WYDAWCA RAPORTU:

OBSERWATORIUM.BIZ

ZŁOTY PARTNER:

asseco DATA SYSTEMS

Trusted Economy Forum

Raport

ZDALNE POTWIERDZANIE TOŻSAMOŚCI, E-PODPIS I E-PIECZĘĆ W BIZNESOWEJ PRAKTYCE

SREBRNY PARTNER:

Namirial Procivis AN ORELL FÜSSLI COMPANY Authologic Poczta Polska aruba.it

BRĄZOWY PARTNER:

KIR SIGNIUS TRUST LYNX billon IDENTT

ZDALNE POTWIERDZANIE TOŻSAMOŚCI, E-PODPIS I E-PIECZĘĆ

Czym jest i na jakie biznesowe potrzeby odpowiada zdalne potwierdzanie tożsamości?

- Pozwala na pozyskanie klientów indywidualnych i biznesowych w formule on-line w sposób bezpieczny, bez potrzeby fizycznego kontaktu.
- Na rynku polskim najczęściej stosuje się takie metody jak Profil Zaufany, Profil Osobisty, aplikację mObywatel, wideoweryfikację, technologie biometryczne czy usługę mojeID.
- Główne sektory wdrażające tę technologie to finanse, ubezpieczenia, telekomunikacja oraz administracja publiczna.
- Nadchodzący Europejski Portfel Tożsamości Cyfrowej umożliwi przechowywanie danych tożsamości i atrybutów oraz ich bezpieczne udostępnianie, a także szerokie zastosowanie tej metody zdalnego potwierdzania tożsamości w praktyce biznesowej.

Co zapewniają kwalifikowane podpisy elektroniczne?

- Stanowią prawnie wiążącą formę podpisu równoważną podpisowi własnoręcznemu.
- Kluczowe zastosowania obejmują podpisywanie umów, dokumentacji finansowej i kontraktów biznesowych, z uwzględnieniem wymogów transgranicznych.
- Akceptację polskich oraz europejskich usług kwalifikowanych dostawców, działających w ramach regulacji eIDAS.
- Na znaczeniu zyskują rozwiązania chmurowe, umożliwiające wydawanie certyfikatówi składanie podpisów w sposób zdalny, przy jednoczesnej ich integracji z procesami biznesowymi.

Co zapewniają kwalifikowane pieczęci elektroniczne?

- Kwalifikowana pieczęć elektroniczna, zgodnie z rozporządzeniem eIDAS, potwierdza autentyczność i integralność dokumentów elektronicznych.
- e-Pieczęć jest szeroko wykorzystywana w sektorze publicznym i prywatnym, umożliwiając instytucjom i firmom zabezpieczanie dokumentów w sposób wiążący prawnie.
- Usługa ta wspiera automatyzację procesów, takich jak zawieranie umów czy wystawianie faktur, przyspiesza obieg dokumentów w formie cyfrowej, eliminując konieczność stosowania fizycznych pieczęci oraz redukując koszty operacyjne.

Spis treści

Cel i zakres raportu 4

1. Zdalne potwierdzanie tożsamości klientów w procesach cyfrowych 4

1.1 Metody zdalnego potwierdzania tożsamości klientów 5

1.2 Regulacje prawne związane z procesami potwierdzania tożsamości 7

1.3 Przykłady wykorzystania zdalnego potwierdzania tożsamości w biznesie 10

1.4 Wpływ eIDAS 2.0 i portfela cyfrowej tożsamości na przyszłość rynku potwierdzania tożsamości 12

1.5 Zestawienie dostawców usług zdalnego potwierdzania tożsamości / on-boardingu 15

2. Kwalifikowane podpisy elektroniczne 19

2.1 Kwalifikowane podpis elektroniczny jako narzędzie zdalnego oświadczenia woli w procesach biznesowych 19

2.2 Regulacje prawne związane z podpisami elektronicznymi 22

2.3 Przykłady wykorzystania kwalifikowanego podpisu elektronicznego w biznesie 23

2.4 Kwalifikowany podpis elektroniczny na tle innych rodzajów podpisów na polskim rynku oraz w perspektywie wdrożenia eIDAS 2.0 27

2.5 Zestawienie dostawców i usług podpisu elektronicznego 29

3. Kwalifikowane pieczęci elektroniczne 36

3.1 Kwalifikowane pieczęci elektroniczne jako narzędzia dla podmiotów prawnych w procesach biznesowych 36

3.2 Wykorzystanie pieczęci elektronicznej w poszczególnych sektorach 38

3.3 Zestawienie dostawców pieczęci elektronicznych 43

Cel i zakres raportu

Celem niniejszego raportu jest dostarczenie wiedzy na temat dostępnych na rynku polskim metod zdalnej weryfikacji tożsamości, kwalifikowanych podpisów elektronicznych oraz kwalifikowanej pieczęci elektronicznej z naciskiem na ich wykorzystanie biznesowe. Zakres raportu obejmuje przegląd kluczowych narzędzi i rozwiązań, ich podstaw prawnych oraz rekomendacje w zakresie stosowania. Opracowany materiał zawiera informacje przydatne dla przedsiębiorców i organizacji wdrażających procesy cyfrowe. Dodatkowo raport został poszerzony o przykłady wykorzystania tych usług w poszczególnych sektorach (use-cases).

1.Zdalne potwierdzanie tożsamości klientów w procesach cyfrowych

Możliwość pozyskania klientów w formule zdalnej stało się już rynkowym obowiązkiem dla podmiotów z wszelkich branż i zakresów działalności gospodarczej. Cyfryzacja kolejnych procesów dnia codziennego pozwala użytkownikom, konsumentom, obywatelom załatwiać coraz więcej spraw drogą elektroniczną. Jednocześnie firmy mogą oszczędzać na ograniczaniu kosztów budowy i utrzymania sieci punktów obsługi klienta oraz rezygnować z metod wymagających przekazania dokumentów papierowych np. z wykorzystaniem kuriera. Nowe pokolenia wręcz preferują możliwość zdalnego kontaktu i „on-boardingu" przez aplikację mobilną czy internetową, uznając wizytę w oddziale, czy kontakt telefoniczny za mniej preferowany.

W **procesie zdalnego pozyskania klienta**, gdy brakuje spotkania fizycznego i okazania oraz weryfikacji dokumentu tożsamości w sposób klasyczny, kluczowe dla obu stron transakcji jest, aby tożsamość składającego była rozpoznana w sposób właściwy, bezpieczny i ergonomiczny. Ważne jest również, aby strona polegająca na przedstawianych danych zyskała możliwie najwyższą pewność, że dotyczą one właściwej osoby.

Potwierdzenie (weryfikacja) tożsamości ma kluczowe znaczenie dla zaufania do wszystkich usług cyfrowych, które wymagają identyfikacji osoby fizycznej lub prawnej. Jest to proces, za pomocą którego dostawca usług **gromadzi i weryfikuje** informacje o wnioskodawcy oraz sprawdza, czy zebrane i zatwierdzone informacje faktycznie należą do wnioskodawcy, który ich używa pod swoją kontrolą.

1.1. Metody zdalnego potwierdzania tożsamości klientów

Poniżej omówiono dostępne i najczęściej stosowne metody potwierdzenia tożsamości w formule zdalnej. Głównymi czynnikami wpływającymi na wybór metody są:

- wymagania prawne usługi i sposobu weryfikacji klientów np. związane z przepisami przeciwdziałania praniu pieniędzy;
- wymagania środowiska użytkownika korzystającego z usługi np. aplikacja mobilna, strona www, dostępność kamery lub czytników;
- wymagania przebiegu procesu w tym także czasu jego trwania;
- wymagania dotyczące bezpieczeństwa w tym także ryzyk i możliwych strat w przypadku błędnego potwierdzenia tożsamości.

Metody zdalnego potwierdzania tożsamości zostały z powodzeniem wdrożone w wielu branżach, natomiast szczególnie powszechnie znajdują zastosowania w usługach finansowych – bankowości, ubezpieczeniach, usługach pożyczkowych czy inwestycyjnych. Potwierdzenie tożsamości jest także z powodzeniem stosowanie w grach losowych, telekomunikacji i mediach (tj. prąd, gaz) oraz we wszystkich usługach publicznych dostępnych drogą elektroniczną.

Dostępnymi **rozwiązaniami zdalnego potwierdzania tożsamości** są:

1) Środki identyfikacji dostarczane przez państwo, które stanowi jedną z kluczowych metod umożliwiających bezpieczny dostęp do usług publicznych i prywatnych. W Polsce narzędziem spełniającym to kryterium są:

a. Profil Zaufany – notyfikowany w UE na poziomie wiarygodności średnim, dostępny tylko na potrzeby usług publicznych – oparty o login, hasło i kod SMS lub systemy bankowości elektronicznej;

b. Profil Osobisty – notyfikowany w UE na poziomie wiarygodności wysokim – oparty o dowód osobisty i numer PIN – dostępny dla usług publicznych i prywatnych;

c. Profil mObywatel – krajowy środek identyfikacji na poziomie wiarygodności średnim – oparty o aplikację mObywatel – dostępny dla usług publicznych i prywatnych.

2) Środki identyfikacji dostarczane przez podmioty komercyjne – na polskim rynku działające jako rozwiązanie mojeID dostarczane przez Krajową Izbę Rozliczeniową i bazujące na tożsamości klienta bankowości elektronicznej. Banki posiadają rozbudowane systemy weryfikacji swoich klientów spełniające wymagania przepisów o przeciwdziałaniu praniu pieniędzy, przechodzą dodatkowe audyty zgodności procesów zarządzania

środkami elektronicznymi. Bankowe środki identyfikacji elektronicznej mogą być używane zarówno na potrzeby podmiotów publicznych za pomocą węzła login.gov.pl oraz usług prywatnych za pomocą usługi mojeID.

3) Wideorozmowa z operatorem – pozwala na powielenie procesu potwierdzenia tożsamości realizowanego fizycznie polegającego na okazaniu dokumentu tożsamości do kamery oraz potwierdzeniu ich zgodności oraz posługiwania się dokumentem przez właściciela. Cały proces weryfikacji tożsamości jest prowadzony i nadzorowany przez operatora, który potwierdza weryfikację dokumentu tożsamości jak i posługiwanie się dokumentem przez właściciela. Metoda jest także wspierana automatycznym pobieraniem danych z dokumentu (OCR), informowania operatora o niezgodnościach z wzorcem dokumentu oraz wsparciem weryfikacji biometrycznej zgodności zdjęcia i osoby identyfikowanej.

4) Wykorzystanie dedykowanej aplikacji mobilnej i automatyczna weryfikacja umożliwia użytkownikom przeprowadzanie procesu weryfikacji w sposób automatyczny w oparciu o udostępnione użytkownikowi narzędzia. Aplikacje mobilne do zdalnej weryfikacji wykorzystują sztuczną inteligencję (AI) do analizy dokumentów, rozpoznawania twarzy i porównania danych z dokumentu z osobą go prezentującą. Algorytmy AI są w stanie automatycznie sprawdzać autentyczność dokumentów, analizując ich cechy, takie jak hologramy, struktura dokumentu, znaki wodne, a także przeprowadzać detekcję „liveness" (żywotności) twarzy, aby upewnić się, że użytkownik jest rzeczywiście obecny i nie korzysta z nagrania lub zdjęcia.

5) Dowód osobisty z warstwą elektroniczną oraz potwierdzenie biometryczne – stanowi rozszerzenie metod automatycznej weryfikacji tożsamości omówione powyżej, w ramach metody dane dokumentu tożsamości są pobierane bezpośredni za pomocą anteny zawartej w telefonie komórkowym (NFC) z dowodu osobistego lub paszportu. Pozwala to jednoznacznie potwierdzić posługiwanie się autentycznym dokumentem przez weryfikowanego.

6) Udostępnienie danych z aplikacji mObywatel – aplikacja mObywatel umożliwia poza korzystaniem z profilu mObywatel także udostępnienie w procesach lokalnych i zdalnych danych z przechowywanych mobilnych dokumentów, które nie tylko zawierają dane identyfikujące, ale mogą zawierać zdjęcie posiadacza, uprawnienia, informacje o adresie.

7) Kwalifikowany podpis elektroniczny - oparty o kwalifikowany certyfikat, który identyfikuje osobę składającą podpis elektroniczny w sposób jednoznaczny i wiarygodny. Wykorzystanie podpisu elektronicznego w procesach rejestracji klienta dostarcza dane identyfikujące osoby składającej podpisany wniosek lub podpisującej umowę oraz dokumentuje w sposób niezaprzeczalny dowody związane z realizowaną transakcją. Warto zaznaczyć, że oma-

wiany w dalszej części raportu Europejski Portfel Tożsamości Cyfrowej umożliwi składanie kwalifikowanego podpisu elektronicznego przez wszystkich posiadaczy takiego portfela.

Na polskim rynku funkcjonują już **integratorzy**, którzy starają się dostarczyć odbiorcom – firmom budującym procesy on-boardingowe dla swoich klientów z różnych sektorów – od bankowego, pożyczkowego, ubezpieczeniowego przez dostawców usług telekomunikacyjnych, energetycznych, aż po serwisy bukmacherskie czy loteryjne. Tacy integratorzy, czy inaczej „eID huby" dostarczają oprócz wspomnianych wyżej metod również narzędzia pomocnicze uzupełniające proces zdalnego on-boardingu, bazujące na przykład na potwierdzaniu wybranych danych dotyczących konta bankowego klienta (usługa AIS), czy innych niezbędnych dla realizacji procesów Know Your Customer (KYC). Przykładem takiej firmy jest Authologic, „która oprócz integrowania rozwiązań lokalnych w Polsce, aktywnie działa międzynarodowo.

Poza wymienionymi powyżej należy wskazać nowy środek identyfikacji elektronicznej, który zacznie być powszechnie używany w roku 2026 – **Europejski Portfel Cyfrowej Tożsamości,** rozwiązanie to umożliwi prawdopodobnie już w roku 2026 udostępnianie danych identyfikujących na poziomie wiarygodności wysokim. Poza udostępnieniem podstawowych danych o tożsamości portfel będzie umożliwiał przechowywanie i udostępnianie elektronicznych potwierdzeń atrybutów, takich jak pełnomocnictwa, uprawnienia, zaświadczenia. W tym zakresie realizacja potwierdzenia tożsamości za pomocą portfela umożliwi zarówno wiarygodne przekazanie wszystkich danych identyfikujących jak i udostępnienie danych dodatkowych, które mogą pochodzić z różnych wiarygodnych źródeł.

1.2. Regulacje prawne związane z procesami potwierdzania tożsamości

Warunki realizacji potwierdzania tożsamości są determinowane przez wiele regulacji na poziomie unijnym oraz prawem krajowym, poniżej określono najczęściej stosowanych regulacji prawnych w zakresie potwierdzania tożsamości.

- **Przepisy dotyczące postępowania administracyjnego i informatyzacji podmiotów realizujących zadania publiczne** – wymagają identyfikacji osób składających podania i korzystających z usług publicznych. Wszystkie podmioty publiczne realizując usługi elektroniczne korzystają z krajowego systemu identyfikacji elektronicznej (login.gov.pl) i udostępnianych tam środków identyfikacji tj. : Profilu Zaufanego, Profilu Osobistego, Profilu mObywatel oraz bankowych środków identyfikacji elektronicznej podłączonych do węzła krajowego.

- **Ustawa o doręczeniach elektronicznych** – wymaga identyfikacji zarówno nadawcy jak i adresata korespondencji rejestrowanej – elektronicznego listu poleconego. W zakresie doręczeń elektronicznych usługi operatora wyznaczonego oparte są o środki identyfikacji elektronicznej udostępniane w ramach login.gov.pl. Kwalifikowani dostawcy usług zaufania stosują różne metody potwierdzenia tożsamości w celu rejestracji w usłudze doręczeń elektronicznych.

- **Przepisy przeciwdziałaniu praniu pieniędzy** – nakładają na podmioty sektora finansowego – w szczególności na banki i ubezpieczycieli wymagania potwierdzenia tożsamości osób zakładających konta, korzystających z instrumentów płatniczych czy ubezpieczeń na życie. W Polsce szczególne wymagania w zakresie zdalnego potwierdzania tożsamości w rejestrowaniu do usług finansowych zostały określone przez Głównego Inspektora Informacji Finansowej, a także przez Urząd Komisji Nadzoru Finansowego. Instytucje finansowe z powodzeniem stosują zdalne i automatyczne sposoby potwierdzania tożsamości użytkowników rozpoczynających korzystanie z usług usługach finansowych.

- **Przepisy prawa telekomunikacyjnego** – wymagają rejestracji klientów usług telekomunikacyjnych oraz potwierdzenia ich tożsamości przed udostępnieniem. Operatorzy telekomunikacyjni mogą polegać na krajowych i notyfikowanych środkach identyfikacji elektronicznej, korzystać z metod zdalnego potwierdzania tożsamości, a także z usług zaufania w szczególności z podpisu elektronicznego.

- **Przepisy rozporządzania eIDAS** – wymagają potwierdzenia tożsamości osób którym wydawane są kwalifikowane certyfikaty podpis oraz pieczęci elektronicznej, kwalifikowane usługi rejestrowanego doręczenia elektronicznego. Potwierdzenie tożsamości wymagane dla realizacji kwalifikowanych usług zaufania podlega szczególnym warunkom jakościowym, musi być realizowane zgodnie z europejskimi normami i okresowo audytowane. W przypadku stosowania środków identyfikacji elektronicznej przepisy wymagają zastosowania notyfikowanych środków identyfikacji na wysokim poziomie bezpieczeństwa i wiarygodności.

WYPOWIEDŹ EKSPERTA

Michał Tabor
Członek Zarządu i Partner, Obserwatorium.biz

Co ze zdalną identyfikacją firm?

Efektywna identyfikacja elektroniczna podmiotów gospodarczych stanowi klucz do sprawnego prowadzenia ich działalności oraz realizacji transakcji. Proces identyfikacji firm obejmuje również ustalanie tożsamości osób działających w ich imieniu. Osoby te, posiadające odpowiednie pełnomocnictwa, składają oświadczenia woli, co wymaga ich weryfikacji. Pełnomocnictwa, często występujące w postaci dokumentów wymagających interpretacji, uniemożliwiają automatyczne przetwarzanie, co spowalnia procesy prawne i administracyjne.

Aktualnie brakuje efektywnych i biznesowo sprawdzonych rozwiązań w tym zakresie. Wprowadzenie elektronicznych potwierdzeń atrybutów w ramach Europejskiego Portfela Cyfrowej Tożsamości ma szansę wyeliminować te ograniczenia. Rozwiązanie to zapewni jednolitą formę i interpretację pełnomocnictw, co umożliwi automatyczne przetwarzanie danych. Identyfikacja osób działających w imieniu podmiotów gospodarczych ma szansę zostać uproszczona, a procesy prawne zyskują na efektywności i spójności. Jednolity format elektronicznych potwierdzeń atrybutów przyspieszy weryfikację pełnomocnictw, zwiększy bezpieczeństwo prawne i zmniejszy ryzyko błędów wynikających z interpretacji dokumentów.

Dopełnieniem potrzeb biznesowych identyfikacji firm będzie Europejski Portfel Cyfrowej Tożsamości dla osób prawnych umożliwiający automatyczne interakcje pomiędzy podmiotami na podstawie wcześniej ustalonych reguł. Rozwiązanie to, oparte na technologii chmurowej, pozwoli na automatyczne przekazywanie danych i atrybutów podmiotu prawnego, bez interakcji z osobą fizyczną. Portfel firmowy w połączeniu z pieczęcią elektroniczną będzie mógł umożliwić składanie oświadczeń woli w imieniu podmiotów prawnych, co zautomatyzuje procesy biznesowe.

1.3 Przykłady wykorzystania zdalnego potwierdzania tożsamości w biznesie

ZAUTOMATYZOWANY PROCES POTWIERDZANIA TOŻSAMOŚCI BAZUJACY NA APLIKACJI PRZY OTWIERANIU KONTA.

Procesy takie zwane „kontem na selfie" dostępne są w wielu bankach – np. w Banku Credit Agricole Polska czy ING Banku Śląskim. W Nest Banku proces obejmujący wykonywanie zdjęć dokumentów, z opcją rozmowy wideo z konsultantem został wdrożony przez IDENTT.

ZAUTOMATYZOWANY PROCES POTWIERDZANIA TOŻSAMOŚCI OPARTY NA PROFILU mOBYWATEL

Santander Bank Polska poinformował w 2024, że umożliwił proces otwarcia konta osobistego w formule zdalnej z użyciem aplikacji mObywatel. Zgodnie z eIDAS 2.0 w przeciągu najbliższych lat Europejski Portfel Cyfrowej Tożsamości, będzie obowiązkowym narzędziem do zdalnego potwierdzanie tożsamości i uwierzytelniania w procesach bankowych.

ZDALNA OBSŁUGA PRODUKTÓW UBEZPIECZENIOWYCH

Usługa mojeID KIR umożliwia założenie konta na portalach ubezpieczeniowych służących do zakupu i obsługi produktów ubezpieczeniowych. Wiodącym przykładem w tym zakresie jest portal mojePZU.

WERYFIKACJA TOŻSAMOŚCI NA RYNKU BNPL.

Dynamicznie rozwijający się rynek usług Kup Teraz, Zapłać Później (BNPL) korzysta z procesów usprawniających weryfikację tożsamości, co pozwala na wydanie zautomatyzowanej decyzji kredytowej przy zmniejszeniu ryzyka oszustw. Przykładem wdrożenie jest tu PayPO współpracujący w tym zakresie z usługą dostarczaną przez IDENTT.

UMOWA NA GAZ W PEŁNI ON-LINE Z UŻYCIEM RÓŻNYCH METOD

Proces zawierania umowy na dostawę gazu w eBOK PGNiG odbywa się w 100% zdalnie, a potwierdzić swoją tożsamość możemy dzięki jednej z dostępnych metod takich jak mObywatel, mojeID czy e-Dowód / eDO App.

POTWIERDZANIE TOŻSAMOŚCI I WIEKU NA PLATFORMACH BUKMACHERSKICH

Sektor bukmacherski ze względu na restrykcyjne prawodawstwo wymaga budowy procesów onboardingowych z naciskiem na weryfikację pełnoletności. Przykładem implementacji jest tu wdrożenie narzędzi Authologc w serisach LV Bet.

/PRZYKŁAD Z ZAGRANICY/ NOWE UMOWY TELEKOMUNIKACYJNE Z UŻYCIEM KART eID

Większość dostawców usług telekomunikacyjnych i użyteczności publicznej w krajach bałtyckich obsługuje krajowe karty eID do identyfikacji użytkowników oraz podpisywania nowych umów telekomunikacyjnych.

POTWIERDZANIE TOŻSAMOŚCI I WIEKU NA PLATFORMIE LOTTO

Wdrożenie usługi mojeID KIR w LOTTO umożliwiło sprzedaż tej znanej usługi w formule online

USE-CASE PARTNERA

Jan Szajda
CEO i współzałożyciel IDENTT

Współpraca IDENTT z Bankiem PEKAO S.A. wprowadziła nowoczesne rozwiązanie KYC, które usprawnia i zabezpiecza proces otwierania kont. System obsługuje wiele metod weryfikacji, w tym fotografię dokumentów, warstwę elektroniczną dowodu osobistego oraz integrację z mObywatel. W 2023 roku 40% wszystkich nowych kont w Banku PEKAO zostało otwartych z wykorzystaniem technologii IDENTT, co znacząco obniżyło koszty pozyskania klientów, jednocześnie minimalizując ryzyko oszustw tożsamościowych. Zaawansowana analiza biometryczna umożliwia wczesne wykrywanie prób oszustw, zwiększając ogólny poziom bezpieczeństwa. Przyjazne dla użytkownika rozwiązanie oferuje klientom możliwość wyboru preferowanej metody weryfikacji, co sprawia, że proces jest zarówno efektywny, jak i bezpieczny.

1.4. Wpływ eIDAS 2.0 i portfela cyfrowej tożsamości na przyszłość rynku potwierdzania tożsamości

Rozporządzenie eIDAS, w 2014 roku ustanowiło jednolity standard dla elektronicznej identyfikacji i usług zaufania w UE, zapewniając wzajemne uznawanie notyfikowanych systemów identyfikacji i umożliwiając obywatelom i firmom korzystanie z usług publicznych i prywatnych online na terenie całej Unii.

Nowelizacja rozporządzenie eIDAS, która weszła w życie w maju 2024, stanowi kluczowy element strategii Unii Europejskiej wdrożenia **Europejskich Ram Tożsamości Cyfrowej** mającej na celu zapewnienie harmonizacji zasad i warunków stosowania usług zaufania w państwach członkowskich, co umożliwi interoperacyjność pomiędzy krajowymi systemami identyfikacji elektronicznej (eID) oraz usługami zaufania. Ma to na celu ułatwienie realizacji transgranicznych transakcji cyfrowych zarówno w sektorze publicznym, jak i prywatnym, poprzez udostepnienie narzędzi i zwiększenie ich interoperacyjności.

Nowelizacja stawia na zaangażowania sektora prywatnego w większym stopniu w rozwój i wykorzystanie usług zaufania, co przyczyni się do przyspieszenia adopcji cyfrowych tożsamości i usług zaufania. Głównym elementem wdrożenia Europejskich Ram Tożsamości Cyfrowej, będzie wdrożenie **Europejskiego Portfela Tożsamości Cyfrowej** (ang. **European Digital Identity Wallet** w skrócie **EUDIW**).

Europejski portfel cyfrowej tożsamości to środek, który umożliwi jego użytkownikowi:

- przechowywanie i udostępnianie danych dotyczących jego tożsamości;
- uwierzytelnienie do usług publicznych i prywatnych online i offline;
- zbieranie atrybutów związanych z jego tożsamością i udostępnianie ich stronom ufającym na żądanie;
- a także składanie kwalifikowanych podpisów i pieczęci elektronicznych.

Portfel stanowić będzie narzędzie umożliwiające użytkownikom zarządzanie swoją tożsamością cyfrową i jej wykorzystanie w różnego rodzaju transakcjach, w tym także transakcjach biznesowych. Podstawową implementacją portfela będzie aplikacja mobilna na telefon komórkowy, która umożliwi obywatelom przechowywanie i udostępnianie cyfrowych wersji dokumentów tożsamości oraz innych danych, takich jak prawo jazdy, dyplomy edukacyjne, dane medyczne, poświadczenia bankowe, polisy ubezpieczeniowe. Potwierdzenia udostępniane przez portfel mogą być wykorzystywane do zdalnego potwierdzania tożsamości oraz potwierdzenia uprawnień.

Europejskie portfele będą obsługiwać różne rodzaje dokumentów identyfikacyjnych, co umożliwi użytkownikom korzystanie z różnych form identyfikacji w jednym, spójnym rozwiązaniu cyfrowej tożsamości. **Użytkownikami tych portfeli będą osoby fizyczne, osoby prawne** oraz **osoby fizyczne reprezentujące osoby fizyczne** lub **osoby prawne.**

Każde państwo członkowskie musi udostępnić i notyfikować co najmniej jeden portfel tożsamości cyfrowej w terminie 24 miesięcy od dnia wejścia w życie aktów wykonawczych, tj. do końca 2026 roku. **Każdy taki portfel będzie musiał być uznawany przez każde inne państwo członkowskie.** Europejski portfel będzie wydawany przez każdy kraj członkowski Unii Europejskiej w oparciu o zbudowane przez siebie rozwiązanie, ale oparty będzie na wspólnym standardzie cyfrowej tożsamości, który będzie akceptowany we wszystkich krajach członkowskich UE. Dzięki temu użytkownicy będą mieli możliwość korzystania z jednego, wspólnego rozwiązania cyfrowej tożsamości na terenie całej Unii Europejskiej.

Europejskie portfele tożsamości będą podlegać certyfikacji m.in. pod kątem spełniania wymogów w odniesieniu do wysokiego poziomu bezpieczeństwa. Ponadto portfel

będzie zgodny z ogólnym rozporządzeniem o ochronie danych (RODO), a państwa członkowskie zobowiązane są do określenia środków technicznych i organizacyjnych w celu zapewnienia wysokiego poziomu ochrony danych osobowych.

Rozporządzenie do końca 2027 roku **wymaga rozpoznawania i akceptacji portfela cyfrowej tożsamości** przez wszystkie podmioty zobowiązane na podstawie prawa Unii, prawa krajowego lub umowy do stosowania silnego uwierzytelnienia. Ponadto **wszystkie duże platformy internetowe będą zobowiązane do wprowadzenia możliwości logowania za pośrednictwem portfeli.**

OPINIA PARTNERA:

Kai Wagner

Head of Products & Partners Procivis AG

Wprowadzenie europejskiego portfela tożsamości cyfrowej (EUDI) w ramach eIDAS 2.0 jest przełomowym krokiem w kierunku stworzenia ujednoliconego ekosystemu tożsamości cyfrowej w całej Europie. Ma on wzmocnić pozycję przedsiębiorstw i obywateli, umożliwiając płynny dostęp do usług zaufania i wspierając bezprecedensowe przypadki użycia tożsamości.

Portfel EUDI oferuje znaczące możliwości zarówno dla sektora publicznego, jak i prywatnego. Jednym z jego najbardziej transformacyjnych aspektów jest możliwość wydawania i korzystania z interoperacyjnych poświadczeń, takich jak dokumenty tożsamości, kwalifikacje, licencje lub zezwolenia na prowadzenie działalności gospodarczej, które są uznawane we wszystkich państwach członkowskich UE. Eliminuje to istniejące obciążenia administracyjne i otwiera drzwi do płynniejszych, bardziej wydajnych operacji w sektorach takich jak usługi finansowe, opieka zdrowotna, hotelarstwo, rozrywka, logistyka czy edukacja.

Interoperacyjność portfela zapewnia, że firmy, które przyjmują te nowe rozwiązania, mogą płynnie pracować ponad granicami krajowymi, umożliwiając bezpieczną i skuteczną weryfikację tożsamości i uwierzytelnianie bez blokowania wen-trznego. Elastyczność portfela EUDI pozwala na jego integrację z istniejącymi platformami i przepływami pracy przy minimalnych zakłóceniach.

Wykorzystując otwarte standardy i wspierając podejście neutralne wobec dostawców, eIDAS 2.0 zapewnia, że firmy mogą zabezpieczyć swoje strategie tożsamości cyfrowej na przyszłość.

Ostatecznie eIDAS 2.0 i portfel EUDI są gotowe do przedefiniowania zaufania i tożsamości w Europie. Umożliwiają one firmom budowanie większej wydajności operacyjnej przy jednoczesnym zwiększaniu zaufania i satysfakcji klientów.

1.5. Zestawienie dostawców usług zdalnego potwierdzania tożsamości / on-boardingu

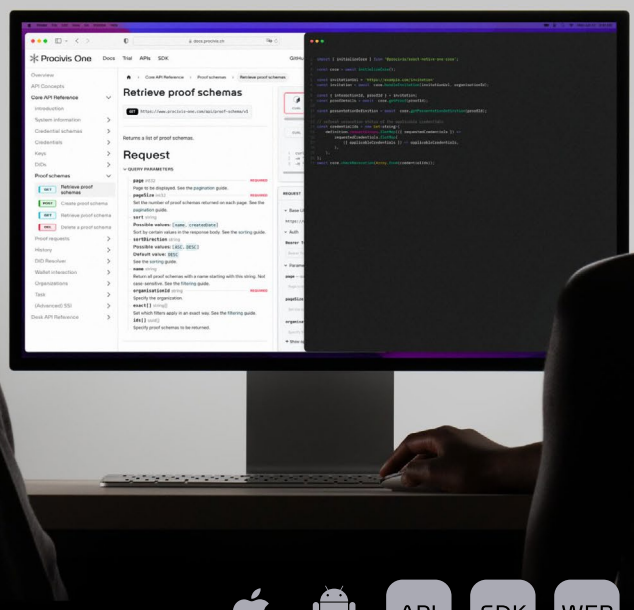
Podmiot	Nazwa rozwiązania	Opis rozwiązania
Authologic	Platforma Authologic	Kompleksowe rozwiązanie zaprojektowane w celu usprawnienia procesów Know Your Customer (KYC), zapewniające zarówno bezpieczeństwo, jak i wygodę dla firm i ich użytkowników. Rozwiązanie integruje różne metody potwierdzania tożsamości w jednym interfejsie API. Korzystając z Authologic można łatwo zintegrować się z różnymi dostawcami i uwzględnić zaawansowane procesy identyfikacji użytkowników, takie jak biometria, kontrole żywotności, weryfikacja tożsamości elektronicznej (eID), OCR dokumentów, identyfikacja bankowa i wiele innych. Rozwiązanie pozwala na skrócenie czasu procesu KYC z 2-3 minut do 10-30 sekund. Obsługa 200 krajów i terytoriów w 13 różnych językach
IDENTT	Identt	IDENTT dostarcza system wyposażony w algorytmy wspierające proces weryfikacji tożsamości. Obsługa różnych scenariuszy weryfikacji tożsamości - w oparciu o zdjęcia dokumentów, wizerunek osoby, warstwę elektroniczną dokumentu tożsamości. Potwierdzenie tożsamości klienta może odbywać się w ramach aplikacji webowej, aplikacji mobilnej, podczas rozmowy video-ochat z konsultantem lub być zintegrowane z bankomatem. Rozwiązanie działające w oparciu o bazę danych zawierającą tysiące dokumentów tożsamości z ponad 194 krajów.
KIR	mojeID	Weryfikacja tożsamości z wykorzystaniem bankowości elektronicznej w usługach komercyjnych i publicznych. W ramach usługi oferowanej na stronie firmy, klienci zostają przekierowani do bankowości elektronicznej, w której w bezpieczny i poufny sposób potwierdzą swoją tożsamość i wyrażają zgodę na przekazanie wymaganych danych. Cały proces potwierdzenie tożsamości w bankowości elektronicznej zajmuje 20 sekund. mojeID dostępne jest dla klientów 11 banków komercyjnych, ponad 500 banków spółdzielczych

Billon	**Platforma tożsamości Billon**	Oparta na blockchainie platforma tożsamości Billon zapewnia użytkownikom suwerenną kontrolę nad ich cyfrową tożsamością, umożliwiając płynne i bezpieczne interakcje z dostawcami usług. Zweryfikowane w procesie KYC (dane dostarczane przez partnerów), rzeczywiste tożsamości są powiązane z cyfrowymi, a dane osobowe są przechowywane poza łańcuchem w bezpiecznym rejestrze tożsamości. Po ustanowieniu suwerennej tożsamości użytkownicy mają wyłączną kontrolę nad swoimi kluczami kryptograficznymi, umożliwiając bezpośredni dostęp do dokumentów i usług w całej sieci bez udziału stron trzecich. Każda interakcja jest unikalnie szyfrowana i uwierzytelniana, wzmacniając zaufanie i integralność danych w każdej transakcji. Każda transakcja weryfikacji tożsamości może być bezpiecznie rejestrowana w łańcuchu bloków a zapis oparty na blockchainie oferuje weryfikowalną historię każdej weryfikacji tożsamości.

Zestawienie zawiera jedynie dostawców, będących partnerami Trusted Economy Forum CommonSign 2024

Przygotuj się na eIDAS 2.0 z Procivis One

Procivis One jest elastycznym i kompleksowym rozwiązaniem dla ekosystemu eIDAS 2.0 bezproblemowo łączącym Twoje rozwiązania biznesowe z Europejskim Portfelem Tożsamości Cyfrowej.



DOSTĘPNE MODELE LICENCYJNE

Procivis One Open Source

Procivis One Enterprise

API SDK WEB

01. Procivis One Issuer

Kompleksowe rozwiązanie pozwalające na wydawanie cyfrowych dokumentów typu PID, QEAA, PuB-EAA oraz EAA do Europejskiego Cyfrowego Portfela

02. Procivis One Verifier

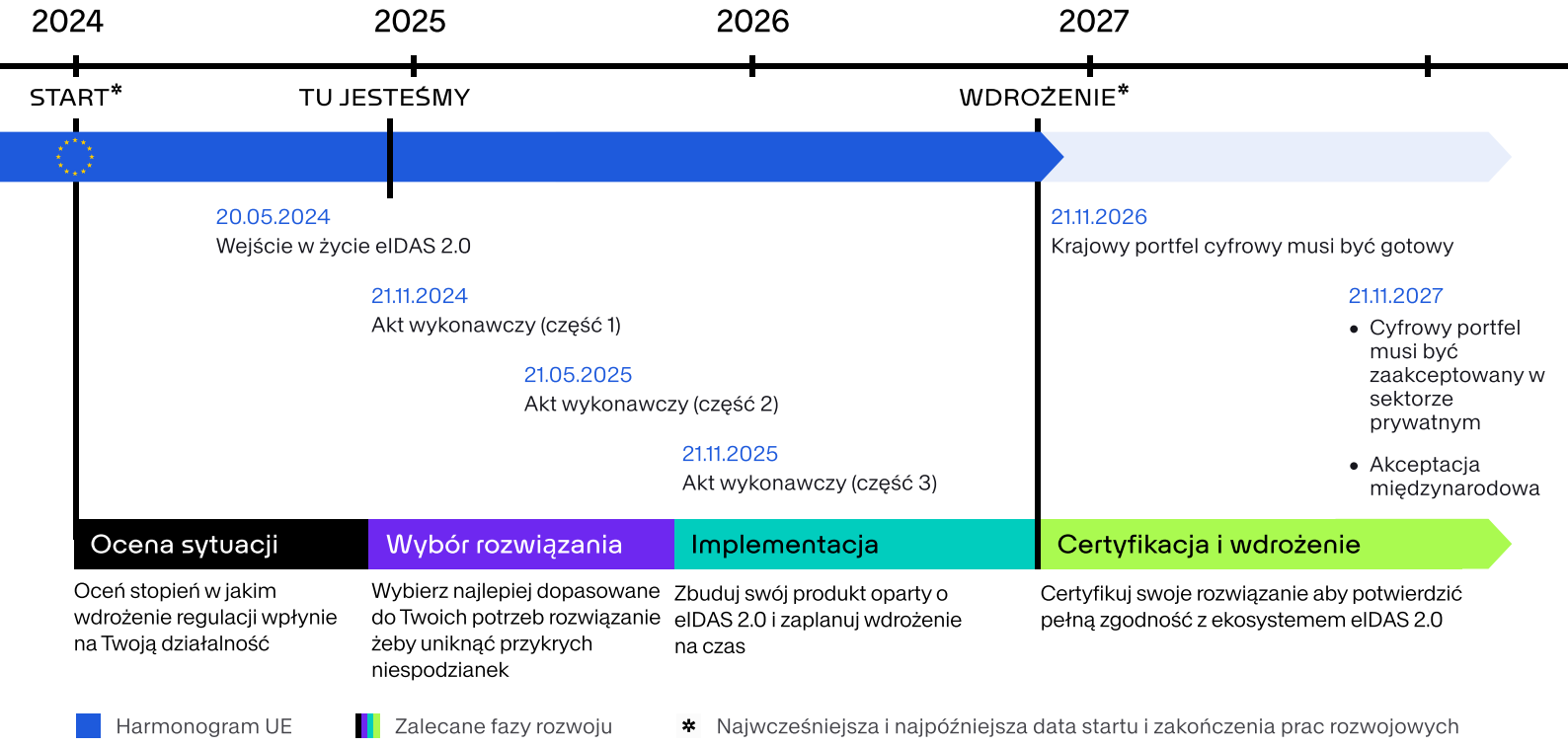
Kompleksowe rozwiązanie pozwalające na weryfikację cyfrowych dokumentów typu PID, QEAA, PuB-EAA oraz EAA z dowolnego Europejskiego Cyfrowego Portfela

03. Procivis One Wallet

Kompletne SDK Europejskiego Cyfrowego Prortfela dla aplikacji z możliwością adaptacji do wymagań kraju członkowskiego

Zapoznaj się z harmonogramem wdrożenia eIDAS 2.0

Regulacje eIDAS 2.0 mogą wpłynąć na Twoją działalność na kilka sposobów. Sprawdź podsumowanie na poniższym harmonogramie i skontaktuj się z nami w celu uzyskania szczegółowego audytu zgodności oraz wyznaczenia potencjalnych kroków w kierunku pełnej zgodności z eIDAS 2.0



Oceń stopień w jakim wdrożenie regulacji wpłynie na Twoją działalność

Wybierz najlepiej dopasowane do Twoich potrzeb rozwiązanie żeby uniknąć przykrych niespodzianek

Zbuduj swój produkt oparty o eIDAS 2.0 i zaplanuj wdrożenie na czas

Certyfikuj swoje rozwiązanie aby potwierdzić pełną zgodność z ekosystemem eIDAS 2.0

Harmonogram UE Zalecane fazy rozwoju * Najwcześniejsza i najpóźniejsza data startu i zakończenia prac rozwojowych

Procivis
AN ORELL FÜSSLI COMPANY

info@procivis.ch
www.procivis.ch
+41 44 523 65 35

Dietzingerstrasse 3
8003 Zurich
Switzerland

Zimmermanngasse 8
1090 Vienna
Austria

ATTESTA ISO 9001 ZERTIFIZIERT

ATTESTA ISO 27001 ZERTIFIZIERT

IDENTT®

We assure you!

By the nature of biometrics

IDENTT to wiodący dostawca rozwiązań opartych na sztucznej inteligencji do **automatycznej weryfikacji dokumentów tożsamości** oraz **biometrycznego rozpoznawania twarzy.**

Oferujemy **zwiększone bezpieczeństwo** poprzez minimalizowanie oszustw tożsamościowych oraz **redukcję kosztów** pozyskiwania klientów.

Nasze usługi pomagają firmom usprawnić **zdalny lub stacjonarny proces onboardingu** klientów oraz spełniać wymogi zgodności z przepisami prawnymi.

- Weryfikacja tożsamości
- Zautomatyzowany i zdalny proces onboardingu klientów
- OCR system
- Zdalna obsługa kontraktowa
- Wykrywanie fraudów i deepfake-ów
- Weryfikacja wieku

2. Kwalifikowane podpisy elektroniczne

Kwalifikowane podpisy elektroniczne to forma podpisów elektronicznych o najwyższym poziomie bezpieczeństwa i zaufania, regulowana w Unii Europejskiej przez rozporządzenie eIDAS (Rozporządzenie Parlamentu Europejskiego i Rady UE nr 910/2014). Są one **prawnie równoważne podpisowi własnoręcznemu**, co oznacza, że dokument podpisany kwalifikowanym podpisem elektronicznym jest traktowany tak, jakby został podpisany własnoręcznie.

Kwalifikowany podpis elektroniczny to narzędzie, które umożliwia **oświadczenie woli - podpisywanie dokumentów w sposób zdalny**, ale z zachowaniem najwyższego poziomu bezpieczeństwa i zgodności prawnej. Jest kluczowy dla osób i organizacji, które potrzebują prawnie wiążącego podpisu akceptowanego we wszystkich państwach UE. Dzięki niemu można bezpiecznie przeprowadzać operacje i zawierać umowy z pełnym zaufaniem do ich autentyczności oraz integralności.

Podpisy elektroniczne zgodnie z rozporządzeniem eIDAS są oferowane na rynku przez **dostawców usług zaufania**, które jako podmioty nadzorowane dostarczają rozwiązania w oparciu o spełnienie wymagań przepisów oraz polityki usługi zaufania. Kwalifikowany podpis elektroniczny zapewnia wiarygodność, integralność i niezmienność dokumentu po podpisaniu oraz zapewnia, że dokonane zostało potwierdzenie tożsamości osoby, która podpisała dokument.

2.1. Kwalifikowane podpis elektroniczny jako narzędzie zdalnego oświadczenia woli w procesach biznesowych

Oświadczenie woli to wyraz decyzji podjętej przez osobę fizyczną lub osobę działającą w imieniu podmioty prawnego, która ma na celu wywołanie określonych skutków prawnych. Funkcjonuje jako formalne potwierdzenie podjęcia zobowiązań lub zawarcia umowy.

W polskim prawie obowiązuje zasada swobody formy oświadczenia woli, zgodnie z nią „z zastrzeżeniem wyjątków w ustawie przewidzianych, wola osoby dokonującej czynności prawnej może być wyrażona przez każde zachowanie się tej osoby, które ujawnia jej wolę w sposób dostateczny, w tym również przez ujawnienie tej woli w postaci elektronicznej (oświadczenie woli)".

Wraz z wejściem w życie Rozporządzenia eIDAS polski ustawodawca wprowadził przepis, który ma na celu ujednolicenie zasad stosowania formy elektronicznej czynności prawnych. W efekcie powyższych zmian w polskim porządku prawnym wyraźnie wyodrębniona została forma elektroniczna jako autonomiczna forma czynności prawnych.

Wcześniej wyróżnienie formy elektronicznej było kwestią sporną, była ona traktowana jako odmiana formy pisemnej.

Nowelizacja Kodeksu Cywilnego wprowadziła również nową formę dokonywania czynności prawnych – formę dokumentową, do której zachowania wystarcza złożenie oświadczenia woli w postaci dokumentu, w sposób umożliwiający ustalenie osoby składającej oświadczenie. Dokument rozumiany jest tu jako nośnik informacji, z którym mogą zapoznać się inne osoby. Nie musi więc to być oświadczenie woli w postaci dokumentu elektronicznego. Dopuszczalny jest także zapis wideo, audio lub email. Forma dokumentowa nie jest automatycznie podpisem elektronicznym i nie niesie domniemań prawnych wynikających ze stosowania podpisów elektronicznych. Ponieważ przepisy prawa nie określają warunków bezpieczeństwa i stosowania formy dokumentowej cały ciężar jej zabezpieczenia oraz dowodu związany z jej stosowaniem jest na stronie skarżącej. Strona przeprowadzająca dowód w zakresie formy dokumentowej powinna potwierdzić jej integralność oraz powiązanie z składającym oświadczenie. W związku z powyższym forma dokumentowa powinna być stosowana tylko tam, gdzie ryzyko związane z wartością transakcji jest niewielkie. Podpisy elektronicznie, jako rozwiązanie alternatywne do formy dokumentowej, w szczególności zaawansowany podpis elektroniczny i kwalifikowany podpis elektroniczny gwarantują integralność dokumentu i powiązanie z podpisującym.

Obecnie mamy zatem do dyspozycji kilka opcji na złożenie oświadczenia woli. Może ono być złożone:

- ustnie,
- pisemnie:
  - w formie zwykłej pisemnej,
  - w formie pisemnej z datą pewną, czyli poświadczoną urzędowo,
  - w formie pisemnej z podpisem notarialnie poświadczonym,
- w formie aktu notarialnego,
- w formie dokumentowej,
- w sposób dorozumiany (poprzez pozajęzykowe zachowanie, ale takie, które ujawnia naszą wolę w sposób dostatecznie zrozumiały dla odbiorcy),
- w formie elektronicznej.

Do zachowania elektronicznej formy czynności prawnej wymagane jest spełnienie dwóch przesłanek:

1.

złożenie oświadczenia woli w postaci elektronicznej

2

opatrzenie go kwalifikowanym podpisem elektronicznym

Oświadczenie woli złożone w formie elektronicznej jest równoważne z oświadczeniem woli złożonym w formie pisemnej. W każdym przypadku, w którym wymagany jest podpis własnoręczny, może on zostać skutecznie zastąpiony poprzez złożenie kwalifikowanego podpisu elektronicznego. **Jeżeli więc przepisy prawa dla ważności czynności prawnej wymagają zachowania formy pisemnej, może ona zostać zastąpiona formą elektroniczną.**

Obecnie zatem dzięki **zrównaniu prawnemu formy pisemnej z formą elektroniczną** przy podpisywaniu dokumentów związanych z działalnością przedsiębiorstwa, w tym umów, dla ważności których nie została prawnie lub umownie zastrzeżona notarialna forma czynności prawnej, strony mogą posłużyć się podpisami własnoręcznymi albo kwalifikowanymi podpisami elektronicznymi. Co więcej, dopuszczalne jest, aby jedna strona czynności prawnej złożyła oświadczenie w formie pisemnej, a druga w formie elektronicznej.

Bezpieczeństwo podpisu kwalifikowanego elektronicznego gwarantowane jest przez dostawców usług zaufania, którzy podlegają rygorystycznym wymogom bezpieczeństwa i nadzorowi realizowanemu przez państwo.

Dla zachowania formy elektronicznej nie jest wymagane złożenie kwalifikowanego podpisu elektronicznego opartego o certyfikat wydany w Polsce, podpisujący może posłużyć się kwalifikowanym podpisem elektronicznym opartym o certyfikat wydany jako kwalifikowany w każdym państwie członkowskim Unii Europejskiej.

Dostawcy kwalifikowanych podpisów elektronicznych wpisani są na europejskie listy zaufania oraz podlegają restrykcyjnym wymogom organizacyjnym, kapitałowym i związanym z cyberbezpieczeństwem i jakością świadczonych usług. Wydanie certyfikatu jest możliwe w formule on-site (w oddziałach tych instytucji, ich punktach partnerskich lub poprzez sieć przedstawicieli), a coraz częściej również on-line z wykorzystaniem określonych narzędzi zdalnego potwierdzania tożsamości.

Dodatkowo funkcjonują na rynku **platformy podpisowe**, które najczęściej udostępniają mechanizmy elektronicznego obiegu dokumentów i obsługi procesu ich podpisywania, z wykorzystaniem różnego typu podpisów elektronicznych, w tym także kwalifikowanych. W Polsce przykładami takich platform są Autenti, Pergamin czy Umownik.

2.2. Regulacje prawne związane z podpisami elektronicznymi

eIDAS określa standardy i zasady dotyczące elektronicznej identyfikacji, uwierzytelniania i usług zaufania, takich jak elektroniczne podpisy, pieczęcie, certyfikaty cyfrowe, usługi doręczania elektronicznego, oraz usługi znakowania czasem.

Wspomniana już wielokrotnie w tym raporcie regulacja, wprowadza w życie proces elektronizacji, oferując ramy stosowania i uznawania podpisów i pieczęci elektronicznych, które pełnią funkcje analogiczne do tradycyjnych odpowiedników na papierze. W szczególności, kwalifikowane podpisy elektroniczne mają moc zastępowania podpisów własnoręcznych, a pieczęcie elektroniczne służą do potwierdzania autentyczności i integralności dokumentów elektronicznych.

Zdefiniowane w eIDAS zaawansowane i kwalifikowane podpisy elektroniczne stanowią specjalne kategorie podpisów elektronicznych, które spełniają dodatkowe wymogi, takie jak **unikalne przyporządkowanie do podpisującego, możliwość jednoznacznej weryfikacji tożsamości podpisującego oraz dowód integralności podpisu i dokumentu.** Kwalifikowane podpisy elektroniczne, oparte na kwalifikowanym certyfikacie i kwalifikowanym urządzeniu do składania podpisu, są prawnie równoważne podpisom własnoręcznym. Kwalifikowane urządzenia do składania podpisu elektronicznego, zapewniają bezpieczne i kontrolowane przez podpisującego środowisko do składania podpisów. Aktualnie jako kwalifikowane urządzenia do składania podpisu stosowane są karty kryptograficzne oraz zdalnie dostępne usługi zarządzania danymi do składania podpisu elektronicznego. Najważniejszą cechą bezpieczeństwa urządzeń do składania podpisu jest wyłączna kontrola podpisującego nad użyciem tego urządzenia. Przepisy prawa zabraniają współdzielenia jednego urządzenia do podpisu elektronicznego przez wiele osób lub wykorzystywania jego przez osobę trzecią.

Kwalifikowane certyfikaty podpisu elektronicznego są wydawane przez dostawców usług zaufania po jednoznacznej weryfikacji tożsamości podpisującego. Certyfikaty te są jawne i dołączane do każdego podpisanego dokumentu, umożliwiają weryfikację złożonych podpisów elektronicznych.

Kwalifikowane podpisy elektroniczne są rozpoznawane w całej UE. Kwalifikowany podpis elektroniczny oparty na kwalifikowanym certyfikacie wydanym w jednym państwie członkowskim jest uznawany za kwalifikowany podpis elektroniczny we wszystkich pozostałych państwach członkowskich UE. To wymaganie przepisów unijnych nakłada na podmioty weryfikujące podpisy elektroniczne obowiązek stosowania rozwiązań pozwalających na rozpoznawanie nie tylko krajowych, lecz także zagranicznych podpisów elektronicznych w rozpoznawalnych formatach.

Znowelizowane w 2024 r. rozporządzenie eIDAS wprowadza wiele zmian zarówno w obszarze identyfikacji jak i usług zaufania. Jedną z najważniejszych zmian jest wprowadzenie europejskich portfeli tożsamości cyfrowej mających na celu ułatwienie dostępu do różnorodnych usług cyfrowych oraz poprawę ochrony prywatności użytkowników. Zgodnie z zapisami Rozporządzenia **użytkownicy indywidualni** tzn. obywatele w każdym kraju członkowskim Unii Europejskiej będą mieli oferowane domyślnie i bez zbędnych procedur administracyjnych rozwiązania obejmujące kwalifikowane podpisy elektroniczne (QES) dostępne za pośrednictwem (EUDIW), z których będą mogli korzystać bezpłatne **w ramach tzw. użytku nieprofesjonalnego.**

Warto zauważyć, że w znowelizowanej wersji eIDAS są jednocześnie zapisy sugerujące, że państwa członkowskie powinny móc ustanowić środki zapobiegające nieodpłatnemu użyciu kwalifikowanych podpisów elektronicznych przez osoby fizyczne do celów profesjonalnych, przy jednoczesnym zapewnieniu, aby wszelkie takie środki były proporcjonalne do zidentyfikowanego ryzyka oraz uzasadnione.

2.3. Przykłady wykorzystania kwalifikowanego podpisu elektronicznego w biznesie

DIGITALIZACJA OBIEGU DOKUMENTÓW W FIRMIE LEASINGOWEJ

Leasingodawcy min. BNP Paribas Lease Group czy Santander Leasing udostępniają możliwość zdalnego podpisywania e-dokumentów np. umów leasingowych kwalifikowanym podpisem elektronicznym. Dostawcą jest Asseco Data Systems oferujący systemy API SimplySign i SIGNER, które mogą być zintegrowane z systemami obiegu dokumentów firm.

WYDAWANIE KWALIFIKOWANYCH PODPISÓW ELEKTRONICZNYCH NA BAZIE TOŻSAMOŚCI BANKOWEJ

Coraz więcej banków w Polsce umożliwia wydawanie kwalifikowanych podpisów elektronicznych swoim klientom na bazie potwierdzania tożsamości przy użyciu bankowych środków identyfikacji. Krajowa Izba Rozliczeniowa umożliwia wydanie certyfikatu podpisu tzw. mSzafir min. klientom PKO BP czy Banku Millennium. Asseco Data Systems analogiczne rowiązanie – produkt SimplySign proponuje klientom Santander Banku Polska.

USE-CASE PARTNERA

Artur Miękina

Dyrektor Działu Sprzedaży Projektowej i Rozwoju e-Biznesu
Asseco Data Systems

Wdrożenie w ING Banku Śląskim to przykład współpracy, chęci i zaangażowania stron na rzecz cyfryzacji procesów HR. Innowacyjna koncepcja wykorzystania jednorazowego podpisu kwalifikowanego jako rozwiązania optymalnego, niezawodnego i bezpiecznego, była istotną częścią tego złożonego projektu. Dzięki kompleksowemu podejściu, procesy HR stały się bardziej efektywne i ekologiczne, przy jednoczesnej eliminacji dokumentów papierowych. Dostrzegamy ogromny potencjał wykorzystania jednorazowego podpisu kwalifikowanego, nie tylko w obszarze HR, ale również w biznesie.

USE-CASE PARTNERA

Bogumiła Cebelińska-Woźniak

Product Director Billon Group

Platforma do zdalnego zarządzania dokumentami i zawierania umów oparta na technologii blockchainie od firmy Billon to zaawansowane rozwiązanie, które integruje e-podpisy, e-doręczenia oraz zarządzanie cyfrową tożsamością oferując różne metody weryfikacji online. Technologia blockchain zapewnia niezmienny, transparentny zapis każdej transakcji, co umożliwia bezpieczną weryfikację oraz pełną ścieżkę audytu procesów biznesowych. Platforma jest zgodna z regulacjami eIDAS, RODO oraz wymogami trwałego nośnika, spełniając najwyższe standardy bezpieczeństwa i ochrony danych. Obecnie jest wdrożona w sektorze finansowym w ramach platformy BIK dla bankowości i ubezpieczeń oraz w sektorze energetycznym u czołowego dostawcy energii, firmy Tauron. Inne wdrożenia obejmują sektor edukacyjny i zielonej energii. Nasze rozwiązanie przeszło również zaawansowane testy w ramach inicjatywy European Blockchain Services Infrastructure (EBSI) dla transgranicznego procesu wymiany danych i dokumentów. Dzięki modułowej architekturze platforma elastycznie dostosowuje się do indywidualnych potrzeb klientów, oferując kompletną obsługę cyfrową dla dokumentacji i kontraktów.

USE-CASE PARTNERA

Andrea Sassetti
CEO
Aruba PEC

Włoska firma świadcząca usługi finansowe, powiązana z Mediolańską giełda papierów wartościowych - Euronext, z powodzeniem, wdrożyła wiele usług zaufania w celu automatyzacji zarządzania Rejestrem Członków dla swoich klientów. Ten kluczowy dokument identyfikuje uprawnionych członków i ustala kworum na potrzeby spotkań, zapewniając legalność udziału i głosowania. Wykorzystując Certyfikowaną Platformę Aruba PEC S.p.A., firma generuje Rejestr Akcjonariuszy w formacie PDF i usprawnia cały proces. Po załadowaniu dokumentu uruchamiany jest zautomatyzowany przepływ dokumentów, umożliwiający e-podpis zarówno przez operatora firmy finansowej, jak i przedstawiciela firmy klienta. Podpisany dokument jest następnie bezpiecznie przesyłany za pomocą kwalifikowanej usługi e-Doręczenia i archiwizowany w kwalifikowanym systemie e-Archiwizacji, zapewniając zgodność z wymogami prawnymi.

Integracja zautomatyzowanych usług e-podpisu i e-doręczenia nie tylko zwiększa bezpieczeństwo i efektywność zarządzania dokumentami, lecz także gwarantuje ich prawomocność, stanowiąc modelowy przykład działania usług zaufania. Połączenie tych usług usprawnia operacje, jednocześnie płynnie dostosowując się doobowiązków regulacyjnych nałożonych na Euronext.

USE-CASE PARTNERA

Edgars Stafeckis

CEO & Co-founder TrustLynx

Platforma Trustlynx's Embedded Trust została wprowadzona na rynek w czasie, gdy usługi zaufania, takie jak podpisy elektroniczne i pieczęcie elektroniczne, były głównie wykorzystywane w usługach publicznych, a w sektorze prywatnym jedynie opcjonalnie. Prawdziwe znaczenie adopcji usług zaufania ujawniło się podczas pandemii COVID-19, kiedy możliwość prowadzenia działalności gospodarczej, świadczenia usług i realizacji transakcji całkowicie zdalnie była możliwa dzięki tożsamościom cyfrowym, podpisom elektronicznym, pieczęciom elektronicznym itp. Wykorzystanie usług zaufania wzrosło wykładniczo i ten trend nadal się utrzymuje. Tożsamości cyfrowe, podpisy elektroniczne i pieczęcie elektroniczne stały się nieodzownym elementem współczesnego biznesu.

Platforma Trustlynx oferuje bezpieczne, elastyczne i wydajne narzędzia do wzbogacenia systemów organizacji o odpowiednie usługi zaufania, w tym wsparcie dla tożsamości cyfrowych i ich atrybutów, podpisy elektroniczne i ich zbieranie, pieczęcie elektroniczne oraz ich walidację. W świecie cyfrowym priorytetem są płynne doświadczenie użytkownika, bezpieczeństwo informacji i ochrona danych – to nie tylko konieczność, ale również przewaga konkurencyjna. Trustlynx opracował technologię integracji i automatyzacji usług zaufania, aby uprościć rozwój procesów biznesowych i produktów cyfrowych, oferując nowoczesnym firmom kompleksowe rozwiązania.

Teraz, gdy podpisy elektroniczne są prawnie równoważne podpisom odręcznym, Trustlynx jest zaufanym partnerem, dostarczającym elastyczne i bezpieczne rozwiązania. Platforma Embedded Trust pozwala firmom uprościć ścieżkę użytkownika i przepływ danych bez kompromisów w zakresie bezpieczeństwa czy zgodności, umożliwiając nadążanie za tempem cyfrowej transformacji.

2.4 Kwalifikowany podpis elektroniczny na tle innych rodzajów podpisów na polskim rynku oraz w perspektywie wdrożenia eIDAS 2.0

Rozporządzenie eIDAS definiuje dwa inne niż kwalifikowane rodzaje podpisu: zaawansowany podpis elektroniczny oraz „zwykły" podpis elektroniczny. W przypadku innych podpisów elektronicznych niż kwalifikowany, każdy dostawca usługi zaufania określa warunki jego bezpieczeństwa oraz zakres świadczonej usługi.

Te dwa pozostałe rodzaje podpisów choć nie spełniają formy pisemnej i nie zastępują podpisu własnoręcznego są jednak w polskiej przestrzeni cyfrowej z powodzeniem wykorzystywane. Stosuje się je też w różnych sytuacjach. Niezależnie od rodzaju podpisu elektronicznego nie można im odmówić skutku prawnego ani dopuszczalności jako dowodu w postępowaniu sądowym wyłącznie z tego powodu, że podpis ten ma postać elektroniczną lub że nie spełnia wymogów dla kwalifikowanych podpisów elektronicznych. Główne różnice pomiędzy poszczególnymi podpisami elektronicznymi przedstawia poniższa tabela.

Rodzaje podpisów elektronicznych

Funkcja	Kwalifikowany podpis elektroniczny	Zaawansowany podpis elektroniczny	Zwykły podpis elektroniczny
Moc prawna	Uznawany we wszystkich krajach Unii Europejskiej w sposób jednolity	Uznawany lokalnie lub w relacjach biznesowych, zapewnia wartość dowodową na poziomie Europejskim	Uznawany lokalnie lub w relacjach biznesowych
Kwalifikowany certyfikat podpisu elektronicznego	Wymagany	Opcjonalny	-
Wystawca kwalifikowanego certyfikatu podpisu elektronicznego	Unijny lub norweski Kwalifikowany Dostawca Usług Zaufania	Kwalifikowany lub niekwalifikowany dostawca usług zaufania	-
Urządzenie do składania podpisu kwalifikowanego	Wymagane	-	-
Może być składany zdalnie	Tak	Tak	Tak
Potwierdzenie tożsamości podpisującego	Wymagane przez prawo na wysokim poziomie pewności; może być lokalne lub zdalne	Wymagane, ale poziom pewności może być ograniczony	-
Akceptowane w przetargach publicznych	Tak	Nie*	Nie

(*) Wyjątek stanowi Podpis Osobisty na potrzeby postępowań krajowych.

Jednocześnie w Polsce funkcjonują takie rozwiązania jak „Podpis zaufany na bazie Profilu Zaufanego" oraz „Podpis osobisty na bazie elektronicznego dowodu osobistego" używane często w usługach elektronicznych administracji publicznej. Poniżej przedstawiono porównanie ich cech z podpisem kwalifikowanym.

Porównanie podpisu kwalifikowanego i rozwiązań rządowych (podpis osobisty i zaufany):

	Podpis kwalifikowany	Podpis zaufany na bazie Profilu Zaufanego	Podpis osobisty na bazie elektronicznego dowodu osobistego
Onboarding	Wniosek o wydanie podpisu składany online + potwierdzenie tożsamości onsite lub zdalnie (wideoweryfikacja, eID, inny podpis kwalifikowany)	Wniosek o wydanie podpisu składany online + potwierdzenie tożsamości onsite lub zdalnie (wideoweryfikacja, eID, inny podpis kwalifikowany, dowód osobisty z warstwą elektroniczną + NFC)	Uzależniony jest od procedury pozyskiwania dowodu osobistego (obecnie wyłącznie stacjonarnie)
Funkcjonalność, kanały dostępu	Podpis składany za pomocą kwalifikowanego urządzenia do składania podpisu elektronicznego (karta lub serwis online), który opiera się na kwalifikowanym certyfikacie podpisu elektronicznego / Aplikacje dostawcy	Możliwość przesłania przez podmioty publiczne (na odpowiednie API) dokumentu do podpisania oraz zwrot podpisanego dokumentu/Przeglądarka internetowa	Aby korzystać z podpisu osobistego, należy mieć czytnik NFC do e-dowodu (lub smartfon z czytnikiem NFC) oraz zainstalować na swoim urządzeniu odpowiednie oprogramowanie (E-dowód podpis osobisty lub eDO App)
Walidacja podpisanych dokumentów/ interoperacyjność	Desktopowe narzędzia dostarczone przez dostawców podpisu, kwalifikowane usługi walidacji, DSS na stronach Komisji Europejskiej, Obywatel.gov.pl	Na stronie obywatel.gov.pl, aplikacją e-Dowód, niektórymi aplikacjami do weryfikacji podpisów kwalifikowanych/brak interoperacyjności poza PL w zakresie tworzenia i składania oraz weryfikacji podpisu	Aplikacją e-Dowód oraz niektórymi aplikacjami do weryfikacji podpisów kwalifikowanych / brak interoperacyjności poza PL w zakresie tworzenia i składania podpisu
Skutki użycia, moc prawna	Podpis kwalifikowany zastępuje tradycyjną papierową dokumentację (automatycznie równoważny podpisowi odręcznemu)	Dane w postaci elektronicznej opatrzone podpisem zaufanym są równoważne pod względem skutków prawnych dokumentowi opatrzonemu podpisem własnoręcznym, chyba, że przepisy odrębne stanowią inaczej	Skutek równoważny podpisowi odręcznemu wywołuje opatrzenie danych podpisem osobistym w stosunku do podmiotu innego niż podmiot publiczny, jeżeli obie strony wyrażą na to zgodę
Przypadki użycia, zasięg	Wszystkie przypadki, w których można podpisać podpisem zaufanym oraz podpisywanie umów B2B i B2C	Załatwianie spraw urzędowych na dedykowanych platformach (ePUAP, obywatel.gov.pl, PUE ZUS, praca.gov.pl). Brak zasięgu akceptacji w obszarze biznesowym	Posiada identyczną funkcjonalności jak Podpis Zaufany i służy do komunikacji z polskimi systemami administracji. W relacjach B2A

Użycie kwalifikowanych podpisów daje najszerszą możliwość uzyskania akceptacji dokumentu podpisanego takim podpisem. Podpis zaufany nie jest rozpoznawany jako podpis poza Polską, natomiast podpis osobisty będzie rozpoznany, ale zaufanie do niego będzie ograniczone. Podpis zaufany nie jest akceptowany w biznesie, natomiast podpis osobisy może być stosowany w usługach komercyjnych za zgodą obu stron. **Podpis kwalifikowany dostarcza najwięcej możliwości użycia zarówno w sektorze publicznym, jak i prywatno-komercyjnym.** Ze względu na oferowane gwarancje bezpieczeństwa coraz częściej stosowany jest kwalifikowany podpis elektroniczny zamiast innych „słabszych" podpisów.

Mimo nierozstrzygniętych jeszcze wielu kwestii technicznych można już dziś przypuszczać, że **szeroka adopcja szerzej omawianego wcześniej Europejskiego Portfela Cyfrowej Tożsamości wśród obywateli państw członkowskich znacząco zmieni liczbę interakcji, w których kwalifikowany podpis elektroniczny będzie mógł być wykorzystany**. Po upowszechnieniu się portfeli każdy obywatel kraju członkowskiego będzie miał możliwość podpisania dowolnej umowy, w tym np. umowy o pracę z pełną mocą prawną wykorzystując łatwo dostępny kwalifikowany podpis elektroniczny. Potencjalnie cyfryzacji na masową skalę ulec będą mogły procesy, które do tej pory zarezerwowane były jedynie do realizacji w bezpośrednim fizycznym kontakcie klienta z instytucją lub w wybranych przypadkach z innymi modelami takimi jak podpis fizyczny przy obecności kuriera, względnie przy których były używane niewystarczające od strony bezpieczeństwa narzędzia jak np. metoda dokumentowa.

2.5. Zestawienie dostawców i usług podpisu elektronicznego.

Podmiot	Nazwa rozwiązania	Opis rozwiązania
Asseco Data Systems	SimplySign (Certum by Asseco)	SimplySign to mobilny podpis elektroniczny, niewymagający fizycznego czytnika ani karty z certyfikatem. Możliwość podpisywania za pomocą smartfona, tabletu, laptopa lub komputera PC lub Mac. Zgodność z kluczowymi usługami i platformami jak e-deklaracje, ePUAP, ZUS, eKRS. Kompatybilny z CertumSign -platformą do podpisywania e-dokumentów przez przeglądarkę. Podpis może być bezproblemowo zintegrowany z dowolnym systemem obiegu dokumentów czy transakcji lub dowolnym systemem bankowości elektronicznej poprzez API SimplySign (rozwiązanie, pozwalające na używanie kwalifikowanego e-podpisu SimlpySign bezpośrednio w systemie do obiegu dokumentów). Kompatybilny z rozwiązaniem SignHUB pozwalającym na podpisywanie dokumentów osobom spoza organizacji, nawet gdy nie posiadają własnego e-podpisu.

Podmiot	Nazwa rozwiązania	Opis rozwiązania
Aruba S.p.A	Firma digitale remota	Zdalny podpis cyfrowy zawiera znacznik czasu, który pozwala powiązać określoną datę i godzinę z podpisywanymi dokumentami i przedłużyć ich ważność prawną do 30 lat. Dzięki dedykowanej aplikacji Aruba OTP do zdalnego podpisu cyfrowego można wygenerować jednorazowy dwuskładnikowy kod uwierzytelniający OTP i podpisać bezpośrednio ze smartfona, bez innych urządzeń. Rozwiązanie kompatybilne z Aruba Webmail i PEC Webmail, dzięki czemu można podpisywać dokumenty bezpośrednio w skrzynce mailowej bez konieczności instalowania żadnego oprogramowania lub aplikacji do podpisu.
Namirial Group	Namirial Digital Signature	Stworzony do zarządzania plikami i dokumentami bezpośrednio ze smartfona. Wliczona w cenę możliwość identyfikacji za pomocą sesji identyfikacji wideo za pośrednictwem kamery internetowej z operatorem Namirial. Pełna zgodność z eIDAS Wieloskładnikowe uwierzytelnianie zapewniające maksymalne bezpieczeństwo. Kompatybilny z platforma podpisową eSignAnyWhere, którą można zintegrować z popularnymi narzędziami, takimi jak Microsoft Office 365, Salesforce czy SharePoint oraz wdrożyć jako usługę w chmurze lub lokalnie.
KIR	mSzafir	Mobilny kwalifikowany podpis elektroniczny mSzafir pozwala podpisywać dokumenty na dowolnym urządzeniu i umożliwia generowanie certyfikatów jednorazowych oraz certyfikatów ważnych 1 rok lub 2 lata z wybranym limitem podpisów. Tożsamość użytkownika jest weryfikowana za pomocą usługi mojeID (z wykorzystaniem bankowości elektornicznej), certyfikatu kwalifikowanego lub osobiście w placówce KIR. Rozwiązanie oferuje ożliwość podpisania do 20 dokumentów jednocześnie.
SIGNIUS S.A.	SIGNIUS Professional - platforma do zdalnego podpisywania dokumentów podpisem kwalifikowanym i zaawansowanym	Platforma umożliwia zdalne i natychmiastowe podpisywanie dokumentów online podpisem zaawansowanym i kwalifikowanym, przez wiele osób. Podpis kwalifikowany (certyfikat firmy Eurocert) wydawany jest na podstawie zdalnej weryfikacji tożsamości realizowanej w formie wideoweryfikacji lub samodzielnie poprzez aplikację Nect Selfie.

Używaj narzędzi ekosystemu
#EnterprisePaperless!

Transformacja cyfrowa zwiększa efektywność, ale wymaga gotowości do zmian w procesach i sposobie myślenia. Dzięki nam odkryjesz korzyści z przejścia na paperless i przeniesiesz swoją organizację do cyfrowej przyszłości, gdzie papier przestaje być nośnikiem dokumentów.

e-Doręczenia

Wysyłaj elektroniczne listy polecone

SignHub

Podpisuj e-dokumenty z osobami spoza organizacji

Signer

Buduj i wdrażaj procesy paperless

WebNotarius

Dbaj o bezpieczeństwo e-dokumentów

Usługi zaufania

Chroń i zabezpieczaj e-dokumenty

e-ID Hub

Potwierdzaj tożsamość online

Dołącz do świadomych przedsiębiorców.
Sprawdź jak na: paperless.asseco.com

asseco

aruba.it

ARUBA FOSTERS TRUST AND TRANSPARENCY WITHIN BOTH THE EUROPEAN AND GLOBAL DIGITAL ECONOMIES

Aruba.it

Namirial

Making Simplicity Meeting Compliance

Harnessing Namirial Intelligent Trust Services for, among other things ...

SALES

- Purchase agreements
- Account opening
- Financing contracts (loan / leasing)
- Consultation records
- Direct debit mandates (SEPA)
- Leases / rental agreements
- Confidentiality agreements (NDA)
- Reseller / referral agreements

HUMAN RESSOURCES

- Working contracts
- Confidentiality agreements (NDA)
- Employee policies
- Consent declarations
- Permits
- Expense processing
- Bonus agreements

SERVICE / SUPPORT

- Support agreements
- Maintenance contracts
- Damage reports
- Repair orders
- Amendments
- Acceptance protocols

PROCUREMENT

- Supplier contracts
- Service contracts
- Consulting agreements
- Requirements acceptance
- Orders
- Amendments
- Payment releases

LEGAL

- License agreements
- Consent declarations (GDPR)
- Agreement amendments
- Distribution agreements
- Facility management contracts
- Memoranda of understanding
- Authorities

QUALITY MANAGEMENT

- Order processing
- Standard operating procedures (SOP)
- Test protocols
- Loan documents
- Proofs of waste disposal

Talk to us about your use cases at Trusted Economy Forum CommonSign 2024

Anthony Skarlatos
Key Account Manager
Namirial

a.skarlatos@external.namirial.com
+30 694 4316 302
linkedin.com/in/antonyskarlatos/

Jörg Lenz
Head of Marketing & Communication
Namirial

j.lenz@namirial.com
+49 174 2409 299
linkedin.com/in/joerglenz

Podpis godny zaufania!

E-podpisy i e-pieczęcie zgodne z wymaganiami polskiego i unijnego prawa.

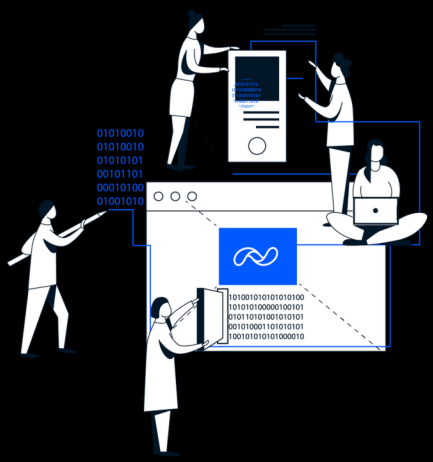
TrustLynx to innowacyjne, bezpieczne i łatwe w użyciu rozwiązanie do integracji, automatyzacji i cyfryzacji procesów biznesowych.

- Integracja z dowolnym CRM, ERP, HRM etc. na rynku
- Zgodność z eIDAS
- Przyjazny interfejs i łatwy w obsłudze proces podpisywania
- Oszczędność czasu i automatyzacja pracy
- Ochrona środowiska

trustlynx.com sales@trustlynx.com

BILLON

Billon to firma technologiczna, która opracowała własny, wyjątkowo wydajny i skoncentrowany na danych protokół blockchain. Platforma w pełni wspiera rozwój Web 3.0 i ustanowiła światowy rekord efektywności energetycznej. Umożliwia przetwarzanie danych, dokumentów, tożsamości, tokenów oraz pieniędzy w ramach jednej infrastruktury, co przekłada się na poprawę procesów, zwiększenie bezpieczeństwa oraz automatyzację operacji. Rozwiązanie Billon stanowi rewolucję w zarządzaniu danymi i zostało przetestowane oraz zweryfikowane przez globalnie uznane firmy.

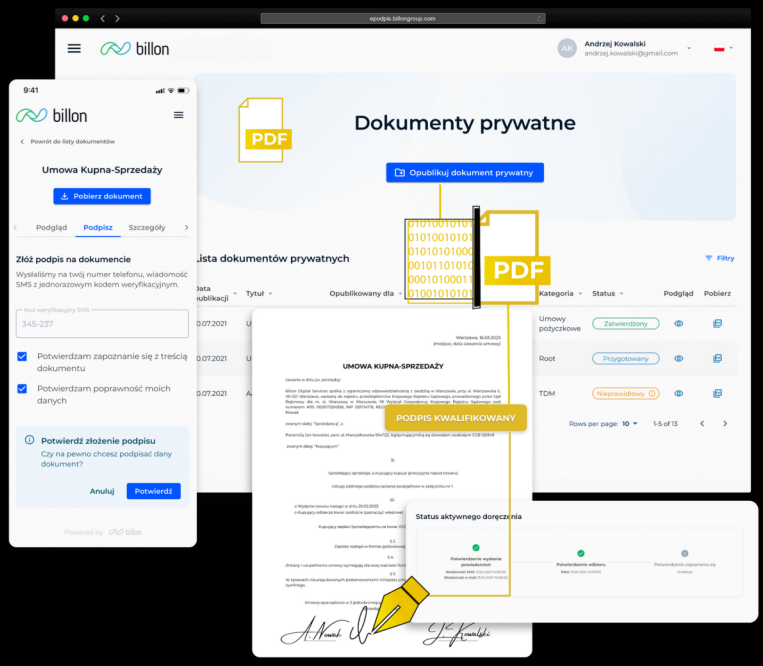


BILLON UNIFIED BLOCKCHAIN

BILLON UNIFIED BLOCKCHAIN

Billon Unified Blockchain to nowoczesna platforma blockchain, która łączy trwały nośnik informacji z bezpieczną wymianą danych i dokumentów on-chain, zgodną z regulacjami krajowymi i europejskimi, w tym eIDAS i RODO. Umożliwia zdalne składanie oświadczeń woli, zawieranie umów oraz obsługę zaawansowanych e-podpisów, wspierając zarządzanie tożsamością cyfrową i elektroniczną identyfikacją. Dzięki funkcji aktywnego doręczenia, platforma potwierdza dostarczenie i odbiór dokumentów na zweryfikowaną tożsamość, zapewniając niezmienność danych, pełną audytowalność oraz bezpieczeństwo operacji w erze Web 3.0.

- Trwały nośnik informacji zarówno dla dokumentów publicznych jak i prywatnych
- Podpisy cyfrowe: SES, AES, QES
- Zróżnicowane metody uwierzytelniania i zarządzania rolami
- Tożsamość cyfrowa jako podstawa dla tożsamości suwerennej (SSI)
- Aktywne doręczenie-jednoznaczne i niezaprzeczalna ewidencja dostarczenia i odbioru kryptograficznie zabezpieczonych dokumentów



CONTACT

General
contact@billongroup.com

Chief Commercial Officer
jacek.figula@billongroup.com

TDM Product Director
bogumila.cebelinska@billongroup.com

www.billongroup.com

3. Kwalifikowane pieczęci elektroniczne

Pieczęć elektroniczna to narzędzie dostarczające dowodów integralności oraz autentyczności pochodzenia dokumentów nią opieczętowanych. Pieczęcią elektroniczną mogą posługiwać się jedynie osoby prawne – na przykład firmy, urzędy oraz organizacje społeczne. Jej najczęstszym sposobem wykorzystanie to autoryzowanie oficjalnej korespondencji firmowej, dokumentów prawnych, dyplomów, legitymacji, potwierdzenia wykonany usług, które dzięki temu nie muszą być wydawane w formule papierowej i nie wymagają interakcji z człowiekiem.

Definicyjnie, zgodnie z rozporządzeniem eIDAS „Pieczęć elektroniczna" oznacza **dane w postaci elektronicznej** dodane do innych danych w postaci elektronicznej lub logicznie z nimi powiązane, **aby zapewnić autentyczność pochodzenia oraz integralność powiązanych danych.**

3.1. Kwalifikowane pieczęci elektroniczne jako narzędzia dla podmiotów prawnych w procesach biznesowych

Najbardziej charakterystyczną cechą pieczęci elektronicznej (w tym również naturalnie i kwalifikowanej) jest to, że **korzystać z niej mogą osoby prawne,** a więc firmy, organizacje czy instytucje.

Jest ona obok podpisu elektronicznego tworzona w wyniku działania usług zaufania, które mają umożliwić realizacje potwierdzenia pochodzenia i integralności dokumentu, który jest elektronicznie „pieczętowany". Kwalifikowana pieczęć elektroniczna jest pod względem konstrukcji prawnej i technicznej bardzo podobna do kwalifikowanego podpisu elektronicznego. **Nie jest** jednak odpowiednikiem podpisu elektronicznego osoby prawnej.

W obecnym stanie prawnym obowiązującym w Polsce kwalifikowana pieczęć elektroniczna nie pozwala na złożenie oświadczenia woli w postaci elektronicznej i nie zastępuje podpisu własnoręcznego.

Kwalifikowana pieczęć elektroniczna może zatem znaleźć zastosowanie wszędzie, gdzie trzeba zapewnić gwarancję integralności danych, gdzie trzeba zwiększyć bezpieczeństwo procesu archiwizacji i cyfryzacji papierowych dokumentów (dzięki tej usłudze możemy mieć pewność, że obie wersje są zgodne). Istotne jest, że za pomocą kwalifikowanej pieczęci elektronicznej można także zabezpieczać wewnętrzne dokumenty firmowe. Dzięki temu nie tylko potwierdzimy autentyczność dokumentów i integralność danych, ale ochronimy je przed sfałszowaniem.

Możliwości zastosowania kwalifikowanej pieczęci elektronicznej występują w wielu obszarach szczególnie takich jak finanse, sektor ubezpieczeń administracja publiczna, logistyka czy usługi medyczne.

Stosowanie pieczęci elektronicznej umożliwia wprowadzenie zautomatyzowanej i bezpiecznej komunikacji elektronicznej B2B i B2C. Pozwala również na długoterminowe zabezpieczenie przechowywanych dokumentów. Kwalifikowane pieczęci elektroniczne można użyć zarówno w dokumentach wysyłanych do kontrahentów, jak i w przypadku dokumentów wewnątrz firmy takich jak:

- Dokumenty seryjne, takie jak komunikaty, zestawienia kont, polisy ubezpieczeniowe itp.;
- Zawiadomienia instytucjonalne, jak potwierdzenia, zaświadczenia, certyfikaty, dyplomy;
- Dokumentacja medyczna pacjentów, w tym raporty wypisu i dokumenty medyczne;
- Akta prawne (np. przepisy prawa, regulacje);
- Dokumenty przedsiębiorstw regulaminy, dokumenty oraganizacyjne;
- Kontrakty oraz propozycje handlowe;
- E-faktury, rachunki, dowody zamówienia i dokumenty dostawy
- Obsługa kancelarii – dokumenty wychodząc i przychodzące,
- Zabezpieczenie akt pracowniczych – zabezpieczenie akt, zmiana postaci.

Wykorzystanie pieczęci ułatwia zautomatyzować procesy w systemach DMS lub ERP i usprawnić wiele czynności biznesowych w działach księgowości, sprzedaży, obsługi klienta i HR. Pozwala na obniżenie kosztów i oszczędność czasu przy obsłudze dokumentów, umożliwia oznaczanie wielu dokumentów równocześnie. Pozwala na mniejsze obciążenie administracyjne dzięki eliminacji czynności biurowych, w których wykorzystywany jest papier. Podnosi wiarygodność transakcji, służy bezpiecznej wymianie dokumentów z podmiotami wewnętrznymi i zewnętrznymi. Pieczęć pozwala na wykorzystanie pełnego zakresu wdrożonych już usług cyfrowych wreszcie wzmacnia profesjonalny wizerunek firmy korzystającej z innowacyjnych rozwiązań.

Ważnym przykładem wykorzystania pieczęci elektronicznej jest możliwość jej użycia w postępowaniu administracyjnym w zastępstwie podpisu elektronicznego. Zgodnie z przepisami Kodeksu postępowania administracyjnego, organy administracji publicznej mają możliwość wydawania pism w postaci elektronicznej przy użyciu systemów teleinformatycznych, opatrzonych kwalifikowaną pieczęcią elektroniczną. Pieczęć elektroniczna, jako zaawansowane narzędzie potwierdzania tożsamości organu wydającego dokument, gwarantuje, że pismo pochodzi od właściwego organu, a jego treść nie została zmieniona. Natomiast taki dokument zawiera w części tekstowej informacje o osobie, która sporządziła pismo. Dokumenty opatrzone kwalifikowaną pieczęcią elektroniczną nie muszą zawierać podpisu elektronicznego.

Pieczęć elektroniczna jest z powodzeniem stosowana także do potwierdzania odbioru pism w systemach administracji publicznej, gdzie urzędowe potwierdzenie odbioru jest realizowane w sposób automatyczny w momencie wpłynięcia pisma do urzędu i opatrywane pieczęcią elektroniczną urzędu. Dodatkowo we wszystkich usługach rejestrowanych doręczeń elektronicznych dowody nadania, udostępnienia oraz wydania przesyłek opatrywane są pieczęcią elektroniczną.

3.2. Wykorzystanie pieczęci elektronicznej w poszczególnych sektorach

DEPAPIERYZACJA PROCESU SPRZEDAŻY USŁUG TELEKOMUNIKACYJNYCH

Plus, wiodący polski operator telekomunikacyjny we współpracy z Asseco Data Systems oraz Samsung i Xtension zbudował nowy proces obsługi klienta w POS-ach. Sprzedaż usług odbywa się tam w pełni elektronicznie przy pomocy tabletu z oprogramowaniem zabezpieczającym sprzęt. Podpisane na nim dokumenty są opatrywane kwalifikowaną pieczęcią elektroniczną oraz kwalifikowanym elektronicznym znacznikiem czasu zgodnymi z europejskim rozporządzeniem eIDAS.

PIECZĘTOWANIE ONLINE DOKUMENTÓW BANKOWYCH

Pieczęć elektroniczna umożliwia pieczętowanie masowej korespondencji kierowanej do klientów banków lub generowanej automatycznie jak np. potwierdzenia transakcji przelewów. Spełnia również wymogi tzw. trwałego nośnika min. ze względu na to że dostawca usługi stanowi zaufaną stronę trzecią w relacjach bank – klient.

USE-CASE PARTNERA

Antony Skarlatos
Key Account Manager
Namirial

Transformacja Operacyjna Biznesu z Zaufanymi Rozwiązaniami Cyfrowymi

Cyfrowa transformacja zmienia współczesny krajobraz biznesowy, a integracja e-podpisów, e-pieczęci oraz rozwiązań eID jest kluczowa dla firm chcących zachować konkurencyjność. Innowacyjne narzędzia cyfrowe Namirial dostarczają organizacjom fundamenty do usprawnienia operacji, zabezpieczenia wrażliwych danych oraz pewnej nawigacji po złożonych wymaganiach regulacyjnych.

Dzięki wieloletniemu doświadczeniu we wspieraniu polskich firm w kluczowych sektorach, takich jak finanse, opieka zdrowotna i telekomunikacja, Namirial oferuje dopasowane rozwiązania, które odpowiadają zarówno na krajowe, jak i europejskie potrzeby w zakresie zgodności. Poprzez strategiczne partnerstwa z doświadczonymi polskimi firmami zapewniamy spełnienie lokalnych wymagań oraz skuteczne stawienie czoła szerszym wyzwaniom regulacyjnym w Europie.

Nasze zaawansowane rozwiązania, w tym Self ID i Video ID, wykorzystują technologię rozpoznawania twarzy opartą na sztucznej inteligencji, aby upraszczać i przyspieszać procesy KYC i AML, gwarantując szybkie, bezpieczne i niemalże odporne na oszustwa potwierdzenie tożsamości. Dodatkowo e-podpisy i e-pieczęcie Namirial odgrywają kluczową rolę w upraszczaniu zarządzania dokumentami i realizacji umów, zapewniając ich prawomocność oraz wspierając interoperacyjność transgraniczną — co jest kluczowe dla firm rozwijających działalność na skalę globalną.

Platforma Namirial, oparta na API i oferująca kompleksowe rozwiązania, integruje się bezproblemowo z istniejącymi infrastrukturami IT, zwiększając efektywność operacyjną, redukując koszty oraz wspierając przejście do przyszłości wolnej od papieru. Dzięki wdrożeniu cyfrowych rozwiązań Namirial polskie firmy odblokowują nowe możliwości wzrostu i innowacji, jednocześnie zapewniając zgodność z ewoluującymi standardami regulacyjnymi.

3.3. Zestawienie dostawców pieczęci elektronicznych

Podmiot	Nazwa rozwiązania	Opis rozwiązania
Asseco Data Systems	Kwalifikowana pieczęć elektroniczna Certum	Kwalifikowana pieczęć elektroniczna Certum jest dostępna w dwóch wariantach: zapisana na karcie włożonej do czytnika oraz w aplikacji mobilnej SimplySign. Pieczęć można bezproblemowo zintegrować z dowolnym systemem obiegu dokumentów/transakcji lub dowolnym systemem bankowości elektronicznej za pomocą API SimplySign, które jest prostym, szybkim i wydajnym rozwiązaniem, szczególnie dla sektora przedsiębiorstw. Możliwa do zastosowania w obiegu zewnętrznym jak i wewnętrznym firmy do uwierzytelnienia oraz zachowania integralności dokumentów (faktury, dokumentacja pracownicza, sprawozdania itp.).
Aruba S.p.A	Certyfikat kwalifikowanej pieczęci dla kart inteligentnych lub sprzętowych modułów bezpieczeństwa (HSM)	Idealne rozwiązanie dla organów publicznych, ponieważ umożliwia wydawanie zaświadczeń online, oszczędzając zasoby zarówno pod względem kosztów, jak i czasu. Rozwiązanie to jest doskonale zintegrowane ze wszystkimi rozwiązaniami do podpisu cyfrowego. Możliwa integracja aplikacji za pośrednictwem infrastruktury wirtualnej Aruba i interfejsów API dla wszystkich zdalnych podpisów cyfrowych.
Namirial Group	Pieczęć elektroniczna Namirial	Pieczęć elektroniczną Namirial można z łatwością stosować na wszelkiego rodzaju dokumentach, takich jak faktury, oficjalne zawiadomienia, oferty lub inne dokumenty wymagające zobowiązania ze strony firmy. Rozwiązanie certyfikuje każdy typ pliku (pliki tekstowe, pliki audio i wideo). Dostępne wersje z okresem ważności 1 lub 6 lat. Rozwiązanie dostępne z dedykowanym oprogramowaniem FirmaCerta. Działa bez dodatkowych urządzeń i bez żadnych kodów autoryzacyjnych do wprowadzenia.
KIR	Pieczęć elektroniczna Szafir	Pieczęć elektroniczna Szafir identyfikuje firmę, zapewnia integralność danych, uwierzytelnia nadawcę i spełnia wszelkie wymogi prawne. To optymalny sposób na szybkie i wiarygodne autoryzowanie oficjalnej korespondencji firmowej, dokumentów prawnych, dyplomów, legitymacji, zaświadczeń czy certyfikatów. Pieczęć elektroniczna wydawana jest na 1 rok lub dwa lata i oferowana jest w zestawie z kartą kryptograficzną (dużą lub SIM), oprogramowaniem oraz opcjonalnie czytnikiem kart kryptograficznych.
SIGNIUS S.A.	SIGNIUS Seal – kwalifikowana pieczęć elektroniczna	Rozwiązanie do kwalifikowanego zautomatyzowanego pieczętowania dokumentacji w zgodzie z eIDAS (certyfikat firmy Eurocert lub innego QTSP), dostępne w różnych modelach wdrożenia: jako usługa SaaS (w chmurze), dedykowana usługa w chmurze prywatnej oraz w modelu on-premise (wdrożenie lokalne).

Zestawienie zawiera jedynie dostawców, będących partnerami Trusted Economy Forum CommonSign 2024

SIGNIUS

Podpisy i pieczęcie elektroniczne

Oferujemy rozwiązania do zdalnego podpisywania i pieczętowania dokumentów oraz budowania wiarygodności online

Dla organizacji każdej wielkości, w różnych modelach wdrożenia (SaaS, API, on-premise)

Zaufali nam:

orange energia · MONDI WIĘCEJ NIŻ PRACA · worktrips.com · INC DOM MAKLERSKI · Jobman Group your choice, your job · PARETTI

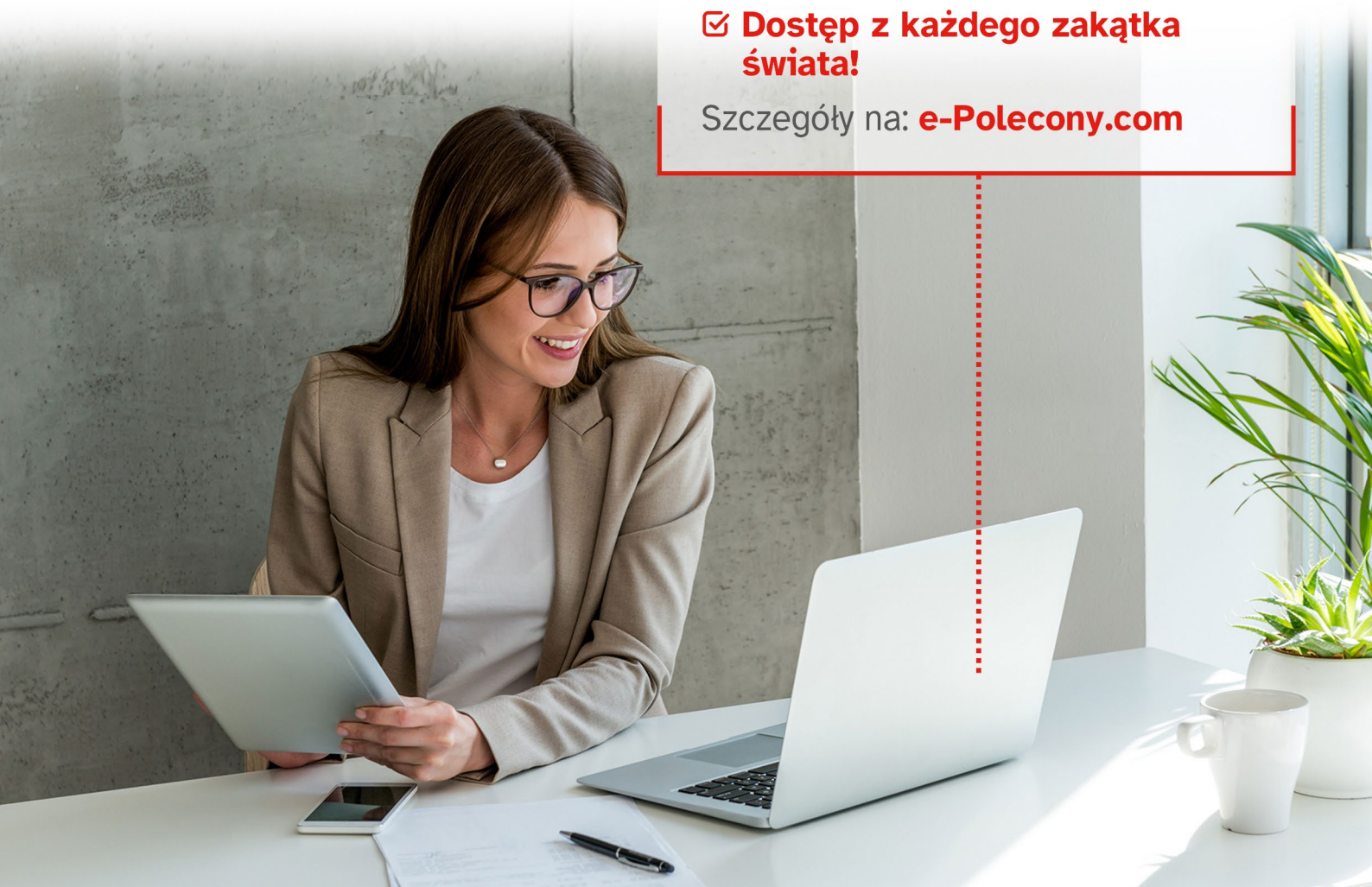
Poczta Polska

e-Polecony

Odbieraj i wysyłaj **listy polecone** bezpiecznie w wersji cyfrowej.

- **Bez Awizo.**
- **Dostarczenie w kilka sekund.**
- **Szybko i wygodnie.**
- **Dostęp z każdego zakątka świata!**

Szczegóły na: **e-Polecony.com**



Autorzy raportu

Miłosz Brakoniecki,
Sławomir Hadryan,
Dominika Rzęsa,
Piotr Sterczała,
Michał Tabor.

Nota prawna

Opinie zawarte w raporcie wydane zostały na podstawie wiedzy pozyskanej z badania rynku i doświadczenia autorów raportu. Autorzy nie biorą odpowiedzialności za decyzje podjęte na podstawie opinii wydanych w ramach raportu „ZDALNE POTWIERDZANIE TOŻSAMOŚCI, E-PODPIS I E-PIECZĘĆ W BIZNESOWEJ PRAKTYCE"