1. Architektura bezpieczeństwa

1.1. Przyjęte założenia

W niniejszym rozdziale zakłada się, że Energa posiada system Active Directory, będący implementacją protokołu LDAP. W Active Directory będą możliwe zmiany wskazane w poszczególnych rozdziałach.

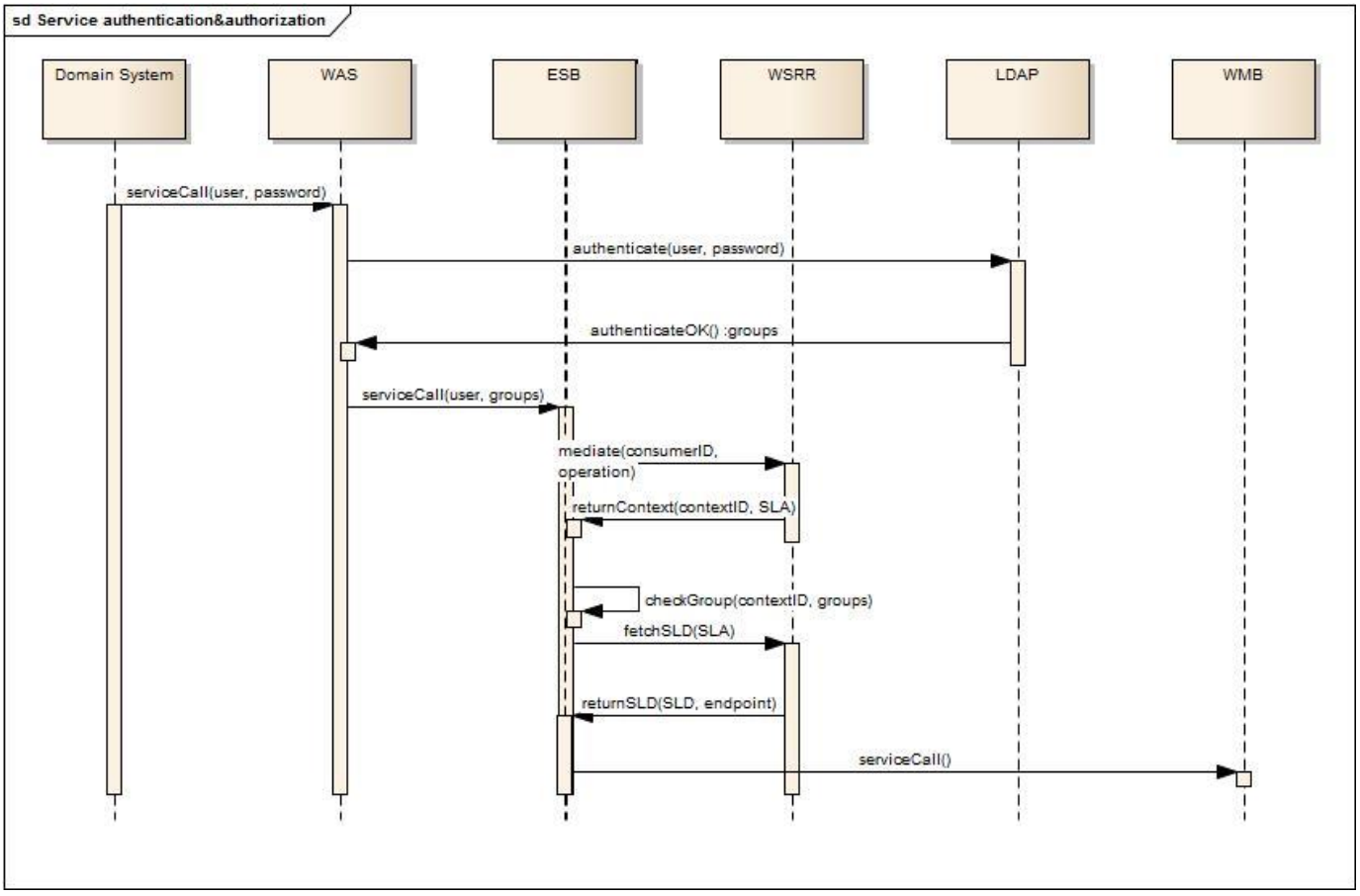
1.2. Koncepcja zabezpieczeń platformy integracyjnej

1.2.1. Założenia

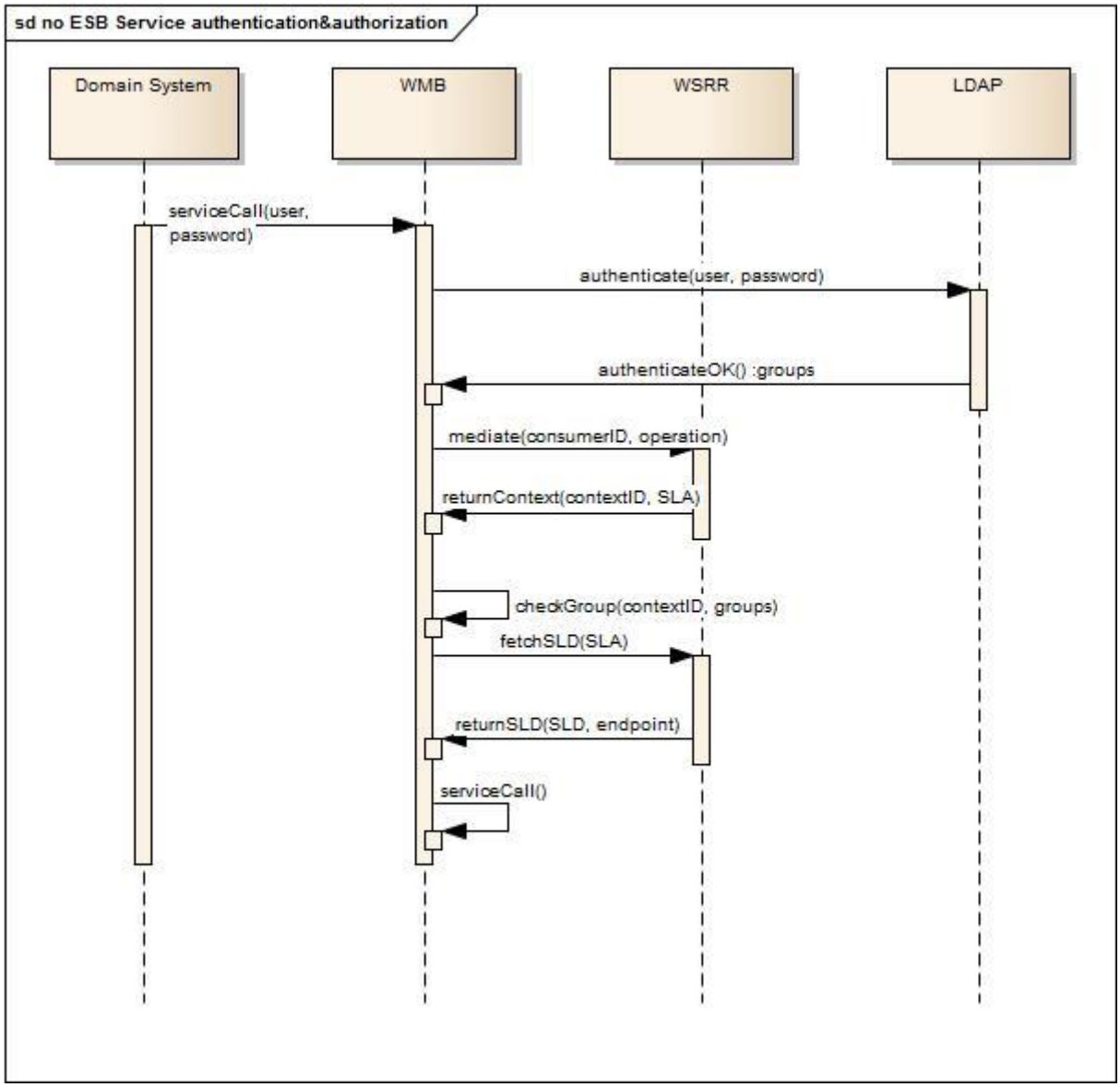
Dla usług typu SOAP zostanie wykorzystane uwierzytelnianie poprzez Basic Authetication.

Security Gateway będzie zabezpieczał usługi typu Web Services dostępne w ramach Energa. Koncepcja zabezpieczeń bazuje na repozytorium użytkowników zdefiniowanym jako struktura katalogowa w Active Directory.

W przyjętym projekcie technicznym zostały opracowane dwa podejścia realizujące zabezpieczanie usług przed niekontrolowanym dostępem stosowane w zależności od wariantu scenariusza komunikacji dla usługi (Załącznik 2). Poniższe diagramy ilustrują przyjęte rozwiązania.



Rysunek 1 - Uwierzytelnienie i autoryzacja usług w wariancie z WESB



Rysunek 2 - Uwierzytelnienie i autoryzacja usług w wariancie bez WESB

1.2.1.1. Uwierzytelnianie

Repozytorium Active Directory zostanie wykorzystane do przeprowadzenia operacji uwierzytelniania podczas obsługi żądań SOAP. Identyfikacja użytkownika wywołującego usługę będzie odbywała się w oparciu o login i hasło przesyłany w ramach komunikatu SOAP. Weryfikowane będzie:

- istnienie danego użytkownika w Active Directory,
- Zgodność hasła dla danego użytkownika w Active Directory

1.2.1.2. Autoryzacja

Błąd! Nie można odnaleźć źródła odwołania. przedstawia schemat mapowania ról dostępowych do określonych usług Web Services na grupy w Active Directory. Zakłada się, że rola dostępowa może obejmować swoim zasięgiem więcej niż jedną usługę, tzn. np. rola nazwana „UslugiRaportowe” może obejmować kilka usług pozwalających na tworzenie raportów, itp. Ogólna proponowana zasada tworzenia nazw jest następująca:

- Rola dostępowa=[Nazwa systemu][Nazwa metody lub grupy metod]_[Domena][Środowisko],
- Grupa LDAP = Rola dostępowa,
- DN grupy LDAP zawiera cn=[Grupa LDAP],
- Domena = [O=OSD, N=nonOSD],
- Środowisko = [P=produkcyjne, T=Testowe, D=Deweloperskie].

Przedstawiony został ogólny schemat sposobu definicji użytkowników usług Web Services Energa. Każde konto użytkownika może określać:

- użytkownika jako osobę,
- użytkownika jako system zewnętrzny (aplikację) wywołującą usługi Energa.

1.2.1.3. Koncepcja zabezpieczenia usług

Założeniem jest, aby każda z metod WSDL posiadała własną definicję zabezpieczeń. W związku z tym dla każdej metody może zostać stworzony oddzielny *endpoint*. Dostęp do danego endpoint będzie określany w większości przypadków przez WESB Security Gateway. Rzadziej, w przypadkach wymagających wysokiej wydajności będziemy stosować WMB Gateway. Szczegółowe podejście do zabezpieczenia poszczególnych usług będzie opisane w kontraktach i projektach szczegółowych usług. Usługa będzie wołana z użyciem Basic Authentication, gdzie będzie podany użytkownik i hasło.

Użytkownicy w AD będą przypisywani do odpowiednich grup w AD. Każda z takich grup będzie miała odpowiednik w WSRR: Context ID. W WSRR dla każdej udostępnionej usługi (odpowiednio dla każdego endpoint) będzie utworzona lista SLA dla odpowiednich Context ID.

1.2.2. Sposób integracji z istniejącą infrastrukturą

1.2.2.1. Konfiguracja Active Directory

Zmiany, które należy wprowadzić w Active Directory są następujące.

- Powinny być pozakładane grupy użytkowników zgodnie z tabelami w pkt.1.2.1.2.
- Powinni być pozakładani użytkownicy. Użytkownicy zakładani dla systemów dziedzinowych powinni mieć określane hasło bez terminu ważności. Użytkownicy zwykli powinni mieć ustawienia zgodne z polityką firmy. Dla użytkowników już zdefiniowanych możliwe są zmiany ustawień celem uspójnienia.
- Użytkownicy ze względu na role powinni być przypisani do konkretnych zdefiniowanych wcześniej grup AD. AD będzie wykorzystane w procesie uwierzytelniania oraz do przekazania grup przypisanych użytkownikowi.

1.2.2.2. WebSphere ESB, WSRR – definicja rejestru użytkowników

Konfiguracja Active Directory jako rejestru użytkowników odbywa się za pomocą konsoli administracyjnej WebSphere (*Integrated Solutions Console*) dostępnej pod adresem https://adres_IP:port/ibm/console (gdzie domyślnym portem jest 9043). Projekt techniczny zakłada wykorzystanie repozytorium typu „Federated repositories", a konfiguracja wymaga wprowadzenia parametrów połączenia z Active Directory wybierając typ serwera LDAP. Na potrzeby szyny KSD zostaną wskazane serwery LDAP funkcjonujące w ENERGA:

Konfigurowane konta użytkowników administracyjnych muszą odpowiadać istniejącym użytkownikom w Active Directory, ponieważ te konta będą potrzebne do zalogowania się do konsoli WebSphere.

1.2.3. WESB i WSRR

Konfiguracja WESB i WSRR obejmuje utworzenie repozytorium LDAP.

1.2.3.1. Podpięcie WSRR pod WESB

Po utworzeniu repozytoriów LDAP w konfiguracji WESB i WSRR należy z poziomu konsoli administracyjnej WESB utworzyć definicję (połączenie do) instancji WSRR. Typ połączenia to „Web service". Konfiguracja wymaga wprowadzenia adresu portu, na którym działa WSRR, a także podania aliasu uwierzytelniania dostępu do WSRR (można go utworzyć za pomocą „JAAS – J2C authentication data") oraz – w przypadku połączenia po https – wybrać konfigurację SSL (klucz serwera WSRR można zaimportować do magazynu kluczy „SSL Configurations").

1.2.3.2. Instalacja i konfiguracja aplikacji Gateway na WESB

Instalacja aplikacji sprowadza się do standardowej procedury na serwerze WebSphere Application Server. Po instalacji (przed uruchomieniem aplikacji) konieczne jest podpięcie polityk bezpieczeństwa i powiązań. Niezbędne jest również uzupełnienie zmiennych modułu SCA(moduł odpowiadający aplikacji Gateway). Najistotniejsza jest wartość zmiennej „CustomMediation.registryName", która powinna wskazywać adres, na którym nasłuchuje WSRR (ten sam adres, który został podany przy definicji WSRR w WESB).

1.3. Opis konfiguracji zabezpieczeń

1.3.1. Konfiguracja szyfrowania transmisji

Architektura Security Gateway uwzględnia zastosowanie serwera HTTP, który zapewni komunikację z wykorzystaniem SSL (HTTPS). Pozwoli to na szyfrowanie transmisji w oparciu o klucz publiczny serwera.

1.3.2. Konfiguracja kluczy

Koncepcja zabezpieczeń nie przewiduje szyfrowania zawartości komunikatów SOAP (szyfrowana będzie transmisja kanałem SSL). W zależności od wymagań zamawiającego certyfikat serwera może być:

- typu self-signed (w tym przypadku musimy zamieścić sposób generowania i instalowania certyfikatu),
- dostarczony przez autoryzowane centrum certyfikacyjne (wówczas opis instalacji na serwerze HTTP).

1.3.3. Konfiguracja systemu autoryzacji

WSRR zapewnia 2 mechanizmy kontroli dostępu (*access control*):

- Bazujący na SLA
- Fine-grained access control (link do strony producenta *http://www.ibm.com/developerworks/websphere/library/techarticles/0705_orchard/0705_orchard.html*)

Reguły SLA pozwalają na określenie zasad/warunków (np. przedział czasowy) w jakim dana usługa jest dostępna. SLA może zostać zdefiniowane z uwzględnieniem identyfikatora klienta. Podczas odpytania o adres usługi WSRR sprawdzi czy posiada regułę SLA dla danego klienta i jeśli nie to nie pozwoli na wywołanie usługi. Rozwiązanie to jest standardem w kwestii biznesowego zabezpieczania usług Web Services, jednak pociąga za sobą duży narzut prac tworzenia i administrowania reguł SLA. Np. jeśli mamy 10 usług i 5 typów klientów (systemów zewn.) tych usług to w celu udostępnienia usługi dla wszystkich konieczne jest utworzenie 10x5=50 reguł SLA.
Drugi sposób również wykorzystuje SLA (1 SLA dla usługi), ale pozwala na konfigurowanie reguł dostępu do danej usługi w oparciu o XACML. Reguły mogą uwzględniać repozytorium użytkowników z jakiego korzysta WSRR i bazować na przynależności użytkownika do określonych grup LDAP.