ENEA Centrum sp. z o.o.
Ul. Górecka 1
60-201 Poznań

NIP 777 00 02 843
REGON 630770227
www.enea.pl

Poznań, 27.04.2021 r.

ODPOWIEDZI NA PYTANIA WYKONAWCÓW
MODYFIKACJA WARUNKÓW ZAMÓWIENIA

Sygnatura postępowania: **1100/DW00/ZT/KZ/2021/0000029545**
Sygnatura pisma: DL/LZ/AT/2021/773

Dotyczy: Dostawa i wdrożenie systemu służącego do obsługi i zarządzania stacjami ładowania pojazdów elektrycznych wraz z modułem rozliczeniowym

Działając na podstawie pkt 1.9 - 1.12 Warunków Zamówienia (dalej: WZ) Zamawiający modyfikuje wybrane zapisy WZ oraz odpowiada na pytania Wykonawców do treści WZ:

1	Zamawiający modyfikuje zapisy Warunków Zamówienia, co następuje: **<u>Rozdział I, pkt 12.1. WZ</u>** BYŁO: *„12.1. Ofertę należy złożyć w formie elektronicznej, za pośrednictwem środków komunikacji elektronicznej przesyłając ją na adresy email wskazane w pkt 1.17 WZ, w terminie do dnia 29.04.2021 r. do godz. 10:00. WAŻNE! Hasło dostępu do pliku ze złożoną ofertą, Wykonawca przesyła Zamawiającemu w innej wiadomości niż wiadomość z przesłaną Ofertą, na adresy email wskazane w pkt. 1.17 WZ, po upływie terminu składania ofert, jednak nie później niż w ciągu 2 godzin od upływu tego terminu, tj. przesyła Zamawiającemu hasło w dniu 29 kwietnia 2021 r. między godziną 10:00, a godziną 12:00.”* JEST: *„12.1. Ofertę należy złożyć w formie elektronicznej, za pośrednictwem środków komunikacji elektronicznej przesyłając ją na adresy email wskazane w pkt 1.17 WZ, w terminie do dnia 05.05.2021 r. do godz. 10:00. WAŻNE! Hasło dostępu do pliku ze złożoną ofertą, Wykonawca przesyła Zamawiającemu w innej wiadomości niż wiadomość z przesłaną Ofertą, na adresy email wskazane w pkt. 1.17 WZ, po upływie terminu składania ofert, jednak nie później niż w ciągu 2 godzin od upływu tego terminu, tj. przesyła Zamawiającemu hasło w dniu 05 maja 2021 r. między godziną 10:00, a godziną 12:00.”*
2.	**PYT:** Czy zabezpieczenia teleinformatyczne wymienione jako systemy antywirusowe, antyspamowe, antymalwareowe w załączniku nr 9, mają być stosowane tylko w dostarczonym Systemie czy mają obejmować także środowiska deweloperskie oraz wszystkie systemy zewnętrzne, w tym system Płatniczy?
	ODP: Zamawiający wymaga objęcia środowisk po stronie Wykonawcy, które będą wykorzystywane dla Systemu, zabezpieczeniami teleinformatycznymi wymienionymi jako systemy antywirusowe, antyspamowe, antymalwareowe w załączniku nr 9. Zamawiający wymaga, aby system Płatniczy spełniał rekomendacje KNF np. rekomendacja D
3.	**PYT:** Jaki system SIEM stosowany jest u Zamawiającego?
	ODP: Zamawiający informuje, że przekaże informacje dotyczące systemu SIEM Wykonawcom, którzy zwrócą się do Zamawiającego z prośbą o ich udostępnienie. Prośbę wraz z podpisanym Oświadczeniem o zachowaniu poufności złożyć należy na adresy email wskazane w pkt 1.17 WZ, nie później niż do terminu składania ofert. **Oświadczenie stanowi Załącznik nr 1 do niniejszego pisma**.

4.	**PYT:** Czy integracja z systemem SIEM ma być wykonana od razu przy wdrożeniu modelu SaaS czy dopiero po migracji na infrastrukturę Zamawiającego?
	ODP: Zamawiający wymaga integracji z systemem SIEM zarówno przy wdrożeniu modelu SaaS jak i po migracji na infrastrukturę Zamawiającego.
5.	**PYT:** W jaki sposób możliwa jest integracja z systemem SIEM Zamawiającego? Czy dostęp ten jest możliwy w publicznym Internecie czy tylko z użyciem połączenia VPN do infrastruktury Zamawiającego?
	ODP: Zamawiający dopuszcza integrację z systemem SIEM Zamawiającego wyłącznie z użyciem połączenia VPN do infrastruktury Zamawiającego.
6.	**PYT:** Czy HSM ma zostać wdrożony w modelu SaaS czy już po migracji na infrastrukturę Zamawiającego?
	ODP: Zamawiający wymaga, aby HSM został wdrożony w modelu SaaS (jak również po przeniesieniu na infrastrukturę Zamawiającego). W przypadku modelu SaaS Zamawiający dopuszcza możliwość wykorzystania HSM dostawcy rozwiązania chmurowego / SaaS.
7.	**PYT:** Czy jako moduł HSM może zostać użyta usługa Azure Dedicated HSM? Jeśli nie i dopuszczalny jest tylko HSM z infrastruktury Grupy ENEA, czy system już w modelu SaaS ma z niego korzystać, np. z użyciem site-to-site VPN?
	ODP: W przypadku modelu SaaS Zamawiający dopuszcza możliwość wykorzystania HSM dostawcy rozwiązania chmurowego / SaaS – np. jako moduł HSM może zostać użyta usługa Azure Dedicated HSM.
8.	**PYT:** Jak stosować zapis "Wszelkie komponenty sprzętowe i software'owe stosowane przez Wykonawcę na potrzeby świadczenia usługi posiadają Wsparcie producenta i mają na bieżąco instalowane po-prawki bezpieczeństwa" w przypadku infrastruktury typu Cloud, np. Microsoft Azure? Wykonawca nie ma w tym miejscu pełnej kontroli nad aktualizacjami oprogramowania komponentów, ale zapewnienie aktualizacji i standardów bezpieczeństwa spoczywa na dostawcy chmury.
	ODP: Zamawiający wymaga, aby Wykonawca posiadał stosowne zapisy w umowie z dostawcą infrastruktury typu Cloud np. Microsoft Azure. Wykonawca ponosi pełną odpowiedzialność za działania i zaniechania podwykonawców jak za swoje własne.
9.	**PYT:** Jak rozumieć zapis "System nie przechowuje i do czasu migracji na Infrastrukturę Grupy ENEA nie będzie przechowywał adresów mailowych użytkowników z Grupy ENEA" w przypadku, gdy System autoryzuje użytkowników na podstawie adresów e-mail? W tym przypadku pracownicy obsługujący system otrzymają e-mailowe powiadomienia np. w przypadku nowego zgłoszenia awarii stacji ładowania.
	ODP: Zamawiający wymaga zastosowania innej metody uwierzytelniania niż adresy mailowe. W przypadku braku skorzystania z innej metody uwierzytelniania, Zamawiający zastosuje anonimizację adresów mailowych użytkowników z Grupy ENEA.
10.	**PYT:** Czy i w jaki sposób, System będzie miał uzyskać dostęp do danych pracowników w zakresie kart PKI, przy wdrożeniu w modelu SaaS?
	ODP: Zamawiający wymaga zapewnienia przez System wieloskładnikowego uwierzytelnienie w oparciu o certyfikaty i klucze prywatne użytkowników Grupy ENEA przechowywane na kartach PKI Grupy ENEA. Wykonawca powinien zapewnić możliwość integracji poprzez import certyfikatów Urzędów Certyfikacji PKI Grupy ENEA. Przykładowym sposobem realizacji wymogu jest wykorzystanie mechanizmu uwierzytelniającego serwera WWW w oparciu o certyfikaty x509.
11.	**PYT:** Pytanie dotyczące punktów "Panel logowania do systemu zarządzającego nie może być dostępny z sieci Internet. Dostęp do panelu logowania dla pracowników obsługujących system tylko przez VPN" oraz "Do panelu klienta dostępnego od strony Internetu mogą mieć dostęp tylko użytkownicy ładowanych pojazdów, każda próba uwierzytelnienia przez użytkownika obsługującego system w panelu dostępnym przez Internet jest zgłaszana Zamawiającemu jako incydent bezpieczeństwa": Czy akceptowany jest scenariusz, w którym system udostępnia jeden panel do logowania dostępny z sieci Internet dla wszystkich użytkowników i na etapie logowania ogranicza zakres dostępów? Jeśli panel logowania dla pracowników obsługujących system ma być bezwzględnie dostępny tylko przez VPN, czy System w modelu SaaS ma zostać połączony z VPNem Grupy ENEA?

	ODP: Zamawiający podtrzymuje wymaganie. Nie jest akceptowalny zaproponowany scenariusz. Panel logowania dla pracowników obsługujących system ma być bezwzględnie dostępny tylko przez VPN. System w modelu SaaS ma zostać połączony z VPNem Grupy ENEA.
12.	**PYT:** Czy szyfrowanie SSL będzie wystarczającym rozwiązaniem dla poniższych punktów? ● "W przypadku uwierzytelniania z aplikacji mobilnej, aplikacja zapewnia uwierzytelnianie przy użyciu certyfikatu x509 wygenerowanego dla użytkownika lub innego klucza wygenerowanego w aplikacji i przechowywanego w bezpieczny sposób na urządzeniu Klienta" ● Wymagania bezpieczeństwa dotyczące aplikacji mobilnej : a. cała komunikacja pomiędzy aplikacją, a serwerem jest szyfrowana, b. system chroni przed atakami typu MiTM, c. aplikacja weryfikuje poprawność certyfikatu serwera, d. serwer weryfikuje poprawność certyfikatu/klucza, przypisanego do danego Klienta, którym posługuje się aplikacja mobilna w celu uwierzytelnienia, e. każdy pakiet przesyłany pomiędzy aplikacją i serwerem w dowolnym kierunku jest podpisywany i szyfrowany, f. w celu umożliwienia prowadzenia testów bezpieczeństwa, aplikacja i serwer mają zaimportowane certyfikaty Urzędów Certyfikacji systemu PKI Zamawiającego,
	ODP: Szyfrowanie TLS 1.2 (i wyższe) uwzględniające powyższe wymagania będzie wystarczającym rozwiązaniem.
13.	**PYT:** Czym jest obsługa Incydentów Bezpieczeństwa opisana w punkcie "Wykonawca zapewni obsługę Incydentów Bezpieczeństwa systemu, zarówno po stronie Infrastruktury Wykonawcy, jak również po stronie Klientów WEB i mobilnych, a także po stronie Stacji Ładowania Pojazdów. Wszelkie incydenty bezpieczeństwa będą zgłaszane do Zamawiającego"? Czy wystarczający jest opis, w Dokumentacji, procedur stosowanych w przypadku wystąpienia ww. incydentów?
	ODP: Zamawiający wymaga dokumentacji (np. procedur, instrukcji) i postępowania zgodnie z zapisami normy ISO/IEC 27001:2013 załącznik A pkt. A.16.
14.	**PYT:** Nie ma w standardzie OCPP komunikatu związanego z otwarciem obudowy urządzenia, wspomnianego w punkcie "Stacje ładowania pojazdów przy użyciu protokołu OCCP wysyłają alarmy o otwarciu obudowy, lub o próbach siłowych sforsowania zabezpieczeń fizycznych". Jak System ma obsługiwać takie zdarzenia? Proszę o wskazanie konkretnych poleceń OCPP, które System powinien tutaj wspierać.
	ODP: Zamawiający posiada stacje, które wysyłają dodatkowe komunikaty nie zawarte w standardzie za pośrednictwem protokołu OCCP v. 1.6. Dokumentacja we wskazanym zakresie zostanie przekazana na etapie wdrożenia Systemu.
15.	**PYT:** Jakie parametry środowiskowe od stacji ładowania mają zostać przekazane do systemu SIEM w zakresie punktu "Stacje ładowania pojazdów przy użyciu protokołu OCCP informują o parametrach środowiskowych"? Większość parametrów zwracanych przez stacje związana jest z parametrami elektrycznymi.
	ODP: Zamawiający posiada stacje, które wysyłają dodatkowe komunikaty nie zawarte w standardzie za pośrednictwem protokołu OCCP v. 1.6. Dokumentacja we wskazanym zakresie zostanie przekazana na etapie wdrożenia Systemu. Przykładowym parametrem jest temperatura.
16.	**PYT:** Jak udowodnić spełnienie wymagań związanych z zabezpieczeniami fizycznymi w przypadku użycia usług chmurowych przy wdrożeniu Systemu w modelu SaaS, np. Microsoft Azure lub Google Cloud?
	ODP: Zamawiający wymaga, aby Wykonawca posiadał stosowne zapisy w umowie z dostawcą infrastruktury typu Cloud/SaaS. Wykonawca ponosi pełną odpowiedzialność za działania i zaniechania podwykonawców jak za swoje własne. Zamawiający wymaga złożenia wraz z ofertą Załącznika nr 9 do Warunków Zamówienia - Oświadczenie o spełnieniu minimalnych wymagań w zakresie stosowanych zabezpieczeń technicznych i organizacyjnych dotyczących ochrony danych osobowych osób fizycznych.
17.	**PYT:** Czy definicja „awarii systemu" opisana w pkt 9 pkt 2 e, zawiera w sobie awarię „procesora płatności"?

	ODP: Przez Incydent będący Awarią Systemu, który jest błędem w procesie płatności należy rozumieć błąd wynikający z nieprawidłowego funkcjonowania Systemu. W przypadku, gdy przyczyną błędu jest usługa operatora płatności, Zamawiający oczekuje od Wykonawcy komunikacji z operatorem płatności, dążącej do rozwiązania Incydentu. Wykonawca odpowiada za działania podwykonawców w pełnym zakresie jak za swoje własne działania.
18.	**PYT:** Zapis w pkt 4.7.2.Wykonawca jest odpowiedzialny za zapewnienie usługi operatora płatności; prawdopodobnie powinien być zamieniony na „Wykonawca jest odpowiedzialny za zapewnienie integracji usługi operatora płatności". Inaczej wykonawca oprócz dostarczenia systemu przejmuje na siebie formalne obowiązki dostawcy usług płatniczych.
	ODP: Zamawiający dokonuje zmiany zapisu w Ogólnym Opisie Przedmiotu Zamówienia: **pkt. 8 Wymagania Funkcjonalne:** Było: *„Wykonawca jest odpowiedzialny za zapewnienie usługi operatora płatności"* Jest: *„Wykonawca jest odpowiedzialny za zapewnienie usługi operatora płatności – Wykonawca może korzystać z usług operatora płatności na zasadach podwykonawstwa lub wykorzystania zasobów podmiotów trzecich w tym integracji operatorem płatności."*
19.	**PYT:** Czy możliwym jest uszczegółowienie zapisów o Awarii i Błędach w ramach kategorii „krytyczne i niekrytyczne"?
	ODP: Zamawiający dokonuje zmiany zapisu w Projekcie Umowy §9 ust. 2 pkt. e: **Kategoria Awaria** Było: *„w przypadku awarii Systemu uniemożliwiającej świadczenie usług ładowania czas reakcji 2 godziny, czas naprawy do 8 godzin"* Jest: *„w przypadku awarii Systemu uniemożliwiającej świadczenie usług ładowania czas reakcji 2 godziny, czas naprawy do 8 godzin. Awaria to rodzaj Incydentu oznaczający sytuację, w której nie działa jedna lub więcej kluczowych funkcjonalności Systemu."* **Kategoria Błąd** Było: *„w przypadku pozostałych błędów (nie zakłócających bezpośrednio procesu ładowania – świadczenia usługi dla użytkowników końcowych) czas reakcji 2 godziny, czas naprawy do 48 godzin."* Jest: *„w przypadku pozostałych błędów (nie zakłócających bezpośrednio procesu ładowania – świadczenia usługi dla użytkowników końcowych) czas reakcji 2 godziny, czas naprawy do 48 godzin. Błąd to rodzaj Incydentu polegający na nieprawidłowym funkcjonowaniu dowolnego komponentu Systemu (nieprawidłowe działanie funkcji lub grupy funkcji) nie będącego kluczową funkcjonalnością Systemu."* Kluczowe funkcjonalności Systemu zostaną określone na etapie przygotowania Koncepcji Biznesowej Systemu.

Z poważaniem

Signed by / Podpisano przez:
Adrianna Targalska
Date / Data:
2021-04-29 15:13

Otrzymują:
1) Wykonawcy – na stronę www.enea.pl/bip/zamowienia (Nowa Platforma Zakupowa),
2) a/a

ENEA Centrum sp. z o.o.
Ul. Górecka 1
60-201 Poznań

NIP 777 00 02 843
REGON 630770227
www.enea.pl

ZAŁĄCZNIK NR 1 DO PISMA O SYG. DL/LZ/AT/2021/773

OŚWIADCZENIE WYKONAWCY O ZACHOWANIU POUFNOŚCI

(pieczęć Wykonawcy)

Dostawa i wdrożenie systemu służącego do obsługi i zarządzania stacjami ładowania pojazdów elektrycznych wraz z modułem rozliczeniowym

Niniejszym oświadczam(-y), że zobowiązuję (-emy) się wszelkie informacje stanowiące tajemnicę przedsiębiorstwa[1] Zamawiającego, przekazane lub udostępnione przez Zamawiającego w ramach prowadzonego postępowania o udzielenie zamówienia, wykorzystywać jedynie do celów uczestniczenia w niniejszym postępowaniu, nie udostępniać osobom trzecim, nie publikować w jakiejkolwiek formie w całości ani w części, lecz je zabezpieczać i chronić przed ujawnieniem. Ponadto zobowiązuję (-emy) się je zniszczyć, wraz z koniecznością trwałego usunięcia z systemów informatycznych, natychmiast po zakończeniu niniejszego postępowania, chyba, że nasza Oferta zostanie wybrana i Zamawiający pisemnie zwolni mnie (nas) z tego obowiązku.

Obowiązki te mają charakter bezterminowy.

Miejscowość i data	Pieczęć imienna i podpis przedstawiciela(i) Wykonawcy

[1] Za tajemnicę przedsiębiorstwa **Zamawiającego** uznaje w szczególności informacje dotyczące działalności gospodarczej **Zamawiającego**, informacje organizacyjne, finansowe, prawne, handlowe, marketingowe, produkcyjne, operacyjne, techniczne oraz technologiczne.