

Logowanie się do innej instytucji w ramach przyznanych uprawnień

Scenariusz	3
Rozważane konfiguracje techniczne	3
Przypadek niekomunikujących się systemów	3
Przypadek komunikujących się systemów	3
Przypadek wspólnego serwera uwierzytelniającego	4

Scenariusz

Jan Nowak pracujący w urzędzie w Garwolinie na stanowisku kierownika zostaje recenzentem w urzędzie w Grójcu, jednak nadal jest kierownikiem w urzędzie w Garwolinie. Jan Nowak ma konto i określone uprawnienia w systemie EZD w Garwolinie. Po objęciu nowego stanowiska administrator systemu EZD w Grójcu powinien nadać Janowi Nowakowi odpowiednie uprawnienia w tym systemie. Jakie akcje musi wykonać administrator aby nadać te uprawnienia?

Rozważane konfiguracje techniczne

Przypadek niekomunikujących się systemów

Założmy całkowitą niezależność systemów EZD w Grójcu i w Garwolinie. W takiej sytuacji administrator systemu w Grójcu może założyć nowe konto dla pana Jana Nowaka i przyznać mu odpowiednie uprawnienia.

Przypadek komunikujących się systemów

Założmy, że systemy EZD w Grójcu i Garwolinie używają serwerów CAS aby uwierzytelnić użytkowników, jednak każdy z tych systemów ma własną bazę użytkowników (i własny serwer CAS). Założmy też, że systemy mogą się komunikować.

W takiej sytuacji administrator systemu w Grójcu może skonfigurować lokalny serwer CAS tak, aby umożliwiał delegowanie procesu uwierzytelnienia do innego systemu. Jan Nowak podczas logowania do systemu w Grójcu będzie wybierał opcję "Uwierzytelnij mnie w innym serwerze" po czym z listy dostępnych serwerów będzie wybierał serwer CAS urzędu w Garwolinie. Przed tym serwerem będzie uwierzytelniał się swoimi danymi logowania do urzędu w Garwolinie. Oprócz tego administrator systemu w Grójcu będzie musiał nadać panu Janowi odpowiednie uprawnienia.

Aby była możliwość zastosowania takiego rozwiązania serwer CAS systemu w Grójcu musi udostępniać możliwość delegacji uwierzytelnienia do innego serwera. Lista serwerów do których możliwa jest delegacja musi być ograniczona. Wszyscy użytkownicy mogący zalogować się na serwerach, do których możliwa jest delegacja będą mogli zalogować się do urzędu w Grójcu - ale większość z nich nie będzie miała żadnych uprawnień. Jeśli serwer w Garwolinie też będzie udostępniał delegację zbiór użytkowników powiększa się. Ponadto będzie możliwość "cyklicznej delegacji uwierzytelnienia" - np z Grójca do Garwolina, z Garwolina do Grójca i tak dalej. Aby wiedzieć jaki będzie to miało wpływ na wydajność systemów, bezpieczeństwo i UX trzeba trochę nad tym pomyśleć.

Powyższe wskazuje, że być może potrzebna będzie delegacja z filtrem użytkowników - to znaczy: np tylko użytkownicy ABC i XYZ mogą delegować logowanie do serwera w Garwolinie.

Należy też przemyśleć, czy takie rozwiązanie wymaga globalnie unikalnych identyfikatorów użytkowników. Być może nie, bo podczas delegacji uwierzytelnienia serwer CAS może stosować mapowanie identyfikatorów. Przykład: użytkownik o id 1234 uwierzytelniony przez serwer w Garwolinie to użytkownik w Grójcu o id 4567.

Przypadek wspólnego serwera uwierzytelniającego

Być może uwierzytelnianie użytkowników w Garwolinie i w Grójcu będzie delegowane do jednego, zewnętrznego serwera uwierzytelniającego. Na przykład może to być logowanie za pośrednictwem banku. W takim przypadku dopuszczenie Jana Nowaka do używania systemu w Grójcu będzie sprowadzało się do nadania mu uprawnień.