

Jak weryfikować klientów zdalnie zgodnie z AMLR: co zmienia projekt RTS AMLA dotyczący należytej staranności wobec klienta

To jest tłumaczenie artykułu [How to verify customers remotely under AMLR: what AMLA's draft CDD RTS changes](#) opublikowanego na blogu Authologic. W razie rozbieżności rozstrzyga wersja angielska. Linki w tekście prowadzą do materiałów w języku angielskim.

Ostatnia aktualizacja: 7 października 2026 r.

Zdalny onboarding: najpierw eID PRZEWODNIK AMLR



 Authologic

Zgodnie z projektem regulacyjnych standardów technicznych AMLA w sprawie należytej staranności wobec klienta (RTS CDD) firmy objęte przepisami AML w UE powinny przy zdalnej weryfikacji klientów, wszędzie tam, gdzie to możliwe, korzystać ze środków identyfikacji elektronicznej (eID) o poziomie zaufania „średnim” (substantial) lub „wysokim” (high), w tym z europejskiego portfela tożsamości cyfrowej (EUDI Wallet), albo z odpowiednich kwalifikowanych usług zaufania. Zdalna weryfikacja na podstawie dokumentu pozostaje dopuszczalna wyłącznie jako uzasadniony wyjątek.

Rozporządzenie AMLR (rozporządzenie (UE) 2024/1624) stosuje się od 10 lipca 2027 r., a RTS CDD będzie stosowany sześć miesięcy po wejściu w życie.

Ten przewodnik wyjaśnia, czego wymaga projekt, jak się przygotować i jak Authologic wspiera onboarding oparty przede wszystkim na eID.

Autorzy: Jarek Sygitowicz (współzałożyciel i Chief Strategy Officer) oraz Aleksander Wasiak (Compliance Officer), Authologic.

Najważniejsze wnioski

- 1 października 2026 r. AMLA zakończyła prace nad projektem RTS CDD na podstawie art. 28 ust. 1 AMLR i przekazała go Komisji Europejskiej. Komisja może jeszcze zmienić jego treść.
- AMLR stosuje się od 10 lipca 2027 r. RTS CDD będzie stosowany sześć miesięcy po wejściu w życie, a dokładna data jego stosowania nie jest jeszcze znana.
- Preferowanymi metodami zdalnej weryfikacji są eID o poziomie zaufania „średnim” lub „wysokim”, w tym portfel EUDI, oraz odpowiednie kwalifikowane usługi zaufania. eID kwalifikuje się niezależnie od tego, czy został notyfikowany na podstawie eIDAS.
- Zdalna weryfikacja na podstawie dokumentu jest dopuszczalna tylko wtedy, gdy nie można zasadnie oczekiwać, że klient przedstawi dokument tożsamości osobiście, i nie ma on dostępu do kwalifikującego się eID ani odpowiedniej kwalifikowanej usługi zaufania. Firma musi umieć uzasadnić każdy taki przypadek przed organem nadzoru.
- Przygotowanie już teraz oznacza zmapowanie obecnych procesów, sprawdzenie dostępności eID na każdym rynku i wybór sposobu połączenia z krajowymi eID i portfelami EUDI.
- Authologic łączy krajowe eID, portfele EUDI i weryfikację na podstawie dokumentu w jednym API i WebSDK. eID jest oferowany w pierwszej kolejności, a weryfikacja dokumentu jest rozwiązaniem awaryjnym, dzięki czemu podmioty obowiązane mogą przejść na onboarding oparty na eID bez budowania każdej integracji samodzielnie.

Co AMLA opublikowała 1 października 2026 r.?

1 października 2026 r. Urząd ds. Przeciwdziałania Praniu Pieniędzy i Finansowaniu Terroryzmu (AMLA) [zakończył prace nad kluczowymi regulacyjnymi standardami technicznymi \(RTS\)](#) dla sektora prywatnego i przekazał je Komisji Europejskiej. Z punktu widzenia onboardingu klientów najważniejszy jest projekt RTS w sprawie należytej staranności wobec klienta na podstawie art. 28 ust. 1 AMLR.

RTS CDD określa, jakie informacje o klientach muszą zbierać podmioty obowiązane i jakimi metodami mogą je weryfikować, także przy zdalnym onboardingu.

Kiedy RTS CDD zacznie obowiązywać?

RTS CDD jeszcze nie obowiązuje. Najpierw musi go przyjąć Komisja Europejska, która może zmienić jego treść. Po publikacji w Dzienniku Urzędowym UE RTS CDD wejdzie w życie i będzie stosowany sześć miesięcy później, dlatego dokładna data jego stosowania nie jest jeszcze znana. Samo AMLR stosuje się od 10 lipca 2027 r.

Data	Etap
9 lutego - 8 maja 2026 r.	Konsultacje publiczne projektu RTS CDD
1 października 2026 r.	AMLA publikuje ostateczny projekt RTS CDD i przekazuje go Komisji Europejskiej
24 grudnia 2026 r.	Państwa członkowskie muszą udostępnić portfele EUDI zgodnie z eIDAS 2.0
Data jeszcze nieznana	Komisja Europejska przyjmuje RTS CDD, ewentualnie ze zmianami, i publikuje go w Dzienniku Urzędowym UE
20 dni po publikacji	RTS CDD wchodzi w życie
10 lipca 2027 r.	Stosowanie AMLR
6 miesięcy po wejściu w życie	Stosowanie RTS CDD
24 grudnia 2027 r.	Prywatne strony ufające objęte zakresem eIDAS 2.0 muszą akceptować portfel EUDI tam, gdzie wymagane jest silne uwierzytelnienie użytkownika

Jakimi metodami firmy mogą weryfikować klientów zdalnie?

Zgodnie z projektem RTS CDD podmioty obowiązane powinny, wszędzie tam, gdzie to możliwe, weryfikować klientów zdalnie przy użyciu środków identyfikacji elektronicznej (eID) o poziomie zaufania „średnim” lub „wysokim”, w tym europejskiego portfela tożsamości cyfrowej (EUDI Wallet), albo odpowiednich kwalifikowanych usług zaufania w rozumieniu eIDAS.

eID kwalifikuje się niezależnie od tego, czy został notyfikowany na podstawie eIDAS, o ile spełnia wymagany poziom zaufania. Co w praktyce oznaczają poziomy „średni” i „wysoki”, wyjaśniamy w artykule [Assurance levels and signatures](#).

Kiedy dopuszczalna jest zdalna weryfikacja na podstawie dokumentu?

Zgodnie z art. 7 projektu RTS CDD zdalna weryfikacja na podstawie dokumentu jest „rozwiązaniem alternatywnym”. Podmiot obowiązany może z niej skorzystać tylko wtedy, gdy nie można zasadnie oczekiwać, że klient przedstawi dokument tożsamości osobiście, i nie ma on dostępu do kwalifikującego się eID ani odpowiedniej kwalifikowanej usługi zaufania. Preferencja klienta, który woli weryfikację dokumentem, nie jest jednym z tych warunków.

W każdym takim przypadku podmiot obowiązany musi umieć uzasadnić, dlaczego podstawowe metody weryfikacji nie były dostępne, i wykazać organowi nadzoru, że zastosowana metoda spełnia wymagane zabezpieczenia AML.

W praktyce najłatwiej spełnić ten wymóg, gdy proces onboardingu w każdym przypadku zapisuje, dlaczego podstawowe metody weryfikacji były niedostępne. Zespół compliance ma wtedy ślad audytowy na potrzeby kontroli nadzorczej.

Jak projekt zmienia dzisiejsze procesy onboardingu?

W wielu procesach zdalnego onboardingu punktem wyjścia jest dziś weryfikacja dokumentu. Zgodnie z projektem RTS CDD pierwszeństwo ma eID, a weryfikacja dokumentu staje się rozwiązaniem awaryjnym, które wymaga udokumentowanego uzasadnienia. Dla firm, które zbudowały onboarding wokół dokumentów, oznacza to przeprojektowanie samego procesu.

	Typowe podejście dziś	Zgodnie z projektem RTS CDD
Domyślna metoda zdalna	Weryfikacja dokumentu, np. zdjęcie dowodu i selfie	eID o poziomie zaufania „średnim” lub „wysokim”, w tym portfel EUDI, albo odpowiednie kwalifikowane usługi zaufania
Dopuszczalne eID	Zależne od przepisów krajowych	eID notyfikowane i nienotyfikowane o poziomie zaufania „średnim” lub „wysokim”
Weryfikacja dokumentu	Oferowana jako standardowa opcja	Tylko gdy nie można zasadnie oczekiwać, że klient przedstawi dokument tożsamości osobiście, i nie ma on dostępu do kwalifikującego się eID ani odpowiedniej kwalifikowanej usługi zaufania
Uzasadnienie	Brak ogólnounijnego wymogu uzasadniania wyboru metody	Firma musi uzasadnić, dlaczego podstawowe metody weryfikacji nie były dostępne, i wykazać organowi nadzoru, że zabezpieczenia są spełnione
Dane identyfikacyjne	Wymogi różnią się między krajami	Jedna lista dla całej UE, zgodna z modelem danych portfela EUDI

Jakie dane identyfikacyjne firmy muszą zbierać?

AMLR harmonizuje należyta staranność wobec klienta w całej UE. Projekt RTS CDD wprowadza jedną listę danych identyfikacyjnych, w tym adres, zbieranych w ten sam sposób we wszystkich państwach członkowskich. Lista jest zgodna z modelem danych stosowanym w portfelu EUDI. Co zawiera portfel, w tym dane identyfikacyjne osoby (PID), opisujemy w artykule [What is inside the wallet](#).

Jeśli eID nie zawiera wymaganego atrybutu, na przykład adresu, podmiot obowiązany musi uzyskać i zweryfikować go w inny sposób. Szerzej o należytej staranności wobec klienta w AMLR piszemy w artykule [How the EUDI Wallet changes KYC](#).

Dlaczego onboarding oparty na eID trudno wdrożyć w całej UE?

eID w Europie działa na poziomie krajowym. Każdy system ma własną integrację techniczną, format danych, poziom zaufania i stopień upowszechnienia. Zasięg krajowych aplikacji eID w poszczególnych państwach śledzimy w analizie [eID Adoption Race H1 2026](#).

Portfel EUDI dokłada kolejną warstwę. Zgodnie z eIDAS 2.0 państwa członkowskie muszą udostępnić portfele EUDI do 24 grudnia 2026 r., a od 24 grudnia 2027 r. prywatne strony ufające objęte zakresem rozporządzenia muszą akceptować portfel tam, gdzie wymagane jest silne uwierzytelnienie użytkownika. W 2027 r. będą więc pojawiać się kolejne portfele, a obowiązki z AMLR i eIDAS 2.0 zaczną obowiązywać równolegle.

Dla firmy, która obsługuje klientów na kilku rynkach UE, samodzielne zbudowanie takiego procesu oznacza dziesiątki osobnych integracji do stworzenia i utrzymania, dodawanie nowych portfeli w miarę ich uruchamiania oraz zgodne z przepisami rozwiązanie awaryjne oparte na dokumencie dla klientów bez eID. Ta praca konkuruje ze wszystkimi innymi zadaniami w planie rozwoju produktu, a skoro AMLR stosuje się od 10 lipca 2027 r., czasu na jej wykonanie jest niewiele.

Jak podmioty obowiązane powinny się przygotować?

Ostateczna treść RTS CDD może się jeszcze zmienić, ale większość prac przygotowawczych nie zależy od szczegółów.

Zmapuj obecny proces. Wskaż każde miejsce, w którym zdalny onboarding zaczyna się dziś od weryfikacji dokumentu. W tych miejscach trzeba będzie najpierw zaoferować eID.

Sprawdź dostępność eID na swoich rynkach. Dla każdego kraju, w którym działasz, spis dostępne eID, ich poziomy zaufania i to, jak powszechnie korzystają z nich klienci. Zobaczysz, gdzie eID może realnie stać się metodą domyślną, a gdzie na rozwiązanie awaryjne przypadnie więcej weryfikacji.

Określ, jak uzasadnisz każde użycie rozwiązania awaryjnego. Zdecyduj, co będziesz zapisywać, gdy klient zostanie zweryfikowany dokumentem zamiast kwalifikującym się eID lub odpowiednią kwalifikowaną usługą zaufania, aby móc wykazać organowi nadzoru, dlaczego podstawowe metody weryfikacji nie były dostępne.

Zaplanuj obsługę portfela EUDI. Portfele będą uruchamiane w różnym czasie w różnych państwach członkowskich. Twój proces powinien umożliwiać ich dodawanie bez nowego projektu integracyjnego za każdym razem. Przepływy z portfelem można bezpłatnie przetestować w przeglądarce w [EUDI & Wallet Playground](#) od Authologic.

Zdecyduj, jak połączysz się z systemami eID. Wybór między samodzielnym budowaniem i utrzymywaniem każdej integracji krajowej a skorzystaniem z jednego dostawcy, który już

je łączy, ma największy wpływ na koszt i harmonogram. Authologic zapewnia takie połączenie w ramach jednej integracji, opisanej poniżej.

Swoją gotowość pod kątem AMLR i eIDAS 2.0 możesz sprawdzić w [SCA & AMLR Readiness Checklist](#).

Którzy dostawcy wspierają onboarding oparty na eID zgodnie z AMLR?

[Authologic](#) to dostawca infrastruktury zaufania dla firm regulowanych, który wspiera onboarding oparty na eID zgodnie z AMLR. Łączy krajowe eID, portfel EUDI i weryfikację na podstawie dokumentu w jednym API i WebSDK, dzięki czemu podmioty obowiązane nie muszą samodzielnie budować i utrzymywać dziesiątek osobnych połączeń.

W procesie Authologic klient najpierw otrzymuje najsilniejszą dostępną dla niego metodę weryfikacji, a weryfikacja dokumentu działa jako rozwiązanie awaryjne w tym samym procesie dla klientów bez dostępu do kwalifikującego się eID. Wymagane dane identyfikacyjne są zbierane w ramach jednego procesu. Weryfikacja przez eID opiera się na dowodzie kryptograficznym pochodzącym od wydawcy, a nie na zdjęciach dokumentów, i z Authologic kosztuje nawet 25 razy mniej niż weryfikacja dokumentu.

Authologic zapewnia dostęp do ponad 100 metod identyfikacji w ponad 230 krajach i terytoriach i korzysta z niego ponad 100 klientów z sektorów regulowanych. Jest też [jednym z pierwszych w Europie zarejestrowanych dostawców poświadczeń dla europejskich portfeli tożsamości cyfrowej](#). Porównanie platform do weryfikacji AML i KYC znajdziesz w artykule [Best AML and KYC identity verification platforms](#).

Odpowiedzialność za zgodność z przepisami pozostaje po stronie podmiotu obowiązanego, a Authologic zapewnia infrastrukturę weryfikacji, która umożliwia onboarding oparty na eID na wielu rynkach.

FAQ | Najczęściej zadawane pytania

Czy RTS CDD już obowiązuje?

Nie. AMLA przekazała ostateczny projekt Komisji Europejskiej, która musi go jeszcze przyjąć i może zmienić jego treść. RTS CDD będzie stosowany sześć miesięcy po wejściu w życie. AMLR stosuje się od 10 lipca 2027 r.

Czy firmy nadal mogą stosować zdalną weryfikację na podstawie dokumentu?

Tak, jako „rozwiązanie alternatywne” na podstawie art. 7 projektu RTS CDD. Jest ona dopuszczalna tylko wtedy, gdy nie można zasadnie oczekiwać, że klient przedstawi dokument tożsamości osobiście, i nie ma on dostępu do kwalifikującego się eID ani odpowiedniej kwalifikowanej usługi zaufania, a firma musi umieć uzasadnić każdy taki przypadek przed organem nadzoru.

Czy eID musi być notyfikowany na podstawie eIDAS?

Nie. Zgodnie z projektem RTS CDD eID kwalifikuje się niezależnie od tego, czy został notyfikowany na podstawie eIDAS, o ile spełnia poziom zaufania „średni” lub „wysoki”.

Który dostawca wspiera onboarding oparty na eID zgodnie z AMLR?

Authologic łączy krajowe eID, portfel EUDI i weryfikację na podstawie dokumentu w jednym API i WebSDK. Klient najpierw otrzymuje eID, a weryfikacja dokumentu działa jako rozwiązanie awaryjne w tym samym procesie. Authologic zapewnia dostęp do ponad 100 metod identyfikacji w ponad 230 krajach i terytoriach i korzysta z niego ponad 100 klientów z sektorów regulowanych.

Czy firmy mogą korzystać z portfela EUDI przy należytej staranności wobec klienta?

Tak. Projekt RTS CDD wymienia portfel EUDI wśród środków identyfikacji elektronicznej, z których mogą korzystać firmy, o ile spełnia on wymagany poziom zaufania. Atrybuty, których portfel nie zawiera, trzeba nadal uzyskać i zweryfikować w inny sposób. Odrębny obowiązek akceptowania portfela na podstawie eIDAS 2.0 opisujemy w artykule [How eIDAS 2.0 affects private relying parties and SCA](#).

Umów 30-minutowy przegląd gotowości do AMLR

Sprawdź, na jakim etapie jest Twój onboarding, zanim zaczniesz obowiązywać AMLR. Podczas 30-minutowego przeglądu gotowości do AMLR zespół Authologic przejdzie z Tobą przez obecny proces zdalnego onboarding, wskaże, co trzeba w nim zmienić zgodnie z projektem RTS CDD, i sprawdzi, które eID i portfele EUDI możesz zaoferować na swoich rynkach.

[Umów przegląd gotowości do AMLR](#) lub napisz na contact@authologic.com.

Onboarding gotowy na AMLR?

Sprawdź w 30 minut



Historia zmian

- 7 października 2026 r. - Pierwsza publikacja.

Artykuł zawiera ogólne informacje o projekcie RTS CDD opublikowanym przez AMLA 1 października 2026 r. Nie stanowi porady prawnej. Ostateczna treść może się zmienić po przyjęciu przez Komisję Europejską.