PKP INTERCITY S.A.
Biuro Teleinformatyki
02-305 Warszawa
Aleje Jerozolimskie 142A

BST-P6/076/41/2022

Warszawa, dnia 2022-10-24

Dot.: *PAM (Privileged Access Management)*

ZAPYTANIE O INFORMACJĘ

Zwracamy się do Państwa z prośbą o udzielenie informacji cenowej dotyczącej dostarczenia licencji, świadczenia usługi wraz ze wsparciem i szkoleniem, opartej na rozwiązaniu typu *PAM (Privileged Access Management) umożliwiającym monitorowanie i nagrywanie sesji zdalnych*, zgodnie z wymaganiami zawartymi w Tabeli nr 1.

I. Wprowadzenie:

PKP Intercity S.A. rozpoczęło proces rozpoznania rynku na okoliczność ewentualnego wyboru dostawcy licencji oraz świadczenia usługi wraz ze wsparciem i szkoleniem opartej na rozwiązaniu typu *PAM (Privileged Access Management)* umożliwiającym monitorowanie i nagrywanie sesji zdalnych, opcjonalnie jako:

A. „virtual appliance"

Przez *„virtual appliance"*, Zamawiający rozumie specjalizowane rozwiązanie, mające postać maszyny wirtualnej w ramach, którego zainstalowana jest całość oprogramowania (system operacyjny, baza danych, aplikacja), realizujące funkcjonalności systemu PAM dostarczonym przez Dostawcę;

B. „physical appliance"

Przez *„physical appliance"*, Zamawiający rozumie specjalizowane rozwiązanie, mające postać fizycznego urządzenia w ramach którego zainstalowana jest całość oprogramowania (system operacyjny, baza danych, aplikacja), realizujące funkcjonalności systemu PAM dostarczonym przez Dostawcę;

Oznaczenie zapytania, na które należy się powoływać we wszelkich kontaktach: *„Usługa rozwiązanie typu PAM (Privileged Access Management*) – *system umożliwiający monitorowanie i nagrywanie sesji zdalnych."*

Tabela nr 1 – wymagania

II. Opis przedmiotu zapytania	**Spełnia wymagania Tak☑Nie☐**
Przedmiotem zapytania jest zaproponowanie szacowanej ceny za dostawę licencji oraz usługę wraz ze wsparciem oraz szkoleniem opartej na rozwiązaniu typu *PAM (Privileged Access Management)* umożliwiającym monitorowanie i nagrywanie sesji zdalnych, z uwzględnieniem terminu wdrożenia usługi do 30 dni roboczych.	
1. Usługa wraz z opisem oferowanego rozwiązania powinna zapewniać	
1.1. Monitoring i rejestrację zdalnych sesji do systemów teleinformatycznych IC; 1.2. Uniemożliwiać ryzyko zatarcia śladów niepożądanych działań, dokonanych przez zdalnych użytkowników; 1.3. nagrywanie sesji, aktywne monitorowanie ruchu w sieci i rejestrowanie sesji dostępu SSH, RDP oraz VNC, zaś w przypadku zauważenia niepokojących działań, dawać możliwość zablokowania sesji danego użytkownika, lub całkowitego zerwania połączenia i odebrania praw dostępu; 1.4. śledzenie trwających sesji dostępu z poziomu przeglądarki internetowej i uniemożliwiać ryzyko zatarcia śladów niepożądanych działań, dokonanych przez zdalnych użytkowników; 1.5. możliwość udostępnienia nagrań materiałów dowodowych; 1.6. rozwiązanie powinno być nowoczesne, bezpieczne i przydatne dla IC z zapewnieniem wsparcia technicznego przez okres opcjonalnie 24 lub 36 miesięcy; 1.7. elementy dostarczone w ramach zakupu muszą być fabrycznie nowe; 1.8. elementy dostarczone w ramach zakupu muszą pochodzić z autoryzowanego kanału dystrybucyjnego dedykowanego na rynek polski.	1.1. ☐ 1.2. ☐ 1.3. ☐ 1.4. ☐ 1.5. ☐ 1.6. ☐ 1.7. ☐ 1.8. ☐
2. Architektura	
2.1. System PAM opcjonalnie powinien mieć postać: 2.1.1. zamkniętej platformy fizycznej *(„physical appliance"),* do implementacji w infrastrukturze Zamawiającego lub postać zamkniętej platformy wirtualnej;	2.1. ☐ 2.2. ☐ 2.3. ☐ 2.4. ☐

2.1.2. zamkniętej platformy wirtualnej *(„virtual appliance"),* do implementacji w ramach środowiska wirtualnego Zamawiającego. 2.2. *Physical appliance* musi istnieć w liniach produktowych producenta systemu PAM; 2.3. *Physical appliance* musi zapewnić redundancję na poziomie zasilania oraz dysków wewnętrznych; 2.4. System PAM musi być zbudowany w architekturze wysokiej dostępności, przez co Zamawiający rozumie, że rozwiązanie ma możliwość konfiguracji klastrowej i działania w trybie multi-master (preferowany) lub master-slave; 2.5. Infrastruktura systemu PAM musi mieć nadmiarowość, która zapewni pełną dostępność danych Zarządzanych przez system PAM w przypadku dowolnej pojedynczej awarii sprzętowej 2.6. (wymóg ten nie stosuje się do nagranych przez system PAM sesji użytkowników) zarządzanych przez system w przypadku awarii dowolnego (jednego z dwóch) data center Zamawiającego (wymóg ten nie stosuje się do nagranych przez system PAM sesji użytkowników); 2.7. System PAM musi zapewnić możliwość wykonania odtworzenia całości i/lub części systemu PAM z kopii bezpieczeństwa w przypadku awarii systemu PAM w lokalizacji Zamawiającego (Disaster Recovery); 2.8. System PAM musi zarządzać kontami na systemach docelowych w modelu bezagentowym; 2.9. Rozwiązanie nie wymaga instalowania dodatkowego oprogramowania (agentów) na monitorowanych serwerach; 2.10. Interfejs użytkownika systemu PAM musi być dostępny przez przeglądarkę internetową. 2.11. Administrowanie, monitorowanie oraz podgląd sesji odbywa się poprzez przeglądarkę dedykowanej pojedynczej konsoli zarządzania.	2.5. ☐ 2.6. ☐ 2.7. ☐ 2.8. ☐ 2.9. ☐ 2.10. ☐ 2.11. ☐
3. W ramach świadczenia usług wsparcia technicznego Dostawca zapewni	
3.1. Posiadanie autoryzacji producenta do świadczenia usługi i serwisu dla oferowanych rozwiązań, gwarancję oraz wsparcie producenta rozwiązania na czas trwania umowy tj. opcjonalnie 24 lub 36 miesięcy, licząc od dnia podpisania protokołu odbioru; 3.2. Czas reakcji dla Awarii sprzętu (rozumianej jako uszkodzenie lub nieprawidłowe działanie dowolnego elementu i/lub komponentu sprzętowego) <= 4 godziny, to okres od chwili przyjęcia i zarejestrowania zgłoszenia do czasu rozpoczęcia realizacji zgłoszenia; 3.3. Czas reakcji dla Awarii (rozumianej jako całkowita niedostępność systemu PAM, cykliczne zawieszanie się systemu PAM lub spadek wydajności systemu PAM poniżej 50% nominalnej wydajności) <= 1 godzina lub błędu (funkcjonowanie systemu PAM niezgodne z dokumentacją, w szczególności działanie ograniczające funkcjonalność lub wydajność lub pojemność systemu PAM); 3.4. Czas reakcji dla Usterki (wada inna niż Awaria i Błąd) <= 4 godziny to okres od chwili przyjęcia i zarejestrowania zgłoszenia do czasu rozpoczęcia realizacji zgłoszenia 3.5. Czas skutecznej naprawy gwarancyjnej awarii lub błędu sprzętowego - 24 godziny od momentu zgłoszenia; 3.6. Czas wymiany uszkodzonego sprzętu - do 24 godzin od momentu zgłoszenia, 3.7. Dostęp do nowych wersji oprogramowania; 3.8. Przyjmowanie zgłoszeń serwisowych realizowane w godzinach od 7:00 do 18:00 w dni robocze, od poniedziałku do piątku, o ile w opisie usługi nie zaznaczono inaczej; 3.9. Usługi serwisowe sprawowane w godzinach od 7:00 do 18:00 w dni robocze, od poniedziałku do piątku, o ile w opisie usługi nie zaznaczono inaczej; 3.10. Gwarantowany czas naprawy lub dostarczenia obejścia - zobowiązanie do zdiagnozowania i naprawienia wady we wskazanym czasie od zgłoszenia dla: 3.10.1.Awarii (definicja, patrz powyżej) <= 12 godzin; 3.10.2.Błędu (definicja, patrz powyżej) <= 5 dni roboczych; 3.10.3.Usterki (definicja, patrz powyżej) <= 90 dni roboczych. 3.11. Zakres wsparcia obejmuje także: konsultacje, warsztaty, asystę, wsparcie, wykonywanie zaawansowanych diagnostyk, migracji, upgrade'ów, instalacji, konfiguracji i innych prac serwisowych dla urządzeń i oprogramowania objętych umową; 3.12. Możliwość zgłoszenia realizowanego telefonicznie, poprzez e-mail lub automatyczny system obsługi zgłoszeń przez autoryzowany ośrodek serwisowy; 3.13. W przypadku uszkodzenia dysków dostarczenie nowego dysku wolnego od wad; 3.14. Dysk uszkodzony nie podlega wymianie i przechodzi na własność IC; 3.15. Dostęp do aktualizacji i baz wiedzy: 3.15.1.Dostęp do nowych wersji, aktualizacji i poprawek do oprogramowania 3.15.2.Licencje na użytkowanie i kopiowanie nowych wersji, aktualizacji i poprawek do oprogramowania	3.1. ☐ 3.2. ☐ 3.3. ☐ 3.4. ☐ 3.5. ☐ 3.6. ☐ 3.7. ☐ 3.8. ☐ 3.9. ☐ 3.10. ☐ 3.11. ☐ 3.12. ☐ 3.13. ☐ 3.14. ☐ 3.15. ☐

3.15.3. Dostęp do elektronicznych kanałów informacji i usług wsparcia (bazy wiedzy, bibliotek 3.15.4. Dostęp do dokumentacji, opisów produktów, specyfikacji, literatury technicznej i innych materiałów).	
4. W zakresie dodatkowej specyfikacji rozwiązanie powinno obejmować	
4.1. Rozwiązanie typu *„solution in a box”* - nie wymaga integracji z żadnym z istniejących elementów infrastruktury sieciowej;	4.1. ☐
4.2. Rozwiązanie pozwala na monitorowanie protokołów: RDP, VNC, SSH, TELNET, HTTP/HTTPS;	4.2. ☐
4.3. Rozwiązanie pozwala na kontrolę wykorzystania/dostępności funkcjonalności w protokołach RDP, SSH, VNC;	4.3. ☐
4.4. Rozwiązanie posiada możliwość uwierzytelniania do systemu monitorowania poprzez zewnętrzne serwery: Active Directory;	4.4. ☐
4.5. Rozwiązanie posiada możliwość uwierzytelniania do serwerów docelowych poprzez usługi katalogowe AD i LDAP, oraz lokalne uwierzytelnianie serwerów Windows i Linux, Unix;	4.5. ☐
4.6. System PAM musi zapewnić integrację z wykorzystywanym przez Zamawiającego systemem SIEM (Splunk) w zakresie przekazywania logów audytowych;	4.6. ☐
4.7. System PAM musi zapewnić integrację z wykorzystywanym przez Zamawiającego systemem monitoringu (Zabbix) w zakresie monitorowania podstawowych parametrów pracy systemu PAM;	4.7. ☐
4.8. System PAM musi udostępniać API pozwalające na realizację podstawowych funkcjonalności systemu PAM;	4.8. ☐
4.9. Poświadczenia przechowywane w systemie monitorującym muszą być zabezpieczone przed niepowołanym dostępem;	4.9. ☐
4.10. W rozwiązaniu analiza i rejestracja sesji dla RDP, SSH, VNC odbywa się na urządzeniu lub na zasobie „virtual appliance”;	4.10. ☐
4.11. Rozwiązanie nagrywa cały ruch sieciowy związany z daną sesją;	4.11. ☐
4.12. Rozwiązanie pozwala na selektywne nagrywanie elementów sesji;	4.12. ☐
4.13. Rozwiązanie umożliwia podmianę loginu i hasła wprowadzonego przez użytkownika na inny, znany na systemie docelowym;	4.13. ☐
4.14. W rozwiązaniu podgląd monitorowanych sesji (zarówno “na żywo” jak i wcześniej nagranych) nie wymaga instalowania dodatkowego oprogramowania;	4.14. ☐
4.15. W rozwiązaniu obraz podglądu sesji jest dynamicznie budowany w dowolnej przeglądarce z zachowanych danych sesji (nie jest to odtwarzanie statycznego zapisu wideo);	4.15. ☐
4.16. W rozwiązaniu, dla zapisanych sesji terminalowych (np. telnet, ssh) istnieje możliwość interakcji z tekstem (np. copy & paste);	4.16. ☐
4.17. Dla protokołów RDP, VNC, SSH, TELNET, rozwiązanie pozwala na uzyskanie dostępu do grupy monitorowanych serwerów poprzez jeden adres sieciowy (jedną parę IP i port). Nazwa docelowego serwera jest wskazywana w nazwie użytkownika przy użyciu separatora, np. 'ssh -l user#mailserv nazwa-serwera’;	4.17. ☐
4.18. Rozwiązanie umożliwia tagowanie i komentowanie przeglądanych sesji;	4.18. ☐
4.19. Rozwiązanie umożliwia przerwanie monitorowanej sesji;	4.19. ☐
4.20. Rozwiązanie umożliwia chwilowe wstrzymanie i wznowienie sesji;	4.20. ☐
4.21. Rozwiązanie umożliwia proaktywny monitoring, powodujący przerwanie sesji oraz alert do administratora po wykryciu zadanych komend lub ciągu znaków;	4.21. ☐
4.22. Rozwiązanie umożliwia kontekstowe przeszukiwanie zachowanej sesji;	4.22. ☐
4.23. Rozwiązanie umożliwia wyszukiwania tekstu w sesjach graficznych (np. RDP);	4.23. ☐
4.24. Rozwiązanie umożliwia dołączenie się administratora do sesji telnet, SSH, RDP, VNC z poziomu przeglądarki (np. dla wprowadzenia hasła, wpisanie polecenia systemowego);	4.24. ☐
4.25. Rozwiązanie ma możliwość monitorowania, raportowania oraz analizy aktywności użytkownika podczas sesji (np. dla oceny produktywności i/lub kontroli stopnia zaangażowania i rozliczeń z firmą zewnętrzną);	4.25. ☐
4.26. Rozwiązanie pozwala na współpracę z rozwiązaniem Microsoft RD Connection Broker;	4.26. ☐
4.27. Rozwiązanie posiada wsparcie dla klawiatury polskiej, niemieckiej i angielskiej w GUI i przy podłączaniu się do sesji z poziomu przeglądarki;	4.27. ☐
4.28. Rozwiązanie posiada scentralizowaną listę zasobów (portal użytkownika), która umożliwia zainicjowanie połączenia za pomocą dedykowanego klienta protokołu, z automatycznie uzupełnianymi danymi logowania;	4.28. ☐
4.29. Rozwiązanie umożliwia synchronizację z serwerem NTP wskazanym przez Zamawiającego oraz znakowanie czasem zapisanych sesji;	4.29. ☐
	4.30. ☐
	4.31. ☐
	4.32. ☐
	4.33. ☐
	4.34. ☐
	4.35. ☐
	4.36. ☐
	4.37. ☐
	4.38. ☐
	4.39. ☐
	4.40. ☐

4.30. Rozwiązanie zapewnia bezpieczeństwo i ochronę kryptograficzną wszystkich zapisanych danych, zapewniać poufność i integralność informacji: 4.31. Komunikacja między wszystkimi elementami systemu do uprzywilejowanego dostępu zdalnego (tj. oprogramowaniem uprzywilejowanego dostępu zdalnego oraz serwerami proxy) musi być szyfrowana (TLS) i odbywać się na jednym porcie 443; 4.32. System PAM musi zapewniać szyfrowanie haseł systemów docelowych przechowywanych przez system PAM, przy czym siła szyfrowania musi być na poziomie AES-256; 4.33. System PAM musi zapewniać szyfrowanie kopii bezpieczeństwa systemu, przy czym siła szyfrowania musi być na poziomie AES-256; 4.34. System musi być certyfikowany na zgodność ze standardem FIPS 140 Level 2 (lub wyższym) lub Common Criteria EAL4+ (lub wyższym); 4.35. W rozwiązaniu klucze szyfrujące używane do ochrony kryptograficznej muszą mieć możliwość przechowywania poza systemem; 4.36. Rozwiązanie posiada min. 10TB przestrzeni na dane; 4.37. Rozwiązanie posiada min. 2 interfejsy sieciowe z możliwością rozszerzenia do obsługi min. 50 jednoczesnych sesji graficznych; 4.38. Rozwiązanie obsługuje VLAN' y; 4.39. Rozwiązanie posiada wsparcie techniczne; 4.40. Liczba licencji opcjonalnie 300, 400 lub 500 na użytkowników jednoczesnych oraz serwery.	
5. Dodatkowe wymagania	
5.1. Wykonawca przez cały okres trwania umowy musi mieć aktywną umowę o poufności NDA z Zamawiającym; 5.2. Wykonawca oprócz zapewnienia pełnego wsparcia na czas trwania umowy przeprowadzi dla pracowników niezbędne szkolenia w zakresie samodzielnego administrowania i eksploatacji systemu; 5.3. Na żądanie i zlecenie, pod kontrolą PKP IC, Wykonawca dokona trwałego usunięcia i kasowania informacji i zapisów pozyskanych w trakcie wykonywania usługi, co zostanie potwierdzone protokołem; 5.4. W momencie dostarczenia rozwiązania innego niż posiada Zamawiający, wykonawca dokona migracji konfiguracji zasobów z istniejącego systemu PAM; 5.5. W przypadku rozwiązania *„virtual appliance"* na infrastrukturze Zamawiającego, Dostawca określi dla systemu min. wymagania i zasoby (CPU, RAM, dysk, liczba I/O, itd.); 5.6. Zamawiający nie dopuszcza rozwiązania opartego o publiczną chmurę; 5.7. System ma być dostarczony w polskiej wersji językowej (zarówno menu konfiguracyjne systemu jak i interfejs klientów za pomocą, których realizowane są sesje); 5.8. Raporty dotyczące przeprowadzonych sesji muszą podlegać filtrowaniu co najmniej w zakresie daty, nazwy użytkownika, nazwy / adresu IP zarządzanego zasobu; 5.9. System powinien umożliwiać tworzenie dedykowanych raportów; 5.10. Migracja konfiguracji z istniejącego systemu PAM.	5.1. ☐ 5.2. ☐ 5.3. ☐ 5.4. ☐ 5.5. ☐ 5.6. ☐ 5.7. ☐ 5.8. ☐ 5.9. ☐ 5.10. ☐
6. Organizacja szkoleń	
6.1. Szkolenia administratorów PAM w liczbie 4, będą przeprowadzone w terminie uzgodnionym z PKP Intercity S.A.; 6.2. Szkolenia odbędą się w autoryzowanym ośrodku producenta oprogramowania i zakończą się uzyskaniem niezbędnych certyfikatów dla administratorów Zamawiającego; 6.3. Zakres szkolenia musi uwzględniać: 6.3.1. Ogólną architekturę systemu PAM; 6.3.2. Bezpieczeństwo systemu PAM 6.3.3. Konfigurację kont systemów docelowych w systemie PAM 6.3.4. Zarządzanie użytkownikami w systemie PAM i integracja z innymi mechanizmami 6.3.5. uwierzytelniania i autoryzacji 6.3.6. Polityki złożoności hasła, harmonogram zmian haseł, walidacja poprawności zmiany hasła 6.3.7. Zarządzanie sesjami w systemie PAM 6.3.8. Zarządzanie schematami wnioskowania i akceptacji dostępu do hasła i/lub sesji w systemie PAM 6.3.9. Auditing i raportowanie w systemie PAM. 6.3.10. Certyfikat ukończenia szkolenia w zakresie administrowania PAM.	6.1. ☐ 6.2. ☐ 6.3. ☐

III. ODPOWIEDŹ POWINNA ZAWIERAĆ:

1. Brak lub szczegółowe potwierdzenie spełnienia wymagań w Tabeli nr 1 (Tak☒ lub Nie☐)

2. Podanie czasu niezbędnego do wykonania usługi – najbliższa data możliwego wdrożenia usługi (liczona od czasu podpisania umowy).
3. Uzupełnienie szacowanych kosztów podanych w poniższej Tabeli nr 2 oraz nr 3.

Tabela nr 2 – szacowane koszty OPCJA A „virtual appliance"

Lp.	Nazwa usługi OPCJA A „virtual appliance"	j.m.	ilość	Cena jednostkowa	Wartość
				(PLN netto)	(PLN netto)
1	Licencje - System PAM (producent, model): ……..	sztuka	300		
2	Licencje - System PAM (producent, model): ……..	sztuka	400		
3	Licencje - System PAM (producent, model): ……..	sztuka	500		
4	Wdrożenie, uruchomienie do użytkowania oprogramowania monitorującego sesje zdalne	-	-		
5	Migracja konfiguracji z istniejącego systemu PAM	-	-		
6	Wsparcie techniczne przez okres trwania umowy 24 miesięcy	m-c	24		
7	Wsparcie techniczne przez okres trwania umowy 36 miesięcy	m-c	36		
8	Szkolenia pracowników dla 4 administratorów	-	4		
9	Czas realizacji wdrożenia, uruchomienia oraz migracji konfiguracji	dzień	…..		

Tabela nr 3 – szacowane koszty OPCJA B „physical appliance":

Lp.	Nazwa usługi OPCJA B „physical appliance":	j.m.	ilość	Cena jednostkowa	Wartość
				(PLN netto)	(PLN netto)
1	Licencje - System PAM (producent, model): ……..	sztuka	300		
2	Licencje - System PAM (producent, model): ……..	sztuka	400		
3	Licencje - System PAM (producent, model): ……..	sztuka	500		
4	Wdrożenie, uruchomienie do użytkowania sprzętu i oprogramowania monitorującego sesje zdalne	-	-		
5	Migracja konfiguracji z istniejącego systemu PAM	-	-		
6	Wsparcie techniczne przez okres trwania umowy 24 miesięcy	m-c	24		
7	Wsparcie techniczne przez okres trwania umowy 36 miesięcy	m-c	36		
8	Szkolenia pracowników dla 4 administratorów	-	4		
9	Czas realizacji wdrożenia, uruchomienia oraz migracji konfiguracji	dzień	…..		

IV. Terminy

Termin składania informacji upływa **w dniu 3 listopada 2022 r. o godzinie 12.00**
(ewentualne pytania prosimy kierować **do dnia 26 października 2022 r. do godziny 12:00**).

PKP INTERCITY S.A.
Biuro Teleinformatyki
02-305 Warszawa
Aleje Jerozolimskie 142A

Odpowiedź prosimy przesłać w formie e-mail na adres: it@intercity.pl

„PKP INTERCITY" S.A. zastrzega, że niniejsze zapytanie nie stanowi elementu jakiegokolwiek postępowania o udzielenie zamówienia, wobec czego PKP INTERCITY S.A. nie jest zobligowane do wyboru którejkolwiek oferty. Niniejsze pismo nie stanowi również oferty w rozumieniu Kodeksu Cywilnego.