Analiza możliwości wdrożenia logowania przez Węzeł Krajowy w SSO Uniwersytetu Medycznego w Poznaniu

Używane skróty

WK - Węzeł Krajowy, system dostępny dla użytkownika pod adresem https://login.gov.pl/

PZ - Profil Zaufany, jeden z dostawców tożsamości zintegrowany z WK

SSO - system Single Sign-On Uniwersytetu, dostępny dla użytkownika pod adresem m.in. https://uczelnia.ump.edu.pl/sso/logowanie.aspx

SAML - dokładnie SAML 2.0 - standard komunikacji pomiędzy systemem SSO Uniwersytetu i WK

Analiza techniczna

Powiązanie użytkowników z PESELami

Powiązanie użytkowników z PESELami jest konieczne, ponieważ WK używa PESELa jako identyfikatora użytkownika.

Tabela bazodanowa użytkowników (`dbo.uzytkownicy`) zawiera kolumnę `pesel`. Nie są potrzebne zmiany struktury bazy danych.

Kolumna jest nullowalna. Użytkownicy bez przypisanego numeru PESEL nie będą mogli się logować przez WK.

Logowanie przez WK dla obcokrajowców

Niektórzy użytkownicy systemów UMP są obcokrajowcami i w kolumnie PESEL mają wpisany ciąg rok-miesiąc-dzień urodzenia. Logowanie przez WK dla takich osób nie będzie działać, ponieważ WK nie będzie przekazywał tego niestandardowego “numeru PESEL” do systemu SSO.

Cudzoziemcy mieszkający w Polsce mają przypisany pełny PESEL. W teorii możliwe powinno być ich logowanie przez WK po podaniu tego PESELa. Muszą oni natomiast być zarejestrowani w systemie dostawcy tożsamości (np. PZ albo konto w banku).

Inną możliwością jest użycie opcji WK, która włącza autentykację przez Węzeł Transgraniczny. Wymaga to dodania odpowiedniego parametru w żądaniu autentykacji (AuthnRequest). Wtedy WK pozwala na uwierzytelnianie za pośrednictwem systemu w wybranym państwie Unii Europejskiej. Zamiast PESELa do SSO przekazywany będzie identyfikator eIDAS, który podobnie jak w przypadku PESELa trzeba przypisać do użytkownika po stronie SSO (dodatkowa kolumna w tabeli `dbo.uzytkownicy`).

Delegacja logowania do WK

Na ekranie logowania (https://uczelnia.ump.edu.pl/sso/logowanie.aspx) należy dodać przycisk “Zaloguj przez WK”. Naciśnięcie przycisku będzie wysyłało formularz logowania

informujący backend, żeby delegować uwierzytelnienie do WK.

Oprócz tego w widoku/kontrolerze przyjmującym dane logowania należy dodać warunkowe przekierowanie do WK. To znaczy, że jeśli użytkownik wybrał logowanie przez WK, wtedy kontroler powinien zwrócić odpowiedź przekierowującą do WK. Wymaga to wszystkich poniższych:

- Zapisania w sesji użytkownika adresu przekierowania “na skróty”.
- Wygenerowania żądania logowania (AuthnRequest). Żądanie musi być podpisane.
- Zwrócenia do przeglądarki formularza zawierającego ukryte pole z żądaniem logowania. Formularz powinien zawierać kod javascript automatycznie wysyłający go na odpowiedni adres WK.

Weryfikacja użytkownika powracającego z WK

Wymagane jest dodanie widoku/kontrolera powrotnego. Na niego WK będzie przekierowywać użytkownika po zakończeniu autentykacji. Kontroler będzie, w kolejności:

- Przyjmował od użytkownika (POST) artefakt SAML.
- Na podstawie artefaktu pobierał asercję. Wymaga to wykonania zapytania HTTPS z serwera SSO do WK, a następnie odszyfrowania otrzymanej asercji.
- Na podstawie PESEL z asercji wybierał użytkownika z lokalnej bazy. Jeśli użytkownik nie istnieje zwracany powinien być odpowiedni komunikat. Alternatywą jest automatyczne tworzenie konta.
- Pobierał zapisany w sesji użytkownika adres “na skróty”.
- Zapisywał identyfikator sesji WK w sesji użytkownika. Użytkownik nie może mieć możliwości zmiany ani podejrzenia tej informacji, czyli odpada niepodpisane i niezaszyfrowane ciasteczko.
- Przetwarzał udaną autentykację tak samo jak dla użytkowniczki logującej się bezpośrednio hasłem.

Wylogowywanie z sesji WK

Użycie funkcji wylogowania w systemie SSO powinno wylogować użytkownika z sesji WK. Realizowane jest to przez wykonanie następujących czynności widoku/kontrolerze wylogowania, w kolejności:

- Pobranie zapisanego identyfikatora sesji WK.
- Skonstruowanie i podpisanie żądania wylogowania.
- Wysłanie żądania do systemu WK, bezpośrednio z serwera, przez HTTPS.

- Zweryfikowanie podpisu otrzymanej odpowiedzi WK oraz jej poprawności.
- Usunięcie identyfikatora sesji WK z danych sesji użytkownika.
- Zakończenie sesji SSO - tak jak się dzieje w przypadku użytkownika zalogowanego lokalnie hasłem.

Opcjonalnie: wyłączenie logowania bezpośredniego

Opcjonalnie można wprowadzić możliwość indywidualnego wyłączenie logowania bezpośrednio w systemie SSO Uniwersytetu. Zaletą jest zmniejszenie powierzchni ataku - użytkownicy chcący korzystać tylko z WK nie będą mieli drugiego, aktywnego hasła w systemie SSO Uniwersytetu.

W celu wprowadzenia takiej funkcji kolumna zawierająca hasła użytkowników (w tabeli `dbo.hasla`) powinna mieć możliwość ustawienia wartości oznaczającej brak hasła i niemożność logowania hasłem (np. `null`). Można to też zrealizować osobną kolumną (`bool`) oznaczającą czy bezpośrednie logowanie hasłem jest włączone.

Usuwanie starych wpisów z DB

Jeśli powstanie potrzeba zapisywania w bazie danych sesji użytkowników - w celu przechowania adresu “na skróty” lub identyfikatora sesji WK - niezbędne będzie usuwanie nieaktualnych już wpisów (np. periodyczne usuwanie starszych niż określona delta czasu). Ma to zapobiec nieograniczonemu rośnięciu rozmiaru bazy danych.

Użycie pośredniczącego serwisu OpenID Connect

Implementacja serwisu pośredniczącego ma na celu zmniejszenie liczby serwisów integrowanych z WK. Ogranicza to koszty certyfikatów oraz koszty procesu integracji z WK (jedna integracja zamiast wielu). Pozwala też na dodawanie nowych serwisów bez udziału załogi WK. W przypadku Uniwersytetu z WK integrowany będzie tylko jeden system - SSO. W tym kontekście wprowadzenie serwisu pośredniczącego nie przynosi zysków.

Drugim argumentem przemawiającym za użyciem serwisu pośredniczącego OIDC jest przypadek, w którym SSO Uniwersytetu byłoby standardowym oprogramowaniem, którego kod źródłowy trudno zmieniać. W takim przypadku integracja z OIDC może być łatwiejsza niż z SAML2 (protokół wykorzystywany przez WK). Natomiast SSO Uniwersytetu jest dedykowanym oprogramowaniem, którego kod źródłowym można zmieniać. W tym kontekście użycie OIDC zamiast SAML2 nie przynosi zysków.

Użycie serwisu pośredniczącego, udostępniającego funkcjonalność WK za pomocą standardu OpenID Connect 1.0 nie wprowadza zalet, a wiąże się z kosztami w formie większej komplikacji systemu, większego kosztu infrastruktury, wolniejszego działania (więcej przekierowań przeglądarki użytkownika). Użycie dodatkowego serwisu pośredniczącego nie jest rekomendowane.

Scenariusze testowe

Logowanie przez WK

Użytkowniczka może zalogować się za pomocą WK

Założenia

1. Użytkownik posiada konto w systemie SSO. Konto ma przypisany PESEL.
2. Użytkownik posiada środki autoryzacji w systemie login.gov.pl (np. konto na Pofilu Zaufanym, logowanie przez hasło).

Przebieg testu

1. Użytkownik na stronie logowania SSO klika “zaloguj przez WK”.
    a. Jest przekierowywany do systemu login.gov.pl.
2. W systemie login.gov.pl dokonuje uwierzytelnienia.
    a. Jest przekierowywany na stronę SSO Uniwersytetu.
    b. Na stronie Uniwersytetu jest już zalogowanym użytkownikiem.

Logowanie przez WK z użyciem przekierowania “na skróty”

Użytkowniczka może zalogować się za pomocą WK z użyciem przekierowania “na skróty”

Założenia - jak w przypadku scenariusza logowania przez WK oraz dodatkowo

1. X oznacza poprawny URL “na skróty” wskazujący do serwisu Y Uniwersytetu.

Przebieg testu

1. Użytkownik wchodzi na stronę SSO z parametrem next=X w URLu.
    a. Wyświetla mu się strona logowania.
2. Użytkownik klika “zaloguj przez WK”.
    a. Jest przekierowywany do serwisu login.gov.pl.
3. Dokonuje udanego logowania w systemie login.gov.pl.
    a. Jest przekierowywany do serwisu Y.
    b. Jest zalogowanym użytkownikiem.

Logowanie przez WK bez konta UMP

Użytkownik dostaje wyjaśniający sytuację komunikat gdy zaloguje się przez WK, ale nie ma konta w systemie UMP.

Założenia

1. Użytkownik posiada środki autoryzacji w systemie login.gov.pl (np. konto na Pofilu Zaufanym, logowanie przez hasło).
2. W systemie SSO nie ma konta z przypisanym PESELem użytkownika.

Przebieg testu

1. Użytkownik na stronie logowania SSO klika “zaloguj przez WK”.
    a. Jest przekierowywany do systemu login.gov.pl.
2. W systemie login.gov.pl dokonuje uwierzytelnienia.
    a. Jest przekierowywany na stronę SSO Uniwersytetu.
    b. Na stronie Uniwersytetu nie jest zalogowanym użytkownikiem.
    c. Prezentowany jest komunikat o braku konta w SSO.
    d. Sesja WK jest niezwłocznie terminowana.

Podwójne logowanie przez WK

Test ma na celu sprawdzić przypadek, gdy zalogowany w SSO użytkownik zaloguje się ponownie przez WK.

Założenia - jak w przypadku scenariusza logowania przez WK

Przebieg testu

1. W karcie A przeglądarki użytkownik na stronie logowania SSO klika “zaloguj przez WK”.
    a. Jest przekierowywany do systemu login.gov.pl.
2. W karcie B przeglądarki użytkownik dokonuje kompletnego uwierzytelnienia w systemie SSO dowolnym sposobem.
3. W karcie A przeglądarki, w systemie login.gov.pl dokonuje uwierzytelnienia.
    a. Jest przekierowywany na stronę SSO Uniwersytetu.
    b. Na stronie Uniwersytetu jest zalogowanym użytkownikiem (na skutek logowania w karcie B przeglądarki).

c. Sesja WK jest niezwłocznie terminowana.

Nieudane logowanie przez WK

Jeśli logowanie przez WK się nie powiedzie użytkownikowi powinien zostać zaprezentowany wyjaśniający sytuację komunikat.

Założenia - jak w przypadku scenariusza logowania przez WK

Przebieg testu

1. Użytkownik na stronie logowania SSO klika “zaloguj przez WK”.
    a. Jest przekierowywany do systemu login.gov.pl.
2. W systemie login.gov.pl dokonuje nieudanego uwierzytelnienia (np. trzykrotnie podając błędny kod SMS logowania przez PZ).
    a. Jest przekierowywany na stronę SSO Uniwersytetu.
    b. Na stronie Uniwersytetu nie jest zalogowanym użytkownikiem.
    c. Prezentowany jest komunikat o błędzie logowania.

Wylogowanie z WK

Wylogowanie z SSO wylogowuje także z WK.

Założenia

1. Użytkownik ma aktywną sesję w systemie SSO, przypisaną do sesji WK (tzn. użytkownik zalogował się za pomocą WK).

Przebieg

1. Użytkownik klika “wyloguj” na stronie serwisu SSO.
    a. Sesja SSO jest terminowana.
    b. Sesja WK jest terminowana.
    c. Użytkownikowi prezentowana jest strona “po wylogowaniu”.

Scenariusze testowe dotyczące bezpieczeństwa

Niebezpieczne przekierowanie “na skróty”

Logowanie nie powinno dojść do skutku gdy adres “na skróty” prowadzi do nieznanych zasobów.

Założenia

1. X oznacza URL “na skróty” wskazujący do nieznanego serwisu.

Przebieg testu

4. Użytkownik wchodzi na stronę SSO z parametrem next=X w URLu.
    a. Wyświetla mu się strona logowania.
5. Użytkownik klika “zaloguj przez WK”.
    a. Prezentowana jest strona z błędem <<nieznany adres “na skróty”>>

Niepoprawny artefakt logowania

Gdy użytkownik poda w endpoincie powrotnym (Weryfikacja użytkownika powracającego z WK) podrobioną asercję, logowanie nie powinno dojść do skutku.

Założenia - brak

Przebieg testu

1. Użytkownik wysyła na adres enpointu powrotnego z WK spreparowane żądanie, zawierające podrobiony artefakt.
    a. Prezentowana jest strona z informacją o błędzie logowania.

Niepoprawna asercja logowania

Jeśli asercja pobrana na podstawie artefaktu z WK (Weryfikacja użytkownika powracającego z WK) nie jest poprawna, logowanie nie powinno dojść do skutku.

Założenia - jak w przypadku scenariusza logowania przez WK oraz dodatkowo

1. System SSO ma skonfigurowany niepoprawny certyfikat do odszyfrowywania komunikacji przychodzącej z WK.

Przebieg testu

1. Użytkownik na stronie logowania SSO klika “zaloguj przez WK”.
    a. Jest przekierowywany do systemu login.gov.pl.
2. W systemie login.gov.pl dokonuje uwierzytelnienia.
    a. Jest przekierowywany na stronę SSO Uniwersytetu.
    b. Prezentowany jest komunikat o błędzie logowania.

Niepoprawna odpowiedź WK podczas wylogowania

Wylogowanie z SSO Uniwersytetu nie powinno dojść do skutku dopóki SSO nie otrzyma od WK potwierdzenia zakończenia sesji. Jest to sytuacja awaryjna, wyjątkowa, w której ze względów bezpieczeństwa lepiej zablokować użytkownikowi możliwość zakończenia sesji niż pozostawić “wiszącą” sesję w WK. Obydwie sesje (SSO i WK) powinny wtedy wygasnąć po pewnym czasie, niezależnie od siebie. W nominalnym przypadku WK powinno od razu potwierdzić zakończenie sesji i wtedy SSO może wylogować użytkownika.

Założenia - jak w przypadku scenariusza wylogowanie z WK oraz dodatkowo

1. System SSO ma skonfigurowany niepoprawny certyfikat do odszyfrowywania komunikacji przychodzącej z WK.

Przebieg testu

1. Użytkownik klika “wyloguj” na stronie serwisu SSO.
    a. Użytkownikowi prezentowany jest błąd wylogowania.

Wymagania formalne

Stałe adresy IP do komunikacji z WK

Na środowiskach dev i test wymagane jest podanie listy adresów IP z których system SSO będzie nawiązywał połączenia do WK. Na niektórych środowiskach chmurowych (np. Heroku) uzyskanie stałego adresu IP jest problematyczne.

Na środowisku dev wymagane jest podanie listy adresów IP z których będą się łączyć użytkownicy. Oznacza to, że deweloperzy pracujący nad systemem muszą mieć stałe IP (np. w biurze albo przez VPNa ze znanym adresem wychodzącym).

Symulator WK - WK_SYM

Symulator (środowisko developerskie) ma za zadanie ułatwić pracę developerom. Pozwala on na testowanie zmian w kodzie “na żywo”.

Wniosek o dostęp do symulatora rozpoczyna procedurę przyłączenia do WK.

Po złożeniu wniosku COI skontaktuje się z integratorem. Trzeba przekazać informacje techniczne typu: adresy IP oraz identyfikator (nazwę) integrowanego systemu. COI daje wtedy dostęp na środowisko dev oraz udawane certyfikaty i można zaczynać prace developerskie.

Środowisko testowe/integracyjne

Środowisko integracyjne (zwane też testowym) jest niezbędne do przeprowadzenia

nadzorowanych testów. Środowisko integracyjne powinno zawierać system możliwie zbliżony do prawdziwego (wersji produkcyjnej).

Gdy takie środowisko jest gotowe należy złożyć wniosek o dostęp do środowiska integracyjnego WK (WK_INT). Podobnie jak w przypadku WK_SYM należy dogadać z COI detale techniczne.

Przeprowadzenie testów integracyjnych

Aby możliwe było produkcyjne wdrożenie integracji z WK konieczne jest wykonanie nadzorowanych testów na środowisku integracyjnym.

Konkretne scenariusze testów przesyła COI na etapie przyłączenia do WK_INT. Prawdopodobnie testy będą polegać na wykonaniu scenariuszy logowania, nieudanego logowania i wylogowania. Po wykonaniu testów należ przesłać do COI daty ich wykonania, żeby COI mogło sprawdzić w logach, czy komunikacja wygląda dobrze.

Certyfikaty do podpisywania i deszyfracji komunikacji z WK

Certyfikaty potrzebne są tylko na środowisko produkcyjne.

Trzeba je kupić od certyfikowanego dostawcy. Zestaw certyfikatów to koszt rzędu 1000 zł. Certyfikaty mają skończoną ważność rzędu kilku lat.

Wdrożenie produkcyjne

Integracja produkcyjna przeprowadzana jest w porozumieniu z COI i KPRM. Trzeba przekazać do COI publiczną część certyfikatów oraz inne dane techniczne systemu (podobnie jak przy integracji WK_SYM i WK_INT).

Trzeba też, oczywiście, zaktualizować kod działający na produkcji SSO Uniwersytetu.

Oficjalna dokumentacja integracji z WK

Dostępna jest dokumentacja i instrukcja integracji z WK - https://mc.bip.gov.pl/interoperacyjnosc-mc/wezel-krajowy-dokumentacja-dotyczaca-integracji-z-wezlem-krajowym.html. Szczególnie przydatne są załączniki 1. (procedura) i 2. (dokumentacja techniczna)