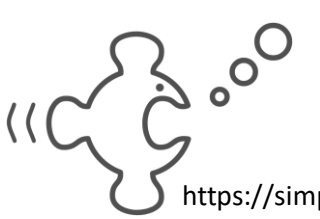
SimpleSAMLphp – eine Alternative zu Shibboleth und MFA mit eduMFA

83. DFN Betriebstagung
See-Ling Wong und Stefan Pfeiffer
GWDG

Single-Sign-On in Deutschland

- Shibboleth IdP schon lange eine etablierte, aber auch komplexe Lösung
- Herausforderung: Wartung, Java-Abhängigkeit, Konfigurationsaufwand, schwer anpassbar
- Motivation für Alternative -> SimpleSAMLphp
  - Aktives Projekt: letztes Release am 11.06.2025 mit SimpleSAMLphp 2.4.2
  - Bedarf an mehr Konfiguration und Anpassung an eigene komplexe Gegebenheiten
- Frank Tröger (RRZE Erlangen) hat bereits Jahre zuvor über SSP referiert…
  … und außerdem schon lange in der Uni als IDP im Einsatz
  https://github.com/frnktrgr/demo_simplesamlphp_sp

Abkürzungen:
SSP – SimpleSAMLphp
IDP – Identity Provider
SP – Service Provider
Shib - Shibboleth



https://simplesamlphp.org/

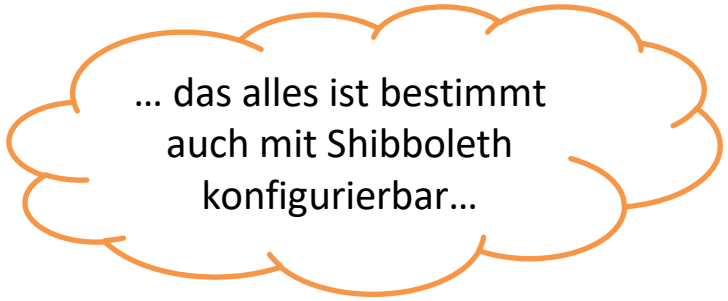
Was ist SimpleSAMLphp?

- Php-basierter SAML 2.0 IdP und SP
- Modular, leichtgewichtig, gut in Webumgebungen integrierbar
- Nutzbar als Service Provider, Identity Provider, Proxy (und alles, was man möchte)
- Vergleich zu Shibboleth
- Durch die Architektur von SSP ist ein Hosting von mehreren IDPs auf einer Instanz möglich

Aspekt	Shibboleth	SimpleSAMLphp
Sprache	Java	PHP
Deployment	Tomcat, XML (komplex)	Webserver + PHP (leichtgewichtiger)
Wartung	Einfacher	Komplexer
Flexibilität	Sehr stabil, aber schwer anpassbar	Leicht selbst erweiterbar
Anpassbarkeit	Feste Module, schwieriger selbst anzupassen	Einfach anpassbar

SimpleSAMLphp
Filter und Module

- Filter und Module sind die zentralen Konzepte um Authentifizierungs- und Attributflüsse zu steuern und zu erweitern
- Es gibt viel Kernfilter und Module
- aber auch viele von anderen (3rd Party): https://simplesamlphp.org/modules/
- SimpleSAMLphp kombiniert mit Filter und Modulen können die eigenen komplexen Szenarien umsetzbar machen
  - Rollenbasierte Zugriffe
  - Attributanreicherung aus externen Quellen
  - Integration von Multifaktorauthentifizierung
  - …



SimpleSAMLphp
Filter und Module

- Filter sind Verarbeitungsschritte, die SSP während des Authentifizierungsprozesses oder der Attributübertragung ausführt
- SSP hat 2 Haupttypen
  - Autentication Processing Filter (AuthProcFilters): beeinflussen Login und Attribute
  - Metadata Filter: verändern Metadaten vor der Übertragung
- Seit Version 1.19.0 gibt es *preconditions*
  - Filter werden nur unter bestimmten Bedingungen ausgeführt, zB nur bei einem bestimmten Dienst

Filter	Zweck
AttributeCopy	Kopiert Attribute in die Antwort
AttributeMap	Ändert den Attributnamen
AttributeValueMap	Mapped Attribute zu neuen Werten und Attributnamen
ScopeAttribute	Fügt Scope zu einem Attribut
TargetedID	Generiert eduPersonTargetedID
AuthnContextClassRef	Setzt authentication context in der Antwort
FilterScopes	Filtert Attribute anhand einer Scope-Whitelist
PersistentNameID2TargetedID	Speichert persistantnameid als eduPersonTargetedID
saml:TransientNameID	Generiert
…	Und viele mehr

https://simplesamlphp.org/docs/stable/simplesamlphp-authproc.html

SimpleSAMLphp
Filter und Module

- Module sind Erweiterungen/Plugins, die zusätzliche Funktionen zu SimpleSAMLphp hinzufügen, zB MFA-Integration, Attributmanipulation, Autorisierung etc

Modul	Zweck
core	Kernfunktionalität
admin	Administrationsoberfläche
saml	SAML-Kernfunktionalität
ldap	LDAP Anbindung
attributerelease	Attributrelease
authorizeadvanced	Autorisierung
Metarefresh	Refresh von Metadaten
tou	Terms-of-Use
mfa	MFA-Integration *(selbstgeschrieben, später mehr)*
…	Und viele mehr

https://simplesamlphp.org/docs/stable/simplesamlphp-modules.html#simplesamlphp-modules

Was machen wir damit?
Die Academic ID

- Universelles Benutzerkonto zur Nutzung der Dienste in der Academic Cloud
- Academic Cloud beinhaltet Dienste, die uA Hochschulen und Universitäten nutzen können
- Anmeldung auch mittels Föderation von universitären bzw wissenschaftlichen IDPs
- Automatische Angliederung der IDPs der DFN-AAI
- SimpleSAMLphp:
  - IDP der Uni Göttingen,
  - IDP der GWDG,
  - Academic ID Proxy
  - MPG Proxy
  - …

SP -> Proxy -> IDP

Academic Cloud

Dienst - Serviceprovider
- momentan direkte Anbindung der Academic ID an den Dienst

Academic ID bzw
Academic Cloud Login

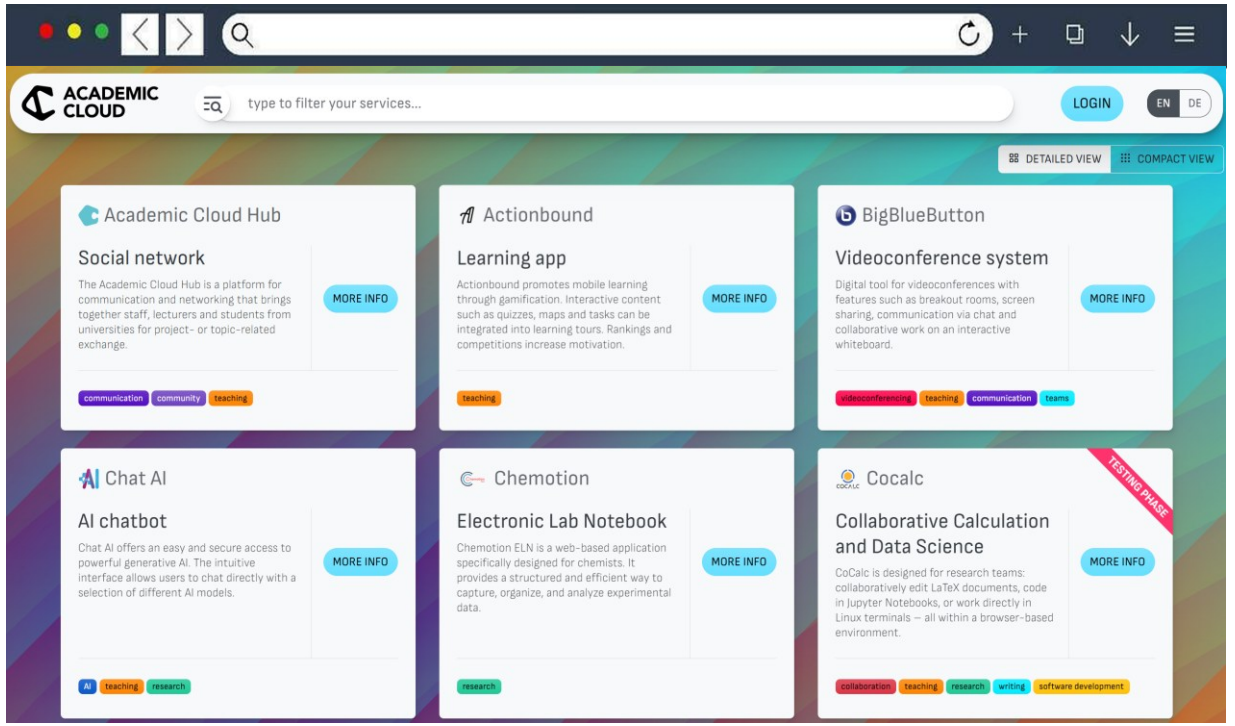
Academic ID Proxy
- eingetragen in der DFN-AAI als Service Provider
- bindet die IDPs der DFN-AAI an

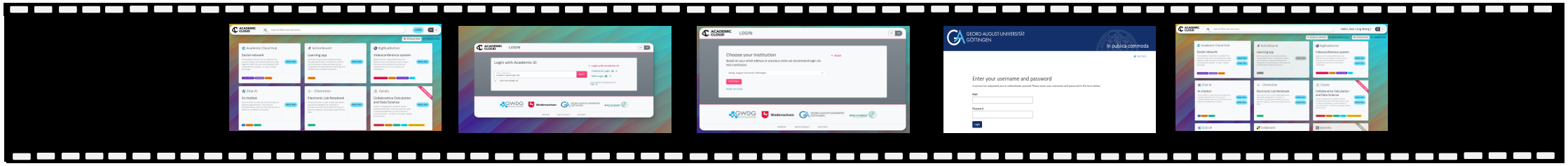
IDP der GWDG, Uni Göttingen, …

Heimat IDP
- eingetragen in der DFN-AAI als IDP

Dienst (SP)

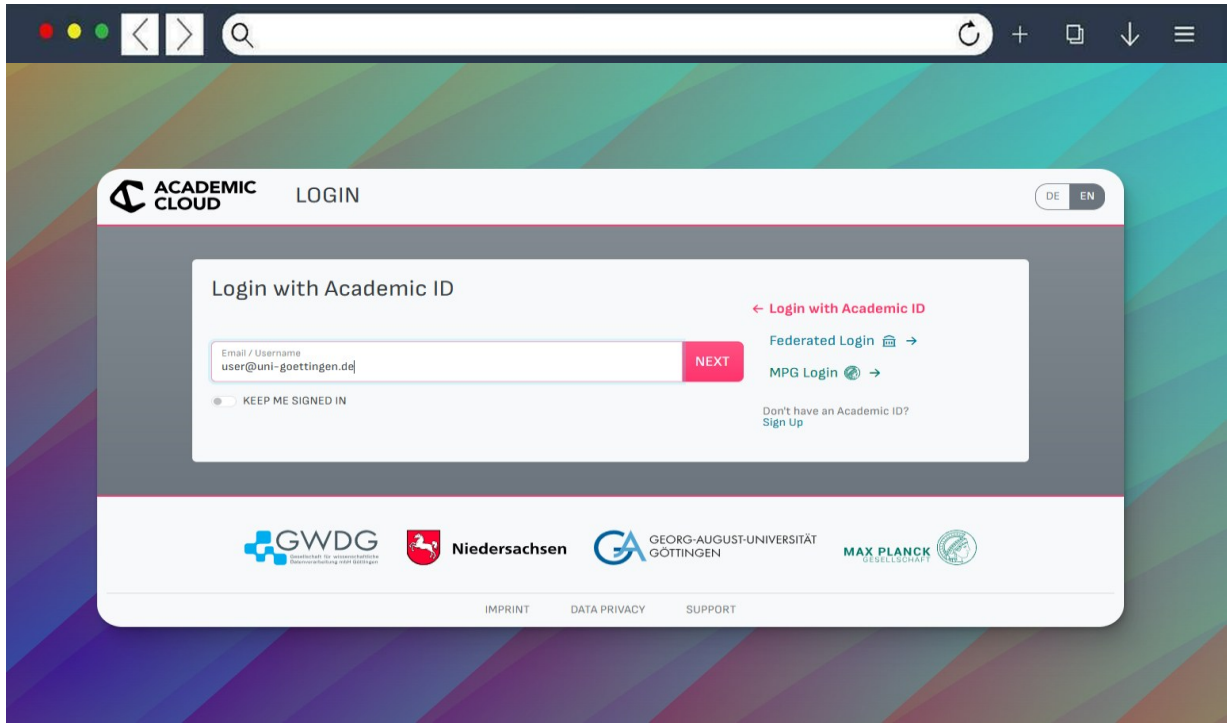

Login vom Dienst


ACADEMIC CLOUD
type to filter your services...
LOGIN
EN
DE
DETAILED VIEW
COMPACT VIEW
Academic Cloud Hub
Social network
The Academic Cloud Hub is a platform for communication and networking that brings together staff, lecturers and students from universities for project- or topic-related exchange.
MORE INFO
communication
community
teaching
Actionbound
Learning app
Actionbound promotes mobile learning through gamification. Interactive content such as quizzes, maps and tasks can be integrated into learning tours. Rankings and competitions increase motivation.
MORE INFO
teaching
BigBlueButton
Videoconference system
Digital tool for videoconferences with features such as breakout rooms, screen sharing, communication via chat and collaborative work on an interactive whiteboard.
MORE INFO
videoconferencing
teaching
communication
teams
Chat AI
AI chatbot
Chat AI offers an easy and secure access to powerful generative AI. The intuitive interface allows users to chat directly with a selection of different AI models.
MORE INFO
AI
teaching
research
Chemotion
Electronic Lab Notebook
Chemotion ELN is a web-based application specifically designed for chemists. It provides a structured and efficient way to capture, organize, and analyze experimental data.
MORE INFO
research
Cocalc
TESTING PHASE
Collaborative Calculation and Data Science
CoCalc is designed for research teams: collaboratively edit LaTeX documents, code in Jupyter Notebooks, or work directly in Linux terminals – all within a browser-based environment.
MORE INFO
collaboration
teaching
research
writing
software development



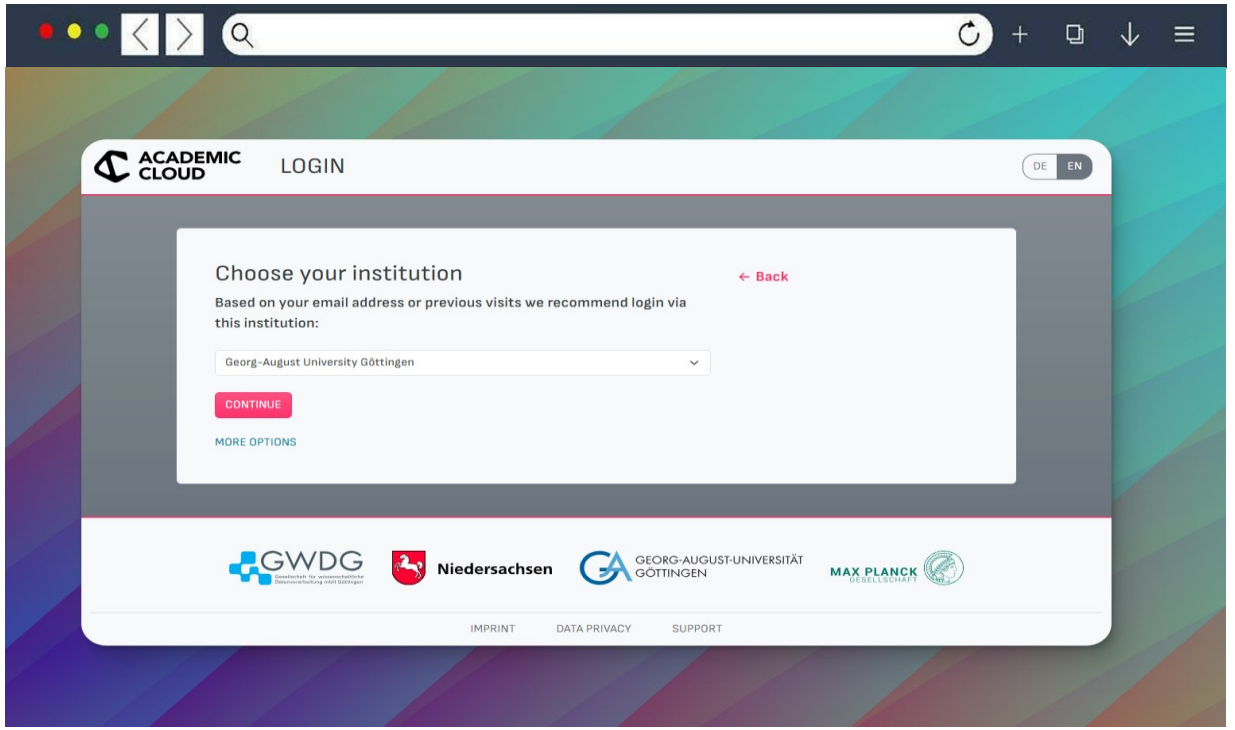
Academic ID (Proxy)

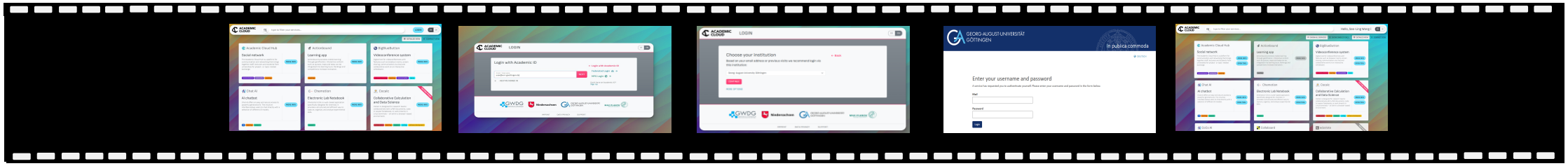
Login mit Academic ID
Verschiedene Loginmöglichkeiten:
- direkt Eingabe von E-Mail
- dann automatische Institutsaufwahl bei der föderierten Anmeldung



Academic ID (Proxy)

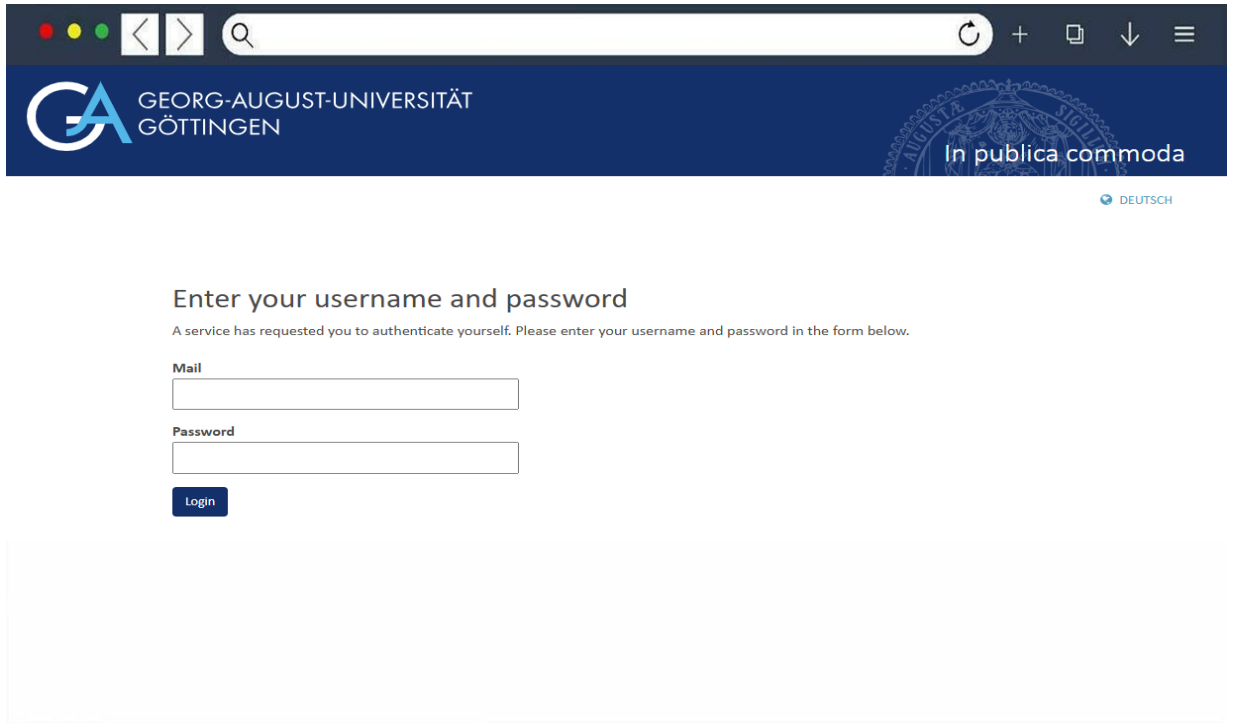
Institutsauswahl und dann
Weiterleitung auf den Heimat IDP





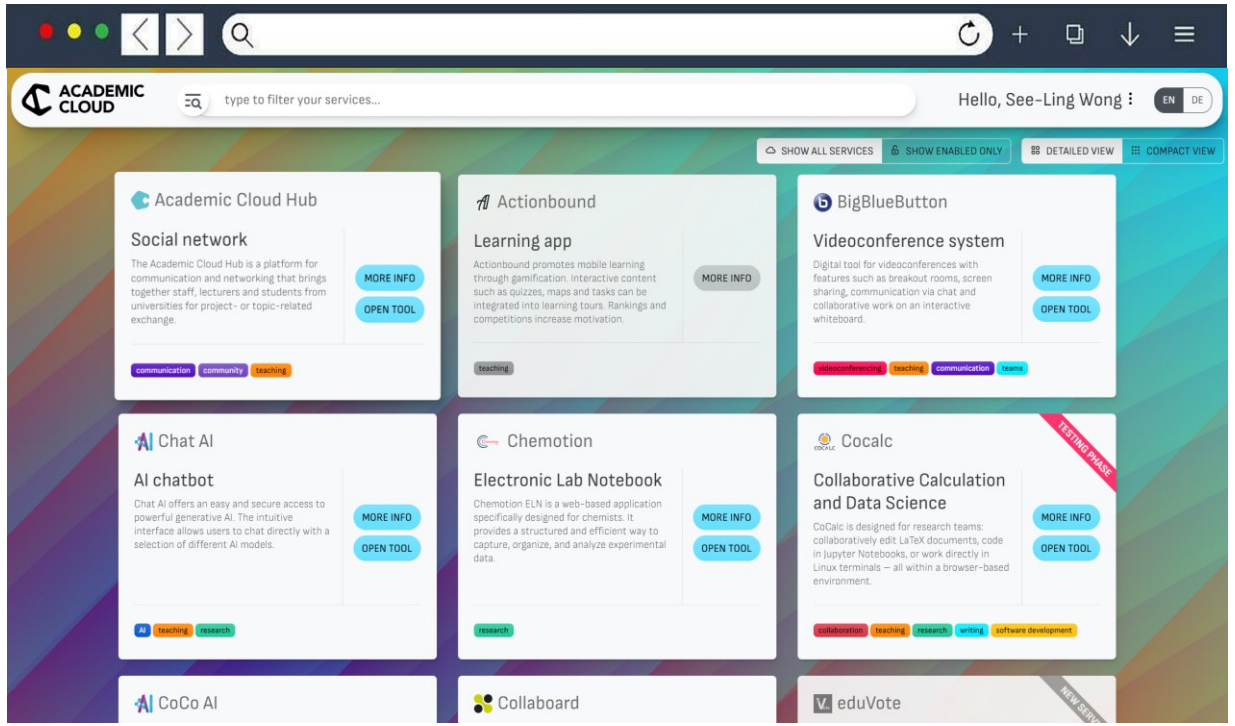
Heimat IDP (Uni Göttingen)

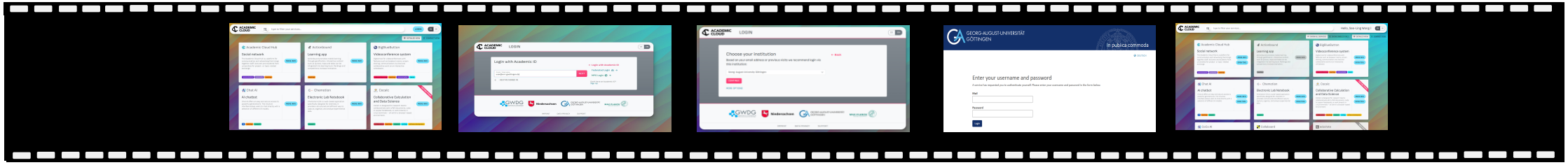
Anmeldung auf dem Heimat IDP und zurück zum Proxy mit den ensprechenden Attributen



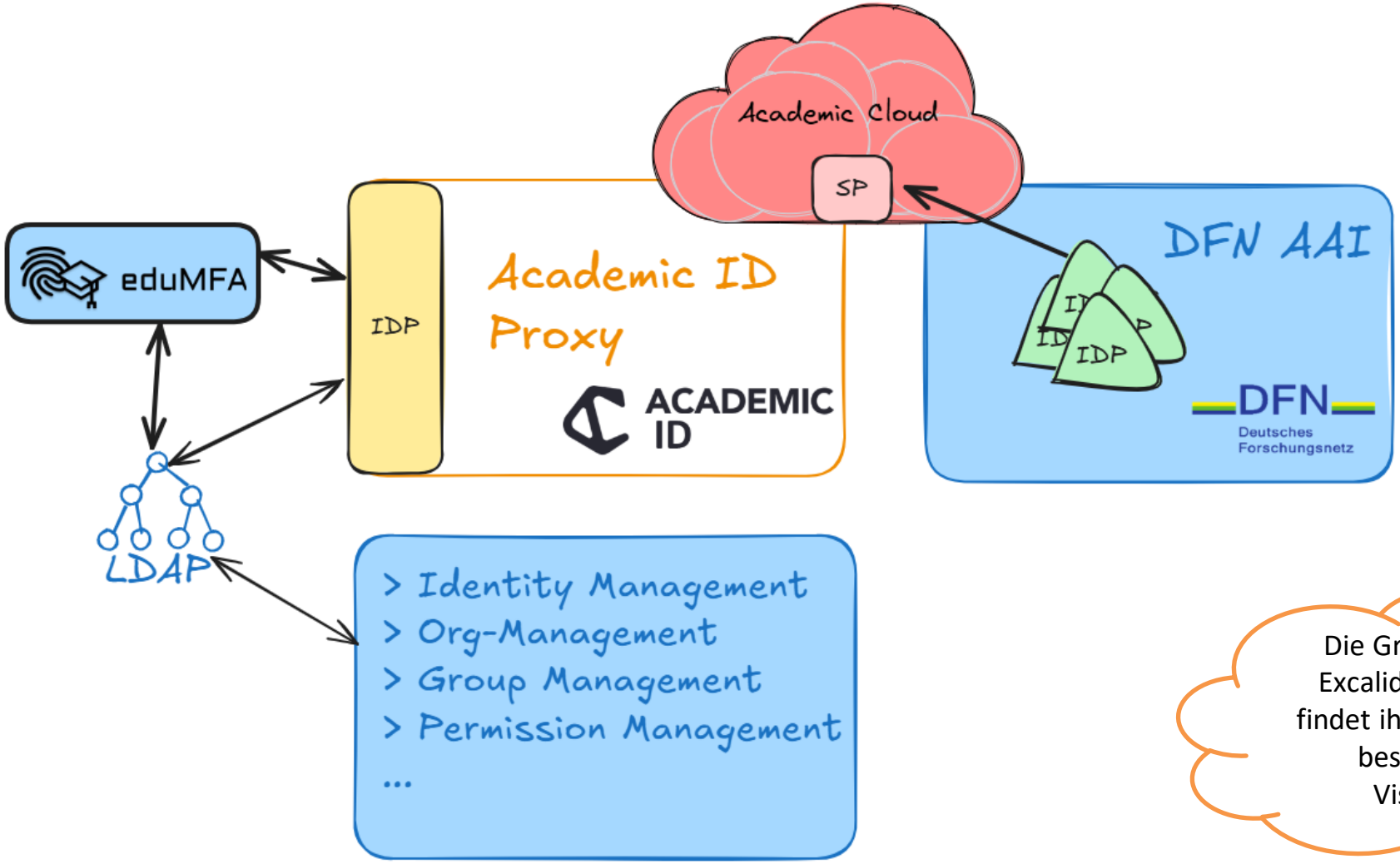
Dienst (Academic Cloud)

Proxy schickt zurück auf den angefragten Dienst





Die Academic ID



Die Grafik habe ich mit Excalidraw erstellt. Wie findet ihr den Stil? Habt ihr bessere Tools zur Visualisierung?

SimpleSAMLphp und Integration von eduMFA

Multifaktorauthentifizierung

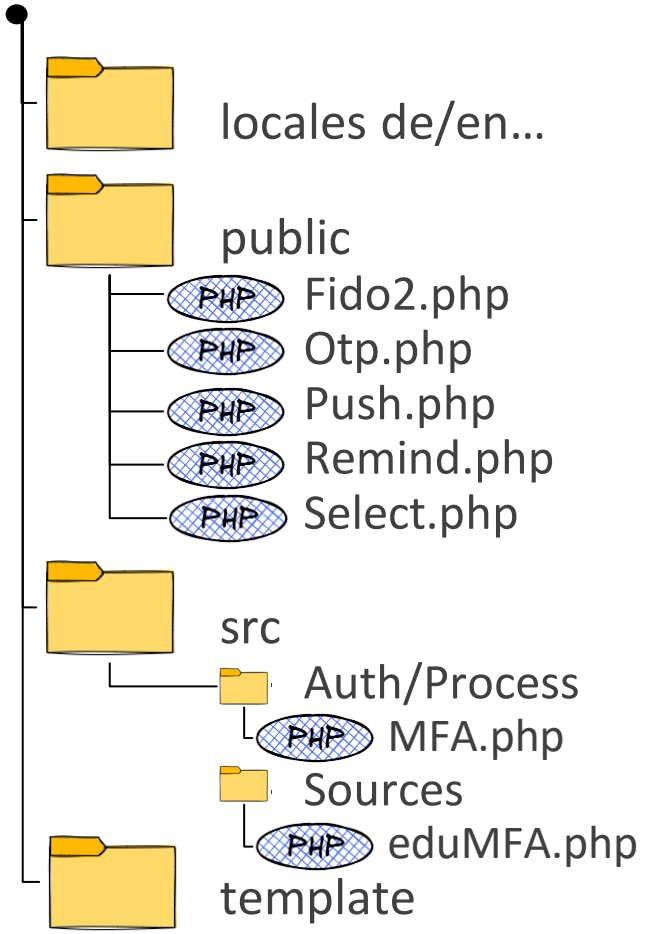
Einführung der verpflichtenden MFA

- Zentrale Verwaltung der Tokens über *eduMFA*
- Flexible MFA-Abfragen je nach Dienst
  - Hohe Schutzanforderung/ Adminrechte
    - MFA-Abfrage bei jeder Anmeldung am Dienst, erneute Abfrage wenn Dienstsession beendet
  - Mittlere Schutzanforderung:
    - MFA-Abfrage einmal pro Tag
  - Normale Dienste
    - MFA-Abfrage bei neuer Session des Academic Ids (zB alle 30 Tage)
- MFA-Pflicht für verschiedene Nutzergruppen
  - Admins, Studierende, Mitarbeitende
  - Differenzierung nach Institute über das Org-Management
  - Eigene Gruppen und Szenarien möglich

→ SP erzwingt MFA

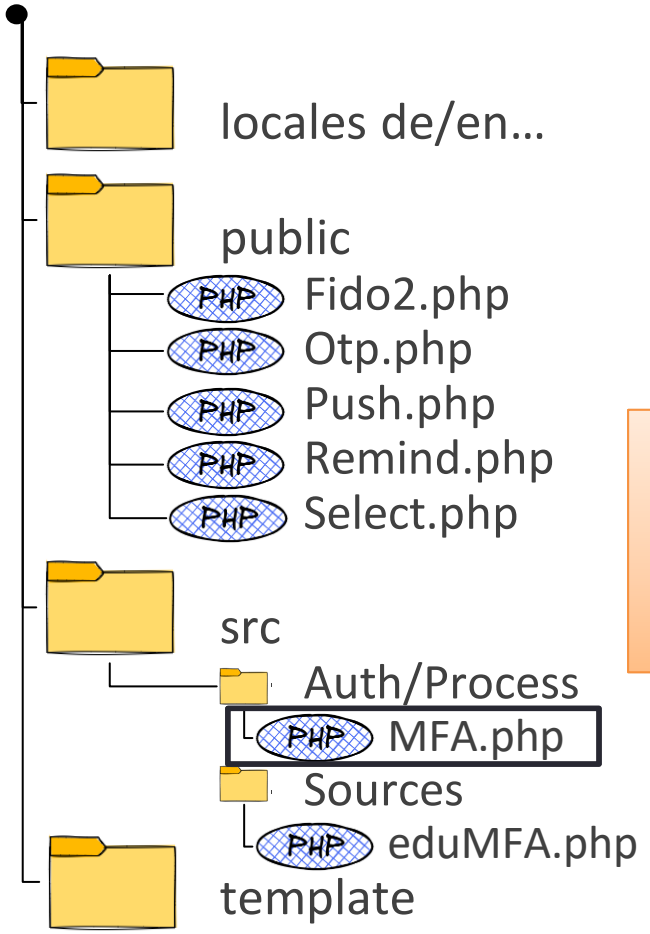
→ MFA über Attribut am Nutzer

Wie macht man das nun?
ssp-module-mfa



- Ein Modul besteht aus:
  - Locales
    - Sprachdateien/Übersetzungen
  - Lib (hier public und src)
    - PHP-Klassen und Hauptlogik des Moduls
  - Template
    - HTML-Templates (twig) für UI Ausgabe

Wie macht man das nun?
ssp-module-mfa

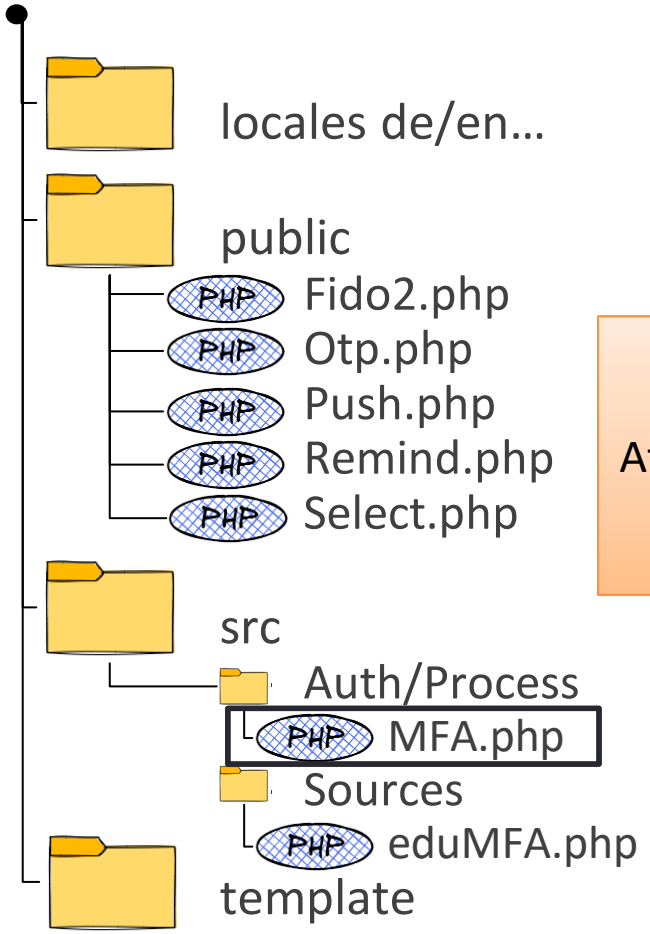


Whitelist mit SPs ohne MFA

Liste mit Diensten, die unbedingt MFA benötigen

```php
<?php
…
class MFA extends ProcessingFilter {
…
    private function gather(array &$state) {
        $factors = [];
           …
        return $factors;
    }
    public function process(array &$state): void {
        $client = ClientId::getClient($state);
        $availableFactors = $this->gather($state, $this->config);
        // allow login without mfa for inital factor registration clients
        if(in_array($client, $this->config['mfa_registration_bypass_whitelist'])) {
            foreach($availableFactors as $source => $factors) {
           …
        }
        Util::saveStateAndRedirect($state, 'select.php');
    }
    private function isMfaRequired(array $state, string $client): bool {
        if (Util::mfaAcrRequestBySp($state)) {
            return true;
        }
    }

…
```

Wie macht man das nun? ssp-module-mfa

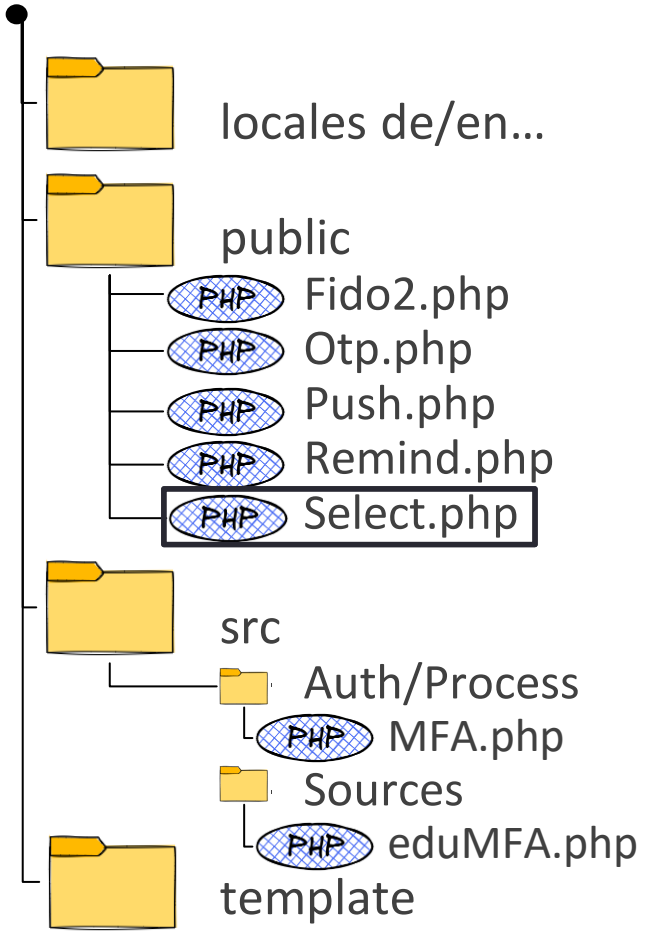


Dienst steht auf der MFA-Pflicht Liste

Wenn Account „MFAPflicht“ Attribut hat, dann immer MFA nachfragen

```
…

    private function getServiceProviderMfaExpiration(array $state, string $client):
?int {

        $loa_conf = $this->config['level_of_assurance'];
        $loa_expire = null;
        foreach($loa_conf as $loa) {
            if(in_array($client, $loa['services'])) {
                $loa_expire = $loa['expire'];
                break;
            }
        }



        if(is_null($loa_expire) && in_array('enforceMFA',
$state['Attributes']['userServices'])) {
            return $this->config['enforce_mfa_default_expire'];
        }
        return $loa_expire;
    }
    }

}
```

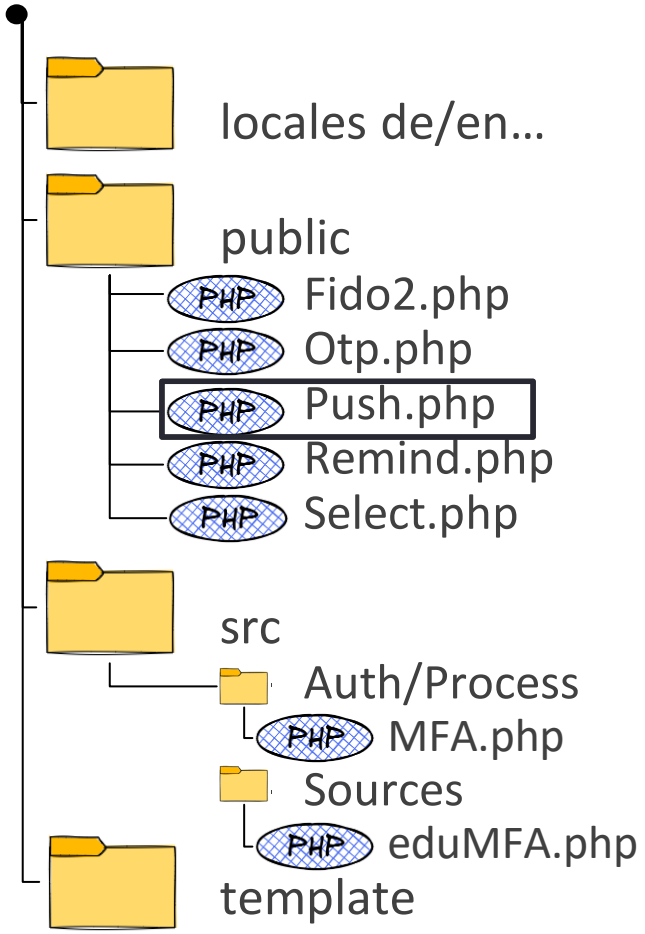
Wie macht man das nun?
ssp-module-mfa



Fragt ab welche Tokens der Account registriert hat

```php
<?php


$state = Util::getState();

if ($_SERVER['REQUEST_METHOD'] === 'POST') {
    list($sourceId, $factorId) = explode('|‘,
…

  if (array_key_exists($sourceId, $state[MFA::STATE_SELECT_FACTORS])) {
    foreach ($state[MFA::STATE_SELECT_FACTORS][$sourceId] as $factor) {
      if ($factor['serial'] == $factorId) {
        $source = Util::getConfig()['sources'][$sourceId];
        Util::getSource($source['source'])::trigger($state, $source['config'],
$factorId);
      }
    }
  }
  throw new BadRequest('Invalid MFA selection.');
}

Util::sendTemplate('select.twig',
  array_merge(
    $state[Util::STATE_TEMPLATE_DATA],
    [
      'selection_url_param' => MFA::URL_PARAM_FACTOR_SELECTION,
      'factors' => $state[MFA::STATE_SELECT_FACTORS],
      'username' => $state[MFA::USERNAME]
    ]
  )
);
```

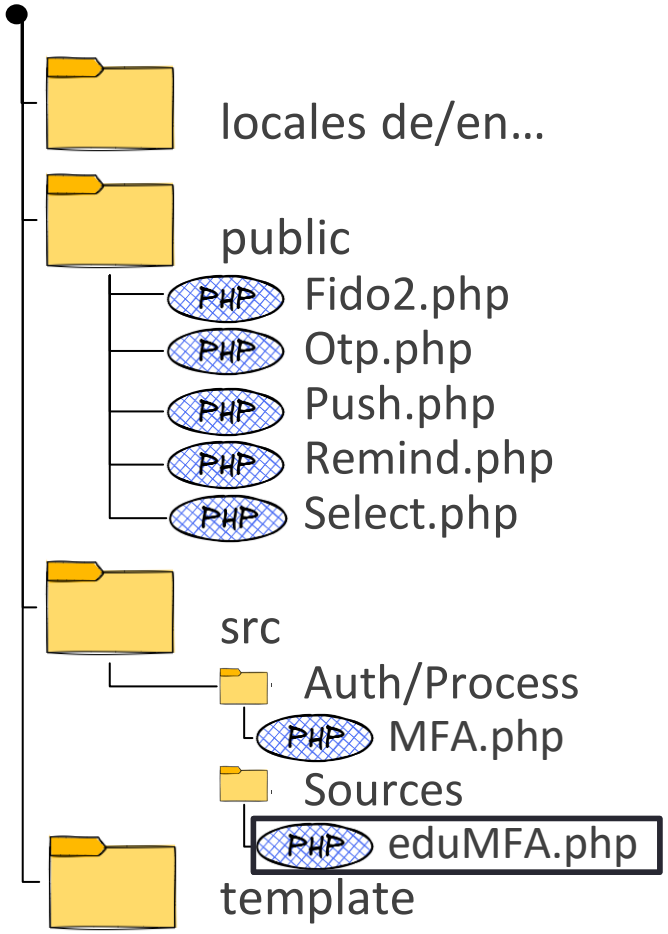
Wie macht man das nun?
ssp-module-mfa



Ruft die push-Methode auf über …

```php
<?php

use SimpleSAML\Module\mfa\sources\eduMFA;
use SimpleSAML\Module\mfa\Util;

# polling was successful and triggered a POST -> continue
if ($_SERVER['REQUEST_METHOD'] === 'POST') {
  PrivacyIdea::consume(['type' => 'push', 'poll' => false]);
}

# polling endpoint. inform frontend
if (array_key_exists('check', $_REQUEST)) {
  $finished = PrivacyIdea::consume(['type' => 'push', 'poll' => true]);
  echo $finished ? 'y' : 'n';

} else {
  Util::sendTemplate('push.twig', ['mfaState' =>
Util::getRequiredUrlParam(Util::URL_PARAM_STATE_ID)]);
}
```

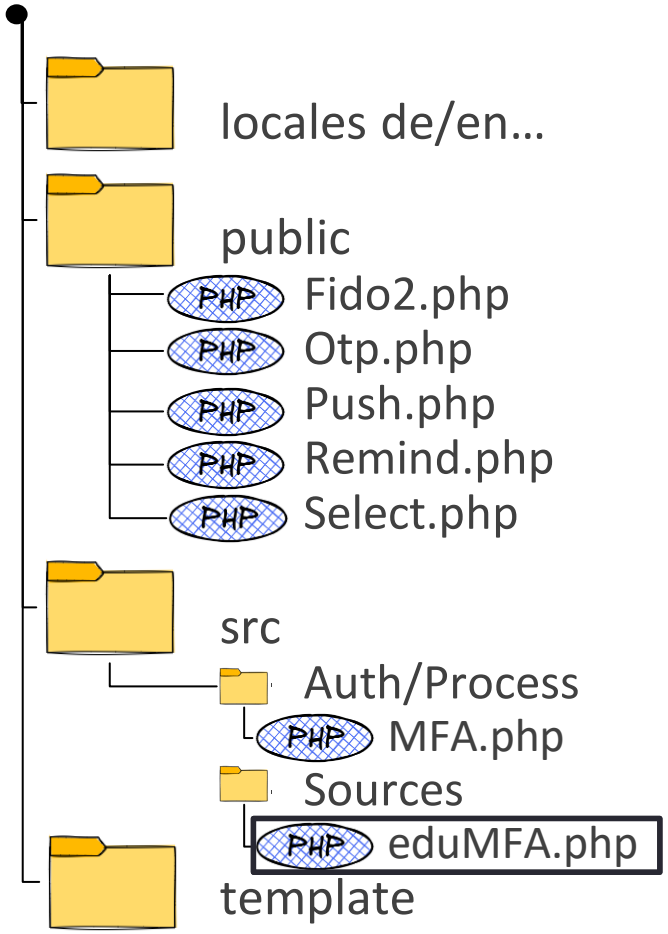
Wie macht man das nun?
ssp-module-edumfa



ruft die entsprechenden eduMFA API Schnittstellen auf

```php
<?php
…

class EduMFA implements SourceInterface {
    public static function gather(array &$state, array $config) : array {

  …

        }
        $tokens = self::getTokens($config,
['Attributes'][$config['Attribute']][0]);
        Logger::debug(self::LOGGER_PREFIX . 'server response: ' .
json_encode($tokens));


    public static function trigger(array &$state, array $config, string
al) {
        $challenge = self::triggerChallenge($config, $tokenSerial);
        if ($challenge === false) {
            return;
        }
        Util::saveStateAndRedirect($state, str_ends_with($challenge['type'],
'push') ? 'push.php' : 'otp.php');
    }
```

Wie macht man das nun?
ssp-module-edumfa

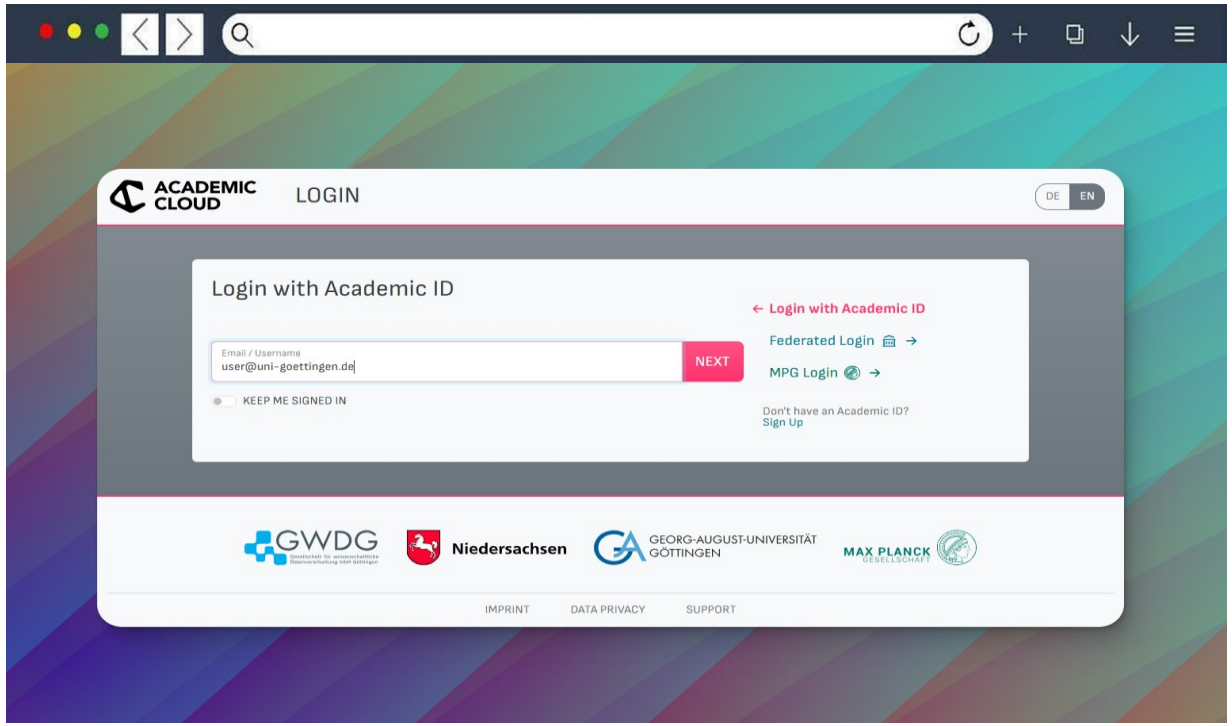


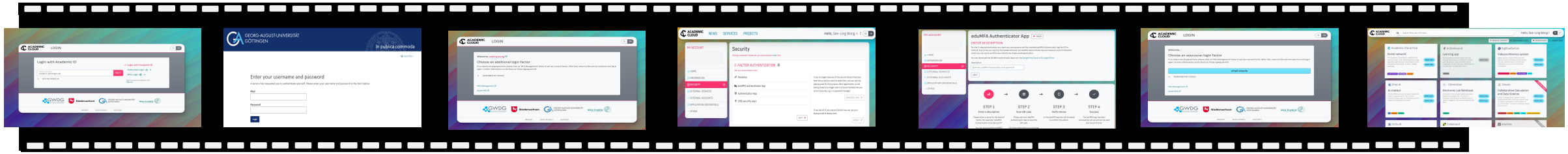
API Aufruf mit den entsprechenden Attributen

```
…
    public static function consume(array $data) {
        if($data['type'] == 'otp') {
            $state = Util::getState();
…

            $query = [
                'user' => $state[self::STATE_USERNAME],
                'pass' => $data[self::OTP_VALUE],
                'serial' => $state[self::TOKEN_SERIAL],
                'transaction_id' => $state[self::TRANSACTION_ID],
                'realm' => $state[self::REALM]
            ];

            if(self::validateToken($state[self::SERVER_CONFIG], $query)) {
                Util::continueAuthProcChain($state);
            }

…
        } elseif(str_ends_with($data['type'], 'push')) {

            $state = Util::getState();

            $finished =
self::isTransactionFinished($state[self::SERVER_CONFIG],
$state[self::TRANSACTION_ID]);
            if($finished && !$data['poll']) {
                Util::continueAuthProcChain($state);
            }
            return $finished;
        }
    }
…
```

Academic ID (Proxy)

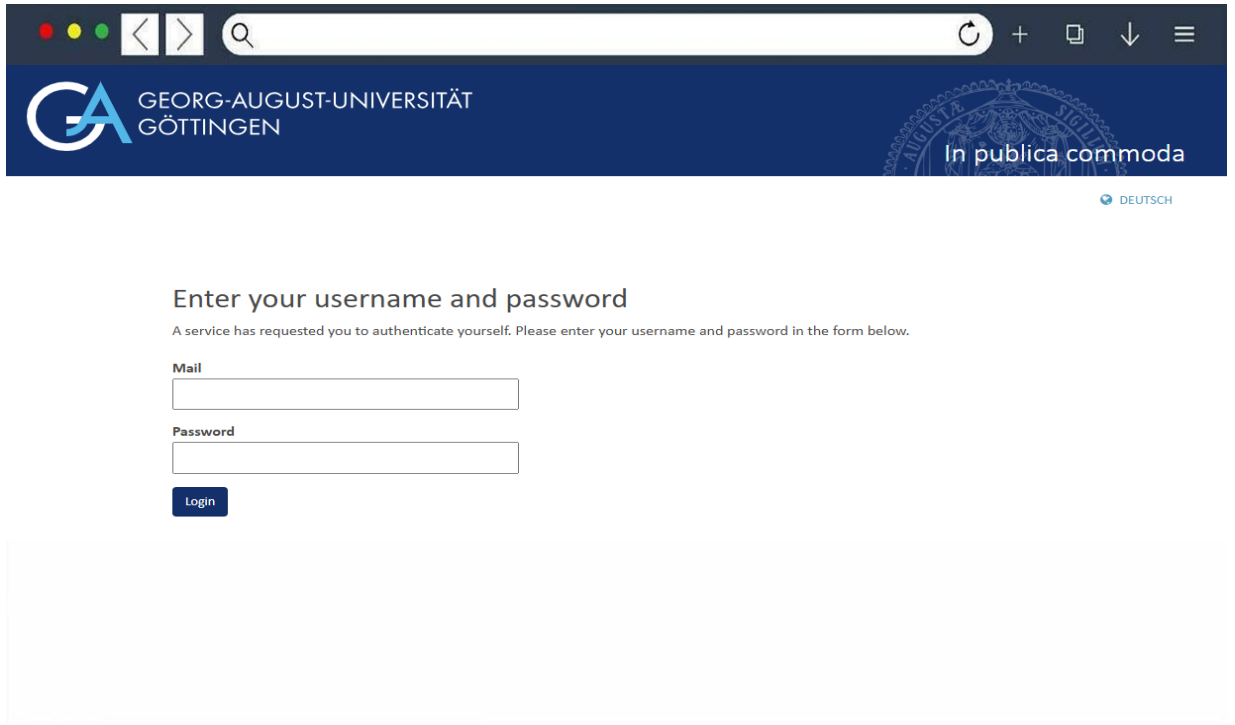
- Mal wieder die Anmeldung

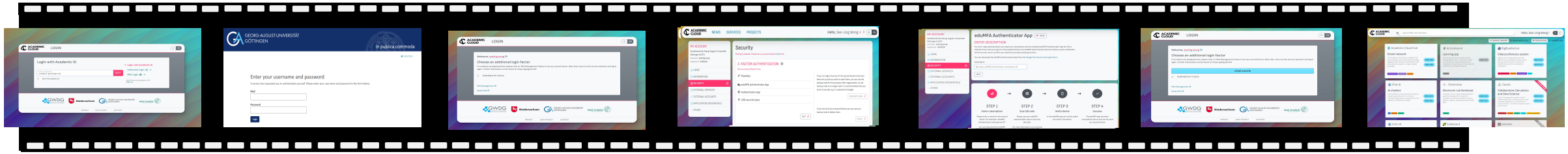




Heimat IDP (Uni Göttingen)

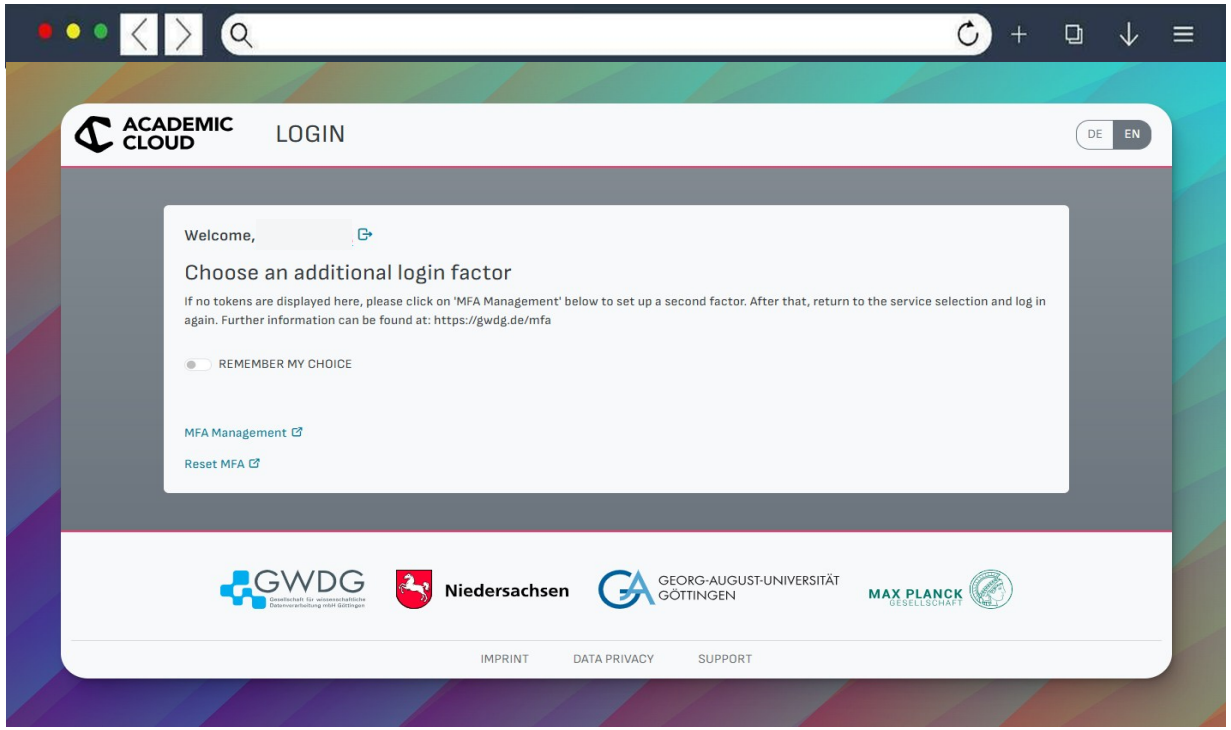
- Über die den Heimat IDP

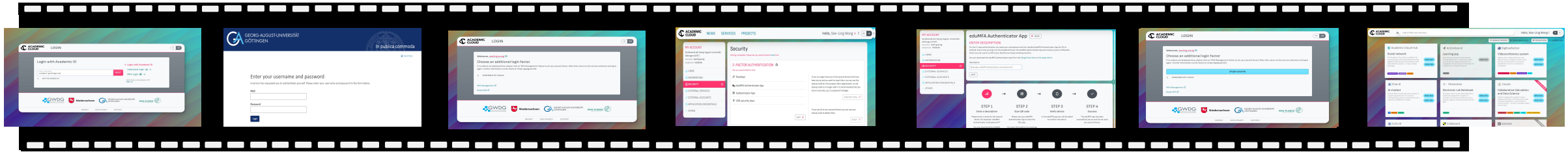




Loginflow mit MFA: noch kein Token

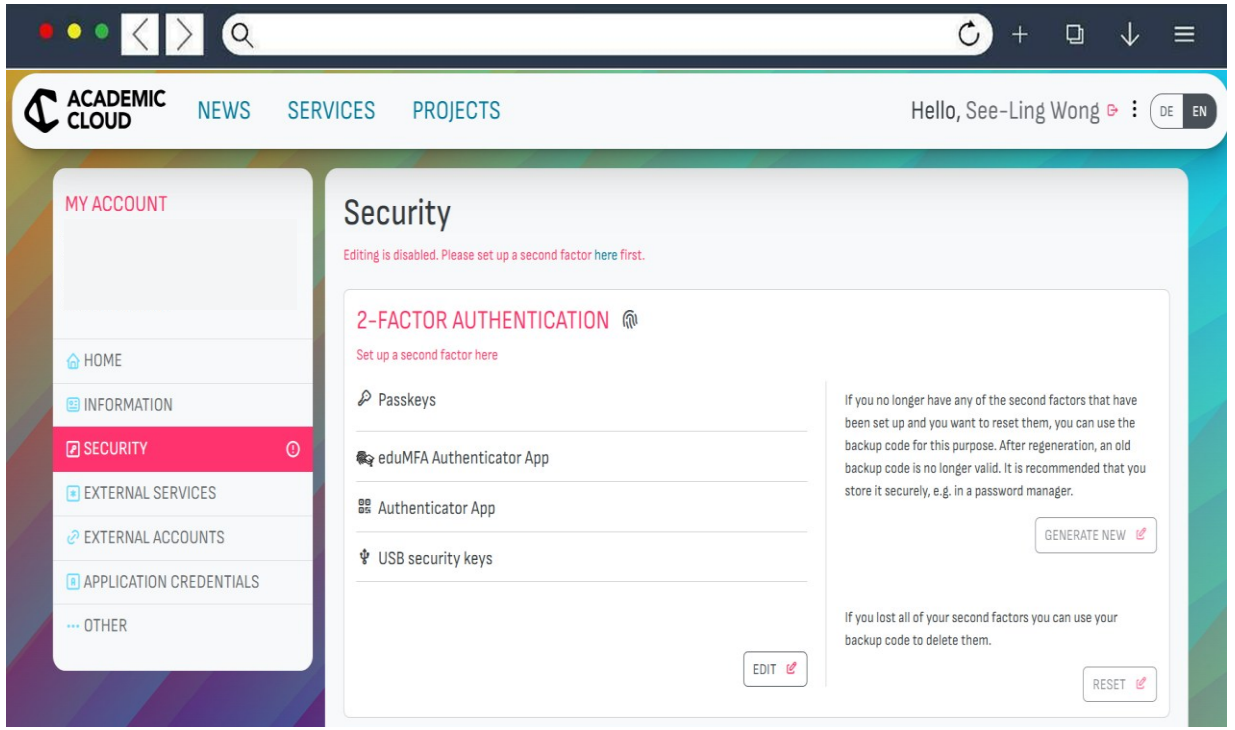
- Man landet auf *select.php*
- hat hier die Möglichkeit über „MFA Management“ auf das Accountportal zu kommen um ein Token zu registrieren.

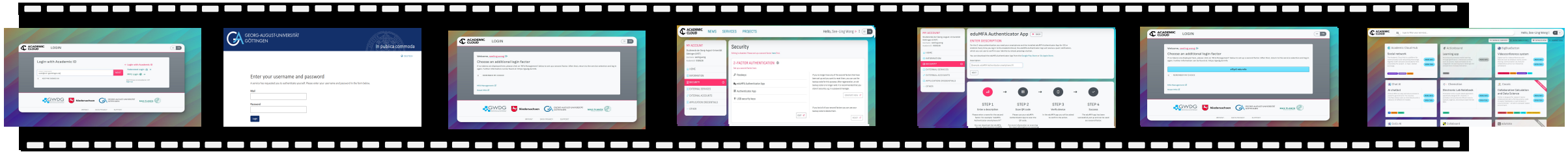




Loginflow mit MFA: noch kein Token

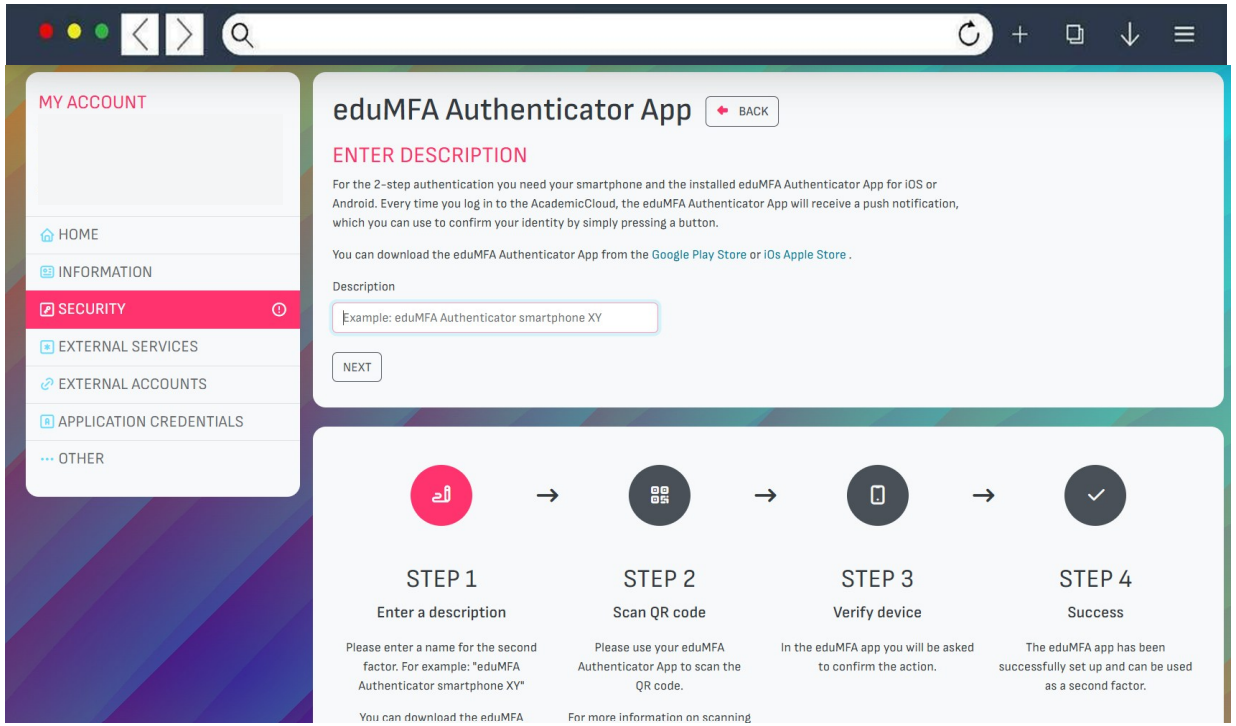
- Im Accountportal kann man nun den zweiten Faktor anlegen
- Wir haben
  - FIDO2
  - eduMFA Push
  - TOTP
  - Yubikey OTP

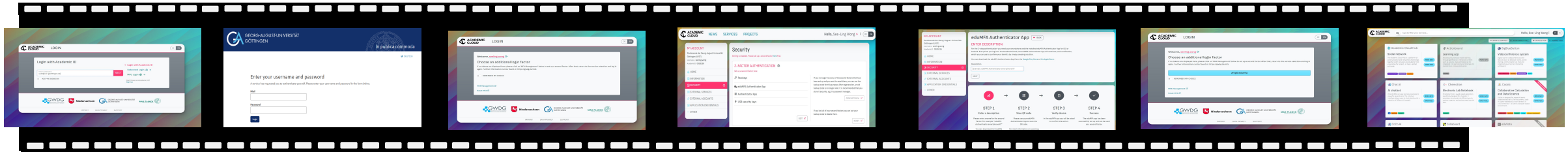




Loginflow mit MFA: noch kein Token

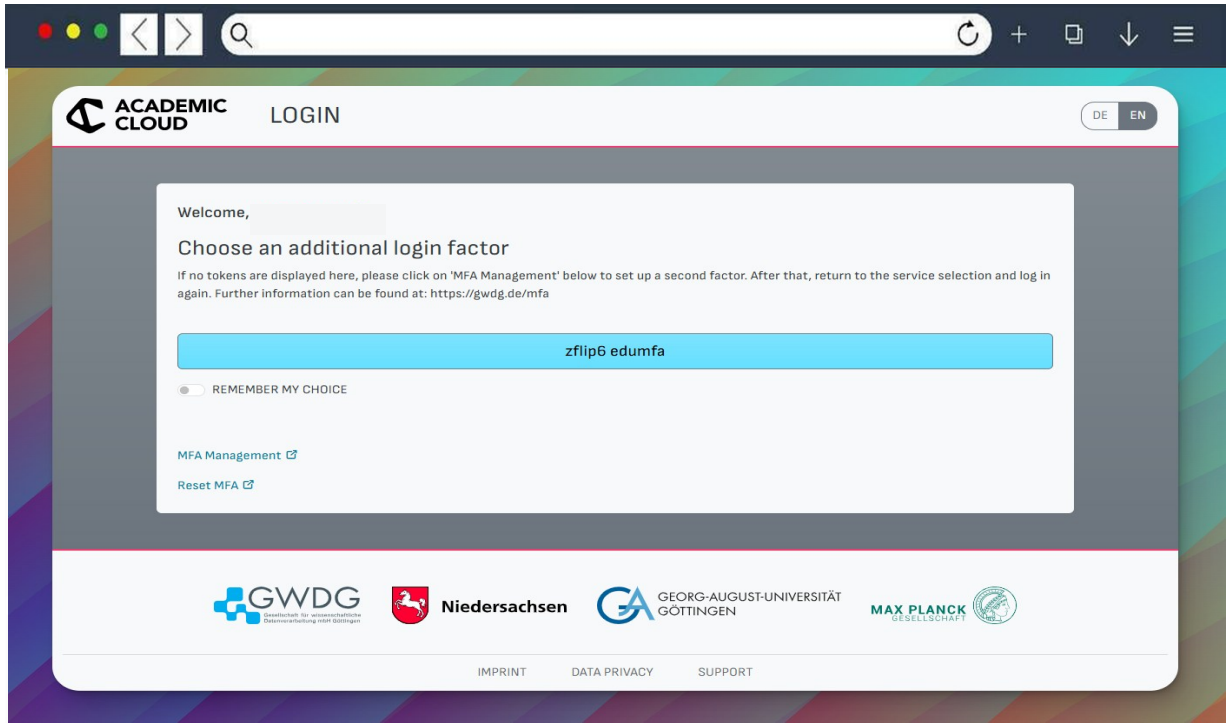
- Hier registrieren wir mal ein eduMFA PUSH Token

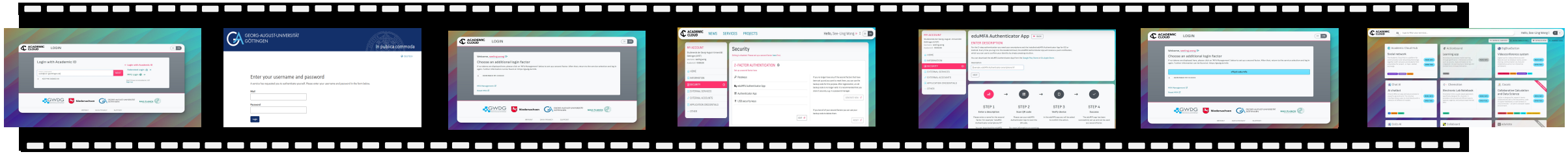




Loginflow mit MFA: noch kein Token

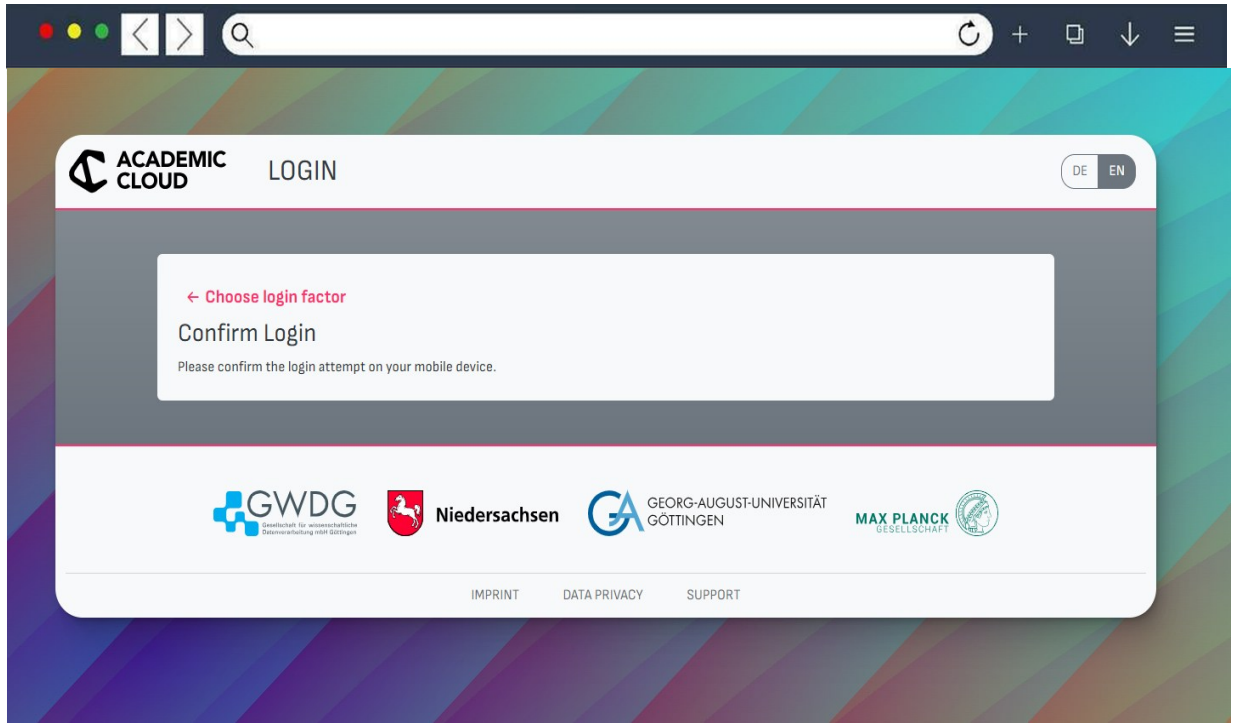
- Wieder im Loginprozess angelangt, taucht auf der MFA-Seite der registrierte Token auf

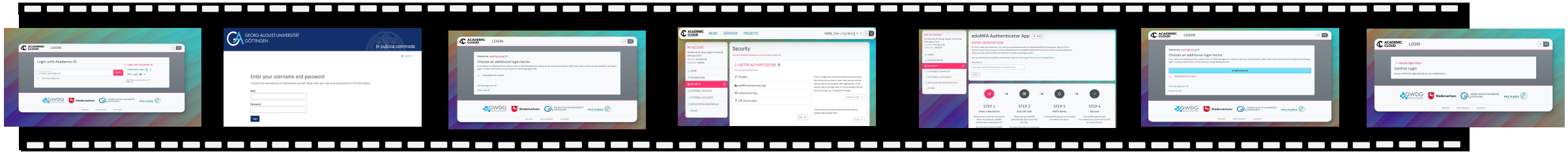




Loginflow mit MFA: noch kein Token

- Warte auf die Bestätigung des Push-Tokens
- Nachdem Bestätigen wird man dann zum Dienst zurückgeleitet.





Fazit

- Wann ist SimpleSAMLphp sinnvoll?
  - Schnelle Anpassung
  - Umsetzung komplexer Anforderungen
- Wann bleibt Shibboleth die bessere Wahl?
  - Wenn das oben nicht zutrifft :D

Zukunft

- Stepup Authentication
- Deployment über Kubernetes
- Zusammenspiel mit EntraID und ADFS
- Und …

Gemeinsam…

- Wer hat Interesse mehr über SimpleSAMLphp zu erfahren?
- Gemeinsam ein Repo aufbauen und pflegen -> Community?
- Austausch und gegenseitige Hilfe
  - Kubernetes Helm-Charts
  - MFA Enrollment
  - …

Vielen Dank an …

- Unser SSO Team: Stefan Pfeiffer, Christian Lorenzen, Shirin Dabbaghi, Ralph Krimmel, Sascha Krull
- eduMFA Projektteam
- SSP-DE – Community
  - RRZE Erlangen, und hoffentlich mehr
- Euch, eure Aufmerksamkeit und evtl künftige gemeinsame Projekte, Austausch und Zusammenarbeit

Austausch über Matrix

- https://matrix.to/#/!lbDwPGSsyqIUUgaeyM:gwdg.de
- Kontakt über: sso-support@gwdg.de
  - oder über swong@gwdg.de