

Backlog

Wirtschaftsprojekt «px: PEAX Command Line Client»

Patrick Bucher

28.II.2019

#	User Story	Status	Story Points
1	Konfiguration sämtlicher Umgebungen	umgesetzt in Sprint 1	1
2	Erweiterung der CI-Pipeline	umgesetzt in Sprint 1	5
3	Login mit Zwei-Faktor-Authentifizierung	umgesetzt in Sprint 1	3
4	Sichere Verwahrung der Tokens	umgesetzt in Sprint 1	5
5	Handhabung mehrerer Umgebungen	umgesetzt in Sprint 2	3
6	Generische GET-Schnittstelle	umgesetzt in Sprint 2	3
7	Automatische Aktualisierung von Tokens	umgesetzt in Sprint 2	5
8	Login für Agent API	umgesetzt in Sprint 2	3
9	Verbesserung der Hilfe-Funktion	umgesetzt in Sprint 2	3
10	Vollzugsmeldungen mit -v/-verbose-Flag	umgesetzt in Sprint 2	1
11	Verbesserung der Quellcodedokumentation	umgesetzt in Sprint 3	1
12	Aktuelle Version ausgeben	umgesetzt in Sprint 3	1
13	Einliefern von Dokumenten per Agent API	umgesetzt in Sprint 3	3
14	Generische POST-Schnittstelle	umgesetzt in Sprint 3	3
15	Generische PUT-Schnittstelle	umgesetzt in Sprint 3	3
16	Generische PATCH-Schnittstelle	umgesetzt in Sprint 3	3
17	Generische DELETE-Schnittstelle	umgesetzt in Sprint 3	1
18	Rekursives Hochladen von Dokument-Ordern	geplant für Sprint 3	5
	Verbesserung der Testabdeckung	offen	
	Variablen in der Ressourcenangabe	offen	
	Automatische Formatierung von JSON-Ausgaben	offen	
	Automatische Tags von hochgeladenen Ordnern	offen	
	Anzeigen der aktiven Logins	offen	
	Auflisten von Dokumenten mit Suche/Filterung	offen	
	Ausführung von Befehlen für mehrere Umgebungen	offen	
	Fortschrittsanzeige bei längeren Vorgängen	offen	
	Ausgabe von Tokens	offen	
	Inspektion von Tokens	offen	
	Code für Login-Funktion vereinheitlichen	offen	

#	User Story	Status	Story Points
	Dokumente mit Metadaten hochladen	offen	
	Überarbeitung der README	offen	

Sprints

Sprint	Stories geplant	Stories umgesetzt	Aufwand	Stories offen	h/SP
1	6 (1-6), 20 SP	4 (1-4), 14 SP	14.5h	2 (5-6), 6 SP	1.05
2	6 (5-10), 18 SP	6 (5-10), 18 SP	20.5h	0	1.15
3	8 (11-18), 20 SP	7 (11-17), 15 SP	15.0h	1 (18), 5 SP	1.00

User Stories

Die User Stories haben drei Grössen: S (small: 1 Story Point), M (medium: 3 Story Points) und L (large: 5 Story Points). Diese Grössen dienen zur relativen Einschätzung der Story-Grössen zueinander, und sollen nicht in eine Stundenplanung heruntergerechnet werden. Vielmehr sollen sie dazu dienen, übergrosse Stories als solche zu erkennen, um diese herunterbrechen zu können. Am Ende eines jeden Sprints soll eingeschätzt werden, wie viele Story Points ungefähr machbar sind.

Story 1: Konfiguration sämtlicher Umgebungen

Als Entwickler möchte ich sämtliche relevanten PEAX-Umgebungen vorkonfiguriert haben, damit diese dem Nutzer zur Verfügung gestellt werden können.

Akzeptanzkriterien:

1. Es sollen die Umgebungen dev, test, devpatch, testpatch, stage, prod, perf und prototype zur Verfügung stehen.
2. Für jede Umgebung muss eine erreichbare URL zum jeweiligen Identity Provider und zu den relevanten APIs (User API, Admin API, Agent API) automatisch generiert werden können.

Notizen

- Die verschiedenen Umgebungen sind in einer statischen Liste aufgezählt.
- Die `init()`-Funktion des `env`-Moduls iteriert über diese Liste und generiert die URLs und Realm-Bezeichnungen anhand des Umgebungsnamens.

- Da bei prod benutzerfreundliche, kurze URLs verwendet werden, wird diese Umgebung separat gehandhabt.

Testprotokoll

- Der Unit Test `env_test.go` ist gemäss *Table Driven Test Design* (Donovan & Kernighan, 2015) entwickelt worden.
- Es wurde manuell mit Logins auf verschiedenen Umgebungen getestet.
- Die Umgebungen `perf` und `'prototype` waren heruntergefahren und konnten so nicht getestet werden.
- Auf der Umgebung `prod` stehen derzeit nur Benutzer mit Zwei-Faktor-Authentifizierung zur Verfügung. Da dies noch nicht umgesetzt
- Die Antworten wiesen wie erwartet die folgenden HTTP-Status auf:
 1. Login vor der Registrierung: 401 (nicht möglich)
 2. Login nach der Registrierung bzw. vor der Verifizierung: 403 (nicht möglich)
 3. Login nach der Verifizierung: 200 (erfolgreich)

Story 2: Erweiterung der CI-Pipeline

Als Entwickler möchte ich `px` in Skripts einbauen können, welche anschliessend in der CI-Pipeline berücksichtigt, d.h. ausgeführt werden.

Akzeptanzkriterien:

1. Der Ausführungsschritt `script` soll nur dann ausgeführt werden, wenn die vorherigen Schritte `build` und `test` erfolgreich waren.
2. Um der Pipeline ein weiteres Skript hinzufügen zu können, soll die neu erstellte Skriptdatei nur an einer einzigen Stelle (Konfigurationsdatei) hinzugefügt werden müssen.

Notizen

- Es wurde zunächst viel Zeit aufgrund mangelhafter Bash-Kenntnisse verloren, v.a. beim Iterieren über Liste von Skriptdateinamen.
- Das erste Akzeptanzkriterium wurde nur teilweise eingehalten. Zwar wird vor den Testskripts immer ein Build ausgeführt, um ein entsprechendes ausführbares Artefakt zur Verfügung zu haben, dies geschieht jedoch nicht über den `build`-Schritt, der ein Artefakt für Windows, Linux und macOS erstellt.
- Nach Überwindung der Anfangsschwierigkeiten konnte die Pipeline sehr schnell umgesetzt werden; der Aufwand wurde letztlich überschätzt.

- Zusätzlich wurde die Pipeline lokal ausführbar gemacht, indem die Umgebungsvariablen nicht zwingend von GitLab, sondern aus einem optionalen, lokalen Skript namens `envvars.sh` geladen werden.
- Der Shell-Code wurde zum Schluss überarbeitet und dabei vereinfacht.

Testprotokoll

- Zunächst wurde ein Skript erstellt, das die anderen Skripts ausführt.
- Es wurde je ein scheiterndes und ein durchlaufendes Skript erstellt und in die Testliste des vorher genannten Skript eingetragen.
- Die Pipeline wurde für GitLab (`.gitlab-ci`) konfiguriert. Der erste Test ist erfolgreich gescheitert, d.h. das scheiternde Skript hat die Pipeline wie gewünscht zum Abbruch gebracht.
- Das scheiternde Skript wurde nun aus der Liste der auszuführenden Tests entfernt, sodass die Pipelien nun durchlief.
- Es wurde ein minimales, jedoch produktives Testskript für `px help` erstellt und integriert.
- Es wurde ein Login-Testfall erstellt, der die Credentials als Umgebungsvariablen von der GitLab-Konfiguration bezieht.
- Die gescheiterten Loginversuche mit `px login` gaben zunächst den Status `0` zurück, was korrigiert werden musste.
- Das Login-Skript hat schliesslich wie gewünscht funktioniert.

Story 3: Login mit Zwei-Faktor-Authentifizierung

Als Benutzer möchte ich mich per Zwei-Faktor-Authentifizierung einloggen können, damit ich `px` auch mit entsprechend konfigurierten Zugängen verwenden kann.

Akzeptanzkriterien:

1. Die Abfrage des zweiten Faktors soll interaktiv passieren.
2. Es sollen die Authentifizierungsarten SMS und OTP (One-Time Password) unterstützt werden.
3. Das Login soll bei entsprechend konfigurierten Benutzerkonti auch weiterhin ohne Zwei-Faktor-Authentifizierung funktionieren.

Notizen

- Bevor die bestehende `login`-Funktion erweitert werden konnte, musste sie zunächst etwas aufgeräumt werden.

- Hierzu wurden verschiedene Teilaspekte (interaktive Abfrage fehlender Credentials, Erstellen des Requests und Parsen der Response) in eigene Funktionen ausgelagert.
- Die script-Pipeline zahlte sich bereits aus, zumal die login-Funktion direkt in `cmd/px.go` implementiert war und darum nicht durch einen Unit Test abgedeckt werden konnte.
- Das Refactoring wurde schliesslich ausgedehnt; es entstanden die neuen Untermodule `px/tokenstore` und `px/utils`.
- Es wurden neue Datenstrukturen erstellt, etwa für die Credentials (mit und ohne 2FA), und für den Login-Payload mit 2FA
- Der Code wurde neu organisieren, was nötig und sinnvoll war.

Testprotokoll

- Beim Refactoring traten immer wieder Build-Fehler auf, die jedoch einfach zu beheben waren.
- Logik-Fehler traten jedoch keine auf.
- Login-Versuche führten zunächst zu einem HTTP-Fehlerstatus 400 (Bad Request). Dieser Fehler wurde lange untersucht, einschliesslich einer Debugging-Session auf dem IDP-Server.
- Es stellte sich heraus, dass beim Login kein JSON-Payload unterstützt wird, sondern nur `form-urlencoded`; die serverseitige Fehlersuche stellte sich als sinnlos heraus.
- Nach der Umstellung von `application/json` auf `form-urlencoded` funktionierte die 2FA schliesslich problemlos.
- Das Login wurde mit SMS und TOTP erfolgreich manuell getestet. Automatisierte Tests sind aufgrund der interaktiven Eingabe inmitten des Prozesses nicht möglich.
- Das Login ohne 2FA wird weiterhin via Skript-Pipeline getestet.

Story 4: Sichere Verwahrung der Tokens

Als Benutzer möchte ich, dass beim Login geholte Tokens sicher lokal verwahrt werden, damit ein Angreifer diese nicht auslesen kann.

Akzeptanzkriterien:

1. Die Credentials (Benutzername und Password) werden zu keinem Zeitpunkt lokal persistent abgespeichert.
2. Refresh Tokens, die von der Produktivumgebung (`prod`) geholt werden, dürfen standardmässig nicht im Klartext abgespeichert werden.

3. Access und Refresh Tokens von nicht-produktiven Umgebungen, sowie Access Tokens der Produktivumgebung, können lokal im Klartext abgespeichert werden, sofern dies der einfacheren Bedienbarkeit zuträglich ist (weniger Passwortabfragen durch den Keystore).
4. Der Benutzer soll das Standardverhalten für die jeweiligen Umgebungen (produktiv: nur sichere Verwahrung; nicht-produktiv: Verwahrung im Klartext) mit den Kommandozeilenparametern `-safe` bzw. `-unsafe` übersteuern können.
5. Die sichere Verwahrung der Tokens muss Windows, macOS und Linux funktionieren.
6. Auf Systemen ohne GUI soll zumindest die unsichere Variante der Token-Verwahrung funktionieren.

Notizen

- Die Umgebungsconfiguration wurde um ein Flag (`Confidential`) erweitert, das besagt, ob für die jeweilige Umgebung die Tokens per default sicher oder unsicher verwahrt werden sollen.
- Die Library `zalando/go-keyring` kann Schlüssel auf Linux, macOS und Windows sicher im nativen Keystore verwahren.
- Die Konfiguration des nativen Keystores ist für jede Plattform anders und ist im README des Projekts dokumentiert.
- Bei einem Anwendungsfall wie dem Upload musste die Logik erweitert werden, so dass der sicher abgelegte Token für die Autorisierung verwendet werden kann.
- Die Tokens sind jeweils mit einem Schlüssel der Form `px:Umgebung:TokenTyp` abgelegt, z.B. `px:prod:accessToken` oder `px:test:refreshToken`.

Testprotokoll

- Der Unit Test `env_test.go` wurde um das `Confidential`-Flag erweitert, wobei nur `prod` entsprechend konfiguriert ist.
- Tests auf `prod` mit Linux (Tokens schreiben) funktionierten nachdem der Keystore mithilfe von `Seahorse` korrekt konfiguriert worden war.
- Der Skript-Test `ci-px-login-test.sh` wurde erweitert und in `ci-px-login-logout-test.sh` umbenannt, sodass fortan auch das Logout getestet wird.
- Darin wird nach dem Login mit `jq` geprüft, ob das Feld `access_token` für die Umgebung `test` in `~/ .px-tokens` vorhanden ist.
- Nach dem Logout wird das Fehlen desselben geprüft
- Auf Windows sind die Tokens in der Anwendung *Credential Manager* unter *Windows Credentials* zu finden.
- Auf macOS sind die Tokens in der Anwendung *Keychain Access* unter *login* zu finden.

Story 5: Handhabung mehrerer Umgebungen

Als Benutzer möchte ich, dass `px` meine Befehle standardmässig gegen die Umgebung ausführt, auf der ich mich zuletzt eingeloggt habe, damit ich nicht immer eine Umgebung per Kommandozeilenparameter anwählen muss.

Akzeptanzkriterien:

1. Es muss einen Unterbefehl geben, der mir die aktuelle Umgebung (d.h. die Umgebung, auf der sich der Benutzer zuletzt eingeloggt hat) anzeigt.
2. Es muss einen Unterbefehl geben, womit eine Umgebung mit bereits aktivem Logging als die Standardumgebung gesetzt werden kann.
3. Bei allen Befehlen, die gegen die API operieren, soll die Umgebung mit einem Kommandozeilenparameter `-e` bzw. `-env` spezifiziert werden können.
4. Fehlt der Parameter `-e` bzw. `-env`, ist die Standardumgebung zu verwenden (zuletzt eingeloggt bzw. manuell als Standard gesetzt via `px env`).

Notizen

- Inspiriert durch `oc project` soll `px` einen Unterbefehl namens `env` enthalten. Wird er ohne Parameter aufgerufen, zeigt er die aktuelle Arbeitsumgebung an. Wird er mit Parameter aufgerufen, wird die aktuelle Arbeitsumgebung entsprechend gesetzt, sofern ein Login (Token Pair) dazu existiert.
- Die Datenstruktur `TokenStore` wird dazu um ein Feld `DefaultEnvironment` erweitert, um die Umgebung über mehrere Aufrufe von `px` hinweg abzuspeichern.
- Das Wechseln auf eine unbekannte Umgebung oder auf eine Umgebung ohne Tokens ist nicht zulässig.

Testprotokoll

- Das Testskript `ci-px-env-test.sh` führt zunächst ein Login auf `test` aus und prüft dann direkt in `~/.px-tokens`, ob `test` die Standardumgebung ist.
- Es wird zudem geprüft, ob `px env` die gleiche Umgebung ausgibt, die in `~/.px-tokens` als Standard abgelegt ist.
- Um den Wechsel der Umgebung zu testen, musste ein weiteres Login eingerichtet werden.
- Das Testskript `ci-px-env-test.sh` verwendet dieses zusätzliche Login, um zwischen den Umgebungen `test` und `dev` hin- und herzuspringen.

Story 6: Generische GET-Schnittstelle

Als Benutzer möchte ich einen `get`-Befehl zur Verfügung haben, damit ich lesend auf meine Ressourcen zugreifen kann.

Akzeptanzkriterien:

1. Dem Befehl kann ein beliebiger Ressourcenpfad mitsamt Query-Parametern mitgegeben werden.
2. Die Base-URL der jeweiligen API und Umgebung wird dem Ressourcenpfad automatisch vorangestellt.
3. Im Falle eines erfolgreichen Zugriffs (200 OK) soll der resultierende Payload auf die Standardausgabe (stdout) ausgegeben werden.
4. Im Falle eines fehlerhaften Zugriffs soll der Status-Code auf die Standardfehlerausgabe (stderr) ausgegeben werden.

Notizen

- Eine komfortable Zusatzfunktion wäre, dass man Pfade nicht komplett mit der PEAX ID ausschreiben müsste (`document/api/v3/account/455.5462.5012.69/collection`), sondern einen Platzhalter wie `{peaxId}` verwenden könnte (`document/api/v3/account/{peaxId}/collection`). Dies soll jedoch nicht Bestandteil dieser Story sein.

Testprotokoll

- Das Testskript `ci-px-get-test.sh` führt ein Login auf test aus und lädt sich die Ressource `document/api/v3/account/455.5462.5012.69/collection`. Das Ergebnis wird mittels Pipe an `jq` weitergeleitet, das scheitern würde, wäre der Payload kein korrektes JSON.

Story 7: Automatische Aktualisierung von Tokens

Als Benutzer möchte ich dass ein Request, der aufgrund eines abgelaufenen Access Tokens scheitert, mit einem neuen Access Token erneut versucht wird, damit ich mich nicht ständig neu einloggen muss.

Akzeptanzkriterien:

1. Der Retry-Mechanismus soll für den Benutzer transparent sein.
2. Der neue Access Token soll anhand des Refresh Tokens ausgestellt werden.
3. Kann aufgrund eines abgelaufenen Refresh Tokens kein neuer Access Token geholt werden, soll dies dem Benutzer gemeldet werden.

Notizen

- Der Token Store wird im Hauptprogramm (`cmd/px.go`) derzeit wie eine Map (Key: Umgebung, Value: Token Pair) angesprochen. Auf die sicher verwahrten Tokens muss separat zugegriffen werden. Dieser Zugriff soll vereinheitlicht werden, was ein Refactoring erfordert.
- Das Usage Log, das die Anzahl Aufrufe und das Datum des letzten Aufrufs von `px` trackte, wurde entfernt.
- Sicher verwahrte Schlüssel werden neu in `./px-tokens` als Dummy-Eintrag abgelegt, sodass der Token Store ohne Zugriffe auf den Keystore über die Information verfügt, ob zu einer Umgebung überhaupt ein sicher verwahrter Schlüssel vorhanden ist.
- Bei den Dummy-Einträgen für sicher verwahrte Tokens wurde zunächst ein eigenartiger Datumswert abgelegt. Hierbei handelte es sich um den Zero-Wert der Struktur `time.Time`. Das Problem konnte behoben werden, indem `time.Time` als Pointer statt als Wert verwendet wird.
- Um den automatischen Retry-Mechanismus umzusetzen, musste zuerst herausgefunden werden, wie man anhand des Refresh Tokens einen neuen Access Token erhalten kann. Dies passiert über den gleichen Endpoint wie das Login, nur dass die Credentials mit dem `grant_type=refresh_token` (statt `grant_type=password`) und dem Refresh Token als Payload (statt Benutzername/Passwort) mitgegeben werden. Dieser Mechanismus wurde per Reverse Engineering ermittelt. Hierzu kann man sich auf dem Portal einloggen, für über fünf Minuten warten, eine Aktion auslösen, die mit dem Server kommuniziert – und schon sieht man den entsprechenden Request ablaufen.
- Die Zwei-Faktor-Authentifizierung läuft ab als Folge von Request, Response, Request, wobei vor dem zweiten Request eine interaktive Eingabe des Benutzers (SMS- oder TOTP-Code) erforderlich ist. Um die Konsoleneingabe vom Request-Mechanismus zu entkoppeln, wurde die Funktion `requestTokenPair` um einen Funktionsparameter namens `secondFactorPrompt` erweitert. Eine entsprechende Funktion `promptSecondFactor` erwartet einen String als Prompt (z.B. "SMS Code" oder "OTP Code", fragt die entsprechende Information vom Benutzer ab und gibt sie zurück – oder einen Fehler, falls die Eingabe abgebrochen wurde. Dank dieser Entkopplung konnte der Request-Code grösstenteils aus dem Hauptprogramm entfernt werden.
- Nachdem aller Code, der HTTP-Requests verwendet, von `cmd/px.go` in das `requests`-Modul verschoben werden konnte, hatte das Hauptprogramm keine Referenz mehr auf das HTTP-Package.
- Der ursprüngliche Ansatz, einen Request (mit aktualisiertem Authorization-Header) erneut abzuschicken, funktioniert leider nicht bei Requests mit einem Body. Grund dafür ist, dass der Request Body bei diesem Vorgang konsumiert wird. Der Request muss also für den erneuten Versuch neu aufgebaut werden. Im neuen Lösungsansatz erwartet zentrale Funktion `doWithTokenRefresh` nicht

mehr einen blossen Request zur Ausführung, sondern eine Funktion, die einen entsprechenden Request generiert. So können die Implementierungsdetails vom Retry-Mechanismus entkoppelt werden.

- Beim Anfordern eines neuen Token Pairs anhand des Refresh Tokens wird nicht ein neuer Access Token ausgestellt, es wird auch der Refresh Token aktualisiert. Somit kann ein Benutzer nach einem Login so lange mit px arbeiten, wie er will, solange zwischen zwei Requests nicht mehr als 30 Minuten vergehen. Wichtig ist, dass auch der aktualisierte Refresh Token im Token Store abgelegt wird.

Testprotokoll

- Verschiedenste Skripts schlugen nach dem Refactoring zunächst fehl. Der env-Befehl funktionierte zunächst nicht mehr. Dies konnte aber mit der neuen Token-Store-Schnittstelle schnell korrigiert werden. Die Skript-Pipeline hat sich dabei als sehr hilfreich erwiesen.
- Das Testskript `standalone-px-upload-test.sh` führt einen Login aus, lädt ein Dokument hoch, wartet etwas länger als fünf Minuten (Gültigkeitsdauer eines Access Tokens) und lädt das Dokument erneut hoch. Da dieser Testfall naturgemäss sehr lange dauert, wird er nicht in die automatische Pipeline integriert, sondern kann bei Bedarf manuell ausgeführt werden.
- Tatsächlich wurde mithilfe dieses Testskripts ein Fehler erkannt: Bei erneuten Versuch eines Requests wurde zwar ein neuer Access Token vom IDP geholt, der neue Request wurde jedoch noch mit dem alten Access Token erstellt, was naturgemäss fehlschlägt. Nach der entsprechenden Korrektur lief der Test dann erfolgreich durch.
- Das Skript `standalone.sh` bietet Hilfestellungen für solche Standalone-Testskripts, indem etwa der Kompilierungsschritt und das Aufräumen nach dem Test vorgegeben wird.
- Für den `get`-Befehl wurde ein testgetriebenes Vorgehen gewählt: `standalone-px-get-test.sh` wurde zuerst als Skript erstellt, das wie geplant scheiterte. Nachdem der `get`-Befehl auch mit Token Refresh arbeitete, funktionierte das Skript anschliessend.

Story 8: Login für Agent API

Als Benutzer möchte ich mich mit als Agent einloggen können, um anderen Benutzern Dokumente einliefern zu können.

Akzeptanzkriterien:

1. Das Login für Agents soll mit einem anderen Subcommand als `login` funktionieren (Vorschlag: `agent-login`).

2. Die Tokens sollen nach der gleichen Logik sicher bzw. unsicher verwahrt werden wie diejenige für die User API.
3. Die Agent Tokens sollen unabhängig von den User Tokens gespeichert werden, d.h. auf einer Umgebung kann gleichzeitig ein User Token und ein Agent Token abgespeichert werden.
4. Der env-Befehl soll keine Agent Tokens berücksichtigen: Ein agent-login ändert die Standardumgebung nicht.

Notizen

- Da login und agent-login die gleichen Flags verwenden, wurde das Parsen der Befehlszeile refactored. Beide Funktionen (login und agentLogin) können nun die gleiche Logik für das Ermitteln der Kommandozeilenoptionen verwenden.
- Beim Login für die Agent API werden eine Client ID und ein Client Secret verwendet, bei User Login eine Client ID, ein Benutzername und ein Passwort. Beim Login-Request unterscheiden sich nur die beiden Payloads, welche mit den Strukturen Credentials und AgentCredentials umgesetzt werden. Die gemeinsame Methode ToFormDataURLEncoded ist in einem Interface definiert, womit der Payload für die beiden Logins abstrahiert werden kann.
- Da neu pro Umgebung mehrere Tokens (Agent und User) abgelegt werden können, muss die Datenstruktur hinter dem Token Store angepasst werden. Bestand der Key vormals nur aus dem Namen der Umgebung, ist es neu eine Kombination aus dem Typ des Tokens ("user", "agent") und der Umgebung. Diese Anpassung erfordert ein Refactoring. Gerade die der logout-Befehl manipulierte die zugrundeliegende Map noch selber. Neu wird dies über eine Methode RemoveToken gemacht. Ein ergänzender agent-logout-Befehl wird zudem benötigt.
- Die Keys im Secret Token Store müssen ebenfalls um den TokenType erweitert werden, um zwischen user- und agent-Tokens unterscheiden zu können.

Testprotokoll

- Zunächst mussten die entsprechenden Credentials (Client ID und Client Secret) auf GitLab hinterlegt werden, um das Login damit testen zu können.
- Aufgrund des Refactorings sind zunächst Unit Tests und Skrittests fehlgeschlagen. Das Zeichen : als Key-Separator zwischen Token Type (agent, user) und Umgebung funktioniert nicht mit dem Utility jq zusammen, das zur Extraktion der JSON-Datenstrukturen in der Test-Pipeline dient. Darum wurde es durch einen Underscore _ ersetzt.
- Der Skrittests ci-px-agent-login-logout-test.sh funktioniert analog zum Testfall ci-px-login-logout-test.sh, nur dass er die Befehle agent-login und agent-logout statt login bzw. logout verwendet.

Story 9: Verbesserung der Hilfe-Funktion

Als Benutzer möchte ich eine ausführliche Hilfefunktion für px als Ganzes wie auch für die einzelnen Subcommands haben.

Akzeptanzkriterien:

1. Es muss eine generische Hilfefunktion `px help` geben.
2. Es muss für jeden Subcommand eine Hilfefunktion `px help [subcommand]` oder `px [subcommand] -h` geben.

Für zukünftige User Stories ist die Hilfefunktion entsprechend nachzuführen.

Notizen

- Das von der Go Standard Library zur Verfügung gestellte `flag`-Modul stellt mit dem Flag `-h` eine Hilfefunktion zur Verfügung, die mit der Syntax `'px [subcommand] -h` aufgerufen werden kann. Diese Funktion ist sinnvoll zum Verständnis der Flags, jedoch ungenügend.
- Der bereits existierende Befehl `px help` (ohne Parameter) zeigt einen Überblick über alle Subcommands an. Diese Funktion ist sinnvoll und soll beibehalten werden. Zusätzlich soll es für jeden Subcommand eine ausführliche Hilfestellung geben, die mittels `px help [subcommand]` aufgerufen wird. `px [subcommand] -h` ist weiterhin für die Erläuterung der Flags zuständig.
- Die derzeitige `main()`-Funktion prüft den eingegebenen Subcommand mittels `switch/case`-Kontrollstruktur. Da die meisten Subcommand-Funktionen der gleichen Signatur folgen – den `TokenStore` erwarten und nichts als einen `error` zurückgeben, können die Beziehungen zwischen eingegebenem Befehl ("`agent-login`") und der aufzurufenden Funktion ("`agentLogin`") mit einer Map modelliert werden. Als Key wird der Befehlsname verwendet, als Value eine Struktur bestehend aus der auszuführenden Funktion – und einer Funktion, die einen Hilfestring zurückgibt.
- Die wenigen Befehle, deren Funktion eine andere Signatur haben, werden weiterhin per `switch/case` abgehandelt. Sie sind trotzdem in der Map abgelegt, wobei die Funktion den Wert `nil` hat. Einen Hilfestring-Funktion enthalten die Einträge in der Map dennoch für jeden Befehl.
- Die Hilfetexte werden als öffentliche Funktionen im Untermodul `help` abgelegt. Für statische Hilfetexte werden mehrzeilige Strings verwendet. Die Hilfe zur Login-Funktion ist etwa per `help.Login()` abrufbar. Andere Texte werden dynamisch generiert, z.B. um alle verfügbaren Umgebungen aufzulisten.
- Jeder Hilfetext enthält neben einer Erklärung des Befehls auch beispielhafte Aufrufe und Verweise auf die Hilfsfunktion zu den jeweiligen Flags, sowie Hinweise auf andere Befehle.

Testprotokoll

- Das Testskript `ci-px-help.sh` ruft die Hilfefunktion auf und prüft, ob dies fehlerfrei abläuft. Das Skript wurde erweitert, sodass es über alle verfügbaren Befehle iteriert, und für jeden dieser Befehle die Hilfefunktion aufruft. Es wird geprüft, ob dies erstens fehlerfrei passiert, und ob der dabei zurückgelieferte Text zweitens kein leerer String ist.
- Nach zahlreichen manuellen Tests wurden die Hilfetexte verbessert.

Story 10: Vollzugsmeldungen mit `-v/-verbose-Flag`

Als Benutzer möchte ich Vollzugsmeldungen aktivieren können, damit ich sehen kann, ob ein Vorgang erfolgreich war.

Akzeptanzkriterien:

1. Es sollen für alle bestehenden Befehle entsprechende Meldungen erstellt werden, wo ein Erfolg nicht schon anderweitig dem Benutzer gemeldet wird.
2. Die Vollzugsmeldungen sollen mit dem Flag `-v` bzw. `-verbose` aktiviert werden.

Notizen

- Von den bestehenden Befehlen produzieren folgende bereits eine Ausgabe im Erfolgsfall:
 - `px help`: Es wird die gewünschte Hilfefunktion angezeigt.
 - `px upload`: Es wird das serverseitig generierte Metadaten-Objekt in seiner JSON-Repräsentation ausgegeben.
 - `px get`: Es wird die geladene Ressource in ihrer JSON-Representation angezeigt.
 - `px env` (ohne Angabe der Umgebung): Es wird die Standardumgebung angezeigt
- Bei den folgenden Befehlen wird im Erfolgsfall keine Ausgabe erzeugt:
 - `px login`
 - `px logout`
 - `px agent-login`
 - `px agent-logout`
 - `px env` (mit Angabe einer Umgebung)
- Die letztgenannten Befehle wurden jeweils mit den Flags `-v` und `-verbose` ausgestattet, die eine kurze Vollzugsmeldung mit relevanten Kontextinformationen (Benutzername und Umgebung beim Login, Umgebung bei Setzen der Umgebung mit `px env`).

Testprotokoll

- Folgende Testskripts wurden erweitert, indem jeweils ein Aufruf mit dem `-v/-verbose`-Flag vollzogen und auf eine entsprechende Ausgabe überprüft wird:
 - `ci-px-env-test.sh`: für `env`
 - `ci-px-login-logout-test.sh`: für `login` und `logout`
- Für den Negativtest wurde jeweils das Flag `-v/-verbose` beim Aufruf im Testskript weggelassen. Nachdem das Flag hinzugefügt wurde, liefen die Tests durch.

Story 11: Verbesserung der Quellcodedokumentation

Als Entwickler möchte ich Dokumentationskommentare zu allen exportierten Elementen (Datentypen, Funktionen/Methoden usw.) haben, damit die Schnittstellen besser verständlich und anderen Entwicklern einfacher zu erläutern sind.

Akzeptanzkriterien:

1. Die Kommentare sollen den den Best Practices entsprechen.
2. Das Werkzeug `go lint` soll über die ganze Codebasis von `px` keine Beanstandungen im Bezug auf undokumentierte, exporte Elemente mehr machen.
3. Dieser Zustand ist auch in Zukunft am Ende eines jeden Sprints herzustellen. Die Aufwände für das Erstellen der entsprechenden Kommentare fließt jeweils in die User Story ein, die neue exportierte (d.h. zu kommentierende) Elemente zur Folge hat.

Notizen

- Das `Makefile` wurde um das Target `lint` erweitert, das den Go-Linter für das ganze Projekt aufruft.
- Um das Package `px` zu dokumentieren, wurde eine neue Datei `px.go` im Root-Verzeichnis des Projekts erstellt, die nur eine kommentierte package-Deklaration enthält.
- Bei Go wird jedes gross geschriebene Symbol exportiert, d.h. anderen Packages zur Verfügung gestellt, was einen Dokumentationskommentar erfordert. Für jede Beanstandung vom Go-Linter soll nicht einfach blind ein solcher Kommentar erstellt, sondern geprüft werden, ob das Feld wirklich exportiert werden muss. Eine kleinere externe Schnittstelle erfordert weniger Dokumentation.
- Die Command-Datenstruktur und ihre Eigenschaften im `main`-Package werden mittels Kleinschreibung nicht länger exportiert.

Testprotokoll

- Der Go-Linter beanstandete zunächst 71 fehlende Kommentare.
- Nach der ersten Session konnten die Beanstandungen auf 36 reduziert werden.
- Nach einer zweiten Session von ungefähr gleicher Länge hab es keine Beanstandungen von golint mehr.

Story 12: Aktuelle Version ausgeben

Als Anwender möchte ich einen Befehl zur Verfügung haben, der die Version von px ausgibt, damit ich sehen kann, ob ich die aktuelle Version der Software verwende, und diese bei Rückmeldungen verwenden kann.

Akzeptanzkriterien:

1. Die Versionierung soll gemäss *Semantic Versioning* erfolgen.
2. Die Version soll beim Kompilieren von Release-Artefakten automatisch aus dem SCM (git) verwendet werden.
3. Die Versionsangabe soll über den Befehl `px version` in der Form `v0.3.1` ausgegeben werden.

Notizen

- Die jeweils aktuelle Versionsangabe wird aus dem SCM mittels `git describe --tags` ermittelt.
- Die uninitialisierte, exportierte String-Variable `Version` in `cmd/px.go` wird mit dem Parameter `-ldflags="-X main.Version=$(git describe --tags)` mit der jeweils aktuellen Versionsangabe initialisiert.
- Die bestehenden Targets `build/mac/px`, `build/linux/px` und `build/windows/px.exe` werden im Makefile mit dem entsprechenden Parameter (als Variable `LDFLAGS`) ausgestattet.
- Das Makefile wurde um ein zusätzliches Target `px` ergänzt, das eine ausführbare Version im aktuellen Arbeitszeichnis (für die jeweilige Plattform) mitsamt Versionsangaben erstellt. Andernfalls müsste zum Testen von `px version` jeweils `go run` mitsamt `-ldflags` aufgerufen werden.

Testprotokoll

- In einem Branch wird die Tag-Nummer jeweils um die Anzahl der Commits und die ersten sieben Stellen des letzten Commit-Hashes ergänzt. Der Tag `v0.2.4-9-gdc83825` sagt etwa aus, dass es sich um Version `0.2.4` mit zusätzlichen neun Commits handelt, und nach dem Präfix `g` die ersten sieben Stellen des letzten Commit-

Hashes (dc83825, hexadezimal) stehen. Das ist nützlich für ad-hoc erstellte Zwischenreleases.

- Im master-Branch wird nur die Tag-Nummer verwendet.
- Das Testskript `ci-px-version.sh` überprüft, ob `px version` einen String zurückgibt, welcher dem regulären Ausdruck `^v[0-9]+\.[0-9]+\.[0-9]+(-[0-9]+-g[0-9a-fA-F]{7})?$` entspricht.
- Der Build-Step der CI-Pipeline muss sicherstellen, dass die Versionsangaben ebenfalls mitkompiliert werden.

Story 13: Einliefern von Dokumenten per Agent API

Als Benutzer der Agent API möchte ich ein einzelnes Dokument mitsamt Metadaten einliefern können, um so Testdaten für verschiedene Benutzer erstellen zu können.

Akzeptanzkriterien:

1. Es sollen alle Dateiformate unterstützt werden, welche von der Delivery-Schnittstelle zugelassen sind.
2. Die Metadaten werden als JSON-Datenstruktur aus einer separaten Datei mitgegeben.
3. Der Befehl zur Einlieferung von Dokumenten soll `px deliver` heissen.

Notizen

- Zunächst wurden die Hilfetexte verfasst, womit auch die Flags für den Befehl festgelegt wurden (`-m/-meta` für die JSON-Metadaten).
- Der Token-Refresh-Mechanismus für die Agent API war noch nicht implementiert. Dies nachzuholen erforderte verschiedene Erweiterungen am Token Store, etwa das Extrahieren/Abspeichern der `clientID`, da diese bei der Agent API im Gegensatz zur User API, wo sie immer `peax.portal` lautet, sich bei jedem Agent unterscheidet.
- Verschiedene manuelle Tests mit einem gültigen Refresh Token ergaben, dass die Aktualisierung eines Token Pairs für die Agent API mit dem `grant_type=refresh_token` (derzeit?) nicht funktioniert. Da die automatische Token-Aktualisierung kein Akzeptanzkriterium ist, und das Problem serverseitig geprüft werden muss, soll diese Funktionalität vorerst offen bleiben.

Testprotokoll

- Der automatische Token Refresh funktionierte zunächst nicht für die Agent API.

- Der delivery-Endpoint gibt nach einer erfolgreichen Einlieferung nicht etwa den HTTP-Status-Code 201 Created sondern 200 OK zurück, wodurch der erste erfolgreiche Test als fehlerhaft interpretiert worden ist.
- Beim Einliefern eines Dokuments kommt ein JSON-Payload mit einem id-Feld zurück, das eine UUID ist. Eine UUID ist eine Sequenz von hexadezimalen Ziffern, die in Gruppen der Grössen acht, vier, vier, vier und zwölf auftreten; dazwischen steht ein Bindestrich. Das Testskript `ci-px-deliver-test.sh` prüft, ob nach dem Einliefern eines Dokuments mit Metadaten eine UUID dieser Form zurückkommt.
- Beim ersten Ausführen der Testpipeline ist es passiert, dass der Backend-Service `portal-document` nicht mehr verfügbar war, und die Tests somit wohl fälschlicherweise gescheitert sind.
- Der Token-Refresh-Mechanismus für die Agent API wurde mithilfe des Testskripts `standalone-px-deliver-retry-test.sh` getestet, wobei zwischen dem ersten und zweiten Versuch etwas mehr als fünf Minuten gewartet wird.
- Das Testskript `ci-px-help-test.sh` wurde um den Aufruf `px help deliver` erweitert.

Story 14: Generische POST-Schnittstelle

Als Benutzer der User API möchte ich einen beliebigen Endpoint mittels POST-Methode ansprechen können, damit ich Ressourcen auf dem PEAX-Portal erstellen kann.

Akzeptanzkriterien:

1. Der angegebene Ressourcenpfad wird automatisch anhand der Umgebungsinformationen zu einer URL ergänzt.
2. Es können beliebige Payloads im JSON-Format angegeben werden.
3. Der Payload soll als separate Datei angegeben werden können.
4. Falls die Anfrage einen Payload zurückliefert, soll dieser auf `stdout` ausgegeben werden.
5. Der Befehl soll `px post` heissen.

Notizen

- Wiederum wurde mit dem Erstellen der Hilfetexte begonnen.
- Der Befehl wurde analog zu `px get` mit automatischem Erneuern der Tokens umgesetzt.
- Bei der Implementierung war kein Refactoring nötig. Die Codebasis scheint somit in einem gut erweiterbaren Zustand zu sein.

Testprotokoll

- Es wurde das Testskript `ci-px-post-test.sh` erstellt, das sich auf der Umgebung `test` einloggt, dort eine neue Organisation erstellt, und sich wieder ausloggt. Es wird mit `jq` geprüft, ob der Response-Payload valides JSON ist.
- Andere Endpoints, z.B. das Erstellen von Tags, wurden manuell getestet. (Ressourcen wie Tags haben eindeutige Namen, d.h. mit dem gleichen Payload kann die Ressource nur einmal erstellt werden, was für wiederholte, automatisierte Tests schlecht geeignet ist.)
- Das Testskript `ci-px-help-test.sh` wurde um den Aufruf `px help post` erweitert.

Story 15: Generische PUT-Schnittstelle

Als Benutzer der User API möchte ich einen beliebigen Endpoint mittels PUT-Methode ansprechen können, damit ich bestehende Ressourcen auf dem PEAX-Portal ersetzen kann.

Akzeptanzkriterien:

1. Der angegebene Ressourcenpfad wird automatisch anhand der Umgebungsinformationen zu einer URL ergänzt.
2. Es können Payloads verschiedener Formate mitgegeben werden (JSON, PNG usw.).
3. Der Payload soll als separate Datei angegeben werden können.
4. Der Befehl soll `px put` heissen.

Notizen

- Die API von PEAX bietet nur sehr wenige Endpoints an, die PUT unterstützen. Das einzige Beispiel, das auf Anhieb ermittelt werden konnte, ist die Aktualisierung des Profilbildes. Da es sich hierbei nicht um JSON-Daten handelt, sondern um ein Bild beliebigen Formats, muss der MIME-Type des Payloads automatisch ermittelt werden. Hierzu wurde im Package `utils` eine Funktion `utils.DetectContentType` entwickelt.
- Zunächst wurde wieder der Hilfetext verfasst.
- Der Befehl ist wie `get` und `post` mit automatischer Token-Erneuerung umgesetzt worden.
- Zusätzlich wurde eine Utility-Funktion `ReadFile` entwickelt, die einen `io.ReadCloser` auf die angegebene Datei sowie den Content-Type zurückgibt. Der `ReadCloser` hat den Vorteil, dass nicht die ganze Datei in den Arbeitsspeicher gelesen werden muss.

Testprotokoll

- Die Funktion `utils.DetectContentType` wird durch einen Unit Test abgedeckt. Hierzu wurde zunächst mit `GraphViz` ein kleiner Graph erstellt (`graph.dot`), woraus mithilfe von `dot` verschiedenste Formate generiert werden konnten: GIF, JPEG, PDF, PNG und PostScript.
- Der Testfall `TestDetectContentType` arbeitet eine Map ab, welche die Dateipfade der generierten Grafiken zu ihrem manuell ermittelten Mime-Type zuordnet. Für jede Iteration wird geprüft, ob für die jeweilige Datei der passende Mime-Type ermittelt werden kann. Für GIF, JPG, PDF, PNG und PostScript hat das auf Anhieb funktioniert.
- Das Testskript `ci-px-put-test.sh` aktualisiert das Profilbild dreimal: im PNG, im JPEG und schliesslich im GIF-Format.
- Das Testskript `ci-px-help-test.sh` wurde um den Aufruf `px help put` erweitert.

Story 16: Generische PATCH-Schnittstelle

Als Benutzer der User API möchte ich einen beliebigen Endpoint mittels PATCH-Methode ansprechen können, damit ich Ressourcen auf dem PEAX-Portal partiell/feingranular aktualisieren kann.

Akzeptanzkriterien:

1. Der angegebene Ressourcenpfad wird automatisch anhand der Umgebungsinformationen zu einer URL ergänzt.
2. Es können JSON-Payloads gemäss RFC6902 mitgegeben werden, wobei der Payload lokal nicht überprüft werden muss.
3. Der Payload soll als separate Datei angegeben werden können.
4. Falls die Anfrage einen Payload zurückliefert, soll dieser auf `stdout` ausgegeben werden.
5. Der Befehl soll `px patch` heissen.

Notizen

- Es wurden wiederum zuerst die Hilfetexte verfasst.
- Da die Command-Funktionen für die generischen HTTP-Funktionen POST, PUT und PATCH die gleichen Flags verwenden (Environment und Payload, inkl. Kurzformen, konnten deren Verarbeitung mit einer Funktion vereinheitlicht werden.
- Weitere Vereinheitlichungen gab es im `requests`-Package; so unterscheiden sich bei POST, PUT und PATCH nur die HTTP-Methoden; bei PUT wird jedoch kein Payload zurückgeliefert.

- Der Rest der Implementierung ist analog zu POST, ausser dass der Header Content-Type nicht einfach application/json, sondern application/json-patch+json lautet (siehe RFC6902).

Testprotokoll

- Das Testskript `ci-px-patch-test.sh` lädt zuerst ein PDF-Dokument per `px upload` hoch. Die UUID des hochgeladenen Dokuments wird ausgelesen. Anschliessend werden die Metadaten dieses Dokuments mittels `px patch` verändert. Für den Ressourcenzugriff wird die zurückgegebene UUID vom ersten Schritt (`px upload`) verwendet. Die PATCH-Operation liefert wiederum Metadaten zurück. Die UUID des modifizierten Dokuments wird wiederum extrahiert und gegen die ursprüngliche UUID auf Gleichheit geprüft. (Natürlich ändert sich die UUID im Fehlerfall nicht; es geht nur darum, den Erfolg der Operation mittels korrekt zurückgelieferter Metadaten zu überprüfen).
- Der Test schlug zunächst fehl, weil fälschlicherweise der `application/json` statt `application/json-patch+json` als Content-Type-Header verwendet worden ist. Nach dieser Korrektur lief er durch.
- Das Testskript `ci-px-help-test.sh` wurde um den Aufruf `px help patch` erweitert.

Story 17: Generische DELETE-Schnittstelle

Als Benutzer der User API möchte ich einen beliebigen Endpoint mittels DELETE-Methode ansprechen können, damit ich Ressourcen auf dem PEAX-Portal entfernen kann.

Akzeptanzkriterien:

1. Der angegebene Ressourcenpfad wird automatisch anhand der Umgebungsinformationen zu einer URL ergänzt.
2. Es soll *kein* Payload mitgegeben werden können.
3. Der Befehl soll `px delete` heissen.

Notizen

- Da `delete` in Go ein reserviertes Keyword ist, musste auf einen anderen Funktionsnamen für den Befehl (`dlete`) ausgewichen werden.
- Es wurden wiederum zunächst die Hilfetexte verfasst.
- Die Request-Logik konnte mit wenig Aufwand analog zu `px get` umgesetzt werden, wobei hier kein Payload zurück- und ausgegeben wird.

Testprotokoll

- Da Testfälle wiederholbar ausführbar sein müssen, wurde für DELETE kein neues Testskript erstellt. Stattdessen werden bestehende Testskripts, die Ressourcen erzeugen, um eine Löschung derselben erweitert.
- Es stellte sich heraus, dass das Profilbild (siehe Testprotokoll zu `px put`) die einzige in den Testskripts erstellte Ressource ist, die auch gelöscht werden kann. Dementsprechend wurde das Testskript `ci-px-put-test.sh` um die Löschung des Profilbildes erweitert und zu `ci-px-put-delete-test.sh` umbenannt.
- Ein erster Aufruf schlug fehl, da beim Authorization-Header der Abstand zwischen Bearer und dem Access Token vergessen worden war. Nach dieser Korrektur lief das Skript durch. Das Profilbild verschwand damit aus dem Portal.
- Das Testskript `ci-px-help-test.sh` wurde um den Aufruf `px help delete` erweitert.

Story 18: Rekursives Hochladen von Dokument-Ordern

Als Benutzer der User API möchte ich einen lokale Ordnerstruktur, die Dokumente beinhaltet, mit einem Befehl hochladen können, sodass alle in dieser Ordnerstruktur enthaltenen Dokumente im Upload-Bereich des PEAX-Portals auftauchen.

Akzeptanzkriterien:

1. Es soll der bereits bestehende Befehl `px upload` um ein `-r/-recursive`-Flag ergänzt werden, der als Parameter ein Verzeichnis erwartet.
2. Es sollen sämtliche in diesem Ordner (und dessen Unterordner beliebiger Tiefe) enthaltenen Dateien hochgeladen werden.
3. Scheitert das Hochladen einer Datei, soll dies entsprechend auf `stderr` inkl. relativem Dateipfad gemeldet werden.
4. Die generierten UUIDs der erfolgreich erstellten Dateien sollen auf `stdout` ausgegeben werden.
5. Optional: Mit dem Parameter `-l/-log`, der ein Dateiname erwartet, wird ein Protokoll im JSON-Format geschrieben, das den Erfolg/Misserfolg für jede Datei (mit absolutem Pfad) angibt. Im Erfolgsfall enthält der Eintrag die generierte UUID des Dokuments, im Fehlerfall eine entsprechende Fehlermeldung.

Bugs

1: Interaktive Eingabe auf Windows funktioniert nicht

Tests auf Windows ergaben, dass es derzeit nicht möglich ist, ein Passwort sicher (ohne Echo) über die Kommandozeile einzugeben. Recherchen haben ergeben, dass es in die-

sem Bereich derzeit einen offenen Bug gibt. Als Workaround wird bis zur Fehlerkorrektur auf die sichere Passworteingabe verzichtet. Mithilfe eines Build Tags konnte dieser Workaround auf Windows eingeschränkt werden, sodass auf macOS und Linux weiterhin die sichere Passworteingabe zum Einsatz kommt.

2: Refresh-Mechanismus funktioniert nicht für Agent API

Es ist derzeit nicht möglich, mit einem Refresh Token eines Agents einen neuen Access Token zu holen. Dieses Problem muss auf dem PEAX Identity Provider näher analysiert werden.