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

Szanowni Państwo,
Poniżej znajdują się odpowiedzi na zadane pytania:

1. Jakie funkcje system Bilkom mają podlegać audytowi i dobrze się skalować?
   Odpowiedź:
   W zakres audytu wchodzi ocena możliwości rozwoju, wydajności oraz opcjonalnie bezpieczeństwa tego systemu.

2. Dla jakich elementów architektury systemu Bilkom należy ocenić skalowalność?
   Odpowiedź:
   Dla wszystkich elementów.

3. W jakich językach oraz przy pomocy jakich narzędzi został wytworzony kod źródłowy systemu Bilkom?
   Odpowiedź:
   JAVA : ok. 200 000 (głównie kod autorski), HTML: 50 000 (głównie kod autorski), JS: ok 2 000 (głównie biblioteki).

4. W przybliżeniu jaka jest ilość linii kodu źródłowego systemu Bilkom?
   Odpowiedź:
   JAVA : ok. 200 000 (głównie kod autorski), HTML: 50 000 (głównie kod autorski), JS: ok 2 000 (głównie biblioteki).

5. Ile serwisów www ma zostać objętych analizą podatności?
   Odpowiedź:
   Jeden serwis.

6. Ile formularzy użytkownika wchodzi w skład każdego z serwisów www, który ma zostać poddany analizie podatności?
   Odpowiedź:
   Tego typu szczegóły Zamawiający zostaną przekazane po podpisaniu stosownej umowy o zachowaniu poufności.

7. Ile profili użytkownika wchodzi w skład każdego z serwisów www, który ma zostać poddany analizie podatności?
   Odpowiedź:
   Serwis sprzedażowy: użytkownicy, Panel administracyjny: superuser, administratorzy przewoźników, administratorzy serwisu. Raporty: każdy z przewoźników.

8. Ile serwerów aplikacji i jakich ma zostać objętych analizą bezpieczeństwa konfiguracji?
   Odpowiedź:

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

Analizą bezpieczeństwa konfiguracji ma być objęte środowisko systemu składające się z 13 serwerów oraz 2 odpowiadających za logi.

9. Ile baz danych i jakich ma zostać objętych analizą bezpieczeństwa konfiguracji?
   Odpowiedź:
   Baza danych jest jedna - Postgresql.

10. Ile mechanizmów bezpieczeństwa i jakich ma zostać objętych analizą bezpieczeństwa konfiguracji?
    Odpowiedź:
    Analizą bezpieczeństwa konfiguracji ma być objęte 10 poniższych mechanizmów.
    Szerszy zakres zostanie niżej wskazanych mechanizmów udostępniony po podpisaniu stosownej umowy o zachowaniu poufności.
    1. **Weryfikacja uwierzytelnienia w aplikacji,**
    2. **Weryfikacja zarządzania sesją ,**
    3. **Weryfikacja kontroli dostępu,**
    4. **Weryfikacja pod kątem złośliwych danych wejściowych,**
    5. **Weryfikacja bezpieczeństwa obsługi logów,**
    6. **Weryfikacja mechanizmów ochrony danych,**
    7. **Wymagania do zabezpieczenia komunikacji,**
    8. **Weryfikacja bezpieczeństwa http,**
    9. **Weryfikacja zabezpieczeń przed złośliwym kodem,**
    10. **Bezpieczeństwo bazy danych.**

11. W jakiej technologii przygotowany jest kod źródłowy, który ma zostać poddany analizie (w podziale na front-end, back-end, warstwa integracji)?
    Odpowiedź:
    JAVA : ok. 200 000 (głównie kod autorski), HTML: 50 000 (głównie kod autorski), JS: ok 2 000 (głównie biblioteki).

12. Ile linii kodu ma zostać poddanych analizie?
    Odpowiedź:
    JAVA : ok. 200 000 (głównie kod autorski), HTML: 50 000 (głównie kod autorski), JS: ok 2 000 (głównie biblioteki).

13. Wykonania jakich czynności oczekują Państwo w ramach "analizy powykonawczej"?
    Odpowiedź:
    Zamawiający w ramach analizy powykonawczej oczekuje wniosków oraz rekomendacji jednoznacznie oceniających system w zakresie będącym przedmiotem audytu.

14. Jakie certyfikaty uznają Państwo za równoważne wobec certyfikatu OSCP?

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

Odpowiedź:
GPEN, GMOB, eWAPT, ECSA, GWAPT.

15. Jakie certyfikaty uznają Państwo za równoważne wobec certyfikatu OSCE?
Odpowiedź:
GPEN, GMOB, eWAPT, ECSA, GWAPT.

16. Jaki system SCM (Source Code Management)/Version Control jest wykorzystywany?
Odpowiedź:
W PKP IC wykorzystywany jest Gitlab.

17. Jaka jest architektura aplikacji? Czy jest to monolit czy system modułowy?
Odpowiedź:
Aplikacja jest modułowa.

18. Czy jest to system pudełkowy (wraz z lokalnymi modyfikacjami) czy system zbudowany od zera przez PKP Informatyka?
Odpowiedź:
Jest to system zbudowany przez PKP Informatykę, nie jest to rozwiązanie pudełkowe.

19. Czy kod źródłowy systemu jest zmodularyzowany czy utrzymywany jako jedno pojedyncze repozytorium?
Odpowiedź:
Tego typu szczegóły Zamawiający zostaną przekazane po podpisaniu stosownej umowy o zachowaniu poufności.

20. Jakim narzędziem system jest budowany z kodu źródłowego?
Odpowiedź:
Tego typu szczegóły Zamawiający zostaną przekazane po podpisaniu stosownej umowy o zachowaniu poufności.

21. Jakie integracje zewnętrzne (rodzaj i ilość) posiada system Bilkom?
Odpowiedź:
Tego typu szczegóły Zamawiający zostaną przekazane po podpisaniu stosownej umowy o zachowaniu poufności.

22. Jakie integracje wewnętrzne (rodzaj i ilość) posiada system Bilkom?
Odpowiedź:
Tego typu szczegóły Zamawiający zostaną przekazane po podpisaniu stosownej umowy o zachowaniu poufności.

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

23. Jakie technologie integracyjne są wykorzystywane?
    Odpowiedź:
    Tego typu szczegóły Zamawiający zostaną przekazane po podpisaniu stosownej umowy o zachowaniu poufności.

24. Czy obecnie wykorzystywane są jakiekolwiek narzędzia do statycznej analizy kodu? Jeśli tak, to jakie?
    Odpowiedź:
    Tego typu szczegóły Zamawiający zostaną przekazane po podpisaniu stosownej umowy o zachowaniu poufności.

25. W jakiej formie utrzymywana jest dokumentacja techniczna systemu (Word, Confluence, inny)?
    Odpowiedź:
    Dokumentacja techniczna jest utrzymywana w Word.

26. Ile linii kodu zostało wytworzonych przez PKP Informatyka?
    Odpowiedź:
    Tego typu szczegóły Zamawiający zostaną przekazane po podpisaniu stosownej umowy o zachowaniu poufności.

27. Ile encji znajduje się w bazie danych?
    Odpowiedź:
    Tego typu szczegóły Zamawiający zostaną przekazane po podpisaniu stosownej umowy o zachowaniu poufności.

28. Jaki system jest używany do monitorowania błędów w systemie?
    Odpowiedź:
    Tego typu szczegóły Zamawiający zostaną przekazane po podpisaniu stosownej umowy o zachowaniu poufności.

29. Od jak dawna system jest rozwijany?
    Odpowiedź:
    Tego typu szczegóły Zamawiający zostaną przekazane po podpisaniu stosownej umowy o zachowaniu poufności.

30. Jaka jest liczba programistów rozwijających system?
    Odpowiedź:
    Tego typu szczegóły Zamawiający zostaną przekazane po podpisaniu stosownej umowy o zachowaniu poufności.

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

31. Ile krytycznych incydentów produkcyjnych wydarzyło się w ostatnim półroczu?
    Odpowiedź:
    Tego typu szczegóły Zamawiający zostaną przekazane po podpisaniu stosownej umowy o zachowaniu poufności.

32. Jakimi rodzajami testów pokryte są funkcjonalności? Jednostkowe, integracyjne, automatyczne, inne?
    Odpowiedź:
    Tego typu szczegóły Zamawiający zostaną przekazane po podpisaniu stosownej umowy o zachowaniu poufności.

33. Czy wykorzystywane są narzędzia CI/CD (jeśli tak to jakie?) do uruchamiania testów jednostkowych/integracyjnych/automatycznych?
    Odpowiedź:
    Tego typu szczegóły Zamawiający zostaną przekazane po podpisaniu stosownej umowy o zachowaniu poufności.

34. Czy integracje wchodzące do systemu realizowane są przez ESB lub inną pośrednią warstwę czy bezpośrednio?
    Odpowiedź:
    Tego typu szczegóły Zamawiający zostaną przekazane po podpisaniu stosownej umowy o zachowaniu poufności.

35. Czy aplikacja posiada dedykowaną warstwę logiki biznesowej? Czy raczej logika biznesowa jest rozproszona w różnych warstwach w systemie (front-end, baza danych etc.)?
    Odpowiedź:
    Tego typu szczegóły Zamawiający zostaną przekazane po podpisaniu stosownej umowy o zachowaniu poufności.

36. Jak wygląda proces dostarczania kodu źródłowego?
    Odpowiedź:
    Tego typu szczegóły Zamawiający zostaną przekazane po podpisaniu stosownej umowy o zachowaniu poufności.

37. Czy przed wgraniem kodu do repozytorium wykonywane było Core Review?
    Odpowiedź:
    Tego typu szczegóły Zamawiający zostaną przekazane po podpisaniu stosownej umowy o zachowaniu poufności.

38. Czy dla rozwiązania Bilkom istnieją standardy deweloperskie dotyczące podziału kodu, nazewnictwa i wytyczne dla deweloperów piszących kod?

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

Odpowiedź:
Tego typu szczegóły Zamawiający zostaną przekazane po podpisaniu stosownej umowy o zachowaniu poufności.

39. Dotyczy punktu I 2.1.4 - Czy zastosowane frameworki są wytworzone wewnętrznie w ramach prac na systemem czy również użyte są frameworki ogólnodostępne (Open Source)? Jeśli OpenSource to jakie?
Odpowiedź:
Tego typu szczegóły Zamawiający zostaną przekazane po podpisaniu stosownej umowy o zachowaniu poufności.

40. Dotyczy punktu I 2.1.5 - Czy wykorzystywane biblioteki są wytworzone wewnętrznie w ramach prac nad systemem czy również użyte są biblioteki ogólnodostępne (Open Source)? Jeśli Open Source to jakie?
Odpowiedź:
Tego typu szczegóły Zamawiający zostaną przekazane po podpisaniu stosownej umowy o zachowaniu poufności.

41. Dotyczy punktu I 2.1.3 - Prośba o doprecyzowanie co kryje się pod "standardów"? Czy pod tym pojęciem kryją się też dobre praktyki?
Odpowiedź:
Zamawiający miał na myśli również dobre praktyki.

42. Jak wygląda proces utrzymania systemu? Czy robi to dostawca oprogramowania czy osobny podmiot?
Odpowiedź:
Tego typu szczegóły Zamawiający zostaną przekazane po podpisaniu stosownej umowy o zachowaniu poufności.

43. Czy środowisko do przeprowadzenia testów wydajnościowych jest zgodne z produkcją (podobna ilość serwerów, ich moc, konfiguracja, ilość danych w bazach, te same zintegrowane systemy, itd.)? Jeżeli nie, to na czym polegają różnice (jaki procent środowiska produkcyjnego stanowią w ilości serwerów, sumarycznej ilości CPU, RAM)?
Odpowiedź:
Tego typu szczegóły Zamawiający zostaną przekazane po podpisaniu stosownej umowy o zachowaniu poufności.

44. Czy bazy danych środowiska testowego są kopią produkcji (wolumen i rozkład danych jest podobny)? Jeżeli nie, to na czym polegają różnice (jaki procent ilości danych środowiska produkcyjnego stanowią)?
Odpowiedź:
Tego typu szczegóły Zamawiający zostaną przekazane po podpisaniu stosownej umowy o zachowaniu poufności.

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

45. Jaka jest orientacyjna ilość scenariuszy i kroków pokrywających główne ścieżki po których poruszają się użytkownicy (przez krok rozumiana jest pojedyncza interakcja użytkownika z systemem)?
Odpowiedź:
Tego typu szczegóły Zamawiający zostaną przekazane po podpisaniu stosownej umowy o zachowaniu poufności.

46. Czy dysponują Państwo biznesowym monitoringiem produkcji, który mierzy ilość i czas trwania poszczególnych kroków użytkownika w systemie, który mógłby zostać wykorzystany na potrzeby budowy modelu obciążeniowego?
Odpowiedź:
Tego typu szczegóły Zamawiający zostaną przekazane po podpisaniu stosownej umowy o zachowaniu poufności.

47. Czy na potrzeby testów możliwa będzie instalacja dodatkowych narzędzi do monitoring (darmowych, dostępnych na licencji „open-source”)?
Odpowiedź:
Na potrzeby testów będzie możliwa instalacja dodatkowych narzędzi do monitoringu pod nadzorem Zamawiającego.