Wymagania bezpieczeństwa dla systemów transmisji danych

Wersja 10.0

Data opracowania:	20 lipca 2008
Data zatwierdzenia aktualizacji:	23 marca 2021
Data wejścia w życie aktualizacji:	23 marca 2021
Daty aktualizacji:	23 marca 2021

Konstancin-Jeziorna, 23 marca 2021

Polskie Sieci Elektroenergetyczne Spółka Akcyjna,
05-520 Konstancin-Jeziorna, ul. Warszawska 165, Sekretariat: tel. +48 22 242 10 92, fax +48 22 242 25 38, www.pse.pl

NIP 526-27-48-966, REGON 015668195, Nr KRS 0000197596
Sąd Rejonowy dla m.st. Warszawy, XIV Wydział Krajowego Rejestru Sądowego,
Wysokość kapitału zakładowego: 9.605.473.000.00, kapitał zakładowy w całości wpłacony

Numer rachunku bankowego:
56124059181111000049137468

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 podłączanego Podmiotu umożliwiający komunikacje pomiędzy routerami dostępowymi, a gateway Podmiotu.
OR	-	Operator Rynku posiadający system WIRE/UR
JWCD		Jednostka Wytwórcza uczestnicząca aktywnie w RB
Podmiot		użytkownik sieci WAN PSE S.A. posiadający własny węzeł (np. OR, JWCD)
Elektrownia	-	Elektrownia posiadająca system SOWE/EL
WIRE/UR	-	System Wymiany Informacji Rynku Energii, (System kliencki po stronie Operatora Rynku)
WAN		Sieć rozległa (Wide Area Network) PSE S.A. z węzłami lokalnymi Podmiotów oraz węzłami centralnymi w Centrach Przetwarzania PSE S.A.
SOWE/EL	-	System Operatywnej Współpracy z Elektrowniami (System kliencki po stronie Elektrowni)
SZOP	-	System Zdalnego Odczytu Pomiarów

SPIS TREŚCI

1 WSTĘP

Dokument przedstawia wymagania techniczne i organizacyjne, stawiane systemom informatycznym wykorzystującym komunikację IP poprzez sieć WAN PSE S.A. w szczególności systemom OR i Elektrowni. Realizacja tych wymagań ma na celu przyłączenie do WAN PSE S.A. i zapewnienie bezpiecznej wymiany danych z systemami informatycznymi OSP takimi jak SOWE, WIRE, SZOP.

Niniejszy dokument nie dotyczy dostępu do aplikacji WIRE/RP przez Internet publiczny oraz do systemów sterowania i nadzoru.

2 WARUNKI DOSTĘPU DO SYSTEMÓW OSP

2.1 Wymagania dla Systemów Podmiotów w zakresie komunikacji IP poprzez sieć WAN PSE S.A.

Każdy z Podmiotów wykorzystujących komunikację IP poprzez sieć WAN PSE S.A. (dalej nazywaną w skrócie także: WAN), zobowiązany jest zapewnić we własnym zakresie odpowiednią infrastrukturę telekomunikacyjną (urządzenia, okablowanie oraz dzierżawę łącz) umożliwiającą dowiązanie do sieci WAN PSE S.A.

Routery dostępowe węzła muszą wspierać następujące wymagania techniczne:

- obsługę dynamicznych protokołów routingu EIGRP, BGP oraz trasowania statycznego;
- filtrację ruchu sieciowego (na podstawie znaczników, prefiksów, ACL);
- obsługę zdalnego zarządzania z wykorzystaniem protokołu SSH;
- obsługę mechanizmu wirtualnej bramy.

Za zakup wszystkich urządzeń wchodzących w skład lokalnego węzła sieci IP oraz wykonanie instalacji okablowania i zasilania odpowiedzialny jest Podmiot realizujący dowiązanie do sieci WAN. Routery dostępowe muszą zostać skonfigurowane zgodnie z wytycznymi przekazanymi przez PSE S.A.. Za zarządzanie urządzeniami lokalnego węzła WAN odpowiedzialny jest Podmiot.
Do synchronizacji czasu dla systemów Podmiotu musi być wykorzystywany protokół NTP, przy czym źródłem czasu dla tych systemów będą wskazane przez PSE S.A. serwery NTP.
Wymagania dla lokalnego węzła sieci WAN Podmiotu podłączonego do sieci WAN PSE S.A. przez, który będzie realizowana komunikacja do systemów nadrzędnych:

- Lokalny węzeł sieci WAN musi zapewnić poprzez router/routery dostępowe jedną drogę transmisji danych dla wszystkich przyznanych podsieci systemów Podmiotu (SOWE, WIRE oraz SZOP);
- Routery dostępowe muszą realizować transmisję danych w standardzie Ethernet lub G.703;
- W celu umożliwienia komunikacji pomiędzy routerami dostępowymi, muszą być zapewnione redundantne przełączniki sieciowe. Pomiędzy routerami dostępowymi, a przełącznikami sieciowymi musi być zapewnione po jednym połączeniu w standardzie Ethernet. Z każdego routera dopuszczalne jest tylko jedno połączenia do jednego z przełączników.

Wymagania w zakresie konfiguracji węzła sieci IP na potrzeby przyłączenia systemów Podmiotu:

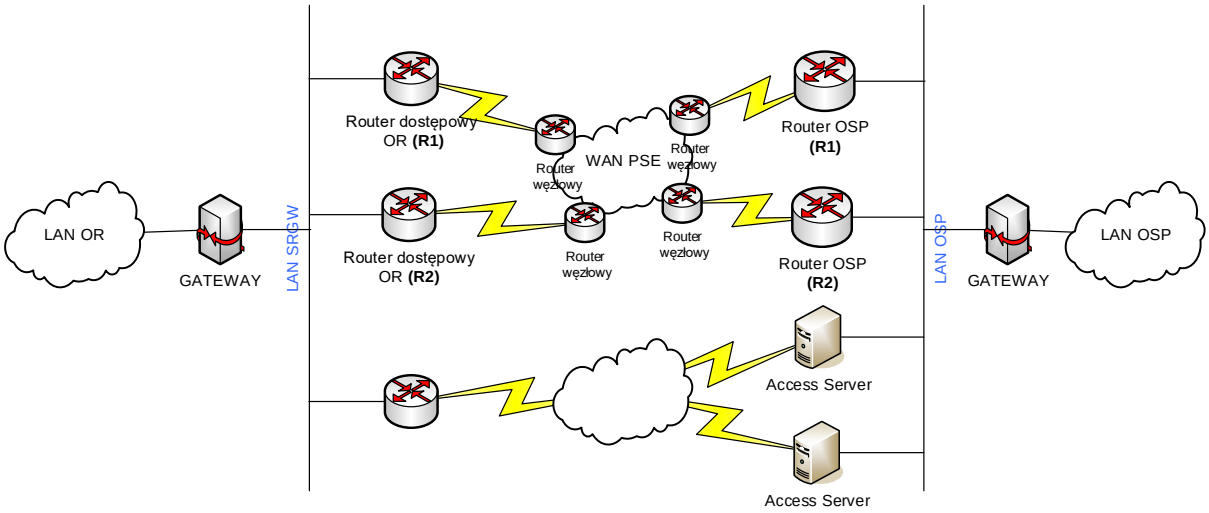
- Adresację IP dla podsieci mających komunikację z siecią WAN PSE, obejmującą również adresację interfejsów fizycznych oraz bram wirtualnych nadaje PSE S.A.;
- Punkt styku pomiędzy infrastrukturą sieci IP Podmiotu, a routerami dostępowymi musi stanowić wydzielona podsieć IP (tzw. segment SRGW), w której będzie możliwość skonfigurowania bramy służącej do kierowania tras dla dwukierunkowej komunikacji pomiędzy Podmiotem, a siecią PSE S.A.;
- W segmencie SRGW wyklucza się instalowanie jakichkolwiek nieuzgodnionych z PSE S.A. elementów systemu Podmiotu,
- Z routerów dostępowych będą wydawane dla segmentu SRGW tylko i wyłącznie interfejsy warstwy trzeciej modelu OSI;
- Wymaga się, aby każdy z systemów, który komunikuje się poprzez sieć WAN PSE S.A. z systemami nadrzędnymi, posiadał wydzieloną podsieć IP wraz z wirtualną bramą, utrzymywaną na infrastrukturze podłączanego Podmiotu. Adresację IP dla tych systemów nadaje w całości PSE S.A..
- O ile zachodzi konieczność migracji komunikacji Systemu do protokołu wykorzystującego stos TCP/IP, to Podmiot odpowiedzialny jest za dostosowanie infrastruktury Systemu oraz dowiązanie jej do węzła sieci WAN. Przyłączenie musi uwzględniać opisaną w rozdz. 3 strukturę fizyczną węzła sieci WAN oraz

pozostałe wymagania dla komunikacji IP Systemów Podmiotów określone w tym podrozdziale. Wymaga się także, by wszelkie kwestie związane z komunikacją po protokole IP tj. adresacja IP, metoda rozgłaszania i ew. filtracji tras była uzgadniania z PSE S.A.

Szczegóły realizacji lokalnego węzła WAN dla potrzeb komunikacji z systemami PSE S.A. (SOWE/WIRE/SZOP) opisane zostały w Rozdziale 3 niniejszego dokumentu.

3 RODZAJE STYKÓW SIECIOWYCH

W warstwie połączeń sieciowych wymagane jest zestawienie niezawodnej komunikacji pomiędzy serwerami systemów po stronie Podmiotu i serwerami systemów po stronie PSE S.A.. W przypadku awarii jednego z redundantnych łączy, routery dostępowe znajdujące się w lokalnym węźle WAN, muszą automatycznie przełączyć ruch na działające łącze.



Routing z lokalnej sieci (LAN OR) do sieci PSE S.A. (LAN OSP) powinien być skierowany przez urządzenie trasujące w sieci OR, na wirtualny adres utrzymywany przez routery dostępowe węzła lokalnego WAN.
W przypadku przyłączania kolejnych systemów wymagających komunikacji poprzez WAN PSE muszą one posiadać wydzieloną podsieć, dla której adresację IP nadaje w całości PSE S.A. Wirtualną bramą powinno być wówczas istniejące urządzenie trasujące (GATEWAY) z przydzielonymi, nowymi adresami IP dla tej podsieci. W wyjątkowych przypadkach dopuszcza się uruchomienie dedykowanych urządzeń trasujących dla systemów i redundantne podłączenie ich do SRGW w uzgodnieniu z administratorami PSE S.A..

Funkcjonalność i konfiguracja urządzeń sieci komputerowej po stronie Podmiotu musi być zgodna z wymaganiami dla transmisji IP, w tym z RFC 1812.
Czas na serwerach Podmiotów połączonych z siecią WAN PSE S.A. musi być synchronizowany przy użyciu protokołu NTP do serwerów czasu wskazanych przez PSE S.A.

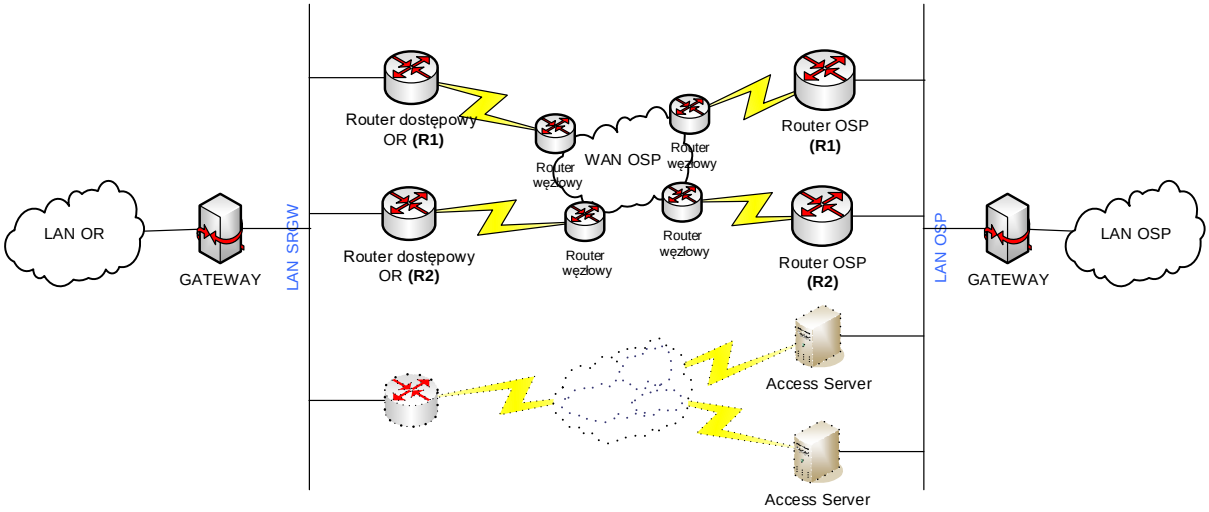
3.1 Opis wariantu z redundantnymi routeremi - zalecany

Węzeł sieci IP po stronie Podmiotu przyłączanego, składa się z dwóch routerów dostępowych, , dwóch przełączników sieci LAN oraz dwóch routerów lub firewalli stanowiących elementy infrastruktury Podmiotu. Z uwagi na niezawodność i elastyczność rozwiązania, jest ono zalecane dla OR oraz **wymagane** dla Elektrowni i podmiotów realizujących usługę typu „cloud" względem innych OR.
Routery dostępowe stanowią bezpośredni punkt styku z:

- siecią WAN PSE S.A., poprzez pojedyncze łącze w standardzie G.703 lub Ethernet z każdego z routerów dostępowych;
- routerami lub firewallami będącymi częścią infrastruktury Podmiotu przyłączanego, poprzez pojedyncze łącza Ethernet RJ45 z każdego z routerów dostępowych. (połączenia te muszą być zestawiane za pośrednictwem dedykowanych dwóch przełączników LAN).

Pomiędzy infrastrukturą sieci IP Podmiotu przyłączanego a routerami dostępowymi zostanie nadana przez PSE S.A. wydzielona podsieć IP (SRGW), w której funkcjonować będą bramy wirtualne (HSRP) służące do kierowania tras statycznych dla dwukierunkowej komunikacji pomiędzy podmiotem, a sieciami PSE S.A. W segmencie tym

wyklucza się instalowania jakichkolwiek innych systemów Podmiotu, których przeznaczeniem jest komunikacja z systemami PSE S.A.
Z routerów dostępowych będą wydawane dla segmentu SRGW tylko i wyłącznie interfejsy warstwy trzeciej modelu OSI.
Każdy z systemów lokalnych, który komunikuje się poprzez sieć WAN PSE S.A. z systemami PSE S.A. musi posiadać wydzieloną podsieć IP wraz z wirtualną bramą, utrzymywaną na infrastrukturze przyłączanego Podmiotu. Adresację IP dla tych systemów nadaje w całości PSE S.A.



3.2 Opis wariantu z pojedynczym routerem

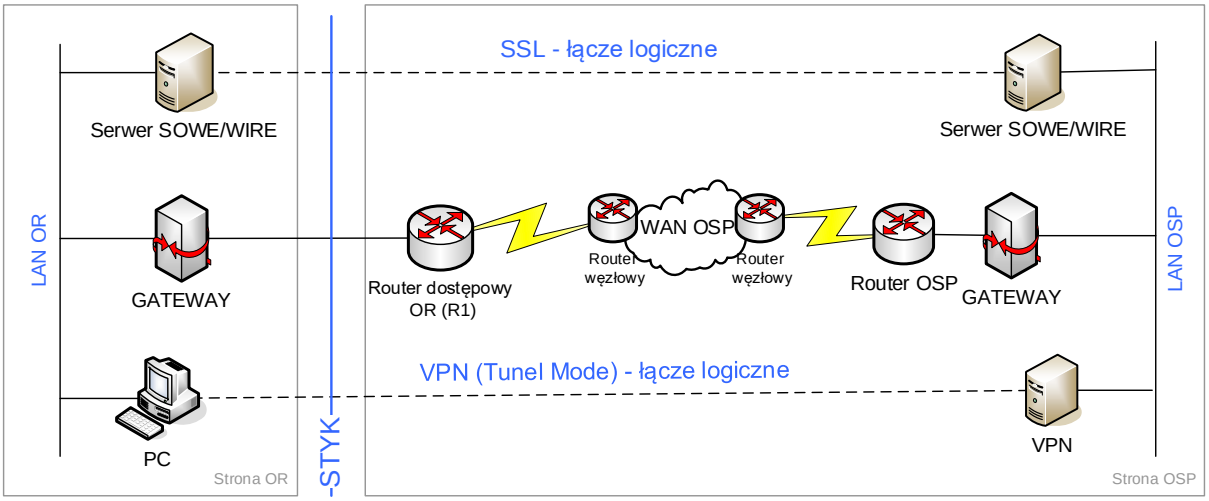
Styk Podstawowy realizuje połączenia IP na potrzeby transmisji danych systemów Podmiotu i serwerami nadrzędnymi w lokalizacjach PSE S.A.
Węzeł składa się z jednego routera dostępowego oraz routera lub firewalla stanowiących elementy infrastruktury Podmiotu przyłączanego do WAN PSE.

Router dostępowy stanowi bezpośredni punkt styku z:

- siecią WAN PSE S.A., który realizowany jest poprzez minimum jedno łącze w standardzie G.703 lub Ethernet;
- routerem lub firewallem Podmiotu przyłączanego z wykorzystaniem połączenia Ethernet (RJ45) poprzez przełącznik LAN

Modyfikację w/w wariantu stanowi zastosowanie drugiego łącza do sieci WAN PSE S.A. w standardzie G.703 lub Ethernet;

Jeśli pomiędzy interfejsem Ethernet routera dostępowego, a routerem Podmiotu nie będzie możliwe ustanowienie parametrów połączenia na drodze autonegocjacji konieczne jest zrealizowanie tego łącza poprzez dedykowany przełącznik sieci LAN, którego dostarczenie i instalacja leży po stronie Podmiotu przyłączanego. Zastosowanie przełącznika może być również konieczne w przypadku zbyt dużej odległości dla połączeń miedzianych pomiędzy routerem dostępowym, a routerem/firewallem.
Pomiędzy infrastrukturą sieci IP Podmiotu przyłączanego, a routerem dostępowym zostanie nadana przez PSE S.A. wydzielona podsieć IP (SRGW), w której funkcjonować będą bramy wirtualne (HSRP) służące do kierowania tras statycznych dla dwukierunkowej komunikacji pomiędzy Podmiotem, a sieciami PSE S.A.
Z routerów dostępowych będą wydawane dla segmentu SRGW tylko i wyłącznie interfejsy warstwy trzeciej modelu OSI.
Każdy z systemów, który komunikuje się poprzez sieć WAN PSE S.A. z systemami PSE S.A., musi posiadać wydzieloną podsieć IP wraz z wirtualną bramą, utrzymywaną na infrastrukturze Podmiotu przyłączanego. Adresację IP dla tych systemów nadaje w całości PSE S.A.



Rys. Schemat wariantu z pojedynczym routerem

3.3 Klasyfikacja urządzeń

Gateway znajdujący się w obszarze administracji Podmiotu przyłączanego może być urządzeniem typu:

- Firewall (zalecany ze względów bezpieczeństwa)
- Router

Oba typy urządzeń mogą posiadać mechanizm NAT dla translacji adresów stacji roboczych VPN z lokalnych adresów IP do adresów przydzielonych przez PSE S.A.. Na routerach dostępowych nie będzie realizowana usługa translacji adresów.

Routery dostępowe stanowią integralną część sieci WAN PSE. Zapewnienie routerów dostępowych oraz zestawienie i utrzymanie połączenia do routerów węzłowych sieci WAN PSE S.A. leży w gestii przyłączanego Podmiotu. Specyfikacja techniczna tych urządzeń określana jest w ramach Procedury autoryzacji połączeń.

3.4 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, a także elementów systemów SZOP.
Każdy serwer SOWE/WIRE powinien posiadać skonfigurowaną drogę odpowiednio do serwera SOWE OSP lub WIRE OSP.

4 WYMAGANIA DLA SYSTEMÓW SOWE/WIRE

4.1 Platforma sprzętowa i programowa w zakresie serwera MQ

W celu ochrony danych transmitowanych w ramach systemów SOWE/WIRE wykorzystany będzie protokół TLS 1.2 na poziomie kanałów serwerów IBM MQ. TLS będzie wykorzystywany również do autentykacji menedżerów kolejek IBM MQ.

Zakłada się stosowanie następujących wersji oprogramowania IBM MQ:

Wersja IBM MQ	Zestaw poprawek
8.0 lub 9.0	**Fix Pack 8.0.0.14 (dla 8.0)**

Aktualna lista dostępnych platform sprzętowych umożliwiających uruchomienie oprogramowania IBM MQ wraz z protokołem TLS 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

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

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

- Kraj - COUNTRY (C=PL)
- Organizacja - Organization (O=PSE S.A.)
- 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 IBM 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.

4.2 Wymagania w zakresie VPN dla stacji użytkownika

Aplikacje Archiwum SOWE, Archiwum WIRE, WIRE/RP, CCO oraz Portal SIRE, 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.

4.2.1 Wymagania sprzętowe

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

4.2.2 Wymagane oprogramowanie

- Oprogramowanie AppGate Client wersja 11.

4.2.3 Wymagania sieciowe

Każda stacja robocza użytkowników Archiwum SOWE, Archiwum WIRE, WIRE/RP, CCO oraz Portalu SIRE powinna posiadać skonfigurowane połączenie sieciowe do odpowiedniego serwera WWW OSP, wykorzystując połączenia sieciowe opisane w Rozdz. 3.

Adresy IP dla stacji roboczych użytkowników, stosowane w sieci WAN PSE S.A. przez Podmioty, przydziela Administrator Bezpieczeństwa OSP. Są one przydzielane w momencie rejestracji nowego Podmiotu.

4.3 Procedury

4.3.1 Procedura przyłączania i akceptacji systemów informatycznych Operatorów Rynku do systemów informatycznych OSP dla WIRE/UR i WIRE

4.3.2 Procedura przyłączania i akceptacji systemów informatycznych Elektrowni do systemów informatycznych OSP dla SOWE/EL i SOWE

Procedury określają 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.

4.4 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 systemami OSP jest szyfrowana przy użyciu TLS.
- Identyfikacja i Autoryzacja Elementów Systemu Operatora Rynku/Elektrowni i OSP – elementy będą jednoznacznie identyfikowane na następujących warstwach:
    - Aplikacji IBM MQ – wszystkie serwery będą jednoznacznie identyfikowane na podstawie certyfikatu elektronicznego zgodnego z normą X.509v 3 używanego w kanałach TLS IBM 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 TLS serwerów IBM MQ poprzez CCO tj. obsługę pozyskiwania, odnawiania i anulowania certyfikatów jest Administrator Certyfikatów – AC.
- Dla wszystkich styków odpowiedzialność ABOSP za bezpieczeństwo kończy się na routerach węzłowych WAN PSE.
- Operator Rynku wnioskujący o przyłączenie do systemu OSP wyznaczy osobę pełniącą funkcję Administratora Bezpieczeństwa Operatora Rynku/Elektrowni - ABOR.:
- 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".
- ABOR odpowiedzialny jest za:
    - Przekazywanie informacji niezbędnych do prawidłowego skonfigurowania konta w systemie VPN AppGate.
    - Zarządzanie certyfikatami dla systemów WIRE/UR / SOWE/EL do komunikacji TLS IBM 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/Elektrownie 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, OR lub EL 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.

5 WYMAGANIA TECHNICZNE

5.1 TLS

Protocol: Transport Layer Security (TLS)

Key Exchange: Rivest Shamir Adleman algorithm (RSA)

Authentication: Rivest Shamir Adleman algorithm (RSA)

Encryption: Advanced Encryption Standard with 128bit key in Galois/Counter mode (AES 128 GCM)

Hash: Secure Hash Algorithm 256 (SHA256)

5.2 VPN

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

5.3 Synchronizacja czasu

- Protokół synchronizacja czasu zgodny ze standardem NTP.

5.4 Routery dostępowe

Powinny zapewniać routing pakietów zgodnie z protokołami BGP i EIGRP, zarządzanie z wykorzystaniem protokołu SNMP w wersji minimum 2c oraz możliwość zdalnego dostępu poprzez protokół SSH

6 WYMAGANIA DLA SYSTEMU SZOP (SYSTEM ZDALNEGO ODCZYTU DANYCH)

6.1 Metody transmisji danych pomiarowych.

Transmisja danych licznikowych on-line z układów pomiarowych odbywa się z wykorzystaniem protokołu SCTM lub DLMS. Do komunikacji z obiektem udostępniającym dane do systemu może być użyta jedna z poniższych metod:

- Dedykowany moduł ethernetowy instalowany bezpośrednio w liczniku (dostęp do urządzenia poprzez sieć TCP/IP – tylko dla WAN)
- Udostępniony za pomocą konwertera RS/IP port RS232/RS485 (dostęp do urządzenia poprzez sieć TCP/IP – tylko dla WAN)
- Udostępniony za pomocą standardowego modemu port RS232/rs485 (dostęp do urządzenia poprzez dedykowaną sieć PSTN – numery telefoniczne wyniesione, zalecana minimalna prędkość i protokół transmisji – 9600Bd /V32)
- Dedykowane moduły PSTN instalowane bezpośrednio w liczniku (dostęp do urządzenia poprzez dedykowaną sieć PSTN – numery telefoniczne wyniesione, zalecana minimalna prędkość i protokół transmisji – 9600Bd /V32)
- Udostępniony za pomocą standardowego modemu port RS232/rs485 (dostęp do urządzenia poprzez publiczną sieć PSTN – standardowe numery telefoniczne , zalecana minimalna prędkość i protokół transmisji – 9600Bd /V32)
- Dedykowane moduły PSTN instalowane bezpośrednio w liczniku (dostęp do urządzenia poprzez dedykowaną sieć PSTN – numery telefoniczne wyniesione, zalecana minimalna prędkość i protokół transmisji – 9600Bd /V32)
- Udostępniony za pomocą modemu GSM port RS232/rs485 (dostęp do urządzenia poprzez publiczną sieć PSTN – komórkowe numery telefoniczne , zalecana minimalna prędkość i protokół transmisji – 9600Bd /V110)
- Dedykowany moduł GSM instalowany bezpośrednio w liczniku (dostęp do urządzenia poprzez publiczną sieć PSTN – komórkowe numery telefoniczne , zalecana minimalna prędkość i protokół transmisji – 9600Bd /V110)

6.2 Rejestracja nowych pomiarów

Rejestracja nowych pomiarów w systemie SZOP wymaga uzgodnień miedzy Podmiotem a OSP i przygotowania przez Podmiot dokumentacji układu pomiarowego, podlegającej weryfikacji przez OSP.

Akceptacja dokumentacji równoznaczna jest ze zgoda OSP na dodanie nowych pomiarów do systemu SZOP.

Zgoda wysyłana jest w postaci Decyzji o zestawieniu transmisji danych z urządzeń pomiarowych do Systemu Zdalnego Odczytu Pomiarów OSP zawierającej adresy IP / numery telefonów wykorzystywanych dla urządzeń pomiarowych na potrzeby zestawienia transmisji.

Warunkiem dodania nowych pomiarów do systemu SZOP jest odbiór układu pomiarowego potwierdzony protokołem.