POBIERANIE ORAZ AKTUALIZACJA DANYCH I INFORMACJI ZAWARTYCH W PROFILU KANDYDATA NA KIEROWCĘ

wersja 1.0

W związku z realizacją zobowiązania organów wydających prawa jazdy lub pozwolenia, wynikających z dyspozycji par. 5 ust. 5 Rozporządzenia Ministra Transportu, Budownictwa i Gospodarki Morskiej z dnia 31 lipca 2012 r. w sprawie wydawania dokumentów stwierdzających uprawnienia do kierowania pojazdami – (Dz. U. z dnia 11 września 2012 r., poz. 1005), PWPW S.A. w ramach realizacji zobowiązań z umów zawartych z organami wydającymi prawo jazdy lub pozwolenie, jako dostawca i dysponent systemu teleinformatycznego „SI KIEROWCA", z wykorzystaniem którego organ wydający prawo jazdy lub pozwolenie wykonuje czynności związane z wydawaniem praw jazdy lub pozwoleń, zamieszcza dane i informacje w bazie danych oraz składa zamówienia na wykonanie praw jazdy tzn. systemu teleinformatycznego, o którym mowa w przepisach wydanych na podstawie art. 20 ust. 1 pkt 2 Ustawy z dnia 5 stycznia 2011 r. o kierujących pojazdami (Dz. U. 2011 nr 30 poz. 151) z dniem 19 stycznia 2013 roku udostępniła w systemie teleinformatycznym SI Kierowca profile kandydatów na kierowców, organom upoważnionym.

PWPW S.A. jako spółka handlowa oraz jako podmiot, któremu podmiot publiczny zlecił realizację zadania publicznego w zakresie wsparcia procesu wydawania dokumentów komunikacyjnych, przy użyciu systemu SI KIEROWCA, zobowiązana jest w świetle Ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (art.2 ust.3 Ustawy - Dz. U. z 2005r Nr 64, poz. 565 z późn. zm.) wyłącznie do zapewnienia z dniem 19 stycznia 2013 roku, aby system teleinformatyczny SI Kierowca, w którym udostępniane są profile kandydatów na kierowców uprawnionym podmiotom, spełniał minimalne wymagania dla systemów teleinformatycznych oraz zapewniał równe traktowanie rozwiązań informatycznych służących do pobierania i aktualizacji danych z profilu kandydata na kierowcę(PKK).

PWPW S.A. realizuje powyższy wymóg ustawowy poprzez uruchomienie, na wniosek zainteresowanych dostawców rozwiązania informatycznego służącego do pobierania i aktualizacji danych PKK przez uprawnione podmioty (Zewnętrzny SI) usługi udostępnienia oprogramowania komunikacyjnego umożliwiającego obsługę procesu pobierania i aktualizowania profilu kandydata na kierowcę przez uprawnione podmioty zgodnie z obowiązującymi regulacjami prawnymi, zwaną dalej Usługą.

Usługa ta będzie świadczona przez PWPW S.A. na podstawie odrębnej umowy cywilnoprawnej zawartej z dostawcą rozwiązania teleinformatycznego (Zewnętrzny SI) dedykowanego dla podmiotów upoważnionych do pobierania i aktualizacji profili kandydatów na kierowców, z zastrzeżeniem uwzględnienia w zawartej umowie następujących warunków:

- Realizacja umowy w żaden sposób nie wpływa, w tym nie utrudnia, realizacji zobowiązań PWPW S.A. wynikających z umów zawartych z organami właściwymi do spraw wydawania uprawnień do kierowania pojazdami lub pozwoleń, w zakresie utrzymania w sprawności eksploatacyjnej i zapewnienia ciągłości funkcjonowania systemu teleinformatycznego SI Kierowca,

- Umowa zapewnia spełnienie wymogów formalno-prawnych i technicznych, wynikających z obowiązujących przepisów prawa w przedmiotowym zakresie,
- Zewnętrzny SI oraz System SI Kierowca spełniają minimalne wymagania bezpieczeństwa dla systemów teleinformatycznych.

Uruchomienie Usługi odbywać się będzie wyłącznie na wniosek dostawców rozwiązań informatycznych (Zewnętrzny SI) po zawarciu umowy na warunkach opisanych powyżej.

Komunikacja w ramach Usługi będzie opierać się na usługach sieciowych Web-Services.

Usługi będą udostępniać funkcjonalność za pośrednictwem standardowego protokołu sieciowego SOAP. Technologia ta umożliwia zestandaryzowaną komunikację pomiędzy programami napisanymi w różnych językach i dla różnych platform systemowych i aplikacyjnych.

Wymiana danych pomiędzy usługą Web-Services systemu teleinformatycznego SI Kierowca - udostępniającego PKK, a rozwiązaniem teleinformatycznym dostawcy służącym do pobierania i aktualizacji danych z PKK przez podmiot uprawniony polegać będzie na wywoływaniu metod udostępnianych publicznie przez usługę Web-Services.

Interfejs wymiany danych określony będzie poprzez definicje Usług wyrażonych w języku WSDL oraz przez schematy XSD określające strukturę i reguły walidacji przesyłanych danych.

Zakłada się udostępnienie na uzgodnionych zasadach:

- Schematów XSD;
- Definicji usług w języku WSDL;

Usługi Web-Services jako bazowe będą wykorzystywały formaty danych oraz protokoły komunikacyjne i szyfrujące oraz sposoby zapewnienia bezpieczeństwa przy wymianie informacji określone w Rozporządzeniu Rady Ministrów z dnia 12 kwietnia 2012 roku w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (Dz.U. z dnia 16.05.2012, poz.526).

Usługa Web-Service PKK w Systemie SI Kierowca będzie udostępniać następujące metody:

Dla rozwiązań teleinformatycznych dedykowanych dla WORD:

- Get – pobranie PKK;
- Return – zwrot PKK;
- ReturnOutdated – zwrot PKK po roku;
- ReturnToIssuingAuthority – zwrot PKK do Starostwa/Urzędu Miasta;
- UpdateAndReturn – zwrot z aktualizacją;
- ReturnExamFailed – zwrot z niezdanym egzaminem;
- ReturnWithHistory – zwrot z przekazaniem historii egzaminowania PKK;

Dla rozwiązań teleinformatycznych dedykowanych dla OSK:

- Get – pobranie PKK;
- Preview – podgląd PKK;
- Return – zwrot PKK;
- ReturnExpired - zwrot PKK po 2 latach;
- ReturnToIssuingAuthority – zwrot PKK do Starostwa/Urzędu Miasta;
- UpdateAndReturn – zwrot z aktualizacja;

Wszystkie komunikaty przesyłane do systemu teleinformatycznego SI Kierowca, którym posługują się organy wydające prawa jazdy lub pozwolenia, w celu zapewnienia ich niezaprzeczalności i wiarygodności, muszą być podpisywane elektronicznie z użyciem certyfikatów x509v3 i klucza prywatnego podmiotu uprawnionego. Przygotowane rozwiązania w ramach Usługi będą przeprowadzać weryfikację podpisu wykorzystując komplementarny klucz publiczny zawarty w certyfikacie. Więcej informacji dotyczących minimalnych wymagań bezpieczeństwa zawiera załącznik.

PWPW udostępni dostawcy Zewnętrznemu SI, który zawarł umowę z PWPW na Usługę: adres usługi testowej i usługi produkcyjnej.

Zapytania prosimy kierować na adres: integracjapkk@cp.pwpw.pl

ZAŁĄCZNIK do dokumentu POBIERANIE ORAZ AKTUALIZACJA DANYCH I INFORMACJI ZAWARTYCH W PROFILU KANDYDATA NA KIEROWCĘ

Minimalne wymagania bezpieczeństwa dla systemów teleinformatycznych

WERSJA 1.1

W celu zapewnienia wiarygodności klucza publicznego, tj. uzyskania pewności, że jest on własnością podmiotu integrującego swoje usługi z PKK oraz jest przeznaczony do współpracy z Oprogramowaniem Interfejsowym oraz utworzenia i aktualizacji listy zaufanych wystawców certyfikatów, konieczne jest dostarczenie do PWPW przez Podmiot Uprawniony pliku zawierającego certyfikat służący do współpracy z Oprogramowaniem Interfejsowym, celem dodania go do listy zaufanych certyfikatów.

Definicje i akronimy

Nazwa	Objaśnienie
PKK	Profil Kandydata na Kierowcę – zestaw danych i informacji, określony w Rozporządzeniu MTBiGM z dnia 31 lipca 2012 roku w sprawie wydawania dokumentów stwierdzających uprawnienia do kierowania pojazdami.
System teleinformatyczny podmiotu upoważnionego do pobierania i aktualizacji PKK (Zewnętrzny SI)	System teleinformatyczny, o którym mowa w Rozporządzeniu MTBiGM z dnia 13 lipca 2012 roku w sprawie egzaminowania osób ubiegających się o uprawnienia do kierowania pojazdami, szkolenia, egzaminowania i uzyskiwania uprawnień przez egzaminatorów oraz wzorów dokumentów stosowanych w tych sprawach, który ma być integrowany z systemem teleinformatycznym SI Kierowca w celu zapewnienia pobierania i aktualizacji PKK. Rozwiązania informatyczne w zakresie Ośrodków Szkolenia Kierowców.
SI Kierowca	System teleinformatyczny, o którym mowa w przepisach wydanych na podstawie art. 20 ust. 1 pkt. 2 Ustawy i rozporządzeniu Ministra Transportu, Budownictwa i Gospodarki Morskiej z dnia 31 lipca 2012 roku w sprawie wydawania dokumentów stwierdzających uprawnienia do kierowania pojazdami (Dz. U. poz. 1005) i którym posługują się organy wydające prawa jazdy i pozwolenia.
PWPW	Polska Wytwórnia Papierów Wartościowych S.A.

Wymagania ogólne

1. Przy projektowaniu rozwiązań w zakresie pobierania i aktualizacji PKK oraz systemów teleinformatycznych należy uwzględniać następujące ogólnie uznane zasady projektowania zabezpieczeń:

   Z1. Compartmentalization of Information – zasoby systemu o różnym poziomie wrażliwości (tzn. wartości i podatności na zagrożenia) powinny znajdować się w różnych strefach bezpieczeństwa.
   Z2. Defense-in-Depth – ochrona wrażliwych zasobów systemu informatycznego powinna opierać się na wielu warstwach zabezpieczeń.
   Z3. The Principle of Least Privilege – użytkownicy i administratorzy systemu powinni posiadać minimalne uprawienia, które umożliwiają poprawne wykonywanie powierzonych im obowiązków.
   Z4. Weakest link in the chain – poziom bezpieczeństwa systemu informatycznego zależy od najsłabiej zabezpieczonego elementu tego systemu.

Ponadto przy projektowaniu zabezpieczeń należy uwzględnić aktualną wiedzę na temat ataków na aplikacje w celu wyeliminowania możliwości ich skutecznego wykorzystania.

2. Wszystkie elementy techniczne i organizacyjne rozwiązania komunikacyjnego i systemu teleinformatycznego w zakresie PKK dostawców rozwiązań dla podmiotów upoważnionych do pobierania i aktualizacji profili kandydatów na kierowców (Zewnętrzny SI) muszą spełniać następujące wymagania:

   1) Ustawy z dnia 29 sierpnia 1997 roku o ochronie danych osobowych (UODO),
   2) Rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 roku w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Rozporządzenie).
   3) Międzynarodową normą ISO/IEC 27001:2005 w zakresie zabezpieczeń technicznych z załącznika normatywnego A, w oparciu na najlepsze praktyki określona w normie ISO/IEC 27002, a także najlepsze praktyki tworzenia aplikacji.
   4) Wymagania i zalecenia bezpieczeństwa MSW dla systemu teleinformatycznego na styku Zewnętrznego SI z systemem urzędów zintegrowanym z Centralną Ewidencją Pojazdów i Kierowców.
   5) Wymagania bezpieczeństwa fizycznego określone przez MSW w związku z przetwarzaniem danych osobowych i planowaną wymianą informacji z CEPiK.

Wymagania szczegółowe

1. Wymiana informacji pomiędzy Zewnętrznym SI i SI Kierowca informacji w zakresie PKK będzie realizowana w oparciu o Web-Service udostępniony przez PWPW z zastosowaniem zabezpieczeń protokołu gwarantującego zachowanie identyfikacji, uwierzytelniania i autoryzacji stron oraz poufności, integralności, niezaprzeczalności i rozliczalności transportowanych w XML informacji (szyfrowanie, podpis, logowanie zdarzeń, etc.). Szczegóły techniczne zostaną ustalone bezpośrednio pomiędzy dostawcą Zewnętrznego SI i PWPW w odrębnej umowie cywilnoprawnej.

2. Połączenie Zewnętrznego SI z SI Kierowca w celu dokonania integracji i wymiany danych i informacji w zakresie PKK musi być realizowane w oparciu o dedykowane łącze sieciowe zabezpieczone w sposób zapewniający spełnienie wymagań o których mowa ww. pkt. 2 ppdkt. 4). Nie dopuszcza się wykorzystania publicznej sieci Internet. Szczegóły techniczne i sposób podłączenia łącza zapewnianego przez dostawcę Zewnętrznego zostaną ustalone bezpośrednio pomiędzy dostawcą Zewnętrznego SI i PWPW w odrębnej umowie cywilnoprawnej.

3. Kanał wymiany danych musi być chroniony przy użyciu SSL/TLS w tunelu IPSEC celu zapewnienia uwierzytelnienia stron transmisji i zapewniania poufności.

4. Tunel IPSec musi być zrealizowany sprzętowo (zaleca się redundancję urządzeń i wsparcie dla FIPS-140 na poziomie wyższym niż 2) przez dedykowane urządzenia sieciowe spełniające wymagania określone w poniższych dokumentach:

    1) VPN:
        - RFC 1828 IP Authentication using Keyed MD5
        - RFC 1829 The ESP DES-CBC Transform
        - RFC 2085 HMAC-MD5 IP Authentication with Replay Prevention
        - RFC 2401 Security Architecture for the Internet Protocol
        - RFC 2402 IP Authentication Header
        - RFC 2403 The Use of HMAC-MD5-96 within ESP and AH
        - RFC 2404 The Use of HMAC-SHA-1-96 within ESP and AH
        - RFC 2405 The ESP DES-CBC Cipher Algorithm With Explicit IV
        - RFC 2406 IP Encapsulating Security Payload (ESP)
        - RFC 2410 The NULL Encryption Algorithm and Its Use With IPsec
        - RFC 2411 IP Security Document Roadmap
        - RFC 2451 The ESP CBC-Mode Cipher Algorithms
        - RFC 2661 Layer Two Tunneling Protocol "L2TP"
        - RFC 2784 Generic Routing Encapsulation (GRE)
        - RFC 3602 The AES-CBC Cipher Algorithm and Its Use with IPsec
    2) IKEv1:
        - RFC 2407 The Internet IP Security Domain of Interpretation for ISAKMP
        - RFC 2408 Internet Security Association and Key Management Protocol (ISAKMP).
        - RFC 2409 The Internet Key Exchange (IKE)

- RFC 2412 The OAKLEY Key Determination Protocol
- RFC 3526 More Modular Exponential (MODP)
- Diffie-Hellman groups for Internet Key Exchange (IKE)
- RFC 3706 A Traffic-Based Method of Detecting Dead Internet Key Exchange (IKE) Peers

3) PKI:

- RFC 2510 Internet X.509 Public Key Infrastructure Certificate Management Protocols
- RFC 2511 Internet X.509 Certificate Request Message Format
- RFC 3279 Algorithms and Identifiers for the Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile
- RFC 3280 Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile
- draft-nourse-scep-06:
- PKCS#1
- PKCS#10
- PKCS#12
- PKCS#7

5. Klucze prywatne wykorzystywane w wymianie powinny być chronione z użyciem modułu sprzętowego HSM.

6. Sewery komunikacyjne stron będą zlokalizowane w strefach zdemilitaryzowanych (DMZ).

7. Niezaprzeczalność, aktualizację PKK należy opatrzyć bezpiecznym podpisem z wykorzystaniem certyfikatów i list CRL z zaufanych źródeł, za które uznaje się:

    1) certyfikaty CCiGK MSW;
    2) certyfikaty kwalifikowane;
    3) certyfikaty komercyjne wystawiane przez wystawców certyfikatów kwalifikowanych pod warunkiem umieszczenia w certyfikacie nr PESEL.
    4) certyfikaty z Enterprise PKI pod warunkiem:
        i. dostarczenia do PWPW:
            a) polityki certyfikacji;
            b) regulaminu certyfikacji;
            c) certyfikatu publicznego CA;
            d) adresu URL do listy CRL;
            e) procedury recertyfikacji CA;
            f) procedury zarządzania incydentem, w tym numerów telefonów i adresów portalu (jeśli istnieje) do funkcji Service Desk lub Help Desk;
            g) procedurę zatwierdzania zmian w środowisku PKI;
            h) nowych wersji dokumentów wymienionych powyżej niezwłocznie po ich zatwierdzeniu;
        ii. stosowania profilu certyfikatu określonego przez operatora SI Kierowca (istotne zalecenie: parametr CRL ustawiony jako krytyczny);

iii. zapewnienia dostępu on-line do listy CRL;
iv. dostarczenia raportu z audytu PKI o którym mowa w dalszej części dokumentu;

8. Dostawca Zewnętrznego SI musi posługiwać się udokumentowanymi procedurami zarządzania zmianą i dysponować środowiskiem testowym do testowania planowanych zmian przed ich implementacją w środowisku produkcyjnym. Procedura musi być uzgodniona z PWPW i gwarantować taki sposób wdrażania, aby zapewnić ciągłość obsługi interesantów w organach wydających prawa jazdy i pozwolenia.

9. Uruchomienie wymiany informacji pomiędzy stronami wymaga każdorazowo przeprowadzenia testów integracyjnych według uzgodnionego scenariusza i przygotowania raportu po testach w oparciu o uzgodnioną procedurę zatwierdzania zmian.

10. Uprawniony podmiot – użytkownik Zewnętrznego SI musi mieć opracowane dokumenty wymagane przez UODO i Rozporządzenie, o którym mowa w ww. pkt. 2 ppdkt. 2).

11. Wspieranie przez aplikację interfejs komunikacyjny Zewnętrznego SI z Web-Service PKK standardów:

    1) XML - Extensible Markup Language;
    2) XSD - Extensible Markup Language;
    3) XSL - Extensible Stylesheet;
    4) XSLT - Extensible Stylesheet Language Transformation;
    5) XMLdsig - XML-Signature Syntax and Processing;
    6) Web Services;
    7) Web Services Security X.509 Certificate;
    8) SOAP 1.x;
    9) WS-Security;

12. W celu poprawnej obsług uprawnień pomiędzy systemami konieczne jest stworzenie Web-Service po stronie podmiotu uprawnionego, z którego PWPW będzie pobierać listę użytkowników podmiotu uprawnionego wraz z ich uprawnieniami po stronie systemu podmiotu uprawnionego. Implementacja, utrzymanie, dostępność Web-Service leży w gestii podmiotu uprawnionego.

```
<?xml version="1.0" encoding="utf-8"?>
<xs:schema id="Security"
    targetNamespace="http://tempuri.org/Security.xsd"
    elementFormDefault="qualified"
    xmlns="http://tempuri.org/Security.xsd"
    xmlns:sec="http://tempuri.org/Security.xsd"
    xmlns:xs="http://www.w3.org/2001/XMLSchema"
>

  <xs:complexType name="Users">
    <xs:sequence>
      <xs:element name="UserList" type="sec:User" minOccurs="0" maxOccurs="unbounded" />
    </xs:sequence>
  </xs:complexType>

```

```
16.
17.   <xs:complexType name ="User">
18.    <xs:sequence>
19.      <xs:element name="UserId" type="sec:UserId" minOccurs="1" maxOccurs="1"  />
20.      <xs:element name="Role" type="sec:Role" minOccurs="1" maxOccurs="1"/>
21.      <xs:element name="OrganizationId" type="sec:OrganizationId" minOccurs="1" maxOccurs="1"/>
22.      <xs:element name="Certificate" type="xs:base64Binary" minOccurs="1" maxOccurs="1" />
23.      <xs:element name="Pesel" type="sec:PESEL" minOccurs="0" maxOccurs="1"/>
24.      <xs:element name="ClientSystem" type="sec:ClientSystem" minOccurs="1" maxOccurs="1"/>
25.      <xs:element name="IsActive" type="xs:boolean" minOccurs="1" maxOccurs="1"/>
26.    </xs:sequence>
27.   </xs:complexType>
28.
29.   <xs:simpleType name="UserId">
30.    <xs:restriction base="xs:string">
31.      <xs:pattern value="[\d\w]{5,32}"/>
32.    </xs:restriction>
33.   </xs:simpleType>
34.
35.   <xs:simpleType name="OrganizationId">
36.    <xs:restriction base="xs:string" >
37.      <xs:maxLength value="128"/>
38.    </xs:restriction>
39.   </xs:simpleType>
40.
41.   <xs:simpleType name="ClientSystem">
42.    <xs:restriction base="xs:string">
43.      <xs:enumeration value="WORD"/>
44.      <xs:enumeration value="OSK" />
45.    </xs:restriction>
46.   </xs:simpleType>
47.
48.   <xs:simpleType name="PESEL">
49.    <xs:restriction base="xs:string">
50.      <xs:pattern value="\d{11}"/>
51.    </xs:restriction>
52.   </xs:simpleType>
53.
54.
55.   <xs:simpleType name="Role">
56.    <xs:restriction base="xs:short"/>
57.   </xs:simpleType>
58.
59.  </xs:schema>
```

13. W celu zapewnienia wiarygodności klucza publicznego, tj. uzyskania pewności, że jest on własnością podmiotu uprawnionego oraz jest przeznaczony do współpracy z Oprogramowaniem Interfejsowym oraz utworzenia i aktualizacji listy zaufanych wystawców certyfikatów, podmiot uprawniony dostarczy do PWPW plik zawierający certyfikat służący do współpracy z Oprogramowaniem Interfejsowym, celem dodania go do listy zaufanych certyfikatów.

Potwierdzenie spełniania wymagań

1. Zgodność z wymaganiami będzie potwierdzana przez niezależny od operatora Zewnętrznego SI audyt oraz test bezpieczeństwa aktualnej wersji interfejsu komunikacyjnego z Web-Service PKK niezależny od operatora Zewnętrznego SI.

2. Specyfikację audytu i testu bezpieczeństwa będą uzgodnione przez strony.

3. Przeprowadzenie audytu spełnienia wymagań i testu bezpieczeństwa interfejsu i przedstawienie raportu z wynikiem pozytywnym (brak niezgodności, brak krytycznych podatności bezpieczeństwa) stanowi warunek uruchomienia wymiany danych w zakresie PKK pomiędzy dostawcą Zewnętrznego systemu SI i PWPW.

4. PWPW ma prawo zlecić, a operator Zewnętrznego SI ma obowiązek przeprowadzić, audyt ad-hoc w przypadku powzięcia informacji o istotnych zmianach w Zewnętrznym SI (nowa wersja interfejsu komunikacyjnego) albo nowych zagrożeniach i podatnościach – mogących mieć zdaniem PWPW wpływ na bezpieczeństwo SI Kierowca.

5. Operator Zewnętrznego SI jest zobowiązany do wdrażania zmian (działania korygujące i zapobiegawcze) określonych po audycie i teście bezpieczeństwa w uzgodnionych z PWPW terminach oraz przeprowadzenia testu weryfikującego implementację poprawek wskazanych w raporcie po teście. Obowiązkiem operatora Zewnętrznego SI jest dostarczenie do PWPW raportu potwierdzającego brak podatności.