TEL-STER Sp. z o.o.
ul. Stefana Stefańskiego 23
62-002 Suchy Las
Tel. +48 61 628 97 50
Fax. +48 61 639 37 11

TelCOMM 6.0

Sąd Rejonowy Poznań – Nowe Miasto i Wilda w Poznaniu, VIII Wydział Gospodarczy Krajowego Rejestru Sądowego
KRS: 0000178284; NIP: 781-17-38-677; REGON: 634530767
Kapitał Zakładowy: 560 000 zł

TEL-STER Sp. z o.o.
ul. Stefana Stefańskiego 23
62-002 Suchy Las
Tel. +48 61 628 97 50
Fax. +48 61 639 37 11

Historia zmian dokumentu:

Data	Wersja dokumentu	Autor	Opis zmiany
2019.04.17	4.0	Michał Siatkowski	Wersja 4.0
2019.05.30	4.0	Elżbieta Sobkowiak	Dostosowanie formy do wymogów ISO
2019.12.18	4.2	Michał Siatkowski	Dodatkowe funkcjonalności
2020.07.07	4.5	Michał Siatkowski	Jeden P-Mode dla obu kierunków
2020.12.14	4.6	Michał Siatkowski	Aktualizacje bezpieczeństwa
2022.05.17	5.0	Michał Siatkowski	Implementacja AS2
2024.01.30	5.1	Michał Siatkowski	Aktualizacje dot. interfejsu do współpracy z programem zewnętrznym
2025.10.14	6.0	Michał Siatkowski, Elżbieta Sobkowiak	Implementacja profilów AS4 BDEW i ENTSOG 4.0, koniec wsparcia AS2

TEL-STER Sp. z o.o.
ul. Stefana Stefańskiego 23
62-002 Suchy Las
Tel. +48 61 628 97 50
Fax. +48 61 639 37 11

Spis treści

Specyfikacja

- Profile AS4: ENTSOG 3.6, ENTSOG 4.0, BDEW
- Wzorce komunikacji (MEP) AS4:
    - Inicjowanie i odpowiadanie: One-Way/Push, Two-Way/Push-Pull
    - Tylko inicjowanie: One-Way/Pull i Two-Way/Sync
- Algorytmy AS4:
    - Funkcje skrótu dla podpisu (hash): sha256, sha384, sha512
    - Podpis cyfrowy:
        - certyfikat RSA: rsa-sha256, rsa-sha384, rsa-sha512
        - certyfikat ECC: ecdsa-sha256, ecdsa-sha384, ecdsa-sha512
        - certyfikat Ed25519: eddsa-ed25519
    - Szyfrowanie danych:
        - aes128-cbc, aes192-cbc, aes256-cbc
        - aes128-gcm, aes192-gcm, aes256-gcm
    - Szyfrowanie klucza:
        - [transport klucza] certyfikat RSA: rsa-oaep-mgf1p, rsa-oaep
            - MGF: mgf1sha1, mgf1sha256, mgf1sha384, mgf1sha512
            - Funkcje skrótu (hash): sha1, sha256, sha384, sha512
        - [uzgadnianie klucza] certyfikat ECC: ECDH-ES, certyfikat X25519: x25519
            - KDF: ConcatKDF, hkdf
            - KW: kw-aes128, kw-aes192, kw-aes256
            - HMAC: sha1, sha256, sha384, sha512
    - Kompresja: gzip
- [ReplyPattern]: Response (synchroniczność), Callback (asynchroniczność)
- [SecurityTokenReference]: BinarySecurityToken X509v3, BinarySecurityToken X509PKIPathv1, IssuerAndSerialNumber, SubjectKeyIdentifier
- [ebCore Agreement Update]: tak, dla certyfikatów
- Wiele załączników w komunikacie: tak
- Jeden [P-Mode] dla obu kierunków (gdy obaj partnerzy używają tego samego certyfikatu do podpisu i szyfrowania): tak

- Walidacja certyfikatów: OCSP/CRL (opcjonalnie)
- Certyfikat TLS serwera i klienta: tak (opcjonalnie)
- Architektura: Microsoft Windows Server, IIS, .NET Framework 4.8, HTTPS, TLS 1.2 i 1.3
- Baza danych: SQLite, Oracle
- Interakcja z programem: przeglądarka internetowa dla użytkowników, usługa sieciowa (web service) dla programów zewnętrznych
- Integracja z Microsoft Defender: tak (opcjonalnie)
- Język interfejsu użytkownika: polski, angielski

Wprowadzenie

Oprogramowanie TelCOMM jest narzędziem umożliwiającym wymianę dokumentów typu B2B za pomocą protokołu AS4.

Protokół AS4 (Applicability Statement 4) to standard opisujący bezpieczne i niezawodne przesyłanie plików przez publiczną sieć Internet. Protokół ten bazuje na powszechnie znanych i sprawdzonych rozwiązaniach, takich jak protokoły HTTP, TLS, SOAP oraz usługach sieciowych (web service). Reprezentuje otwarty standard wymiany danych typu B2B opisany w specyfikacji OASIS ebMS 3.0. Elementami odpowiedzialnymi za bezpieczeństwo i wiarygodność przesyłanych danych są podpisy cyfrowe oraz mechanizmy szyfrujące (WS-security).

Architektura

Oprogramowanie TelCOMM jest rozwiązaniem adresowanym dla środowiska MS Windows Server, bazującym na podsystemie IIS oraz .NET Framework w wersji co najmniej 4.8. Program może być udostępniany jedynie poprzez protokół HTTPS, a wersja używanego protokołu TLS podczas wysyłania komunikatów to 1.2 lub 1.3. Korzysta on z wbudowanej bazy danych **SQLite** lub ma możliwość korzystania z bazy danych **Oracle**. Program składa się z trzech komponentów:

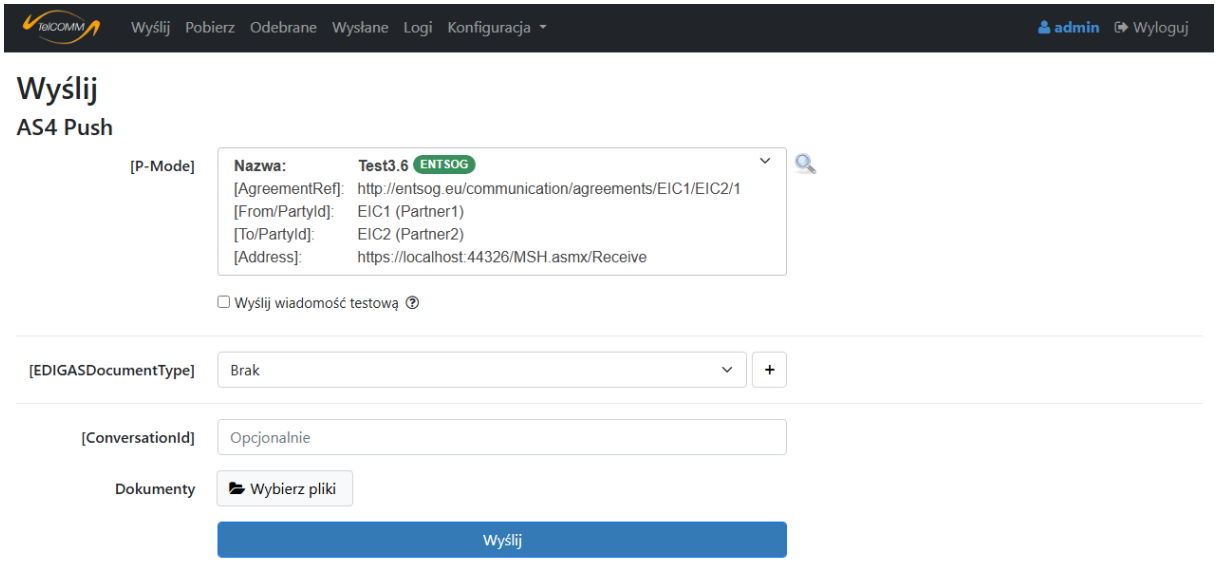
- interfejsu webowego dostępnego przez przeglądarkę internetową, umożliwiającego konfigurację i interaktywną wymianę dokumentów,
- usługi sieciowej /WebServices/Gateway.asmx umożliwiającej wymianę dokumentów z poziomu programu zewnętrznego,
- usługi sieciowej /MSH.asmx/Receive umożliwiającej odbiór dokumentów od partnerów.

Interfejs webowy

Pierwszym ekranem w TelCOMM jest ekran logowania. W programie istnieje nieusuwalny użytkownik, dla którego początkowy login i hasło to „admin”. Kliknięcie w ikonę TelCOMM w lewym górnym rogu programu spowoduje wyświetlenie numeru wersji.

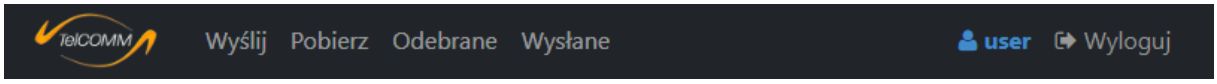
Rysunek 1. Ekran logowania

Po zalogowaniu pojawia się główny ekran „Wyślij”.



Rysunek 2. Pierwszy ekran po zalogowaniu

U góry ekranu znajduje się pasek nawigacyjny wspólny dla ekranów po zalogowaniu. Po ikonie programu znajduje się hiperłącze do ekranu „Wyślij” oraz „Pobierz”, a następnie do pozostałych ekranów systemu. Na końcu znajduje się nazwa zalogowanego użytkownika wraz z opcją wylogowania. Pasek ten różni się w zależności od tego czy zalogowany użytkownik jest administratorem. Zwykły użytkownik ma dostęp do ekranów „Wyślij”, „Pobierz”, „Odebrane” i „Wysłane”. Poniżej zrzut ekranu paska nawigacyjnego dla zwykłego użytkownika.



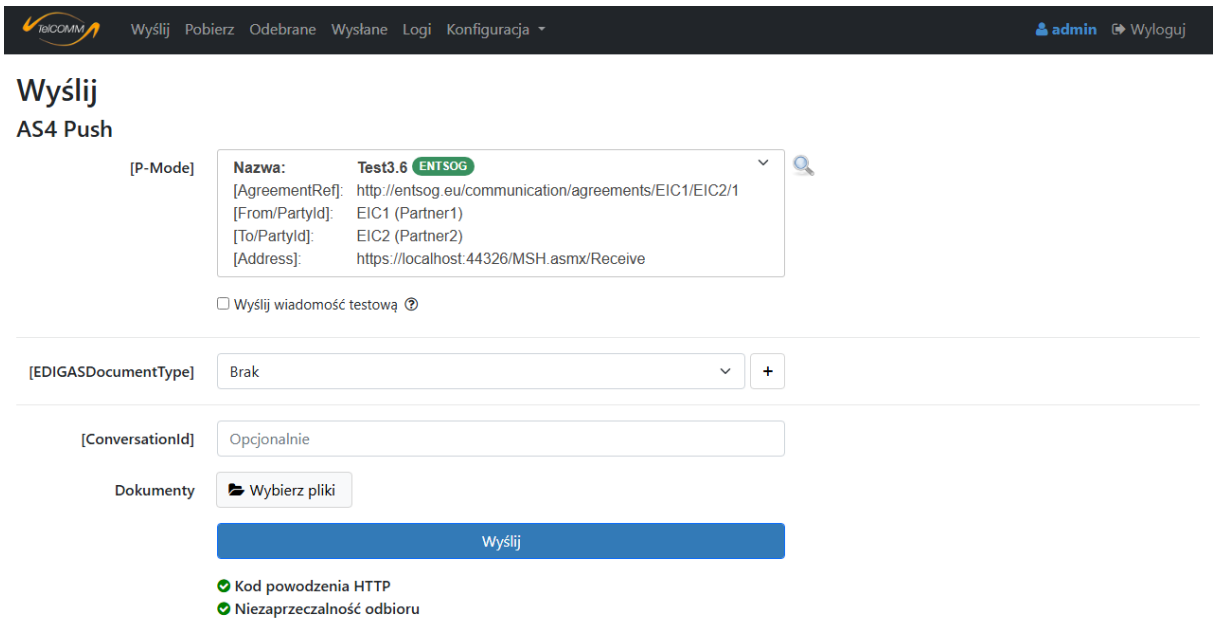
Rysunek 3. Pasek nawigacyjny zwykłego użytkownika

Ekran „Wyślij”

Służy do wysyłania plików za pomocą wzorca komunikacji **One-Way/Push**. Polega on na wysłaniu wiadomości od jednego partnera do drugiego. W celu wysłania komunikatu AS4 należy:

- wybrać wcześniej zdefiniowany [P-Mode] ([Processing mode]), w którym zawarte są ustawienia dotyczące połączenia komunikacyjnego między partnerami,
- w polu „Dokumenty” wybrać plik lub pliki, które mają zostać wysłane.

Kliknięcie przycisku „Wyślij” inicjuje komunikację - dokumenty zostają wysłane zgodnie z protokołem komunikacyjnym AS4. W przypadku braku błędów wysłania wiadomości pojawia się kod powodzenia HTTP. W zależności od ustawień w konfiguracji połączenia między partnerami, może nastąpić również analiza odpowiedzi od odbiorcy pod kątem niezaprzeczalności odbioru (Non Repudiation of Receipt) lub potwierdzenia odbioru (Reception Awareness), gdy odpowiedź przesyłana jest synchronicznie (Response) – możliwe jest również asynchroniczne odebranie odpowiedzi w osobnym komunikacie (Callback).



Rysunek 4. Ekran „Wyślij”– po analizie odpowiedzi

W przypadku otrzymania w odpowiedzi błędów komunikacji AS4 zostaną one wyświetlone na dole ekranu i zapisane w celu późniejszego podglądu na ekranie „Logi”.

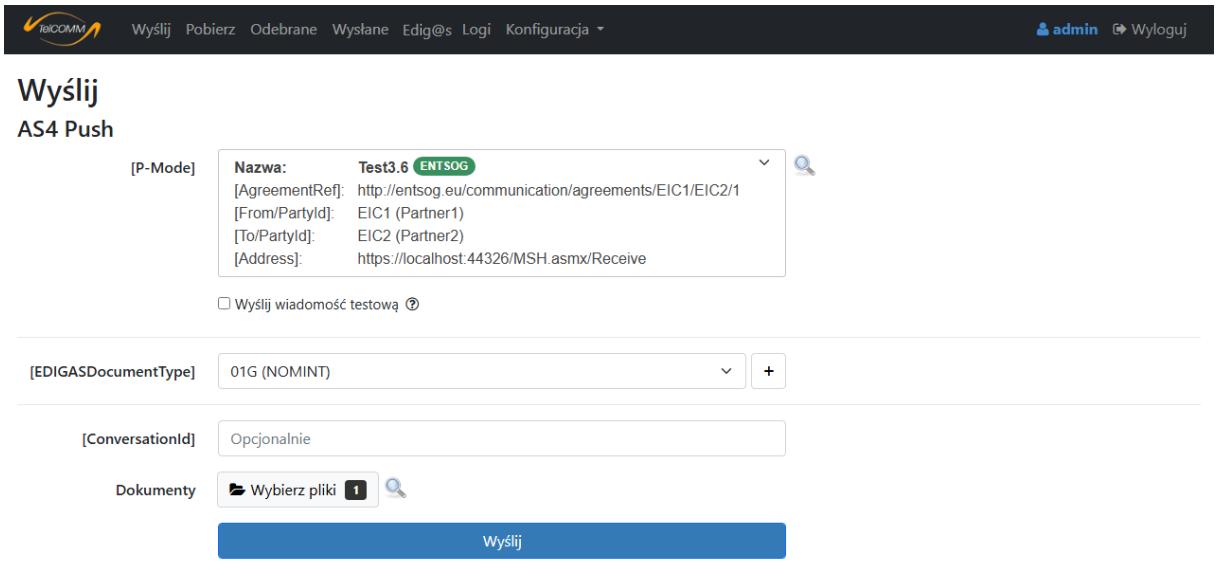
Przydatnymi opcjami ekranu wysyłania są:

- możliwość wysłania wiadomości z testowymi parametrami komunikacji AS4 w celu przetestowania połączenia między partnerami – należy zaznaczyć opcję „Wyślij wiadomość testową”,
- w sytuacji wysyłania wielu plików, możliwość wysłania ich pojedynczo w osobnych wiadomościach – opcja pojawi się po wybraniu więcej niż jednego pliku.

W przypadku włączenia w konfiguracji programu opcji „Wysyłanie dokumentów Edig@s” dodatkowymi wariantami dla profilu AS4 ENTSOG będzie:

- możliwość wypełnienia pola [EDIGASDocumentType] lub pobrania go z załączonych plików Edig@s – opcja „Pobierz z załączonych dokumentów” w rozwijanej liście,
- kryjące się pod przyciskiem „+” dodatkowe pola „Identyfikator transakcji” i „Opis transakcji” służące do opisania wysłanych nominacji jako pojedynczej transakcji zawierającej jeden lub wiele plików. Umożliwia to opcjonalne grupowanie nominacji na ekranie „Edig@s”.

W przypadku wysyłania plików niebędących dokumentami Edig@s w polu [EDIGASDocumentType] należy zostawić opcję „Brak”. Przykład ekranu w trybie „Wysyłanie dokumentów Edig@s” przedstawia poniższy rysunek.

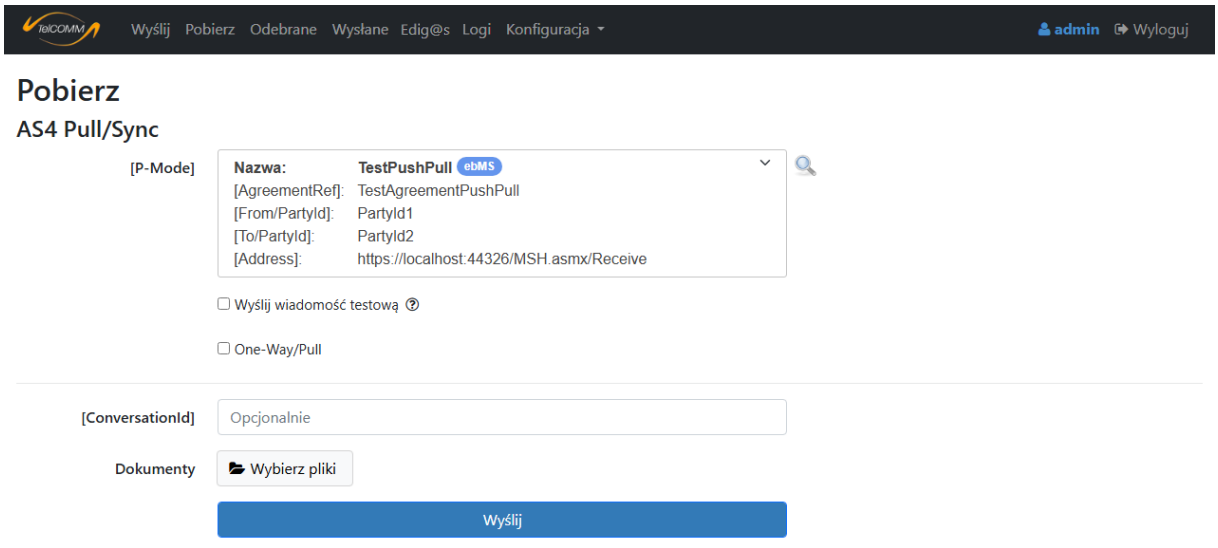


Rysunek 5. Ekran „Wyślij” w trybie "Wysyłanie dokumentów Edig@s"

Ekran „Pobierz”

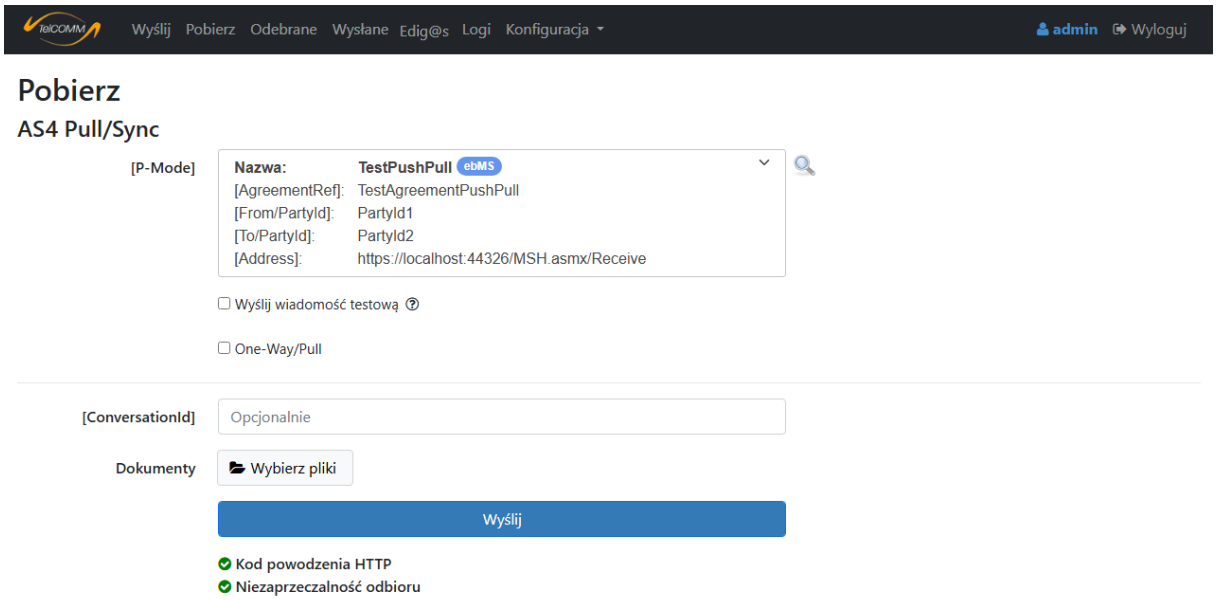
Służy do pobierania danych od partnera z użyciem wzorca komunikacji **Two-Way/Push-Pull**, **Two-Way/Sync** lub **One-Way/Pull**. Two-Way/Push-Pull składa się z dwóch etapów: wysyłany jest dokument z żądaniem określającym jakie dane partner ma udostępnić, a w drugim etapie dane te są w sposób automatyczny pobierane. Two-Way/Sync wykonuje to samo ale w jednym etapie tzn. dane są od razu zwracane w odpowiedzi pierwszego żądania. One-Way/Pull obejmuje tylko drugi etap – utworzenie żądania Pull i dodanie go do puli żądań realizowanych automatycznie. W celu pobrania danych AS4 należy:

- wybrać wcześniej zdefiniowany [P-Mode] ([Processing mode]), w którym zawarte są ustawienia dotyczące połączenia komunikacyjnego między partnerami,
- w polu „Dokumenty” wybrać plik lub pliki zawierające żądanie o udostępnienie konkretnych danych. Struktura pliku jest ustalana między partnerami.



Rysunek 6. Ekran „Pobierz”

Kliknięcie przycisku „Wyślij” inicjuje pierwszą fazę komunikacji – plik z żądaniem zostaje wysłany zgodnie z protokołem komunikacyjnym AS4 oraz następuje analiza odpowiedzi od odbiorcy.



Rysunek 7. Ekran „Pobierz”– po analizie odpowiedzi

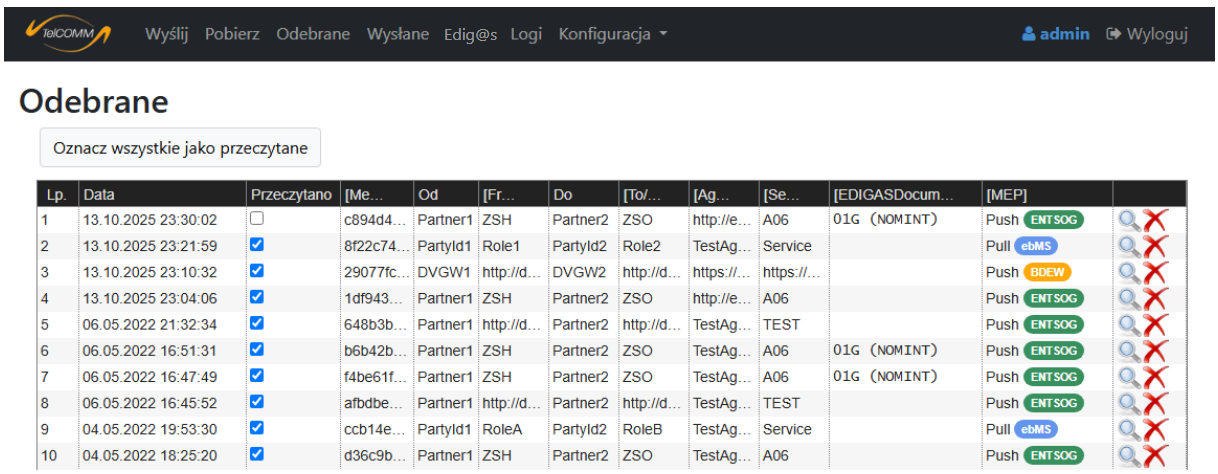
W przypadku otrzymania w odpowiedzi błędów komunikacji AS4 zostaną one wyświetlone na dole ekranu pobierania i zapisane w celu późniejszego podglądu na ekranie „Logi”.

Gdy będzie zaznaczona opcja „One-Way/Pull” wykonane zostanie tylko pobranie danych bez uprzedniego wysłania żądania. Wtedy nie ma możliwości dodania dokumentów.

Dodatkową opcją ekranu pobierania jest, w przypadku wysyłania wielu żądań, możliwość wysłania ich pojedynczo w osobnych wiadomościach – opcja pojawi się po wybraniu więcej niż jednego pliku.

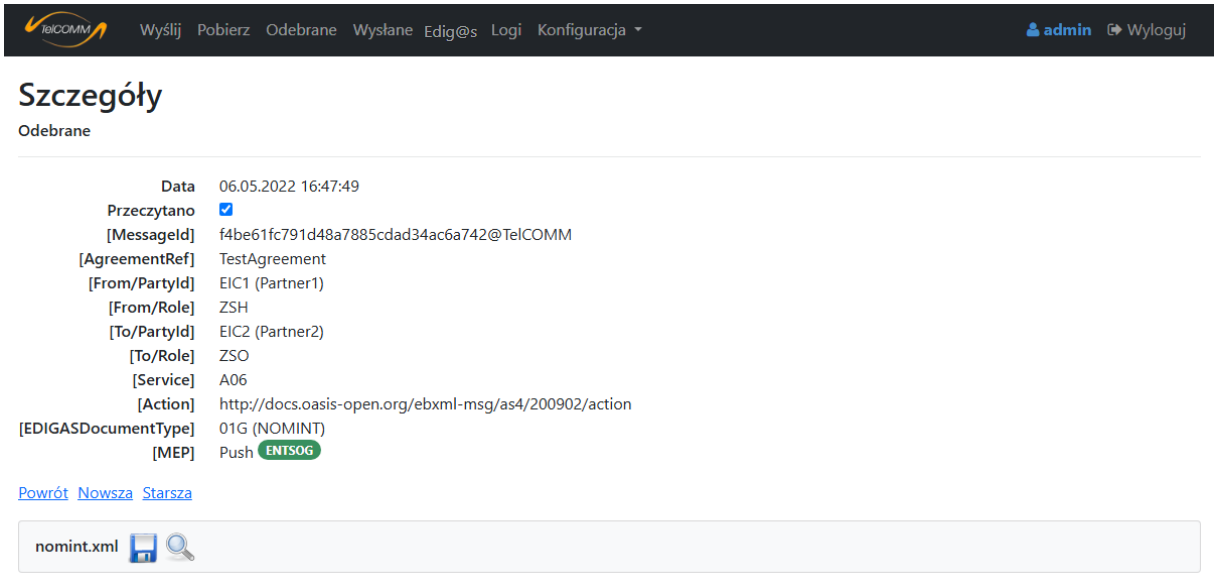
Ekran „Odebrane”

Ekran „Odebrane” spełnia rolę skrzynki odbiorczej programu. Dla każdej odebranej wiadomości istnieje możliwość nadania jej statusu przeczytanej/nieprzeczytanej – funkcjonalność ta ma przede wszystkim znaczenie przy korzystaniu z programu przez funkcję usługi sieciowej (web service), gdzie pobierane są wszystkie nieprzeczytane pozycje. Można również oznaczyć wszystkie pozycje jako przeczytane za pomocą przycisku na górze ekranu.



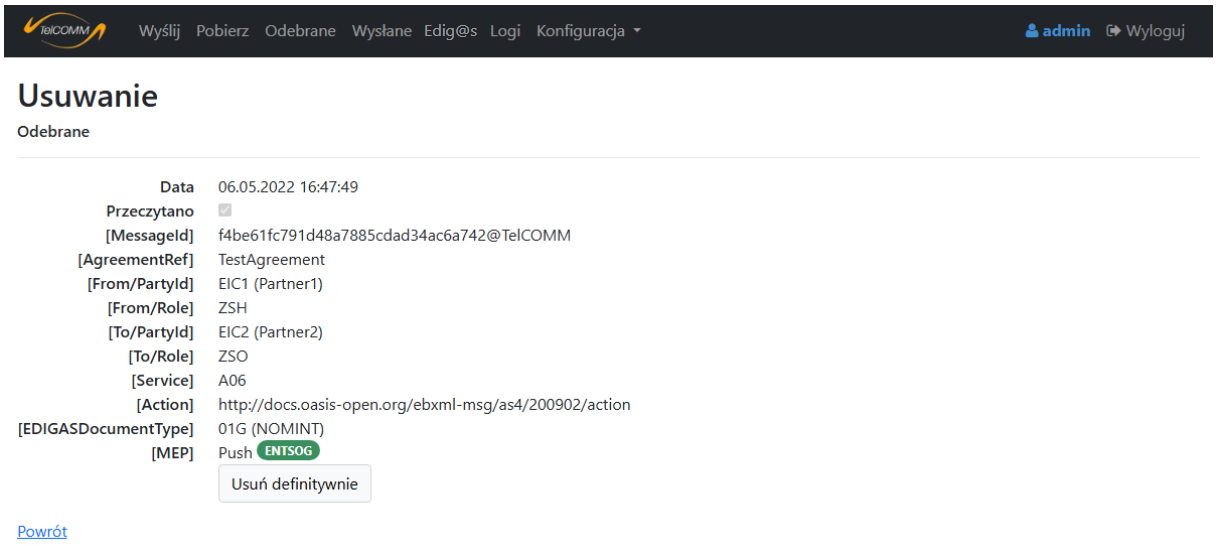
Rysunek 8. Ekran „Odebrane”

W obrębie programu użyto zestawu ikonek  , które odpowiednio służą do dodawania, podglądu szczegółów, edycji i usuwania danego elementu. Aby wyświetlić przesłane pliki w danym komunikacie AS4 należy przejść do szczegółów komunikatu. Można również przełączać się między pozycjami bezpośrednio na ekranie szczegółów korzystając z hiperłączy „Nowsza” i „Starsza”.



Rysunek 9. Ekran „Odebrane” – szczegóły komunikatu

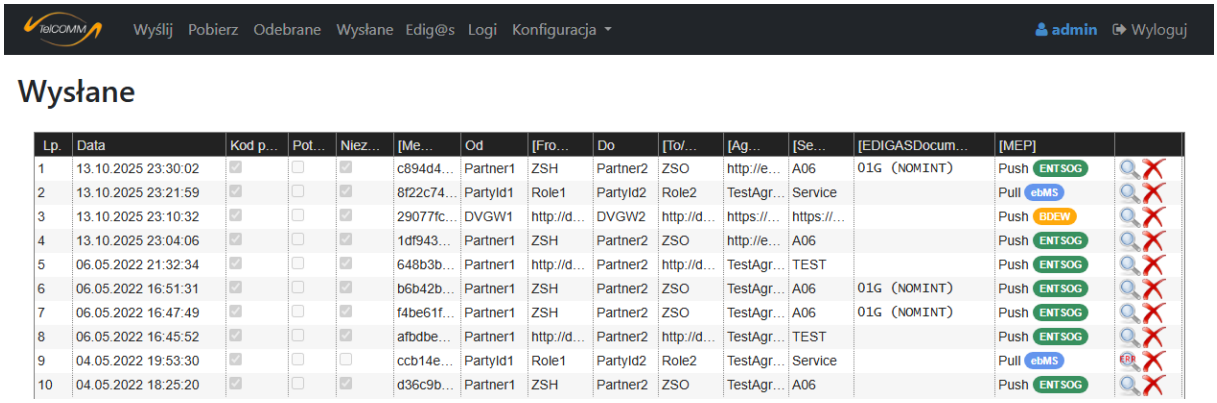
Na ekranie „Odebrane” istnieje również opcja usunięcia wiadomości. Kliknięcie przycisku powoduje wyświetlenie ekranu usuwania danego komunikatu i dopiero na nim należy potwierdzić jej usunięcie przyciskiem „Usuń definitywnie”, aby odpowiedni wpis z bazy danych został trwale usunięty. Taka procedura usuwania, polegająca na potwierdzeniu na osobnym ekranie, jest stosowana w obrębie całego programu.



Rysunek 10. Ekran „Odebrane” – usuwanie wiadomości

Ekran „Wysłane”

Ekran „Wysłane” wyświetla wszystkie komunikaty, które zostały wysłane, a jego struktura jest analogiczna do ekranu „Odebrane”, z tą różnicą, że zamiast opcji nadania statusu wiadomości przeczytanej/nieprzeczytanej znajdują się informacje dotyczące wyniku analizy odpowiedzi od odbiorcy, opisane wcześniej. Również w przypadku wysłania wiadomości z błędami pojawia się nieco zmodyfikowana ikona podglądu szczegółów wiadomości widoczna na poniższym rysunku.



Rysunek 11. Ekran „Wysłane”

Ekran „Edig@s”

Ekran „Edig@s” dostępny jest tylko przy zaznaczonej opcji „Wysyłanie dokumentów Edig@s” w konfiguracji programu. Pozwala on przeglądać wysłane oraz odebrane dokumenty Edig@s na zasadzie parowania. Funkcja parowania pozwala powiązać dokument NOMINT z ACKNOW i NOMRES oraz REQEST z REQRES w sposób, jaki przedstawiono na poniższym rysunku. Dokumenty odpowiedzi wyróżnione są kolorem w zależności od tego czy mają status zatwierdzenia (kolor zielony) czy odrzucenia (czerwony). Dokumenty można posortować według informacji zawartych w pliku (Identyfikator i nr Umowy). Przyciski „Godzinowo”, „Dobowo” i „Transakcyjnie” pozwalają pogrupować dokumenty wg. godziny, daty lub według „Identyfikatora” i „Opisu Transakcji” (jeżeli podano podczas wysłania). Przycisk „Rozwiń wszystkie” pozwala pokazać na ekranie wszystkie dokumenty, natomiast „Zwiń wszystkie” ukrywa dokumenty, dając możliwość wyświetlenia dokumentów tylko z wybranej grupy. Domyślnie nie wszystkie kolumny są widoczne na ekranie - opcja „Pokaż/ukryj kolumny” pozwala na zarządzanie widocznością kolumn. Kliknięcie w przycisk pozwala zapisać dokument na komputerze, przycisk pozwala podejrzeć zawartość pliku w karcie przeglądarki, a przycisk to hiperłącze do ekranu szczegółów wiadomości, w której został przesłany dany dokument.

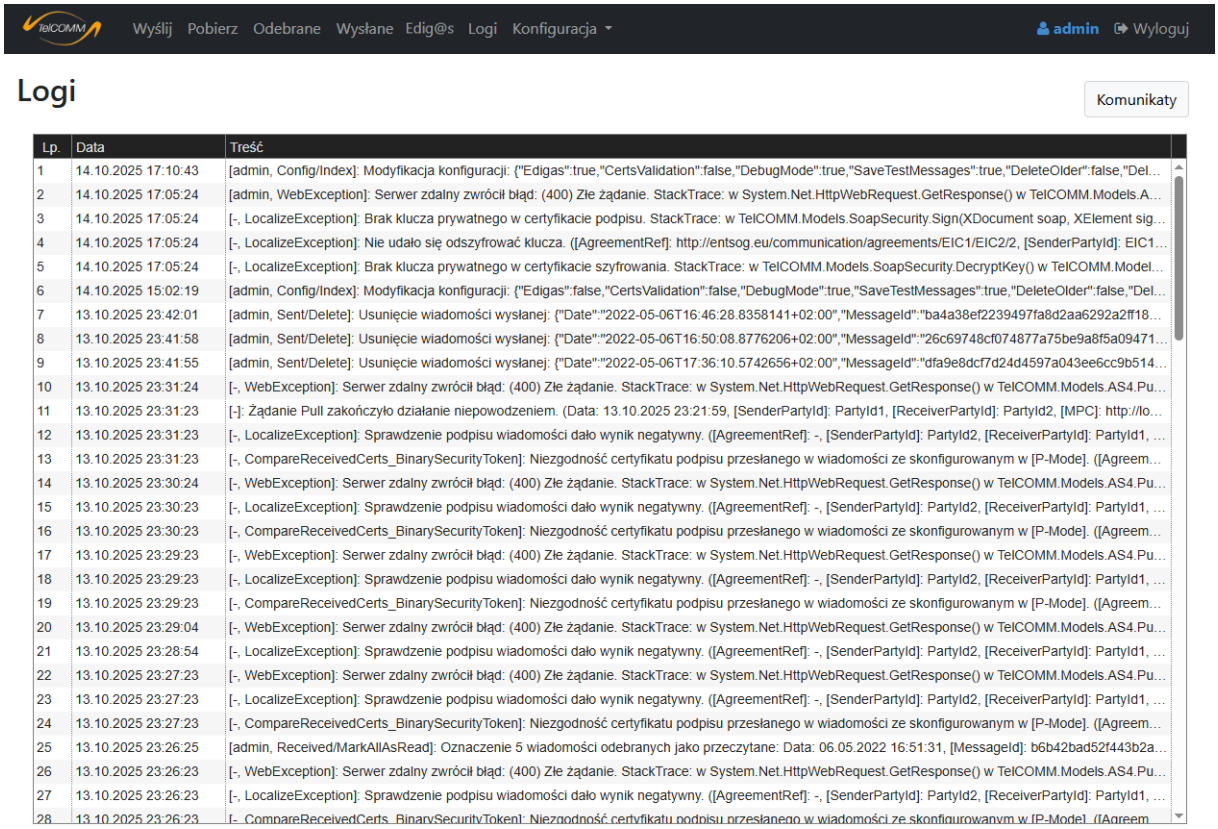
TEL-STER Sp. z o.o.
ul. Stefana Stefańskiego 23
62-002 Suchy Las
Tel. +48 61 628 97 50
Fax. +48 61 639 37 11

Rysunek 12. Ekran „Edig@s"

Ekran „Logi"

Kolejne ekrany dostępne są jedynie dla administratora. Ekran „Logi" zawiera błędy komunikacji AS4 oraz wybrane informacje na temat działań użytkowników. Dwukrotne kliknięcie w kolumnie „Treść" pozwala wyświetlić pełną treść komunikatu.

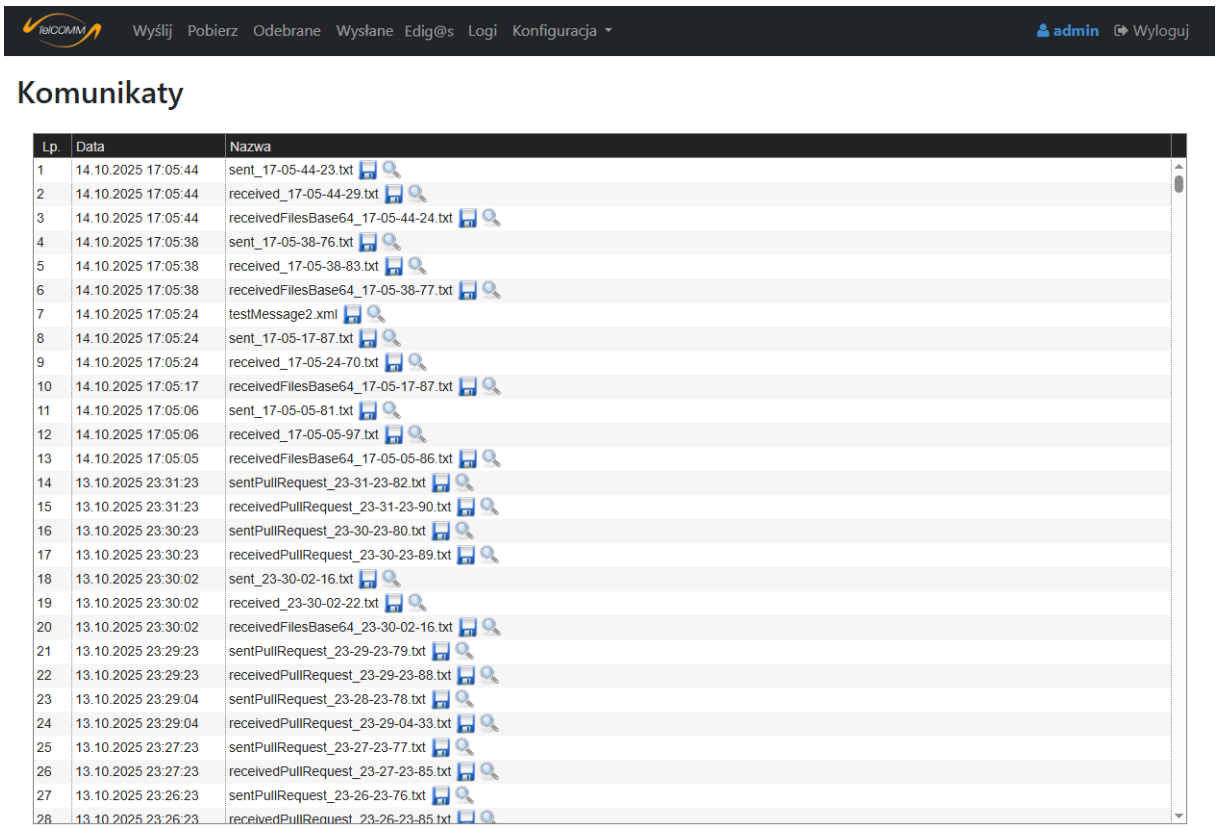
TEL-STER Sp. z o.o.
ul. Stefana Stefańskiego 23
62-002 Suchy Las
Tel. +48 61 628 97 50
Fax. +48 61 639 37 11



Lp.	Data	Treść
1	14.10.2025 17:10:43	[admin, Config/Index]: Modyfikacja konfiguracji: {"Edigas":true,"CertsValidation":false,"DebugMode":true,"SaveTestMessages":true,"DeleteOlder":false,"Del…
2	14.10.2025 17:05:24	[admin, WebException]: Serwer zdalny zwrócił błąd: (400) Złe żądanie. StackTrace: w System.Net.HttpWebRequest.GetResponse() w TelCOMM.Models.A…
3	14.10.2025 17:05:24	[-, LocalizeException]: Brak klucza prywatnego w certyfikacie podpisu. StackTrace: w TelCOMM.Models.SoapSecurity.Sign(XDocument soap, XElement sig…
4	14.10.2025 17:05:24	[-, LocalizeException]: Nie udało się odszyfrować klucza. ([AgreementRef]: http://entsog.eu/communication/agreements/EIC1/EIC2/2, [SenderPartyId]: EIC1…
5	14.10.2025 17:05:24	[-, LocalizeException]: Brak klucza prywatnego w certyfikacie szyfrowania. StackTrace: w TelCOMM.Models.SoapSecurity.DecryptKey() w TelCOMM.Model…
6	14.10.2025 15:02:19	[admin, Config/Index]: Modyfikacja konfiguracji: {"Edigas":false,"CertsValidation":false,"DebugMode":true,"SaveTestMessages":true,"DeleteOlder":false,"Del…
7	13.10.2025 23:42:01	[admin, Sent/Delete]: Usunięcie wiadomości wysłanej: {"Date":"2022-05-06T16:46:28.8358141+02:00","MessageId":"ba4a38ef2239497fa8d2aa6292a2ff18…
8	13.10.2025 23:41:58	[admin, Sent/Delete]: Usunięcie wiadomości wysłanej: {"Date":"2022-05-06T16:50:08.8776206+02:00","MessageId":"26c69748cf074877a75be9a8f5a09471…
9	13.10.2025 23:41:55	[admin, Sent/Delete]: Usunięcie wiadomości wysłanej: {"Date":"2022-05-06T17:36:10.5742656+02:00","MessageId":"dfa9e8dcf7d24d4597a043ee6cc9b514…
10	13.10.2025 23:31:24	[-, WebException]: Serwer zdalny zwrócił błąd: (400) Złe żądanie. StackTrace: w System.Net.HttpWebRequest.GetResponse() w TelCOMM.Models.AS4.Pu…
11	13.10.2025 23:31:23	[-]: Żądanie Pull zakończyło działanie niepowodzeniem. (Data: 13.10.2025 23:21:59, [SenderPartyId]: PartyId1, [ReceiverPartyId]: PartyId2, [MPC]: http://lo…
12	13.10.2025 23:31:23	[-, LocalizeException]: Sprawdzenie podpisu wiadomości dało wynik negatywny. ([AgreementRef]: -, [SenderPartyId]: PartyId2, [ReceiverPartyId]: PartyId1, …
13	13.10.2025 23:31:23	[-, CompareReceivedCerts_BinarySecurityToken]: Niezgodność certyfikatu podpisu przesłanego w wiadomości ze skonfigurowanym w [P-Mode]. ([Agreem…
14	13.10.2025 23:30:24	[-, WebException]: Serwer zdalny zwrócił błąd: (400) Złe żądanie. StackTrace: w System.Net.HttpWebRequest.GetResponse() w TelCOMM.Models.AS4.Pu…
15	13.10.2025 23:30:23	[-, LocalizeException]: Sprawdzenie podpisu wiadomości dało wynik negatywny. ([AgreementRef]: -, [SenderPartyId]: PartyId2, [ReceiverPartyId]: PartyId1, …
16	13.10.2025 23:30:23	[-, CompareReceivedCerts_BinarySecurityToken]: Niezgodność certyfikatu podpisu przesłanego w wiadomości ze skonfigurowanym w [P-Mode]. ([Agreem…
17	13.10.2025 23:29:23	[-, WebException]: Serwer zdalny zwrócił błąd: (400) Złe żądanie. StackTrace: w System.Net.HttpWebRequest.GetResponse() w TelCOMM.Models.AS4.Pu…
18	13.10.2025 23:29:23	[-, LocalizeException]: Sprawdzenie podpisu wiadomości dało wynik negatywny. ([AgreementRef]: -, [SenderPartyId]: PartyId2, [ReceiverPartyId]: PartyId1, …
19	13.10.2025 23:29:23	[-, CompareReceivedCerts_BinarySecurityToken]: Niezgodność certyfikatu podpisu przesłanego w wiadomości ze skonfigurowanym w [P-Mode]. ([Agreem…
20	13.10.2025 23:29:04	[-, WebException]: Serwer zdalny zwrócił błąd: (400) Złe żądanie. StackTrace: w System.Net.HttpWebRequest.GetResponse() w TelCOMM.Models.AS4.Pu…
21	13.10.2025 23:28:54	[-, LocalizeException]: Sprawdzenie podpisu wiadomości dało wynik negatywny. ([AgreementRef]: -, [SenderPartyId]: PartyId2, [ReceiverPartyId]: PartyId1, …
22	13.10.2025 23:27:23	[-, WebException]: Serwer zdalny zwrócił błąd: (400) Złe żądanie. StackTrace: w System.Net.HttpWebRequest.GetResponse() w TelCOMM.Models.AS4.Pu…
23	13.10.2025 23:27:23	[-, LocalizeException]: Sprawdzenie podpisu wiadomości dało wynik negatywny. ([AgreementRef]: -, [SenderPartyId]: PartyId2, [ReceiverPartyId]: PartyId1, …
24	13.10.2025 23:27:23	[-, CompareReceivedCerts_BinarySecurityToken]: Niezgodność certyfikatu podpisu przesłanego w wiadomości ze skonfigurowanym w [P-Mode]. ([Agreem…
25	13.10.2025 23:26:25	[admin, Received/MarkAllAsRead]: Oznaczenie 5 wiadomości odebranych jako przeczytane: Data: 06.05.2022 16:51:31, [MessageId]: b6b42bad52f443b2a…
26	13.10.2025 23:26:23	[-, WebException]: Serwer zdalny zwrócił błąd: (400) Złe żądanie. StackTrace: w System.Net.HttpWebRequest.GetResponse() w TelCOMM.Models.AS4.Pu…
27	13.10.2025 23:26:23	[-, LocalizeException]: Sprawdzenie podpisu wiadomości dało wynik negatywny. ([AgreementRef]: -, [SenderPartyId]: PartyId2, [ReceiverPartyId]: PartyId1, …
28	13.10.2025 23:26:23	[-, CompareReceivedCerts_BinarySecurityToken]: Niezgodność certyfikatu podpisu przesłanego w wiadomości ze skonfigurowanym w [P-Mode]. ([Agreem…

Rysunek 13. Ekran „Logi”

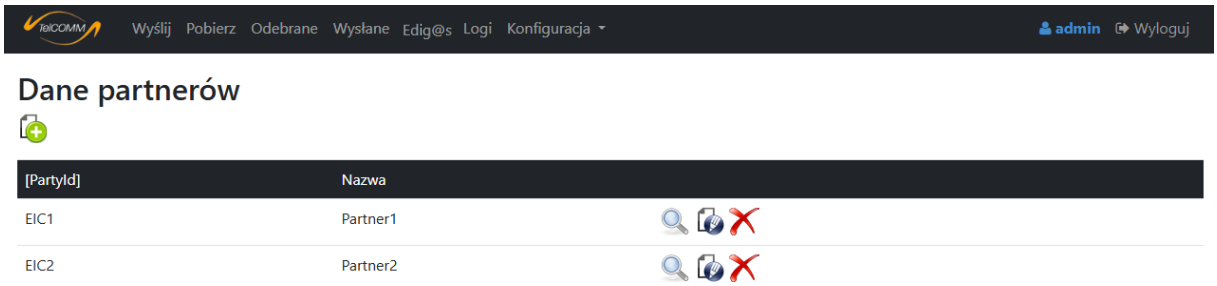
Z ekranu „Logi” można przejść na dodatkowy ekran „Komunikaty”, na którym istnieje możliwość podejrzenia całych żądań i odpowiedzi HTTP, które były wysyłane i odbierane przez program. Ekran służy szczegółowej analizie surowych komunikatów AS4.



Rysunek 14. Ekran „Komunikaty”

Ekran „Partnerzy”

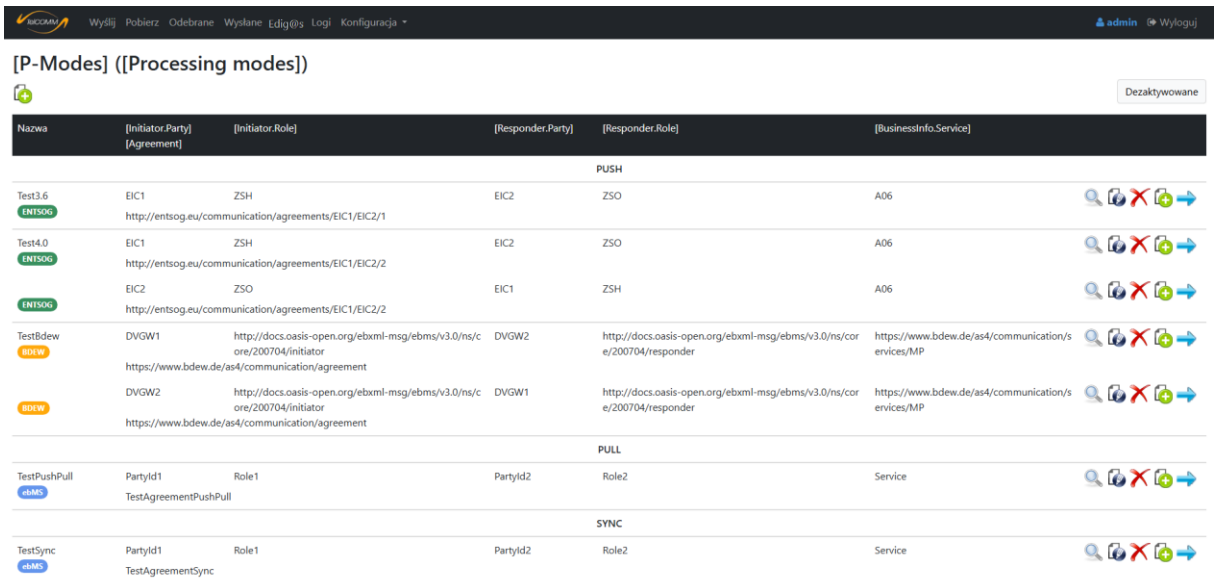
Na ekranie „Konfiguracja->Partnerzy” istnieje możliwość powiązania wartości [PartyId] z przyjazną nazwą, która będzie wyświetlana na ekranach programu zamiast identyfikatora partnera. W komunikacji Edig@s dla AS4 identyfikatorem tym jest kod EIC.



Rysunek 15. Ekran „Partnerzy”

Ekran „[P-Modes]”

Ekran „Konfiguracja->[P-Modes]” ([Processing modes]) służy definiowaniu wszystkich informacji związanych z połączeniem między partnerami komunikacji. Dane te są ściśle związane z protokołem AS4 i jest to kluczowy ekran konfiguracyjny systemu. [P-Modes] podzielone są na trzy grupy: PUSH – dotyczy wysyłania, PULL i SYNC – dotyczą pobierania. Istnieje możliwość przejścia na ekran [P-Modes] wyłączonych z użycia klikając przycisk Dezaktywowane ([P-Mode] na ekranie usuwania można trwale usunąć z bazy danych lub jedynie dezaktywować, zostawiając sobie ewentualną możliwością późniejszego przywrócenia do aktywnych).



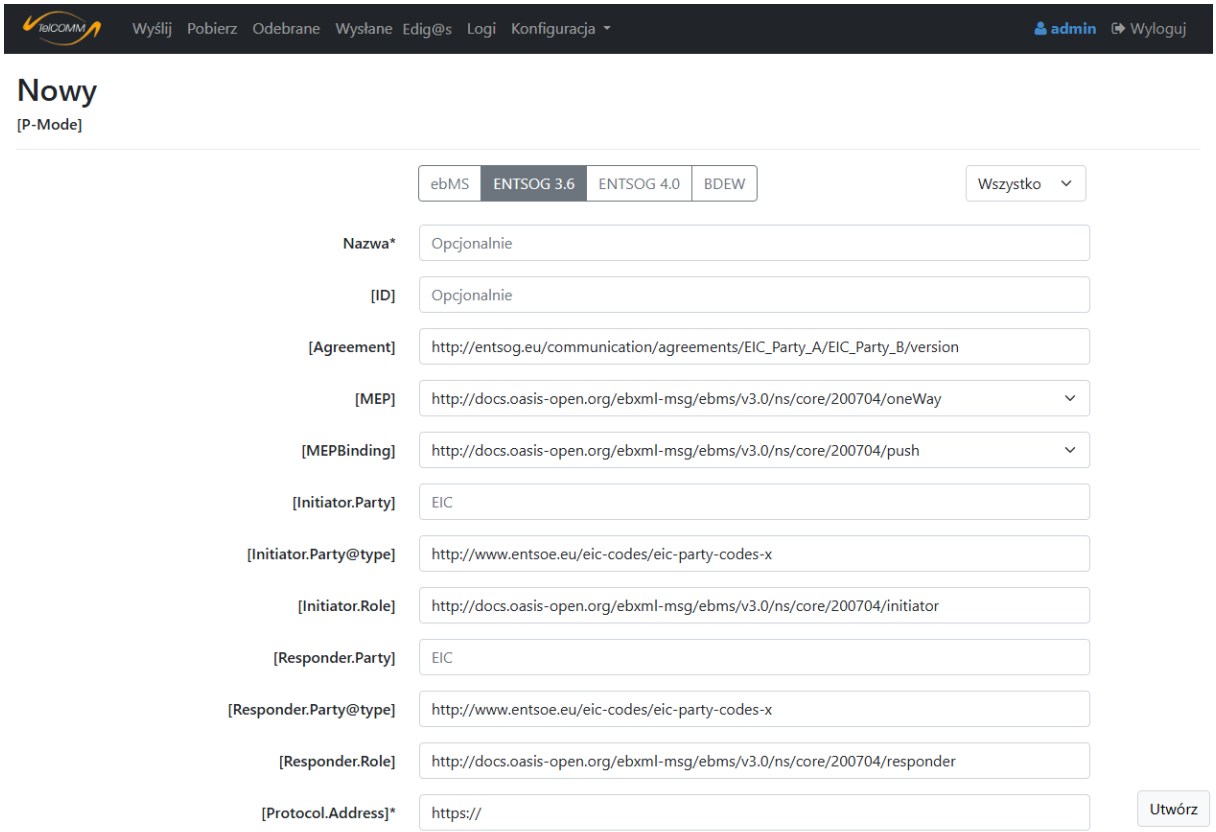
Rysunek 16. Ekran „[P-Modes]"

Jedną z informacji zawartych w [P-Mode] są certyfikaty partnerów komunikacji. Importowanie certyfikatu odbywa się na ekranie tworzenia i edycji [P-Mode]. Może się ono odbyć na dwa sposoby: poprzez podanie przyjaznej nazwy lub części pola podmiot certyfikatu zainstalowanego w magazynie certyfikatów Windows albo ewentualnie poprzez wczytanie pliku certyfikatu wraz z podaniem hasła do pliku, skutkującego zapisem w bazie danych programu. [P-Mode] odzwierciedla komunikację w jednym kierunku, dlatego jeśli komunikacja ma przebiegać w obydwu kierunkach należałoby zdefiniować dwa [P-Mode], jednak gdy używany jest ten sam certyfikat przez partnerów do podpisu i szyfrowania, wystarczy zdefiniować [P-Mode] w jednym kierunku. W przypadku definiowania [P-Mode] w obu kierunkach w [P-Mode] służącym do wysyłania certyfikat podpisu musi posiadać klucz prywatny, po to aby można było nim podpisać wysyłaną wiadomość, natomiast w [P-Mode] służącym do odbierania klucz prywatny musi być zawarty w certyfikacie szyfrowania, aby odszyfrować wiadomość odebraną. Stąd konieczność podania hasła podczas wczytywania, ponieważ plik certyfikatu posiadający klucz prywatny zostaje zabezpieczony hasłem. W przypadku definiowania jednego [P-Mode] dla obu kierunków lepszym rozwiązaniem będzie zdefiniowanie [P-Mode] wysyłającego.

Na ekranie tworzenia nowego [P-Mode] niektóre wartości są odgórnie ustalone w oparciu o dokumentację protokołu i nie można ich zmienić, dla wielu pozostałych pojawiają się wartości domyślne, również w zależności od wybranego u góry profilu AS4, które mogą zostać zmienione na inne. Ważnym polem jest [Agreement], którego wartość staje się identyfikatorem umowy w komunikacji między partnerami. Pola [MEP] i [MEPBinding] służą określeniu wzorca komunikacji, w polach [Initiator.Party] i [Responder.Party] należy podać identyfikator partnera – w komunikacji Edig@s jest nim kod EIC, a [Protocol.Address] odpowiada adresowi URL na jaki wysyłane są dokumenty.

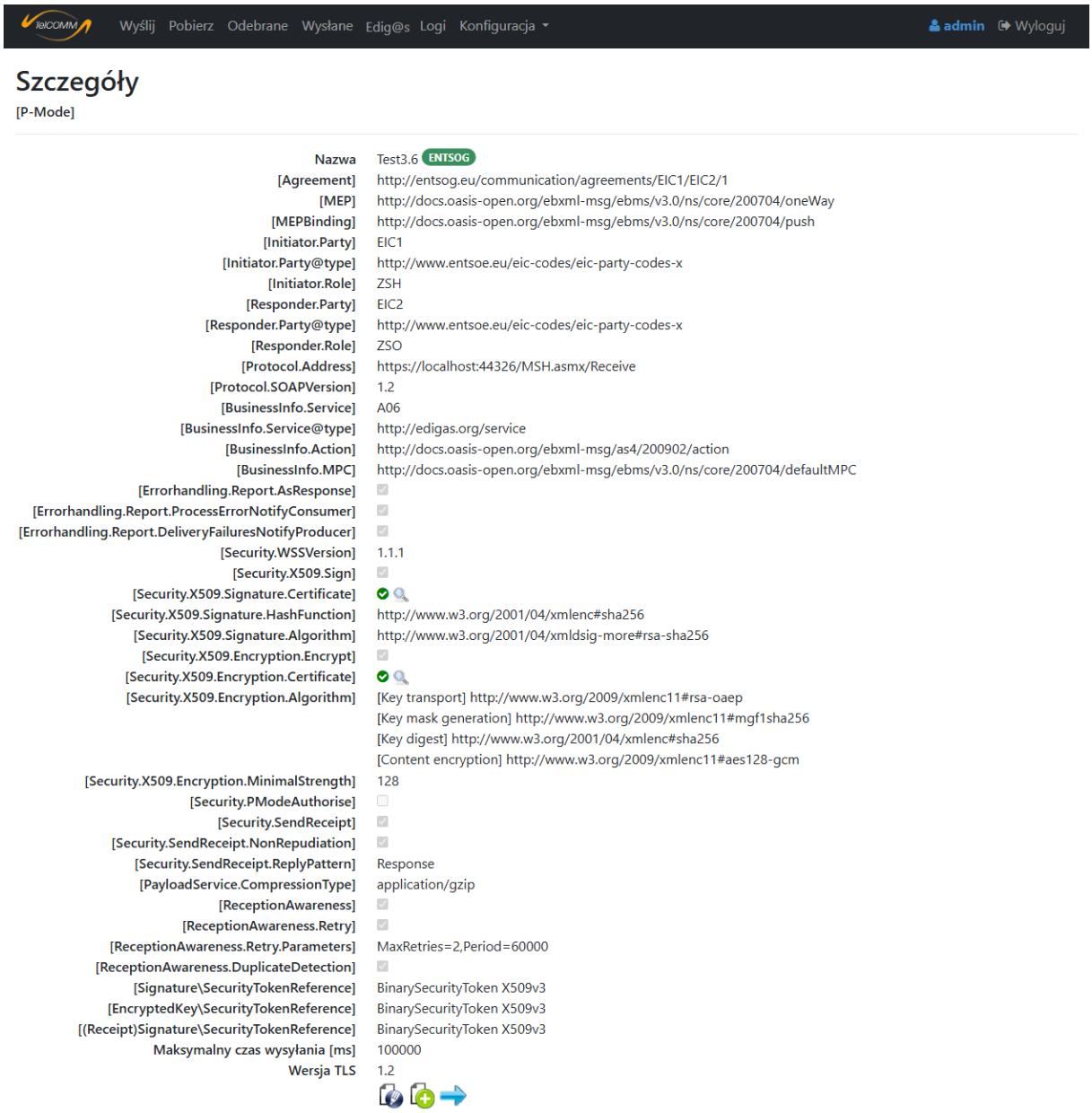
Jest również kilka pól dodatkowych, niezawartych w dokumentacji, jak np. Nazwa czy Certyfikat TLS serwera bądź klienta. Nazwa oprócz tego, że pozwala na łatwiejszą identyfikację danego [P-Mode] na ekranach programu, jest używana podczas wysyłania wiadomości przez usługę sieciową (web service). Wczytanie certyfikatu TLS serwera nie jest wymagane, ponieważ domyślnie podczas wysyłania certyfikat znajdujący się po stronie serwera jest sprawdzany czy jest prawidłowy (ma to miejsce gdy adres URL odbiorcy rozpoczyna się od „https://", a nie „http://"). Można go wczytać gdy jedyną walidację jaką chcemy wykonać to sprawdzenie czy certyfikat po stronie serwera jest identyczny co wczytany (mamy wtedy silniejszą weryfikację, ale nie ma sprawdzenia czy certyfikat

jest prawidłowy, czyli np. czy nie wygasł). Załączenie certyfikatu TLS klienta przyda się w niestandardowym przypadku gdy partner wymaga walidacji klienta.



Rysunek 17. Część ekranu tworzenia nowego [P-Mode]

Na ekranie szczegółów istnieje możliwość podglądu właściwości [P-Mode], w tym także podglądu certyfikatów podpisu, szyfrowania i TLS.

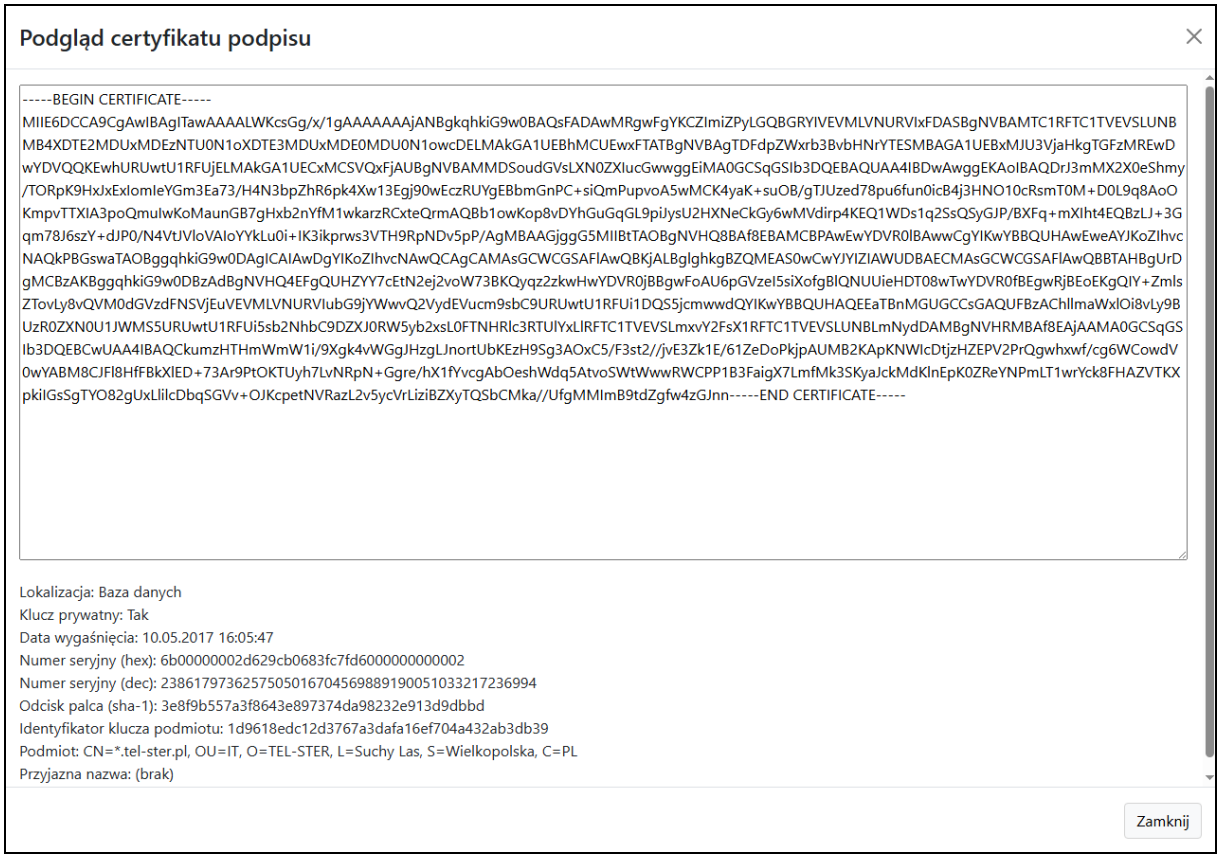


Rysunek 18. Ekran szczegółów [P-Mode]

Zawartość okna „Podgląd certyfikatu” przedstawia certyfikat z kluczem publicznym w standardzie X.509 kodowany metodą Base64 wraz z wyróżnionymi informacjami (szczegóły na poniższym rysunku). W przypadku włączonej w konfiguracji programu opcji „Walidacja certyfikatów”, pojawia się dodatkowa informacja, jeśli walidacja certyfikatu zakończyła się wynikiem negatywnym. Własne certyfikaty należy przekazać partnerowi komunikacji bez klucza prywatnego (!) w postaci tekstowej (zawartość okna) lub pliku (.cer, .pem), aby korzystając z zawartego w certyfikacie klucza publicznego mógł on:

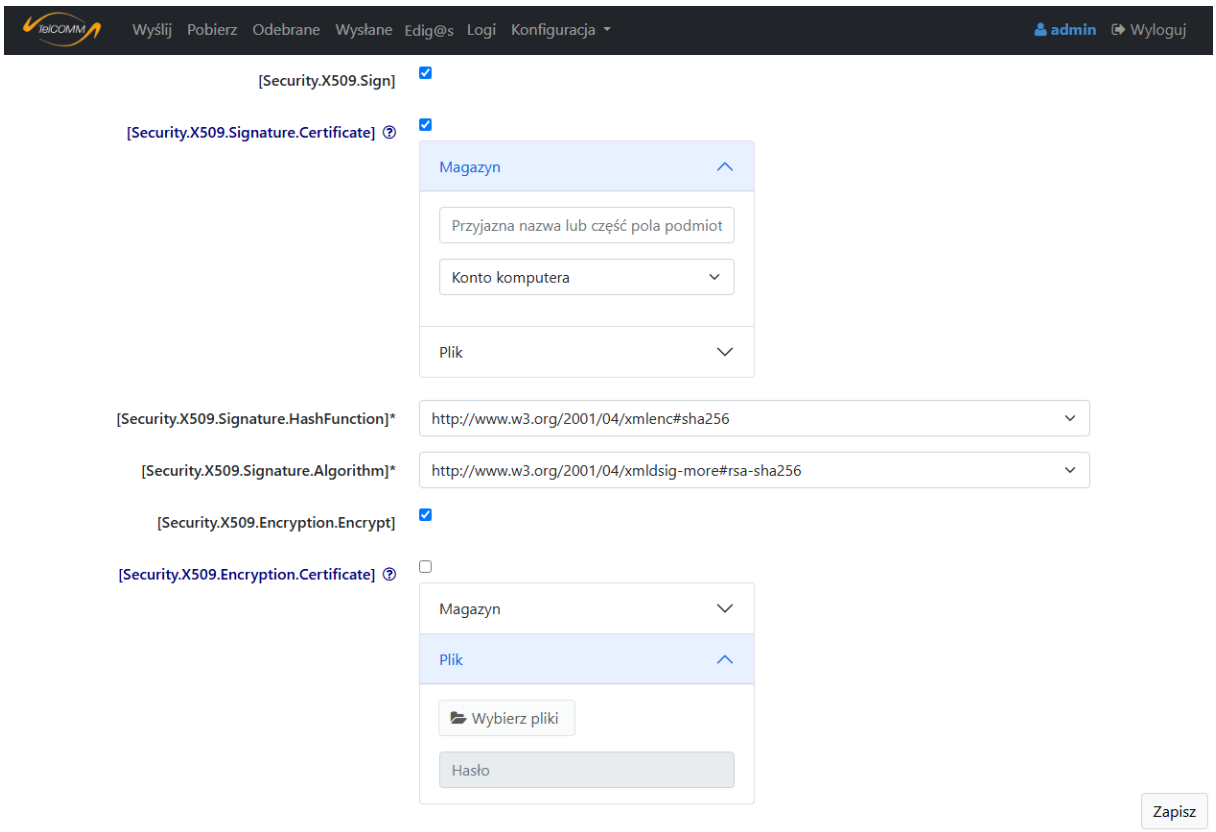
- zweryfikować podpis wysłanej do niego wiadomości,
- zaszyfrować wysyłaną przez niego do nas wiadomość.

TEL-STER Sp. z o.o.
ul. Stefana Stefańskiego 23
62-002 Suchy Las
Tel. +48 61 628 97 50
Fax. +48 61 639 37 11



Rysunek 19. Podgląd przykładowego certyfikatu podpisu na ekranie szczegółów [P-Mode]

W przypadku edycji [P-Mode] zmiana certyfikatu jest możliwa po zaznaczeniu pola wyboru „Wczytaj” przy polu certyfikatu. Dzięki temu podczas edycji można zachować wcześniej wczytane certyfikaty lub zmienić dowolny z nich.

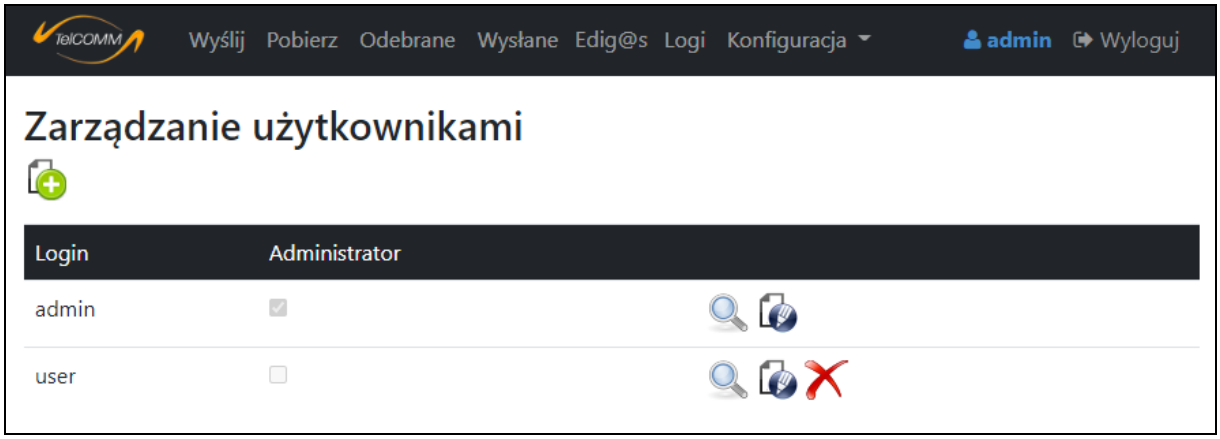


Rysunek 20. Część ekranu edycji [P-Mode]

Edycja certyfikatów w istniejącym [P-Mode] nie jest preferowanym rozwiązaniem – zalecane jest stworzyć nową wersję dla danego [P-Mode]. Na ogólnym ekranie jak i na ekranie szczegółów istnieje taka możliwość jako jedna z opcji dla [P-Mode] – pojawia się wtedy ekran tworzenia nowej wersji [P-Mode] z wypełnionymi polami aktualnymi wartościami. Korzystanie z takiego podejścia powoduje, że w komunikacji nadal będzie używany aktualny [P-Mode], do czasu gdy partner przestanie używać danej konfiguracji – wtedy nastąpi jego dezaktywowanie oraz automatyczne przełączenie się na korzystanie z nowego [P-Mode] (więcej w rozdziale Automatyczna aktualizacja certyfikatów). Na obu wyżej wspomnianych ekranach istnieje również możliwość wyeksportowania [P-Mode] do XML. Usunąć [P-Mode] można definitywnie lub jedynie dezaktywować tj. [P-Mode] przestaje być używane w programie, ale pozostaje dostępne na ekranie dezaktywowanych [P-Modes], z opcją ewentualnego przywrócenia do działania.

Ekran „Użytkownicy”

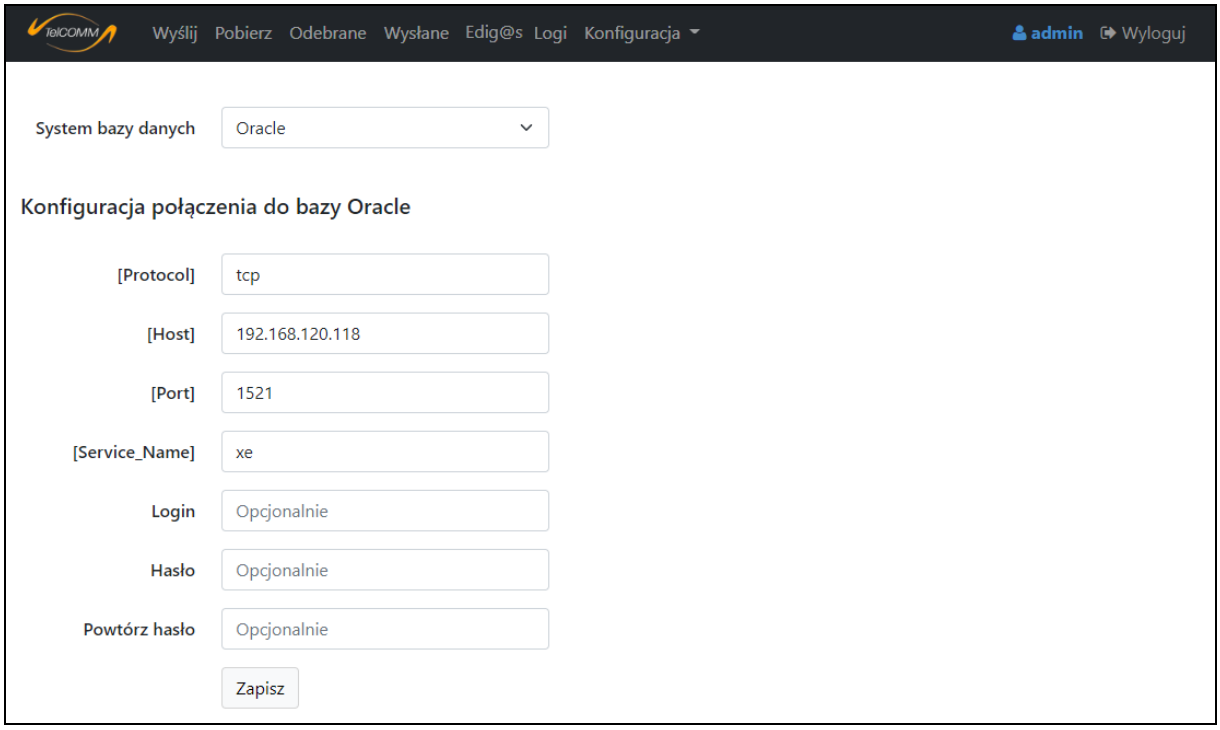
Ekran „Konfiguracja->Użytkownicy” służy do zarządzania użytkownikami. Użytkownik może otrzymać uprawnienia zwykłe lub administratora. W programie istnieje nieusuwalny użytkownik „admin”, którego początkowe hasło, również „admin”, należy zmienić na ekranie edycji użytkownika po pierwszym logowaniu (login ewentualnie też).



Rysunek 21. Ekran „Użytkownicy"

Ekran „Baza danych"

Na ekranie „Konfiguracja-> Baza danych" istnieje możliwość wyboru systemu bazy danych SQLite lub Oracle i konfiguracji połączenia do bazy w przypadku wyboru systemu Oracle.



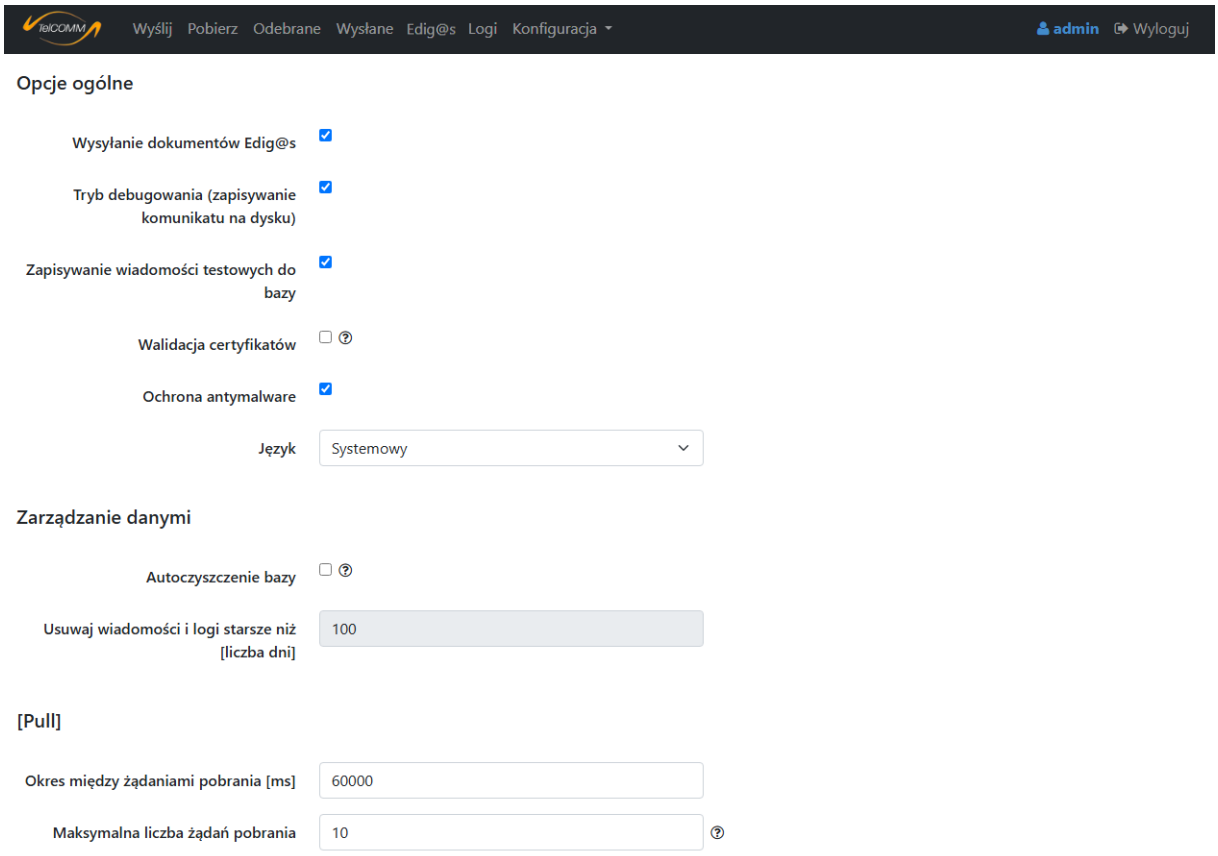
Rysunek 22. Ekran „Baza danych"

Ekran „Opcje"

Ekran „Konfiguracja->Opcje" posiada pogrupowane w sekcje następujące opcje:

- „Wysyłanie dokumentów Edig@s" – w przypadku wybrania tej opcji pojawią się na pasku nawigacyjnym zakładka „Edig@s", a na ekranie wysyłania wiadomości elementy związane z komunikacją Edig@s.
- „Tryb debugowania (zapisywanie komunikatu na dysku)" – program posiada możliwość pracy w trybie debugowania, który sprowadza się do zapisywania całych żądań i odpowiedzi HTTP wysłanych i odebranych w folderze Debug (przechowywane są komunikaty z ostatnich 100 dni, a w programie podejrzeć je można na ekranie „Komunikaty").

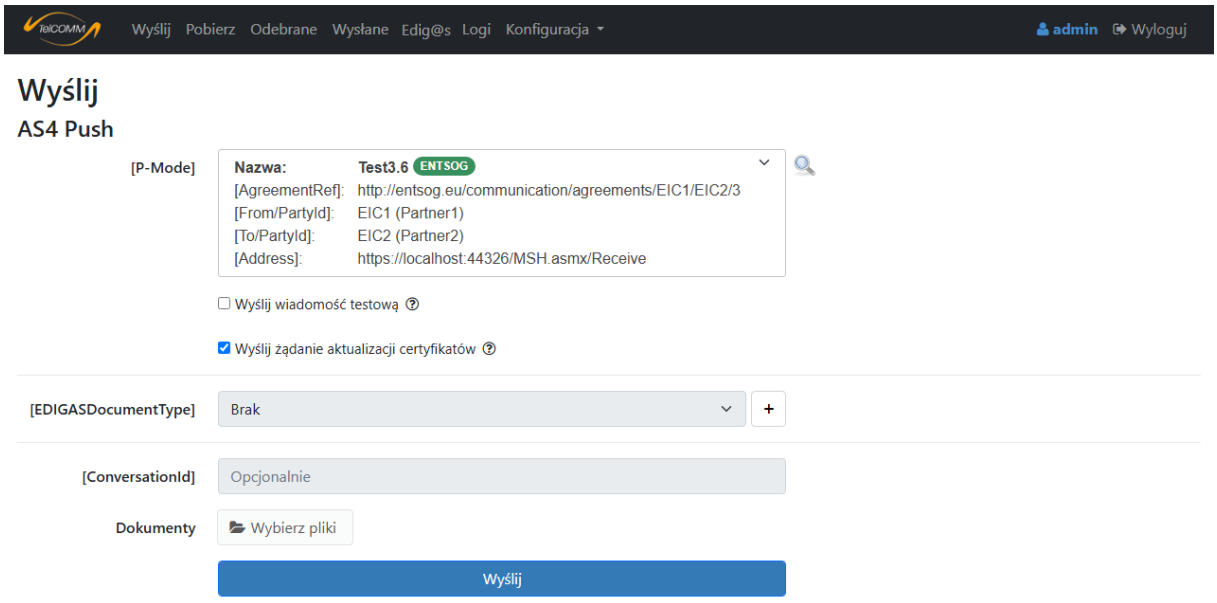
- „Zapisywanie wiadomości testowych do bazy” – opcja pozwala określić czy wiadomości testowe mają być zapisywane w bazie danych i tym samym widoczne na ekranach „Odebrane” i „Wysłane”.
- „Walidacja certyfikatów” – sprawdzanie poprawności używanych w programie certyfikatów (również OCSP/CRL, dlatego wymagane jest połączenie z serwerem urzędu certyfikacji) i w przypadku nieprawidłowości blokowanie komunikatu,
- „Ochrona antymalware” – skanowanie plików wysyłanych oraz odbieranych za pomocą Microsoft Defender i w przypadku pozytywnego wyniku zwrócenie błędu komunikacji
- „Język” – możliwość ustawienia języka polskiego lub angielskiego w interfejsie użytkownika.
- „Autoczyszczenie bazy” – opcja ta odpowiada za automatyczne usuwanie z bazy danych starszych wiadomości i wpisów w logu w oparciu o wartość z pola „Usuwaj wiadomości i logi starsze niż [liczba dni]”. Operacja jest wykonywana raz na dobę (dlatego odtwarzanie puli powinno być ustawione nie częściej niż co 24 godziny).
- „Okres między żądaniami pobrania [ms]” – parametr ten jak i następny dotyczą pobierania plików Pull – określa ile czasu ma upłynąć do następnej próby pobrania.
- „Maksymalna liczba żądań pobrania” – liczba wskazuje programowi ile razy po wysłaniu żądania ma próbować pobrać plik od partnera.
- „Ścieżka do pliku dll” – parametr ten jak i następny dotyczą HSM (Hardware Security Module), czyli zabezpieczenia polegającego na przechowywaniu certyfikatów (a w szczególności kluczy prywatnych) na osobnym dedykowanym urządzeniu sprzętowym – ścieżka do biblioteki udostępniającej metody komunikacji z HSM.
- „Pin użytkownika” – uwierzytelnienie w HSM.



Rysunek 23. Ekran „Opcje”

Automatyczna aktualizacja certyfikatów

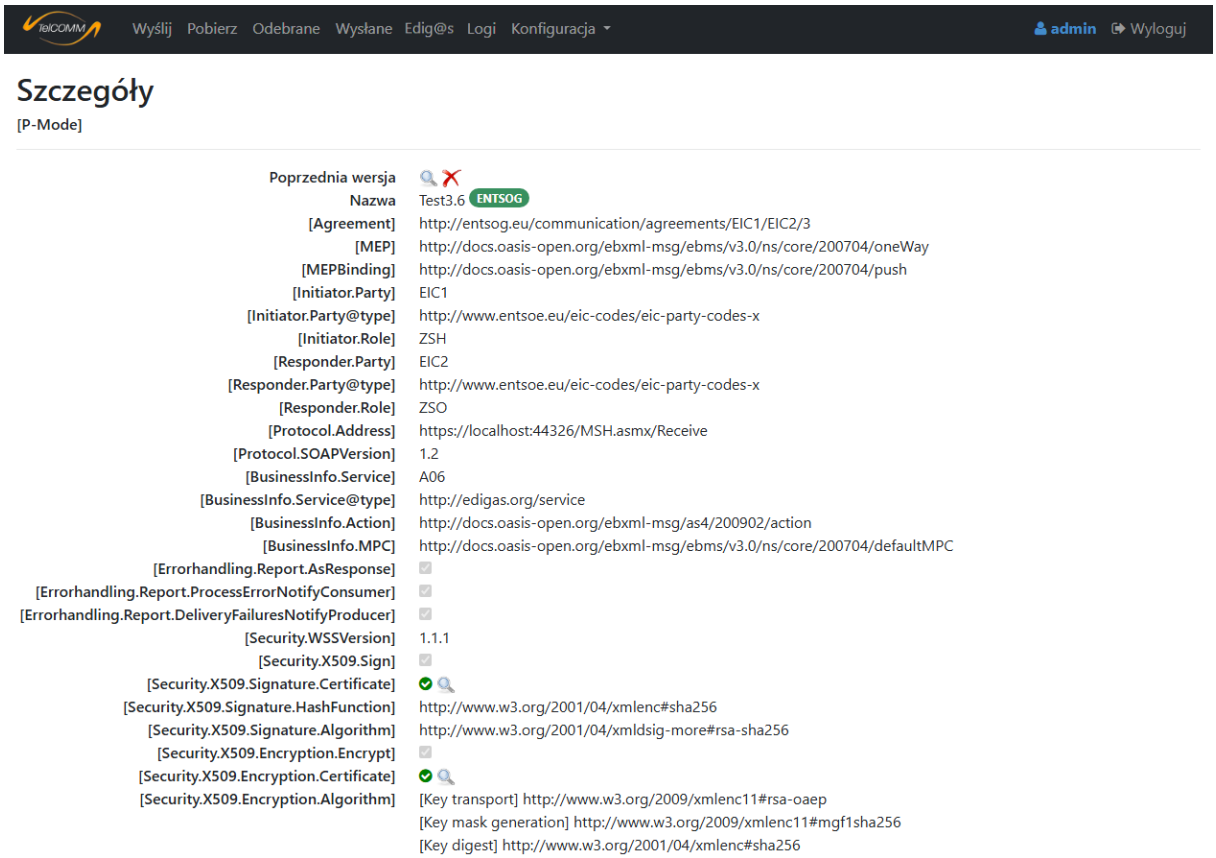
Funkcjonalność ta ma na celu zautomatyzowanie procesu aktualizacji certyfikatów podpisu i szyfrowania u partnerów komunikacji, który wynika z ograniczonej ważności certyfikatów. Aby można z niej skorzystać oprogramowanie po obu stronach komunikacji musi wspierać to rozwiązanie. Program TelCOMM przyjmuje żądania aktualizacji certyfikatów od partnerów, gdy chcą oni poinformować o aktualizacji swojego certyfikatu. Jeśli chodzi o ten kierunek aktualizacji nie są wymagane żadne działania ze strony użytkownika – wszystkie potrzebne operacje wykonywane są w sposób automatyczny, a ich wynik odnotowany w logu (podczas przełączenia na nowy certyfikat pojawi się wpis z błędem dotyczący odbioru, a następnie informacja o zakończeniu używania dotychczasowego [P-Mode]). Sytuacja ma się inaczej gdy aktualizacji wymaga certyfikat po stronie TelCOMM. Należy wtedy dla [P-Mode], w którym występuje dany certyfikat, dodać nie nowy [P-Mode], a nową wersję dla danego [P-Mode] z nowym certyfikatem. Jeśli [P-Mode] posiadających zmieniany certyfikat jest więcej, należy zaznaczyć przy dodawaniu nowego certyfikatu opcję „aktualizacja dla wszystkich [P-Mode]" – wtedy dla odpowiednich [P-Mode] zostanie również utworzona nowa wersja z nowym certyfikatem. Przy selekcji odpowiednich [P-Mode] brany jest pod uwagę jedynie certyfikat tego samego rodzaju np. podpisu, dlatego jeśli certyfikat, który ma zostać zmieniony jest używany także jako np. szyfrowania w [P-Mode] w kierunku odwrotnym, przy definiowaniu [P-Mode] w obu kierunkach, to również należy dla tego [P-Mode] dodać nową wersję i skorzystać z opcji „aktualizacja dla wszystkich [P-Mode]". Teoretycznie w nowej wersji [P-Mode] powinna pojawić się nowa wartość dla [AgreementRef], ale jest dopuszczone zachowanie aktualnej wartości, chociaż wiąże się z tym ograniczenie. Na ekranie wysyłania (lub pobierania) dla każdej nowej wersji [P-Mode] (pod warunkiem, że w nowej wersji jest nowa wartość [AgreementRef]) pojawi się opcja „Wyślij żądanie aktualizacji certyfikatu", którą należy zaznaczyć i wysłać komunikat.



Rysunek 24. Ekran „Wyślij" – żądanie aktualizacji certyfikatu

Wysłanie żądania aktualizacji certyfikatu jest specjalnym komunikatem AS4, ale działającym na tych samych zasadach co pozostałe komunikaty AS4. Po wysłaniu reszta procesu polegająca na dezaktywowaniu aktualnej wersji [P-Mode] i aktywowaniu nowej odbywa się automatycznie w momencie gdy partner zaktualizuje konfigurację po swojej stronie, a szczegóły tej operacji zostaną odnotowane w logu (podczas przełączenia na nowy certyfikat pojawi się wpis z błędem dotyczący wysłania, a następnie informacja o zakończeniu używania dotychczasowego [P-Mode]).

W przypadku gdy chcemy od razu rozpocząć korzystanie z nowej wersji [P-Mode] należy na górze ekranu szczegółów dla nowej wersji [P-Mode] dezaktywować poprzednią wersję. Wtedy dla danego [P-Mode] będzie używany od tego momentu nowy certyfikat.



Rysunek 25. Ekran szczegółów [P-Mode] – dezaktywowanie poprzedniej wersji

Interfejs do współpracy z programem zewnętrznym

Program TelCOMM może spełniać zadanie bramki do komunikacji B2B, przez którą inny program może automatycznie wysyłać i odbierać wiadomości za pomocą protokołu AS4, ponieważ udostępnia dedykowane metody w usłudze sieciowej /WebServices/**Gateway.asmx**. Aby móc korzystać z tych metod należy najpierw zalogować się w programie TelCOMM. Można to uczynić korzystając z metod HTTP:

a) /Login/LogOnExternal – metoda typu POST służąca do logowania programu zewnętrznego w TelCOMM. Login i hasło należy przekazać w parametrach „login" i „password". W przypadku poprawnego zalogowania w odpowiedzi HTTP umieszczone zostaną ciastka (cookie), które należy załączyć do żądania HTTP adresowanego do metody z usługi sieciowej Gateway.asmx,

b) /Login/LogOffExternal – metoda typu GET wylogowująca program zewnętrzny z TelCOMM.

lub bezpośrednio w usłudze sieciowej Gateway.asmx, za pomocą analogicznych metod:

a) LogOn

b) LogOff

Sposób drugi jest preferowany.

W usłudze sieciowej **Gateway.asmx** udostępniono metody, z których najważniejsze to:

a) SendByPModeName – metoda służąca do wysyłania za pomocą protokołu AS4, jako argumenty przyjmuje pliki (nazwa pliku i binarna treść) oraz nazwę zdefiniowanego [P-Mode]. Poza tym ewentualnie podawana jest informacja o typie wysyłanego dokumentu Edig@s i o wysyłaniu plików w osobnych wiadomościach, a zwracany jest obiekt z wynikiem analizy odpowiedzi od odbiorcy,

b) GetSendOptions – metoda pomocnicza zwracająca możliwe wartości dla niektórych parametrów, z których można skorzystać w powyższych metodach,

c) GetUnreadMessagesIds – zwraca listę wartości tekstowych „MessageId" wiadomości odebranych, które nie są oznaczone jako przeczytane; GetUnreadPushMessagesIds, GetUnreadPullMessagesIds, GetUnreadSyncMessagesIds – jw. z tą różnicą, że wyniki dotyczą odpowiedniego wzorca komunikacji,

d) GetMessage – pobiera szczegóły wiadomości odebranej podając jako argument „MessageId"; GetMessages – pobiera szczegóły wielu wiadomości odebranych podając jako argument listę wartości „MessageId"; GetMessageSent - pobiera szczegóły wiadomości wysłanej,

e) MarkAsRead - oznacza wiadomości jako przeczytane, przyjmując jako argument listę wartości „MessageId",

f) AddPullRequestByPModeName – bezpośrednie pobranie korzystając z wzorca One-Way/Pull,

g) AddPullResponseByReceivedMessageId – metoda wykorzystywana przy udostępnianiu danych z użyciem wzorca Two-Way/Push-Pull.

Poniższa tabela przedstawia jakich metod usługi sieciowej Gateway.asmx należy użyć aby wysłać do lub odebrać od partnera komunikat dla danego wzorca komunikacji AS4 przez program zewnętrzny:

Wzorzec komunikacji AS4	Kierunek	Metody web service Gateway.asmx
One-Way/Push	Wysłanie	1. SendByPModeName
	Odebranie	1. GetUnreadPushMessagesIds 2. GetMessage lub GetMessages 3. MarkAsRead
Two-Way/Push-Pull	Wysłanie	1. SendByPModeName
	Odebranie	1. GetUnreadPullMessagesIds 2. GetMessage lub GetMessages 3. MarkAsRead 4. AddPullResponseByReceivedMessageId (w przypadku udostępniania danych)
Two-Way/Sync	Wysłanie	1. SendByPModeName
	Odebranie	1. GetUnreadSyncMessagesIds 2. GetMessage lub GetMessages 3. MarkAsRead
One-Way/Pull	Wysłanie	1. AddPullRequestByPModeName

Tab. 1. Metody web service Gateway używane przy wysyłaniu i odbieraniu dla danego wzorca komunikacji

Na następnym rysunku przedstawiony został przykład synchronicznego wykorzystania metod usługi sieciowej Gateway.asmx w środowisku .NET Framework w języku C#. W podanym przykładzie skorzystano z wcześniej dodanego web reference o nazwie „localhost”.

```
localhost.Gateway gate = new localhost.Gateway
{
    CookieContainer = new CookieContainer()
};

string logOnResult = gate.LogOn("admin", "admin");

string[] unreadMessagesIds = gate.GetUnreadPushMessagesIds();

var receivedMessages = gate.GetMessages(unreadMessagesIds);

bool markAsReadResult = gate.MarkAsRead(unreadMessagesIds);

gate.LogOff();
```

Rysunek 26. Przykład wykorzystania metod web service Gateway [.NET Framework C#, web reference, synchronicznie]

Kolejny przykład pokazuje wysłanie komunikatu AS4 w oparciu o zdefiniowany [P-Mode] o nazwie „nomint”. Wysyłane pliki zostały przekazane w argumencie „files” funkcji „SendByPModeName”, który jest listą obiektów o dwóch właściwościach: dane binarne i nazwa pliku. Dodatkowo określony zostaje typ wysyłanego dokumentu Edig@s i każdy plik zostaje wysłany w osobnej wiadomości (opcja ta jest brana pod uwagę przy wysyłaniu więcej niż jednego pliku).

TEL-STER Sp. z o.o.
ul. Stefana Stefańskiego 23
62-002 Suchy Las
Tel. +48 61 628 97 50
Fax. +48 61 639 37 11

```
localhost.AS4SendModelPModeName sendModelPModeName = new localhost.AS4SendModelPModeName()
{
    PModeName = "nomint",
    EDIGASDocumentTypeCode = "01G",
    AttachmentsApart = true
};

localhost.SendResult result = gateway.SendByPModeName(files, sendModelPModeName);
```

Rysunek 27. Przykład wysłania komunikatu AS4 [.NET Framework C#, web reference, synchronicznie]

Usługa umożliwiająca odbiór dokumentów od partnerów

Integralną częścią programu TelCOMM jest usługa do odbierania komunikatów AS4. Służy do tego metoda **Receive** w usłudze sieciowej (web service) **MSH.asmx**. Adres względny odbierania to: **/MSH.asmx/Receive.**

Po odebraniu wiadomości wysyłana jest odpowiedź (synchronicznie lub w osobnym komunikacie) spełniająca wymaganie niezaprzeczalności odbioru (pod warunkiem, że wiadomość była podpisana i program dysponuje certyfikatem podpisu dla nadawcy odpowiedzi) lub z potwierdzeniem odbioru. Moduł odbierania wyposażony jest również w funkcjonalność wykrywania duplikatów wiadomości (duplicate detection) oraz obsługę błędów (error handling).

Udostępnianie danych

W przypadku korzystania z programu TelCOMM w celu udostępniania danych za pomocą wzorca komunikacji **Two-Way/Push-Pull** analiza żądań o dane i zwracanie wyników do programu odbywa się poza TelCOMM z wykorzystaniem odpowiednich metod usługi sieciowej (web service) Gateway.asmx podanych w tabeli 1.

Załączniki

TelCOMM – Wymagania i architektura

TelCOMM – Procedura instalacji

TelCOMM – Konfiguracja AS4 – Szablon 1

TelCOMM – Konfiguracja AS4 – Szablon 2

Materiały źródłowe

Program TelCOMM został wykonany w oparciu o poniższe dokumenty, w których znajdują się szczegółowe informacje na temat komunikacji z użyciem protokołu AS4.

[ENTSOG] AS4 Profile version 3.6

[ENTSOG] AS4 Profile version 4.0

[BDEW] AS4 Profil

[BDEW] Regelungen zum Übertragungsweg für AS4

[OASIS] AS4 Profile of ebMS 3.0 Version 1.0

[OASIS] ebCore Agreement Update Specification Version 1.0

[GAZ-SYSTEM] Instrukcja w zakresie wymiany danych protokołem AS4

[GAZ-SYSTEM] Techniczny opis rozwiązania dla wymiany komunikatów Edig@s z wykorzystaniem standardu AS4

[GAZ-SYSTEM] Techniczny opis rozwiązania dla udostępniania danych pomiarowych i zagregowanych z wykorzystaniem standardu AS4