Fundusze Europejskie Polska Cyfrowa | Rzeczpospolita Polska | Rozwój Systemu Rejestrów Państwowych | Unia Europejska Europejski Fundusz Rozwoju Regionalnego

Standardy technologiczne

Systemu Rejestrów Państwowych

Numer wersji: 1.0

Data ostatniej aktualizacji: 2019-12-22

1 Wstęp

Celem dokumentu jest przedstawienie standardów technologicznych funkcjonowania Systemu Rejestrów Państwowych (SRP). Uzupełnienie niniejszego dokumentu stanowi dokument opisujący standardy wymiany danych przetwarzanych w rejestrach publicznych z wykorzystaniem Systemu Rejestrów Państwowych.

W skład Systemu Rejestrów Państwowych wchodzą rejestry:

- PESEL - Powszechny Elektroniczny System Ewidencji Ludności
- RSC - Rejestr Stanu Cywilnego
- RDO - Rejestr Dowodów Osobistych
- SOP - System Odznaczeń Państwowych
- CRS - Centralny Rejestr Sprzeciwów
- RDK - Rejestr Danych Kontaktowych

Zakres przetwarzanych i przechowywanych danych przez poszczególne rejestry jest określony przez przyjęte akty prawne (ustawy, rozporządzenia) podobnie jak sposób ich udostępniania oraz upoważnione do przetwarzania tych danych podmioty.

2 Protokoły wymiany danych

Wymiana danych pomiędzy SRP a systemami zewnętrznymi realizowana jest w oparciu o zestaw wystawianych usług sieciowych opartych o protokół zdalnego dostępu SOAP w wersji 1.1 bazujący na języku XML. Opis formalny poszczególnych usług jest zawarty w dokumentach WSDL. Warstwę transportową stanowi protokół HTTP w wersji 1.1 wykorzystujący szyfrowanie w oparciu o protokół TLS w wersji 1.2.

W przypadku rejestru RDK wymiana danych z systemami zewnętrznymi realizowana jest w oparciu o zestaw wystawionych usług sieciowych opartych na podejściu REST w formacie JSON i opisanych formalnie w dokumentach zgodnych ze specyfikacją Open API w wersji 3.0. Warstwa transportowa stanowi protokół HTTP w wersji 1.1 wykorzystujący szyfrowanie w oparciu o protokół TLS w wersji 1.2.

3 Struktury wymiany danych

Aktualnie obowiązujące kontrakty dla usług udostępnianych przez System Rejestrów Państwowych są opisane w dokumencie "Standardy wymiany danych przetwarzanych w rejestrach".

4 Integracja z podmiotami zewnętrznymi

Na postawie odrębnych procedur systemy zewnętrzne mogą otrzymać dostęp do usług sieciowych SRP. Podmioty uzyskując prawa do korzystania z usług otrzymują stosowną dokumentację w zakresie API usług (WSDL i OpenAPI odpowiednio).

5 Mechanizmy bezpieczeństwa

5.1 Procesy uwierzytelnienia

Proces uwierzytelniania odbywa się w oparciu o certyfikaty X.509 wydawane przez Centrum Certyfikacji Ministerstwa Cyfryzacji. W oparciu o posiadane certyfikaty nawiązywane jest szyfrowane połączenie w oparciu o protokół TLS w wersji 1.2, gdzie przeprowadzana jest weryfikacja ważności certyfikatu, jego wystawcy oraz czy certyfikat nie został odwołany w oparciu o listy CRL. Poprawne uwierzytelnienie użytkownika/systemu zewnętrznego pozawala na zestawienie szyfrowanego kanału komunikacyjnego umożliwiającego również dostępu do systemu. W przypadku niepowodzenia procesu uwierzytelniania kończy się błędem i brakiem dostępu do Systemu Rejestrów Państwowych.

5.2 Identyfikacja użytkownika

Użytkownik identyfikowany jest na podstawie informacji zawartej w polu SubjectDN certyfikatu, za pomocą, którego nawiązał połączenie TLS (informacja zawarta w SubjectDN jest jednocześnie loginem użytkownika w ramach SRP).

Każdy system zewnętrzny zobowiązany jest do zapewnienia po swojej stronie logowania wszystkich żądań przesłanych do SRP wraz z informacją o tym, jaki użytkownik (pracownik jednostki) odpowiada za przesłanie zapytania, a co za tym idzie, który pracownik uzyskał za pomocą zapytania dostęp do określonych danych.

5.3 Procesy autoryzacji

Proces autoryzacji rozpoczyna się po poprawnym uwierzytelnieniu i identyfikacji użytkownika/systemu zewnętrznego w Systemie Rejestrów Państwowych weryfikacją posiadanych przez podmiot uprawnień. Autoryzacja dostępu do poszczególnych

funkcjonalności w oparciu o posiadane uprawnienia odbywa się każdorazowo przed ich wywołaniem. Brak autoryzacji kończy się błędem i brakiem dostępu do funkcjonalności.

5.4 Procesy audytu

Wszystkie operacje wykonywane w Systemie Rejestrów Państwowych są rejestrowane w logu audytowym. W logu tym zapisywane są wszystkie wchodzące do systemu zlecenia aktualizacji lub udostępnienia danych. Wszystkie dane audytowe muszą zawierać informacje dotyczące podmiotu/osoby wysyłającej żądanie, parametry żądania, datę i czas żądania oraz rezultat żądania.

Ponadto w logu zapisywane są wybrane informacje diagnostyczne dotyczące poprawności działania poszczególnych rejestrów, co ma na celu szybsze wykrywanie i usuwanie problemów z funkcjonowaniem SRP.

5.5 Nadawanie uprawnień użytkownikom

Uprawnienia w SRP są nadawane przez administratora systemu w module autoryzacji Systemu Rejestrów Państwowych. Proces polega na zarejestrowaniu użytkownika przez administratora w module autoryzacji na podstawie wpisu w LDAP, który zawiera dane oraz certyfikat użytkownika. Następnie do użytkownika przypisywane są uprzednio zdefiniowane role, które są zbiorem uprawnień do określonych funkcjonalności systemu. Administrator z odpowiednim dostępem ma możliwość zdefiniowania nowej roli z istniejących uprawnień. Zarejestrowani użytkownicy, role i uprawnienia przechowywane są w wewnętrznej bazie modułu autoryzacji. Na takiej samej zasadzie administrator dodaje do systemu nowy zewnętrzny podmiot i nadaje mu uprawnienia do łączenia się do systemu, charakterystyczne dla połączeń pomiędzy systemowych.

W analogiczny sposób uprawnienia nadawane są wszystkim aplikacjom zewnętrznym, w tym aplikacjom wspierającym. Dla aplikacji zostaje wydany certyfikat przez Centrum Certyfikacji oraz zostaje wykonany wpis do bazy LDAP. Administrator SRP na tej podstawie tworzy wpis w bazie autoryzacji nadający aplikacji odpowiedni dostęp do systemu. Przypisując role do aplikacji można nadać jej uprawnienia do realizacji określonych usług i pobierania odpowiednich subskrypcji.

5.6 Poufność (ang. confidentiality)

System Rejestrów Państwowych eliminuje kradzież danych wprowadzając szyfrowanie komunikacji w oparciu o protokół TLS 1.2. Wydawanie certyfikatów w standardzie X.509 jest

realizowane przez urząd certyfikacji (CA) działający w Ministerstwie Cyfryzacji (Centrum Certyfikacji Ministerstwa Cyfryzacji).

5.7 Integralność (ang. integrity)

Wszystkie zmiany wykonywane w rejestrach państwowych wymagają podpisu operatora. Aplikacje wspierające muszą to uwzględnić w swojej konstrukcji. Po wygenerowaniu komunikatu (XML/JSON) opisującego zmianę w systemie, musi on zostać przekazany operatorowi i zostać przez niego podpisany. Następnie podpisany przez operatora komunikat (XML/JSON) zostaje osadzony w wywołaniu usługi WebService.

Podpisów nie wymagają operacje udostępniania danych (wyszukiwanie, pobranie danych, itp.). W przypadku udostępnienia usług zewnętrznej aplikacji wykorzystującej jedynie ograniczony zestaw usług realizujących weryfikację danych, ze względu na niskie ryzyko usługi, do połączenia wystarczy jedynie bezpieczny kanał mTLS zestawiony po dedykowanym łączu.

5.8 Dostępność (ang. availability)

System Rejestrów Państwowym został zbudowany w oparciu o architekturę wysokiej dostępności. Ma to na celu ograniczenie niedostępności dostarczanych przez system funkcjonalności w przypadku awarii któregoś z elementów systemu, jak również ograniczenia wpływu na niedostępność w trakcie prowadzenia prac serwisowych. Gwarantowany poziom dostępności systemu (SLA) wynosi 98 %.

6 Architektura poszczególnych warstw Systemu Rejestrów Państwowych

6.1 Architektura warstwy prezentacji danych (GUI)

Systemu Rejestrów Państwowych posiada interfejs graficzny użytkownika udostępniający funkcje SRP osobom uprawnionym. Interfejs użytkownika (GUI) umożliwia realizację procesów biznesowych w rejestrach w sposób przewidywalny i kontrolowany, zgodnie z zakresem funkcjonalnym. GUI użytkownika jest głównie oparte na architekturze "cienkiego klienta", czyli modelu, w którym logika biznesowa wykonywana jest na serwerach zarządzanych centralnie. Komponenty składające się na warstwę to przede wszystkim strony JSP odpowiedzialne za samą prezentację danych oraz Servlety, odpowiadające za kontrolę przepływu sterowania w aplikacji.

Wybrane komponenty wykorzystują wzorzec SPA (ang. Single Page Application) dostarczając graficzny interfejs użytkownika.

6.2 Architektura warstwy logiki biznesowej

Większość rejestrów wchodzących w skład System Rejestrów Państwowych wykorzystuje platformę JEE. Komponenty logiki biznesowej oraz Interfejs ŹRÓDŁO działają w obrębie wspólnego klastra serwera aplikacyjnego JEE (Java Enterprise). Logika biznesowa jest enkapsulowana w standardowych komponentach EJB (Enterprise JavaBeans, w wersji 3.0 i wyższej). Są to komponenty wykorzystywane do tworzenia złożonych aplikacji klasy enterprise. Działają one po stronie serwera aplikacji i są zarządzane przez kontener EJB serwera aplikacyjnego. Kontener implementuje zbiór systemowych funkcji zapewniających łatwą implementację lokalnych i zdalnych interfejsów komunikacyjnych, bezpieczeństwa komunikacji komponentów i obsługę transakcji.

Wybrane komponenty wchodzące w skład System Rejestrów Państwowych są elementami architektury EDA (ang. Event-Driven Architecture). Wykorzystują one koncepcje związane z architekturą mikrousług integrowanych za pomocą wymiany komunikatów (za pośrednictwem klastra EventHub). Architektura ta z definicji posiada cechy niezależnej skalowalności poszczególnych usług.

6.3 Architektura warstwy danych

Dane wszystkich Rejestrów przechowywanych w Systemie Rejestrów Państwowych są przechowywane w relacyjnej bazie danych. Poszczególne rejestry znajdują się w odrębnych schematach, obsługiwane są przez ten sam silnik bazodanowy, dzięki czemu możliwe jest zapewnienie własności ACID dla operacji dotyczących więcej niż jednego rejestru.

Niektóre moduły pomocnicze uruchomione są na odrębnych silnikach bazy danych. W uzasadnionych przypadkach dla komponentów wspierających mają również zastosowanie bazy typu NoSQL.

System Rejestrów Państwowym został zbudowany w oparciu o architekturę wysokiej dostępności. Ma to na celu ograniczenie niedostępności dostarczanych przez system funkcjonalności w przypadku awarii któregoś z elementów systemu, jak również ograniczenia wpływu na niedostępność w trakcie prowadzenia prac serwisowych. Minimalna dopuszczalna niedostępność systemy (SLA) wynosi 98 %.