
S_01 - Standard Integracji Systemów w Grupie Energa

WŁAŚCICIEL REGULACJI	NR WYDANIA	DATA WEJŚCIA W ŻYCIE
Departament IT	VI	03.10.2024

Spis treści

Wstęp	3
1. Wytyczne standardu integracji systemów	3
2. Dokumenty powiązane	6
3. Zasady wyłączenia ze stosowania	6
Historia wersji	7

Wstęp

Niniejszy dokument powstał w związku z wprowadzaniem Katalogu Standardów IT wynikającego z Kodeksu Architektury GK Energa będącego częścią Polityki IT Grupy Energa.

Celem standaryzacji sposobu integracji systemów w Grupie Energa jest wskazanie wytycznych ogólnych, na których bazować powinien proces uzgadniania, zamawiania i projektowania (bez ograniczenia do) integracji systemów IT na potrzeby Spółek Grupy Kapitałowej Energa.

Uregulowania zawarte w Standardzie Integracji Systemów w Grupie Energa obowiązują każdą jednostkę organizacyjną realizującą czynności związane z rozwojem i/lub utrzymaniem oprogramowania.

1. Wytyczne standardu integracji systemów

Wymaganiem jest, aby integracja systemów na potrzeby Grupy Energa realizowana była w sposób uwzględniający następujące oczekiwania:

1. Co do zasady integracja systemów powinna być asynchroniczna.
 - 1.1. Komunikacja synchroniczna może być stosowana w uzasadnionych przypadkach tj. gdy charakterystyka realizowanej operacji wymaga natychmiastowej odpowiedzi w szczególności na potrzeby wywołań cyklicznych (np. quasi-real-time, komunikaty związane z diagnostyką np. typu healthcheck, związane z aktualizacją danych cache-owanych) oraz gdy usługi zwracające dane są w stanie udostępnić wynik bez ryzyka generowania timeout-ów na całej ścieżce wywołania.
2. W komunikacji opartej o usługi dopuszczalnymi standardami są REST API oparty na protokole HTTPS wykorzystujący format danych taki jak JSON oraz SOAP 1.2, WSDL 2.0 i XML Schema 1.1. Preferowanym standardem jest REST API/JSON. Dobre praktyki w zakresie stosowania REST API znajdują się w załączniku 1.
3. Integracja:
 - a) Korporacyjnych Systemów Wspólnych (KSW) z innymi systemami IT lub OT co do zasady musi odbywać się poprzez Korporacyjną Szynę Danych nonOSD Grupy Energa (KSD nonOSD).
 - b) systemów IT i OT Energa Operator S.A. co do zasady musi odbywać się poprzez Korporacyjną Szynę Danych OSD (KSD OSD) Energa Operator S.A.
 - c) systemów IT Spółek Grupy Energa poza Energa Operator S.A. co do zasady musi odbywać się poprzez Korporacyjną Szynę Danych nonOSD Grupy Energa (KSD nonOSD)
 - d) w przypadku wymiany komunikatów, pomiędzy Systemami IT lub OT, niewymagających ich konwersji dopuszcza się komunikację poprzez instancję systemu kolejkowego zapewniającą persystencję, buforowanie komunikatów oraz mechanizmy publish/subscribe, monitoringu, logowania zdarzeń
 - 3.1. Interfejsy oparte na protokole LDAP (komunikacja oparta na natywnych konektorach „z pudełka” rozwiązań COTS) do komunikacji z Active Directory nie wymagają oparcia o szynę danych.
 - 3.2. Bezpośrednie przekazywanie danych może być stosowane w przypadku konieczności przesłania dużej ilości danych, które nie musi być realizowane na bieżąco (zazwyczaj cyklicznie, np. w trybie dziennym). Dotyczy to w szczególności sytuacji:
 - 3.2.1. Ładowanie danych do hurtowni danych w celu ich cyklicznego przetwarzania na potrzeby raportowe,
 - 3.2.2. Ładowanie dużych zbiorów danych na potrzeby analityczne, np. na potrzeby analiz w zewnętrznym narzędziu,
 - 3.3. Bezpośrednie przekazywanie plików binarnych może być stosowane w przypadku konieczności przekazywania plików binarnych (np. skanów dokumentów), którego celem jest odłożenie obrazu do repozytorium dokumentów (DMS - Document Management System) i pobranie nadanego identyfikatora dokumentowi przez repozytorium. W powyższym przypadku należy stosować następujące zasady:
 - 3.3.1. Komunikacja bezpośrednia musi służyć tylko i wyłącznie do złożenia dokumentu w repozytorium. Wraz z przesłaniem pliku do repozytorium nie można przekazywać dodatkowych danych

- biznesowych, poza metadanymi pliku niezbędnymi do jego identyfikacji (np. typ/klasa dokumentu, ID Klienta powiązanego z dokumentem, ID sprawy/reklamacji, etc.).
- 3.3.2. Nadany identyfikator przez repozytorium dokumentów należy wykorzystywać w dalszej komunikacji między systemami, bez przysyłania samego pliku.
- 3.4. Bezpośrednie przekazywanie plików binarnych może być stosowane w przypadku udostępniania ich do odczytu.
4. Co do zasady w przypadku stosowania bezpośredniego przekazywania plików binarnych, komunikacja pomiędzy systemami niebędącymi repozytorium dokumentów powinna być oparta na usługach, natomiast samo udostępnienie obrazu powinno nastąpić poprzez współdzieloną lokalizację (np. SFTP, DMS), zgodnie ze standardem MTOM¹, lub poprzez natywny konektor. Uprawnienia do współdzielonej lokalizacji powinny uwzględniać poziom poufności danych – w szczególności konieczne może być utworzenie odrębnych lokalizacji w zależności od aplikacji i klasyfikacji poufności przekazywanych danych. Ponadto, system docelowy po pobraniu danych ze współdzielonej lokalizacji powinien każdorazowo usuwać wykorzystane dane, aby ograniczyć czas życia zmniejszając tym samym zagrożenie dla poufności.
5. Przed zastosowaniem bezpośredniego przekazywania danych należy rozważyć następujące scenariusze realizacji komunikacji w modelu opartym na usługach:
- 5.1. Zastąpienie cyklicznego ładowania danych komunikacją zdarzeniową (notyfikacje o zdarzeniach pozwalające na bieżącą aktualizację po stronie systemu docelowego),
 - 5.2. Zastąpienie tworzenia kopii danych (z systemu źródłowego przechowującego dane do systemu docelowego działającego na kopii danych) bieżącymi zapytaniami z systemu docelowego o dane obiektu biznesowego gromadzone przez system źródłowy, zwłaszcza jeśli kopia danych nie jest często wykorzystywana.
6. Przy bezpośrednim przekazywaniu danych należy stosować następujące zasady:
- 6.1. System źródłowy przygotowuje dane do pobrania przez system docelowy i umieszcza je we współdzielonej lokalizacji.
 - 6.2. Implementowany sposób współdzielenia danych począwszy od przygotowania danych, a kończąc na ich zaczytaniu do bazy systemu docelowego bezwzględnie powinien uniemożliwiać ingerencję osób nieautoryzowanych zarówno w strukturę jak i zawartość danych. Nie dopuszcza się sytuacji, w której użytkownik biznesowy posiada jakikolwiek dostęp do edycji i modyfikacji przesyłanych informacji w sposób inny niż dostępne funkcjonalności edycji danych podstawowych (master data) w systemie źródłowym.
 - 6.3. Współdzielona lokalizacja powinna znajdować się poza podstawowymi strukturami danych systemu źródłowego i docelowego – może to być np. dedykowany zasób dyskowy (sieciowy lub SFTP) lub schemat bazodanowy (ma to na celu ograniczenie ryzyka dla działania obydwu systemów).
 - 6.4. Udostępniane dane mogą być przygotowane i zapisane w formie pliku lub tabel bazodanowych.
 - 6.5. Do ładowania danych do systemu docelowego wykorzystywane są narzędzia po stronie systemu docelowego. Należy rozważyć wykorzystanie narzędzi ETL/ELT, jeśli są one dostępne po stronie bazy danych systemu docelowego.
7. Każdorazowo dla usług asynchronicznych należy zastosować mechanizm kolejkowania na wypadek tymczasowej niedostępności systemu docelowego.
8. W projektowaniu integracji systemów należy przestrzegać i stosować wzorce architektoniczne integracji aplikacji.
9. Integracja musi być udokumentowana zgodnie ze:
- 9.1. Standardem Dokumentacji Oprogramowania (S_08),
 - 9.2. Standardem Dokumentacji Interfejsów (S_02).
10. Bezpośrednie przekazywanie danych przez pliki może być stosowane również w przypadku systemów zastanych, dla których ze względów technologicznych (wykonalność) lub biznesowych (opłacalność) konieczna jest rezygnacja z komunikacji opartej na usługach. W takich przypadkach zalecane jest wykorzystanie odpowiedniego adaptera korporacyjnej szyny usług (np. File Adapter) wraz z odpowiednim mapowaniem struktur danych w celu utworzenia interfejsu. Dzięki temu inne systemy IT komunikujące się z

¹ MTOM - SOAP Message Transmission Optimization Mechanism.

- systemem zastanym mogą korzystać z komunikacji opartej na usługach (korporacyjna szyna usług pełni rolę fasady – wzorec Legacy Wrapper).
11. W przypadku potrzeby realizacji funkcjonalności wspieranej przez system informatyczny, w pierwszej kolejności należy przeanalizować możliwość wykorzystania usług istniejących systemów informatycznych. W przypadku braku odpowiedniej usługi (możliwej do wykorzystania wprost lub rozszerzenia), konieczne jest zaprojektowanie nowej usługi.
 12. Nowa usługa powinna mieć rozłączny zakres funkcjonalny względem istniejących usług. Przy identyfikacji usługi należy zwrócić uwagę, aby nie pokrywała się ona (również częściowo) z zakresami innych usług. Ma to na celu ograniczenie złożoności środowiska IT (uniknięcie niekontrolowanego rozrostu liczby usług i powielania w wielu miejscach tej samej lub podobnej logiki).
 13. Przy identyfikacji usług i realizowanych przez nie operacji należy zwrócić szczególną uwagę na zapewnienie możliwości wykorzystania usługi w różnych kontekstach i przez różnych konsumentów. Należy zadbać o realizację – oprócz celów biznesowych danego projektu – również przewidywanych przyszłych potrzeb związanych z potencjalnymi zastosowaniami nowej usługi. W szczególności należy:
 - 13.1. Unikać wprowadzania w ramach usługi elementów specyficznych dla konkretnej wymiany danych pomiędzy dwoma systemami,
 - 13.2. W przypadku usług warstwy encji każdorazowo zapewnić udostępnienie operacji typu CRUD operujących na pełnym obiekcie,
 - 13.3. Uwzględnić przy projektowaniu usługi wszystkie zidentyfikowane potencjalne przyszłe operacje (tj. takie, które mogą być użyteczne w przyszłości, ale nie są niezbędne z perspektywy realizowanego projektu); operacje te nie muszą być implementowane w ramach projektu, ale powinny być uwzględnione w kontrakcie usługi ze statusem POTENCJALNA.
 14. Dla usług zidentyfikowanych do wykonania, w pierwszej kolejności projektowany jest kontrakt usługi (podejście tzw. contract first). Kontrakt projektowany jest w odniesieniu do założeń biznesowych (funkcjonalnych i dotyczących poziomu świadczenia usługi), abstrahując od struktury i sposobu realizacji usługi w konkretnym systemie informatycznym. Podejście takie pozwala uzyskać kontrakt usługi spełniający wymagania dla usługi, nie uzależniając go od technologii realizacji samej usługi.
Po opracowaniu i zatwierdzeniu kontraktu usługi należy przejść do zaprojektowania sposobu jej realizacji w systemie informatycznym, a następnie jej wytworzenia.
 15. Dla każdej Spółki Grupy Energa wszystkie kontrakty usług powinny być zgromadzone w jednym repozytorium w celu umożliwienia łatwego dostępu do nich osobom zaangażowanym w rozwój architektury IT danej Spółki Grupy Energa.
 16. Kanał komunikacji (warstwa transportowa) powinien być szyfrowany zawsze przy stosowaniu komunikacji opartej na usługach.
 - 16.1. Do szyfrowania powinien być wykorzystywany protokół HTTPS oraz certyfikaty X.509, minimalna dopuszczalna wersja protokołu TLS to 1.2 (wyklucza się z użycia w Grupie Energa wersje SSL).
 - 16.2. Rekomendowane jest stosowanie możliwie najnowszych dostępnych na danej platformie technologicznej zabezpieczeń w integracji systemów.
 - 16.3. Wybór zabezpieczeń musi odbyć się z poszanowaniem zasady proporcjonalności. Zasada ta powinna znaleźć swoją konkretyzację na etapie szacowania ryzyka przetwarzania i adekwatności stosowanych zabezpieczeń przetwarzanych informacji.
 17. Każdy z komponentów realizujących usługi powinien posiadać własne logi. Ma to na celu zapewnienie autonomii usług – możliwość logowania przebiegu przetwarzania i błędów nie powinna być ograniczona przez zależności od innych systemów.
 18. Szyna danych musi monitorować przepływy komunikatów (m.in. wykorzystanie wzorca Monitor Usług (proaktywne badanie dostępności), monitorowanie błędów, wydajności i wąskich gardeł).
 19. W przypadku wprowadzenia centralnego systemu logów powinien on być wykorzystywany jako podrzędna warstwa logowania (zapis pierwotny w logu własnym, a dodatkowo zdarzeniowe odłożenie danych w logu centralnym). Zapis do logu centralnego powinien być realizowany przez odpowiednią usługę warstwy narzędzi.
 20. W celu ułatwienia wykorzystania raz zbudowanych usług, stosowana jest spójna konwencja nazewnicza dla usług i operacji. W nazwach usług i operacji stosowany jest wyłącznie język angielski.

20.1. Nazwy usług powinny być krótkie i odzwierciedlać zakres funkcjonalny usługi. W większości przypadków nazwy usług powinny być rzeczownikami.

Nazwy usług powinny odpowiadać:

20.1.1. Nazwom czynności w procesach biznesowych, które realizują lub wspierają – w przypadku usług warstwy zadań, np. CalculatePayments,

20.1.2. Nazwom obiektów biznesowych, których dotyczą – w przypadku usług warstwy encji, np. Customer, Meter,

20.1.3. Udostępnianej funkcjonalności – w przypadku usług warstwy narzędziowej, np. Email, StateRepository.

20.1.4. W nazwach usług nie są stosowane oznaczenia numerów wersji, dookreślenia dotyczące technologii, protokołu komunikacji itp. Nie są również stosowane słowa nie odnoszące się do zakresu funkcjonalnego, takie jak Entity, Service, itp.

20.2. Nazwy operacji powinny być krótkie i odpowiadać realizowanej funkcjonalności. Zazwyczaj powinny być one czasownikami. Nazwa operacji powinna zaczynać się z małej litery, a kolejne słowa w nazwach operacji powinny rozpoczynać się od wielkich liter (np. sendEmail).

20.2.1. W szczególności, nazwy typowych operacji powinny być zgodne z poniższym słownikiem:

create – utworzenie obiektu,

read – pobranie obiektu,

update – aktualizacja obiektu,

delete – usunięcie obiektu,

cancel wraz z nazwą operacji do anulowania – zaniechanie działania i wycofanie jego skutków.

W przypadku operacji Read warunki zapytania określane są przez parametr wywołania usługi (przekazywana jest struktura danych wypełniona na polach zawierających warunki; nie są stosowane operacje typu readByName, readByPesel, itd.).

20.2.2. Dla operacji notyfikacji stosowane są czasowniki w czasie przeszłym, np. created, updated, deleted.

20.2.3. W nazwach operacji nie są stosowane oznaczenia numerów wersji, dookreślenia dotyczące technologii, protokołu komunikacji itp. Nie są również stosowane słowa nie odnoszące się do zakresu funkcjonalnego, takie jak Method, Operation, itp.

2. Dokumenty powiązane

- ✓ Instrukcje szczegółowe dla poszczególnych szyn danych (dostępne u poszczególnych zespołów odpowiedzialnych za rozwój i utrzymanie).
- ✓ Standard Wytwarzania Oprogramowania w Grupie Energa.
- ✓ Standard Dokumentacji Oprogramowania w Grupie Energa.
- ✓ Kodeks Architektoniczny Grupy Energa wydanie VI (załącznik nr 2 do Polityki IT).
- ✓ Katalog Standardów IT.

3. Zasady wyłączenia ze stosowania

Zgodnie z Punktem 3.4. Kodeksu Architektonicznego Grupy Energa wydanie VIII (Załącznik nr 2 do Polityki IT Grupy Energa) „W przypadku istnienia uzasadnionej potrzeby odstępstwa od przyjętych Standardów IT, istnieje możliwość uzyskania zgody na takie odstępstwo. Decyzję o wprowadzeniu odstępstwa podejmuje Dyrektor Departamentu IT (Energa S.A.) w formie pisemnej w wyniku otrzymania od wnioskującego pisemnego uzasadnienia. Wszelkie odstępstwa zaakceptowane przez Dyrektora Departamentu IT są ewidencjonowane i monitorowane przez Wydział Architektury Korporacyjnej w Departamencie IT (Energa S.A.)”.

Historia wersji

Numer wersji	Zmiany wprowadził(a)	Opis zmian	Nazwa pliku
1.0	Marcin Bromirski Artur Noworyta	Utworzenie dokumentu	S_01 - Standard Integracji Systemów w Grupie Energa - wersja 0.1.docx
2.0	Marcin Bromirski	Zmiany w Rozdziale 1: - Dodanie w punkcie 2 jako obowiązujących wersji w Grupie Energa: SOAP 1.1, WSDL 1.1 i XML Schema 1.0. - Połączenie punktów 3. i 4. (Ogólne zasady integracji IT i OT) w jeden punkt 3.; dodanie podpunktów 3.A i 3.B dla lepszego zrozumienia przez odbiorców; - Doprecyzowanie punktu 3.1 (dot. LDAP), że dotyczy każdej szyny danych, a nie tylko KSD nonOSD; - Wykreślony wyraz „rozważyć” z punktu 4.1 dotyczącego zastosowania kolejek, przez co punkt staje się obligatoryjny do stosowania. - Usunięcie w punkcie 6. Zapisu „(np. Enterprise Integration Patterns)”, ponieważ nic nie wnosi; - Poprawka wychwyconego błędu logicznego zdania w punkcie 8.1, tj. zmiana „system źródłowy” na „system docelowy”; - Dodanie do punktu 8.1 uszczegółowienia, że edycja współdzielonych danych nie jest możliwa przez użytkownika „w sposób inny niż dostępne funkcjonalności edycji danych podstawowych (master data) w systemie źródłowym”; - Dodanie do punktu 9 standardu MTOM. - Zmiana nazwy stanu operacji z „PLANOWANA” na „POTENCJALNA” w punkcie 13.3. - Dodano w rozdziale 16. zapis „minimalna dopuszczalna wersja protokołu TLS to 1.0 (wyklucza się z użycia w Grupie Energa wersje SSL).” - Dodanie w rozdziale 2 Dokumenty powiązane pozycji: Instrukcje szczegółowe dla poszczególnych szyn danych (dostępne u poszczególnych zespołów odpowiedzialnych za rozwój i utrzymanie).	S_01 - Standard Integracji Systemów w Grupie Energa - wersja 0.2.docx
3.0	Marcin Bromirski	Dodanie zapisu w rozdziale 1 punkt 3 o sposobie integracji systemów KSW: „Integracja Korporacyjnych Systemów Wspólnych (KSW) z innymi systemami IT lub OT co do zasady musi odbywać się poprzez Korporacyjną Szynę Danych nonOSD Grupy Energa (KSD nonOSD).”	S_01 - Standard Integracji Systemów w Grupie Energa - wersja 0.3-2020-05-13.docx
4.0	Marcin Bromirski	- Zmiana minimalnej dopuszczalnej wersji TLS z 1.0 na 1.2 (punkt 16). - Rozdział punktu 16 na podpunkty i dodanie zapisów o adekwatności zabezpieczeń i rekomendacji stosowania najnowszych zabezpieczeń: „16. Kanał komunikacji (warstwa transportowa) powinien być szyfrowany zawsze przy stosowaniu komunikacji opartej na usługach. 16.1. Do szyfrowania powinien być wykorzystywany protokół HTTPS oraz certyfikaty X.509, minimalna dopuszczalna wersja protokołu TLS to 1.2 (wyklucza się z użycia w Grupie Energa wersje SSL). 16.2. Rekomendowane jest stosowanie możliwie najnowszych dostępnych na danej platformie technologicznej zabezpieczeń w integracji systemów. 16.3. Wybór zabezpieczeń musi odbyć się z poszanowaniem zasady proporcjonalności. Zasada ta powinna znaleźć swoją konkretyzację na etapie szacowania ryzyka przetwarzania i adekwatności stosowanych zabezpieczeń przetwarzanych informacji.”	S_01 - Standard Integracji Systemów w Grupie Energa - wersja 0.4-2020-05-29.docx
5.0	Marcin Bromirski	Doprecyzowanie zapisów w związku z problemami w interpretacji dot. komunikacji bezpośredniej dla przypadków przekazywania plików binarnych do repozytorium dokumentów (DMS), poprzez: - wydzielenie z reguł „przekazywania danych” wprost zasad „przekazywania plików binarnych do repozytorium”. Dodany punkt 3.3 - zreorganizowana kolejność punktów w celu zebrania powiązanych reguł tematycznie.	S_01 - Standard Integracji Systemów w Grupie Energa - wersja 5.0.docx
6.0	Artur Liwanowski (20241001)	Zmodyfikowano pkt.2 jako standard uznajemy REST, SOAP jest alternatywą. Dodano regulacje dot. wykorzystania standardu REST jako rekomendowanego oraz systemu kolejkowego jako warstwy transportowej.	S_01 - Standard Integracji Systemów w Grupie Energa - wersja 6.0.docx

Załącznik 1: Dobre Praktyki stosowania REST API

1. Zastosowanie odpowiedniego nazewnictwa dla endpointów. Stosujemy tutaj tylko rzeczowniki.

Poprawne endpointy dla obiektu licznika:

- GET /meters (pobranie liczników)
- GET /meters/10 (pobranie licznika)
- POST /meters (dodanie licznika)
- PUT /meters (aktualizowanie licznika)
- DELETE /meters (usuwanie użytkownika)
- DELETE /meters/permission (usuwanie uprawnień do licznika)

2. Akcje muszą zwracać kody błędów http.

Kody HTTP:

- 100-199 odpowiedź informacyjna
- 200-299 sukces
- 300-399 przekierowanie
- 400-499 błąd klienta
- 500-599 błąd serwera

3. Umożliwianie klientowi stosowania paginacji, sortowania i filtrowania danych, aby w przypadku pobierania danych, klient mógł zawęzić, jak najbardziej potrzebne informacje i nie przeciążać serwera.
4. Wersjonowanie API poprzez wpisanie wersji API w endpoint, np. /api/v1/metres.
5. Stosowanie uwierzytelnienia i autoryzacji do endpointów i zasobów REST API.
6. Stosowanie strategii bufowania.
7. Walidacja danych wejściowych.
8. Wykorzystywanie autoryzacji opartej o OAuth2 o ile jest to możliwe,
9. Dla usług zwracających listy rekordów uruchomienie mechanizmu paginowania (stronicowania - Paging).

Sandra
Ewa
Dąbrowska

Elektronicznie
podpisany przez
Sandra Ewa
Dąbrowska
Data: 2025.12.23
13:05:48 +01'00'