Moduł Integracji z Węzłem Krajowym (MIWK) – opis (stan na 29.01.2020)

Autor Modułu Integracji z Węzłem Krajowym zastrzega, że informacje tu zawarte są zgodne ze stanem faktycznym z dnia utworzenia dokumentu, jednakże z uwagi na fakt, że komponent jest cały czas w fazie rozwoju, pewne szczegóły/elementy mogą jeszcze ulec zmianie.

1. *Węzeł Krajowy*

Węzeł Krajowy (WK) to system nadzorowany przez Ministerstwo Cyfryzacji i administrowany przez COI, który umożliwia - w reakcji na odpowiednie żądania z zewnętrznej aplikacji, zwanej Systemem Dostawcy Usług (DU):

- uwierzytelnienie użytkownika posiadającego konto w ramach jednego z zaufanych i obsługiwanych przez WK z systemów Dostawców Tożsamości (np. takim systemem jest Profil Zaufany),
- następnie (w przypadku udanego uwierzytelnienia) przekazanie, w bezpieczny sposób, do systemu DU zestawu danych takiegoż użytkownika (numer identyfikacyjny, imię, nazwisko, nazwisko panieńskie, data urodzenia, miejsce urodzenia, płeć, adres + dodatkowe dane techniczne)

System DU w oparciu o ten zestaw danych może podjąć odpowiednie kroki zmierzające do uwierzytelnienia takiego użytkownika w swoim systemie (dać dostęp, odmówić dostępu, utworzyć konto lokalne, powiązać z kontem istniejącym, itp.)

Ważne! WK nie zastępuje logowania w Systemie DU – tylko je uzupełnia, oferując zaufane źródło informacji o użytkowniku.

Kompletna dokumentacja systemu Węzeł Krajowy znajduje się pod adresem:

https://mc.bip.gov.pl/interoperacyjnosc-mc/wezel-krajowy-dokumentacja-dotyczaca-integracji-z-wezlem-krajowym.html

Jest tu zarówno dokumentacja techniczna opisująca wymagania, jakie system DU musi spełnić od strony programistycznej by móc zintegrować się z WK, jak i procedura formalna, jaką należy przejść zanim konkretny system DU zostanie zintegrowany z WK.

2. *Moduł Integracji z Węzłem Krajowym – opis*

Moduł Integracji z Węzłem Krajowym (MIWK) to rozwiązanie własne Centrum Informatyki Statystycznej, które powstało na użytek wewnętrzny CIS/GUS, w celu spełnienia m.in. następujących wymagań:

- Potrzeby zaistnienia jednego uniwersalnego rozwiązania informatycznego implementującego, wymaganą przez WK, funkcjonalność związaną z generowaniem struktur SAML, podpisywaniem struktur oraz deszyfracją danych – tak by nie musiał tego robić, za każdym razem od początku, istniejące już i dopiero powstające, usługi/systemy Statystyki (funkcjonującej, jako Dostawca Usług).

- Potrzeby udostępniania systemom Statystyki zestawu kilku metod (API), które by były wywoływane w odpowiednich momentach interakcji z Węzłem Krajowym.

Dzięki takiemu podejściu, systemy (praktycznie niezależnie od ich technologii wykonania) chcące się zintegrować z Węzłem Krajowym, mogłyby zostać odciążone z potrzeby implementacji większości mechanizmów bezpośredniej interakcji z Węzłem Krajowym, a mogłyby wykorzystać do tego celu API udostępnianego komponentu.

Przyczynić się to miałoby do skrócenia czasu wykonania integracji przez Dostawę Usług oraz ujednolicenia wdrożenia takiej integracji.

Moduł Integracji z Węzłem Krajowym powstał w oparciu o dokumentację udostępnioną publicznie przez Ministerstwo Cyfryzacji (oraz COI). Wpisuje się on w schemat wymiany komunikatów z systemem Węzeł Krajowy.

W obecnej chwili znajduje się on jeszcze w fazie testowej.

3. *Moduł Integracji z Węzłem Krajowym (MIWK) –API*

Moduł Integracji z Węzłem Krajowym jest usługą sieciowa wykonaną w technologii .NET. Wspierana jest tu zarówno komunikacja SOAP jak i REST

Moduł udostępnia trzy metody (funkcje) – funkcjonalność każdej z nich jest ściśle powiązana z konkretnym etapem wymiany komunikatów systemu DU z systemem WK:

- **`WygenerujAuthnRequest`**

Metoda generująca początkowy (w komunikacji z WK) komunikat AuthnRequest.

Komunikat AuthnRequest jest zwracany do klienta usługi jako BASE64 – czyli dokładnie w takiej postaci jakiej oczekuje Węzeł Krajowy. Klient usługi, zatem musi w zasadzie tylko podstawić go pod odpowiednie pole na formularzu wysyłki do WK.

- **`PrzekazArtifactResolve`**

Metoda generuje, podpisuje i **przesyła** komunikat ArtifactResolve na wskazaną w konfiguracji usługę po stronie WK.

Jej rolą jest wsparcie procesu pozyskania danych konkretnego użytkownika – przede wszystkim rozkodowanie asercji do postaci czytelnej dla klienta usługi.

Metoda po wysłaniu ArtifactResolve, otrzymuje z WK komunikat ArtifactResponse i przetwarza go. A następnie zwraca do klienta usługi **rozszyfrowaną** asercję (zestaw danych o użytkowniku).

- **`PrzekazLogoutRequest`**

Metoda generuje, podpisuje i przesyła komunikat LogoutRequest na wskazaną w konfiguracji usługę po stronie WK.

Jej rolą jest obsługa wylogowania użytkownika z Węzła Krajowego.

4. *Klient usługi MIWK – zalecenia dotyczące integracji*

Na samym początku sugeruję zapoznać się z dokumentacją umieszczoną na stronach Ministerstwa (https://mc.bip.gov.pl/interoperacyjnosc-mc/wezel-krajowy-dokumentacja-dotyczaca-integracji-z-wezlem-krajowym.html)– przydatna może być Instrukcja Integratora Dostawcy Usług, tak by był znany chociaż ogólny obraz, jak przebiega interakcja między systemami.

Podstawowym wymaganiem dla systemu chcącego się zintegrować z Węzłem Krajowym za pośrednictwem Modułu Integracji jest to, by taki system miał możliwość wywołania usługi sieciowej SOAP lub REST.

Musi też posiadać następujące funkcjonalności (wynikające z oficjalnej dokumentacji opisującej integrację z Węzłem Krajowym):

1. Stronę WWW z ukrytym formularzem HTTP POST, która będzie służyć do inicjacji komunikacji z WK. Strona będzie komunikować się z MIWK, a następnie wysyłać do WK wygenerowany komunikat AuthnRequest. Strona teoretycznie nie powinna być widoczna dla użytkownika i powinna automatycznie dokonywać wysyłki formularza (a więc np. JAVASCRIPT)
2. Stronę WWW oczekującą na zwrócenie przez WK obiektu SAML Artifact. Strona taka powinna otrzymany obiekt przekazać do MIWK i oczekiwać na rozkodowane dane o użytkowniku.
3. Funkcjonalność przetworzenia otrzymanych z WK danych o użytkowniku – a więc funkcjonalność np. zalogowania w systemie na podstawie tych danych lub też utworzenie wcześniej nowego konta na podstawie tych danych
4. Funkcjonalność wylogowania użytkownika z Węzła Krajowego. Realizuje się to poprzez wywołanie odpowiedniej metody MIWK.

Wiedza w zakresie SAML nie jest wymagana – korzystając z MIWK, klient ma ograniczoną styczność z tymi strukturami i nie musi się nimi zajmować, pomijając momenty, kiedy:

- musi wysłać do WK formularzem POST HTTP zakodowaną w BASE64 gotową (otrzymaną od MIWK) strukturę AuthnRequest,

- otrzyma z MIWK już rozkodowaną asercję, która jest strukturą SAML, ale nawet wtedy może ona być potraktowana, jako zwykły XML,

Tak samo ma się sprawa z podpisywaniem struktur XML i deszyfracją danych – to robi usługa MIWK.

Klient usługi, chcący być uznanym przez WK, jako system Dostawcy Usług, musi taki system zarejestrować w MC/COI. Procedura jest opisana w dokumentacji na stronie Ministerstwa. W przypadku integracji systemów Statystyki procedura rejestracji jest prowadzona przy wsparciu przez pracowników CIS.

5. *Moduł Integracji z Węzłem Krajowym (MIWK) – schemat wymiany komunikatów z WK (wersja SOAP)*