DECYZJA RADY (UE) 2018/1926

z dnia 19 listopada 2018 r.

w sprawie stanowiska, jakie ma być zajęte w imieniu Unii Europejskiej w grupie ekspertów Europejskiej Komisji Gospodarczej ONZ ds. Umowy europejskiej dotyczącej pracy załóg pojazdów wykonujących międzynarodowe przewozy drogowe

RADA UNII EUROPEJSKIEJ,

uwzględniając Traktat o funkcjonowaniu Unii Europejskiej, w szczególności jego art. 91, w związku z art. 218 ust. 9,

uwzględniając wniosek Komisji Europejskiej,

a także mając na uwadze, co następuje:

(1) Umowa europejska dotycząca pracy załóg pojazdów wykonujących międzynarodowe przewozy drogowe (AETR) ([1]) weszła w życie w dniu 5 stycznia 1976 r.

(2) Europejska Komisja Gospodarcza Organizacji Narodów Zjednoczonych (EKG ONZ) powołała w ramach AETR grupę ekspertów ds. AETR. Grupa ta jest podmiotem uprawnionym do opracowywania propozycji zmian AETR i przedstawienia ich Grupie Roboczej ds. Transportu Drogowego EKG ONZ.

(3) Grupa ekspertów ds. AETR omawia obecnie zmiany AETR na podstawie wniosku Unii będącego następstwem stanowiska Unii przyjętego w tym celu decyzją Rady (UE) 2016/1877 ([2]). Dalsza zmiana AETR wydaje się konieczna, by zapewnić umawiającym się stronom AETR spoza UE możliwość udziału w wymianie informacji na temat kart kierowców na podstawie ujednoliconych norm bezpieczeństwa i ochrony danych.

(4) Na mocy rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 165/2014 ([3]) państwa członkowskie są zobowiązane do wzajemnego połączenia swoich elektronicznych rejestrów kart kierowcy za pomocą systemu informacyjnego sieci telematycznej na potrzeby wymiany informacji dotyczących wydawania kart do tachografów (Tachonet) lub, w przypadku korzystania z systemu kompatybilnego, do zapewnienia możliwości wymiany danych elektronicznych ze wszystkimi pozostałymi państwami członkowskimi za pomocą systemu informacyjnego Tachonet. Tachonet stanowi platformę wymiany informacji na temat kart kierowcy między państwami członkowskimi w celu zapewnienia, aby kierowcy nie posiadali więcej niż jednej karty kierowcy.

(5) W celu osiągnięcia ogólnoeuropejskiej harmonizacji w dziedzinie elektronicznej wymiany informacji na temat kart kierowcy konieczne jest wykorzystywanie Tachonet jako jedynej platformy przez wszystkie umawiające się strony AETR.

(6) Podłączenie do systemu informacyjnego Tachonet jest obecnie możliwe albo bezpośrednio poprzez transeuropejską telematyczną sieć komunikacyjną między administracjami (TESTA), albo pośrednio poprzez państwo członkowskie już podłączone do TESTA. Zważywszy, że TESTA stanowią usługi ograniczone do państw członkowskich i instytucji Unii, umawiające się strony AETR spoza UE mogą zostać podłączone do Tachonet wyłącznie pośrednio.

(7) Komisja dokonała ostatnio oceny pośrednich połączeń z systemem informacyjnym Tachonet i stwierdziła, że nie zapewniają one takiego samego poziomu bezpieczeństwa jak TESTA. W szczególności nie ma wystarczającej gwarancji autentyczności, integralności i poufności informacji wymienianych za pomocą pośrednich połączeń. Pośrednie połączenia z Tachonet powinny zatem zostać zastąpione bezpiecznym połączeniem.

(8) Platforma eDelivery to sieć węzłów przyłączeniowych na potrzeby łączności cyfrowej opracowana przez Komisję, w której każdy uczestnik na poziomie krajowym staje się węzłem przy użyciu standardowych protokołów komunikacyjnych i polityki bezpieczeństwa. Platforma eDelivery jest elastycznym narzędziem, które może zostać dostosowane do poszczególnych usług.

(9) W ramach platformy eDelivery wykorzystuje się powszechnie stosowane technologie bezpieczeństwa, takie jak infrastruktura klucza publicznego (PKI), w celu zapewnienia autentyczności, integralności i poufności wymienianych informacji. Dostęp umawiających się stron AETR spoza UE do Tachonet powinien odbywać się za pośrednictwem platformy eDelivery.

([1]) Dz.U. L 95 z 8.4.1978, s. 1.

([2]) Decyzja Rady (UE) 2016/1877 z dnia 17 października 2016 r. dotycząca stanowiska, jakie ma zostać zajęte w imieniu Unii Europejskiej w grupie ekspertów ds. Umowy europejskiej dotyczącej pracy załóg pojazdów wykonujących międzynarodowe przewozy drogowe (AETR) oraz w Grupie Roboczej ds. Transportu Drogowego Europejskiej Komisji Gospodarczej ONZ (Dz.U. L 288 z 22.10.2016, s. 49).

([3]) Rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 165/2014 z dnia 4 lutego 2014 r. w sprawie tachografów stosowanych w transporcie drogowym i uchylające rozporządzenie Rady (EWG) nr 3821/85 w sprawie urządzeń rejestrujących stosowanych w transporcie drogowym oraz zmieniające rozporządzenie (WE) nr 561/2006 Parlamentu Europejskiego i Rady w sprawie harmonizacji niektórych przepisów socjalnych odnoszących się do transportu drogowego (Dz.U. L 60 z 28.2.2014, s. 1).

(10) Umawiające się strony AETR powinny postępować zgodnie z określoną procedurą w celu otrzymania certyfikatów elektronicznych oraz odpowiednich kluczy elektronicznych umożliwiających dostęp do systemu Tachonet.

(11) Połączenie z Tachonet za pośrednictwem platformy eDelivery oznacza, że umawiające się strony AETR są zobowiązane zapewnić ochronę kluczy i certyfikatów elektronicznych umożliwiających dostęp do systemu oraz zapewnić, aby nie były one wykorzystywane przez strony nieuprawnione. Umawiające się strony AETR powinny również zagwarantować, że klucze objęte certyfikatami, które utraciły ważność, nie będą dalej wykorzystywane.

(12) Konieczne jest zagwarantowanie ochrony danych osobowych udostępnianych stronom za pośrednictwem Tachonet zgodnie z Konwencją o ochronie osób w związku z automatycznym przetwarzaniem danych osobowych, sporządzoną dnia 28 stycznia 1981 r.

(13) Organy krajowe połączone z Tachonet mają obowiązek przeprowadzenia odpowiednich wdrożeń technicznych w celu zapewnienia, aby Tachonet funkcjonował zgodnie z wysokimi poziomami skuteczności działania. Zadaniem Komisji jest przygotowanie testów potwierdzających osiągnięcie tych poziomów skuteczności działania i ich wdrożenie we współpracy z właściwymi organami krajowymi.

(14) W wyroku z dnia 31 marca 1971 r. w sprawie 22/70 AETR ([1]) Trybunał Sprawiedliwości Unii Europejskiej potwierdził, że praca załóg pojazdów w transporcie drogowym wchodzi w zakres zewnętrznych kompetencji Unii. Kompetencje te były od tego czasu realizowane za pośrednictwem szeregu aktów prawnych przyjętych przez Unię, w tym rozporządzeń Parlamentu Europejskiego i Rady (WE) nr 561/2006 ([2]) oraz (UE) nr 165/2014. Ponieważ przedmiot AETR wchodzi w zakres stosowania rozporządzenia (WE) nr 561/2006, Unia posiada wyłączną kompetencję do negocjowania i zawarcia wszelkich stosownych umów oraz dokonywania ich zmian.

(15) Propozycje przedstawione przez umawiające się strony mogą – pod warunkiem akceptacji przez grupę ekspertów ds. AETR – doprowadzić do zmiany AETR po wszczęciu i przeprowadzeniu procedury zmiany tej umowy. Po przyjęciu propozycji przez grupę ekspertów ds. AETR państwa członkowskie Unii jako umawiające się strony AETR będą z kolei zobowiązane do współpracy w celu uruchomienia mechanizmu rewizji AETR zgodnie z obowiązkiem lojalnej współpracy wynikającym z art. 4 ust. 3 Traktatu o Unii Europejskiej oraz z zastrzeżeniem, w odpowiednim przypadku, decyzji Rady zgodnie z art. 218 ust. 6 Traktatu o funkcjonowaniu Unii Europejskiej. Proponowane zmiany AETR staną się skuteczne dopiero po przeprowadzeniu procedury rewizji AETR.

(16) Należy ustalić stanowisko, jakie powinno zostać zajęte w imieniu Unii w grupie ekspertów ds. AETR, ponieważ Unia będzie związana zmianą AETR.

(17) Ponieważ Unia nie jest umawiającą się stroną AETR i jej status nie pozwala jej na przedstawienie proponowanych zmian, państwa członkowskie, działając w interesie Unii, powinny przedstawić proponowane zmiany grupie ekspertów ds. AETR w duchu lojalnej współpracy, aby promować osiągnięcie celów Unii.

(18) Stanowisko Unii zostanie wyrażone przez działające wspólnie państwa członkowskie będące członkami grupy ekspertów ds. AETR oraz Grupy Roboczej ds. Transportu Drogowego EKG ONZ,

PRZYJMUJE NINIEJSZĄ DECYZJĘ:

Artykuł 1

Stanowisko, jakie ma być zajęte w imieniu Unii w grupie ekspertów ds. Umowy europejskiej dotyczącej pracy załóg pojazdów wykonujących międzynarodowe przewozy drogowe (AETR), wyraża poparcie dla proponowanych zmian AETR określonych w dokumencie dołączonym do niniejszej decyzji.

Artykuł 2

Stanowisko, o którym mowa w art. 1, zostaje wyrażone przez działające wspólnie państwa członkowskie Unii będące umawiającymi się stronami AETR.

Formalne i drobne modyfikacje stanowiska, o którym mowa w art. 1, mogą być uzgadniane bez konieczności zmiany tego stanowiska.

([1]) ECLI: EU:C:1971:32.

([2]) Rozporządzenie (WE) nr 561/2006 Parlamentu Europejskiego i Rady z dnia 15 marca 2006 r. w sprawie harmonizacji niektórych przepisów socjalnych odnoszących się do transportu drogowego oraz zmieniające rozporządzenia Rady (EWG) nr 3821/85 i (WE) nr 2135/98, jak również uchylające rozporządzenie Rady (EWG) nr 3820/85 (Dz.U. L 102 z 11.4.2006, s. 1).

Artykuł 3

Niniejsza decyzja wchodzi w życie następnego dnia po jej przyjęciu.

Sporządzono w Brukseli dnia 19 listopada 2018 r.

W imieniu Rady
E. KÖSTINGER
Przewodnicząca

ZAŁĄCZNIK

NOWY DODATEK DO AETR

Dodatek 4

Specyfikacje Tachonet

1. **Zakres i cel**

1.1. Niniejszy dodatek określa warunki dotyczące połączenia umawiających się stron AETR z systemem Tachonet za pośrednictwem platformy eDelivery.

1.2. Umawiające się Strony łączące się z systemem Tachonet za pośrednictwem eDelivery przestrzegają przepisów określonych w niniejszym dodatku.

2. **Definicje**

a) „Umawiająca się Strona" lub „Strona" oznacza Umawiającą się Stronę AETR;

b) „eDelivery" oznacza opracowaną przez Komisję usługę umożliwiającą przesyłanie danych między stronami trzecimi drogą elektroniczną, zapewniającą dowody związane z posługiwaniem się przesyłanymi danymi, w tym dowód wysłania i otrzymania danych, oraz chroniącą przesyłane dane przed ryzykiem jakiejkolwiek nieupoważnionej zmiany;

c) „Tachonet" oznacza system elektronicznej wymiany informacji dotyczących kart kierowcy między | Umawiającymi się Stronami, o którym mowa w art. 31 ust. 2 rozporządzenia (UE) nr 165/2014;

d) „węzeł centralny" oznacza system informacyjny umożliwiający przekazywanie komunikatów Tachonet między Stronami zgłaszającymi zapytanie i Stronami udzielającymi odpowiedzi na zapytanie;

e) „Strona zgłaszająca zapytanie" oznacza Umawiającą się Stronę wysyłającą zapytanie lub zgłoszenie Tachonet, które są następnie kierowane do odpowiedniej Strony udzielającej odpowiedzi na zapytanie za pośrednictwem węzła centralnego;

f) „Strona udzielająca odpowiedzi na zapytanie" oznacza Stronę, do której skierowane jest zapytanie lub zgłoszenie Tachonet;

g) „organ wydający karty" lub „CIA" oznacza podmiot upoważniony przez Umawiającą się Stronę do wydawania kart do tachografu i zarządzania nimi.

3. **Obowiązki ogólne**

3.1. Żadna z Umawiających się Stron nie może zawierać umów na dostęp do systemu Tachonet w imieniu innej Strony lub w jakikolwiek inny sposób reprezentować drugiej Umawiającej się Strony na podstawie niniejszego dodatku. Żadna z Umawiających się Stron nie może działać jako podwykonawca drugiej Umawiającej się Strony przy prowadzeniu działań, o których mowa w niniejszym dodatku.

3.2. Umawiające się Strony zapewniają dostęp do swoich krajowych rejestrów kart kierowcy za pośrednictwem Tachonet, w sposób i na poziomie usług określonych w poddodatku 4.6.

3.3. Umawiające się Strony niezwłocznie informują się nawzajem, jeśli zauważą w swoim obszarze odpowiedzialności zakłócenia lub błędy, które mogą zagrozić realizacji normalnego działania systemu Tachonet.

3.4. Każda ze Stron wyznacza osoby do kontaktów w sprawie Tachonet dla sekretariatu AETR. Każda zmiana punktów kontaktowych musi zostać zgłoszona na piśmie sekretariatowi AETR.

4. **Testy dotyczące połączenia z systemem Tachonet**

4.1. Połączenie Umawiającej się Strony z systemem Tachonet uznaje się za ustanowione po wykonaniu z wynikiem pozytywnym testów połączenia, integracji i funkcjonowania zgodnie z instrukcjami Komisji Europejskiej i pod jej nadzorem.

4.2. W przypadku niepowodzenia testów wstępnych Komisja Europejska może czasowo wstrzymać etap testowania. Testy wznawia się po poinformowaniu Komisji Europejskiej przez Umawiającą się Stronę o przyjęciu koniecznych udoskonaleń technicznych na szczeblu krajowym, pozwalających na pomyślne przeprowadzenie testów wstępnych.

4.3. Maksymalny czas trwania tych testów wstępnych wynosi sześć miesięcy.

5. **Architektura zaufania**

5.1. Architektura zaufania systemu Tachonet musi zapewniać poufność, integralność i niezaprzeczalność komunikatów Tachonet.

5.2. Architektura zaufania systemu Tachonet musi opierać się na usłudze infrastruktury klucza publicznego (PKI) utworzonej przez Komisję Europejską, której wymogi są określone w poddodatkach 4.8 i 4.9.

5.3. Następujące podmioty tworzą architekturę zaufania systemu Tachonet:

a) centrum certyfikacji odpowiedzialne za generowanie certyfikatów elektronicznych wydawanych organom krajowym Umawiających się Stron przez organ rejestrujący (za pośrednictwem zaufanych kurierów wyznaczonych przez te organy), a także za utworzenie infrastruktury technicznej w zakresie wydawania, unieważniania i odnawiania certyfikatów elektronicznych;

b) właściciel domeny odpowiedzialny za funkcjonowanie węzła centralnego, o którym mowa w poddodatku 4.1, oraz zatwierdzanie i koordynację architektury zaufania systemu Tachonet;

c) organ rejestrujący odpowiedzialny za rejestrację i zatwierdzanie wniosków o wydanie, unieważnienie i odnowienie certyfikatów elektronicznych oraz weryfikację tożsamości zaufanych kurierów;

d) zaufany kurier, wyznaczony przez organy krajowe, odpowiedzialny za przekazanie klucza publicznego organowi rejestrującemu i uzyskanie odpowiedniego certyfikatu generowanego przez centrum certyfikacji;

e) organ krajowy Umawiającej się Strony, który:

(i) generuje klucze prywatne i odpowiadające im klucze publiczne, które mają być zawarte w certyfikatach generowanych przez centrum certyfikacji;

(ii) zgłasza centrum certyfikacji zapotrzebowanie na wydanie certyfikatów elektronicznych;

(iii) wyznacza zaufanego kuriera.

5.4. Centrum certyfikacji oraz organ rejestrujący wyznaczane są przez Komisję Europejską.

5.5. Każda z Umawiających się Stron łączących się z systemem Tachonet musi poprosić o wydanie certyfikatu elektronicznego zgodnie z poddodatkiem 4.9, aby podpisywać i szyfrować komunikaty Tachonet.

5.6. Certyfikat może zostać cofnięty zgodnie z poddodatkiem 4.9.

6. **Ochrona i poufność danych**

6.1. Strony, zgodnie z przepisami o ochronie danych na szczeblu międzynarodowym i krajowym, w szczególności z Konwencją o ochronie osób w związku z automatycznym przetwarzaniem danych osobowych, przyjmują wszelkie niezbędne środki techniczne i organizacyjne w celu zapewnienia bezpieczeństwa danych w systemie Tachonet i zapobieżenia zmianie bądź utracie lub nieuprawnionemu przetwarzaniu lub dostępowi do tych danych (w szczególności gwarantując autentyczność, poufność, identyfikowalność, integralność, dostępność, niezaprzeczalność i bezpieczeństwo komunikatów).

6.2. Każda ze stron chroni swoje własne krajowe systemy przed nielegalnym używaniem, kodami złośliwymi, wirusami komputerowymi, zainfekowaniem komputera, naruszeniami i nielegalną ingerencją w dane oraz innymi podobnymi działaniami przez osoby trzecie. Strony zgadzają się wykorzystywać komercyjnie uzasadnione rozwiązania w celu uniknięcia przekazywania wszelkich wirusów, bomb zegarowych, robaków komputerowych lub podobnych zagrożeń czy też procedur programowania komputerowego, które mogą kolidować z systemami komputerowymi drugiej Strony.

7. **Koszty**

7.1. Umawiające się Strony ponoszą swoje własne koszty rozwoju i eksploatacji w związku ze swoimi własnymi systemami danych i procedurami, stosownie do wymogów, w celu wypełnienia zobowiązań wynikających z niniejszego dodatku.

7.2. Usługi wyszczególnione w poddodatku 4.1, świadczone przez węzeł centralny, są bezpłatne.

8. **Podwykonawstwo**

8.1. Strony mogą podzlecać świadczenie wszelkich usług, za które są odpowiedzialne zgodnie z niniejszym dodatkiem.

8.2. Takie podwykonawstwo nie zwalnia Strony z odpowiedzialności wynikającej z niniejszego dodatku, w tym odpowiedzialności za odpowiedni poziom usług zgodnie z poddodatkiem 4.6.

Poddodatek 4.1

Ogólne aspekty systemu Tachonet

1. **Ogólny opis**

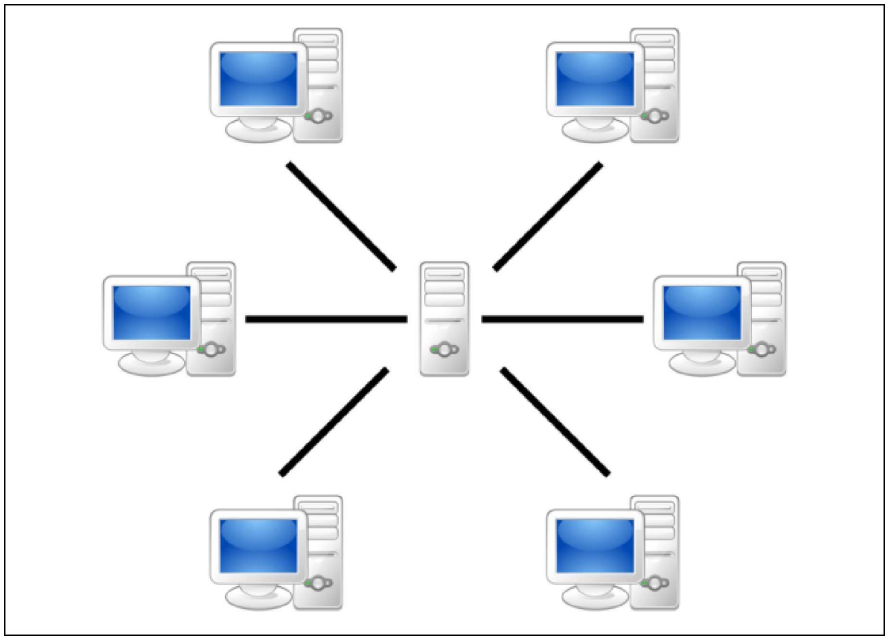
Tachonet jest systemem elektronicznej wymiany informacji dotyczących kart kierowcy między Umawiającymi się Stronami AETR. Tachonet przekierowuje zapytania Stron zgłaszających zapytanie Stronom udzielającym odpowiedzi, jak również odpowiedzi tych ostatnich tym pierwszym. Umawiające się Strony uczestniczące w systemie Tachonet muszą podłączyć do niego swoje krajowe rejestry kart kierowcy.

2. **Architektura**

System informacyjny Tachonet obejmuje następujące części:

2.1. Węzeł centralny, który umożliwia przyjęcie zapytania od Strony zgłaszającej zapytanie, dokonania jego zatwierdzenia i przetworzenia poprzez przekazanie go Stronom udzielającym odpowiedzi na zapytanie. Węzeł centralny czeka na odpowiedź poszczególnych Stron udzielających odpowiedzi na zapytanie, dokonuje konsolidacji wszystkich odpowiedzi i przekazuje skonsolidowaną odpowiedź Stronie zgłaszającej zapytanie.

2.2. Systemy krajowe Stron, które muszą być wyposażone w interfejs umożliwiający zarówno wysyłanie zapytań, jak i odbieranie odnośnych odpowiedzi. Systemy krajowe mogą wykorzystywać oprogramowanie zamknięte lub komercyjne do przekazywania i odbierania komunikatów z węzła centralnego.



3. **Zarządzanie**

3.1. Węzłem centralnym zarządza Komisja Europejska, która jest odpowiedzialna za eksploatację techniczną i utrzymanie węzła centralnego.

3.2. W węźle centralnym nie można przechowywać przez okres przekraczający sześć miesięcy danych innych niż dane dotyczące logowania i dane statystyczne określone w poddodatku 4.7.

3.3. Węzeł centralny nie może umożliwiać dostępu do danych osobowych, z wyjątkiem dostępu dla upoważnionych pracowników Komisji Europejskiej, jeżeli jest to konieczne do celów monitorowania, utrzymania i usuwania usterek.

3.4. Każda z Umawiających się Stron jest odpowiedzialna za:

3.4.1. utworzenie swoich systemów krajowych i zarządzanie nimi, z uwzględnieniem interfejsu z węzłem centralnym;

3.4.2. instalację i utrzymanie swoich systemów krajowych, zarówno sprzętu, jak i oprogramowania zamkniętego lub komercyjnego;

3.4.3. prawidłowo funkcjonującą interoperacyjność swoich systemów krajowych i węzła centralnego, w tym za zarządzanie komunikatami o błędach otrzymywanymi z węzła centralnego;

3.4.4. wprowadzanie wszelkich środków w celu zapewnienia poufności, integralności i dostępności informacji;

3.4.5. działanie systemów krajowych zgodnie z poziomami obsługi określonymi w poddodatku 4.6.

Poddodatek 4.2

Funkcje systemu Tachonet

1. Za pomocą systemu informacyjnego Tachonet zapewnia się następujące funkcje:

1.1. Check Issued Cards (CIC) (kontrola wydanych kart): umożliwia Stronie zgłaszającej zapytanie wysłanie zapytania w sprawie kontroli wydanych kart (Check Issued Cards Request) do jednej lub wszystkich Stron udzielających odpowiedzi na zapytanie w celu ustalenia, czy osoba ubiegająca się o kartę posiada już kartę kierowcy wydaną przez Strony udzielające odpowiedzi na zapytanie. Strony udzielające odpowiedzi na zapytanie muszą odpowiedzieć, przesyłając odpowiedź w sprawie kontroli wydanych kart (Check Issued Cards Response).

1.2. Check Card Status (CCS) (kontrola statusu karty): umożliwia Stronie zgłaszającej zapytanie zwrócenie się do Strony udzielającej odpowiedzi o podanie szczegółowych informacji dotyczących karty wydanej przez tę ostatnią poprzez wysłanie zapytania w sprawie kontroli statusu karty (Check Card Status Request). Strona udzielająca odpowiedzi odpowiada na zapytanie, przesyłając odpowiedź w sprawie kontroli statusu karty (Check Card Status Response).

1.3. Modify Card Status (MCS) (modyfikacja statusu karty): umożliwia Stronie zgłaszającej zapytanie – za pośrednictwem zapytania w sprawie modyfikacji statusu karty (Modify Card Status Request) – powiadomienie Strony udzielającej odpowiedzi, że status karty wydanej przez to drugie państwo uległ modyfikacji. Strona udzielająca odpowiedzi musi odpowiedzieć za pomocą potwierdzenia modyfikacji statusu karty (Modify Card Status Acknowledgement).

1.4. Issued Card Driving License (ICDL) (wydanie karty na podstawie prawa jazdy): umożliwia Stronie zgłaszającej zapytanie – za pośrednictwem zapytania w sprawie wydania karty na podstawie prawa jazdy (Issued Card Driving Licence Request) – zawiadomienie Strony udzielającej odpowiedzi na zapytanie, że karta została wydana przez to pierwsze państwo na podstawie prawa jazdy wydanego przez to drugie państwo. Strona udzielająca odpowiedzi musi odpowiedzieć za pomocą potwierdzenia modyfikacji statusu karty (Modify Card Status Acknowledgement).

2. Strona udzielająca odpowiedzi na zapytanie musi odpowiedzieć za pomocą odpowiedzi w sprawie wydania karty na podstawie prawa jazdy (Issued Card Driving Licence Response).

3. Należy uwzględnić inne rodzaje komunikatów uznanych za właściwe dla sprawnego funkcjonowania systemu Tachonet, np. powiadomienia o błędach. Systemy krajowe muszą rozpoznawać statusy kart wymienione w tabeli 1 w przypadku użycia którejkolwiek z funkcji opisanych w pkt 1.

4. Jednakże Strony nie są zobowiązane do wdrożenia procedury administracyjnej, w której wykorzystuje się wszystkie wymienione statusy. W przypadku gdy Strona otrzyma odpowiedź lub powiadomienie o statusie, który nie jest stosowany w jego procedurach administracyjnych, system krajowy przekłada status odebranego komunikatu na odpowiednią wartość w danej procedurze. Komunikat nie może zostać odrzucony przez Stronę udzielającą odpowiedzi na zapytanie, jeżeli status komunikatu jest wymieniony w tabeli 1.

5. Statusu karty wymienionego w tabeli 1 nie można wykorzystywać w celu ustalenia, czy karta kierowcy uprawnia do prowadzenia pojazdu. W przypadku gdy Strona zgłasza zapytanie do rejestru organu krajowego wydającego kartę za pośrednictwem funkcji CCS, odpowiedź musi zawierać specjalne pole „uprawnia do prowadzenia pojazdu" (valid for driving). Krajowe procedury administracyjne muszą być takie, aby odpowiedzi przy użyciu CCS zawsze obejmowały odpowiednią wartość pola „uprawnia do prowadzenia pojazdu" (valid for driving).

Tabela 1

Statusy kart

Card Status (Status karty)	**Definicja**
Application (wniosek)	CIA otrzymał wniosek o wydanie karty kierowcy. Przedmiotowe informacje zostały zarejestrowane i zachowane w bazie danych, a także wygenerowano klucze wyszukiwania.
Approved (zatwierdzony)	CIA zatwierdził wniosek dotyczący karty do tachografu.
Rejected (odrzucony)	CIA nie zatwierdził wniosku.
Personalised (spersonalizowana)	Karta do tachografu została spersonalizowana.

Card Status (Status karty)	Definicja
Dispatched (wysłana)	Organ krajowy wysłał kartę kierowcy do odpowiedniego kierowcy lub do odpowiedniej agencji dostarczającej.
Handed Over (przekazana)	Organ krajowy przekazał kartę kierowcy odpowiedniemu kierowcy.
Confiscated (skonfiskowana)	Karta kierowcy została odebrana kierowcy przez właściwy organ.
Suspended (zawieszona)	Karta kierowcy została tymczasowo odebrana kierowcy.
Withdrawn (wycofana)	CIA podjął decyzję o wycofaniu karty kierowcy. Karta została ostatecznie unieważniona.
Surrendered (zwrócona)	Karta do tachografu została zwrócona CIA i uznana za niepotrzebną.
Lost (zagubiona)	CIA zgłoszono zaginięcie karty do tachografu.
Stolen (skradziona)	CIA zgłoszono kradzież karty do tachografu. Skradzioną kartę uznaje się za zagubioną.
Malfunctioning (niesprawna)	CIA zgłoszono niesprawność karty do tachografu.
Expired (wygasła)	Wygasł okres ważności karty do tachografu.
Replaced (zastąpiona)	Karta do tachografu zgłoszona jako zagubiona, skradziona lub niesprawna została zastąpiona nową kartą. Dane na nowej karcie są takie same, z wyjątkiem indeksu zastąpienia numeru karty, który został zwiększony o jeden.
Renewed (odświeżona)	Karta do tachografu została odświeżona z powodu zmiany danych administracyjnych lub zbliżającego się końca okresu ważności karty. Numer nowej karty jest taki sam, z wyjątkiem indeksu odświeżenia numeru karty, który został zwiększony o jeden.
In Exchange (w trakcie wymiany)	CIA, który wydał kartę kierowcy, otrzymał powiadomienie, że rozpoczęła się procedura wymiany danej karty kierowcy na kartę kierowcy wydaną przez CIA innej Strony.
Exchanged (wymieniona)	CIA, który wydał kartę kierowcy, otrzymał powiadomienie, że zakończyła się procedura wymiany danej karty kierowcy na kartę kierowcy wydaną przez CIA innej Strony.

Poddodatek 4.3

Przepisy dotyczące komunikatów Tachonet

1. **Ogólne wymogi techniczne**

1.1. Węzeł centralny zapewnia zarówno interfejsy synchroniczne, jak i asynchroniczne na potrzeby wymiany komunikatów. Strony mogą wybrać najodpowiedniejszą technologię interfejsu na potrzeby połączenia z własnymi aplikacjami.

1.2. Wszystkie komunikaty wymieniane między węzłem centralnym a systemami krajowymi muszą być zakodowane w UTF-8.

1.3. Systemy krajowe muszą mieć zdolność do odbioru i przetwarzania komunikatów zawierających litery alfabetu greckiego i cyrylicy.

2. **Struktura komunikatów XML i definicja schematu (XSD)**

2.1. Ogólna struktura komunikatów XML musi odpowiadać formatowi zdefiniowanemu w schematach XSD zainstalowanych w węźle centralnym.

2.2. Węzeł centralny i systemy krajowe muszą przesyłać i odbierać komunikaty zgodne ze schematem XSD komunikatu.

2.3. Systemy krajowe muszą mieć zdolność do wysyłania, odbierania i przetwarzania wszystkich komunikatów odnoszących się do którejkolwiek z funkcji określonych w poddodatku 4.2.

2.4. Komunikaty XML muszą spełniać co najmniej minimalne wymogi określone w tabeli 2.

Tabela 2

Minimalne wymogi dotyczące treści komunikatów XML

Wspólny nagłówek		**Informacje obowiązkowe**
Version (Wersja)	Oficjalna wersja specyfikacji XML jest określana poprzez przestrzeń nazw określoną w komunikacie XSD i w atrybucie version elementu nagłówka każdego komunikatu XML. Numer wersji („n.m") definiuje się jako ustaloną wartość dla każdej wersji pliku definicji schematu XML (xsd).	Tak
Test Identifier (Identyfikator testowy)	Nieobowiązkowy identyfikator dla testu. Inicjator testu uzupełnia identyfikator, a wszyscy uczestnicy przepływu pracy przesyłają/odsyłają ten sam identyfikator. W produkcji należy go pominąć i nie wykorzystywać go, jeżeli zostanie dostarczony.	Nie
Technical identifier (Identyfikator techniczny)	UUID jednoznacznie identyfikujący każdy indywidualny komunikat. Nadawca generuje UUID i uzupełnia ten atrybut. Dane te nie są wykorzystywane w funkcjach użytkowych.	Tak
Workflow Identifier (Identyfikator przepływu pracy)	Identyfikator przepływu pracy jest UUID i powinien zostać wygenerowany przez Stronę zgłaszającą zapytanie. Identyfikator ten jest następnie wykorzystywany we wszystkich komunikatach do celów korelacji przepływu pracy.	Tak
Sent At (Czas wysłania)	Data i godzina (UTC) wysłania komunikatu.	Tak
Timeout (Czas oczekiwania)	Jest to opcjonalny atrybut daty i godziny (w formacie UTC). Wartość ta będzie ustalona jedynie przez węzeł centralny na potrzeby przekazywanych zapytań. Umożliwi to powiadomienie Strony udzielającej odpowiedzi na zapytanie o tym, kiedy nastąpi przekroczenie czasu oczekiwania dla zapytania. Wartość ta nie jest konieczna w MS2TCN_<x>_Req i wszystkich komunikatach odpowiedzi. Wartość ta nie jest obowiązkowa, dzięki czemu ta sama definicja nagłówka może być używana dla wszystkich typów komunikatów bez względu na to, czy wymagany jest atrybut timeoutValue.	Nie
From (Od)	Kod ISO 3166-1 Alpha 2 Strony wysyłającej komunikat lub „UE".	Tak
To (Do)	Kod ISO 3166-1 Alpha 2 Strony, do której komunikat jest wysyłany, lub „UE".	Tak

Poddodatek 4.4

Transliteracja i usługi NYSIIS (system identyfikacyjno-informacyjny stanu Nowy Jork)

1. Algorytm NYSIIS wdrożony w węźle centralnym jest wykorzystywany do kodowania nazwisk wszystkich kierowców w rejestrze krajowym.

2. Przy wyszukiwaniu karty za pomocą funkcji CIC należy używać kluczy NYSIIS jako podstawowego mechanizmu wyszukiwania.

3. Ponadto Strony mogą stosować algorytm niestandardowy w celu uzyskania dodatkowych wyników.

4. Wyniki wyszukiwania muszą wskazywać mechanizm wyszukiwania, który został użyty do znalezienia zapisu – NYSIIS albo niestandardowy.

5. Jeżeli Strona zdecyduje się na rejestrowanie powiadomień ICDL, wówczas klucze NYSIIS zawarte w powiadomieniu muszą zostać zapisane jako część danych ICDL. Przy wyszukiwaniu danych ICDL Strona musi korzystać z kluczy NYSIIS dla nazwy/nazwiska wnioskodawcy.

Poddodatek 4.5

Wymogi w zakresie bezpieczeństwa

1. HTTPS wykorzystuje się do wymiany komunikatów między węzłem centralnym a systemami krajowymi.

2. Systemy krajowe używają certyfikatów elektronicznych, o których mowa w poddodatkach 4.8 i 4.9, na potrzeby zabezpieczenia przesyłania komunikatów między systemem krajowym a węzłem centralnym.

3. W systemach krajowych należy wdrożyć jako minimum certyfikaty wykorzystujące algorytm skrótu podpisu SHA-2 (SHA-256) oraz klucz publiczny o długości 2 048 bitów.

Poddodatek 4.6

Poziomy usług

1. Systemy krajowe muszą zapewniać następujące minimalne poziomy usług:

1.1. Muszą być dostępne 24 godziny na dobę, 7 dni w tygodniu.

1.2. Ich dostępność musi być monitorowana za pomocą komunikatu typu HEARTBEAT wysyłanego z węzła centralnego.

1.3. Ich wskaźnik dostępności musi wynosić 98 % zgodnie z poniższą tabelą (dane liczbowe zaokrąglono do najbliższej jednostki):

Dostępność na poziomie	oznacza niedostępność		
	dziennie	miesięcznie	rocznie
98 %	0,5 godz.	15 godz.	7,5 dnia

Zachęcając Strony do przestrzegania wskaźnika dostępności dziennej, uznaje się jednak, że pewne niezbędne działania, takie jak utrzymanie systemu, wymagają wyłączenia systemu na czas dłuższy niż 30 minut. Jednakże miesięczne i roczne wskaźniki dostępności pozostają obowiązkowe.

1.4. Systemy krajowe muszą odpowiadać na minimum 98 % zapytań przesyłanych im w ciągu jednego miesiąca kalendarzowego.

1.5. Systemy krajowe muszą dostarczać odpowiedź na zapytania w ciągu 10 sekund.

1.6. Globalny czas oczekiwania dla zapytania (czas, w którym osoba przedstawiająca zapytanie może czekać na odpowiedź) nie może przekraczać 20 sekund.

1.7. Systemy krajowe muszą być w stanie obsługiwać 6 komunikatów na sekundę.

1.8. Systemy krajowe nie mogą przesyłać zapytań do węzła sieci Tachonet z prędkością przekraczającą 2 zapytania na sekundę.

1.9. Każdy system krajowy musi być w stanie poradzić sobie z potencjalnymi problemami technicznymi węzła centralnego lub systemów krajowych innych Stron. Problemy te obejmują między innymi:

a) utratę połączenia z węzłem centralnym;

b) brak odpowiedzi na zapytanie;

c) otrzymanie odpowiedzi po upływie czasu oczekiwania na komunikat;

d) otrzymanie niezamówionych komunikatów;

e) otrzymanie nieważnych komunikatów.

2. Węzeł centralny musi:

2.1. Osiągać wskaźnik dostępności na poziomie 98 %.

2.2. Zapewniać krajowym systemom powiadamianie o wszelkich błędach za pośrednictwem komunikatu odpowiedzi albo za pośrednictwem specjalnego komunikatu o błędzie. Systemy krajowe muszą natomiast odbierać takie specjalne komunikaty o błędach i posiadać eskalacyjny przepływ pracy w celu podjęcia wszelkich właściwych działań, aby skorygować zgłoszony błąd.

3. Utrzymanie

Strony powiadamiają za pośrednictwem aplikacji internetowej pozostałe Strony oraz Komisję Europejską o wszelkich rutynowych czynnościach serwisowych, najpóźniej na tydzień przed rozpoczęciem tych czynności, jeżeli jest to technicznie możliwe.

Poddodatek 4.7

Rejestr zdarzeń i statystyki dotyczące danych gromadzonych w węźle centralnym

1. W celu zapewnienia prywatności dane przekazywane do celów statystycznych mają charakter anonimowy. Dane identyfikujące konkretną kartę, konkretnego kierowcę lub konkretne prawo jazdy nie mogą być dostępne do celów statystycznych.

2. Rejestr zdarzeń stanowi zapis wszystkich operacji na potrzeby monitorowania i diagnostyki oraz umożliwia wygenerowanie statystyk dotyczących tych operacji.

3. Dane osobowe nie mogą być przechowywane w dziennikach dłużej niż sześć miesięcy. Informacje statystyczne są przechowywane bezterminowo.

4. Dane statystyczne wykorzystywane do celów sprawozdawczości obejmują:

   a) Stronę zgłaszającą zapytanie;

   b) Stronę udzielającą odpowiedzi na zapytanie;

   c) rodzaj komunikatu;

   d) kod statusu odpowiedzi;

   e) daty i godziny komunikatów;

   f) czas odpowiedzi.

Poddodatek 4.8

Przepisy ogólne dotyczące elektronicznych kluczy i certyfikatów związanych z systemem Tachonet

1. Dyrekcja Generalna ds. Informatyki Komisji Europejskiej (DIGIT) udostępnia usługę PKI ([1]) (zwaną dalej „usługą infrastruktury klucza publicznego CEF") Umawiającym się Stronom AETR łączącym się z systemem Tachonet (zwanym dalej „organami krajowymi") poprzez platformę eDelivery.

2. Procedura wnioskowania o wydanie i unieważnienie certyfikatów elektronicznych oraz szczegółowe warunki ich stosowania określone są w dodatku.

3. Wykorzystanie certyfikatów:

3.1. Po wydaniu certyfikatu organ krajowy ([2]) korzysta z niego wyłącznie w ramach systemu Tachonet. Certyfikat może być stosowany do:

   a) uwierzytelnienia pochodzenia danych;

   b) zaszyfrowania danych;

   c) zapewnienia wykrywania naruszeń integralności danych.

3.2. Zabrania się jakiegokolwiek wykorzystania bez wyraźnego zezwolenia w ramach dozwolonych zastosowań certyfikatu.

4. Umawiające się Strony:

   a) chronią swoje klucze prywatne przed nieuprawnionym użyciem;

   b) powstrzymują się od przekazywania lub ujawniania swoich kluczy prywatnych osobom trzecim nawet jako przedstawicielom;

([1]) Infrastruktura klucza publicznego (PKI) jest zbiorem ról, polityk, procedur i systemów niezbędnych do tworzenia certyfikatów elektronicznych, zarządzania nimi, ich dystrybucji i unieważniania.

([2]) Identyfikowany za pomocą wartości atrybutu „O=" w podsekcji zawierającej nazwę (Subject Distinguished Name) wydanego certyfikatu.

c) zapewniają poufność, integralność i dostępność kluczy prywatnych wygenerowanych, przechowywanych i używanych na potrzeby systemu Tachonet;

d) powstrzymują się od dalszego korzystania z klucza prywatnego po upływie okresu ważności lub unieważnieniu certyfikatu, z wyjątkiem w celu przeglądania zaszyfrowanych danych (np. odszyfrowywania wiadomości przekazywanych drogą elektroniczną); Klucze, których ważność wygasła, są niszczone lub przechowywane w sposób uniemożliwiający ich używanie;

e) dostarczają organowi rejestrującemu dane identyfikacyjne upoważnionych przedstawicieli, którzy są uprawnieni do występowania o unieważnienie certyfikatów wydanych danej organizacji (wnioski o unieważnienie rejestracji zawierają również wniosek o stwierdzenie wygaśnięcia hasła oraz szczegółowe informacje na temat zdarzeń, które prowadzą do unieważnienia certyfikatów);

f) zapobiegają niewłaściwemu wykorzystywaniu kluczy prywatnych, poprzez zwrócenie się o unieważnienie powiązanego certyfikatu klucza publicznego w przypadku narażenia na szwank bezpieczeństwa klucza prywatnego lub danych dotyczących aktywacji klucza prywatnego;

g) ponoszą odpowiedzialność i są zobowiązane do złożenia wniosku o unieważnienie certyfikatu w sytuacjach określonych w polityce certyfikacji i w oświadczeniu na temat praktyk dotyczących certyfikacji (CPS) centrum certyfikacji;

h) bezzwłocznie powiadamiają organ rejestrujący o utracie, kradzieży lub potencjalnym narażeniu na szwank jakichkolwiek kluczy AETR stosowanych w ramach systemu Tachonet.

5. Zobowiązania

Bez uszczerbku dla odpowiedzialności Komisji Europejskiej w przypadku naruszenia jakichkolwiek wymogów ustanowionych w mającym zastosowanie prawie krajowym lub w odniesieniu do odpowiedzialności za kwestie, które na mocy tego prawa nie mogą zostać wyłączone, Komisja Europejska nie ponosi odpowiedzialności w odniesieniu do:

a) treści certyfikatu, za którą jest odpowiedzialny wyłącznie właściciel certyfikatu. Sprawdzenie prawidłowości treści certyfikatu jest obowiązkiem właściciela certyfikatu;

b) wykorzystania certyfikatu przez jego właściciela.

Poddodatek 4.9

Opis usługi PKI dla systemu Tachonet

1. **Wprowadzenie**

Infrastruktura klucza publicznego (PKI) jest zbiorem ról, polityk, procedur i systemów niezbędnych do tworzenia certyfikatów elektronicznych, zarządzania nimi, ich dystrybucji i unieważniania ([1]). Usługa infrastruktury klucza publicznego CEF platformy eDelivery umożliwia wydawanie certyfikatów elektronicznych i zarządzanie nimi w celu zapewnienia poufności, integralności i niezaprzeczalności informacji wymienianych między punktami dostępu.

Usługa PKI platformy eDelivery opiera się na Trust Center Services TeleSec Shared Business CA (centrum certyfikacji), do którego zastosowanie ma polityka certyfikacji (CP)/oświadczenie na temat praktyk dotyczących certyfikacji (CPS) TeleSec Shared-Business-CA T-Systems International GmbH ([2]).

Usługa infrastruktury klucza publicznego wydaje certyfikaty odpowiednie do zabezpieczenia różnych procesów biznesowych wewnątrz i na zewnątrz przedsiębiorstw, organizacji, organów publicznych i instytucji, którym są one potrzebne do zapewnienia średniego poziomu ochrony w celu udowodnienia autentyczności, integralności i wiarygodności podmiotu końcowego.

2. **Procedura składania wniosku o wydanie certyfikatu**

2.1. Role i obowiązki

2.1.1. „Organizacja" lub „organ krajowy" występujący o certyfikat.

2.1.1.1. Organ krajowy zwraca się o wydanie certyfikatów w ramach Tachonet.

2.1.1.2. Organ krajowy:

a) zwraca się o wydanie certyfikatów przy użyciu usługi infrastruktury klucza publicznego CEF;

([1]) https://pl.wikipedia.org/wiki/Infrastruktura_klucza_publicznego

([2]) Najnowszą wersję polityki certyfikacji i oświadczenia na temat praktyk dotyczących certyfikacji (CPS) można pobrać na stronie internetowej: https://www.telesec.de/en/sbca-en/support/download-area/

b) generuje klucze prywatne i odpowiadające im klucze publiczne, które mają być zawarte w certyfikatach wydanych przez centrum certyfikacji;

c) pobiera certyfikat po jego zatwierdzeniu;

d) podpisuje i odsyła do organu rejestrującego:

(i) formularz identyfikacyjny z danymi osób wyznaczonych do kontaktów i zaufanych kurierów,

(ii) podpisane indywidualne pełnomocnictwo ([1]).

2.1.2. Zaufany kurier

2.1.2.1. Organ krajowy wyznacza zaufanego kuriera.

2.1.2.2. Zaufany kurier:

a) przekazuje klucz publiczny organowi rejestrującemu w trakcie bezpośredniej identyfikacji i procesu rejestracji;

b) uzyskuje odpowiedni certyfikat od organu rejestrującego.

2.1.3. Właściciel domeny

2.1.3.1. Właścicielem domeny jest DG MOVE.

2.1.3.2. Właściciel domeny:

a) zatwierdza i koordynuje sieć Tachonet i architekturę zaufania systemu Tachonet, w tym zatwierdzanie procedur wydawania certyfikatów;

b) obsługuje węzeł centralny Tachonet oraz koordynuje działania Stron dotyczące funkcjonowania systemu Tachonet;

c) przeprowadza, wraz z organami krajowymi, testy łączenia się z systemem Tachonet.

2.1.4. Organ rejestrujący

2.1.4.1. Organem rejestrującym jest Wspólne Centrum Badawcze (JRC).

2.1.4.2. Organ rejestrujący jest odpowiedzialny za weryfikację tożsamości zaufanych kurierów w celu rejestracji i zatwierdzania wniosków o wydanie, unieważnienie i odnowienie certyfikatów elektronicznych.

2.1.4.3. Organ rejestrujący:

a) nadaje organowi krajowemu niepowtarzalny identyfikator;

b) uwierzytelnia tożsamość organu krajowego, jego punktów kontaktowych i zaufanych kurierów;

c) kontaktuje się z zespołem wsparcia w ramach CEF odnośnie do autentyczności organu krajowego, jego punktów kontaktowych i zaufanych kurierów;

d) informuje organ krajowy o zatwierdzeniu lub odrzuceniu certyfikatu.

2.1.5. Centrum certyfikacji

2.1.5.1. Centrum certyfikacji jest odpowiedzialne za zapewnienie infrastruktury technicznej do celów wnioskowania o wydanie, wydawania i unieważniania certyfikatów elektronicznych.

2.1.5.2. Centrum certyfikacji:

a) zapewnia infrastrukturę techniczną do celów składania wniosków o wydanie certyfikatu przez organy krajowe;

b) zatwierdza lub odrzuca wniosek o wydanie certyfikatu;

c) w razie potrzeby kontaktuje się z organem rejestrującym w celu weryfikacji tożsamości organizacji składającej wniosek.

2.2. Wydanie certyfikatu

2.2.1. Wydanie certyfikatu odbywa się zgodnie z następującymi kolejnymi etapami przedstawionymi na rysunku 1:

a) **Etap 1:** Identyfikacja zaufanych kurierów;

([1]) Pełnomocnictwo jest dokumentem prawnym, na mocy którego organizacja uprawnia i upoważnia Komisję Europejską reprezentowaną przez wyznaczonego urzędnika odpowiedzialnego za usługę infrastruktury klucza publicznego CEF do zwrócenia się o wygenerowanie certyfikatu w jej imieniu przez T-Systems International GmbH TeleSec Shared Business CA. Zob. również pkt 6.

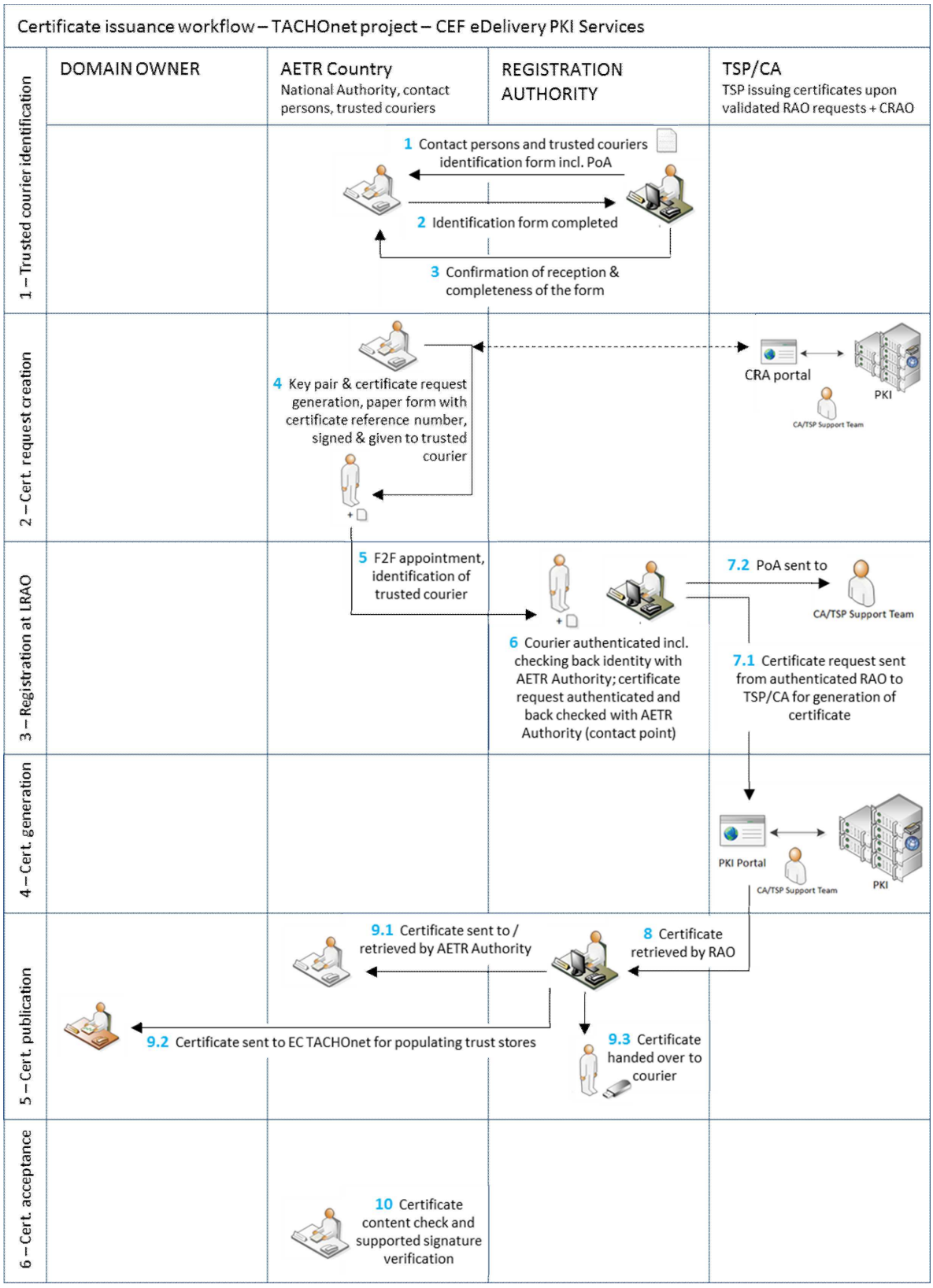
b) **Etap 2:** Utworzenie wniosku o wydanie certyfikatu;

c) **Etap 3:** Rejestracja w organie rejestrującym;

d) **Etap 4:** Generowanie certyfikatu;

e) **Etap 5:** Publikacja certyfikatu;

f) **Etap 6:** Akceptacja certyfikatu.



Rysunek 1 – Przebieg procedury wydawania certyfikatów

2.2.2. Etap 1: Identyfikacja zaufanego kuriera

Na potrzeby identyfikacji zaufanego kuriera przeprowadza się następującą procedurę:

a) Organ rejestrujący przekazuje organowi krajowemu formularz identyfikacyjny z danymi osób wyznaczonych do kontaktów oraz zaufanych kurierów ([1]). Formularz ten zawiera również pełnomocnictwo, które organizacja (organ AETR) podpisuje.

b) Organ krajowy odsyła wypełniony formularz i podpisane pełnomocnictwo do organu rejestrującego.

c) Organ rejestrujący potwierdza odbiór i kompletność formularza.

d) Organ rejestrujący przekazuje właścicielowi domeny zaktualizowaną kopię listy osób wyznaczonych do kontaktów i zaufanych kurierów.

2.2.3. Etap 2: Utworzenie wniosku o wydanie certyfikatu

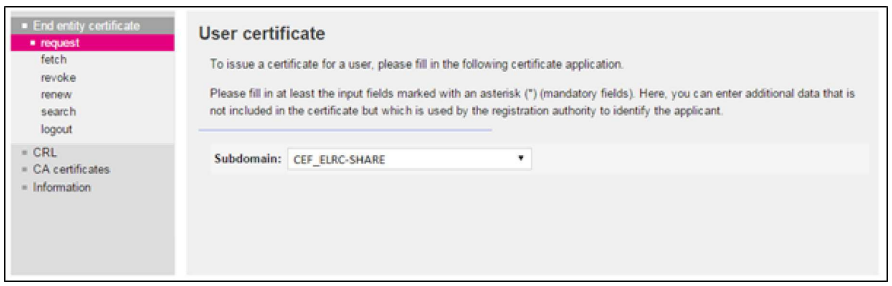
2.2.3.1. Wniosek o wydanie certyfikatu i jego pobranie odbywa się na tym samym komputerze i przy użyciu tej samej przeglądarki.

2.2.3.2. Na potrzeby utworzenia wniosku o wydanie certyfikatu przeprowadza się następującą procedurę:

a) W celu zwrócenia się o wydanie certyfikatu za pośrednictwem adresu URL organizacja przechodzi do internetowego interfejsu użytkownika https://sbca.telesec.de/sbca/ee/login/displayLogin.html?locale=en: i wpisuje nazwę użytkownika „**sbca/CEF_eDelivery.europa.eu**” oraz hasło „**digit.333**”

Rysunek 2

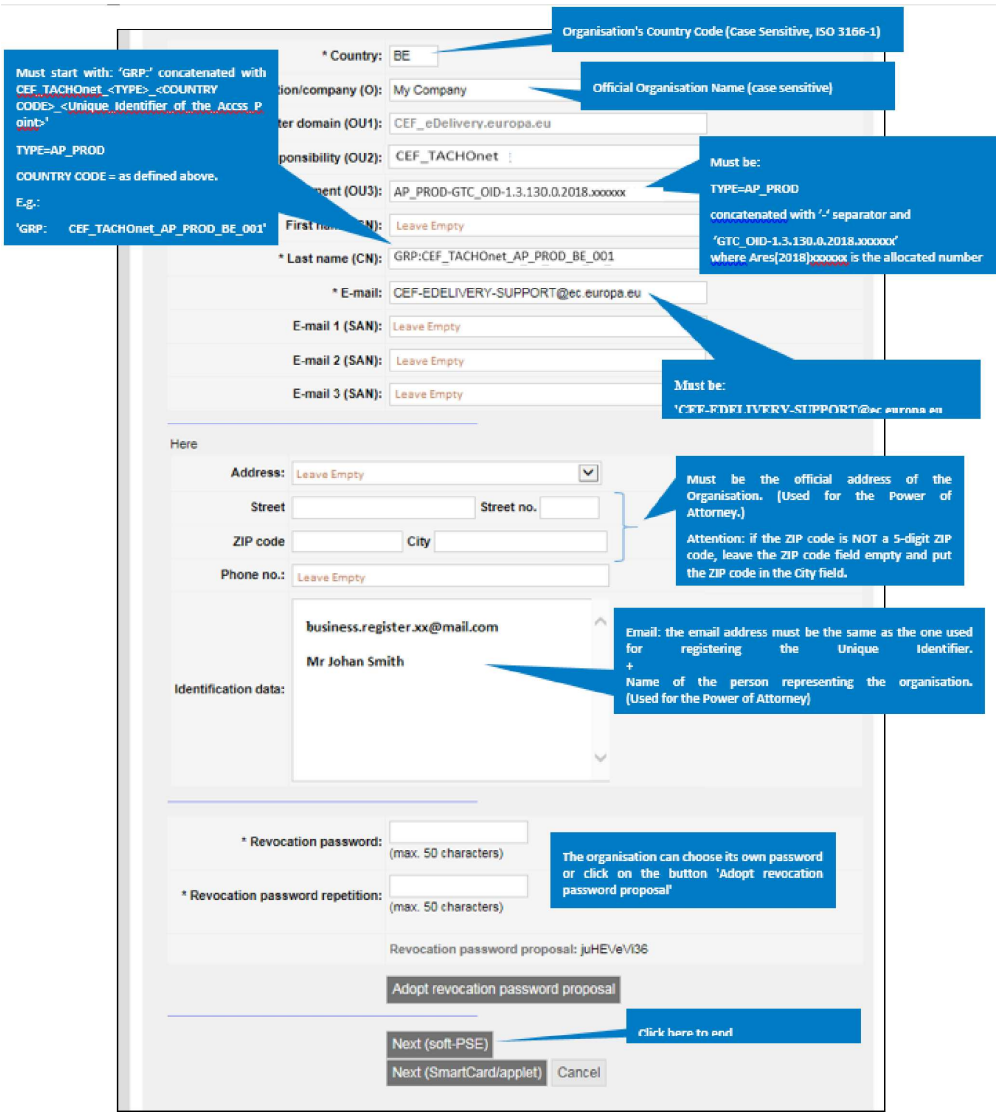
b) Organizacja klika na „request” (wniosek) po lewej stronie panelu i wybiera „CEF_TACHOnet” na rozwijanej liście.



Rysunek 3

c) Organizacja uzupełnia formularz wniosku o wydanie certyfikatu przedstawiony na rysunku 4 informacjami podanymi w tabeli 3, klikając na „Next (»soft-PSE«)” w celu zakończenia procesu.

([1]) Zob. pkt 5.



Rysunek 4

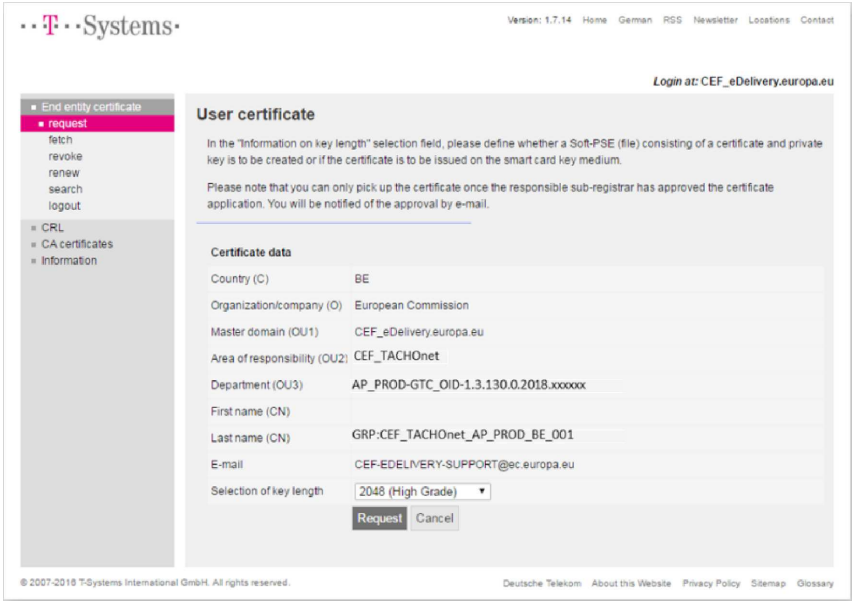
Wymagane pola	Opis
Country [państwo]	**C = kod państwa**, lokalizacja właściciela certyfikatu, zweryfikowana przy użyciu publicznego spisu; Ograniczenia: 2 znaki, zgodnie z normą ISO 3166-1, alpha-2; rozróżnianie wielkich i małych liter; przykłady: DE, BE, NL, Przypadki szczególne: UK (dla Wielkiej Brytanii), EL (dla Grecji)
Organisation/Company (O) [organizacja/przedsiębiorstwo]	**O = nazwa organizacji właściciela certyfikatu**
Master domain (OU1) [główna domena]	**OU = CEF_eDelivery.europa.eu**
Area of responsibility (OU2) [obszar odpowiedzialności]	**OU = CEF_TACHOnet**

Wymagane pola	Opis
Department (OU3) [wydział]	Wartość obowiązkowa dla „AREA OF RESPONSIBILITY" [obszar odpowiedzialności] W przypadku gdy wymagany jest certyfikat, jego treść musi zostać sprawdzona z wykorzystaniem wykazu pozytywnego (biała lista). Jeżeli informacje nie są zgodne z wykazem, wniosek zostaje zablokowany. Format: **OU=<TYPE>-<GTC_NUMBER>** Gdzie „< TYPE >" zostaje zastąpiony przez AP_PROD: Punkt dostępu w środowisku produkcyjnym. Oraz gdzie <GTC_NUMBER> to **GTC_OID-1.3.130.0.2018.xxxxxx**, gdzie Ares(2018)xxxxxx jest numerem GTC dla projektu Tachonet. Np.: AP_PROD-GTC_OID-1.3.130.0.2018.xxxxxx
First name (CN) [imię]	Musi pozostać puste.
Last name (CN) [nazwisko]	Musi zaczynać się od „GRP", po czym następuje nazwa zwyczajowa. Format: **CN = GRP:<AREA OF RESPONSIBILITY>_<TYPE>_<COUNTRY CODE>_<UNIQUE IDENTIFIER>** Np.: GRP:CEF_TACHOnet_AP_PROD_BE_001
E-mail	**E = CEF-EDELIVERY-SUPPORT@ec.europa.eu**
E-mail 1 (SAN)	Musi pozostać puste.
E-mail 2 (SAN)	Musi pozostać puste.
E-mail 3 (SAN)	Musi pozostać puste.
Address [adres]	Musi pozostać puste.
Street [ulica]	Musi być oficjalnym adresem organizacji właściciela certyfikatu. (Stosowane w przypadku pełnomocnictwa.)
Street no.	Musi być oficjalnym adresem organizacji właściciela certyfikatu. (Stosowane w przypadku pełnomocnictwa.)
Zip Code [kod pocztowy]	Musi być oficjalnym adresem organizacji właściciela certyfikatu. (Stosowane w przypadku pełnomocnictwa.) **Uwaga:** jeżeli kod pocztowy nie jest 5-cyfrowym kodem pocztowym, pole to należy pozostawić puste i wpisać kod pocztowy w polu dotyczącym miejscowości.
City [miejscowość]	Musi być oficjalnym adresem organizacji właściciela certyfikatu. (Stosowane w przypadku pełnomocnictwa.) **Uwaga:** jeżeli kod pocztowy nie jest 5-cyfrowym kodem pocztowym, pole to należy pozostawić puste i wpisać kod pocztowy w polu dotyczącym miejscowości.
Phone no [numer telefonu]	Musi pozostać puste.

Wymagane pola	Opis
Identification data [dane identyfikacyjne]	Adres poczty elektronicznej musi być taki sam, jak adres stosowany do rejestracji niepowtarzalnego identyfikatora. + Musi być imię i nazwisko osoby reprezentującej organizację. (Stosowane w przypadku pełnomocnictwa.) **+ Commercial Register No** [numer w rejestrze handlowym] (obowiązkowe wyłącznie dla organizacji prywatnych) **Entered at the Local Court of** [wpis w lokalnym sądzie] (wymagane tylko w przypadku niemieckich i austriackich organizacji prywatnych)
Revocation password [hasło unieważnienia]	Pole obowiązkowe wybrane przez wnioskodawcę
Revocation password repetition [powtórzenie hasła unieważnienia]	Pole obowiązkowe wybrane przez wnioskodawcę (powtórzenie)

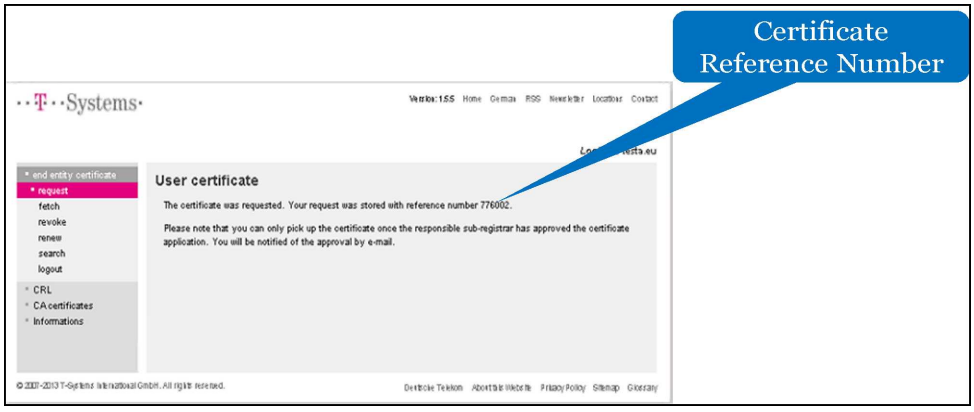
Tabela 3. Pełne dane o każdym wymaganym polu

d) Wybrana długość klucza powinna wynosić 2 048 (High Grade).



Rysunek 5

e) Organizacja rejestruje numer referencyjny w celu pobrania certyfikatu.



Rysunek 6

f) Zespół wsparcia CEF sprawdza nowe wnioski o wydanie certyfikatów oraz weryfikuje, czy informacje zawarte we wniosku o wydanie certyfikatu są ważne, tj. czy są zgodne z konwencją nazewnictwa określoną w dodatku 5.1 do Konwencji o nazwach certyfikatów.

g) Zespół wsparcia CEF sprawdza, czy informacje zawarte we wniosku są w prawidłowym formacie.

h) Jeżeli weryfikacja przewidziana w pkt 5 lub 6 powyżej nie powiedzie się zespół wsparcia CEF przesyła wiadomość e-mail na adres poczty elektronicznej podany w polu „Dane identyfikacyjne" formularza wniosku, wraz z kopią (w „cc") do właściciela domeny, w którym organizacja proszona jest o ponowne rozpoczęcie tej procedury. Nieudany wniosek o wydanie certyfikatu zostaje unieważniony.

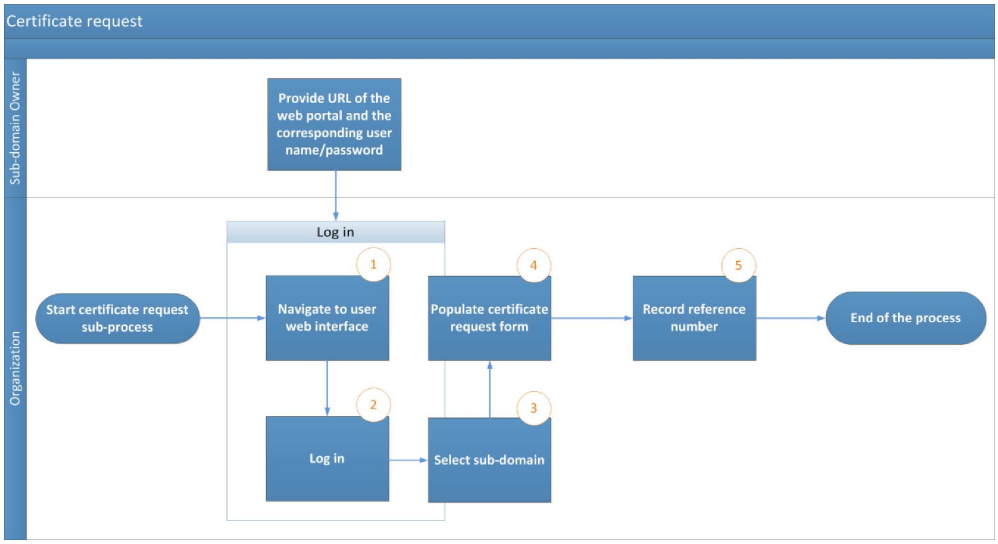
i) Zespół wsparcia CEF wysyła do organu rejestrującego wiadomość e-mail dotyczącą ważności wniosku. Wiadomość e-mail zawiera:

1) nazwę organizacji dostępną w polu „Organisation (O)" [organizacja] wniosku o wydanie certyfikatu;

2) dane dotyczące certyfikatu, w tym nazwę podmiotu, dla którego certyfikat ma zostać wydany, dostępną w polu „Last Name (CN)" [nazwisko] wniosku o wydanie certyfikatu;

3) numer referencyjny certyfikatu;

4) adres organizacji, jej adres e-mail oraz imię i nazwisko osoby ją reprezentującej.



Rysunek 7 – Procedura składania wniosku o wydanie certyfikatu

2.2.4. Etap 3: Rejestracja w organie rejestrującym (zatwierdzenie certyfikatu)

2.2.4.1. Zaufany kurier lub punkt kontaktowy ustala –w drodze wymiany wiadomości e-mail – termin spotkania z organem rejestrującym, podając dane zaufanego kuriera, który osobiście weźmie udział w spotkaniu.

2.2.4.2. Organizacja przygotowuje pakiet dokumentów składający się z:

a) wypełnionego i podpisanego pełnomocnictwa;

b) kopii ważnego paszportu zaufanego kuriera, który weźmie udział w spotkaniu. Kopia ta musi być podpisana przez jeden z określonych na etapie 1 zidentyfikowanych punktów kontaktowych organizacji;

c) formularza wniosku w papierowej formie o wydanie certyfikatu podpisanego przez jeden z punktów kontaktowych organizacji.

2.2.4.3. Organ rejestrujący przyjmuje zaufanego kuriera po przeprowadzeniu kontroli tożsamości w recepcji budynku. Organ rejestrujący przeprowadza bezpośrednią rejestrację wniosku o wydanie certyfikatu, dokonując:

a) identyfikacji i uwierzytelnienia zaufanego kuriera;

b) weryfikacji fizycznego wyglądu zaufanego kuriera w oparciu o przedstawiony przez niego paszport;

c) weryfikacji ważności paszportu przedstawionego przez zaufanego kuriera;

d) weryfikacji ważnego paszportu przedstawionego przez zaufanego kuriera w porównaniu z kopią ważnego paszportu zaufanego kuriera podpisaną przez jeden ze zidentyfikowanych punktów kontaktowych organizacji. Podpis jest uwierzytelniany w oparciu o oryginalny „formularz identyfikacyjny z danymi osób wyznaczonych do kontaktów oraz zaufanych kurierów";

e) weryfikacji wypełnionego i podpisanego pełnomocnictwa;

f) weryfikacji formularza wniosku w papierowej formie o wydanie certyfikatu oraz jego podpisu w oparciu o oryginalny „formularz identyfikacyjny z danymi osób wyznaczonych do kontaktów oraz zaufanych kurierów";

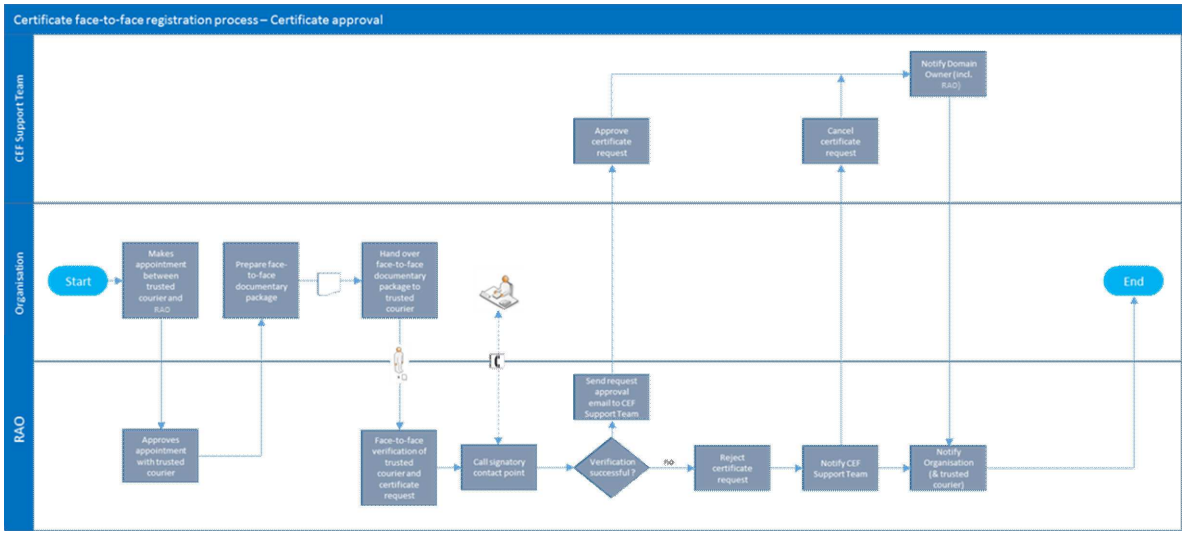
g) ponownego sprawdzenia, w drodze rozmowy telefonicznej z punktem kontaktowym, który podpisał wniosek, tożsamości zaufanego kuriera oraz treści wniosku o wydanie certyfikatu.

2.2.4.4. Organ rejestrujący potwierdza zespołowi wsparcia CEF, że organ krajowy w istocie jest uprawniony do korzystania z elementów, w odniesieniu do których występuje o wydanie certyfikatów, oraz że odpowiedni proces rejestracji bezpośredniej był skuteczny. Potwierdzenie wysyła się pocztą elektroniczną zabezpieczoną przy użyciu certyfikatu „CommiSign", załączając zeskanowaną kopię poświadczonego pakietu z rejestracji bezpośredniej oraz podpisaną listę kontrolną z weryfikacji przeprowadzonej przez organ rejestracyjny.

2.2.4.5. Jeżeli organ rejestrujący potwierdzi ważność wniosku, proces przeprowadza się zgodnie z wymogami określonymi w pkt 2.2.4.6 i 2.2.4.7. W przeciwnym razie wniosek o wydanie certyfikatu zostaje odrzucony, a organizacja zostaje o tym poinformowana.

2.2.4.6. Zespół wsparcia CEF zatwierdza wniosek o wydanie certyfikatu i powiadamia organ rejestrujący o zatwierdzeniu certyfikatu.

2.2.4.7. Organ rejestrujący powiadamia organizację, że certyfikat można pobrać za pośrednictwem portalu użytkownika.



Rysunek 8 – Zatwierdzenie certyfikatu

2.2.5. Etap 4: Generowanie certyfikatu

Po zatwierdzeniu wniosku o wydanie certyfikatu certyfikat zostaje wygenerowany.

2.2.6. Etap 5: Publikacja i pobieranie certyfikatu

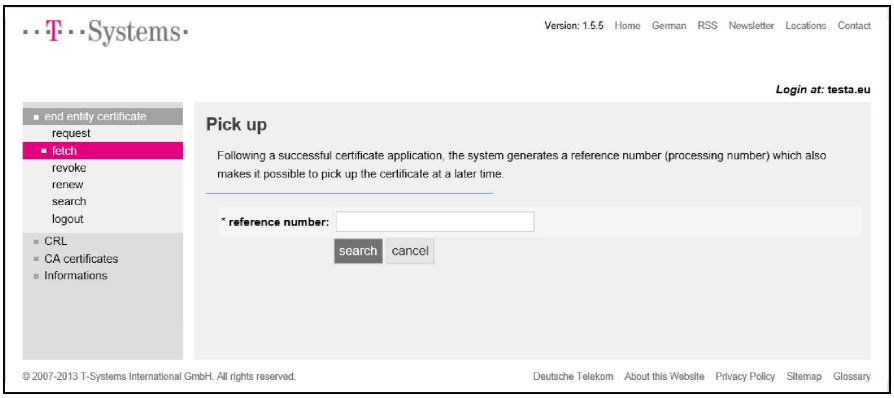
2.2.6.1. Po zatwierdzeniu wniosku o wydanie certyfikatu organ rejestrujący pobiera certyfikat i przekazuje jego kopię zaufanemu kurierowi.

2.2.6.2. Organizacja otrzymuje powiadomienie od organu rejestrującego, że certyfikat może zostać pobrany. Organizacja przechodzi do portalu użytkownika:

2.2.6.3. Organizacja przechodzi do portalu uzytkownika: https://sbca.telesec.de/sbca/ee/login/displayLogin.html?locale=en i loguje się przy użyciu nazwy użytkownika „**sbca/CEF_eDelivery.europa.eu**” oraz hasła „**digit.333**”.

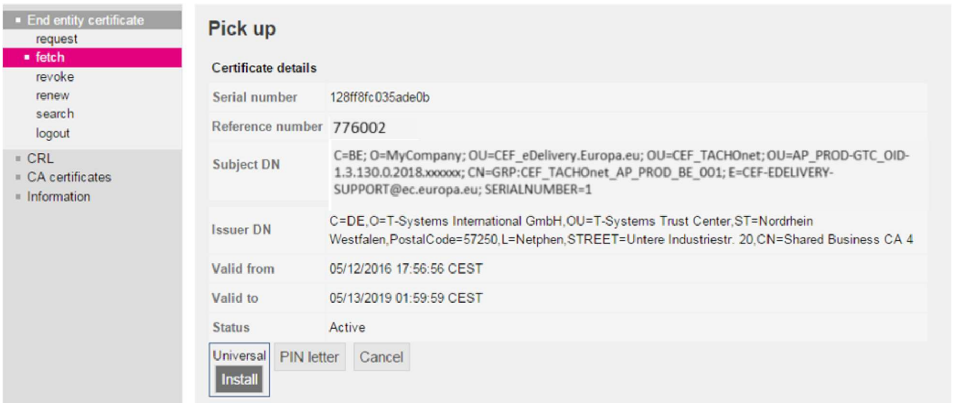
Rysunek 9

2.2.6.4. Organizacja powinna kliknąć na zakładkę „fetch” (pobierz) po lewej stronie ekranu i podać numer referencyjny zarejestrowany na etapie składania wniosku o wydanie certyfikatu;



Rysunek 10

2.2.6.5. Organizacja instaluje certyfikaty, klikając na zakładkę „install” (zainstaluj);



Rysunek 11

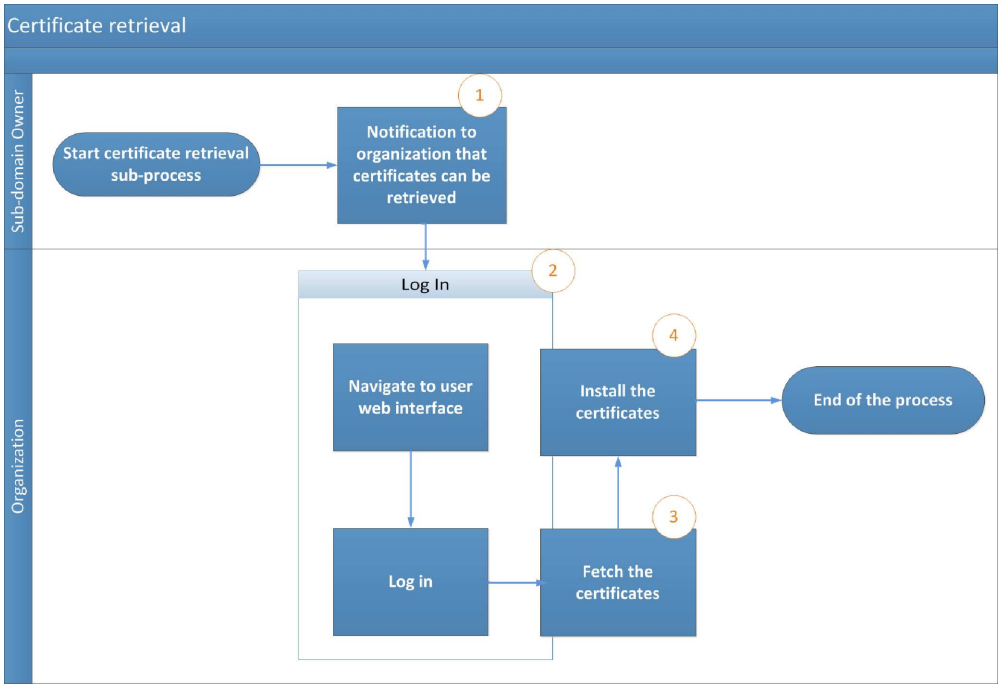
2.2.6.6. Certyfikat należy zainstalować w punkcie dostępu. W związku z tym, że instalacja zależy od wdrożenia, organizacja powinna zwrócić się do swojego dostawcy punktu dostępu w celu uzyskania opisu tej procedury.

2.2.6.7. Instalację certyfikatu w punkcie dostępu przeprowadza się w następujących etapach:

a) eksport klucza prywatnego i certyfikatu;

b) utworzenie „keystore” i „truststore”;

c) zainstalowanie „keystore” i „truststore” w punkcie dostępu.

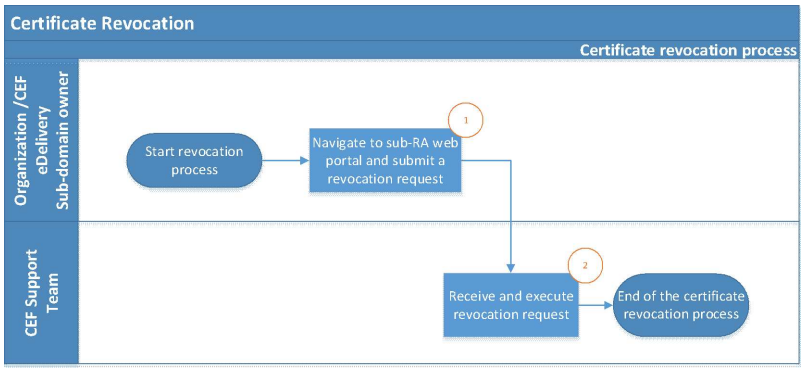


Rysunek 12 – Pobranie certyfikatu

3. **Proces unieważnienia certyfikatu**

3.1. Organizacja przedkłada wniosek o unieważnienie certyfikatu za pośrednictwem internetowego portalu użytkownika;

3.2. Zespół wsparcia CEF przeprowadza unieważnienie certyfikatu.



Rysunek 13 – Unieważnienie certyfikatu

4. **Ogólne warunki korzystania z usługi infrastruktury klucza publicznego CEF**

4.1. Kontekst

Jako dostawca rozwiązań modułu eDelivery instrumentu „Łącząc Europę”, DIGIT udostępnia usługę infrastruktury klucza publicznego ([1]) („usługę infrastruktury klucza publicznego CEF”) Umawiającym się Stronom AETR. Usługa infrastruktury klucza publicznego CEF jest wykorzystywana przez organy krajowe („użytkowników końcowych”) uczestniczących w systemie Tachonet.

DIGIT jest dzierżawcą PKI w ramach rozwiązania TeleSec Shared-Business-CA solution („SBCA”) wykorzystywanego w ramach Trust Center jednostki grupy T-Systems International GmbH („T-Systems” ([2])). DIGIT pełni funkcję Master Registrar dla domeny „CEF_eDelivey.europa.eu” SBCA. W tej roli DIGIT tworzy poddomeny w obrębie domeny „CEF_eDelivery.europa.eu” dla każdego projektu za pośrednictwem usługi infrastruktury klucza publicznego CEF.

([1]) Infrastruktura klucza publicznego (PKI) jest zbiorem ról, polityk, procedur i systemów niezbędnych do tworzenia certyfikatów elektronicznych, zarządzania nimi, ich dystrybucji i unieważniania.

([2]) Zaufana rola operatora Trust Center umiejscowionego w Trust Center T-Systems obejmuje również zadania wewnętrznego organu rejestrującego.

Niniejszy dokument zawiera szczegółowe warunki dotyczące poddomeny Tachonet. DIGIT odgrywa rolę podrejestratora dla tej poddomeny. W tym charakterze wydaje, unieważnia i odnawia certyfikaty dla tego projektu.

4.2. Klauzula o wyłączeniu odpowiedzialności

Komisja Europejska nie ponosi żadnej odpowiedzialności za treść certyfikatu, która leży wyłącznie w gestii właściciela certyfikatu. Sprawdzenie prawidłowości treści certyfikatu jest obowiązkiem właściciela certyfikatu.

Komisja Europejska nie ponosi żadnej odpowiedzialności za sposób wykorzystania certyfikatu przez jego właściciela, będącego trzecim podmiotem prawnym poza Komisją Europejską.

Celem niniejszej klauzuli o wyłączeniu odpowiedzialności nie jest ograniczenie odpowiedzialności Komisji Europejskiej w sposób sprzeczny z wymogami ustanowionymi w obowiązującym ustawodawstwie krajowym lub wyłączenie jej odpowiedzialności w przypadkach, które nie mogą zostać objęte wyłączeniem, zgodnie ze wspomnianym ustawodawstwem.

4.3. Dozwolone/niedozwolone sposoby korzystania z certyfikatów

4.3.1. Dozwolone wykorzystanie certyfikatów

Po wydaniu certyfikatu właściciel certyfikatu ([1]) korzysta z niego wyłącznie w ramach systemu Tachonet. W tym kontekście certyfikat może być stosowany do:

— uwierzytelnienia pochodzenia danych,

— zaszyfrowania danych,

— zapewnienia wykrywania naruszeń integralności danych.

4.3.2. Niedozwolone wykorzystanie certyfikatów

Zabrania się jakiegokolwiek wykorzystania bez wyraźnego zezwolenia w ramach dozwolonych zastosowań certyfikatu.

4.4. Dodatkowe obowiązki właściciela certyfikatu

Szczegółowe warunki SBCA określone są przez T-Systems w polityce certyfikacji (CP)/oświadczeniu na temat praktyk dotyczących certyfikacji (CPS) usługi SBCA ([2]). Niniejszy dokument zawiera specyfikacje i wytyczne dotyczące bezpieczeństwa w odniesieniu do aspektów technicznych i organizacyjnych oraz opisuje działania operatora Trust Centre w rolach centrum certyfikacji i organu rejestrującego, a także delegowanej strony trzeciej organu rejestrującego.

Jedynie podmioty uprawnione do udziału w systemie Tachonet mogą wystąpić o wydanie certyfikatu.

Jeżeli chodzi o akceptację certyfikatu, zastosowanie ma klauzula 4.4.1 polityki certyfikacji i oświadczenia na temat praktyk dotyczących certyfikacji SBCA; ponadto warunki użytkowania i przepisy opisane w niniejszym dokumencie są uznawane za przyjęte przez organizację, dla której wydano certyfikat („O=”), w momencie jego pierwszego użycia.

Jeżeli chodzi o publikację certyfikatu, zastosowanie ma klauzula 2.2 polityki certyfikacji i oświadczenia na temat praktyk dotyczących certyfikacji SBCA.

Wszyscy właściciele certyfikatów muszą przestrzegać poniższych wymogów:

1) chronią swoje klucze prywatne przed nieuprawnionym użyciem;

2) powstrzymują się od przekazywania lub ujawniania swoich kluczy prywatnych osobom trzecim nawet jako przedstawicielom;

3) powstrzymują się od dalszego korzystania z klucza prywatnego po upływie okresu ważności lub unieważnieniu certyfikatu, z wyjątkiem w celu przeglądania zaszyfrowanych danych (np. odszyfrowywania wiadomości przekazywanych drogą elektroniczną);

4) właściciel certyfikatu jest odpowiedzialny za kopiowanie lub przekazywanie klucza podmiotowi lub podmiotom końcowym;

([1]) Identyfikowany za pomocą wartości atrybutu „O=” w podsekcji zawierającej nazwę (Subject Distinguished Name) wydanego certyfikatu.
([2]) Najnowsza wersja polityki certyfikacji/oświadczenia na temat praktyk dotyczących certyfikacji T-Systems SBCA jest dostępna pod adresem https://www.telesec.de/en/sbca-en/support/download-area/.

5) właściciel certyfikatu musi zobowiązać podmiot końcowy/wszystkie podmioty końcowe do przestrzegania aktualnych warunków, w tym polityki certyfikacji i oświadczenia na temat praktyk dotyczących certyfikacji SBCA w odniesieniu do klucza prywatnego;

6) właściciel certyfikatu musi przedstawić identyfikację upoważnionych przedstawicieli, którzy są uprawnieni do występowania o unieważnienie certyfikatów wydanych organizacji, oraz szczegółowe informacje na temat zdarzeń, które prowadzą do unieważnienia, a także hasło unieważnienia;

7) w przypadku certyfikatów związanych z grupami osób i funkcji lub osobami prawnymi, po opuszczeniu grupy przez daną osobę (np. ustanie stosunku pracy) właściciel certyfikatu musi zapobiec niewłaściwemu wykorzystywaniu klucza prywatnego poprzez unieważnienie certyfikatu;

8) Właściciel certyfikatu jest odpowiedzialny za wystąpienie z wnioskiem o unieważnienie certyfikatu w sytuacjach, o których mowa w klauzuli 4.9.1 polityki certyfikacji i oświadczenia na temat praktyk dotyczących certyfikacji SBCA.

Jeżeli chodzi o odnowienie certyfikatu lub utworzenie nowego klucza dla certyfikatów, zastosowanie ma klauzula 4.6 lub 4.7 polityki certyfikacji i oświadczenia na temat praktyk dotyczących certyfikacji SBCA.

Jeżeli chodzi o zmianę certyfikatu, zastosowanie ma klauzula 4.8 polityki certyfikacji i oświadczenia na temat praktyk dotyczących certyfikacji SBCA.

Jeżeli chodzi o unieważnienie certyfikatu, zastosowanie ma klauzula 4.9 polityki certyfikacji i oświadczenia na temat praktyk dotyczących certyfikacji SBCA.

5. **Formularz identyfikacyjny z danymi osób wyznaczonych do kontaktów i zaufanych kurierów (wzór)**

Ja, niżej podpisany, *[imię i nazwisko oraz adres przedstawiciela organizacji],* **zaświadczam, że następujące informacje mają być wykorzystywane w kontekście wniosku, generowania i pobierania certyfikatów cyfrowych klucza publicznego dla punktów dostępu systemu Tachonet wspierających poufność, integralność i niezaprzeczalność komunikatów Tachonet:**

Informacje na temat osób wyznaczonych do kontaktów:

— **Osoba wyznaczona do kontaktów #1**	— **Osoba wyznaczona do kontaktów #2**
— Nazwisko:	— Nazwisko:
— Imię lub imiona;	— Imię lub imiona;
— Telefon komórkowy:	— Telefon komórkowy:
— Telefon:	— Telefon:
— E-mail:	— E-mail:
— Wzór odręcznego podpisu —	— Wzór odręcznego podpisu — — —

Informacje na temat zaufanych kurierów:

— **Zaufany kurier #1**	— **Zaufany kurier #2**
— Nazwisko:	— Nazwisko:
— Imię lub imiona;	— Imię lub imiona;
— Telefon komórkowy:	— Telefon komórkowy:
— E-mail:	— E-mail:
— Państwo, które wydało paszport:	— Państwo, które wydało paszport:
— Nr paszportu:	— Nr paszportu:
— Data zakończenia ważności paszportu:	— Data zakończenia ważności paszportu:

Miejsce, data, pieczęć firmowa lub pieczęć organizacji:

Podpis upoważnionego przedstawiciela:

6. **Dokumenty**

6.1. Indywidualne pełnomocnictwo (wzór)

Przykładowe indywidualne pełnomocnictwo, które musi zostać podpisane i przedstawione przez zaufanego kuriera w trakcie rejestracji bezpośredniej w organie rejestrującym, można znaleźć pod adresem:

Please print the text of this document on your letterhead, add your company stamp and have it signed by the administrative contact or admin-c of the domain.
The power of attorney must be signed by an authorized representative of the organization (principal).

The Shared-Business-CA customer will then submit this document together with the order document to the T-Systems International GmbH Trust Center.

Individual power of attorney / Power of attorney granted to one person

I, ***[name and address of the end-user]***, empower as an authorized person of this organization *

[name of the company receiving the certificate]

(e. g. sample company, sample authority, to be registered in the O-field of the certificate *)

following company and/or person:

Company: **European Commission**
Address: **DG DIGIT, 28 rue Belliard, 1000 Brussels**
Represented by Mr/Mrs/Ms: **Adrien FERIAL**

On my behalf, by complying with all and any regulations and formalities (particularly Certificate Policy (CP) / Certification Practice Statement (CPS)), for authorisation to manage (i.e. issue, revoke, renew) X.509v3-certificates, including the complete key-material, issued by the certification authority „TeleSec Shared-Business-CA", in respect of the domain as above mentioned.

This power of attorney relates to issuing and management of the following certificate types (the applicable type has to be marked):

☒ user[1]: e.g. mail security (signature, encryption), virtual private network (VPN), TLS/SSL client

☐ server[2]: e.g. identity of web server, TLS/SSL client server authentication
Please enter additionally the country, organization, locality, state or province name of the server:
_____

☐ eMail-Gateway[3]: e.g. identity of eMail gateways / eMail-Appliance, virtual mail-administrating centre.

Validity

☒ The power of attorney is valid until further notice, but up to a **maximum of 27 months**[2] or **maximum of 36 months**[1,3] from date of issuance.

☐ The power of attorney is valid until _____ (mm.dd.yyyy), but up to a **maximum of 27 month**[2] months or **maximum of 36 months**[1,3] from date of issuance.

Please note that a time limit on the power of attorney can cause that a request for certificate order, renewal or revocation may not be possible because the validity period of the authorization has been exceeded!

Place, date, company stamp or seal of the organisation (principal)

Signature of the authorized representative

6.2. Formularz wniosku w papierowej formie o wydanie certyfikatu (wzór)

Wzór formularza wniosku w papierowej formie o wydanie certyfikatu, który musi zostać podpisany i przedstawiony przez zaufanego kuriera w trakcie rejestracji bezpośredniej w siedzibie organu rejestrującego, można znaleźć pod adresem:

TACHOnet certificate request paper form

I, ***[name and address of the organisation representative]***, certifies that the following information are to be used in the context of the request, generation and retrieval of public key digital certificates for TACHOnet access points supporting the confidentiality, integrity and non-repudiation of the TACHOnet messages:

Please reproduce the certificate data information provided by CEF Support Team acknowledging the completeness of the electronic certificate request, e.g.:

Certificate data	
Country (C)	BE
Organization/company (O)	European Commission
Master domain (OU1)	CEF_eDelivery.europa.eu
Area of responsibility (OU2)	CEF_TACHOnet
Department (OU3)	AP_PROD-GTC_OID-1.3.130.0.2018.xxxxxx
First name (CN)	
Last name (CN)	GRP:CEF_TACHOnet_AP_PROD_BE_001
E-mail	CEF-EDELIVERY-SUPPORT@ec.europa.eu

Certificate request reference number: *insert reference number (e.g. 776002)*
Identification of the trusted courier proceeding to the face-to-face registration of the request: *please fill in*

Trusted courier #1
Name:
First names:
Mobile phone:
Email:
Passport issuing country:
Passport number:
Passport validity end date:

Place, date, company stamp or seal of the Organisation:

Signature of the authorised representative:

7. **Glosariusz**

Najważniejsze terminy stosowane w niniejszym poddodatku zdefiniowane są w sekcji „CEF Definitions” [definicje CEF] na jednolitym portalu internetowym instrumentu „Łącząc Europę”:

https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/CEF+Definitions

Najważniejsze skróty stosowane w niniejszym poddodatku zdefiniowane są w sekcji „CEF Glossary” [glosariusz CEF] na jednolitym portalu internetowym instrumentu „Łącząc Europę”:

https://ec.europa.eu/cefdigital/wiki/pages/viewpage.action?spaceKey=CEFDIGITAL&title=CEF+Glossary