Karlsruher Institut für Technologie

# 2FA mit Shibboleth mit LinOTP

**Michael Simon (SCC)**

STEINBUCH CENTRE FOR COMPUTING - SCC

# Vorstellung KIT

- Karlsruher Institut für Technologie
- Grüdung 1. Oktober 2009
- Zusammenschluss aus Forschungszentrum Karlsruhe und Universität Karlsruhe
- Etwa 9000 Beschäftige und 25000 Studierende

# Motivation 2FA

- Ausführliche Behandlung der Thematik: siehe 64. Betriebstagung DFN – Vortrag von Henning Brune „Aufbau einer 2-FaktorAuthentifizierung“ Link zum Vortrag

- Grundsätzlich Stand der Technik
  - Wird mehr und mehr eingesetzt (Apple, Google, Twitter, Facebook, …)
  - Gestiegene Akzeptanz bei Benutzern durch Gewohnheit
  - Häufig bei Accountdienstleistern, wenn die Accounts durch Technologien wie Oauth oder OpenID bei vielen Diensten verwendet werden können
  - Selbe Situation im Hochschulumfeld mit Shibboleth

- Betrachtung am KIT
  - Schutzbedarf von Diensten mit sensiblen Daten (Personendaten, Finanzdaten, …)

# Ansiedelung 2FA

- Wo soll der zweite Faktor angesiedelt werden
- Beim den Diensten
  - Jeder Dienst muss separat angepasst werden
- Zentral
  - Nicht jeder zentrale Dienst bietet die Möglichkeit einen zweiten Faktor abzufragen
  - Bei Shibboleth durch Erweiterung bei WebSSO möglich

# Produkt oder Eigenentwicklung

- Kurze Recherche ergab wenige kostenfreie Produkte, die schon länger am Markt sind
  - LinOTP
  - PrivacyIDEA (Fork von LinOTP)

- Weitere Kriterien
  - Gute Integration in bestehende Umgebung
  - Möglichst wenig Administrationsaufwand

- Teststellung mit LinOTP
- Vorläufig alle benötigten Features mit LinOTP gedeckt, daher keine Eigenentwicklung

# LinOTP

- Veröffentlicht unter AGPL v3
- Seit 2014 Opensource und freie Nutzung möglich
  - „With this recent open source offering, customers now have the option to pick the solution that best suits their usage scenario. This encompasses both deployments that are fully-featured yet completely free-of-charge, as well as business-critical deployments with all their requirements on support and quality-assurance processes, including a firm commitment by LSE to the continuous development of its solution.” - https://linotp.org/linotp-open-source.html
- Lizenzierung und Support durch LSExperts möglich

- Python
- Praktisch komplett über REST API steuerbar

- Quellcode: https://github.com/LinOTP/LinOTP
- Webseite: https://linotp.org/

# Anbindung LinOTP an Shibboleth

- Benötigt wird eine Shibboleth Erweiterung zur Abfrage eines weiteren Faktors
- Mit Version 3.2 des Shibboleth IDP gibt es viel mehr Möglichkeiten zur Realisierung
- Mit Version 3.3 weitere Änderungen in Richtung Multifaktor
  - Sollten weitgehend kompatibel sein
  - Im Grunde wird die Konfiguration „präziser“
- Realisiert als zusätzliche AuthnContextClass
- Quellcode: https://github.com/cyber-simon/idp-auth-linotp

# Eine zusätzliche AuthnContextClass

- Der ServiceProvider kann in der AuthnRequest einen AuthnConextClass Wunsch mitschicken
  - Der SP kann also die Anforderung „Zweiter Faktor“ an den IDP stellen

- Durch Konfiguration in der idp.properties kann pro Benutzer festgelegt werden, ob ein zweiter Faktor verlangt wird
  - `idp.authn.resolveAttribute = eduPersonAssurance`

- Registrierung der zusätzlichen AuthnContextClass mit Authentication Flow in authn/general-authn.xml:

```
<bean id="authn/linotp" parent="shibboleth.AuthenticationFlow"
            p:nonBrowserSupported="false" p:forcedAuthenticationSupported="true"
            p:lifetime="PT15M" p:inactivityTimeout="PT15M">
  <property name="supportedPrincipals">
    <list>
      <bean parent="shibboleth.SAML2AuthnContextClassRef"
            c:classRef="https://idp.scc.kit.edu/authn/linotp" />
    </list>
  </property>
</bean>
```

# Installation IDP

- JAR Datei integrieren (shib-2fa.jar)
  - Je nach Installationsart leicht verschieden
- XML Flow Dateien kopieren
  - src/main/resources/conf/authn/linotp-authn-* to {idp.home}/conf/authn/
  - src/main/resources/flows/authn/linotp to {idp.home}/flows/authn/
- View anpassen und kopieren
  - src/main/resources/views/linotp.vm to {idp.home}/views/

- LinOTP Server in der idp.properties konfigurieren
  - Zusätzlichen Flow konfigurieren

```
idp.authn.flows = Password|linotp
idp.authn.flows.initial = Password
```

- General-authn.xml erweitern (siehe vorhergehende Folie)

# Demo Step Up Authentication

# Verfeinerung Assurance

- Verwendung von Script im attribute-resolver.xml
- Definition in global.xml und Verwendung beim attribute-resolver: customObjectRef="kit.CombiRequest„

```
<util:list id="kit.CombiRequest">
   <ref bean="shibboleth.HttpServletRequest" />
   <ref bean="shibboleth.HttpServletResponse" />
   <ref bean="shibboleth.DataSealer" />
</util:list>
```

- Mittels ServletRequest und –Response können Cookies gelesen und gesetzt werden
- Der DataSealer verschlüsselt Cookie Inhalte

- Möglichkeit: Anzahl der Logins per Browser, User und IP zählen und davon abhängig machen, ob ein zweiter Faktor eingegeben werden muss oder nicht

# Verwaltung der Tokens

- Selfservice Portal für die Benutzer
  - Benutzer kann Tokens erstellen, deaktivieren und teilweise löschen
  - Benutzer kann wählen, wie oft der zweite Faktor abgefragt wird, selbst wenn der SP es nicht fordert
  - Benutzer soll eine Liste von SPs einrichten können, bei denen immer der zweite Faktor abgefragt wird

- Verwaltungsansicht für Servicedesk
  - Anzeigen von Tokens
  - Verknüpfung von Hardwaretokens mit Account
  - Workflow für Verlustmeldung
  - Workflow für Ausgabe eines temporären Tokens (unter ähnlichen Voraussetzungen wie ein Passwortreset)

# Demo Tokenverwaltung

# Umfang der Nutzung 2FA am KIT

- Wie weit ein zweiter Faktor am KIT ausgerollt wird, ist im Moment in Diskussion

- Grundsätzlich wird es die Möglichkeit geben, einen zweiten Faktor an einem Selfservice Portal freiwillig zu registrieren
  - Richtet sich z.B. an sicherheitsbewußte Studierende
  - Häufigkeit der Nutzung kann vom Nutzer selbst festgelegt werden

# Vielen Dank für Ihre Aufmerksamkeit

Michael Simon – simon@kit.edu