Po co jest potrzebny system RWSS?

- łączenie środowisk rozproszonych w ramach jednej aplikacji

Jaki cel?

- ułatwienie komunikacji i kumulacja całej struktury do jednej aplikacji bardziej przyjaznej klientowi

Jaka jest główna zaleta RWSS?

- uatrakcyjnienie wizerunku systemu

System RWSS dzieli się na poszczególne zależne od siebie moduły (podsystemy) które możemy wyrazić jako elektronicznych klientów według określonej hierarchii, które pełnią określone zadania oraz dane uprawnienia.

a) e – Student - obsługa zdalna studenta

- propozycja nowego działania
- sprawdzenie dostępności systemu
- bezpieczna komunikacja z organem Samorządu Studentów działającym na danym Wydziale
- możliwości logowania się za pomocą SSO*
- możliwość logowania się za pomocą Węzła Krajowego*

***SSO** - Pojedyncze logowanie (ang. single sign-on, SSO) – możliwość jednorazowego zalogowania się do usługi sieciowej i uzyskania dostępu do wszystkich autoryzowanych zasobów zgodnych z tą usługą.

***Węzeł Krajowy** - Do zalogowania się w ten sposób potrzebny jest potwierdzony Profil Zaufany lub dowód osobisty z warstwą elektroniczną czyli e-dowód.

b) e – Dziekanat – zarządzanie pismami RWSS

- generowanie unikalnych znaków dla danej spraw
- dopisywanie użytkowników do poszczególnych ról
- bezpieczna wymiana dokumentacji między jednostkami organizacyjnymi

c) e – Członek – obsługa bieżąca studenta w związku z bezpośrednim kontaktem studenta z jednostką

- rejestracja czasu w systemie zmianowym wykorzystując bieżącą lokalizację
- obsługa studenta na podstawie SSO uczelni
- dostęp do bezpiecznego komunikatora
- przypisywanie samemu sobie zadań w ramach działań RWSS
- organizacja eventów

d) e – Przewodniczący - administracja

- nadawanie specjalnych uprawnień poszczególnym członkom RWSS
- możliwość komunikacji ze starostami poprzez drogę elektroniczną
- importowanie bazy starostów z odpowiedniego pliku co miesiąc

- ieklaracja konkretnych wzorów pism na których standaryzację ma wpływ: → RWSS → Uczelnia → Sekcja Magazynu → Kanclerz → Zespół Kontrolingu
- wprowadzanie dyżurów danych członków
- wprowadzanie do systemu wydarzeń
- generacja poszczególnych pism do innych jednostek uczelni

Funkcjonalności modułów

Obowiązki modułu:

- skalowalność
- jednolitość
- klarowność

Projekt modułu:

- układ logiczny
- aktualne standardy programistyczne

Z wykorzystaniem odpowiedniej bazy danych i i platform programistycznych modułom podlega ich ewolucja, a ich budowa będzie odpowiednio zrozumiała dla każdego programisty.

Obowiązki funkcjonalności krytycznych:

- zdolność funkcjonalna na koniec pierwszej fazy wydania oprogramowania
- SLA* na poziomie min. 96%
- aktywacja logowania awaryjnego w razie błędu dwóch poprzednich
- dostęp do logowania awaryjnego dla każdego klienta z odpowiednimi uprawnieniami
- wyświetlanie odpowiedniej wiadomości dla administratora w razie wątpliwości co do zasadności danych uprawnień
- odebranie nadmiarowych uprawnień w razie braku akcji po 7 dniach roboczych
- kontrola nad odpowiednimi uprawnieniami raz na 2 tygodnie

Lista funkcjonalności krytycznych:

- logowanie przez SSO uczelniane
- logowanie przez Węzeł Krajowy
- logowanie awaryjne
- U2FA*
- nadanie uprawnień i ich kontrola
- e-Moduł Członka RWSS
- e-moduł Przewodniczącego RWSS

Celowość projektu

Rozwinięcie możliwości organizacyjne oraz możliwość bezpiecznej komunikacji poszczególnych jednostek organizacyjnych.

Bezpieczeństwo

Całośc ma być oparta na podstawie logowania do SSO uczelnianego oraz przez Węzeł Krajowy i umożliwiać podpisanie pisma zdalnie za pomocą metody U2F

Monitoring wydajności

W module e-Przewodniczącego mają być widoczne poszczególne wskaźniki efektywności każdego z członków RWSSu

*__SLA__ - Service Level Agreement (umowa o gwarantowanym poziomie świadczenia usług) – umowa utrzymania i systematycznego poprawiania ustalonego między usługodawcą a usługobiorcą poziomu jakości usług poprzez stały cykl obejmujący:

- uzgodnienia
- monitorowanie usługi
- raportowanie
- przegląd osiąganych wyników

*__U2FA__ (Universal 2nd Factor Authentication) - to protokół uwierzytelniania dwuetapowego, który wymaga od użytkownika podania dwóch form uwierzytelnienia, poza hasłem, aby uzyskać dostęp do konta. U2FA jest zwykle implementowany za pomocą sprzętu, takiego jak token USB lub token FIDO (Fast IDentity Online) lub za pomocą aplikacji na smartfonie. U2FA pozwala na zwiększenie bezpieczeństwa logowania, ponieważ nawet jeśli hakerzy uzyskają dostęp do hasła użytkownika, nadal nie będą mogli się zalogować, jeśli nie posiadają fizycznego urządzenia lub aplikacji uwierzytelniającej.

Wymagania techniczne systemu:

- charakter klastrowy
- redundancja
- codzienna replikacja bezpieczeństwa: → bazy danych → folderu z pismami wygenerowanymi → folderu z pismami wysłanymi do poszczególnych jednostek organizacyjnych