PSE-Operator S.A.

Wymagania bezpieczeństwa dla systemów transmisji danych SOWE/EL, WIRE/UR

Wersja 8.1

Data opracowania:	20 lipca 2008
Data zatwierdzenia:	24 lipca 2008
Data wejścia w życie:	24 lipca 2008
Daty aktualizacji:	24 lipca 2008

Warszawa, 24 lipca 2008

Metryka dokumentu

Historia dokumentu

Autor	Nr wersji	data	Treść zmian
Winuel SA, HP Polska	1.0	03-08-2000	Propozycja dokumentu do zaakceptowania
Winuel SA, HP Polska	2.0	25-08-2000	Uzupełnienie
Winuel SA, HP Polska	3.0	31-08-2000	Wprowadzenia zmian i rozszerzenie zakresu
Winuel SA, HP Polska	4.0	1-11-2000	Wprowadzenia zmian i rozszerzenie zakresu
Winuel SA, HP Polska	5.0	14-11-2000	Wprowadzenia zmian i rozszerzenie zakresu
Winuel SA, HP Polska	6.0	16-11-2000	Wprowadzenia zmian i rozszerzenie zakresu
Polskie Sieci Elektroenergetyczne - Info Sp. z o.o.	7.3	26-07-2002	Wprowadzenia zmian i rozszerzenie zakresu
Polskie Sieci Elektroenergetyczne - Info Sp. z o.o.	7.5	25-09-2002	Wprowadzenia zmian i rozszerzenie zakresu
Polskie Sieci Elektroenergetyczne - Info Sp. z o.o.	7.5a	30-09-2002	Wprowadzenia zmian i rozszerzenie zakresu
Winuel SA, Polskie Sieci Elektroenergetyczne - Info Sp. z o.o.	8.0	12-09-2007	Zmiany związane z wprowadzeniem SSL WebSphere MQ
Polskie Sieci Elektroenergetyczne - Info Sp. z o.o.	8.1	24-07-2008	Wprowadzono zapis dotyczący wymagań odnośnie funkcjonalność i konfiguracja urządzeń sieci komputerowej po stronie Operatora Rynku/Elektrowni oraz zapis dotyczący konfiguracji połączeń ICCP/OSP lub IEC104/OSP

Dane dotyczące dokumentu

tytuł dokumentu :	Wymagania bezpieczeństwa dla systemów transmisji danych SOWE/ EL, WIRE/UR.
Autor :	Winuel SA, Polskie Sieci Elektroenergetyczne - Info Sp. z o.o.
wersja :	8.1
poufność :	Do użytku wewnętrznego OSP i Operatorów Rynku
Liczba kopii :	- N/D
Data publikacji :	24-07-2008
Termin ważności :	Bezterminowa – kolejna wersja anuluje obecną
nazwa pliku i format :	Wymagania bezpieczeństwa dla systemów transmisji danych SOWE_EL, WIRE_UR.pdf
Streszczenie :	Dokument opisuje wymagania techniczne niezbędne do podłączenia systemu SOWE/EL, WIRE/UR do Systemu OSP.

Skróty i definicje użyte w dokumencie:

ABOR	-	Administrator Bezpieczeństwa Operatora Rynku
ABOSP	-	Administrator Bezpieczeństwa OSP
CCO	-	Centrum Certyfikacji OSP
AC	-	Administrator Certyfikatów
SRGW	-	Lokalny wydzielony lan sieci komputerowej w siedzibie OR umożliwiający komunikacje pomiędzy routerami dostępowymi, a gateway OR
OR	-	Operator Rynku posiadający system WIRE/UR
Elektrownia	-	Elektrownia posiadająca system SOWE/EL

SPIS TREŚCI

1 WSTĘP

Dokument przedstawia wymagania techniczne i organizacyjne, stawiane systemom Operatorów Rynku tj. WIRE/UR i Elektrowni tj. SOWE/EL, których spełnienie ma na celu zapewnić bezpieczną wymianę informacji z systemami informatycznymi OSP tj. odpowiednio SOWE lub WIRE. Niniejszy dokument nie dotyczy dostępu do Archiwum WIRE przez Internet.

2 WARUNKI DOSTĘPU DO SYSTEMU SOWE ORAZ WIRE

2.1 Platforma sprzętowa i programowa

W celu ochrony danych transmitowanych w ramach systemów SOWE/WIRE wykorzystany będzie protokół SSL (Secure Sockets Layer) na poziomie kanałów serwerów WebSphere MQ. SSL będzie wykorzystywany również do autentykacji menedżerów kolejek WebSphere MQ.

Zakłada się stosowanie następujących wersji oprogramowania IBM WebSphere MQ:

Wersja WebSphere MQ	Zestaw poprawek
6.0	**Fix Pack 6.0.1.1**

Aktualna lista dostępnych platform sprzętowych umożliwiających uruchomienie oprogramowania IBM WebSphere MQ wraz z protokołem SSL znajduje się na stronach producenta:

http://www-1.ibm.com/support/docview.wss?rs=171&uid=swg27006467

Zestaw poprawek aktualizacji oprogramowania znajduje się na stronach producenta:

http://www-1.ibm.com/support/docview.wss?rs=171&uid=swg27006037

2.2 Wymagania sieciowe

Konfiguracja serwera SOWE/EL, WIRE/UR dla warstwy sieciowej musi spełniać wymagania dot. styku sieciowego:

- Styk sieciowy - systemy OR lub Elektrowni komunikują się z Systemem OSP wykorzystując następujące drogi transmisji danych: 2 łącza minimum 64 kbit sieci SOWE/WIRE lub awaryjne łącze DialUp w przypadku awarii obu łącz sieci SOWE/WIRE.

2.3 Ochrona dostępu

Ochrona dostępu komunikacji serwerów SOWE/EL i WIRE/UR będzie realizowana na poziomie kanału SSL WebSphere MQ. Zakłada się włączenie dwustronnej autentykacji SSL. Do ustanawiania komunikacji poprzez SSL przeznaczone będą certyfikaty cyfrowe podpisane za pomocą aplikacji CCO przez Administratora Certyfikatów.

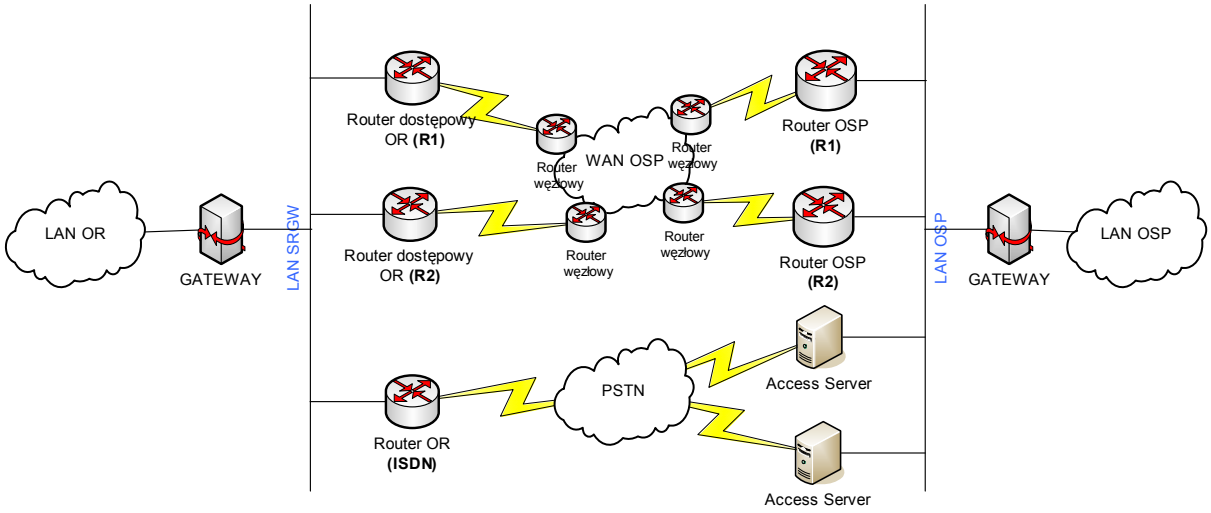
3 RODZAJE STYKÓW SIECIOWYCH

W warstwie połączeń sieciowych wymagane jest zestawienie redundantnego połączenia sieciowego pomiędzy serwerami SOWE/EL, WIRE,UR i serwerami SOWE/OSP, WIRE/OSP. W przypadku awarii któregoś z łącz

redundantnych routery dostępowe znajdujące się u Operatora Rynku/Elektrowni powinny automatycznie przełączyć ruch na działające łącze, a w przypadku awarii obu łącz, na połączenie Dial-Up.

W przypadku jednoczesnego realizowania połączeń pomiędzy systemami SOWE/EL i SOWE/OSP oraz WIRE/UR i WIRE/OSP na routerach dostępowych znajdujących się u Operatora Rynku/Elektrowni w strefie SRGW powinny zostać skonfigurowane dwa „routery wirtualne" (jeden dla ruchu SOWE, drugi dla ruchu WIRE), na które powinien być skierowany odpowiedni routing z gateway'a Elektrowni/OR.
Jeżeli z gateway'a poprzez SRGW poza połączeniami systemów WIRE lub systemów SOWE będą realizowane połączenia ICCP/OSP lub IEC104/OSP, to połączenia ICCP/OSP, IEC104/OSP powinny być skonfigurowane analogicznie jak połączenia WIRE i SOWE tj. jako kolejny „router wirtualny".
Wymagana jest synchronizacja czasu serwerów SOWE/EL, WIRE/UR z siecią SOWE/WIRE. Powinno to następować przy użyciu protokołu NTP; serwerami czasu są routery dostępowe sieci SOWE/WIRE dołączone do SRGW danego Elektrowni/OR.

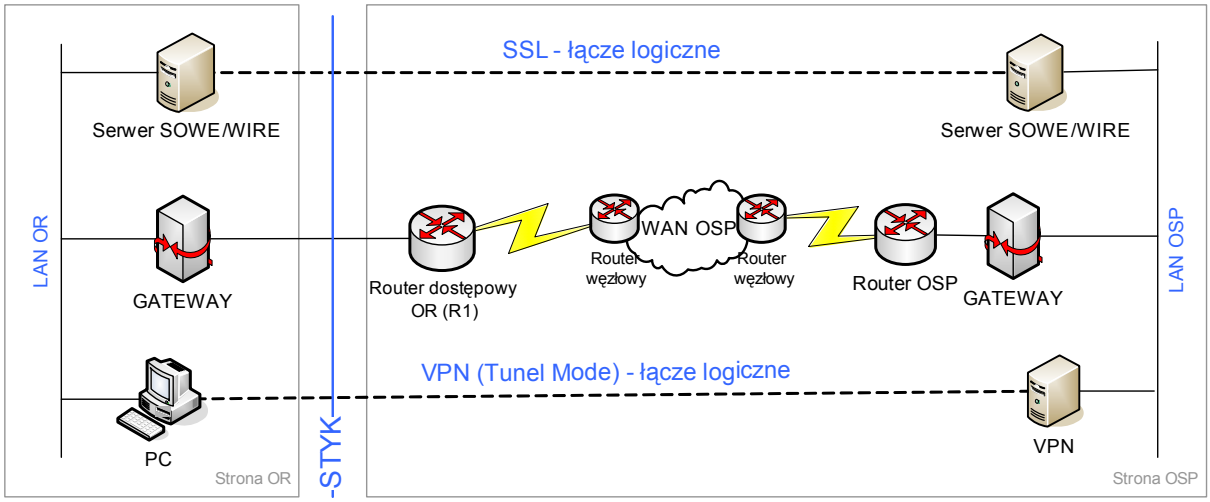
Funkcjonalność i konfiguracja urządzeń sieci komputerowej po stronie Operatora Rynku/Elektrowni powinny być zgodne z wymaganiami dla transmisji IP, w tym z RFC 1812.



Rys. Rodzaje styków sieciowych

3.1 Styk Podstawowy

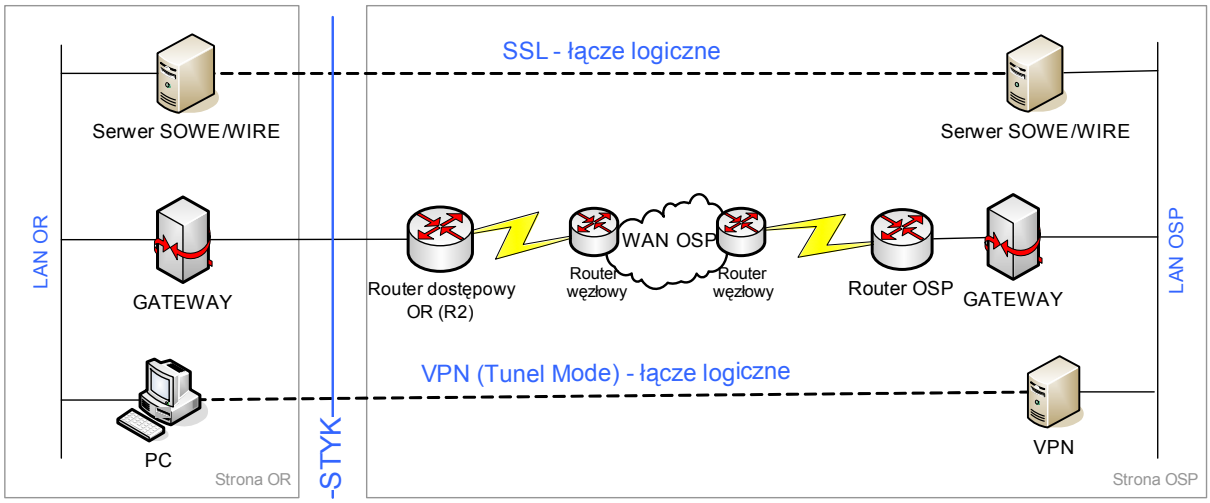
Styk Podstawowy realizuje połączenia IP na potrzeby transmisji danych pomiędzy serwerami SOWE/EL, WIRE/UR i serwerami SOWE/OSP, WIRE/OSP (menadżerami WebSphere MQ SOWE i WIRE) oraz VPN .



Rys. Styk podstawowy

3.2 Styk Zapasowy I

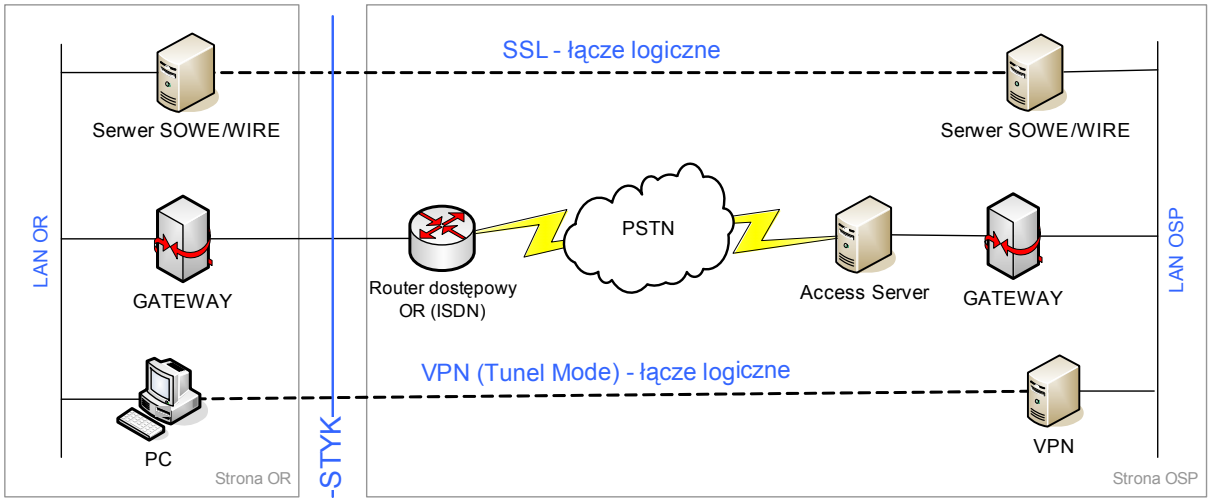
Styk Zapasowy I odpowiada funkcjonalnie stykowi podstawowemu. Styk ten jest wykorzystywany w sytuacjach awaryjnych, w przypadku braku dostępności styku podstawowego. Schemat rozwiązania przedstawiony został poniżej.



Rys. Styk zapasowy I

3.3 Styk Zapasowy II

Styk Zapasowy II odpowiada funkcjonalnie stykowi zapasowemu I, z tą różnicą, że wykorzystywane są połączenia komutowane ISDN. Ponadto jest to styk wykorzystywany w sytuacjach awaryjnych, przy braku dostępności Styku Podstawowego oraz Styku Zapasowego I. Schemat rozwiązania przedstawiony został poniżej.



Rys. Styk zapasowy II

3.4 Klasyfikacja urządzeń OR

Gateway znajdujący się w obszarze administracji Elektrowni/Operatora Rynku może być urządzeniem typu:

- Firewall (np. Checkpoint, PIX) – zaleca się ze względów bezpieczeństwa Elektrowni/Operatora Rynku.
- Router

Oba typy urządzeń mogą posiadać mechanizm NAT dla translacji adresów stacji roboczych VPN z lokalnych adresów IP do adresów przydzielonych przez OSP.

Routery dostępowe znajdujące się w obszarze administracji OSP stanowią integralną część sieci OSP. Zapewnienie routerów dostępowych oraz zestawienie i utrzymanie połączenia do routerów węzłowych sieci WAN OSP leży w gestii Elektrowni/Operatora Rynku. Specyfikacja techniczna tych urządzeń jest określana w ramach Procedury autoryzacji połączeń.

3.5 Adresacja IP

Serwery SOWE/EL i WIRE/UR muszą stosować osobne, przyznane przez OSP adresy IP. Wszystkie pakiety IP wychodzące z serwera SOWE/EL muszą mieć adres źródłowy IP dla SOWE/EL przyznany przez ABOSP. Analogicznie dotyczy to serwerów WIRE/UR.
Każdy serwer SOWE/WIRE powinien posiadać skonfigurowaną drogę odpowiednio do serwera SOWE OSP lub WIRE OSP.

4 WYMAGANIA W ZAKRESIE SSL SERWERA MQ

Do celów autoryzacji i identyfikacji serwerów WebSphere MQ SOWE/EL i WIRE/UR przy zestawianiu kanału SSL stosowana jest para kluczy dla serwera WebSphere MQ –, generowana przez ABOR i certyfikowana w Centrum Certyfikacji OSP przez AC.
Dla klucza serwera WebSphere MQ wymagane są następujące dane (w nawiasach podano obowiązujące wartości):

- Kraj - COUNTRY (C=PL)
- Organizacja - Organization (O=PSE-Operator)
- Jednostka Organizacyjna – Organization Unit (OU=CCO-WIRE) lub (OU=CCO-SOWE)

- Kod węzła - Common Name (CN=[Kod węzła])

  Wniosek o podpisanie certyfikatu generowany jest przy użyciu narzędzi WebSphere MQ lub innych narzędzi tworzących żądania certyfikatów zgodnych ze standardem X.509 w formacie DER lub PEM i wysyłany jest do podpisania do OSP poprzez aplikację webową CCO – Centrum Certyfikacji OSP.

5 WYMAGANIA W ZAKRESIE VPN DLA STACJI UŻYTKOWNIKA

Aplikacje Archiwum SOWE, Archiwum WIRE oraz WIRE/RP po stronie systemów OSP są udostępniane z wykorzystaniem bezpiecznego serwera WWW. Dostęp do bezpiecznego serwera WWW będzie realizowany ze stacji roboczych klasy PC. Bezpieczeństwo wymiany informacji jest uzyskiwane poprzez szyfrowanie danych za pomocą technologii VPN (AppGate) oraz autoryzację poprzez narzędzia RSA SecurID.

5.1 Wymagania sprzętowe

- Stacja kliencka użytkownika, umożliwiająca uruchomienie oprogramowania VPN.
- Token SecurID firmy RSA Security Inc.

5.2 Wymagane oprogramowanie

- System operacyjny stacji roboczej - Windows 2000/2003, Windows XP
- Oprogramowanie AppGate Client wersja 8.

5.3 Wymagania sieciowe

Każda stacja robocza użytkowników Archiwum SOWE/WIRE lub WIRE/RP powinna posiadać skonfigurowane połaczenie sieciowe do odpowiedniego serwera WWW OSP, wykorzystując połączenia sieciowe dla serwerów SOWE/EL, WIRE/UR opisanych w Rozdz. 3.

Adresy IP dla stacji roboczych użytkowników, stosowane w sieci SOWE/WIRE przez Operatorów Rynku, przydziela Administrator Bezpieczeństwa OSP. Są one przydzielane w momencie rejestracji nowego użytkownika Archiwum SOWE/WIRE.

6 PROCEDURY

Bezpieczeństwo systemów SOWE/WIRE jest uzależnione od wszystkich elementów tego systemu, w tym także od podłączonych systemów i aplikacji Elektrowni/Operatorów Rynku. W celu ograniczenia potencjalnych punktów zagrożeń, bezpieczeństwo całości podzielono na następujące aspekty:

- Organizacyjne – określające procedury i wymagania organizacyjne podłączania i uruchamiania systemów Elektrowni/Operatorów Rynku
- Techniczne – określające narzędzia i mechanizmy ochrony danych - poufność, autoryzacja i niezaprzeczalność transakcji.

6.1 Zalecenia Organizacyjne

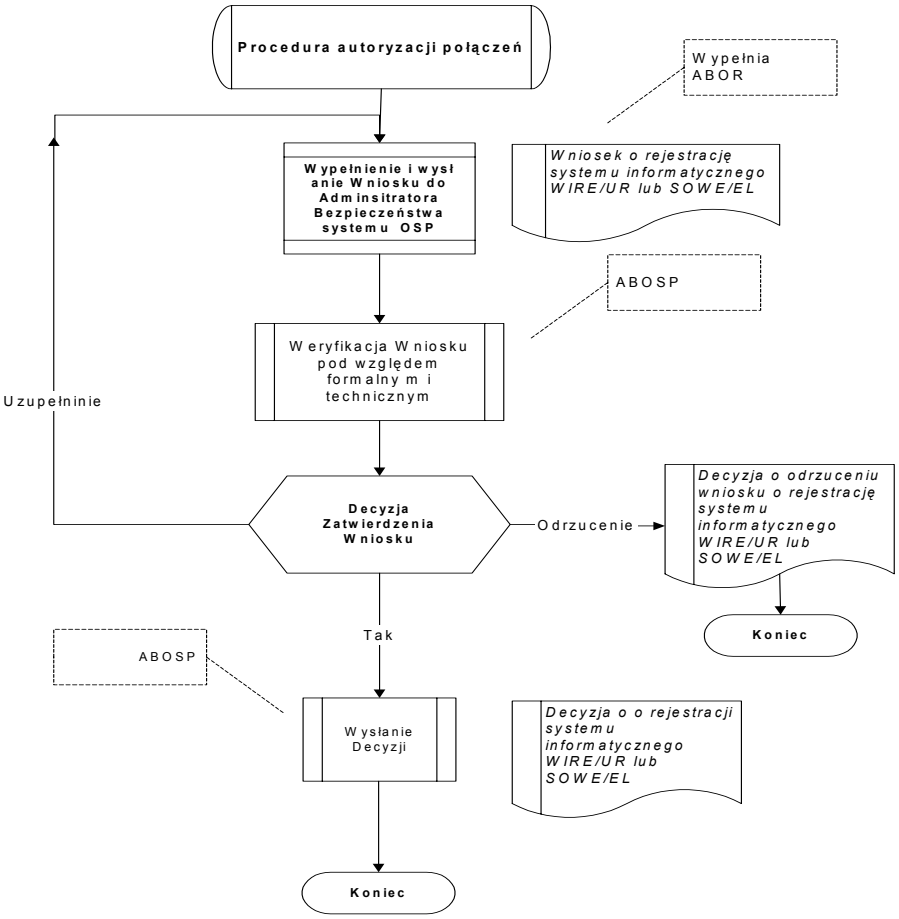
Zalecenia organizacyjne specyfikują zasady podłączania systemów SOWE/EL, WIRE/UR do systemu OSP oraz procedury kontroli i dystrybucji informacji niezbędnych do podłączenia systemów SOWE/WIRE Operatorów Rynku. Podstawowe elementy zaleceń organizacyjnych to procedury:

1. Procedura autoryzacji połączeń
2. Zarządzanie bezpieczeństwem systemów SOWE/WIRE

6.2 Procedura autoryzacji połączeń

Procedura określa proces składania wniosku o podłączenie systemu SOWE/WIRE Elektrowni/Operatora Rynku do systemu OSP, rozpatrywanie wniosku pod względem formalnym i technicznym, wymagania dotyczące personelu zarządzającego bezpieczeństwem. W procedurze są stosowane następujące formularze:

- Wniosek o rejestrację systemu informatycznego WIRE/UR lub SOWE/EL
- Decyzja o rejestracji systemu informatycznego WIRE/UR lub SOWE/EL
- Decyzja o odrzuceniu wniosku o rejestracji systemu informatycznego WIRE/UR lub SOWE/EL



6.3 Zarządzanie bezpieczeństwem systemów SOWE/WIRE

W ramach zarządzania bezpieczeństwem systemów SOWE/WIRE realizowane są następujące zasady:

- Poufność Transakcji – komunikacja użytkowników i aplikacji działających w ramach współpracy z system OSP jest szyfrowana przy użyciu SSL.
- Identyfikacja i Autoryzacja Elementów Systemu Operatora Rynku i OSP –elementy będą jednoznacznie identyfikowane na następujących warstwach:
    - Aplikacji Websphere MQ – wszystkie serwery będą jednoznacznie identyfikowane na podstawie certyfikatu elektronicznego zgodnego z normą X.509v 3 używanego w kanałach SSL WebSphere MQ.
    - Sesji – zestawianie sesji będzie możliwe tylko dla wskazanych portów TCP/UDP, po identyfikacji i autoryzacji przez warstwę Użytkownika i warstwę Aplikacji.
    - Sieci – zestawianie połączeń sieciowych będzie identyfikowane na podstawie adresów IP.

      Osobą odpowiedzialną za nadzorowanie wymagań bezpieczeństwa Systemu OSP jest Administrator Bezpieczeństwa – ABOSP. W szczególności odpowiada on za:
    - Określanie zasad bezpiecznego przechowywania kluczy prywatnych oraz kluczy identyfikacyjnych w OSP.
    - Określanie parametrów technicznych niezbędnych do podłączenia nowych węzłów SOWE/EL i WIRE/UR do węzła centralnego OSP.
    - Zarządzanie konfiguracją w zakresie systemu bezpiecznego dostępu AppGate.
- Osobą odpowiedzialną za dystrybucje certyfikatów do komunikacji SSL serwerów WebSphere MQ poprzez CCO tj. obsługę pozyskiwania, odnawiania i anulowania certyfikatów jest Administrator Certyfikatów – AC.
- Dla wszystkich styków odpowiedzialność ABOSP za bezpieczeństwo kończy się na urządzeniach aktywnych sieci SOWE/WIRE znajdujących się u Operatora Rynku/Elektrowni
- Operator Rynku wnioskujący o przyłączenie do systemu OSP wyznaczy osobę pełniącą funkcję Administratora Bezpieczeństwa Operatora Rynku - ABOR.:
- Podłączenie do systemu OSP realizowane jest po rozpatrzeniu „Wniosku o rejestrację systemu informatycznego WIRE/UR lub SOWE/EL" oraz uzyskaniu przez OR „Decyzji o rejestracji systemu informatycznego WIRE/UR lub SOWE/EL".
- Administrator Bezpieczeństwa Operatora Rynku odpowiedzialny jest za:
    - Przekazywanie informacji niezbędnych do prawidłowego skonfigurowania konta w systemie VPN AppGate.
    - Zarządzanie certyfikatami Operatora Rynku do komunikacji SSL WebSphere MQ
    - Określanie zasad bezpiecznego przechowywania kluczy prywatnych oraz kluczy identyfikacyjnych
- Podłączenie do Systemu OSP realizowane jest po rozpatrzeniu „Wniosku o rejestrację systemu informatycznego WIRE/UR lub SOWE/EL" oraz uzyskaniu przez OR/EL „Decyzji o rejestracji systemu informatycznego WIRE/UR lub SOWE/EL".
- Operatorzy Rynku po przejściu procedury Autoryzacji połączeń uzyskują dostęp do informacji o sposobie zamawiania i uzyskiwania niezbędnego oprogramowania, kluczy i certyfikatów w tym dostęp do aplikacji CCO

- Każdy użytkownik systemu SOWE/WIRE ma przydzielone uprawnienia i zasoby wg. zasady „każdemu wyłącznie to co niezbędne". Nie dopuszcza się możliwości udostępniania „pełnego dostępu" do poszczególnych serwerów, łączy, urządzeń czy zespołów elementów, każdy użytkownik korzysta wyłącznie z indywidualnego konta z indywidualnie przydzielonymi uprawnieniami wynikającymi z funkcji jakie pełni w systemie SOWE/WIRE lub jakie wynikają z zaleceń ABOSP.
- Każda zmiana konfiguracji systemów OSP lub OR wymaga weryfikacji pod względem zgodności z polityką bezpieczeństwa.
- Nie spełnienie norm polityki bezpieczeństwa systemów SOWE/WIRE powoduje fizyczne odłączenie systemu SOWE/WIRE od sieci OSP
- Decyzję o dołączeniu lub odłączeniu systemu SOWE/WIRE podejmują osoby upoważnione przez OSP.
- Osoby odpowiedzialne ze strony OSP zatwierdzają wszystkie wnioski i dokumenty określone w procedurze Autoryzacji połączeń.
- Podstawowym mechanizmem autoryzacji i identyfikacji użytkowników systemu OSP jest RSA – SecureID.- każdy użytkownik posiada narzędzie RSA SecurID.

7 WYMAGANIA TECHNICZNE

7.1 SSL

- Długość klucza prywatnego oraz publicznego w standardzie DSS nie mniejsza niż 512bitów.
- Mechanizm autoryzacji i szyfrowania komunikacji sieciowej serwer-serwer systemów SOWE/WIRE przy użyciu kanałów SSL WebSphere MQ, w szczególności obsługujący:
  - SHA-1- algorytm skrótu
  - 3DES lub DES jako algorytm szyfrowania
- Certyfikaty Elektroniczne zgodne ze standardem X.509 wersja 3.

7.2 VPN

- Mechanizm identyfikacji użytkownika zgodny ze standardem stosowanym w systemie OSP.

7.3 Synchronizacja czasu

- Protokół synchronizacja czasu zgodny ze standardem NTP.

7.4 Routery dostępowe

- Powinny zapewniać routing pakietów zgodnie z protokołami RIP, OSPF, EIGRP oraz możliwość szyfrowania DES, 3DES, AES.