ROZPORZĄDZENIE DELEGOWANE KOMISJI (UE) 2026/1436

z dnia 1 lipca 2026 r.

uzupełniające dyrektywę Parlamentu Europejskiego i Rady (UE) 2024/2841 w odniesieniu do określenia kodu QR na fizycznej wersji europejskiej karty osoby z niepełnosprawnością oraz określenia kodu QR i ustanowienia wspólnych specyfikacji technicznych zapewniających bezpieczeństwo fizycznej wersji europejskiej karty parkingowej dla osób z niepełnosprawnościami, a także w odniesieniu do kwestii interoperacyjności

(Tekst mający znaczenie dla EOG)

KOMISJA EUROPEJSKA,

uwzględniając Traktat o funkcjonowaniu Unii Europejskiej,

uwzględniając dyrektywę Parlamentu Europejskiego i Rady (UE) 2024/2841 z dnia 23 października 2024 r. w sprawie ustanowienia europejskiej karty osoby z niepełnosprawnością i europejskiej karty parkingowej dla osób z niepełnosprawnościami ([1]), w szczególności jej art. 7 ust. 7 i art. 8 ust. 7,

a także mając na uwadze, co następuje:

(1) W dyrektywie (UE) 2024/2841 ustanowiono przepisy regulujące wydawanie europejskiej karty osoby z niepełnosprawnością i europejskiej karty parkingowej dla osób z niepełnosprawnościami oraz wspólne wzory tych kart. Zgodnie z art. 7 ust. 2 i art. 8 ust. 2 dyrektywy (UE) 2024/2841 europejskie karty osoby z niepełnosprawnością i europejskie karty parkingowe dla osób z niepełnosprawnościami wydane przez państwa członkowskie mają być wzajemnie uznawane we wszystkich państwach członkowskich.

(2) Uprawnienia przewidziane w art. 7 ust. 7 i art. 8 ust. 7 dyrektywy (UE) 2024/2841 mają ten sam cel, a mianowicie zapobieganie oszustwom i ich zwalczanie, zapewnienie bezpieczeństwa fizycznych wersji europejskiej karty osoby z niepełnosprawnością i europejskiej karty parkingowej dla osób z niepełnosprawnościami, w tym za pomocą odpowiednich środków bezpieczeństwa w odniesieniu do danych osobowych zgodnie z rozporządzeniem Parlamentu Europejskiego i Rady (UE) 2016/679 ([2]), a także zapewnienie interoperacyjności. Ponieważ przedmiot i cele tych uprawnień są w dużej mierze zbieżne, należy ustanowić przepisy uzupełniające dyrektywę (UE) 2024/2841 w odniesieniu do tych kwestii w jednym akcie delegowanym.

(3) W dyrektywie (UE) 2024/2841 przewidziano, że fizyczne wersje europejskiej karty osoby z niepełnosprawnością i europejskiej karty parkingowej dla osób z niepełnosprawnościami zawierają kod QR jako najnowocześniejszy element cyfrowy, który wykorzystuje środki elektroniczne do zapobiegania oszustwom i ich zwalczania. W związku z tym kody QR stanowią obowiązkowy element cyfrowy, który należy nadrukować na wszystkich kartach fizycznych. Aby zapewnić jednolite podejście państw członkowskich do tworzenia i stosowania kodów QR, Komisja powinna przyjąć specyfikacje techniczne w celu określenia kodów QR, w tym ich zawartości.

(4) Europejska karta parkingowa dla osób z niepełnosprawnościami zastąpi wszystkie istniejące karty parkingowe dla osób z niepełnosprawnościami wydane zgodnie z zaleceniem Rady 98/376/WE ([3]). Zalecenie to nie zostało zaktualizowane w celu odzwierciedlenia rozwoju technologicznego i cyfryzacji, a państwa członkowskie doświadczyły problemów związanych z oszustwami i fałszerstwami. W związku z tym konieczne jest określenie elementów zapewniających bezpieczeństwo fizycznej wersji europejskiej karty parkingowej dla osób z niepełnosprawnościami, z uwzględnieniem jej specyfiki, takiej jak fakt, że kartę tę zazwyczaj umieszcza się za przednią szybą pojazdu.

([1]) Dz.U. L, 2024/2841, 14.11.2024, ELI: http://data.europa.eu/eli/dir/2024/2841/oj.

([2]) Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz.U. L 119 z 4.5.2016, s. 1, ELI: http://data.europa.eu/eli/reg/2016/679/oj).

([3]) Zalecenie Rady 98/376/WE z dnia 4 czerwca 1998 r. w sprawie karty parkingowej dla osób niepełnosprawnych (Dz.U. L 167 z 12.6.1998, s. 25, ELI: http://data.europa.eu/eli/reco/1998/376/oj).

(5) Należy wprowadzić obowiązkowe wspólne specyfikacje techniczne, aby zapewnić bezpieczeństwo fizycznej wersji europejskiej karty parkingowej dla osób z niepełnosprawnościami. Drukowanie karty na odpowiednim materiale, takim jak poliwęglan, z zastosowaniem elementu dyfrakcyjnego optycznie zmiennego skutecznie chroniłoby przed fałszowaniem i podrabianiem. Tło antykseryczne jeszcze bardziej zwiększyłyby poziom bezpieczeństwa, umożliwiając wykrywanie duplikatów kart, ponieważ takie tło powinno zawierać ukryty tekst lub wzór, który ujawnia się w przypadku kopiowania lub skanowania karty. Zastosowanie tych cech elementów nie powinno wpływać na format fizycznej wersji europejskiej karty parkingowej dla osób z niepełnosprawnościami określony w załączniku II do dyrektywy (UE) 2024/2841, w tym na wygląd karty.

(6) Oprócz kodu QR i innych obowiązkowych specyfikacji technicznych ustanowionych niniejszym rozporządzeniem państwa członkowskie powinny mieć możliwość włączenia opcjonalnych cyfrowych lub fizycznych zabezpieczeń, opartych na wspólnych specyfikacjach technicznych określonych w niniejszym rozporządzeniu, do fizycznej wersji europejskiej karty parkingowej dla osób z niepełnosprawnościami w celu zwiększenia jej bezpieczeństwa. W przypadku gdy opcjonalne elementy cyfrowe zawierają więcej danych osobowych, niż przewidziano dla fizycznych wersji kart, zgodnie z pkt 3 lit. b) załącznika II do dyrektywy (UE) 2024/2841 dostęp do takich danych musi być ograniczony do organów publicznych wydających państw członkowskich oraz wyłącznie do upoważnionych użytkowników. Aby utrzymać zharmonizowane ramy dotyczące elementów zabezpieczających w państwach członkowskich, wykaz elementów opcjonalnych powinien mieć charakter wyczerpujący. Ponadto państwa członkowskie powinny zapewnić, aby wprowadzenie jednego lub większej liczby opcjonalnych cyfrowych lub fizycznych elementów zabezpieczających nie wpływało na uznawanie ważnych kart wydanych przez inne państwa członkowskie ani nie naruszało interoperacyjności ani funkcjonalności obowiązkowych specyfikacji technicznych.

(7) Fizyczna wersja europejskiej karty parkingowej dla osób z niepełnosprawnościami może zawierać czip identyfikacji radiowej (RFID) jako opcjonalny cyfrowy element zabezpieczający. RFID wykorzystuje fale promieniowania elektromagnetycznego lub sprzężenie strefy reaktancyjnej w części widma częstotliwości radiowej w celu przekazywania do identyfikatora lub od niego różnych schematów modulacji i kodowania, aby jednoznacznie odczytać tożsamość identyfikatora częstotliwości radiowej lub inne przechowywane w nim dane ([4]). Czipy RFID mogą wzmocnić ochronę przed fałszerstwem i wprowadzaniem nieuprawnionych zmian poprzez bezpieczne przechowywanie lub przekazywanie danych związanych z kartą. Fizyczna wersja europejskiej karty parkingowej dla osób z niepełnosprawnościami może również zawierać farbę optycznie zmienną lub farbę o zmiennej barwie. Tego rodzaju farby zapewniają odpowiednią ochronę przed kopiowaniem karty i wprowadzaniem na niej nieuprawnionych zmian bez konieczności personalizacji. Aby zapewnić odpowiednie zabezpieczenie danych zawartych na karcie przed próbami podrabiania i fałszowania, tekst pól danych można zintegrować z podstawowym materiałem karty za pomocą technologii grawerowania laserowego. Fizyczne elementy zabezpieczające, zarówno określone w niniejszym rozporządzeniu jako obowiązkowe, jak i opcjonalne, które nie są widoczne lub stają się widoczne dopiero w wyniku określonych działań, nie są sprzeczne z formatem europejskiej karty parkingowej dla osób z niepełnosprawnościami określonym w załączniku II do dyrektywy (UE) 2024/2841.

(8) Postęp technologiczny, systemy weryfikacji parkowania i zagrożenia dla bezpieczeństwa stale się zmieniają. Stan wiedzy technicznej rozwija się, a korzystanie z europejskiej karty osoby z niepełnosprawnością i europejskiej karty parkingowej dla osób z niepełnosprawnościami ewoluuje, zarówno pod wpływem informacji zwrotnych od użytkowników, jak i postępu technologicznego – podobnie jak techniki oszustw i fałszerstw, co prowadzi do pojawiania się nowych wyzwań w zakresie bezpieczeństwa. W związku z tym nowe rozwiązania technologiczne, w tym w zakresie weryfikacji parkowania, a także potrzeby w zakresie bezpieczeństwa i zapobiegania oszustwom mogą wymagać zmian w architekturze zabezpieczeń kart i przeciwdziałania oszustwom w odniesieniu do kart, w tym poprzez aktualizację kategoryzacji elementów cyfrowych jako obowiązkowych albo opcjonalnych. W zależności od rozwoju technologicznego może to wymagać aktualizacji niniejszego rozporządzenia.

(9) Aby zapewnić możliwość bezproblemowego korzystania z fizycznych wersji europejskiej karty osoby z niepełnosprawnością i europejskiej karty parkingowej dla osób z niepełnosprawnościami we wszystkich państwach członkowskich, konieczne jest zagwarantowanie interoperacyjności elementów cyfrowych na kartach fizycznych, w szczególności kodów QR. Interoperacyjność powinna umożliwiać weryfikację autentyczności i ważności fizycznych wersji kart przez weryfikatorów kart – każdą osobę fizyczną lub prawną, która weryfikuje ważność i autentyczność fizycznych wersji kart, na przykład za pomocą aplikacji służącej do weryfikacji. W tym celu konieczne jest ustanowienie przepisów dotyczących kwestii związanych z interoperacyjnością, aby umożliwić przeprowadzanie transgranicznych weryfikacji fizycznych wersji kart w sposób spójny i niezawodny.

([4]) Zalecenie Komisji 2009/387/WE z dnia 12 maja 2009 r. w sprawie wdrażania zasad ochrony prywatności i ochrony danych w zastosowaniach wspieranych identyfikacją radiową (Dz.U. L 122 z 16.5.2009, s. 47, ELI: http://data.europa.eu/eli/reco/2009/387/oj).

(10) Aby zapewnić integralność i pochodzenie danych zawartych w kodach QR na fizycznych wersjach europejskiej karty osoby z niepełnosprawnością i europejskiej karty parkingowej dla osób z niepełnosprawnościami, dane te powinny być opatrzone kwalifikowaną pieczęcią elektroniczną zdefiniowaną w art. 3 pkt 27 rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 910/2014 ([5]). Kod QR potwierdza autentyczność i ważność fizycznej karty przy porównywaniu z parametrami weryfikacyjnymi i nie powinien sam w sobie potwierdzać statusu osoby z niepełnosprawnością ani uprawnienia do określonych usług z uwagi na niepełnosprawność.

(11) Aby ułatwić interoperacyjność i ustanowienie wiarygodnego i bezpiecznego systemu weryfikacji fizycznych wersji europejskiej karty osoby z niepełnosprawnością i europejskiej karty parkingowej dla osób z niepełnosprawnościami w całej Unii, należy ustanowić mechanizmy powiadamiania i publikowania informacji. W tym kontekście w celu umożliwienia weryfikacji, że fizyczne wersje kart zostały wydane przez właściwy organ lub podmiot, państwa członkowskie powinny przekazywać informacje niezbędne do procesu weryfikacji, w szczególności informacje wymagane do weryfikacji kwalifikowanej pieczęci elektronicznej. W związku z tym państwa członkowskie powinny być zobowiązane do powiadamiania Komisji o właściwych organach lub podmiotach odpowiedzialnych za wydawanie fizycznych wersji kart (wydawcach kart), a także do przekazywania odpowiednich informacji administracyjnych i technicznych dotyczących tych kart. Informacje przekazywane Komisji, powinny być ograniczone do tego, co jest niezbędne do ustanowienia interoperacyjnych mechanizmów weryfikacji ważności i autentyczności fizycznych wersji europejskiej karty osoby z niepełnosprawnością i europejskiej karty parkingowej dla osób z niepełnosprawnościami. Komisja powinna zapewnić publiczny dostęp do tych informacji.

(12) Ponadto w przypadku unieważnienia karty informacje o jej unieważnieniu należy niezwłocznie udostępnić, aby umożliwić weryfikatorom kart sprawdzenie ważności karty. W tym celu wydawcy kart powinni prowadzić i publikować w odpowiednim czasie wykazy zawierające informacje o statusie unieważnienia wszystkich kart unieważnionych przed upływem ich okresu ważności (wykazy unieważnionych kart). Taka publikacja powinna odbywać się z poszanowaniem prywatności oraz z zapewnieniem ochrony danych osobowych posiadaczy kart. Ponadto wykazy unieważnionych kart nie powinny zawierać żadnych danych osobowych innych niż niepowtarzalne identyfikatory unieważnień i powinny być publikowane pod specjalnym jednolitym identyfikatorem zasobów (URI) zgodnie ze specyfikacjami technicznymi w celu zapewnienia interoperacyjnej weryfikacji.

(13) Aby odczytać kod QR oraz zweryfikować autentyczność i ważność fizycznych wersji europejskiej karty osoby z niepełnosprawnością i europejskiej karty parkingowej dla osób z niepełnosprawnościami, można korzystać z dostosowanych do indywidualnych potrzeb aplikacji służących do weryfikacji na szczeblu krajowym. Komisja może wspierać ten proces poprzez udostępnienie wspólnego przykładowego kodu źródłowego służącego do odczytu danych zawartych w kodach QR oraz do przeprowadzania głównych etapów procesu weryfikacji, który to kod źródłowy może stanowić podstawę dla aplikacji służących do weryfikacji w państwach członkowskich. Wszystkie aplikacje służące do weryfikacji powinny opierać się na tej samej logice weryfikacji łańcucha zaufania w odniesieniu do tej samej infrastruktury zaufania, umożliwiając w ten sposób odczyt danych zakodowanych na kartach przez wydające państwo członkowskie. Ponadto w załączniku I do dyrektywy Parlamentu Europejskiego i Rady (UE) 2019/882 ([6]) określono wymogi dostępności, których państwa członkowskie muszą przestrzegać w stosownych przypadkach.

(14) Uznając dynamiczny charakter postępu technologicznego i zmieniających się zagrożeń w zakresie cyberbezpieczeństwa, Unia zobowiązuje się do zapewnienia, aby mechanizmy kryptograficzne stosowane w jej ramach regulacyjnych pozostały skuteczne i bezpieczne. W świetle tego zobowiązania ważne jest przyjęcie norm kryptograficznych zatwierdzonych przez Europejską Grupę ds. Certyfikacji Cyberbezpieczeństwa i rozpowszechnianych za pośrednictwem Agencji Unii Europejskiej ds. Cyberbezpieczeństwa (ENISA).

(15) Do przetwarzania danych osobowych prowadzonego w ramach niniejszego rozporządzenia ma zastosowanie rozporządzenie (UE) 2016/679. Z przetwarzaniem danych osobowych wiąże się w szczególności weryfikacja kodów QR na fizycznych wersjach europejskiej karty osoby z niepełnosprawnością i europejskiej karty parkingowej dla osób z niepełnosprawnościami. W związku z tym należy ustanowić odpowiednie zabezpieczenia w zakresie ochrony danych, aby zapewnić ochronę danych osobowych zawartych w kodach QR zgodnie z rozporządzeniem (UE) 2016/679, w stosownych przypadkach. Ogólne środki bezpieczeństwa przewidziane w niniejszym rozporządzeniu powinny również zapewniać ochronę danych osobowych zawartych w kodach QR. Ponadto dane osobowe zawarte w kodach QR powinny być ograniczone do tego, co jest absolutnie niezbędne do celów niniejszego rozporządzenia. Poza tym należy zakazać przechowywania tych danych po zakończeniu weryfikacji. Konieczne jest również zapewnienie odpowiedniego bezpieczeństwa wykazów unieważnionych kart.

([5]) Rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 910/2014 z dnia 23 lipca 2014 r. w sprawie identyfikacji elektronicznej i usług zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznym oraz uchylające dyrektywę 1999/93/WE (Dz.U. L 257 z 28.8.2014, s. 73, ELI: http://data.europa.eu/eli/reg/2014/910/oj).

([6]) Dyrektywa Parlamentu Europejskiego i Rady (UE) 2019/882 z dnia 17 kwietnia 2019 r. w sprawie wymogów dostępności produktów i usług (Dz.U. L 151 z 7.6.2019, s. 70, ELI: http://data.europa.eu/eli/dir/2019/882/oj).

(16) Zgodnie z art. 14 ust. 4 dyrektywy (UE) 2024/2841 podczas przygotowywania niniejszego rozporządzenia Komisja skonsultowała się z osobami z niepełnosprawnościami i reprezentującymi je organizacjami, a także z ekspertami wyznaczonymi przez każde państwo członkowskie zgodnie z zasadami określonymi w Porozumieniu międzyinstytucjonalnym z dnia 13 kwietnia 2016 r. w sprawie lepszego stanowienia prawa ([7]).

(17) Europejska karta osoby z niepełnosprawnością i europejska karta parkingowa dla osób z niepełnosprawnościami stanowią transeuropejską cyfrową usługę publiczną w rozumieniu rozporządzenia Parlamentu Europejskiego i Rady (UE) 2024/903 ([8]). W związku z tym przeprowadzono ocenę interoperacyjności, a sprawozdanie z tej oceny ma zostać opublikowane w portalu Interoperacyjna Europa, o którym mowa w art. 8 rozporządzenia (UE) 2024/903.

(18) Zgodnie z art. 42 ust. 1 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2018/1725 ([9]) w sprawie niniejszego rozporządzenia skonsultowano się z Europejskim Inspektorem Ochrony Danych, który wydał opinię w dniu 12 maja 2026 r.,

PRZYJMUJE NINIEJSZE ROZPORZĄDZENIE:

Artykuł 1

Przedmiot i zakres

Niniejsze rozporządzenie określa przepisy uzupełniające dyrektywę (UE) 2024/2841 w odniesieniu do:

a) określenia kodu QR dla fizycznych wersji europejskiej karty osoby z niepełnosprawnością i europejskiej karty parkingowej dla osób z niepełnosprawnościami, w tym odpowiednich środków bezpieczeństwa w odniesieniu do danych osobowych;

b) ustanowienia wspólnych obowiązkowych i opcjonalnych specyfikacji technicznych zapewniających bezpieczeństwo fizycznej wersji europejskiej karty parkingowej dla osób z niepełnosprawnościami;

c) ustanowienia wymogów w zakresie interoperacyjności niezbędnych do zapewnienia, aby kody QR na fizycznych wersjach europejskiej karty osoby z niepełnosprawnością lub europejskiej karty parkingowej dla osób z niepełnosprawnościami wydanych w jednym państwie członkowskim mogły być w sposób niezawodny odczytywane i weryfikowane w innym państwie członkowskim.

Artykuł 2

Kod QR na fizycznej wersji europejskiej karty osoby z niepełnosprawnością

Specyfikacje kodu QR, który ma być umieszczony na fizycznej wersji europejskiej karty osoby z niepełnosprawnością, określono w załączniku I.

Artykuł 3

Kod QR na fizycznej wersji europejskiej karty parkingowej dla osób z niepełnosprawnościami

Specyfikacje kodu QR, który ma być umieszczony na fizycznej wersji europejskiej karty parkingowej dla osób z niepełnosprawnościami, określono w załączniku II.

([7]) Dz.U. L 123 z 12.5.2016, s. 1, ELI: http://data.europa.eu/eli/agree_interinstit/2016/512/oj.

([8]) Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2024/903 z dnia 13 marca 2024 r. w sprawie ustanowienia środków na rzecz wysokiego poziomu interoperacyjności sektora publicznego na terytorium Unii (akt w sprawie Interoperacyjnej Europy) (Dz.U. L, 2024/903, 22.3.2024, ELI: http://data.europa.eu/eli/reg/2024/903/oj).

([9]) Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2018/1725 z dnia 23 października 2018 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych przez instytucje, organy i jednostki organizacyjne Unii i swobodnego przepływu takich danych oraz uchylenia rozporządzenia (WE) nr 45/2001 i decyzji nr 1247/2002/WE (Dz.U. L 295 z 21.11.2018, s. 39, ELI: http://data.europa.eu/eli/reg/2018/1725/oj).

Artykuł 4

Obowiązkowe wspólne specyfikacje techniczne dotyczące europejskiej karty parkingowej dla osób z niepełnosprawnościami

1. Fizyczne wersje europejskiej karty parkingowej dla osób z niepełnosprawnościami spełniają następujące wspólne specyfikacje techniczne:

a) są wykonane z materiału, który chroni przed rozwarstwieniem i jest w stanie spełnić wymogi określone w załączniku II do dyrektywy (UE) 2024/2841 oraz inne obowiązkowe wspólne specyfikacje techniczne określone w niniejszym artykule;

b) zawierają element dyfrakcyjny optycznie zmienny jako element struktury warstwowej, który staje się widoczny przy oglądaniu karty pod określonym kątem;

c) są wykonane z zastosowaniem tła antykserycznego, które ujawnia się w przypadku kopiowania lub skanowania karty.

2. Element dyfrakcyjny optycznie zmienny, o którym mowa w ust. 1 lit. b), znajduje się na awersie fizycznej wersji europejskiej karty parkingowej dla osób z niepełnosprawnościami nad co najmniej jednym polem danych po lewej stronie. Ma on w przybliżeniu 20 mm wysokości i 20 mm szerokości. Obraz przedstawiony na tym elemencie składa się z uproszczonej mapy wydającego państwa członkowskiego lub indywidualnego kodu wydającego państwa członkowskiego otoczonego kręgiem 12 gwiazd symbolizujących Unię.

3. Tło antykseryczne, o którym mowa w ust. 1 lit. c), umieszcza się na awersie fizycznej wersji europejskiej karty parkingowej dla osób z niepełnosprawnościami, nad polami danych po lewej stronie lub po prawej stronie poza kodem QR i jego strefą ciszy. Zawiera ono ukryty tekst lub wzór ujawniający się w przypadku kopiowania lub skanowania karty. W przypadku gdy tło antykseryczne zawiera ukryty tekst, składa się on z następujących słów wraz z ich tłumaczeniem na co najmniej jeden język urzędowy wydającego państwa członkowskiego: „COPY" („KOPIA") lub „VOID" („NIEWAŻNE"). W przypadku gdy tło antykseryczne zawiera ukryty wzór, składa się on z linii poziomych lub pionowych.

Artykuł 5

Opcjonalne specyfikacje techniczne i elementy zapewniające bezpieczeństwo europejskiej karty parkingowej dla osób z niepełnosprawnościami

1. Oprócz obowiązkowych wspólnych specyfikacji technicznych, o których mowa w art. 4, państwa członkowskie mogą stosować wyłącznie opcjonalne specyfikacje techniczne i elementy określone w niniejszym artykule.

2. Fizyczne wersje europejskiej karty parkingowej dla osób z niepełnosprawnościami mogą zawierać czip identyfikacji radiowej (RFID). Czip RFID służy do zapobiegania oszustwom i zwalczania ich za pomocą środków elektronicznych oraz jako dodatkowy środek weryfikacji autentyczności lub ważności fizycznej wersji europejskiej karty parkingowej dla osób z niepełnosprawnościami na szczeblu krajowym. Czip RFID nie może wpływać na funkcjonowanie kodu QR na karcie.

3. Każdy czip RFID, o którym mowa w ust. 2, musi spełniać następujące specyfikacje:

a) jest pasywny;

b) jest fizycznie zintegrowany z korpusem karty i umieszczony na awersie po prawej stronie;

c) jest logicznie powiązany z zapisem kodu QR i zawiera ten sam identyfikator unieważnienia (RID) co zakodowany w kodzie QR;

d) funkcja RFID musi umożliwiać odczyt z odległości około 1 metra lub większej, jeżeli jest to wymagane do celów operacyjnych, ale nie może być zaprojektowana w taki sposób, aby umożliwiała niezawodny odczyt na odległość większą niż 5 metrów w referencyjnych warunkach testowych;

e) po wydaniu karty organ wydający uniemożliwia dostęp z możliwością zapisu do czipu RFID lub do odpowiedniego obszaru danych tego czipu lub w inny sposób kontroluje taki dostęp;

f) jest zaprojektowany i skonfigurowany w taki sposób, aby zminimalizować ryzyko klonowania, podmiany, nieuprawnionej modyfikacji oraz nieuprawnionego ponownego zapisu;

g) spełnia wymagania dyrektywy Parlamentu Europejskiego i Rady 2014/53/UE ([10]);

h) oprócz identyfikatora RID, o którym mowa w lit. c), w czipie RFID można przechowywać wyłącznie jeden lub więcej z następujących rodzajów danych:

(i) dane zakodowane w kodzie QR fizycznej wersji europejskiej karty parkingowej dla osób z niepełnosprawnościami;

(ii) numer rejestracyjny pojazdu lub numery rejestracyjne pojazdu;

(iii) dane służące do weryfikacji kryptograficznej.

4. Awers fizycznych wersji europejskiej karty parkingowej dla osób z niepełnosprawnościami może zawierać jeden lub więcej z następujących elementów:

a) symbol wózka inwalidzkiego po lewej stronie lub słowa w języku angielskim i w co najmniej jednym języku urzędowym wydającego państwa członkowskiego „European Parking Card for persons with disabilities" („europejska karta parkingowa dla osób z niepełnosprawnościami") po prawej stronie, wydrukowane farbą optycznie zmienną lub farbą o zmiennej barwie, ujawniającą zmieniające się barwy przy oglądaniu pod różnymi kątami;

b) zastosowanie technologii grawerowania laserowego przenikającej przez warstwy karty w celu naniesienia tekstu w polach danych.

5. Wprowadzenie opcjonalnych specyfikacji technicznych i elementów, o których mowa w niniejszym artykule, nie ma wpływu na uznawanie – w państwie członkowskim, które wprowadziło takie elementy w odniesieniu do wydawanych przez siebie kart – ważnych kart wydanych w innych państwach członkowskich.

Artykuł 6

Kwestie interoperacyjności

1. Informacje zawarte w kodzie QR opatruje się kwalifikowaną pieczęcią elektroniczną w rozumieniu art. 3 pkt 27 rozporządzenia (UE) nr 910/2014.

2. Każde państwo członkowskie przekazuje Komisji informacje o właściwych organach lub podmiotach odpowiedzialnych za wydawanie fizycznych wersji europejskiej karty osoby z niepełnosprawnością lub europejskiej karty parkingowej dla osób z niepełnosprawnościami („wydawcy kart") oraz wszelkie późniejsze aktualizacje tych informacji zgodnie z załącznikiem III. Komisja zapewnia publiczny dostęp do tych informacji.

3. Wydawcy kart prowadzą i publikują pod jednolitym identyfikatorem zasobów (URI) zgłoszonym Komisji aktualne wykazy unieważnionych kart zawierające informacje na temat statusu unieważnienia wszystkich kart, które unieważnili, zgodnie ze specyfikacjami technicznymi określonymi w załączniku IV. Informacje o unieważnieniu publikuje się w ciągu 24 godzin od jego dokonania.

4. Państwa członkowskie mogą korzystać z aplikacji służących do weryfikacji w celu sprawdzania autentyczności i ważności fizycznych wersji europejskiej karty osoby z niepełnosprawnością i europejskiej karty parkingowej dla osób z niepełnosprawnościami.

5. W przypadku gdy państwa członkowskie korzystają z aplikacji służących do weryfikacji w celu sprawdzania autentyczności i ważności fizycznych wersji europejskiej karty osoby z niepełnosprawnością i europejskiej karty parkingowej dla osób z niepełnosprawnościami, aplikacje takie umożliwiają weryfikację autentyczności i ważności karty poprzez sprawdzenie pieczęci elektronicznej i statusu unieważnienia karty. Te aplikacje służące do weryfikacji odczytują dane osobowe zakodowane w kodzie QR karty oraz przedstawiają ich wizualną reprezentację, jak określono w załącznikach I i II, aby umożliwić ich porównanie z danymi widocznymi w odpowiednich polach danych na karcie, oraz wskazanie statusu ważności karty.

([10]) Dyrektywa Parlamentu Europejskiego i Rady 2014/53/UE z dnia 16 kwietnia 2014 r. w sprawie harmonizacji ustawodawstw państw członkowskich dotyczących udostępniania na rynku urządzeń radiowych i uchylająca dyrektywę 1999/5/WE (Dz.U. L 153 z 22.5.2014, s. 62, ELI: http://data.europa.eu/eli/dir/2014/53/oj).

Artykuł 7

Środki bezpieczeństwa w zakresie ochrony danych osobowych

1. Dane osobowe zawarte w kodach QR na fizycznych wersjach europejskiej karty osoby z niepełnosprawnością i europejskiej karty parkingowej dla osób z niepełnosprawnościami są ograniczone do tego, co jest absolutnie niezbędne do weryfikacji autentyczności i ważności kart, jak określono w załącznikach I i II.

2. Po zakończeniu weryfikacji autentyczności i ważności fizycznej wersji europejskiej karty osoby z niepełnosprawnością lub europejskiej karty parkingowej dla osób z niepełnosprawnościami przez weryfikatorów kart dane zawarte w kodach QR nie są przez nich przechowywane.

3. Weryfikacja kodu QR na fizycznej wersji europejskiej karty osoby z niepełnosprawnością lub europejskiej karty parkingowej dla osób z niepełnosprawnościami nie skutkuje powiadomieniem o tej weryfikacji właściwego organu lub podmiotu odpowiedzialnego za wydanie karty.

4. Informacje zawarte w wykazie unieważnionych kart opublikowanym zgodnie z art. 6 ust. 3 są ograniczone do identyfikatora unieważnienia unieważnionych kart.

5. Organ lub podmiot odpowiedzialny za publikowanie wykazów unieważnionych kart zgodnie z art. 6 ust. 3 zapewnia stosowanie odpowiednich technicznych i organizacyjnych środków bezpieczeństwa w odniesieniu do przetwarzania danych osobowych zawartych w tych wykazach.

6. Jeżeli państwo członkowskie podejmie decyzję o dodaniu czipu RFID do fizycznej wersji europejskiej karty parkingowej dla osób z niepełnosprawnościami, ust. 2–3 mają zastosowanie do przetwarzania danych osobowych zawartych na tym czipie. Dane osobowe zawarte w czipie RFID są ograniczone do tego, co jest absolutnie niezbędne do weryfikacji autentyczności lub ważności kart, jak określono w art. 5 ust. 3.

W przypadku gdy państwo członkowskie przechowuje w czipie RFID dane osobowe, o których mowa w art. 5, które nie są przewidziane w fizycznej wersji europejskiej karty parkingowej dla osób z niepełnosprawnościami określonej w załączniku II do dyrektywy (UE) 2024/2841, dostęp do takich danych jest ograniczony do organów publicznych wydającego państwa członkowskiego oraz wyłącznie do upoważnionych użytkowników.

Artykuł 8

Niniejsze rozporządzenie wchodzi w życie dwudziestego dnia po jego opublikowaniu w *Dzienniku Urzędowym Unii Europejskiej*.

Niniejsze rozporządzenie wiąże w całości i jest bezpośrednio stosowane we wszystkich państwach członkowskich.

Sporządzono w Brukseli dnia 1 lipca 2026 r.

W imieniu Komisji
Przewodnicząca
Ursula VON DER LEYEN

ZAŁĄCZNIK I

SPECYFIKACJE KODU QR NA POTRZEBY FIZYCZNEJ WERSJI EUROPEJSKIEJ KARTY OSOBY Z NIEPEŁNOSPRAWNOŚCIĄ

1. **Format kodu QR na potrzeby fizycznej wersji europejskiej karty osoby z niepełnosprawnością (EDC)**

   a) **Format kodu QR Model 2**, zgodny z międzynarodowymi normami ISO/IEC 18004:2024 dotyczącymi kodów QR lub równoważnymi.

   b) **Poziom korekcji błędów M** (15 % redundancji) zapewniający odporność na zarysowania lub częściowe uszkodzenie wydrukowanego kodu QR.

   c) **Tryb kodowania**: ładunek QR składa się z połączonej struktury issuerSigned w formacie Concise Binary Object Representation (CBOR) oraz odpowiadającego jej obiektu podpisu issuerAuth COSE_Sign1, zgodnie ze specyfikacją CBOR Object Signing and Encryption (COSE, RFC 9052 sekcje 3.1, 4.2 i 4.4), według wzorca modelu danych mDOC dla elementów issuerSigned, dostosowanego jednak do użycia w statycznej fizycznej karcie. issuerAuth jest obiektem COSE_Sign1 z parametrem alg = ES256 oraz chronionym nagłówkiem zawierającym x5t (parametr nagłówka skrótu certyfikatu COSE X.509 określony w RFC 9360 (sekcja 2)); do celów interoperacyjności algorytmem skrótu stosowanym w x5t jest SHA-256).

   d) Przed zakodowaniem w kodzie QR połączony obiekt CBOR/COSE **jest kompresowany w formacie zlib** (RFC 1950, sekcja 2.2) z **wykorzystaniem algorytmu deflate** (RFC 1951, sekcje 3.2 i 4). Powstałą w ten sposób skompresowaną tablicę bajtów koduje się w **trybie bajtowym kodu QR**, co zapewnia pełną obsługę binarnych ładunków CBOR/COSE oraz interoperacyjność skanerów.

   Dla wszystkich pól tekstowych zawartych w ładunku QR wydawcy kodują znaki jako Unicode UTF-8 w ciągach tekstowych CBOR. Do danych ładunku podpisywanego nie stosuje się transliteracji. Do celów interoperacyjności wydawcy stosują formę normalizacji Unicode C (NFC) do wszystkich pól tekstowych przed podpisaniem ładunku.

   e) **Prefiks:** ciąg QR EDC rozpoczyna się od „ED1:MDOC:". Pozwala to zidentyfikować typ karty oraz profil kodowania. Prefiksy są wrażliwe na wielkość liter i muszą być obecne. Nieznane lub nieobsługiwane prefiksy powodują odrzucenie. Prefiks i skompresowany ładunek są kodowane w kodzie QR jako pojedynczy segment danych w trybie bajtowym.

   f) **Minimalny rozmiar modułu ≥ 0,25 mm** w celu zapewnienia czytelności na drukowanych kartach.

   g) **Wersja maksymalna 20**; z maksymalnie 97 × 97 modułów z każdej strony.

2. **Specyfikacje generowania podpisu EDC**

   Kwalifikowana pieczęć elektroniczna (QSeal) stosowana do zabezpieczenia kodów QR EDC zapewnia, by zakodowane dane pochodziły od upoważnionego organu wydającego i nie zostały zmienione.

   a) **Algorytm podpisu**: algorytmem podpisu jest ES256 (algorytm podpisu cyfrowego krzywej eliptycznej – ECDSA – z wykorzystaniem SHA-256 przy użyciu krzywej P-256), jak określono w RFC 9053 (sekcja 2.1); w COSE identyfikacja algorytmu odbywa się za pomocą parametru nagłówka alg zgodnie z RFC 9052 (sekcja 3.1).

   b) **Klucz podpisu**: ładunek QR jest podpisywany przy użyciu klucza prywatnego odpowiadającego kwalifikowanemu certyfikatowi pieczęci elektronicznej (QSealC).

   c) **Struktura COSE**: kontenerem podpisu jest obiekt COSE_Sign1. Chroniony nagłówek zawiera alg (ES256) i x5t (parametr nagłówka skrótu certyfikatu COSE X.509 określony w RFC 9360 (sekcja 2); do celów interoperacyjności algorytmem skrótu stosowanym w x5t jest SHA-256). Weryfikacja polega na wykorzystaniu wartości x5t do odnalezienia odpowiedniego certyfikatu w lokalnym repozytorium zaufania weryfikatora, utworzonym na podstawie informacji z zaufanej listy, a następnie na sprawdzeniu łańcucha certyfikatów oraz statusu certyfikatu zgodnie z ramami zaufania eIDAS.

   d) **Standard podpisu**: ładunek kodu QR jest podpisywany jako obiekt COSE_Sign1 zgodnie z RFC 9052 (sekcja 4), CBOR Object Signing and Encryption. Obiekt COSE_Sign1 jest zawarty w issuerAuth i kodowany bez tagu CBOR dla COSE_Sign1. Pole ładunku obiektu COSE_Sign1 jest oddzielone i kodowane jako CBOR null. Do celów generowania i weryfikacji podpisów zewnętrzny ładunek jest strukturą zakodowaną w deterministycznym formacie CBOR, zawierającą wartość docType oraz wartość issuerSigned z mapy CBOR najwyższego poziomu.

e) **Algorytm skrótu**: SHA-256 jest stosowany jako część ES256 do generowania podpisów i weryfikacji integralności.

f) **Kodowanie**: ładunek jest kodowany przy użyciu CBOR (RFC 8949, sekcja 4.2), zgodnie z wymaganiami specyfikacji COSE i mDOC, co zapewnia poprawne kodowanie i odtwarzalność podpisanych danych.

3. **Specyfikacje druku**

a) **Strefa ciszy**: kod QR jest otoczony z każdej strony czystym marginesem o szerokości **4 modułów**, wolnym od jakiegokolwiek druku, wzoru lub tła.

b) **Kontrast**: kod QR jest drukowany na białym tle, przy minimalnym współczynniku kontrastu **4:1**, aby zapewnić wysoką czytelność w różnych warunkach oświetleniowych.

c) Kod QR jest drukowany przy użyciu koloru zdefiniowanego w załączniku I do dyrektywy (UE) 2024/2841, który zapewnia maksymalny kontrast.

d) **Umiejscowienie i rozmiar**: kod QR, wraz ze strefą ciszy, ma wymiary 26,25 mm × 26,25 mm i znajduje się na rewersie karty w prawym dolnym rogu. Kod QR jest stosowany maksymalnie w wersji 20 (97 × 97 modułów), przy czym rozmiar modułu wynosi co najmniej 0,25 mm.

Kod QR, wraz ze strefą ciszy, jest umieszczony w odległości przynajmniej 5 mm od prawego brzegu kraty i w odległości przynajmniej 5 mm od dolnego brzegu karty.

4. **Dane w kodzie QR EDC**

Kod QR zawiera minimalny zestaw danych możliwych do weryfikacji offline, zgodnie z zasadą minimalizacji danych określoną w art. 5 ust. 1 lit. c) rozporządzenia (UE) 2016/679. Struktura ładunku jest następująca:

a) Atrybuty karty są kodowane w formacie CBOR w ramach obiektu issuerSigned.

b) Struktura ta jest opakowana i podpisana QSeal organu wydającego jako issuerAuth (COSE_Sign1, ES256, z uwzględnieniem x5t, czyli parametru nagłówka skrótu certyfikatu COSE X.509).

c) Powstały obiekt CBOR/COSE jest kompresowany zgodnie z pkt 1 lit. d) niniejszego załącznika. Ładunek kodu QR składa się z prefiksu „ED1:MDOC:", po którym następuje skompresowana tablica bajtów, a cały ładunek jest kodowany w trybie bajtowym jako pojedynczy segment danych kodu QR.

Zawartość danych obejmuje podzbiór danych widocznych z pól na awersie karty wymienionych w załączniku I do dyrektywy (UE) 2024/2841 (imię, nazwisko, numer seryjny karty, termin ważności), wraz z identyfikatorem unieważnienia, podpisem elektronicznym oraz informacjami o schemacie.

Podpis elektroniczny zawiera:

(i) issuerAuth – obiekt COSE_Sign1 podpisany przy użyciu **klucza prywatnego QSealC** organu wydającego;

(ii) chroniony nagłówek zawierający alg = ES256 (algorytm podpisu) i x5t (parametr nagłówka skrótu certyfikatu COSE X.509).

5. **Dane nieobowiązkowe**

Kod QR nie może zawierać żadnych danych nieobowiązkowych.

6. **Identyfikator unieważnienia (RID)**

Oprócz widocznego numeru seryjnego karty kod QR zawiera specjalny identyfikator unieważnienia (RID).

RID jest wykorzystywany do określania statusu unieważnienia oraz do zarządzania wykazem unieważnionych kart. RID nie jest drukowany na karcie ani wyświetlany weryfikatorom kart.

6.1. *Wymogi dotyczące RID*

RID:

a) jest uwzględniony w podpisanym ładunku QR;

b) jest niepowtarzalny co najmniej w obrębie domeny wydawania danego organu wydającego;

c) nie jest drukowany na karcie ani nie jest przeznaczony do odczytu przez człowieka;

d) nie ujawnia danych osobowych ani nie ma bezpośredniego znaczenia;

e) nie może bezpośrednio wynikać z widocznego numeru seryjnego karty; oraz

f) jest kryptograficznie powiązany z ładunkiem QR za pomocą kwalifikowanej pieczęci elektronicznej.

6.2. *Format i rozmiar RID*

RID jest kodowany jako ciąg bajtów CBOR (bstr). RID ma długość 16 bajtów (128 bitów).

RID jest generowany przez organ wydający przy użyciu metody znajdującej się pod jego kontrolą, która to metoda zapewnia wystarczającą entropię i odporność na odgadnięcie lub wyliczenie.

6.3. *Wykazy unieważnionych kart*

Wykazy unieważnionych kart publikowane do celów weryfikacji odnoszą się wyłącznie do RID unieważnionych kart. Numery seryjne kart nie są publikowane w wykazach unieważnionych kart.

7. **Ładunek CBOR (w kodzie QR) EDC**

W ładunku QR uwzględnia się wyłącznie następujące dane, zgodnie z widocznymi polami danych EDC określonymi w załączniku I do dyrektywy (UE) 2024/2841.

Zawartość najwyższego poziomu:

a) docType = "eu.edc";

b) issuerSigned.nameSpaces."eu.edc" z atrybutami podanymi w tabeli poniżej;

c) issuerAuth = COSE_Sign1 (QSeal).

Pole	Ścieżka mDOC	Rodzaj/Format
Wersja schematu danych	issuerSigned.nameSpaces."eu.edc".ver	Ciąg znaków (np. "1.0")
Rodzaj karty: EDC	docType	Enum ("eu.edc")
Numer seryjny karty	issuerSigned.nameSpaces."eu.edc".sub	Ciąg znaków
Identyfikator unieważnienia	issuerSigned.nameSpaces."eu.edc".rid	CBOR bstr (16 bajtów)
Imię posiadacza karty	issuerSigned.nameSpaces."eu.edc".givenName	Ciąg tekstowy Unicode (UTF-8)
Nazwisko posiadacza karty	issuerSigned.nameSpaces."eu.edc".familyName	Ciąg tekstowy Unicode (UTF-8)
Termin ważności karty	issuerSigned.nameSpaces."eu.edc".exp	tag CBOR 1004, zdefiniowany w RFC 8943 (sekcja 2.1), zawierający ciąg tekstowy w UTF-8 przedstawiający pełną datę w formacie RFC 3339: RRRR-MM-DD.

Podpis elektroniczny jest zawarty w issuerAuth (obiekt COSE_Sign1). Łańcuch certyfikatów nie jest osadzany w ładunku kodu QR; zamiast tego chroniony nagłówek COSE zawiera x5t, odcisk palca certyfikatu umożliwiający odnalezienie odpowiedniego certyfikatu QSealC w lokalnym repozytorium zaufania weryfikatora.

8. **Przykład ładunku kodu QR EDC: reprezentacja logiczna w konwencji JavaScript Object Notation (JSON) z komentarzem**

Poniższy przykład stanowi czytelną dla człowieka reprezentację logicznego widoku EDC w JavaScript Object Notation (JSON). W praktyce struktura ta nie ma postaci czytelnej dla człowieka, ponieważ:

a) jest kodowana w CBOR (RFC 8949, sekcja 3);

b) jest podpisana przy użyciu struktury COSE_Sign1 bez tagów z oddzielonym ładunkiem (RFC 9052, sekcja 4);

c) zawiera termin ważności jako wartość stanowiącą pełną datę w formacie tagu CBOR 1004 zgodnie z RFC 8943 (sekcja 2.1);

d) zawiera parametr x5t w nagłówku chronionym zgodnie z RFC 9360, przy użyciu skrótu SHA-256 do zakodowanego w formacie DER certyfikatu podmiotu końcowego QSealC; oraz

e) jest kompresowana i opatrzona prefiksem w postaci ciągu ED1:MDOC: zanim zostanie zakodowana w kod QR.

```
{
  // konwencja JSON, jedynie logiczny widok EDC czytelny dla człowieka.
  // Faktyczny ładunek QR to deterministyczny format CBOR, a nie JSON.
  "docType": "eu.edc", // poświadczenie EDC. Zawiera wartość docType, wraz z
     //issuerSigned, w ładunku zewnętrznym COSE_Sign1.

  "issuerSigned": {
     // dane chronione przez issuerAuth; użyte jako oddzielony ładunek.
     // Do celów generowania i weryfikacji podpisów oddzielony ładunek zewnętrzny obejmuje zarówno
     // docType jak i issuerSigned.
     "nameSpaces": {
       "eu.edc": {
         "ver": "1.0", // wersja profilu/schematu kodu QR

         // Numer seryjny karty; określony przez wydawcę, maksymalnie 24 znaki.
         "sub": "AB123456789012345678 90CD",

         // Identyfikator unieważnienia: rzeczywista wartość CBOR bstr, 16 bajtów/128 bitów.
         // dla czytelności pokazana tutaj jako 32-znakowy ciąg heksadecymalny.
         "rid": "9f8c4d3a7b1e2c0a55aa33ff8899ee11",

         "givenName": "Anna", // imię wydrukowane na EDC
         "familyName": "Kowalska", // nazwisko wydrukowane na EDC

         // Faktyczne kodowanie CBOR wykorzystuje tag 1004 dla pełnej daty w formacie RFC 3339.
         "exp": "2030-12-31"
       }
     }
   },

   "issuerAuth": {
     // Faktyczny format: COSE_Sign1 bez tagów, a nie obiekt JSON.
     "type": "COSE_Sign1",
```

```
    "tagged": false, // zakodowany bez tagu COSE_Sign1 CBOR
    "payload": "detached", // pole ładunku COSE to CBOR null

    "protectedHeader": {
      // alg: ES256; równoważny parametr nagłówka COSE 1 = -7.
      "alg": "ES256",

      // x5t: odcisk palca certyfikatu; parametr nagłówka COSE 34.
      "x5t": {
        "hashAlg": "SHA-256", // równoważna wartość skrótu COSE -16

        // skrót SHA-256 zakodowanego w formacie DER certyfikatu podmiotu końcowego QSealC.
        // 32 bajty reprezentowane jako 64-znakowy ciąg heksadecymalny.
        "hashValue":
        "0123456789abcdef0123456789abcdef0123456789abcdef0123456789abcdef"
      }
    },

    "unprotectedHeader": {}, // pusty w tym przykładzie

    // podpis COSE z algorytmem ES256: 64 bajty = 128-znakowy ciąg heksadecymalny
    "signature":
    "0123456789abcdef0123456789abcdef0123456789abcdef0123456789abcdef0123456789abcde-
    f0123456789abcdef0123456789abcdef0123456789abcdef"
  }
}
```


9. **Stosowanie mechanizmów kryptograficznych**

Stosowanie mechanizmów kryptograficznych w kontekście niniejszego załącznika odbywa się zgodnie z uzgodnionymi mechanizmami kryptograficznymi zatwierdzonymi przez Europejską Grupę ds. Certyfikacji Cyberbezpieczeństwa i opublikowanymi przez Agencję Unii Europejskiej ds. Cyberbezpieczeństwa (ENISA).

ZAŁĄCZNIK II

SPECYFIKACJE KODU QR DLA FIZYCZNEJ WERSJI EUROPEJSKIEJ KARTY PARKINGOWEJ DLA OSÓB Z NIEPEŁNOSPRAWNOŚCIAMI

1. **Format kodu QR na fizycznej wersji europejskiej karty parkingowej dla osób z niepełnosprawnościami (EPC)**

   a) **Format kodu QR Model 2**, zgodny z międzynarodowymi normami ISO/IEC 18004:2024 dotyczącymi kodów QR lub równoważnymi.

   b) **Poziom korekcji błędów M** (15 % redundancji) zapewniający odporność na zarysowania lub częściowe uszkodzenie wydrukowanego kodu QR.

   c) **Tryb kodowania:** ładunek QR składa się z połączonej struktury issuerSigned w formacie Concise Binary Object Representation (CBOR) oraz odpowiadającego jej obiektu podpisu issuerAuth COSE_Sign1, zgodnie ze specyfikacją CBOR Object Signing and Encryption (COSE, RFC 9052 sekcje 3.1, 4.2 i 4.4), według wzorca modelu danych mDOC dla elementów issuerSigned, dostosowanego jednak do użycia w statycznej fizycznej karcie. issuerAuth jest obiektem COSE_Sign1 z parametrem alg = ES256 oraz chronionym nagłówkiem zawierającym x5t (parametr nagłówka skrótu certyfikatu COSE X.509 określony w RFC 9360 (sekcja 2)); do celów interoperacyjności algorytmem skrótu stosowanym w x5t jest SHA-256).

   d) Przed zakodowaniem w kodzie QR połączony obiekt CBOR/COSE **jest kompresowany w formacie zlib** (RFC 1950, sekcja 2.2) z **wykorzystaniem algorytmu deflate** (RFC 1951, sekcje 3.2 i 4). Powstałą w ten sposób skompresowaną tablicę bajtów koduje się w **trybie bajtowym kodu QR**, co zapewnia pełną obsługę binarnych ładunków CBOR/COSE oraz interoperacyjność skanerów.

   Dla wszystkich pól tekstowych zawartych w ładunku QR wydawcy kodują znaki jako Unicode UTF-8 w ciągach tekstowych CBOR. Do danych ładunku podpisywanego nie stosuje się transliteracji. Do celów interoperacyjności wydawcy stosują formę normalizacji Unicode C (NFC) do wszystkich pól tekstowych przed podpisaniem ładunku.

   e) **Prefiks**: ciąg QR EPC rozpoczyna się od „EP1:MDOC:". Pozwala to zidentyfikować typ karty oraz profil kodowania. Prefiksy są wrażliwe na wielkość liter i muszą być obecne. Nieznane lub nieobsługiwane prefiksy powodują odrzucenie. Prefiks i skompresowany ładunek są kodowane w kodzie QR jako pojedynczy segment danych w trybie bajtowym.

   f) **Minimalny rozmiar modułu ≥ 0,35 mm** w celu zapewnienia czytelności na drukowanych kartach.

   g) **Wersja maksymalna 20**; z maksymalnie 97 × 97 modułów z każdej strony.

2. **Specyfikacje generowania podpisu EPC**

   Kwalifikowana pieczęć elektroniczna (QSeal) stosowana do zabezpieczenia kodów QR EPC zapewnia, by zakodowane dane pochodziły od upoważnionego organu wydającego i nie zostały zmienione.

   a) **Algorytm podpisu**: algorytmem podpisu jest ES256 (ECDSA z wykorzystaniem SHA-256 przy użyciu krzywej P-256), jak określono w RFC 9053 (sekcja 2.1); w COSE identyfikacja algorytmu odbywa się za pomocą parametru nagłówka alg zgodnie z RFC 9052 (sekcja 3.1).

   b) **Klucz podpisu**: ładunek QR jest podpisywany przy użyciu klucza prywatnego odpowiadającego kwalifikowanemu certyfikatowi pieczęci elektronicznej (QSealC).

   c) **Struktura COSE**: kontenerem podpisu jest obiekt COSE_Sign1. Chroniony nagłówek zawiera alg (ES256) i x5t (parametr nagłówka skrótu certyfikatu COSE X.509 określony w RFC 9360 (sekcja 2); do celów interoperacyjności algorytmem skrótu stosowanym w x5t jest SHA-256. Weryfikacja polega na wykorzystaniu wartości x5t do odnalezienia odpowiedniego certyfikatu w lokalnym repozytorium zaufania weryfikatora, utworzonym na podstawie informacji z zaufanej listy, a następnie na sprawdzeniu łańcucha certyfikatów oraz statusu certyfikatu zgodnie z ramami zaufania eIDAS.

   d) **Standard podpisu**: ładunek kodu QR jest podpisywany jako obiekt COSE_Sign1 zgodnie z RFC 9052 (sekcja 4), CBOR Object Signing and Encryption. Obiekt COSE_Sign1 jest zawarty w issuerAuth i kodowany bez tagu CBOR dla COSE_Sign1. Pole ładunku obiektu COSE_Sign1 jest oddzielone i kodowane jako CBOR null. Do celów generowania i weryfikacji podpisów zewnętrzny ładunek jest strukturą zakodowaną w deterministycznym formacie CBOR, zawierającą wartość docType oraz wartość issuerSigned z mapy CBOR najwyższego poziomu.

e) **Algorytm skrótu**: SHA-256 jest stosowany jako część ES256 do generowania podpisów i weryfikacji integralności.

f) **Kodowanie**: ładunek jest kodowany przy użyciu CBOR (RFC 8949, sekcja 4.2), zgodnie z wymaganiami specyfikacji COSE i mDOC, co zapewnia poprawne kodowanie i odtwarzalność podpisanych danych.

3. **Specyfikacje druku**

a) **Strefa ciszy**: kod QR jest otoczony z każdej strony czystym marginesem o szerokości **4 modułów**, wolnym od jakiegokolwiek druku, wzoru lub tła.

b) **Kontrast**: kod QR jest drukowany na białym tle, przy minimalnym współczynniku kontrastu **4:1**, aby zapewnić wysoką czytelność w różnych warunkach oświetleniowych.

c) Kod QR jest drukowany przy użyciu koloru zdefiniowanego w załączniku II do dyrektywy (UE) 2024/2841, który zapewnia maksymalny kontrast.

d) **Umiejscowienie i rozmiar**: kod QR, wraz ze strefą ciszy, ma wymiary **37 mm × 37 mm** i jest umieszczony na awersie karty, nieco na prawo od środka, w pobliżu dolnej krawędzi. Kod QR jest stosowany maksymalnie w wersji 20 (97 × 97 modułów), przy czym rozmiar modułu wynosi co najmniej 0,35 mm.

Kod QR, wraz ze strefą ciszy, jest umieszczony w odległości przynajmniej 5 mm od dolnego brzegu karty.

4. **Dane w kodzie QR EPC**

Kod QR zawiera minimalny zestaw danych możliwych do weryfikacji offline, zgodnie z zasadą minimalizacji danych zawartą w art. 5 ust. 1 lit. c) rozporządzenia (UE) 2016/679. Struktura ładunku jest następująca:

a) atrybuty karty są kodowane w formacie CBOR w ramach obiektu issuerSigned;

b) struktura ta jest opakowana i podpisana QSeal organu wydającego jako issuerAuth (COSE_Sign1, ES256, z uwzględnieniem x5t, czyli parametru nagłówka skrótu certyfikatu COSE X.509);

c) Powstały obiekt CBOR/COSE jest kompresowany zgodnie z pkt 1 lit. d) niniejszego załącznika. Ładunek kodu QR składa się z prefiksu „EP1:MDOC:", po którym następuje skompresowana tablica bajtów, a cały ładunek jest kodowany w trybie bajtowym jako pojedynczy segment danych kodu QR.

Zawartość danych obejmuje podzbiór danych widocznych z pól na awersie karty wymienionych w załączniku II do dyrektywy (UE) 2024/2841 (termin ważności, numer seryjny karty), wraz z identyfikatorem unieważnienia, podpisem elektronicznym oraz informacjami o schemacie.

Podpis elektroniczny zawiera:

(i) issuerAuth – obiekt COSE_Sign1 podpisany przy użyciu **klucza prywatnego QSealC** organu wydającego;

(ii) chroniony nagłówek zawierający alg = ES256 (algorytm podpisu) i x5t (parametr nagłówka skrótu certyfikatu COSE X.509).

5. **Dane nieobowiązkowe**

Kod QR nie może zawierać żadnych danych nieobowiązkowych.

6. **Identyfikator unieważnienia (RID)**

Identyfikator unieważnienia EPC jest zgodny z pkt 6 załącznika I.

Wykazy unieważnionych kart EPC zawierają jedynie odniesienie do RID. Numery seryjne kart nie są publikowane w wykazach unieważnionych kart.

7. **Ładunek CBOR (w kodzie QR) EPC**

W ładunku QR uwzględnia się wyłącznie następujące dane, zgodnie z widocznymi polami karty EPC określonymi w załączniku II do dyrektywy (UE) 2024/2841:

Pole	Ścieżka mDOC	Rodzaj/Format
Wersja schematu danych	issuerSigned.nameSpaces."eu.epc".ver	Ciąg znaków (np. "1.0")
Rodzaj karty: EPC	docType	Enum ("eu.epc")
Numer seryjny karty	issuerSigned.nameSpaces."eu.epc".sub	Ciąg znaków
Identyfikator unieważnienia	issuerSigned.nameSpaces."eu.epc".rid	CBOR bstr (16 bajtów)
Termin ważności karty	issuerSigned.nameSpaces."eu.epc".exp	tag CBOR 1004, zdefiniowany w RFC 8943 (sekcja 2.1), zawierający ciąg tekstowy w UTF-8 przedstawiający pełną datę w formacie RFC 3339: RRRR-MM-DD.

Podpis elektroniczny jest zawarty w issuerAuth (obiekt COSE_Sign1). Łańcuch certyfikatów nie jest osadzany w ładunku kodu QR; zamiast tego chroniony nagłówek COSE zawiera x5t, odcisk palca certyfikatu umożliwiający odnalezienie odpowiedniego certyfikatu QSealC w lokalnym repozytorium zaufania weryfikatora.

8. **Przykład ładunku kodu QR EPC: reprezentacja logiczna w konwencji JavaScript Object Notation (JSON) z komentarzem**

Poniższy przykład stanowi czytelną dla człowieka reprezentację logicznego widoku EPC w JavaScript Object Notation (JSON). W praktyce struktura ta nie ma postaci czytelnej dla człowieka, ponieważ:

a) jest kodowana w CBOR (RFC 8949, sekcja 3);

b) jest podpisana przy użyciu struktury COSE_Sign1 bez tagów z oddzielonym ładunkiem (RFC 9052, sekcja 4);

c) zawiera termin ważności jako wartość stanowiącą pełną datę w formacie tagu CBOR 1004 zgodnie z RFC 8943 (sekcja 2.1);

d) zawiera parametr x5t w nagłówku chronionym zgodnie z RFC 9360, przy użyciu skrótu SHA-256 do zakodowanego w formacie DER certyfikatu podmiotu końcowego QSealC; oraz

e) jest kompresowana i opatrzona prefiksem w postaci ciągu EP1:MDOC: zanim zostanie zakodowana w kod QR.

```
{
  // konwencja JSON, jedynie logiczny widok EPC czytelny dla człowieka.
  // Faktyczny ładunek QR to deterministyczny format CBOR, a nie JSON.
  "docType": "eu.epc", // poświadczenie EPC. Zawiera wartość docType, wraz z
    //issuerSigned, w ładunku zewnętrznym COSE_Sign1.

  "issuerSigned": {
    // dane chronione przez issuerAuth; użyte jako oddzielony ładunek.
    // Do celów generowania i weryfikacji podpisów oddzielony ładunek zewnętrzny obejmuje zarówno
```

```
  // docType jak i issuerSigned.
  "nameSpaces": {
    "eu.epc": {
      "ver": "1.0", // wersja profilu/schematu kodu QR

      // Numer seryjny karty; określony przez wydawcę, maksymalnie 24 znaki.
      "sub": "EF123456789012345678 90GH",

      // Identyfikator unieważnienia: rzeczywista wartość CBOR bstr, 16 bajtów/128 bitów.
      // dla czytelności pokazana tutaj jako 32-znakowy ciąg heksadecymalny.
      "rid": "4a8d9c11223344556677889 9aabbccdd",

      // Faktyczne kodowanie CBOR wykorzystuje tag 1004 dla pełnej daty w formacie RFC 3339.
      "exp": "2030-12-31"
    }
  }
},

"issuerAuth": {
  // Faktyczny format: COSE_Sign1 bez tagów, a nie obiekt JSON.
  "type": "COSE_Sign1",
  "tagged": false, // zakodowany bez tagu COSE_Sign1 CBOR
  "payload": "detached", // pole ładunku COSE to CBOR null

  "protectedHeader": {
    // alg: ES256; równoważny parametr nagłówka COSE 1 = -7.
    "alg": "ES256",

    // x5t: odcisk palca certyfikatu; parametr nagłówka COSE 34.
    "x5t": {
      "hashAlg": "SHA-256", // równoważna wartość skrótu COSE -16

      // skrót SHA-256 zakodowanego w formacie DER certyfikatu podmiotu końcowego QSealC.
      // 32 bajty reprezentowane jako 64-znakowy ciąg heksadecymalny.
      "hashValue":
      "0123456789abcdef0123456789abcdef0123456789abcdef0123456789abcdef"
    }
  },

  "unprotectedHeader": {}, // pusty w tym przykładzie

  // podpis COSE z algorytmem ES256: 64 bajty = 128-znakowy ciąg heksadecymalny
  "signature":
  "0123456789abcdef0123456789abcdef0123456789abcdef0123456789abcdef0123456789abcde-
  f0123456789abcdef0123456789abcdef0123456789abcdef"
 }
}
```

9. **Stosowanie mechanizmów kryptograficznych**

Stosowanie mechanizmów kryptograficznych w kontekście niniejszego załącznika odbywa się zgodnie z uzgodnionymi mechanizmami kryptograficznymi zatwierdzonymi przez Europejską Grupę ds. Certyfikacji Cyberbezpieczeństwa i opublikowanymi przez Agencję Unii Europejskiej ds. Cyberbezpieczeństwa (ENISA).

ZAŁĄCZNIK III

PRZEKAZYWANIE INFORMACJI, O KTÓRYCH MOWA W ART. 6 UST. 2

1. Państwa członkowskie przekazują Komisji następujące informacje na temat każdego właściwego organu lub podmiotu odpowiedzialnego za wydawanie fizycznych wersji europejskiej karty osoby z niepełnosprawnością lub europejskiej karty parkingowej dla osób z niepełnosprawnościami:

   a) nazwę właściwego organu lub podmiotu odpowiedzialnego za wydawanie fizycznych wersji europejskiej karty osoby z niepełnosprawnością lub europejskiej karty parkingowej dla osób z niepełnosprawnościami;

   b) numer rejestracyjny właściwego organu lub podmiotu odpowiedzialnego za wydawanie fizycznych wersji europejskiej karty osoby z niepełnosprawnością lub europejskiej karty parkingowej dla osób z niepełnosprawnościami;

   c) adres e-mail i numer telefonu właściwego organu lub podmiotu odpowiedzialnego za wydawanie fizycznych wersji europejskiej karty osoby z niepełnosprawnością lub europejskiej karty parkingowej dla osób z niepełnosprawnościami;

   d) co najmniej jeden certyfikat, który można wykorzystać do weryfikacji pieczęci elektronicznej utworzonej przez właściwy organ lub podmiot odpowiedzialny za wydawanie fizycznych wersji europejskiej karty osoby z niepełnosprawnością lub europejskiej karty parkingowej dla osób z niepełnosprawnościami i w odniesieniu do którego poświadczone dane dotyczące tożsamości obejmują nazwę i numer rejestracyjny wydawcy, jak określono odpowiednio w lit. a) i b);

   e) adres URL miejsca, w którym wydawca publikuje informacje o statusie ważności fizycznych wersji europejskiej karty osoby z niepełnosprawnością lub europejskiej karty parkingowej dla osób z niepełnosprawnościami.

2. Państwa członkowskie mogą przekazywać Komisji następujące informacje na temat każdego właściwego organu lub podmiotu odpowiedzialnego za wydawanie fizycznych wersji europejskiej karty osoby z niepełnosprawnością lub europejskiej karty parkingowej dla osób z niepełnosprawnościami:

   a) adres URL strony internetowej zawierającej polityki i warunki właściwego organu lub podmiotu odpowiedzialnego za wydawanie fizycznych wersji europejskiej karty osoby z niepełnosprawnością lub europejskiej karty parkingowej dla osób z niepełnosprawnościami, które to polityki i warunki mają zastosowanie do wydawania fizycznych wersji europejskiej karty osoby z niepełnosprawnością i europejskiej karty parkingowej dla osób z niepełnosprawnościami i korzystania z nich;

   b) w stosownych przypadkach adres URL strony internetowej zawierającej dodatkowe informacje na temat właściwego organu lub podmiotu odpowiedzialnego za wydawanie fizycznych wersji europejskiej karty osoby z niepełnosprawnością lub europejskiej karty parkingowej dla osób z niepełnosprawnościami.

ZAŁĄCZNIK IV

SPECYFIKACJE TECHNICZNE WYKAZU UNIEWAŻNIONYCH KART DLA FIZYCZNYCH WERSJI EUROPEJSKIEJ KARTY OSOBY Z NIEPEŁNOSPRAWNOŚCIĄ LUB EUROPEJSKIEJ KARTY PARKINGOWEJ DLA OSÓB Z NIEPEŁNOSPRAWNOŚCIAMI

1. Na potrzeby niniejszego załącznika identyfikator odpowiada identyfikatorowi unieważnienia (RID) zdefiniowanemu w pkt 6 załącznika I i pkt 6 załącznika II.

2. Wykaz unieważnionych kart wdraża się jako token listy identyfikatorów w formacie CWT (RFC 8392, sekcja 7), zgodnie z pkt 5.2 specyfikacji listy statusu tokenów (draft-ietf-oauth-status-list-14), z następującymi zmianami:

   a) wartość elementu „type” wynosi „application/identifierlist+cwt”;

   b) obecny jest element czasu wygaśnięcia;

   c) element StatusList nie jest obecny w zbiorze elementów CWT;

   d) struktura IdentifierList określona w pkt 3 jest obecna jako element w zbiorze elementów CWT przy użyciu klucza 65530;

   e) CWT stanowi obiekt COSE_Sign1, przy czym do obliczenia podpisu stosuje się algorytm podpisu zgodny z uzgodnionymi mechanizmami kryptograficznymi zatwierdzonymi przez Europejską Grupę ds. Certyfikacji Cyberbezpieczeństwa i opublikowanymi przez Agencję Unii Europejskiej ds. Cyberbezpieczeństwa (ENISA);

   f) CWT zawiera parametr x5chain zdefiniowany w RFC 9360 (sekcja 2) w chronionym nagłówku zawierającym certyfikat lub łańcuch certyfikatów służący do weryfikacji podpisu wykazu unieważnionych kart;

   g) rozszerzone użycie klucza OID określone w specyfikacji listy statusu tokenów (draft-ietf-oauth-status-list-14) można stosować na potrzeby certyfikatu podpisującego listę identyfikatorów; zaleca się, aby weryfikatorzy obsługiwali ten identyfikator OID oraz aby infrastruktury wydawców nie oznaczały pola rozszerzonego użycia klucza jako krytycznego w przypadku stosowania identyfikatora OID rozszerzonego użycia klucza.

3. Struktura IdentifierList stanowi strukturę CBOR zdefiniowaną przy użyciu języka Concise Data Definition Language (CDDL) w następujący sposób:

```
IdentifierList = {

  "identifiers": { * Identifier => IdentifierInfo },

  ? "aggregation_uri": Aggregation_uri,

  * tstr => RFU

}

IdentifierInfo = {

  (tstr/int) => RFU

}

Identifier = bstr

Aggregation_uri = tstr
```