online Übungssystem & online Prüfungssystem

Single Sign-On

Hinweise zur Umsetzung von Single Sign-On (SSO) im Online-Übungssystem

Autor:
Immo Schulz-Gerlach, ZDI

Version:
1.1 – 05.07.2022

FernUniversität in Hagen

Inhaltsverzeichnis

Single Sign-On (SSO)

Seit dem 01.07.2022 ist das Online-Übungssystem (vorerst im Beta-Stadium) an den Single-Sign-On-Dienst <https://login.fernuni-hagen.de> der FernUniversität angebunden. Dieser ermöglicht es insbesondere, dass Benutzer/-innen, die sich bereits in ebenfalls dort angebundene Portale oder Systeme wie StudyPort, LVU oder Moodle eingeloggt haben, einfach per Link zum Online-Übungssystem weitergeleitet werden können und sich dort nicht erneut per Eingabe ihrer Logindaten anmelden müssen.

Aus technischen Gründen (bezüglich der Arbeitsweise der bisherigen lokalen Logins im Online-Übungssystem) *wird empfohlen, dort im Zweifel spezielle SSO-Links zum Online-Übungssystem einzusetzen*, die den Single-Sign-On-Prozess so einfach und unauffällig wie möglich machen. Wie diese aufgebaut sind und wozu genau sie dienen, wird im Folgenden beschrieben.

Adressaten

Diese Dokumentation richtet sich vornehmlich an Mitarbeiter/-innen der FernUniversität, die

- Portale wie LVU oder StudyPort entwickeln und dort Links zum Online-Übungssystem aus anderen Daten automatisch generieren möchten oder
- Moodle-Kursumgebungen verwalten und darin manuell Links zu Übungssystem-Umgebungen einfügen möchten.

Der Vollständigkeit halber soll im Folgenden vorab aber auch keine kurze Beschreibung der Endnutzersicht von SSO-Anmeldungen im Online-Übungssystem folgen.

Einloggen im Online-Übungssystem (Endnutzersicht)

Wenn ein/-e Nutzer/-in direkt (nicht über einen Link von einem Portal) das Online-Übungssystem aufsucht, wird er/sie typischerweise die Übungssystem-Startseite <https://online-uebungssystem.fernuni-hagen.de> oder die Startseite einer bestimmten Kursumgebung aufrufen. Diese Startseiten sind öffentlich und ohne Login direkt abrufbar.

Ruft jemand eine solche loginfreie Startseite auf, findet sich ab sofort oben rechts auf der Seite ein Menüpunkt »Login«, der zu einer Loginseite führt, die genauer über die beiden Alternativen (Single Sign-On versus lokaler Login) aufklärt und einen Button zur SSO-Anmeldung enthält.

Drückt der/die Benutzer/-in nun diesen SSO-Button, so wird er/sie zum Loginserver weitergeleitet, wo er/sie Loginnamen und Kennwort eingeben muss (sofern er/sie sich nicht bereits zuvor dort angemeldet hatte) und dann wieder zu der Übungssystem-Seite zurückgeleitet wird, wo er/sie den Login-Link betätigt hatte. Ab sofort ist er/sie nun eingeloggt und kann über weiterführende Links auch zu autorisierungspflichtigen Seiten wechseln.

Navigiert der/die Nutzer/-in direkt zu einer autorisierungspflichtigen Seite, *ohne* vorher eine SSO-Anmeldung vorgenommen zu haben, fragt das Online-Übungssystem selbst direkt nach Loginname und Kennwort für einen *lokalen Login*. Der/die Nutzerin kann dann immer noch den lokalen Logindialog abbrechen/schließen und erhält daraufhin auch wieder einen Link zum Single Sign-On (sowie einen weiteren für erneuten lokalen Loginversuch) angeboten.

Ruft ein/-e Nutzerin direkt einen URL (z.B. per Bookmark oder „Deep Link“) auf, der zu einer autorisierungspflichtigen Seite (wie der Aufgabenübersicht einer Kursumgebung) führt, so verhält sich das System genauso wie im letzten Absatz beschrieben: Da zuvor kein SSO-Login stattgefunden

hatte, fragt das Übungssystem *lokal* nach Loginname und Kennwort[1], aber nach Abbruch des lokalen Logindialogs kann man auch eine SSO-Anmeldung vornehmen.

Links von anderen (an SSO angebundenen) Plattformen zum Übungssystem

Der wichtigste Anwendungsfall von Single Sign-On dürfte jedoch sein, dass sich Studierende oder Mitarbeiter/-innen nicht zuerst beim Online-Übungssystem (und später ggf. noch bei anderen Plattformen) anmelden, sondern dass sie sich zuerst in einer anderen (Portal-)Plattform via SSO anmelden und von dort aus einem Link zum Online-Übungssystem folgen.

Im Idealfall sollten die Nutzer dann vom Online-Übungssystem unmittelbar und ohne Notwendigkeit, erst noch auf »Login« zu klicken, als eingeloggt angesehen werden.

Um diesen möglichst komfortablen und transparenten Single-Sign-On-Prozess zu nutzen, sollten in diesen (Portal-)Plattformen nach Möglichkeit **spezielle SSO-URLs** in den Links verwendet werden (deren Aufbau im folgenden Unterabschnitt beschrieben wird). Diese weisen das Übungssystem an, vor Anzeige der Zielseite zunächst eine passive SAML-Authentifizierung beim IdP (Shibboleth) zu versuchen und dann erst (unabhängig vom Ergebnis) zum Linkziel weiterzuleiten:

- War der User im Portal bereits per SSO eingeloggt, so wird das unmittelbar erkannt. Der User ist dann also, wenn er einem solchen SSO-Link folgt, sofort und ohne weitere Interaktion automatisch auch im OÜS eingeloggt. (Das funktioniert sowohl bei loginfreien als auch loginpflichtigen Linkzielen.)
- Schlägt der passive SSO-Login fehl, weil beim Shibboleth keine SSO-Sitzung (mehr) offen ist, so verhält sich das Übungssystem anschließend genauso wie bei „normalen" Links, also wie im Folgenden beschrieben. Hat sich also z.B. ein User in VU oder Moodle *lokal* eingeloggt (explizit gegen SSO entschieden) und folgt dann einem solchen Link zum OÜS, wird auch dort bevorzugt nach einem lokalen Login gefragt (aber auch eine SSO-Möglichkeit geboten).

Wird dagegen ein „normaler" Nicht-SSO-URL als Linkziel verwendet, z.B. ein URL, der aus der Adresszeile des Browsers nach Aufruf der Zielseite (z.B. mit einem Teststudenten-Login) kopiert wurde, so wird das Online-Übungssystem ab sofort *dennoch* versuchen, dasselbe transparente Verhalten umzusetzen. Genauer wird es dazu anhand des `Referer`-Headers des HTTP-Requests versuchen, zu erkennen, ob der Link, den der Benutzer angeklickt hat, von einer Moodle-Instanz oder einem Portal wie StudyPort oder dem LVU stammt.

Ist dies der Fall, d.h. wurde erkannt, dass der Benutzer einem Link von Moodle, StudyPort oder LVU gefolgt ist, so verhält sich das Online-Übungssystem genau wie für SSO-URLs, also wie oben beschrieben.

Wenn dagegen ein „Nicht-SSO-URL" verwendet und *keine* bekannte Verweisquelle erkannt wurde[2], so wird sich das Online-Übungssystem aus Abwärtskompatibilitätsgründen wie folgt verhalten:

- Führt der Link zu einer loginfreien Seite im OÜS (wie der Übungssystem-Startseite oder der Kursstartseite einer Kursumgebung), dann ist der User im OÜS zwar nicht unmittelbar automatisch eingeloggt, kann sich aber per »Login«-Link und anschließend »SSO-Anmeldung«-Button über den IdP einloggen, ohne dabei noch einmal Benutzername und Kennwort eingeben zu müssen. Alternativ ist auch ein lokaler Login möglich.
- Führt der Link zu einer loginpflichtigen Seite (z.B. Deep-Link zu einer konkreten Aufgabe oder Aufgabenübersicht), wird immer erst nach einem lokalen Login gefragt. Falls dieser HTTP-Auth-Dialog abgebrochen wird, werden unter anderem ein SSO-Login oder ein erneuter lokaler

Loginversuch zur Auswahl angeboten.

Links in LVU, StudyPort oder Moodle sollten also nach aktuellem Stand in der Regel unabhängig davon funktionieren, ob das im folgenden Unterabschnitt beschriebene spezielle SSO-URL-Format verwendet wird oder nicht.

Dennoch sollte die Verwendung der SSO-Links bevorzugt werden, insbesondere aus folgenden Gründen:

- Sie funktionieren auch für Links aus Plattformen, die noch nicht explizit im Übungssystem als bekannte SSO-Verweisquellen freigeschaltet wurden.
- Sie funktionieren unabhängig von Browsersupport.
  - Die automatische Erkennung der Link-Quelle bei „Nicht-SSO-URLs“ dagegen hängt vom Browser-Support eines zu Tracking-Zwecken verwendbaren HTTP-Headers ab. Daher kann derzeit nicht garantiert werden, dass diese automatische Erkennung auch in zukünftigen Browserversionen „ewig“ weiter so funktionieren wird, nicht einmal, dass jetzt bereits in jedem Browser bei jeder Privacy-Einstellung funktioniert. Browser könnten aus Datenschutzgründen den Support dafür einschränken oder einstellen – auch wenn das angesichts der lokalen Übertragung (zwischen zwei Servern unter derselben Domain `fernuni-hagen.de` über https[3]) nicht sehr wahrscheinlich scheint und auch nur der Servername der Verweisquelle ausgewertet wird, es also egal ist, ob der Browser aus Datenschutzgründen weitergehende Teilinformationen (wie Pfad oder Query-String) aus dem URL der Quellseite entfernt.
- Des Weiteren behalten wir uns vor, den Support für die automatische Erkennung bei „Nicht-SSO-URLs“ zu deaktivieren, falls sich damit wider Erwarten noch Kompatibilitätsprobleme in anderen Nutzungsszenarien ergeben sollten.

Der Support für die „Referer-Erkennung bei Nicht-SSO-URLs“ wurde daher auch nicht für den Einsatz als Regelfall gedacht, sondern vor allem für den Fall eingebaut, dass jemand, der diese Anleitung nicht gelesen hat, aus Unwissen einfach einen z.B. aus der Browser-Adressleiste kopierten URL als Linkziel verwendet. Und auch, damit bestehende Links aus Portalen (aus der Zeit vor der SSO-Einführung) möglichst sofort das gewünschte Verhalten zeigen, ohne dass sie erst aufs SSO-Format konvertiert werden müssen.

URL-Aufbau von SSO-Links

Fast jeder Link zum Online-Übungssystem lässt sich in einen solchen SSO-Link „konvertieren“, indem im URL als erste Pfadkomponente `/SSO` immer direkt hinter dem Servernamen eingefügt wird.

Beispiele:

- Link zur Übungssystem-Startseite:
  `https://online-uebungssystem.fernuni-hagen.de/SSO/`
  (statt `https://online-uebungssystem.fernuni-hagen.de/`)
- Link zu einer konkreten, semesterspezifischen Kursstartseite:
  `https://online-uebungssystem.fernuni-hagen.de/SSO/vus/KursStartSeite/01614/SS10/`
  (statt `https://online-uebungssystem.fernuni-hagen.de/vus/KursStartSeite/01614/SS10/`)
- Veranstalterunabhängiger Link zu einer Kursstartseite (mit Weiche, falls es mehrere konkrete Angebote zur Kursnummer und Semester gibt):
  `https://online-uebungssystem.fernuni-hagen.de/SSO/KursStartSeite/55108/WS21/`
  (statt `https://online-uebungssystem.fernuni-hagen.de/KursStartSeite/55108/WS21/`)
- Smart-Link <https://online-uebungssystem.fernuni-hagen.de/download/smartlinks/smartlinks.html> zur Kursstartseite des laufenden Semesters (bzw. des Semesters des letztmaligen Kursangebots):
  `https://online-uebungssystem.fernuni-hagen.de/SSO/desel/KursStartSeite/01613/current/`
  (statt `https://online-uebungssystem.fernuni-hagen.de/desel/01613/KursStartSeite/current/`)

Links erzeugen

Wenn Portale eigenständig Links zu Online-Übungssystem-Umgebungen erzeugen, so sollte diese Linkerzeugung also einfach einmalig so angepasst werden, dass der Zusatz `/SSO` mit in den URL-Path aufgenommen wird.

Betreuer/-innen, die manuell Links zu von ihnen betreuten Übungssystem-Kursumgebungen in z.B. eine ebenfalls von ihnen betreute Moodle-Kursumgebung einfügen möchten, können hierzu auf einen einfachen **Linkgenerator** zurückgreifen:

Sie finden im Betreuerzugang ihrer Übungssystem-Kursumgebung unter Menüpunkt »Verknüpfungen« nun neben der Möglichkeit, einen LTI-Launch-URL (für die direkte Einbettung von Aufgaben oder Aufgabenheften ihres Kurses in Moodle) zu erzeugen, auch einen SSO-Link-Generator. Dort wählen Sie ein *Linkziel* aus, z.B. die Kursstartseite, die gesamte Aufgabenübersicht (über alle Hefte), eine spezielle Aufgabenübersicht spezifisch für ein bestimmtes Heft oder direkt eine Aufgabe. Sie können auch auswählen, ob Sie immer konkret auf diese bestimmte Kursumgebung (für ein bestimmtes Semester) verlinken möchten, oder ob Sie einen Smart Link <https://online-uebungssystem.fernuni-hagen.de/download/smartlinks/smartlinks.html> erstellen möchten. Der Link-URL kann dann einfach in die Zwischenablage kopiert und später z.B. in Moodle eingefügt werden.

Fußnoten

1. Der lokale Login ist in diesen Fällen unter anderem auch deshalb der Default, da manche Funktionen (für Mitarbeitende) nur über lokale Logins verfügbar sind (z.B. Alias-Logins, lokale Teststudenten- und Korrektorenzugänge).
2. Mögliche Gründe, warum die Erkennung nicht funktioniert, sind z.B.: Der Browser unterstützt den Referer-Header nicht oder unterdrückt ihn explizit aufgrund von Trackingschutz-

Einstellungen, oder er verwendet ein Format, das vom Ubungssystem nicht erkannt wird, oder der Link steht in keiner dem Übungssystem als gültige Verweisquelle bekannten FernUni-Plattform (wie `moodle*.fernuni-hagen.de`, `studyport.fernuni-hagen.de` oder `vu.fernuni-hagen.de`). Auch wenn Sie einen `http://`- statt eines `https://`-URLs verwenden sollten, wird aus Datenschutzgründen in der Regel kein Referer-Header mit gesendet.

3. Es wird hier vorausgesetzt, dass Sie HTTPS-URLs verwenden, also auf `https://online-uebungssystem.fernuni-hagen.de/…` verlinken und *nicht* auf `http://…`. In letzterem Fall würde eine unverschlüsselte Verbindung aufgebaut und der Browser wird sicherheitshalber keine Tracking-Informationen übertragen. (Auch eine anschließende serverseitige Umleitung zurück auf HTTPS ändert daran dann nichts mehr.)