►B

ROZPORZĄDZENIE WYKONAWCZE KOMISJI (UE) 2015/1502

z dnia 8 września 2015 r.

w sprawie ustanowienia minimalnych specyfikacji technicznych i procedur dotyczących ►C1 poziomów bezpieczeństwa ◄ w zakresie środków identyfikacji elektronicznej na podstawie art. 8 ust. 3 rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 910/2014 w sprawie identyfikacji elektronicznej i usług zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznym

(Tekst mający znaczenie dla EOG)

(Dz.U. L 235 z 9.9.2015, s. 7)

zmienione przez:

		Dziennik Urzędowy		
		nr	strona	data
►M1	Rozporządzenie wykonawcze Komisji (UE) 2022/960 z dnia 20 czerwca 2022 r.	L 165	40	21.6.2022

sprostowane przez:

►C1 Sprostowanie, Dz.U. L 345 z 20.12.2016, s. 142 (2015/1502)

▼B

ROZPORZĄDZENIE WYKONAWCZE KOMISJI (UE) 2015/1502

z dnia 8 września 2015 r.

w sprawie ustanowienia minimalnych specyfikacji technicznych i procedur dotyczących ►C1 poziomów bezpieczeństwa ◄ w zakresie środków identyfikacji elektronicznej na podstawie art. 8 ust. 3 rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 910/2014 w sprawie identyfikacji elektronicznej i usług zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznym

(Tekst mający znaczenie dla EOG)

Artykuł 1

1. Niski, średni i wysoki ►C1 poziom bezpieczeństwa ◄ w odniesieniu do środka identyfikacji elektronicznej wydanego zgodnie z notyfikowanym systemem identyfikacji elektronicznej ustala się z uwzględnieniem wymagań i procedur określonych w załączniku.

2. Specyfikacje i procedury określone w załączniku są wykorzystywane do określenia ►C1 poziomu bezpieczeństwa ◄ środka identyfikacji elektronicznej wydanego zgodnie z notyfikowanym systemem identyfikacji elektronicznej za pomocą określenia wiarygodności i jakości następujących elementów:

a) wprowadzenie do systemu, jak określono w sekcji 2.1 załącznika do niniejszego rozporządzenia zgodnie z art. 8 ust. 3 lit. a) rozporządzenia (UE) nr 910/2014;

b) zarządzanie środkiem identyfikacji elektronicznej, jak określono w sekcji 2.2 załącznika do niniejszego rozporządzenia zgodnie z art. 8 ust. 3 lit. b) rozporządzenia (UE) nr 910/2014;

c) uwierzytelnianie, jak określono w sekcji 2.3 załącznika do niniejszego rozporządzenia zgodnie z art. 8 ust. 3 lit. c) rozporządzenia (UE) nr 910/2014;

d) zarządzanie i organizacja, jak określono w sekcji 2.4 załącznika do niniejszego rozporządzenia zgodnie z art. 8 ust. 3 lit. d) oraz e) rozporządzenia (UE) nr 910/2014.

3. Jeśli środek identyfikacji elektronicznej wydany w ramach notyfikowanego systemu identyfikacji elektronicznej spełnia wymaganie wymienione w odniesieniu do wyższego ►C1 poziomu bezpieczeństwa ◄, wówczas zakłada się, że spełnia on równoważne wymaganie dotyczące niższego ►C1 poziomu bezpieczeństwa ◄.

4. Wszystkie elementy wymienione w załączniku w odniesieniu do danego ►C1 poziomu bezpieczeństwa ◄ środka identyfikacji elektronicznej wydanego zgodnie z notyfikowanym systemem identyfikacji elektronicznej powinny zostać spełnione, aby zapewnić zgodność z deklarowanym ►C1 poziomem bezpieczeństwa ◄, chyba że w odpowiedniej części załącznika określono inaczej.

Artykuł 2

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.

▼B

ZAŁĄCZNIK

Specyfikacje techniczne i procedury dotyczące niskiego, średniego i wysokiego ►C1 poziomu bezpieczeństwa ◄ w odniesieniu do środka identyfikacji elektronicznej wydanego w ramach notyfikowanego systemu identyfikacji elektronicznej

1. **Stosowane definicje**

Na potrzeby niniejszego załącznika stosuje się następujące definicje:

1) „wiarygodne źródło” oznacza każde źródło, niezależnie od jego formy, co do którego można mieć pewność, że dostarcza ono dokładnych danych, informacji lub dowodów, które mogą służyć do potwierdzenia tożsamości;

2) „czynnik uwierzytelniania” oznacza czynnik, którego związek z osobą jest potwierdzony i który należy do jednej z poniższych kategorii:

   a) „czynnik uwierzytelniania na podstawie posiadania” oznacza czynnik uwierzytelniania, w przypadku którego od podmiotu podlegającego uwierzytelnieniu wymaga się wykazania jego posiadania;

   b) „czynnik uwierzytelniania na podstawie wiedzy” oznacza czynnik uwierzytelniania, w przypadku którego od podmiotu podlegającego uwierzytelnieniu wymaga się wykazania jego znajomości;

   c) „czynnik uwierzytelniania na podstawie cech przyrodzonych” oznacza czynnik uwierzytelnienia, który opiera się na rzeczywistym atrybucie osoby fizycznej, w którego przypadku od podmiotu podlegającego uwierzytelnieniu wymaga się wykazania, że tę cechę fizyczną posiada;

3) „uwierzytelnianie dynamiczne” oznacza proces elektroniczny z zastosowaniem kryptografii lub innych technik służący dostarczeniu na żądanie elektronicznego dowodu, iż podmiot podlegający uwierzytelnieniu jest w posiadaniu danych identyfikacyjnych lub dane te znajdują się pod jego kontrolą, oraz który ulega zmianie z każdym uwierzytelnieniem zachodzącym między podmiotem podlegającym uwierzytelnieniu a systemem weryfikacji tożsamości danego podmiotu;

4) „system zarządzania bezpieczeństwem informacji” oznacza zbiór procesów i procedur służących do zarządzania dopuszczalnymi ►C1 poziomami bezpieczeństwa ◄ związanych z bezpieczeństwem informacji.

2. **Specyfikacje techniczne i procedury**

Elementy specyfikacji technicznych i procedury przedstawione w niniejszym załączniku stosuje się do określenia, w jaki sposób wymagania i kryteria określone w art. 8 rozporządzenia (UE) nr 910/2014 należy stosować w odniesieniu do środka identyfikacji elektronicznej wydanego w ramach systemu identyfikacji elektronicznej.

2.1. *Wprowadzenie do systemu*

2.1.1. Wniosek o rejestrację i rejestracja

►C1 Poziom bezpieczeństwa ◄	Wymagane elementy
Niski	1. Zapewnienie znajomości przez wnioskodawcę warunków odnoszących się do stosowania środków identyfikacji elektronicznej. ►C1 2. Zapewnienie znajomości przez wnioskodawcę zalecanych środków bezpieczeństwa odnoszących się do środków identyfikacji elektronicznej. ◄ 3. Zebranie odpowiednich danych identyfikacyjnych wymaganych do sprawdzenia i weryfikacji tożsamości.
Średni	Takie same jak przy poziomie niskim.
Wysoki	Takie same jak przy poziomie niskim.

▼B

2.1.2. Sprawdzenie i weryfikacja tożsamości (osoba fizyczna)

►C1 Poziom bezpieczeństwa ◄	Wymagane elementy
Niski	1. Można zakładać, że dana osoba posiada dowody uznane przez państwo członkowskie, w którym złożono wniosek o środek identyfikacji elektronicznej, oraz reprezentuje deklarowaną tożsamość. 2. Dowody te można uznać za autentyczne lub istniejące zgodnie z informacjami z wiarygodnego źródła i dowody wydają się zachowywać ważność. 3. Wiadomo z wiarygodnego źródła, że deklarowana tożsamość istnieje, oraz można przypuszczać, że deklaruje ją jedna i ta sama osoba.
Średni	Jak przy poziomie niskim oraz konieczność spełnienia jednego z alternatywnych warunków wymienionych w pkt 1–4: 1. potwierdzono, że dana osoba posiada dowody uznane przez państwo członkowskie, w którym złożono wniosek o środek identyfikacji elektronicznej, oraz reprezentuje deklarowaną tożsamość, oraz dowody zostały sprawdzone w celu ustalenia ich autentyczności lub z wiarygodnego źródła wiadomo, że dowody istnieją i dotyczą rzeczywistej osoby, oraz podjęto działania w celu zminimalizowania ryzyka, że tożsamość danej osoby nie jest tożsamością deklarowaną, biorąc pod uwagę np. ryzyko utraty, kradzieży, zawieszenia, unieważnienia bądź upływu terminu ważności dowodu; lub 2. dokument tożsamości zostaje przedstawiony w trakcie procesu rejestracji w państwie członkowskim, w którym go wydano, i okazuje się, że odnosi się on do osoby okazującej, oraz podjęto działania w celu zminimalizowania ryzyka, że tożsamość danej osoby nie jest tożsamością deklarowaną, biorąc pod uwagę np. ryzyko utraty, kradzieży, zawieszenia, unieważnienia bądź upływu terminu ważności dokumentów; lub 3. w przypadku gdy procedury stosowane uprzednio przez podmiot publiczny lub prywatny w tym samym państwie członkowskim w celu innym niż wydawanie środków identyfikacji elektronicznej zapewniają ►C1 poziom bezpieczeństwa ◄ równoważny do zapewnionego przez środki określone w sekcji 2.1.2 dla średniego ►C1 poziomu bezpieczeństwa ◄, podmiot odpowiedzialny za rejestrację nie musi powtarzać tych wcześniejszych procedur, pod warunkiem że taki równoważny ►C1 poziom bezpieczeństwa ◄ jest potwierdzony przez jednostkę oceniającą zgodność, o której mowa w art. 2 ust. 13 rozporządzenia Parlamentu Europejskiego i Rady (WE) nr 765/2008 ([1]), lub przez równoważny organ; lub 4. jeżeli środki identyfikacji elektronicznej są wydawane na podstawie ważnych zgłoszonych środków identyfikacji elektronicznej charakteryzujących się średnim lub wysokim ►C1 poziomem bezpieczeństwa ◄ i biorąc pod uwagę ryzyko zmiany danych identyfikujących osobę, nie jest konieczne powtarzanie sprawdzania tożsamości oraz procedur weryfikacji. Jeżeli środek identyfikacji elektronicznej służący jako podstawa nie został notyfikowany, średni lub wysoki ►C1 poziom bezpieczeństwa ◄ musi być potwierdzony przez jednostkę oceniającą zgodność, o której mowa w art. 2 ust. 13 rozporządzenia (WE) nr 765/2008, lub przez równoważny organ.

▼B

►C1 Poziom bezpieczeństwa ◄	Wymagane elementy
Wysoki	Muszą zostać spełnione wymagania pkt 1 albo pkt 2: 1. jak przy poziomie średnim oraz konieczność spełnienia jednego z alternatywnych warunków wymienionych w lit. a)–c): a) potwierdzono, że dana osoba posiada dowody identyfikacji fotograficznej lub biometrycznej uznane przez państwo członkowskie, w którym złożono wniosek o wydanie środka identyfikacji elektronicznej, oraz że dowody te stanowią potwierdzenie deklarowanej tożsamości, dowody są sprawdzane w celu ustalenia, czy zachowują ważność zgodnie z informacjami z wiarygodnego źródła, oraz wnioskodawca jest identyfikowany jako osoba o deklarowanej tożsamości poprzez porównanie jego jednej cechy fizycznej lub większej liczby takich jego cech z informacjami z wiarygodnego źródła; lub b) w przypadku gdy procedury stosowane uprzednio przez podmiot publiczny lub prywatny w tym samym państwie członkowskim w celu innym niż wydawanie środków identyfikacji elektronicznej zapewniają ►C1 poziom bezpieczeństwa ◄ równoważny do zapewnionego przez środki określone w sekcji 2.1.2 dla wysokiego ►C1 poziomu bezpieczeństwa ◄, podmiot odpowiedzialny za rejestrację nie musi powtarzać tych wcześniejszych procedur, pod warunkiem że taki równoważny ►C1 poziom bezpieczeństwa ◄ jest potwierdzony przez jednostkę oceniającą zgodność, o której mowa w art. 2 ust. 13 rozporządzenia (WE) nr 765/2008, lub przez równoważny organ, oraz podejmowane są działania mające na celu wykazanie, że wyniki poprzednich procedur zachowują ważność; lub c) jeżeli środki identyfikacji elektronicznej są wydawane na podstawie ważnych zgłoszonych środków identyfikacji elektronicznej charakteryzujących się wysokim ►C1 poziomem bezpieczeństwa ◄ i biorąc pod uwagę ryzyko zmiany danych identyfikujących osobę, nie jest konieczne powtarzanie sprawdzania tożsamości oraz procedur weryfikacji. Jeżeli środek identyfikacji elektronicznej służący jako podstawa nie został notyfikowany, wysoki ►C1 poziom bezpieczeństwa ◄ musi być potwierdzony przez jednostkę oceniającą zgodność, o której mowa w art. 2 ust. 13 rozporządzenia (WE) nr 765/2008, lub przez równoważny organ, oraz podejmowane są działania mające na celu wykazanie, że rezultaty tej poprzedniej procedury wydawania notyfikowanych środków identyfikacji elektronicznej zachowują ważność; LUB 2. jeżeli wnioskodawca nie przedstawił uznanych dowodów identyfikacji fotograficznej lub biometrycznej, zastosowanie mają te same procedury uzyskiwania takich uznanych dowodów identyfikacji fotograficznej lub biometrycznej co stosowane na poziomie krajowym w państwie członkowskim podmiotu odpowiedzialnego za rejestrację.

([1]) Rozporządzenie Parlamentu Europejskiego i Rady (WE) nr 765/2008 z dnia 9 lipca 2008 r. ustanawiające wymagania w zakresie akredytacji i nadzoru rynku odnoszące się do warunków wprowadzania produktów do obrotu i uchylające rozporządzenie (EWG) nr 339/93 (Dz.U. L 218 z 13.8.2008, s. 30).

2.1.3. Sprawdzenie i weryfikacja tożsamości (osoba prawna)

►C1 Poziom bezpieczeństwa ◄	Wymagane elementy
Niski	1. Deklarowaną tożsamość osoby prawnej wykazuje się na podstawie dowodów uznanych przez państwo członkowskie, w którym złożono wniosek o środek identyfikacji elektronicznej.

▼B

►C1 Poziom bezpieczeństwa ◄	Wymagane elementy
	2. Dowody wydają się zachowywać ważność i można uznać, że są autentyczne lub istniejące zgodnie z informacjami z wiarygodnego źródła, jeżeli wprowadzenie osoby prawnej do wiarygodnego źródła jest dobrowolne i jest regulowane za pomocą ustalenia między osobą prawną oraz wiarygodnym źródłem. 3. Wiarygodne źródło nie dysponuje wiedzą o statusie osoby prawnej, który uniemożliwiałby jej działanie jako osoby prawnej.
Średni	Jak przy poziomie niskim oraz konieczność spełnienia jednego z alternatywnych warunków wymienionych w pkt 1–3: 1. deklarowaną tożsamość osoby prawnej wykazuje się na podstawie dowodów uznanych przez państwo członkowskie, w którym złożono wniosek o środek identyfikacji elektronicznej, obejmujących nazwę osoby prawnej, jej formę prawną oraz, w stosownych przypadkach, jej numer rejestracyjny, oraz dowody są sprawdzane w celu ustalenia, czy są autentyczne bądź czy wiadomo, że istnieją zgodnie z informacjami z wiarygodnego źródła, jeżeli wprowadzenie osoby prawnej do wiarygodnego źródła jest wymagane do prowadzenia przez nią działalności w odnośnym sektorze, oraz podjęto działania w celu zminimalizowania ryzyka, że tożsamość danej osoby prawnej nie jest tożsamością deklarowaną, biorąc pod uwagę np. ryzyko utraty, kradzieży, zawieszenia, unieważnienia bądź upływu terminu ważności dokumentów; lub 2. w przypadku gdy procedury stosowane uprzednio przez podmiot publiczny lub prywatny w tym samym państwie członkowskim w celu innym niż wydawanie środków identyfikacji elektronicznej zapewniają ►C1 poziom bezpieczeństwa ◄ równoważny do zapewnionego przez środki określone w sekcji 2.1.3 dla średniego ►C1 poziomu bezpieczeństwa ◄, podmiot odpowiedzialny za rejestrację nie musi powtarzać tych wcześniejszych procedur, pod warunkiem że taki równoważny ►C1 poziom bezpieczeństwa ◄ jest potwierdzony przez jednostkę oceniającą zgodność, o której mowa w art. 2 ust. 13 rozporządzenia (WE) nr 765/2008, lub przez równoważny organ; lub 3. jeżeli środki identyfikacji elektronicznej są wydawane na podstawie ważnych zgłoszonych środków identyfikacji elektronicznej charakteryzujących się średnim lub wysokim ►C1 poziomem bezpieczeństwa ◄, nie jest konieczne powtarzanie sprawdzania tożsamości oraz procedur weryfikacji. Jeżeli środek identyfikacji elektronicznej służący jako podstawa nie został notyfikowany, średni lub wysoki ►C1 poziom bezpieczeństwa ◄ musi być potwierdzony przez jednostkę oceniającą zgodność, o której mowa w art. 2 ust. 13 rozporządzenia (WE) nr 765/2008, lub przez równoważny organ.
Wysoki	Jak przy poziomie średnim oraz konieczność spełnienia jednego z alternatywnych warunków wymienionych w pkt 1–3: 1. deklarowaną tożsamość osoby prawnej wykazuje się na podstawie dowodów uznanych przez państwo członkowskie, w którym złożono wniosek o środek identyfikacji elektronicznej, obejmujących nazwę osoby prawnej, jej formę prawną oraz co najmniej jeden niepowtarzalny identyfikator osoby prawnej stosowany w warunkach krajowych, oraz dowody zostały sprawdzone w celu ustalenia ich ważności zgodnie z wiarygodnym źródłem; lub

▼B

►C1 Poziom bezpieczeństwa ◄	Wymagane elementy
	2. w przypadku gdy procedury stosowane uprzednio przez podmiot publiczny lub prywatny w tym samym państwie członkowskim w celu innym niż wydawanie środków identyfikacji elektronicznej zapewniają ►C1 poziom bezpieczeństwa ◄ równoważny do zapewnionego przez środki określone w sekcji 2.1.3 dla wysokiego ►C1 poziomu bezpieczeństwa ◄, podmiot odpowiedzialny za rejestrację nie musi powtarzać tych wcześniejszych procedur, pod warunkiem że taki równoważny ►C1 poziom bezpieczeństwa ◄ jest potwierdzony przez jednostkę oceniającą zgodność, o której mowa w art. 2 ust. 13 rozporządzenia (WE) nr 765/2008, lub przez równoważny organ, oraz podejmowane są działania mające na celu wykazanie, że wyniki poprzednich procedur zachowują ważność; lub 3. jeżeli środki identyfikacji elektronicznej są wydawane na podstawie ważnych zgłoszonych środków identyfikacji elektronicznej charakteryzujących się wysokim ►C1 poziomem bezpieczeństwa ◄, nie jest konieczne powtarzanie sprawdzania tożsamości oraz procedur weryfikacji. Jeżeli środek identyfikacji elektronicznej służący jako podstawa nie został notyfikowany, wysoki ►C1 poziom bezpieczeństwa ◄ musi być potwierdzony przez jednostkę oceniającą zgodność, o której mowa w art. 2 ust. 13 rozporządzenia (WE) nr 765/2008, lub przez równoważny organ, oraz podejmowane są działania mające na celu wykazanie, że rezultaty tej poprzedniej procedury wydawania notyfikowanych środków identyfikacji elektronicznej zachowują ważność.

2.1.4. Powiązanie między środkami identyfikacji elektronicznej osób fizycznych i prawnych

W stosownych przypadkach w odniesieniu do powiązania między środkami identyfikacji elektronicznej osoby fizycznej i środkami identyfikacji elektronicznej osoby prawnej („powiązania”) mają zastosowanie następujące warunki:

1) Musi istnieć możliwość zawieszania lub cofnięcia powiązania. Cykl życia powiązania (np. aktywacja, zawieszenie, odnowienie, cofnięcie) odbywa się zgodnie z krajowymi uznanymi procedurami.

2) Osoba fizyczna, której środek identyfikacji elektronicznej jest powiązany ze środkiem identyfikacji elektronicznej osoby prawnej, może powierzyć użytkowanie powiązania innej osobie fizycznej w oparciu o krajowe uznane procedury. Jednakże delegująca osoba fizyczna nadal ponosi odpowiedzialność.

3) Powiązanie realizowane jest w następujący sposób:

►C1 Poziom bezpieczeństwa ◄	Wymagane elementy
Niski	1. Sprawdzenie tożsamości osoby fizycznej działającej w imieniu osoby prawnej jest weryfikowane jako przeprowadzone na co najmniej niskim poziomie. 2. Powiązanie zostało ustanowione w oparciu o krajowe uznane procedury. 3. Wiarygodne źródło nie dysponuje wiedzą o statusie osoby fizycznej, który uniemożliwiałby jej działanie w imieniu osoby prawnej.
Średni	Pkt 3 z poziomu niskiego oraz: 1. Sprawdzenie tożsamości osoby fizycznej działającej w imieniu osoby prawnej jest weryfikowane jako przeprowadzone na poziomie średnim lub wysokim. 2. Powiązanie zostało ustanowione w oparciu o krajowe uznane procedury, które doprowadziły do jego zarejestrowania w wiarygodnym źródle. 3. Powiązanie zostało zweryfikowane na podstawie informacji z wiarygodnego źródła.

▼B

►C1 Poziom bezpieczeństwa ◄	Wymagane elementy
Wysoki	Pkt 3 z poziomu niskiego i pkt 2 z poziomu średniego oraz: 1. Sprawdzenie tożsamości osoby fizycznej działającej w imieniu osoby prawnej jest weryfikowane jako przeprowadzone na poziomie wysokim. 2. Powiązanie zostało zweryfikowane w oparciu o niepowtarzalny identyfikator osoby prawnej stosowany w warunkach krajowych oraz na podstawie informacji z wiarygodnego źródła w sposób jednoznaczny identyfikujących osobę fizyczną.

2.2. *Zarządzanie środkami identyfikacji elektronicznej*

2.2.1. Cechy charakterystyczne i konstrukcja środków identyfikacji elektronicznej

►C1 Poziom bezpieczeństwa ◄	Wymagane elementy
Niski	1. Środek identyfikacji elektronicznej wykorzystuje co najmniej jeden czynnik uwierzytelniania. 2. Środek identyfikacji elektronicznej jest zaprojektowany w taki sposób, aby wystawiający podejmował rozsądne kroki w celu sprawdzenia, czy jest on stosowany jedynie przez osobę, do której należy, lub pod jej kontrolą.
Średni	1. Środek identyfikacji elektronicznej wykorzystuje co najmniej dwa czynniki uwierzytelniania należące do różnych kategorii. 2. Środek identyfikacji elektronicznej jest zaprojektowany w taki sposób, że można zakładać, iż jest on stosowany jedynie przez osobę, do której należy, lub pod jej kontrolą.
Wysoki	Jak przy poziomie średnim oraz: 1. Środek identyfikacji elektronicznej stanowi ochronę przed powielaniem i manipulacją oraz przed atakującymi dysponującymi wysokim potencjałem ataku. 2. Środek identyfikacji elektronicznej jest zaprojektowany w taki sposób, że może być niezawodnie chroniony przez osobę, do której należy, przed wykorzystaniem przez innych.

2.2.2. Wydawanie, dostarczanie i aktywacja

►C1 Poziom bezpieczeństwa ◄	Wymagane elementy
Niski	Po wydaniu środek identyfikacji elektronicznej jest dostarczany za pośrednictwem mechanizmu, co do którego można zakładać, iż przez jego zastosowanie środek dotrze wyłącznie do przeznaczonej osoby.
Średni	Po wydaniu środek identyfikacji elektronicznej jest dostarczany za pośrednictwem mechanizmu, co do którego można zakładać, iż przez jego zastosowanie środek zostanie oddany w posiadanie wyłącznie osobie, do której należy.
Wysoki	W procesie aktywacji sprawdza się, czy środek identyfikacji elektronicznej został oddany w posiadanie wyłącznie osobie, do której należy.

2.2.3. Zawieszenie, cofnięcie i przywrócenie

►C1 Poziom bezpieczeństwa ◄	Wymagane elementy
Niski	1. Można zawiesić lub wycofać środek identyfikacji elektronicznej w sposób terminowy i skuteczny. 2. Istnieją środki umożliwiające zapobieżenie nieuprawnionemu zawieszeniu, cofnięciu lub przywróceniu środka. ►C1 3. Przywrócenie środka odbywa się jedynie, jeśli w dalszym ciągu spełnione są wymagania w zakresie bezpieczeństwa ustanowione przed zawieszeniem lub cofnięciem. ◄
Średni	Takie same jak przy poziomie niskim.
Wysoki	Takie same jak przy poziomie niskim.

▼B

2.2.4. Wznowienie i wymiana

►C1 Poziom bezpieczeństwa ◄	Wymagane elementy
Niski	►C1 Biorąc pod uwagę ryzyko wystąpienia zmiany w danych identyfikujących osobę, przy wznowieniu bądź wymianie muszą zostać spełnione te same wymagania w zakresie bezpieczeństwa jak przy wstępnym sprawdzeniu i weryfikacji tożsamości lub wznowienia bądź wymiany dokonuje się na podstawie ważnego środka identyfikacji elektronicznej o tym samym lub wyższym poziomie bezpieczeństwa. ◄
Średni	Takie same jak przy poziomie niskim.
Wysoki	Jak przy poziomie niskim oraz: w przypadku gdy wznowienie bądź wymiana odbywają się się na podstawie ważnego środka identyfikacji elektronicznej, dane dotyczące tożsamości są weryfikowane z wykorzystaniem wiarygodnego źródła.

2.3. *Uwierzytelnienie*

W tej części opisano zagrożenia związane ze stosowaniem mechanizmu uwierzytelniania i wymieniono wymagania odnoszące się do każdego ►C1 poziomu bezpieczeństwa ◄. W niniejszej części kontrolę uznaje się za proporcjonalną do ryzyka na danym poziomie.

2.3.1. Mechanizm uwierzytelniania

W poniższej tabeli zestawiono wymagania na poszczególnych ►C1 poziomach bezpieczeństwa ◄ w odniesieniu do mechanizmu uwierzytelniania, za którego pośrednictwem osoba fizyczna lub prawna używa środka identyfikacji elektronicznej do potwierdzenia swojej tożsamości wobec strony ufającej.

►C1 Poziom bezpieczeństwa ◄	Wymagane elementy
Niski	1. Uwolnienie danych identyfikujących osobę jest poprzedzone wiarygodną weryfikacją środka identyfikacji elektronicznej oraz jego ważności. 2. Jeżeli dane identyfikujące osobę są przechowywane w ramach mechanizmu uwierzytelniania, informacje ta są zabezpieczone w celu ochrony przed utratą i narażeniem na szwank, w tym analizą *off-line*. ►C1 3. Mechanizm uwierzytelniania jest sposobem realizacji kontroli bezpieczeństwa na potrzeby weryfikacji środków identyfikacji elektronicznej, dzięki któremu jest mało prawdopodobne, aby takie działania jak zgadywanie, podsłuchiwanie, odtwarzanie lub manipulowanie komunikacji przez atakującego o wyższym podstawowym potencjale ataku mogło zachwiać mechanizmami uwierzytelniania. ◄
Średni	Jak przy poziomie niskim oraz: 1. Uwolnienie danych identyfikujących osobę jest poprzedzone wiarygodną weryfikacją środka identyfikacji elektronicznej oraz jego ważności za pomocą uwierzytelniania dynamicznego. ►C1 2. Mechanizm uwierzytelniania jest sposobem realizacji kontroli bezpieczeństwa na potrzeby weryfikacji środków identyfikacji elektronicznej, dzięki któremu jest mało prawdopodobne, aby takie działania jak zgadywanie, podsłuchiwanie, odtwarzanie lub manipulowanie komunikacji przez atakującego o umiarkowanym potencjale ataku mogło zachwiać mechanizmami uwierzytelniania. ◄
Wysoki	Jak przy poziomie średnim oraz: ►C1 mechanizm uwierzytelniania jest sposobem realizacji kontroli bezpieczeństwa na potrzeby weryfikacji środków identyfikacji elektronicznej, dzięki któremu jest mało prawdopodobne, aby takie działania jak zgadywanie, podsłuchiwanie, odtwarzanie lub manipulowanie komunikacji przez atakującego o wysokim potencjale ataku mogło zachwiać mechanizmami uwierzytelniania. ◄

▼B

2.4. *Zarządzanie i organizacja*

Wszystkie podmioty świadczące usługi związane z identyfikacją elektroniczną w obrocie transgranicznym („dostawcy”) ustanawiają udokumentowane praktyki zarządzania bezpieczeństwem informacji, strategie, sposoby podejścia do zarządzania ryzykiem oraz inne uznane mechanizmy kontrolne, aby właściwe organy zarządzające odpowiedzialne za systemy identyfikacji elektronicznej w poszczególnych państwach członkowskich mogły mieć pewność, że skuteczne praktyki zostały wprowadzone. W części 2.4 wszystkie wymagania/elementy należy rozumieć jako współmierne z poziomem ryzyka dla danego poziomu.

2.4.1. Przepisy ogólne

►C1 Poziom bezpieczeństwa ◄	Wymagane elementy
Niski	1. Dostawcami świadczącymi usługi operacyjne objęte niniejszym rozporządzeniem są organy publiczne lub podmioty prawne uznane za takie przez prawo krajowe państwa członkowskiego, posiadające ugruntowaną organizację i pełną zdolność operacyjną we wszystkich elementach istotnych dla świadczenia usług. 2. Dostawcy przestrzegają wszelkich wymogów prawnych nałożonych na nich w związku z funkcjonowaniem i świadczeniem usług, w tym dotyczących rodzajów informacji, o jakie można się zwracać, sposobów dokonywania potwierdzania tożsamości, a także tego, jakie informacje mogą być przechowywane i przez jak długi czas. 3. Dostawcy są w stanie wykazać zdolność do ponoszenia ryzyka odpowiedzialności za szkody, jak również posiadanie wystarczających środków finansowych na kontynuowanie działalności i świadczenie usług. 4. Dostawcy odpowiadają za realizację wszystkich zobowiązań przekazanych innemu podmiotowi oraz zapewnienie zgodności z założeniami systemu, tak jakby sami wykonywali te zadania. 5. W odniesieniu do systemów identyfikacji elektronicznej nieustanowionych prawem krajowym musi istnieć opracowany skuteczny plan zakończenia działalności. Plan taki obejmuje uporządkowane zaprzestawanie świadczenia usług lub kontynuację przez innego dostawcę, sposób informowania właściwych organów i użytkowników końcowych, jak również szczegółowe informacje na temat sposobu ochrony, przechowywania i niszczenia rejestrów zgodnie z założeniami systemu.
Średni	Takie same jak przy poziomie niskim.
Wysoki	Takie same jak przy poziomie niskim.

2.4.2. Opublikowane informacje i informacje dla użytkowników

►C1 Poziom bezpieczeństwa ◄	Wymagane elementy
Niski	1. Istnienie opublikowanej definicji usługi obejmującej wszystkie mające zastosowanie zasady, warunki i opłaty, w tym ewentualne ograniczenia dotyczące korzystania z niej. Definicja usługi obejmuje politykę ochrony prywatności. 2. Należy ustanowić odpowiednie działania i procedury w celu zapewnienia, że użytkownicy usługi zostaną poinformowani w odpowiednim czasie i w niezawodny sposób o wszelkich zmianach w definicji usług i wszelkich mających zastosowanie zasadach i warunkach oraz polityce prywatności w odniesieniu do określonej usługi. 3. Należy zastosować odpowiednie działania i procedury w celu zapewnienia udzielania pełnych i prawidłowych odpowiedzi na wnioski o informacje.
Średni	Takie same jak przy poziomie niskim.
Wysoki	Takie same jak przy poziomie niskim.

▼B

2.4.3. Zarządzanie bezpieczeństwem informacji

►C1 Poziom bezpieczeństwa ◄	Wymagane elementy
Niski	►C1 Istnieje skuteczny system zarządzania bezpieczeństwem informacji w zakresie zarządzania i kontroli zagrożeń dla bezpieczeństwa informacji. ◄
Średni	Jak przy poziomie niskim oraz: ►C1 system zarządzania bezpieczeństwem informacji odpowiada sprawdzonym normom lub zasadom zarządzania i kontroli zagrożeń dla bezpieczeństwa informacji. ◄
Wysoki	Takie same jak przy poziomie średnim.

2.4.4. Prowadzenie rejestrów

►C1 Poziom bezpieczeństwa ◄	Wymagane elementy
Niski	1. Zapisywanie i zachowywanie właściwych informacji przy użyciu skutecznego systemu zarządzania rejestrami z uwzględnieniem obowiązujących przepisów i dobrych praktyk w odniesieniu do ochrony danych i ich zatrzymywania. ►C1 2. Zatrzymywanie, o ile jest to dozwolone przez prawo krajowe lub inne krajowe ustalenia administracyjne, i ochrona rejestrów tak długo, jak długo jest to wymagane do celów kontroli, dochodzenia w sprawach naruszeń bezpieczeństwa oraz przechowywania, po czym rejestry te są niszczone w bezpieczny sposób. ◄
Średni	Takie same jak przy poziomie niskim.
Wysoki	Takie same jak przy poziomie niskim.

2.4.5. Obiekty i personel

W poniższej tabeli przedstawiono wymagania dotyczące obiektów i personelu oraz – w stosownych przypadkach – podwykonawców, wykonujących obowiązki objęte niniejszym rozporządzeniem. Zgodność ze wszystkimi wymaganiami powinna być proporcjonalna do poziomu ryzyka związanego z ustalonym ►C1 poziomem bezpieczeństwa ◄.

►C1 Poziom bezpieczeństwa ◄	Wymagane elementy
Niski	1. Istnienie procedur zapewniających, że pracownicy i podwykonawcy są odpowiednio przeszkoleni i wykwalifikowani oraz dysponują doświadczeniem w zakresie umiejętności potrzebnych do wykonywania swoich funkcji. 2. Wystarczająca liczba pracowników i podwykonawców do odpowiedniego funkcjonowania i zapewnienia obsługi usługi, zgodnie z jej zasadami i procedurami. 3. Obiekty służące do świadczenia usługi są stale monitorowane i chronione przed szkodami spowodowanymi przez wydarzenia związane ze środowiskiem naturalnym, nieuprawniony dostęp i inne czynniki, które mogą mieć wpływ na bezpieczeństwo usługi. 4. Obiekty służące do świadczenia usługi gwarantują, że dostęp do stref przechowywania lub przetwarzania danych osobowych, kryptograficznych lub innych informacji podlegających szczególnej ochronie jest ograniczony do upoważnionych pracowników lub podwykonawców.
Średni	Takie same jak przy poziomie niskim.
Wysoki	Takie same jak przy poziomie niskim.

▼B

2.4.6. Kontrole techniczne

►C1 Poziom bezpieczeństwa ◄	Wymagane elementy
Niski	1. Istnienie proporcjonalnych kontroli technicznych w celu zarządzania ryzykiem, na jakie narażone jest bezpieczeństwo świadczonych usług, zapewnienie ochrony poufności, integralności i dostępności przetwarzanych informacji. 2. Elektroniczne kanały komunikacji wykorzystywane do wymiany informacji podlegających szczególnej ochronie lub informacji osobowych są zabezpieczone przed podsłuchem, manipulacją i odtwarzaniem. 3. Dostęp do szczególnie chronionych materiałów kryptograficznych, jeżeli są wykorzystywane do wydawania środków identyfikacji elektronicznej i elektronicznego uwierzytelniania, jest ograniczony do funkcji i zakresu zastosowania bezwzględnie wymagających dostępu. Należy zapewnić, aby materiały te nigdy nie były trwale przechowywane w postaci zwykłego tekstu. ►C1 4. Istnieją procedury zapewniające, że bezpieczeństwo jest trwale utrzymywane oraz że istnieje zdolność reagowania na zmiany poziomu ryzyka, incydenty i przypadki naruszenia bezpieczeństwa. ◄ 5. Wszystkie nośniki zawierające informacje osobowe, kryptograficzne lub inne podlegające szczególnej ochronie są przechowywane, transportowane i usuwane w bezpieczny sposób.
Średni	Takie same jak przy poziomie niskim oraz: materiały kryptograficzne podlegające szczególnej ochronie, jeżeli są wykorzystywane do wydawania środków identyfikacji elektronicznej i uwierzytelniania elektronicznego, są chronione przed nieuprawnionymi manipulacjami.
Wysoki	Takie same jak przy poziomie średnim.

2.4.7. Zgodność i audyt

►C1 Poziom bezpieczeństwa ◄	Wymagane elementy
Niski	Istnienie okresowych audytów wewnętrznych ukierunkowanych na wszystkie elementy istotne dla dostawy świadczonych usług w celu zapewnienia zgodności ze stosowną polityką.
Średni	Istnienie okresowych niezależnych audytów wewnętrznych lub zewnętrznych ukierunkowanych na wszystkie elementy istotne dla dostawy świadczonych usług w celu zapewnienia zgodności ze stosowną polityką.
Wysoki	1. Istnienie okresowych niezależnych audytów zewnętrznych ukierunkowanych na wszystkie elementy istotne dla dostawy świadczonych usług w celu zapewnienia zgodności ze stosowną polityką. 2. Jeśli system zarządzany jest bezpośrednio przez organ publiczny, audyty przeprowadza się zgodnie z prawem krajowym.