Federation (Föderation)

FabAccess ist als selbstständiges selbstgehostetes System für jeden Space gedacht, so können die Spaces selber über das komplette System verfügen und es eigenständig bis in kleinste Detail konfigurieren. Um die Zusammenarbeit von Spaces zu ermöglichen und zu fördern, können die einzelnen FabAccess Instanzen (BFFH) mit einander föderieren. Dadurch können Nutzer zwischen diesen Spaces mit verringertem Verwaltungsaufwand hin und her wechseln. Wir wollen so die Spezialisierung von Spaces ermöglichen, ohne dass Nutzer die Vorteile eines vollausgestatten Spaces verlieren. Auch kleineren Spaces wird so der Einstieg vereinfacht.

Föderation ist dabei als aktive Zusammenarbeit erdacht, also müssen sich die Betreiber dieser Spaces dazu entscheiden zu föderieren. Jeder Space kann so den Partner für die Föderation selber wählen.

Der FabAccess Client Borepin ist bereits insofern für Föderation ausgelegt, als dass er mehrere Serveradressen und Benutzer speichern kann. So ist ein Wechsel zwischen verschiedenen Spaces und/oder Nutzermodellen praktisch möglich.

Vorteile und Ziele der Föderation

- beliebiger Wechsel der Nutzer verschiedener Spaces trotz technisch getrennter FabAccess-Instanzen
- Zusammenarbeit von Spaces unterstützen - durch Teilen von Berechtigungen ihrer Nutzerschaften
- FabAccess verbreiten, ähnlich wie das Matrix Chat-Protokoll dies mit Kommunikation macht
- kann langfristig dabei helfen, Maschinendokumentationen und Maschineneinweisungen (Maschinenführerscheinen) zu vereinheitlichen
- Spart NFC Karten (FabCards) ein, denn die Karten können dann in alle föderierten Spaces genutzt werden
- Mit Föderation is theoretisch auch das Bilden von standortübergreifenden Clustern möglich, also eine Art Filialbildung (das ist ein wertungsfreier Fakt)
- ist dabei als aktive Zusammenarbeit erdacht: die Betreiber der Spaces können sich selbst entscheiden, ob sie föderieren wollen. Föderation ist also immer optional und kann zudem jederzeit wieder deaktiviert werden

Modi oder Stufen der Föderation

Die folgenden Stufen bauen aufeinander auf, so können sich Betreiber einfacher an eine Föderation wagen und die Vorteile mit jeder Stufe erfahren.

1. Stufe (Authentifizierung: Teilen von Nutzern)

- Nutzer aus anderen Spaces können ihre FabCard auch in deinem Space verwenden
- Die Nutzer sind auch in deinem Space registriert
- Der föderierte Space übernimmt die Authentifizierung für den anderen Nutzer (wie bei SSO)

Unter dem Teilen von Nutzern verstehen wir, dass Nutzer von Space B bei dir im Space A sich mit der FabCard aus Space B authentifizieren können. Um bei dir im Space A die Maschinen nutzen zu dürfen, müssen die Nutzer aus Space B sich bei dir anmelden und deinen Nutzungsvertrag ausfüllen. Da die Nutzer aus Space B FabAccess schon kennen, werden Sie sich selbstständig registrieren und du musst nur nach einer kurzen Prüfung der Daten diese Nutzer akzeptieren. Dabei erhältst du immer die Kontaktdaten deiner Nutzer und bist nicht auf die Nutzerdaten des anderen Spaces angewiesen, sollte bei dir mal ein Unfall passieren. Die Authentifizierung der Nutzer übernimmt dann die BFFH Instanz des Space B. Um nicht immer mit jedem Space sofort aktiv föderieren zu müssen, ermöglichen wir es dir auch das Teilen von Nutzern für unbekannte Spaces zu erlauben. So kannst du nach einer aktiven Föderation mit dem anderen Space gleich die Nutzerdaten übernehmen, um so nicht noch mal alle Nutzer anzupassen. Bei einer Föderation sind nämlich die IDs der Nutzer in den beiden Spaces gleich und ermöglichen den nächsten Schritt in der Föderation.

2. Stufe (1. Stufe ergänzt um Teilen von Berechtigungen)

- Nutzer aus anderen Spaces können ihre FabCard und ihre Gruppen auch in deinem Space verwenden
- Die Nutzer sind auch in deinem Space registriert
- die Gruppen des anderen Space können in deinem Space verwendet werden, wenn zum Beispiel die gleichen Maschinen im Besitz sind. Das spart Zeit bei der Einweisung und der Dokumentation.

Nach dem das Teilen von Nutzern erfolgt ist und du sich mit dem Betreiber des Space B gut verstehst, stellt ihr beide fest, dass ihr einige gleiche Maschinen in euren Spaces besitzt. Da du dem Betreiber von Space B auch bei den Einweisungen von den Maschinen vertraust, könnt ihr in der 2. Stufe auch Berechtigungen teilen. Somit müssen Nutzer von Space B, die bei dir die gleiche Maschine wie im Space B verwenden wollen, von dir nicht noch mal eingewiesen werden. Das spart Zeit bei dir und bei den Nutzern von Space B. Du

behältst dabei die Kontrolle, welche Gruppen von Space B bei dir im Space A welche Maschinen nutzen können, somit kannst du dir sicher sein, dass die Nutzer wirklich eingewiesen sind.

3. Stufe (2. Stufe ergänzt um Teilen von Abrechnungen)

- Nutzer aus anderen Spaces können ihre Karte und ihre Gruppen auch in deinem Space verwenden
- Die Abrechung für diese Nutzter übernimmt dabei der andere Space für deinen Space. Über beispielsweise monatlich gesammelte Differenzrechnungen kann gegen den andere Spacecs abgerechnet werden. Das spart Zeit bei der Buchführung und die Nutzer können auch Ihre Rechnungen besser im Blick behalten.

Das Teilen von Abrechnungen stellt die letzte Stufe der Föderierbarkeit da. Da wir uns bei dem Thema noch nicht vollständig sicher sind, inwieweit das umgesetzt werden kann, steht es noch in Klammern. Die Idee zu der Föderation ist, dass Nutzer von Space B, die bei dir eine kostenpflichtige Maschine nutzen, ihre Abrechnung von Space B erhalten und nicht von dir. Das Geld der Nutzer von Space B kannst du dann mit dem Betreiber von Space B zum Beispiel monatlich verrechnen. Der Vorteil für den Nutzer liegt dabei darin, dass sie nicht bei jedem Space ihre Abrechnung machen müssen, sondern gesammelt bezahlen können.

Wie sicher ist Föderation?

Föderation benötigt Vertrauen, jedoch möchten wir nicht, dass dieses Vertrauen einfach missbraucht werden kann. Daher ist der oben beschriebene Ansatz, dass du jeden deiner Nutzer auch kennst.

Sicherheit des Servers

Für den Austausch von Benutzern und Berechtigungen ist ein sicherer Datenaustausch über das Internet notwendig. Das bedeutet auch, dass ein Dienst Ziel eines Angriffs von außen sein kann. Sobald der Dienst auf einem geöffneten Port lauscht, muss sichergestellt sein, dass nur authorisierte Server bzw. Personen darauf Zugriff haben und keinen Missbrauch begehen. Daraus ergeben sich verschiedene Fragen und Anforderungen, wie zum Beispiel

- erfolgt der Informationsaustausch zwischen den föderierenden Servern auf dem gleichen Port oder gibt es hierfür z.B. eine https-verfügbare API (z.B. REST, Json, XML RPC, ...)?

- wie wird das Verhalten gemonitored und Schadverhalten abgewehrt (z.B. Greylisting, Blacklisting, DDoS Vermeidung, Bruteforce-Login Attacken, Fail2Ban Jails, Firewall-Regeln...)
- welche APIs sind unterinander kompatibel? Nicht jeder Space wird schnell genug seinen Server auf die aktuelle Version updaten können
- Wie isolieren wir den FabAccess-Server ausreichend gegen Angriffe von außerhalb? Immerhin hat bffh Zugriff auf physische Geräte durch das Schalten von Strom an Aktoren

Sicherheit von FabFire Karten

Um die Authentifizierung sicher zu gestalten, haben wir uns für die etwas teureren NXP MIFARE DESFire EV2 Karten entschieden (ca. 1-5 € pro Karte bzw. Tag). Diese haben den Vorteil, dass sie ein Ende-zu-Ende (E2EE) Verfahren unterstützen und bisher als ungehacked gelten. Somit musst Du nicht die Schlüssel deiner Karten an jeden Reader in einem anderen Space verteilen, sondern deine BFFH Instanz kommuniziert verschlüsselt direkt mit der Karte. Auf den FabCards befinden sich auch keine Informationen der Nutzer, sondern nur der DNS-Eintrag deines Space sowie eine pseudonymisierte Nutzer ID. Somit wollen wir die technische Seite der Föderation absichern und eine Zusammenarbeit möglichst einfach gestalten.

Die Anforderungen an ein föderierbar einsetzbares SmartCard-System sind hoch, da so die jeweils andere Partei keine einfache Validierung der Karte durchführen kann. Auch das Authentifizieren mit einem Schlüssel gestaltet sich über Föderationen hinweg schwierig, da der Reader dem einen Space gehört und die Karte dem anderen. Ein Reader hat daher nicht immer die Schlüssel für die gelesenen Karten. Die DESFire-Karte besitzt ein Feature, mit dem eine Karte via OTA-Verfahren (Over-the-Air) direkt mit einem entfernten Server kommunizieren kann, ohne dass der Reader Schlüssel für die Karte benötigt. Der Reader übernimmt dabei nur die Rolle eines Proxys (Brücke/Vermittler). Mit diesem Ansatz stellen wir ein sicher föderierbares Kartensystem, was wir so bisher noch nicht im OpenSource-Bereich finden konnten.

Fragen und Ansprüche an Föderation und potentielle Probleme

- muss stabil sein
- es muss sicher sein (siehe oben)

- Benutzer und Berechtigungen anderer Spaces können sich ändern. Nutzer könnten dem Space nicht mehr angehören. Wie halten wir den Informationsstamm ausreichend aktuell?
- es müssen verschiedene Server-/API-Versionen interoperabel funktionieren
- es braucht eine Whitelist bzw. ggf. sogar Blacklist für alle Spaces, die für FabAccess nutzbar sein sollen
- Vertrags-, Datenschutz- und Haftungsfragen: ist die Übertragung der Nutzerdaten an andere Spaces geregelt, und wenn ja, wie? Welche vertraglichen Regeln müssen für eine Föderation mit FabAccess festgehalten werden?
- Föderierte Spaces arbeiten ggf. sehr unterschiedlich, was Maschineneinweisungen und Co. angeht - wie kann sichergestellt werden, dass dazu übergreifende Standards geteilt werden?

Stand der Föderation

> Das Feature Föderation ist aktuell (Stand Dezember 2024) noch nicht in FabAccess implementiert.

Wer nutzt heute schon FabAccess?

Potentielle Nutzer für FabAccess-Föderation findest du unter Mitmachen / Unterstützen / Join the Community

---

Version #13
Erstellt: 18 Oktober 2024 09:03:48 von Mario Voigt (Stadtfabrikanten e.V.)
Zuletzt aktualisiert: 14 Dezember 2024 17:19:33 von Mario Voigt (Stadtfabrikanten e.V.)