden und am Chat-Dienst nicht ohne manuelle Passwortsynchronisation teilnehmen konnten, andererseits wurden neue User schon direkt über KeyCloak angelegt. Dadurch stieg der Bedarf einerseits das Dashboard für die Verwaltung fertig zu stellen, andererseits die fehlenden Daten und Passwörter zu übernehmen.

Die Ursache für das Problem mit den Passwörtern war eine strikte und durchaus sinnvolle Password-Policy, die über die Schnittstelle schlagend geworden ist. Diese musste also für die Migration der User noch einmal ausgeschaltet werden. Die fehlenden Felder zu erweitern war trivial und somit war dann im Laufe des Septembers 2017 die Migration auf LDAP erfolgreich.

Parallel konnten wir die ownCloud User direkt über das LDAP anlegen und haben die eigene User-Verwaltung im ownCloud deaktiviert.

Nun wollten wir weitere wichtige Anwendungen anbinden. GroupOffice und ISPConfig sind zentrale Anwendungen, die jedoch in den derzeit produktiven Versionen keine LDAP bzw. SAML2, OAuth2 bzw. OpenID API hatten. Weiterhin hatten wir schon eigene Integrationen von GroupOffice mit DokuWiki und ownCloud die über die reine Authentifizierung hinausgingen.

Bevor wir hier also weitermachen konnten, mussten diese erst einmal auf die aktuelle Versionen angehoben werden. Denn erst mit Nextcloud gab es die Möglichkeit mit SAML2 das Login einzurichten, einstweilen haben wir dies über LDAP realisiert. Es wurde notwendig dafür eine neue Test-Umgebungen aufzubauen, um diese Umstellung inkl. der Integration zu testen. Diesen Aufwand hatten wir unterschätzt, konnten trotz allem bis zum Projektabschluss weitere fairkom Cloud Dienste erfolgreich anbinden.

Keycloak bietet eine 2-Faktorauthentifizierung an, die über alle Dienste eine zusätzliche Sicherheitsstufe bietet.

3.4 Arbeitspaket 4 – *Integration Cloud Services & Community*

Kurzbeschreibung der Haupttätigkeiten

- Cloud Community Implementation, integriert mit der Cloud Identity
- Sondierungs-Befragung & Usability Tests mit Usern

Besondere Erfolge/ Probleme

Keine

Gab es große Abweichungen zum Plan? Warum?

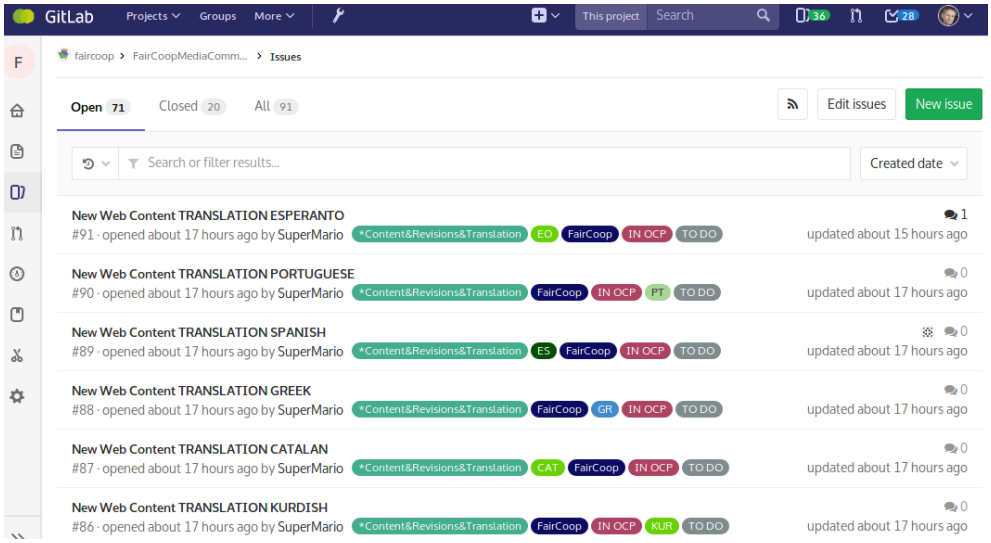
Keine

Erkenntnisse zur Vorgangsweise

Ende August 2017 haben wir fairlogin erstmals einer internationalen Community von AktivistInnen bei einem Sommercamp im Jura in der Schweiz präsentiert. Diese verwendete etwa 30 Webseiten, hunderte Etherpads und Telegram zur Koordination ihrer Aktivitäten. Der Vorschlag, mittels fairlogin das Management der Zugänge zu vereinfachen sowie eine gemeinsame ID zu nutzen stieß auf großes Interesse. Es wurden rasch Projekte auf GitLab angelegt sowie fairchat adaptiert, um wichtige Diskussionsgruppen zu spiegeln und mittelfristig nur mehr diese zu nutzen. Es folgte bald darauf die Anbindung deren WIKI Systems.

Darüber hinaus präsentierten wir am 17. und 18. November 2017 fairlogin bei einem Workshop vor etwa 25 IT-Verantwortlichen für Nachhaltigkeitsinitiativen in Wien. Ziel war es, einige davon über fairlogin anzubinden.

Auf nachhaltiges Interesse stießen wir beim Makers4Humanity Meeting in Gräfenhainichen zu Pfingsten 2018. Provider großer Nachhaltigkeitsplattformen wie wechange.de, kartevonmorgen.org oder human-connection.org beabsichtigen, in ihrem technischen Entwicklungsplan Single-Sign-On mit fairlogin zu integrieren.



3.5 Arbeitspaket 5 – *Dashboard Features*

Kurzbeschreibung der Haupttätigkeiten

- Dashboard Erweiterung (Federation, Quota Handling, Billing, Payment)
- Integration weiterer Services
- NutzerInnen-Tests

Besondere Erfolge/ Probleme

Der Aufwand, Anwendungen an fairlogin anzuschließen wurde von uns unterschätzt. Vor allem die dazu notwendigen Vorbereitungen, wie der Aufbau der Umgebungen und die notwendigen, umfassenden Tests der angebundenen Applikationen haben die Fertigstellung des Projekts zeitlich sehr verzögert.

Gab es große Abweichungen zum Plan? Warum?

Keine

Erkenntnisse zur Vorgangsweise

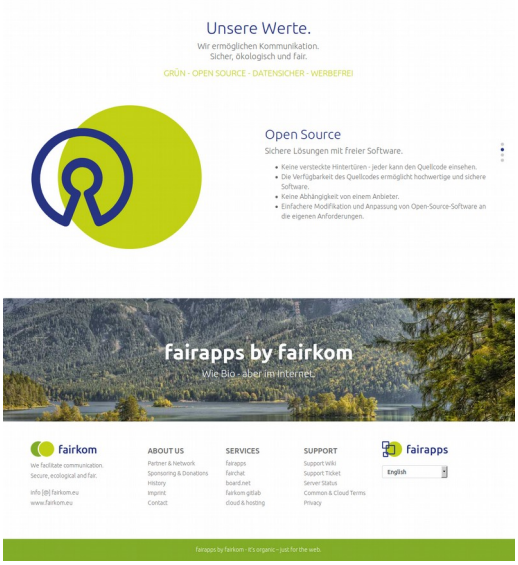
Wir entschieden im Laufe des Projektes, das Portfolio der Open Source Web Dienste von fairkom, die nun mit fairlogin verbunden waren, über ein gemeinsames Dashboard unter fairapps.net sichtbar zu machen.

Wir entschieden im Laufe des Projektes, das Portfolio der Open Source Web Dienste von fairkom, die nun mit fairlogin verbunden waren, über ein gemeinsames Dashboard unter fairapps.net sichtbar zu machen. Dabei ging es vornehmlich um Gestaltungsfragen und auch, wie die Eigenschaften „fairer“ Software und Services kommuniziert werden sollten.

Manche Anbindungen haben noch nicht die Güte erreicht, die man bei Single-Sign-On erwarten könnte. Etwa dass der Login Button auf der Startseite der fairchat Anwendung verschwindet, wenn man mit SSO angemeldet ist. Oder dass auch Single-Logout durchgehend auf allen Plattform funktioniert. Hier gibt es auch nach dem netidee Projekt noch Bedarf, die Anbindungen nachzuschärfen.

Nationale Tests wurden mit fairkom Bestandskunden sowie mit fairchat Usern durchgeführt. Internationale Tests wurden mit der FairCoop Community sowie mit VertreterInnen oben angeführter Plattformen durchgeführt, die einen fairchat Kanal, einen fairmeeting Videokonferenzraum sowie das board.net Etherpad von fairkom nutzt.

Mit der Entwicklung des fairapps.net mock-up und die darauf aufbauende Webseite konnten wir die Single-Sign-On Dienste anschaulich aufbereiten. Die zeitintensive Arbeit hat sich gelohnt, wie die Screenshots zeigen.



4 Liste Projektendergebnisse

Kurzbeschreibung der erreichten Projektendergebnisse jeweils mit Open Source Lizenz und Webadresse (netidee Vorgaben beachten!)

1	*Projektendbericht*	*CC-BY-SA 3.0 AT*	*netidee.at/fairlogin*
2	*Entwickler-Dokumentation vom Dashboard*	*CC BY-SA 3.0 AT*	*git.fairkom.net/fairlogin/fairkom/wikis*
3	*Anwender-Dokumentation*	*CC BY-SA 3.0 AT*	*git.fairkom.net/fairlogin/fairkom/wikis* *fairkom.eu/fairlogin/faqs*
4	*Veröffentlichungsfähiger Einseiter*	*CC BY-SA 3.0 AT*	*netidee.at/fairlogin* *fairkom.eu/fairlogin*
5	*Evaluierung von IdP Lösungen*	*CC-BY-ND*	*netidee.at/fairlogin*
6	*Einrichtung von KeyCloak als IdP*	*CC-BY-SA*	*git.fairkom.net/fairlogin/fairkom/wikis*

7	*Entwicklungsbericht vom Dashboard*	*GPL 3.0*	*git.fairkom.net/ fairlogin/dashboards/ fairapps*
8	*Interne Anwendungsintegration*	*GPL 3.0*	*git.fairkom.net/ fairlogin/fairkom*
9	*Einbindung von Externen Communities und Cloud Diensten*	*CC-BY-ND*	*git.fairkom.net/ fairlogin/faircoop/ issues*

5 Verwertung der Projektergebnisse in der Praxis

Angaben zur Verwertung der Projektergebnisse in der Praxis

Wir haben fairlogin nun intern sowohl mit SAML2, OIDC wie Authentifizierung per Webtechnologie als auch per LDAP für die Internen Dienste verwendet. Unter fairapps.net werden alle von fairkom betriebenen und angebundenen Applikationen dargestellt.

Technologie Anwendung	OIDC	SAML2	LDAP	Sonstige
Dashboard	Aktiv			
GroupOffice	geplant		Aktiv	
GitLab		Aktiv		OAuth
fairchat [Rocket Chat]	Aktiv			
ownCloud / nextcloud		WIP	Aktiv	
DokuWiki	Aktiv			
Discourse Forum		Aktiv		
Odoo ERP	WIP			
Redmine Projektmanagement	WIP			
ERPnext	Aktiv			

fairapps.net bietet nun Open Source SaaS in Paketen an:

- fairapps free
- fairapps basic
- fairapps pro
- fairapps für Organisationen

Die Kommunikation zu diesen Paketen, die an ERPnext zur Verrechnung angebunden sind, startet im Oktober 2018. Für Organisationen soll mit fairoffice ein attraktives Paket ausgebaut werden.

Weiters bieten wir ein Paket an, fremde Dienste an fairlogin anzubinden.

Die Föderierung mit der Bürgerkarte Österreich funktioniert, sollte jedoch noch formalisiert getestet werden.

6 Öffentlichkeitsarbeit/ Vernetzung

Beschreibung der im Rahmen Ihres netidee-Projektes bereits erfolgten bzw. noch geplanten Öffentlichkeitsarbeit oder Vernetzung

Erfolgte Öffentlichkeitsarbeit und Vernetzung:

- fairlogin wurde auf folgenden Veranstaltungen vorgestellt:
  - Linuxday Vorarlberg 2017
  - FairCoop Summercamp 2017
  - Change-IT-Camp Wien 2017
  - TIIME Conference Wien 2018 (facheinschlägig zu Identity Management)
  - Makers4Humanity Lab 2018
- Ankündigung sowie regelmäßige Blogbeiträge auf fairkom.eu und netidee.at
- Bewerbung auf SocialMedia Kanälen und Pressearbeit
- Verstärkte Vernetzungsarbeit und Austausch mit der FairCoop und Fairmove-IT Community sowie mit weiteren PartnerInnen
- Zielgruppenorientierte Öffentlichkeitsarbeit

Geplante Aktivitäten:

- Weitere Bewerbung auf SocialMedia Kanälen, Homepage und Pressearbeit

- Zusätzliche zielgruppenorientierte Öffentlichkeitsarbeit und Bewerbung bei weiteren Netzwerktreffen
- Vorstellung beim Linuxday Vorarlberg 2018; Messe WearFair +mehr 2018 sowie weiteren einschlägigen Veranstaltungen

7 Geplante Aktivitäten nach netidee-Projektende

Sind weiterführende Aktivitäten nach dem netidee-Projektende geplant?

Der Umfang des Projekts war uns anfangs nicht annähernd klar. Technologisch gab es zwar schon viele Projekte auf die man aufbauen konnte, jedoch zeigte sich schnell, dass diese alle sehr unterschiedliche Ausgangspunkte in der Implementation hatten und die Protokolle oft noch nicht von den Produktivversionen der Anwendungen unterstützt wurden, die wir und unsere Communties einsetzen.

Daher werden wir noch einige Zeit damit beschäftigt sein, sowohl bestehende Integrationen zu optimieren also auch Plugins voranzutreiben, um weiter Applikationen sowohl mit SSO über OIDC und SAML2 auszuweiten als auch die Berechtigungskonzepte umzusetzen.

Erst wenn sich hier in der Praxis besser anwendbare Konzepte in den IdP Lösungen etabliert haben, können wir diese Berechtigungskonzepte auch für unseren internen Gebrauch also auch für die Föderation sinnvoll einsetzen.

Daher wird fairlogin auf absehbare Zeit weiterentwickelt und angepasst werden, damit ein zuverlässiges Netz an Federated Identity Netzwerke im Nachhaltigkeitsumfeld den Mehrwert bietet, den wir uns erhoffen.

Der Aufbau einer sauberen Testumgebung, war auf Grund eines kleinen Teams schwierig. Für jede Änderung müsste eigentlich von einem Team an Entwicklern Tests auf einer umfassenden Infrastruktur durchgeführt werden. Dies wollen wir durch die Migration auf eine Docker basierte Containerlösung erreichen.

Der Code von unserem Dashboard und die Einrichtungshinweise von KeyCloak sind öffentlich zugänglich. Sie werden während der Integrationsarbeit von Anwendungen und Identity Providern stetig erweitert und angepasst. Die dabei errungenen Erkenntnisse und Herausforderungen werden wir auf einschlägigen Veranstaltungen und in der Community der Identity Provider thematisieren, um Zukünftig leichter Integrationen durchführen zu können.

8 Anregungen für Weiterentwicklungen durch Dritte

Welche Nutzungs- und Weiterentwicklungsmöglichkeiten für Dritte ergeben sich durch Ihr netidee-Projekt bzw. empfehlen Sie?

Eine wesentliche Weiterentwicklungsmöglichkeit wäre die konzeptionelle Ausarbeitung von Rollen, Berechtigungen und Zugehörigkeiten über diverse Services zu implementieren.

BenutzerInnen werden von einem Haupt IdP verwaltet, der Stammdaten und das Passwort des Users verwaltet. Die Dienste sollten von Service Providern verwaltet, in denen die Berechtigungen der Anwendungen abgebildet werden. Diese Berechtigungen sollten dabei auf der Seite der Service Provider in Rollen zusammengefasst werden können. Oft macht es Sinn, diese auch in Hierarchien zu organisieren.

Rollen könne aber auch im IdP verwendet werden, um die organisatorische Struktur abzubilden.

Interessant wird hier besonders die Zuordnung der organisatorischen Rollen eines IdP zu Berechtigungsrollen eines anderen föderierten Service Providers.

Wir hoffen, dies in naher Zukunft, vielleicht auch mit weiteren PartnerInnen umsetzen zu können.