RAPORT ANALITYCZNY

KONSEKWENCJE WPROWADZENIA W ROZPORZĄDZENIU PARLAMENTU EUROPEJSKIEGO I RADY (UE) 2024/1183 Z DNIA 11 KWIETNIA 2024 R. W SPRAWIE ZMIANY ROZPORZĄDZENIE (UE) NR 910/2014 W ODNIESIENIU DO USTANOWIENIA EUROPEJSKICH RAM TOŻSAMOŚCI CYFROWEJ (TZW. EIDAS2) DOKUMENTU 3.0 DLA UMÓW BANKOWYCH

SYGN. PAB/WIB 21/2024

ISBN 978-83-973493-3-9

Raport opracowany na zlecenie Programu Analityczno-Badawczego Fundacji Warszawski Instytut Bankowości

PROGRAM ANALITYCZNO BADAWCZY

Warszawa, grudzień 2024

O Raporcie

Raport **Konsekwencje wprowadzenia w Rozporządzeniu Parlamentu Europejskiego i Rady (UE) 2024/1183 z dnia 11 kwietnia 2024 r w sprawie zmiany rozporządzenie (UE) nr 910/2014 w odniesieniu do ustanowienia europejskich ram tożsamości cyfrowej (tzw. eIDAS2) dokumentu 3.0 dla umów bankowych** został opracowany na zlecenie Programu Analityczno-Badawczego Fundacji Warszawski Instytut Bankowości.

Autorzy:

Raport przygotowany przez zespół w składzie:

dr hab. prof. UŚ Daiusz Szostek (redakcja i autor)
– profesor Uniwersytetu Śląskiego, założyciel Szostek_Digital i Wspólnicy. Realizator projektów Horizon 2020 związanych z innowacjami w przemyśle – SHOP4CF i MAS4AI. Autor licznych książek i opracowań w zakresie prawa nowych technologii – „Legal tech. Czyli jak bezpiecznie korzystać z narzędzi informatycznych w organizacji, w tym w kancelarii oraz dziale prawnym"; „Blockhcian i Prawo", „Bezpieczeństwo danych i IT" i inne. Inicjator serii metodyk związanych z technologią i prawem w wydawnictwie C.H. Beck. Członek licznych projektów w zakresie cyfryzacji. Założycie wyjątkowego w skali kraju, i nagradzanego konsorcjum CYBER SCIENCE – Śląskiego Centrum Inżynierii Prawa, Technologii i Kompetencji Cyfrowych, zrzeszającego Uniwersytet Śląski, Politechnikę Śląską, Uniwersytet Ekonomiczny w Katowicach, NASK i EMAG Łukasiewicza. Działacz w zakresie zarządzania Internetem, członek rady programowej IGF Poland. Popularyzator wiedzy w zakresie Blockchian – członek Blockhaton EUiPO oraz autor między innymi Blockchain i Prawo (w wersji angielskiej Blockchain and law wyd Nomos). Ekspert kadencji 2020-2024 Obserwatorium Parlamentu Europejskiego ds Sztucznej inteligencji. Przewodniczący Komisji ds. Cyberbezpieczeństwa KRASP (kadencja 2024-2028 r.).

Rafał Tomasz Prabucki
– doktor nauk prawnych i inżynier. COO w Szostek_Digital i wspólnicy. Auditor wiodący ISO/IEC 27001, BCMS ISO 22301 oraz ISO/IEC 42001/2023. Posiadacz tytułu Certified in Cybersecurity (CC) wydanym przez (ISC)². Adiunkt na Uniwersytecie Śląskim. Członek CYBER SCIENCE i SABI. Założyciel LegalHackers Katowice. Asystent w zakończonych projektach dotyczących wykorzystania nowych technologii w przemyśle: MAS4AI na Uniwersytecie Śląskim i SHOP4CF na Uniwersytecie Opolskim. Alumn stypendiów w Polsce, Hiszpani i Niemczech. Prowadzący wykłady na Uczelniach w Polsce, Litwie i we Francji. Kierownik studiów podyplomowych „Tokenizacja i automatyzacja procesów w gospodarce cyfrowej" na Uniwersytecie Śląskim. Autor książek i komentarzy, uczestnik Hackathonów i konkursów na innowacje – finalista w Młodzi i Innowacyjni dla PGNiG w 2017 roku oraz drugie miejsce w #hack4law w edycji z 2024 roku.

Mateusz Jakubik
– prawnik, Compliance Officer w Bonnier Business Polska oraz CTO w Szostek_Digital i wspólnicy. Auditor wiodący norm ISO/IEC 27001, BCMS ISO 22301 oraz ISO/IEC 42001:2023, a także auditor wewnętrzny ISO 27701. Specjalizuje się w ochronie danych osobowych, nowych technologiach i cyberbezpieczeństwie, prowadząc wykłady i szkolenia w tych dziedzinach. Doświadczenie zawodowe zdobywał m.in. w renomowanej warszawskiej kancelarii specjalizującej się w obszarze ochrony danych osobowych. Obecnie pełni funkcję Inspektora Ochrony Danych w jednostkach sektora publicznego i prywatnego, a także odpowiadał za obszar ochrony danych osobowych w spółce Skarbu Państwa z branży energetycznej. W pracy naukowej i zawodowej łączy wiedzę prawniczą z zakresu ochrony danych osobowych i prawa nowych technologii, koncentrując się na zagadnieniach IT oraz cyberbezpieczeństwa. Autor licznych publikacji, uczestnik Hackathonów i konkursów na innowacje – drugie miejsce w #hack4law w edycji z 2024 roku.

PROGRAM ANALITYCZNO BADAWCZY

O Programie

Program Analityczno-Badawczy przy Fundacji Warszawski Instytut Bankowości powstał w 2019 r. jako odpowiedź na potrzeby sektora bankowego w zakresie wysokiej jakości analiz i badań z obszaru cyberbezpieczeństwa i nowych technologii, a także szeroko rozumianego otoczenia sektora bankowego, kształtującego warunki działania banków w Polsce. Prace analityczno-badawcze w ramach programu realizowane są pod kątem możliwości praktycznego wykorzystania wyników w celu rozwoju sektora bankowego, podnoszenia poziomu bezpieczeństwa usług oraz – w ostateczności – kreowania wartości dla klientów końcowych – użytkowników bankowości.

W ramach programu realizowane są analizy i badania w następujących obszarach:

- Nowe technologie w sektorze bankowym, cyberbezpieczeństwo banków i systemy płatnicze
- Ekonomiczna analiza rozwoju sektora bankowego, stabilności banków, otoczenia makroekonomicznego
- Prawno-regulacyjne i legislacyjne uwarunkowania działalności sektora bankowego oraz wyzwania wynikające z orzecznictwa sądów krajowych i europejskich
- ESG i sustainable finance
- Prace analityczno-badawcze w zakresie poszczególnych obszarów funkcjonowania banków oraz w zakresie funkcjonowania wskaźników referencyjnych

Więcej na temat działalności programu na stronie www.pabwib.pl

Kontakt:

dr Tomasz Pawlonka
Dyrektor Programu
m: 505 917 778
e: tpawlonka@wib.org.pl

Warszawski Instytut Bankowości
00-380 Warszawa, ul. Kruczkowskiego 8
t: (22) 182 31 70
e: pab@wib.org.pl

Agnieszka Nierodka
m: 607 484 391
e: anierodka@wib.org.pl

dr Agnieszka Wicha
m: 661 646 474
e: agnieszka.wicha@zbp.pl

Bartosz Przyborowski
m: 795 933 104
e: bartosz.przyborowski@zbp.pl

Spis treści

Wykaz skrótów

eIDAS – Electronic Identification, Authentication and Trust Services (Rozporządzenie UE dotyczące identyfikacji elektronicznej i usług zaufania)

DLT – Distributed Ledger Technology (Technologia rozproszonego rejestru)

DLT Pilot – Rozporządzenie Pilotażowe DLT

AI Act – Artificial Intelligence Act (Akt prawny UE dotyczący regulacji sztucznej inteligencji)

NIS 2 – Network and Information Security Directive (Dyrektywa dotycząca bezpieczeństwa sieci i informacji)

NFT – non-fungible token (niezamienny/ niewymienialny token)

RODO – Rozporządzenie o Ochronie Danych Osobowych (Ogólne rozporządzenie o ochronie danych osobowych, znane jako GDPR)

GDPR – General Data Protection Regulation (Ogólne rozporządzenie o ochronie danych osobowych, RODO)

MiCA – Markets in Crypto-Assets (Rozporządzenie UE dotyczące rynku aktywów kryptograficznych)

DORA – Digital Operational Resilience Act (Rozporządzenie dotyczące cyfrowej odporności operacyjnej)

ICT – Information and Communication Technology (Technologie informacyjno-komunikacyjne)

MSP – Małe i Średnie Przedsiębiorstwa

EU – European Union (Unia Europejska)

EU Wallet – European Digital Identity Wallet (Europejski Portfel Tożsamości Cyfrowej)

ESMA – European Securities and Markets Authority (Europejski Urząd Nadzoru Giełd i Papierów Wartościowych)

SSI – Self-Sovereign Identity (Tożsamość cyfrowa)

AI – Artificial Intelligence (Sztuczna inteligencja)

PSD2 – Payment Services Directive 2 (Dyrektywa UE w sprawie usług płatniczych)

KPI – Key Performance Indicators (Kluczowe wskaźniki efektywności)

Źródła prawa

1. Rozporządzenie eIDAS
   - **Pełna nazwa:** Rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 910/2014 z dnia 23 lipca 2014 r. w sprawie identyfikacji elektronicznej i usług zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznym.
   - **Dziennik Urzędowy UE:** L 257 z 28.8.2014,

2. **eIDAS 2** – Zmiana rozporządzenia eIDAS
   - **Pełna nazwa:** Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2024/1183 z dnia 11 kwietnia 2024 r. zmieniające rozporządzenie (UE) nr 910/2014 w odniesieniu do ustanowienia europejskich ram tożsamości cyfrowej.
   - **Dziennik Urzędowy UE:** Dz.U. L1183 z 30.4.2024

3. RODO (GDPR)
   - **Pełna nazwa:** Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych (ogólne rozporządzenie o ochronie danych).
   - **Dziennik Urzędowy UE:** L 119 z 4.5.2016,

4. **AI Act**
   - **Pełna nazwa:** Rozporządzenie Parlamentu Europejskiego i Rady w sprawie zharmonizowanych przepisów dotyczących sztucznej inteligencji i zmiany rozporządzeń 9WE) nr 300/2008 (UE) nr 167/2013, (UE) nr 168/2013, (UE) 2018/858, (UE) 2018/1139 i (UE) 2019/2144 oraz dyrektyw 2014/90/UE, (UE) 2016/797 i (UE) 2020/1828 (AI ACT) z dnia 13 czerwca 2024r
   - **Dziennik Urzędowy UE:** L 1689 z 12.7.2024

5. Dyrektywa NIS 2
   - **Pełna nazwa:** Dyrektywa Parlamentu Europejskiego i Rady (UE) 2022/2555 z dnia 14 grudnia 2022 r. w sprawie środków na rzecz zapewnienia wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych w Unii (Dyrektywa NIS2).
   - **Dziennik Urzędowy UE:** L 333 z 27.12.2022

6. MiCA (Markets in Crypto-Assets Regulation)
   - **Pełna nazwa:** Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2023/1114 z dnia 31 maja 2023 r. w sprawie rynków kryptowalutowych i kryptoaktywów.
   - **Dziennik Urzędowy UE:** L 150 z 9.6.2023,

7. DORA (Digital Operational Resilience Act)
   - **Pełna nazwa:** Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2022/2554 z dnia 14 grudnia 2022 r. w sprawie cyfrowej odporności operacyjnej sektora finansowego.
   - **Dziennik Urzędowy UE:** L 333 z 27.12.2022,

8. Dyrektywa PSD2
   - **Pełna nazwa:** Dyrektywa Parlamentu Europejskiego i Rady (UE) 2015/2366 z dnia 25 listopada 2015 r. w sprawie usług płatniczych w ramach rynku wewnętrznego.
   - **Dziennik Urzędowy UE:** L 337 z 23.12.2015,

9. DLT Pilot
   - **Pełna nazwa:** Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2022/858 z dnia 30 maja 2022 r. w sprawie systemu pilotażowego na potrzeby infrastruktur rynkowych opartych na technologii rozproszonego rejestru, a także zmiany rozporządzeń (UE) nr 600/2014 i (UE) nr 909/2014 oraz dyrektywy 2014/65/UE.
   - **Dziennik urzędowy:** L 151/1 z 02.06.2023,

10. MFiD II
    - **Pełna nazwa:** Dyrektywa Parlamentu Europejskiego i rady 2014/65/UE z dnia 15 maja 2014 r. w sprawie rynków instrumentów finansowych oraz zmieniająca dyrektywę 2002/92/we i dyrektywę 2011/61/UE.
    - **Dziennik urzędowy:** L 173/349 z 12.06.2014,

Wprowadzenie

Rozporządzenie eIDAS Parlamentu Europejskiego (UE) nr 910/2014 w sprawie identyfikacji elektronicznej i usług zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznym (eIDAS) z 27 lipca 2014[1] ma już 10 lat. „Przyjmując w 2014 r. rozporządzenie eIDAS, UE otworzyła nowe możliwości, regulując pierwsze transgraniczne ramy dla wiarygodnej tożsamości cyfrowej i usług zaufania, które w chwili obecnej są uznane i przestrzegane na całym świecie. Rozporządzenie eIDAS miało umożliwić wszystkim obywatelom Unii uzyskanie dostępu do usług publicznych w całej UE przy użyciu środków identyfikacji elektronicznej wydawanych w kraju pochodzenia. Celem tego rozporządzenia było zwiększenie zaufania do transakcji elektronicznych na rynku wewnętrznym poprzez zapewnienie wspólnej podstawy bezpiecznej i ciągłej interakcji elektronicznej między obywatelami, przedsiębiorstwami i organami publicznymi, co miało pozwolić podnieść efektywność publicznych i prywatnych usług online, e-biznesu i e-handlu w Unii”[2].

Utworzone ramy dla usług zaufanych oraz ich kwalifikowanych odpowiedników, ówcześnie rewolucyjne, w chwili obecnej nie są już wystarczającą podstawą dla realizacji celów Unii Europejskiej na najbliższe lata – utworzenia jednolitej, transparentnej, interoperacyjnej, a przede wszystkim bezpiecznej gospodarki cyfrowej. eIDAS1 wprowadził zmiany pozwalające w Europie na digitalizację zasobów oraz przejście z dokumentów tradycyjnych (dokument 1.0) na dokumenty w postaci elektronicznej (dokument 2.0). Ówczesne, nowatorskie ujęcie dokumentu elektronicznego (m.in. nie tylko jako tekst, ale także jako obraz, dźwięk czy multimedia), domniemanie z nimi powiązane, wprowadzenie kwalifikowanych usług zaufanych wraz z domniemaniami prawnymi (dotyczącymi m.in. kwalifikowanego podpisu elektronicznego, kwalifikowanej pieczęci elektronicznej, kwalifikowanego doręczenia elektronicznego czy certyfikacji witryn internetowych bądź walidacji usług zaufanych) zmieniło europejski obraz i legislację w odniesieniu do dokumentów elektronicznych, istotnie wpłynęło na postępowania dowodowe związane z dowodami z dokumentów elektronicznych, wprowadziło jednolite europejskie zasady, ale także istotnie wpłynęło na krajowe zasady postępowania dowodowego z dokumentem elektronicznym, niezależnie – a czasami wbrew lokalnym – konserwatywnym regulacjom. Jak istotne dla Europy i europejskiego obrotu gospodarczego były to zmiany, uwidoczniło się w okresie pandemii Covid-19, kiedy cała Europa, przedsiębiorcy, administracja a także konsumenci nagle zostali zobligowani do pełnego, wyłącznie elektronicznego obiegu dokumentów i pracy zdalnej. I w taki też sposób zwierano umowy. Bez podstaw prawnych wynikających z eIDAS byłoby to niemożliwe, a przynajmniej bardzo utrudnione. Olbrzymie znaczenie miała też wówczas działalność banków, możliwości zawierania umów online, wykorzystanie w Polsce bankowości elektronicznej dla potwierdzania profilu zaufanego itd. Bez banków i instytucji finansowych byłoby o wiele trudniej przejść przez pandemię.

eIDAS1 umożliwił konwersję dokumentu tradycyjnego w dokument elektroniczny i zastąpienie obiegu tradycyjnego obiegiem elektronicznym, a podpis tradycyjny – kwalifikowanym podpisem elektronicznym.

Ostatnia dekada to istotna zmiana technologiczna i rozwój gospodarki cyfrowej opierającej się o nowe technologie, takie jak DLT (Distributed Ledger Technology) – technologię rozproszonego rejestru, blockchain, wykorzystanie smart contracts, tokenizację procesów (wykorzystanie w procesie transakcyjnym tokenów, także do przenoszenia wartości) i ich automatyzację. Dotychczasowe usługi zaufane i ich kwalifikowane odpowiedniki okazały się niewystarczające dla nowoczesnego obrotu oraz nowego rynku cyfrowego. W chwili obecnej przeżywamy intensywny rozwój algorytmów czy też programów samouczących się o pewnym poziomie autonomii, funkcjonujących w ramach systemów AI, a przed nami wdrożenie rozporządzenia AI Act[3], a także cały pakiet przepisów

[1] DzU EU L257/73 z 28 sierpnia 2014r.

[2] Sprawozdanie Komisji dla Parlamentu Europejskiego i Rady w w sprawie oceny rozporządzenia numer 910/2014 w sprawie identyfikacji elektronicznej i usług zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznym. COM (2021) 290 final

[3] Rozporządzenie Parlamentu Europejskiego i Rady 2024/1689 z 13 czerwca 2024 r w sprawie ustanowienia zharmonizowanych przepisów dotyczących sztucznej inteligencji

dotyczących bezpieczeństwa, bezpieczeństwa informacji, cyberbezpieczeństwa, podatności systemów – takich jak rozporządzenie DORA[4], rozporządzenie MiCA[5] czy implementacja dyrektywy NIS 2[6] i inne. Rozporządzenie eIDAS2 jest istotnym i bardzo ważnym uzupełnieniem powyższego pakietu, w sporej mierze będąc łącznikiem pomiędzy tymi aktami, mającym znaczenie dla nowego obiegu dokumentów, ale także do sposobu zawierania umów – w tym przez banki i instytucje finansowe.

Istotny wpływ na konieczność zmiany rozporządzenia eIDAS miała praca i raport dr Michele Finck (Max Planc Instytut) „Blockchain and the General Data Protection Regulation. Cam distributed ledgers be squared with European data protection Law" (2019 r.)[7] w którym wykazano problem, a właściwie niezgodność tradycyjnie ujmowanego zapisu w blockchain i jego nieusuwalności oraz wymogu przepisów RODO dotyczących konieczności usuwania danych po upływie czasu, jaki jest konieczny dla ich przechowywania, prawa do bycia zapomnianym, weryfikacji i modyfikacji danych osobowych itd. W raporcie zaproponowano, aby „wyciągnąć" dane osobowe poza blockchain do odrębnych baz danych, łącząc je algorytmem z zapisem transakcji czy też innej operacji w technologii blockchain. Komisja Europejska uwzględniła ten postulat w pracach nad eIDAS 2, EU Wallet oraz European ID, tworząc tym samym podwaliny pod nową europejską gospodarkę cyfrową.

Zgodnie z zasadami legislacyjnymi UE, 5 lat po wejściu w życie przepisów eIDAS (wszedł w życie 1 lipca 2016 r.) opublikowano sprawozdanie Komisji dla Parlamentu Europejskiego i Rady w sprawie oceny rozporządzenia numer 910/2014 w sprawie identyfikacji elektronicznej i usług zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznym[8]. Zauważono, iż eIDAS1 nie przewidywał obowiązku notyfikowania krajowych systemów identyfikacji elektronicznej (pozostawiając w tym zakresie dowolność państwom), koncentrował się głównie na sektorze publicznym oraz nie miał poważniejszych zachęt dla korzystania z systemów identyfikacji elektronicznej przez podmioty prywatne. Poważnym problemem było to, że europejski ekosystem tożsamości elektronicznej był, a właściwie dalej jest rozproszony między różne krajowe otoczenia regulacyjne, różne poziomy administracji cyfrowej czy kultury cyfrowej oraz zróżnicowane poziomy zaufania do instytucji publicznych. Założono przy tym, iż podmioty prywatne takie jak banki, dostawcy usług łączności elektronicznej, które zobowiązane są do gromadzenia atrybutów umożliwiających identyfikację, będą coraz częściej wykorzystywać potencjał swoich procedur, aby występować w charakterze zweryfikowanych dostawców tożsamości. Dokonało się to co najwyżej lokalnie i w ograniczonym zakresie.

Istotne, ale także niebezpieczne dla obrotu cyfrowego w Unii Europejskiej jest to, iż w chwili obecnej pośrednicy internetowi, w tym duże platformy mediów społecznościowych i przeglądarki internetowe, a nie banki i instytucje finansowe jak zakładano, występują jako faktyczni dostawcy tożsamości cyfrowej dla uwierzytelniania w ramach usług zewnętrznych za pomocą swoich profili użytkowników. Przykładem mogą być platformy Facebook czy Google, które stały się podmiotami uwierzytelniającymi tożsamość (zob. rys. 1)[9], gdzie wygoda rozwiązania jest akceptowalna przez miliony obywateli Unii Europejskiej nawet kosztem utraty kontroli nad ujawnionymi danymi osobowymi, co wpływa na zagrożenie dla cyberbezpieczeństwa. Z badań Eurobarometr[10] wynika, iż obywatele Unii Europejskiej, a przynajmniej znaczna ich większość, chciałaby mieć dostęp do bezpiecznej tożsamości cyfrowej, za pomocą której mogliby uzyskiwać dostęp do usług online. Bezpieczna identyfikacja elektroniczna i wymiana danych uwierzytelniających opierających się na atrybutach ma coraz to większe znaczenie wraz ze wzrostem ilości usług wymagających potwierdzenia tożsamości. Zapewnienie tożsamości cyfrowej stanowi element strategiczny dla cyberbezpieczeństwa w Unii Europejskiej. Obywatele Unii Europejskiej oczekują możliwości cyfrowej identyfikacji począwszy od logowania się do platform internetowych, co dzisiaj zapewniają im prywatni dostawcy jak Facebook i Google (Rys. 1), ale poprzez możliwość użycia danych pseudonimicznych, po bezpieczną identyfikację dla korzystania z usług e-zdrowia, ale także usług bankowych, w tym zawierania w ten sposób umów.

[4] Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2022/2554 z 14 grudnia 2022 r w sprawie operacyjnej odporności sektora finansowego Dz.U L33/1

[5] Rozporządzenie Parlamentu Europejskiego i Rady 2023/1114 z dnia 31 maja 2023 w sprawie rynków kryptoaktywów Dz.U L 150/40

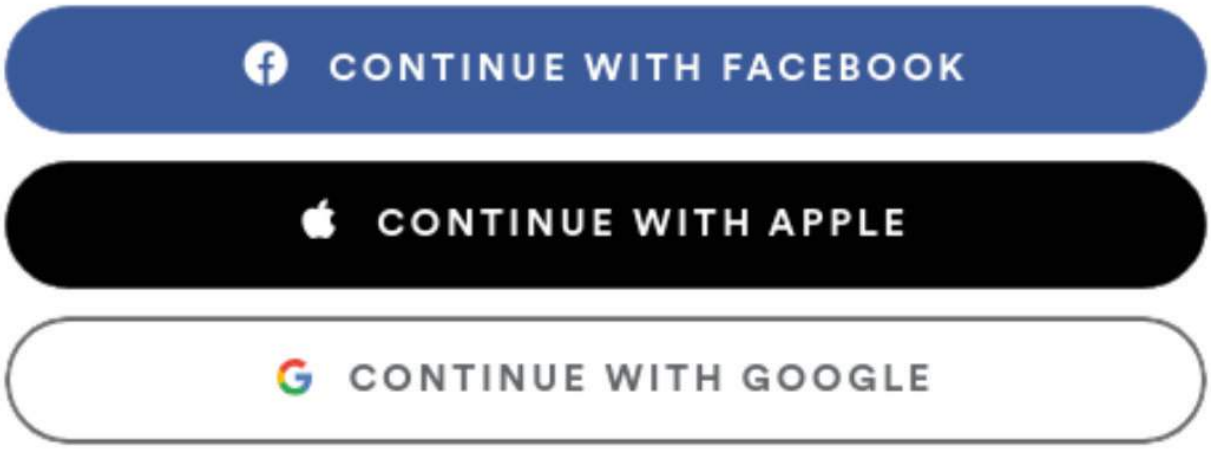
[6] Dyrektywa Parlamentu Europejskiego i Rady (UE) 2022/2555 z dnia 14 grudnia 2022r w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa na terytorium UE Dz.U L 333/80

[7] https://www.europarl.europa.eu/RegData/etudes/STUD/2019/634445/EPRS_STU(2019)634445_EN.pdf pobrano 15 lipca 2024r.

[8] COM (2021) 290 final

[9] Są to technologie „dostawców tożsamości", zob.: https://cert.pl/posts/2022/01/kompleksowo-o-haslach/

[10] Badanie Eurobarometr 503: Postawy wobec wpływu cyfryzacji na życie codzienne, grudzień 2019 r., zob.: https://ec.europa.eu/commfrontoffice/publicopinion/index.cfm/Survey/getSurveyDetail/instruments/SPECIAL/surveyKy/2228. Pobrano 15 lipca 2024 r.



Rys. 1. Przykład guzików „dostawców tożsamości", jako alternatywa dla hasła w procesie autoryzacji.
Źródło: https://cert.pl/posts/2022/01/kompleksowo-o-haslach/.

„W orędziu o stanie Unii z dnia 16 września 2020 r. przewodnicząca Komisji Europejskiej ogłosiła, że celem Komisji jest zapewnienie bezpiecznej i wiarygodnej tożsamości cyfrowej wszystkim obywatelom UE: „Chcemy zestawu przepisów, które będą ukierunkowane na ludzi.(...) Obejmuje to także kontrolę nad naszymi danymi osobowymi, której dziś wciąż brakuje. Za każdym razem, gdy aplikacja lub strona internetowa prosi nas o stworzenie nowej tożsamości cyfrowej lub o łatwe zalogowanie się na dużej platformie, nie mamy pojęcia, co w rzeczywistości dzieje się z naszymi danymi. Dlatego też Komisja wkrótce zaproponuje bezpieczną europejską tożsamość elektroniczną. Taką, której będziemy mogli zaufać i z której każdy obywatel będzie mógł skorzystać z każdego miejsca w Europie, aby na przykład zapłacić podatki czy wynająć rower. Mówimy o technologii, w ramach której sami możemy kontrolować, jakie dane są wykorzystywane i w jaki sposób[11]".

W sprawozdaniu wskazano, iż pomimo wprowadzenia odniesień do rozwiązań eIDAS w szeregu sektorowych przepisów UE, to w praktyce nie zapewniono rozwiązań dostosowanych do potrzeb występujących w konkretnych i bardzo ważnych sektorach, jak na przykład bankowość czy też edukacja. Jednym z czynników ograniczających jest brak szczególnych atrybutów w podziale na dziedziny. Wskazano na potrzebę umożliwienia zarówno obywatelom, jak i przedsiębiorstwom cyfrowych poświadczeń swojej tożsamości lub swoich atrybutów bez konieczności przedstawiania dokumentów w postaci fizycznej. Współczesny rynek, a także gospodarka cyfrowa wymagają zapewnienia szczególnych atrybutów powiązanych z daną osobą, a nie tylko sztywnych ram tożsamości cyfrowych, z jakimi dotychczas mieliśmy do czynienia.

Te wszystkie przedstawione powyżej argumenty, stanowią podstawę dla nowego ujęcia dokumentu. Już nie tradycyjnego, jak dokument 1.0, czy jego cyfrowy odpowiednik – dokument 2.0, ale nowego, opartego o danatyzację[12] procesów, tak zwanego dokumentu 3.0. Zmiany te, ale przede wszystkim wejście w życie przepisów eIDAS 2 wpłyną w istotny sposób na funkcjonowanie banków i innych instytucji finansowych, a także na sposób zawierania przez nie umów. Nowe ujęcie dokumentu uwzględnia nie tylko potrzeby rynku, ale przede wszystkim bezpieczeństwo tożsamości cyfrowej, cyberbezpieczeństwo, a także pewność obrotu, w tym zgodność z przepisami RODO.

[11] Sprawozdanie Komisji dla Parlamentu Europejskiego i Rady w w sprawie oceny rozporządzenia numer 910/2014 w sprawie identyfikacji elektronicznej i usług zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznym.

[12] Nazywane też danyfikacją, lub też także datyfikacją (z ang. Datafication) – pozyskiwanie danych z różnych źródeł (systemów informatycznych), w miejsce tradycyjnego dokumentu. Dane a nie tradycyjny dokument (1.0).

Droga do Cyfrowej Dekady – polityka UE i jej wpływ na działalność banków i nowe usługi

W dniu 5 grudnia 2022 Ursula von der Leyen wraz z przewodniczącą Parlamentu Europejskiego Robertą Metsolą podpisały „Europejską deklarację praw i zasad cyfrowych w cyfrowej dekadzie" (2023/C 23/01)[13].

W ramach dokumentu ustalono sześć podstawowych zasad: 1. Ukierunkowanie transformacji cyfrowej na człowieka; 2. Wspieranie solidarności i wykluczenia społecznego poprzez łączność, edukację cyfrową, szkolenia i umiejętności, uczciwe i sprawiedliwe warunki pracy oraz dostęp do cyfrowych usług publicznych online; 3. Potwierdzenie znaczenia wolności wyboru i sprawiedliwego środowiska cyfrowego; 4. Wspieranie udziału społeczeństwa w przestrzeni publicznej; 5. Zwiększenie bezpieczeństwa, ochrony i upodmiotowienia w środowisku cyfrowym, przede wszystkim w przypadku młodych ludzi; 6. Promowanie zrównoważonego rozwoju.

Deklaracja jest uzupełnieniem przyjętej wcześniej decyzją Parlamentu Europejskiego i Rady (UE) 2022/2481 z dnia 14 grudnia 2022 r. programu polityki „Droga ku cyfrowej dekadzie" do 2030 r. (tekst mający znaczenie dla EOG)[14], która jest podstawową polityką UE w zakresie nie tylko cyfryzacji, ale także legislacji w tym zakresie. Jej konsekwencją jest m.in. wyżej wzmiankowana zmiana rozporządzenia eIDAS. Polityka, ale przede wszystkim idące za nią zmiany prawne oraz zmiana „filozofii" działania europejskiego rynku cyfrowego, wpłynie także na działania banków, o czym szerzej poniżej.

Jako cele ogólne dokument wskazuje: a) promowanie skoncentrowanego na człowieku i opartego na prawach podstawowych, inkluzywnego, przejrzystego i otwartego środowiska cyfrowego, w tym bezpieczne i interoperacyjne technologie oraz usługi cyfrowe zgodne z zasadami, prawami i wartościami Unii, które je wzmacniają; b) wzmocnienie zbiorowej odporności państw członkowskich i niwelowanie przepaści cyfrowej, osiągnięcie równowagi płci i równowagi geograficznej w zakresie zaawansowanych umiejętności i kompetencji cyfrowych, c) zapewnienie strategicznej cyfrowej suwerenności Unii z zachowaniem otwartości, w szczególności poprzez bezpieczną i dostępną infrastrukturę cyfrową i infrastrukturę danych zdolne do efektywnego przechowywania, przesyłania i przetwarzania bardzo dużej ilości danych; d) promowanie wprowadzania i wykorzystywania zdolności cyfrowych z myślą o zmniejszeniu przepaści cyfrowej w celu osiągnięcia wysokiego wskaźnika wykorzystania technologii cyfrowych i innowacji w przedsiębiorstwach unijnych, w szczególności MSP; e) opracowanie kompleksowego i zrównoważonego ekosystemu interoperacyjności infrastruktury cyfrowej, w której obliczenia wielkiej skali, przetwarzanie brzegowe, przetwarzanie w chmurze, obliczenia kwantowe, AI, zarządzanie danymi i konektywność sieciowa działają w sposób jednolity (tak, aby UE dysponowała konkurencyjną, bezpieczną i zrównoważoną chmurą o wysokich standardach bezpieczeństwa i prywatności), f) promowanie unijnego cyfrowego otoczenia regulacyjnego, g) poprawa odporności na cyberataki, przyczynianie się do zwiększenia świadomości ryzyka i szerzenia wiedzy na temat procedur cyberbezpieczeństwa.

W artykule czwartym polityki wskazano na bardziej szczegółowe cele, tzw. cele cyfrowe, dzieląc je na cztery obszary: społeczeństwo, infrastruktura, transformacja cyfrowa przedsiębiorstw oraz cyfryzacja usług publicznych. W każdym z tych obszarów w sposób bezpośredni lub pośredni będą miały wpływ banki, chociażby poprzez dostęp do infrastruktury czy też swoje usługi, jak również ze względu na konieczność uwzględniania (a co za tym idzie – promowania) europejskiej tożsamości cyfrowej w EU Wallet.

W ramach obszaru „społeczeństwo" celem jest podniesienie kwalifikacji cyfrowej społeczeństwa i wyedukowanie wysoko wykwalifikowanych profesjonalistów (20 mln specjalistów w dziedzinie ICT) poprzez podniesienie kompetencji cyfrowych wśród społeczeństwa, aby do 2030 r. 80% osób w wieku 16-74 lat posiadało przynajmniej podstawowe umiejętności cyfrowe. W obszarze „infrastruktura" celami są: objęcie wszystkich użytkowników końcowych przebywających w stałej lokalizacji siecią gigabajtową, aż do punktu zakończenia sieci, a wszystkie obszary zaludnione ultraszybką siecią nowej generacji o wydajności dorównującej 5G zgodnie z zasadą neutralności technologicznej; rozwój produkcji najnowocześniejszych półprzewodników w UE, aby stanowiła co najmniej 20% wartości produkcji światowej; co najmniej 10 tys. neutralnych dla klimatu węzłów brzegowych (zdolności w zakresie rozproszonego przetwarzania danych podłączone do sieci i zlokalizowane blisko fizycznego punktu końcowego lub fizycznie w punkcie końcowym, gdzie generowane są dane, które to zdolności umożliwiają obliczenia rozproszone i przechowywanie rozproszone na potrzeby przetwarzania danych charakteryzujące się niskim opóźnieniem – art. 2 pkt. 6 polityki) gwarantujących wysoki stopień bezpieczeństwa i rozmieszczonych w sposób gwarantujący dostęp z danymi usług charakteryzujący się niskim opóźnieniem (milisekundy) niezależnie od lokalizacji przedsiębiorstwa, a co za tym idzie promocja na poziomie unijnym rozproszonego sposobu zapisywania danych w tym DLT; podniesienie zdolności

[13] https://eur-lex.europa.eu/legal-content/PL/TXT/PDF/?uri=CELEX:32023C0123(01).

[14] https://sip.lex.pl/akty-prawne/dzienniki-UE/decyzja-2022-2481-ustanawiajaca-program-polityki-droga-ku-cyfrowej-dekadzie-72098586.

kwantowych. Dla banków istotnym obszarem rozwoju jest transformacja cyfrowa, w ramach której celem jest, aby co najmniej 75% przedsiębiorstw unijnych korzystało z usługi przetwarzania w chmurze dużych zbiorów danych lub AI, a ponad 90% MŚP osiągnęło co najmniej podstawowy wskaźnik wykorzystania technologii cyfrowych, oraz poprawę przez UE dostępu do finansowania. Podniesienie kompetencji cyfrowych w MŚP wpłynie istotnie na potrzebę, a nawet konieczność korzystania z nowych, bezpiecznych usług świadczonych przez banki i to nie tylko w zakresie usług bankowych. Uzupełnieniem powyższych celów (m.in. aby wytworzone narzędzia, infrastruktura oraz podniesione kompetencje cyfrowe wskazane w powyższych obszarach miały uzasadnienie) jest cyfryzacja usług publicznych w ramach których 100% kluczowych usług publicznych ma być dostępne online dla obywateli i przedsiębiorców UE i interakcji usług online z administracją publiczną. Ponadto 100% obywateli Unii ma mieć dostęp do swojej elektronicznej dokumentacji medycznej; oraz co kluczowe w aspekcie niniejszego raportu 100% obywateli Unii ma mieć dostęp do środków w zakresie identyfikacji elektronicznej (eID) uznawanych w całej Unii i zapewniających im pełną kontrolę nad transakcjami wymagającymi weryfikacji tożsamości i nad udostępnionymi danymi osobowymi.

Rozwój powyższych obszarów jest kluczowy, wręcz strategiczny dla szerokiego, powszechnego i zestandaryzowanego rozwoju modelu obiegu informacji, czy też szerzej – danych w ramach dokumentu 3.0. Bez rozwoju infrastruktury, zwiększenia cyberbezpieczeństwa, odporności, utworzenia i upowszechnienia węzłów brzegowych, ale także podniesienia kompetencji cyfrowych społeczeństwa UE oraz wytworzenia nowych, opartych o dokument 3.0 usługach przedsiębiorców oraz administracji – danatyzacja gospodarki cyfrowej w dalszym ciągu pozostanie na poziomie pilotaży czy też punktowych wdrożeń. Kluczowe w ocenie autorów niniejszego raportu jest włączenie banków i instytucji finansowych do ekosystemu gospodarki cyfrowej. Obserwując raporty roczne poszczególnych państw członkowskich w zakresie wdrażania polityki (pierwsze są z 2024 r.) istnieje uzasadniona obawa nieosiągnięcia przez administrację, ale też przez MSP założonych celów, a co za tym idzie brak wystarczającej ilości usług determinujących wykorzystywanie dokumentu 3.0. Banki m.in. rozporządzeniem eIDAS2 zostały zobligowane najpóźniej od 2027 r. do akceptacji EU ID, a więcej wejścia w ekosystem danatyzacji, co naszym zdaniem gwarantuje przekroczenie masy krytycznej dla rozwoju gospodarki cyfrowej. Stanowi też gwarancję bezpieczeństwa i prawidłowości wdrożenia.

1.2. Krajowy plan działania do programu polityki „Droga ku cyfrowej dekadzie" do 2030 r.

W opublikowanym w 2023 r. Digital Decade Country Raport (DDCR) zawierającym obiektywne kryteria DESI Polska dosyć istotnie odbiega w większości wskaźników od dojrzałości cyfrowej społeczeństwa, gospodarki jak i administracji. W sumie na 32 wskaźniki poniżej średniej unijnej jest 26. Niskie kompetencje będą miały znaczenie dla wykorzystania cyfrowych narzędzi przygotowanych przez UE, a koniecznych do wdrażania przez banki.

W obszarze kompetencje cyfrowe – zaledwie 43% Polaków posiada co najmniej podstawowe umiejętności cyfrowe (średnia UE 54%), natomiast ponadpodstawowe tylko 21% (UE 26%). Także w zakresie specjalistów ICT udział ich w ogólnej liczbie pracujących wynosi 3,6% (UE 4,6%), a z tego zaledwie 16,7% to kobiety. Jak wykazała Rada UE „niski poziom umiejętności cyfrowych ogranicza zdolność polskich przedsiębiorców do inwestowania w zaawansowane rozwiązania cyfrowe, a jednocześnie przyczynia się do niedoboru siły roboczej i wykwalifikowanej kadry".

Odnośnie przedsiębiorców obraz kompetencji cyfrowych także nie jawi się optymistycznie. Aż 71% polskich przedsiębiorców prezentuje niski lub bardzo niski stopień intensywności cyfrowej (z 12 kryteriów określających kompetencje cyfrowe spełniało mniej niż 6). Wysoki lub bardzo wysoki poziom odnotowano w 29% przedsiębiorców. Widoczna jest jednak mocna dywersyfikacja, gdyż 89% z nich to duże podmioty. Dane te wyraźnie wskazują na bardzo poważny problem polskiej gospodarki, a co za tym idzie – trudności absorpcji w przyszłości korzyści ze zmian wprowadzanych cyfrową dekadą, a także istotnego wykluczenia cyfrowego MŚP stanowiących w państwach o wyższych kompetencjach cyfrowych fundament rozwoju rynku cyfrowego. Znacznie odbiegamy (na co wskazano w raporcie DESI) w zakresie korzystania z najnowszych rozwiązań cyfrowych – z chmury korzysta zaledwie 19% polskich przedsiębiorców (przy średniej unijnej 34%), big data 9% (UE –14%), natomiast z AI prawie trzykrotnie rzadziej niż średnia unijna – tylko 3% polskich przedsiębiorców przy unijnej średniej 8%, co sytuuje nas w europejskim ogonie. Niestety polska strategia AI nie gwarantuje, aby w tym zakresie nastąpiła istotna zmiana mimo głośnych (także w 2024 r.) zapowiedzi polityków. Jak wskazano w Krajowym planie działania „główną barierą w cyfryzacji przedsiębiorstw jest kultura organizacyjna. Hamulcem rozwoju polskich firm jest niewystarczający poziom kompetencji cyfrowych oraz brak odpowiedniej świadomości wagi znaczenia transformacji cyfrowej, zarówno po stronie kadry zarządzającej, jak i pracowników. Ponadto istotnym czynnikiem są wysokie koszty

wdrożenia narzędzi cyfrowych oraz deficyt czasu na przeprowadzenie zmian". Jest to bardzo pesymistyczny obraz polskiej gospodarki cyfrowej – stanowiący z jednej strony istotne ryzyko w zakresie spełnienia przez polskich przedsiębiorców kryteriów Dekady Cyfrowej 2030, z drugiej szansą na ich cyfrowy rozwój, w którym niebagatelną rolę odegrają instytucje bankowe, stanowiące istotny element ekosystemu cyfrowego.

W obszarze cyfrowe usługi publiczne Polska także odbiega od średniej unijnej. Dostępność e-usług dla obywateli wynosi 60% (UE 77%), a dla przedsiębiorców 73% (przy średniej unijnej 84%). Polska wskazuje, że środkiem identyfikacji elektronicznej w naszym kraju jest profil zaufany, e-dowód a także ostatnimi czasy mObywatel, wskazując na dużą ilość instalacji oprogramowania (10,6 mln). Pokazuje to spory potencjał w zakresie potrzeby cyfrowej tożsamości. Niestety dokładna analiza tych narzędzi wskazuje, iż żadne z nich (mimo wypowiedzi publicznych niektórych polityków) nie stanowi narzędzia wymaganego w eIDAS2, a sposób wykorzystania oraz częstotliwość jest na niskim poziomie. Także jakość e-usług publicznych pozostawia wiele do życzenia, brak interoperacyjności oraz silosowość rozwiązań, co bardzo negatywnie wpływa na ekosystem cyfrowy polskiej gospodarki. Polska cyfryzacja administracji opiera się najczęściej na dokumencie 2.0, przy nie zawsze zmienionych procesach w porównaniu do obiegu dokumentów 1.0. Barierą w rozwoju jest mentalność i niska kultura organizacyjna, nieprzystosowane do obiegu cyfrowego (w tym dokumentu 3.0) procesów a także niski poziom kompetencji cyfrowych. Wśród decydentów zarówno na poziomie administracji rządowej, regionalnej czy samorządowej jest niski poziom wiedzy w zakresie transformacji cyfrowej, jak i możliwości, jakie za sobą niesie cyfryzacja i optymalizacja procesów. Nie bez znaczenia są znacznie niższe niż rynkowe wynagrodzenia dla specjalistów ICT w administracji. W Polsce brak w chwili obecnej węzłów brzegowych, rozwiązań opartych o rozproszony zapis danych (DLT) czy szerszego wykorzystania AI, co stanowić będzie istotną barierę w zakresie rozwoju usług opierających się o dokument 3.0 i danatyzację procesów. Konieczne jest w najbliższym czasie podniesienie kompetencji cyfrowych polskiej administracji, w szczególności samorządowej.

Odrębnym, istotnym w ujęciu raportu jest niewystarczający poziom interoperacyjności usług i przepływu danych w polskich e-usługach publicznych. W unijnym raporcie przedstawiającym stan transformacji cyfrowej administracji publicznej Digital Public Administration factsheet 2023 wskazano na konieczność większej przejrzystości usług, które należy tworzyć w sposób zapewniający przejrzystość procesów i reguł administracyjnych, przepływu danych i podejmowanych decyzji. Na niskim poziomie jest zasada wielojęzyczności e-usług publicznych. Rozwiązania teleinformatyczne muszą przewidywać możliwość wielojęzycznej komunikacji z użytkownikiem i obywatelem. W związku ze swobodą przepływu osób, użytkownikami systemów w e-administracji mogą być, bądź też są osoby obcojęzyczne. Wiele usług w Polsce jest wyłącznie w języku narodowym. Wreszcie wskazano na konieczność uproszczenia procesów w administracji. Polska procedura, ale przede wszystkim procesy – w tym obieg dokumentów – są nadmiarowe i powodują zbytnią złożoność organizacji administracji, a co za tym idzie jej efektywność. Współczesne polskie e-usługi administracji publicznej w sporej mierze są zdigitalizowanymi procesami obiegu dokumentu 1.0, dopuszczającymi możliwość korzystania z dokumentu 2.0 (zdigitalizowany 1.0), ale najczęściej w procesach identycznych lub bardzo zbliżonych do obiegu dokumentu 1.0, konsekwencją czego jest niepełne, wręcz minimalistyczne wykorzystanie możliwości jakie daje nie tyle digitalizacja, ile cyfryzacja procesów i zwiększenie jej efektywności, zmniejszenie złożoności organizacyjnej, a co za tym idzie zmniejszenie nadmiarowości zatrudnienia w administracji. Polityka Cyfrowa Dekada stanowi podstawę dla szerszego wykorzystania tzw. dokumentu 3.0, interoperacyjności administracji, a przede wszystkim przemyślenia i w wielu obszarach zbudowania na nowo usług e-administracji opartych na danatyzacji w miejsce tradycyjnego bądź cyfrowego dokumentu 2.0. Wymaga to jednak istotnych zmian w filozofii i koncepcji funkcjonowania polskiej administracji i odejścia od tzw. silosowej administracji na rzecz współdzielenia danych – w tym w systemach rozproszonych, a także stworzenia infrastruktury opartej o węzły brzegowe oraz większego wykorzystania algorytmów samouczących się, w tym systemów AI w administracji. W ocenie autorów, sposób realizacji polityki UE przedstawiony przez Ministerstwo Cyfryzacji w 2023 r. w Krajowym planie działania do programu „Droga ku cyfrowej dekadzie" do 2030 r. nie uwzględnia wszystkich możliwości, w szczególności związanych z danatyzacją i dokumentem 3.0 w usługach e-administracji[15]. Jakkolwiek w przedstawionym do konsultacji dokumencie „Strategia Cyfryzacji Państwa" przez Ministerstwo Cyfryzacji założono już jako trzeci cel do 2035 r., że: „20 mln Polek i Polaków aktywowało portfel tożsamości cyfrowej". W ocenie autorów cel ten wiąże się jednak z innymi elementami, które muszą być zrealizowane, w tym z założeniem lit. c w celu 1: „Dostosowanie wymaganych i kluczowych e-usług publicznych do wymogów krajowego i europejskiego portfela tożsamości cyfrowej, będącej certyfikowanym, uznawanym środkiem identyfikacji elektronicznej na wysokim poziomie bezpieczeństwa"[16]. W ocenie autorów istotne

[15] https://digital-strategy.ec.europa.eu/en/library/country-reports-digital-decade-report-2023

[16] Ministerstwo Cyfryzacji, Strategia Cyfryzacji Państwa (Projekt do konsultacji społecznych), 2024, s. 7 i 75.

jest podkreślenie, że tego typu dostosowanie powinno objąć również kwestie ram prawnych. Dla przykładu dostęp do wymiaru sprawiedliwości, tj. np. złożenie pisma w sądzie zgodnie z eIDAS nie jest możliwe w Polsce, bo jak zauważono w wyroku TSUE, polski KPC nie uwzględnia takiej możliwości[17]. Równocześnie wraz z budowaniem systemów informatycznych, powinny iść zmiany w prawie. Autorzy zauważyli, że w Strategii poświecono też rozdział Cyfrowej tożsamości, w tym analizie aktualnych środków identyfikacji elektronicznej, które są notyfikowane. Zwrócono uwagę, że dostępne środki, pod kątem ich wykorzystania za granicą, nie są akceptowalne. Dodano jednak, że to problem na skalę europejską, który wyeliminuje pojawienie się eIDAS 2.0. Diagnoza mocno akcentuje kwestie cyberbezpieczeństwa: „Niezbędna jest również dalsza edukacja publiczna w zakresie możliwości realizacji spraw urzędowych online oraz właściwego sposobu korzystania ze środków identyfikacji elektronicznej, tak aby zapobiegać kradzieżom tożsamości, naruszeniom danych osobowych, cyberatakom i innym niebezpiecznym sytuacjom w Internecie.”. W kontekście Tożsamości Cyfrowej w Strategii sformułowano 4 cele: pierwszy dotyczy osób prawnych, drugi podpisów elektronicznych, trzeci środków identyfikacji, a ostatni bezpieczeństwa i swobody użycia, w tym użycia transgranicznego.

Autorzy pozytywnie oceniają działania związane z sformułowaniem celów, które są zgodne z kierunkiem UE. W przypadku pierwszego celu w strategii wskazano następujące działania, które mają umożliwić dojście do celu, jakim jest prostota i szybkość załatwienia sprawy urzędowej dla osoby prawnej[18]:

a) Utworzenie w ramach publicznego systemu identyfikacji elektronicznej środka identyfikacji elektronicznej dla osoby prawnej oraz środka identyfikacji elektronicznej dla osoby fizycznej reprezentującej osobę prawną;

b) Skuteczne umocowanie prawne środka identyfikacji elektronicznej dla osoby prawnej oraz środka identyfikacji elektronicznej dla osoby fizycznej repezentującej osobę prawną, aby mógł on służyć do automatycznego uwierzytelniania w usługach publicznych online, bez konieczności każdorazowej manualnej weryfikacji przez urzędnika prawidłowości i aktualności przedstawianych pełnomocnictw lub upoważnień do reprezentacji;

c) Stworzenie nowych lub zmodyfikowanie istniejących usług publicznych tak, aby akceptowały wydane środki identyfikacji elektronicznej dla osób prawnych i środki identyfikacji elektronicznej dla osób fizycznych reprezentujących osoby prawne;

d) Utworzenie narzędzia zapewniającego możliwość łatwego i wygodnego składania podpisów elektronicznych niezależnie od ich rodzaju i formatu dokumentu w przypadku wieloosobowej reprezentacji osoby prawnej (“wielopodpis”);

e) Udostępnienie europejskiego portfela tożsamości cyfrowej do użytku osób prawnych.

Wedle autorów powyższe działania, mimo swej ogólności, wskazują na jasne działania, które mogą pomóc. Niemniej powinny być realizowane wraz z celem drugim, który zakłada zwiększenie dostępności i powszechności używanych podpisów tak, aby ich weryfikacja była prosta i niezawodna bez względu na format dokumentu i rodzaj podpisu. W tym celu w Strategii wskazuje się dwa działania, które bazują na rozwoju narzędzi do podpisywania i weryfikowania dokumentów podpisem zaufanym, podpisem osobistym oraz kwalifikowanym podpisem elektronicznym oraz rozpowszechnienie informacji o korzyściach wynikających z korzystania z możliwości składania i weryfikowania podpisów elektronicznych w ich systemach, w tym wspierających realizację e-usług publicznych, poprzez integrację z komponentem węzła podpisu. Cel trzeci zakłada osiągniecie bezpieczeństwa i wygody w użyciu środków identyfikacji. W tym zakresie planuje się:

1. Budowę oraz wdrożenie modelu szerokiego wykorzystywania warstwy elektronicznej dowodu osobistego oraz certyfikatów elektronicznych związanych z wykonywanym zawodem w systemach teleinformatycznych;

2. Dodanie do węzła krajowego środka identyfikacji o wysokim poziomie bezpieczeństwa, jakim będzie europejski portfel tożsamości cyfrowej;

3. Dodanie do węzła krajowego historii użycia środków identyfikacji elektronicznej;

4. Dodanie weryfikacji czy urządzenie, z którego następuje logowanie do systemów teleinformatycznych przyłączonych do węzła krajowego, jest na liście urządzeń zaufanych użytkownika;

5. Realizacja działań edukacyjnych, które wspomogą użytkowników w bezpiecznym korzystaniu ze środków identyfikacji elektronicznej.

Również i te działania wpisują się w ocenie autorów do realizacji zbieżnych w eIDAS 2.0 założeń

[17] C-302/23 Marek Jarocki przeciwko C.J.
[18] Ministerstwo Cyfryzacji, …, s. 91-93.

i wykorzystania możliwości z tym związanych. Ostatni cel zakłada osiągnięcie swobody i bezpieczeństwa w użyciu tożsamości cyfrowej przez obywateli, jak i przedsiębiorców, na poziomie krajowym, jak i transgranicznym na potrzeby publiczne, a także komercyjne. Zgodnie z założeniami, będzie to możliwe poprzez:

1. Utworzenie obowiązkowego rejestru podmiotów, które będą chciały świadczyć swoje usługi w oparciu o europejski portfel tożsamości cyfrowej;

2. Stworzenie i udostępnienie weryfikacji niektórych danych użytkowników w rejestrach państwowych, aby można było wydawać elektroniczne poświadczenia danych równoważne prawnie z zaświadczeniami tradycyjnymi i uznawane również za granicą;

3. Udostępnienie nieodpłatnych kwalifikowanych podpisów elektronicznych w europejskim portfelu tożsamości cyfrowej dla osób fizycznych, przynajmniej do użytku nieprofesjonalnego;

4. Wprowadzenie procedur jednoznacznego transgranicznego dopasowywania tożsamości, w którym dane identyfikujące osobę są przyporządkowywane do istniejącego konta należącego do tej samej osoby w danej usłudze publicznej;

5. Modyfikację krajowych systemów teleinformatycznych, w tym wspierających realizację e-usług publicznych, aby w szerszym zakresie uznawały transgraniczne środki identyfikacji elektronicznej, w tym europejskie portfele tożsamości cyfrowej wydawane przez inne państwa członkowskie oraz ułatwiały korzystanie z publicznych usług elektronicznych użytkownikom z innych państw członkowskich (dostępność usługi i wsparcia w innym języku niż polski).

W ocenie autorów same założenia są zgodne i poprawne. Rok 2035 wydaje się też bardziej realistyczny, aniżeli inny wcześniejszy. Autorzy wychodzą jednak z założenia, że samo upowszechnienie się dokumentu 3.0, w związku z tym powszechne życie tożsamości cyfrowej, będzie rozwijać się dłużej, chociażby ze względu na pewne braki systemowe w prawie[19].

[19] Ministerstwo Cyfryzacji, …, s. 94.96.

Pojęcie dokumentu 1.0, 2.0, 3.0

2.1. Pojęcie i elementy dokumentu na gruncie prawa polskiego i rozporządzenia eIDAS

Definicja, a co za tym idzie pojęcie dokumentu, w istotny sposób uległa, a w związku z eIDAS2 dalej ulega ewolucji. Rozporządzenie eIDAS2 wprowadza nowe narzędzia, możliwości, ale także obowiązki, w tym dla banków oraz wymusza zmianę procesów biznesowych przy równoczesnym zachowaniu funkcji, jakie przepisy prawa oraz doktryna przewidują dla dokumentów. A są nimi: 1) funkcja konstytutywna polegająca na tym, że sporządzenie dokumentu stanowi konieczną przesłankę ważności czynności prawnej, 2) funkcja dowodowa polegająca na tym, że dokument, który w chwili obecnej w polskiej procedurze cywilnej cieszy się największym uprzywilejowaniem spośród wszystkich środków dowodowych w procesie, stanowi dowód często powiązany z domniemaniami prawnymi, 3) funkcja legitymacyjna polegająca na tym, że posiadanie dokumentu może być niezbędne do rozporządzenia prawami lub wykonywania uprawnień, 4) funkcja gwarancyjna polegająca na tym, że sporządzenie dokumentu ma w stosunkach cywilnoprawnych charakter stabilizujący oraz ograniczający możliwość ewentualnych nieporozumień co do treści dokonywanych czynności, 5) funkcja informacyjna polegająca na tym, że dokument ujawnia treść czynności prawnej w stosunku do osób trzecich, 6) funkcja instrukcyjna polegająca na tym, że dokument zawiera wskazania stron dotyczące sposobu wykonania umowy[20]. W polskiej doktrynie na ciekawą funkcję, powiązaną ze zmianami wskazywanymi w niniejszym raporcie, wskazał prof. W. Kocot uznając za istotną funkcję utrzymanie naniesionej informacji, w tym ujawnionego oświadczenia woli czy też innego oświadczenia, na tyle długo, aby możliwe było ich późniejsze ujawnienie, odtworzenie i powielenie lub przeniesienie na inny nośnik w stanie niezmienionym[21]. Koresponduje to z kodeksową definicją dokumentu jako nośnika informacji umożliwiającego zapoznanie się z jej treścią (art. 77(3) k.c.). W uzasadnieniu projektu komisji kodyfikacyjnej prawa cywilnego wskazano, że pod względem sposobu sporządzenia dokumentu definicja jest technologicznie neutralna. Treść dokumentu może zostać zatem dowolnie ujawniona (znaki graficzne, dźwięk, obraz) a także utrwalona na dowolnym nośniku (papier, urządzenie informatyczne) i przy pomocy dowolnych środków. Granicę tej neutralności wyznacza jednak realizowana przez dokument funkcja dowodowa, która wymaga, aby sposób utrwalenia informacji umożliwiał jej zachowanie i odtworzenie[22].

Definicja ta koresponduje z definicją dokumentu elektronicznego w rozporządzeniu eIDAS (art. 3 pkt. 35) zgodnie z którą jest nim każda treść przechowywana w postaci elektronicznej, w szczególności tekst lub nagranie dźwiękowe, wizualne lub audiowizualne. Przy czym, w szczególności w ujęciu dokumentu 3.0 sposób zapisu dokumentu nie został zdeterminowany, dopuszczając współdzielenie, a w ujęciu rozporządzenia eIDAS2 także tokenizację oraz interaktywność.

2.1.1. Nośnik

Jednym z konstytutywnych elementów definicji dokumentu jest zapis informacji na nośniku. Użyte pojęcie co do zasady jest neutralne technologicznie i odnosi się zarówno do nośników dotychczas uznawanych za tradycyjne, jak i nośników pozwalających na zapisanie dokumentów w postaci elektronicznej. Jednakże sposób zapisu jest jednym z elementów determinujących podział dokumentu na dokument 1.0, 2.0 oraz 3.0.

Obok pojęcia „nośnik", w szczególności w prawie bankowym, istotne znaczenie ma definicja trwałego nośnika zdefiniowana w prawie UE, jak i jego implementacjach. W dyrektywie Parlamentu Europejskiego i Rady (UE) 2023/2025 z dnia 18 października 2023 r. w sprawie umów o kredyt konsumencki oraz uchylająca dyrektywę 2008/48/WE „trwały nośnik" oznacza dowolne urządzenie umożliwiające konsumentowi przechowywanie informacji kierowanych do niego osobiście w sposób, który daje mu do nich dostęp w przyszłości przez okres odpowiedni do celów, jakim te informacje służą, i pozwalające na odtworzenie przechowywanych informacji w niezmienionej postaci (art. 3 pkt. 11). Zbliżoną definicję zawiera dyrektywa 2002/65/WE Parlamentu Europejskiego i Rady z dnia 23 września 2002 dotycząca sprzedaży konsumentom usług finansowych na odległość oraz zmieniająca dyrektywę Rady 90/619/EWG oraz dyrektywy 97/7/WE i 98/27/WE, zgodnie z którą „trwały nośnik informacji" oznacza każdy instrument pozwalający konsumentowi na przechowywanie informacji kierowanych osobiście do niego w sposób dostępny do przyszłego korzystania przez okres czasu odpowiedni do celów informacji i który pozwala na niezmienione odtworzenie przechowywanej informacji. Czy wreszcie definicja z dyrektywy Parlamentu Europejskiego i Rady (UE) 2015/2366 z dnia 25 listopada 2015r. w sprawie usług płatniczych w ramach rynku wewnętrznego, zmieniająca dyrektywy 2002/65/WE, 2009/110/WE 2013/36/UE i rozporządzenie (UE) nr 1093/2010, gdzie przez „trwały nośnik" rozumiemy instrument umożliwiający użytkownikowi usług płatniczych przechowywanie informacji osobiście do niego adresowanych w sposób umożliwiający dostęp do

[20] K. Górska, Zachowanie zwykłej formy pisemnej, Warszawa 2007, str. 69.
[21] W. Kocot, Wpływ Internetu na prawo umów, Warszawa 2004, str. 334.
[22] Księga Pierwsza Kodeksu Cywilnego. Projekt z uzasadnieniem, Warszawa 2009, str. 119-120).

tych informacji w przyszłości przez okres właściwy do celów tych informacji i pozwalający na odtworzenie przechowywanych informacji w niezmienionej postaci (art. 4 pkt. 35). Co ciekawe, w propozycji PSD3 nie ujęto już definicji trwałego nośnika[23].

Trybunał Sprawiedliwości UE kilkukrotnie odnosił się do pojęcia i problematyki trwałego nośnika. W wyroku z 5 lipca 2012 roku stwierdził, iż dla uznania danego nośnika za trwałe konieczne jest udowodnienie, że przekazanie w nim informacji gwarantuje brak możliwości dokonywania zmian zawartości w dokumencie za pomocą niego doręczonego, i gwarantuje dostępność w odpowiednim okresie umożliwiając konsumentom odtworzenie treści dokumentu w niezmienionej postaci[24]. W nowszym, wydanym orzeczeniu z 25 stycznia 2017 roku uznano, iż serwis internetowy banku, a w jego ramach działająca poczta elektroniczna, aby mogła zostać uznana za trwały nośnik informacji powinna „umożliwić użytkownikowi usług płatniczych przechowywanie informacji adresowanych osobiście do niego przesyłanych w sposób umożliwiający dostęp do nich w przyszłości przez okres właściwy do celów tych informacji i odtworzenie ich w niezmienionej postaci ponadto, aby stronę internetową można było uznać za trwały nośnik należy wykluczyć możliwość wszelkiej jednostronnej zmiany jej treści przez dostawcę usług płatniczych lub innego przedsiębiorcę, któremu powierzy się zarządzanie tą stroną"[25].

W wyrokach powyższych wskazano, iż aby dane narzędzie informatyczne mogło zostać uznane za trwały nośnik, klient musi mieć swobodny dostęp do informacji przesyłanych na ten nośnik, w tym dokumentów, przy czym ich zapisanie na trwałym nośniku oraz przechowywanie musi umożliwiać ich odtworzenie w niezmienionej postaci przez czas odpowiedni. Zarówno definicje, jak i orzeczenia TSUE wskazują na ewolucję pojęcia trwałego nośnika. Począwszy od nośnika papierowego, tradycyjnego, poprzez dokument elektroniczny na fizycznym trwałym nośniku (np. CD) do dokumentu zapisanego w chmurze, w tym także w DLT. Jest to ewolucja z dokumentu 1.0 do 2.0 zapisanego w chmurze obliczeniowej. Czas na szersze wykorzystanie dokumentu 3.0 i zapis w rejestrze rozproszonym.

2.1.2. Danatyzacja dokumentu. Informacja jako element dokumentu

Dokument spełnia szereg funkcji. Jedną z podstawowych jest transmisja informacji. Zresztą element ten został wyraźnie wyodrębniony i wpisany do polskiej kodeksowej definicji dokumentu. W tradycyjnym ujęciu, w tym przede wszystkim dokumentu 1.0 oraz 2.0, informacja w dokumencie była „scalona" w sposób umożliwiający percepcję przez człowieka. Zresztą samo pojęcie „informacja" jest różnie rozumiane w różnych dziedzinach. Inaczej przez prawników, matematyków cybernetyków czy też informatyków[26]. Zmieniająca się technologia, zmienia równocześnie sposób zapisu informacji. Do niedawna uznawano, iż informacją są wyłącznie dane możliwe do bezpośredniej percepcji przez człowieka, możliwe do przedłożenia procesowo w dokumencie jako dowód przed sądem. W chwili obecnej, także w aspekcie eIDAS2, nie ma wątpliwości, iż informacją, o której mowa w definicji dokumentu jest informacja możliwa do percepcji bezpośredniej przez urządzenia, algorytmy itd. a tylko w sposób pośredni przez człowieka. Gro informacji jest w postaci binarnej, cyfrowej, gdzie tylko ich wizualizacja jest możliwa do odczytania przez osoby fizyczne. Współcześnie to dane stanowią informację. To dane są przetwarzane, to dane są udostępniane i to niekoniecznie bezpośrednio człowiekowi. Stanowią podstawę funkcjonowania AI czy też innych algorytmów. Dane te ulegają ciągłej zmianie, a co za tym idzie zmienia się informacja, co powinno mieć wpływ na treść dokumentów. W dokumencie 1.0 czy też 2.0 zapis danych, a co za tym idzie informacji, jest stały, niezmienny. W dokumencie 3.0 podlega aktualizacji, zmianom w miarę zgodnie ze zmieniającymi się danymi odzwierciedlającymi fakt. Jest dokumentem aktywnym, a nie statycznym jak klasyczne dokumenty[27].

Gospodarka cyfrowa, w tym regulowana zgodnie z polityką „Cyfrowa Dekada 2030" w tym przemysł 4.0, rozwój AI, opierają się przede wszystkim o dane. Tokenizacja, automatyzacja, wykorzystanie DLT, blockchain a także rozwój AI wymaga innego podejścia do danych, do informacji, a także do dokumentów – w tym dokumentów w znaczeniu cywilno-materialnym lub procesowym. Dane, a co za tym idzie dokument 3.0 jest „pożywieniem" dla AI i algorytmów. Zwykłe, tradycyjne dokumenty, a właściwie dane

[23] Wniosek COM (2023) 366 final 2023/0209 (COD) z dnia 28 czerwca 2023 https://eur-lex.europa.eu/legal-content/PL/TXT/HTML/?uri=CELEX:52023PC0366 pobrano 2 sierpnia 2024r.

[24] C-49/11 Content Services Ltd przeciwko Bundesarbeitskammer

[25] C-375/15 BAWAG PSK Bank für Arbeit und Wirtschaft und Österreichische Postsparkasse AG przeciwko Verein für Konsumenteninformation

[26] Autorzy raportu pisali o tym w innych pracach – np. D. Szostek, R, Prabucki, R. Skibicki, J. Wyczik, Algorithmisation and Tokenisation of Law [w:] D. Szostek, M. Załucki, Legal Tech : information technology tools in the administration of justice, 2022.

[27] Autorzy raportu pisali o tym w innych pracach – np. D. Szostek, Dokument 3.0 a postępowanie dowodowe, [w:] Prawo nowych technologii. Księga zokazji jubileuszu 20-lecia działalności Centrum Badań Problemów Prawnych i Ekonomicznych Komunikacji Elektronicznej i Studenckiego Koła Naukowego — Blok Prawa Komputerowego, red. J. Gołaczyński, Warszawa 2023, s.268 n.

w nich zawarte nie są w stanie wspierać czy też uczyć AI. Tradycyjny dokument w wersji 1.0 jest tylko wizualizacją danych czy też informacji, które zawiera. Systemy informatyczne, dla percepcji danych, analizy, wykorzystania czy podejmowania decyzji nie potrzebują takiej wizualizacji. Istotą współczesnego dokumentu jest odpowiednio utrwalona treść zawierająca informację możliwą do percepcji przynajmniej pośrednio poprzez wykorzystanie systemów informatycznych.

2.2. Dokument 1.0, 2.0, 3.0

Rozporządzenie eIDAS2 – ale także aktualnie wchodzące przepisy jak DORA, MiCA, NIS 2 itd. – stanowią podstawę prawną dla dokumentu 3.0. eIDAS spina w sobie narzędziowo, ale także prawnie i w połączeniu z domniemaniami prawnymi szereg regulacji tworzących europejski cyfrowy rynek. Podstawą dla tworzącego się rynku cyfrowego jest danatyzacja i możliwość wykorzystania danych przez algorytmy, w tym poprzez AI do dalszego przetwarzania, ale także podejmowania decyzji. I właśnie to kryterium determinuje podział dokumentu na 1.0, 2.0 oraz 3.0.

Za dokument 1.0 uznaje się tradycyjne dokumenty w postaci papierowej, wykorzystywane w tradycyjnym czy też klasycznym obiegu, odnośnie których zastosowanie mają dotychczasowe, klasyczne najczęściej krajowe przepisy odnoszące się do postępowania dowodowego. Dane z takich dokumentów po prostu odczytuje się i podlegają bezpośredniej percepcji przez człowieka. Pozyskanie danych z dokumentu 1.0 bez ich digitalizacji czy wykorzystania oprogramowania OCR lub innego o podobnej funkcji, jest niemożliwe. Praca z danymi czy informacją zawartą w takim dokumencie jest możliwa wyłącznie przez człowieka. Zapisana informacja w dokumencie jest stała i co do zasady niezmienna. Zapewnienie „oryginalności" dokumentu jest powiązane z klasycznymi sposobami, jak własnoręczny podpis czy ewentualnie nałożenie klasycznej pieczęci, a sama informacja zostaje zapisana na klasycznych nośnikach, najczęściej papierze. Dokument 1.0 można dzielić według różnych kryteriów w tym na oryginał, kopię oraz poświadczony za zgodność z oryginałem.

Dokumentem 2.0 jest „klasyczny" czy też „tradycyjny" dokument elektroniczny, opierający się o narzędzia wynikające m.in. z eIDAS1, powstały albo w sposób pierwotny w postaci elektronicznej, albo w sposób wtórny (zdigitalizowany dokument 1.0), w którym dane są zapisane w pewnej zamkniętej całości (w zamkniętym formacie) i są danymi statycznymi, a informacja zawarta w dokumencie 2.0 jest co do zasady niezmienna. Różnicą w stosunku do dokumentu 1.0 jest możliwość „wyciągnięcia" bezpośrednio z dokumentu elektronicznego danych, a następnie wykorzystanie przez algorytmy. Zapis dokumentu 2.0 jest najczęściej binarny a percepcja przez człowieka możliwa pośrednio poprzez wykorzystanie urządzeń oraz oprogramowania pozwalającego na zapoznanie się z jego treścią (informacją). Autentyczność oraz integralność dokumentu 2.0 jest powiązana z narzędziami informatycznymi, w tym wynikającymi z eIDAS1 jak zaawansowany podpis elektroniczny czy jego kwalifikowana postać lub zaawansowana pieczęć elektroniczna lub jej kwalifikowana postać. Dokument 2.0 może być zapisywany w wielu różnych formatach (doc, pdf, xml itd.) ale, podobnie jak dokument 1.0 w zamkniętej całości (np. pliku pdf), gdzie dane co do zasady nie podlegają zmianie. Może być zapisany na różnych nośnikach, w tym fizycznych jak CD, ale także w technologii chmurowej oraz w DLT lub blockchain – jednakże, jak już wskazano, jako zamknięta całość. Kwestie dotyczące DLT i blockchain zaadresowano w rozdziale 6.0.

Zarówno dokument 1.0 jak i 2.0 zawierają informacje historyczne, co nie jest równoznaczne z "nieaktualne", a zapis takiego dokumentu (2.0) w systemach rozproszonych wprawdzie jest poprawny i często dokonywany, nie uwzględnia jednakże wszystkich możliwości, jakie daje ta technologia. Istotą tej technologii jest możliwość zapisywania danych, a co za tym idzie informacji w sposób nielinarny, niebędący zamkniętą całością, w sposób ciągły i aktywny, uwzględniający nowe fakty, zmiany (nawet w czasie rzeczywistym, chociaż nie zawsze) dając większą aktualność dokumentu 3.0 w odniesieniu do jego starszych odpowiedników. Dokument 3.0 charakteryzuje się także tym, iż dane nie są zapisywane w jednym „miejscu" czy w zamkniętej całości. Dane, które tworzą informację, mogą być zapisywane w różnych bazach, nawet w wielu krajach w sposób transgraniczny, są aktualizowane z możliwością odczytania wersji historycznych i ich weryfikacji. Technologia ta jest znana od lat i wykorzystywana przez wiele podmiotów w ramach tokenizacji procesów i wykorzystywania smart contracts (inteligentnych umów). Dotychczas jednak dokument 3.0, co do zasady nie był na gruncie prawa europejskiego (co najwyżej w pojedynczych państwach) powiązany z domniemaniami prawnymi. Sytuację tę zmienia w chwili obecnej eIDAS2. Dokumentu 3.0 nie dzielimy na dokument oryginalny i kopie jak dokument 1.0. Przy czym, co odróżnia go od dokumentu 2.0, nie wszystkie jego elementy (dane składające się na informacje) będą powiązane z domniemaniami prawnymi. O czym szerzej w dalszej części raportu.

Kolejną cechą dla dokumentu 3.0 jest łatwość wykorzystania danych przez algorytmy – w tym AI – bez konieczności dodatkowych działań, jak przy dokumencie 1.0 czy 2.0. Dokument 3.0 co do zasady

nie jest możliwy dla bezpośredniej percepcji przez człowieka. Dla zapoznania się z nim konieczne jest odpowiednie oprogramowanie i urządzenia, a także dostęp do Internetu, aby pozyskać w czasie bieżącym dane z wielu baz czy też z systemu tworzącego dokument 3.0.

2.3. Zapis danych na trwałym nośniku w DLT lub blockchain a obowiązek usuwania danych dotychczasowym problemem dla dokumentu 3.0

Proces dopełnienia wymogów prawa przez podmioty zobowiązane do obowiązków informacyjnych (w tym banki) należy podzielić następująco: 1) wygenerowanie dokumentu zawierającego informację czy też oświadczenie wymagane przepisami prawa, w tym zachowanie odpowiedniej formy dla czynności; 2) właściwe zabezpieczenie w celu zapewnienia autentyczności integralności oraz 3) skuteczne doręczenie lub udostępnienie osobie uprawnionej na trwałym nośniku – ale w taki sposób, aby osoba ta miała możliwość przechowywania na nim informacji, odtwarzania jej w niezmienionej postaci i aby była ona trwała, to znaczy funkcjonowała w taki sposób, aby był zapewniony niezakłócony dostęp, przynajmniej przez czas odpowiedni, najczęściej określony przepisami prawa do celów, jakim zgromadzone na nim informacje służą. Równocześnie adresat nie powinien mieć możliwości manipulowania, samodzielnego usuwania, zmieniania treści, ale także metadanych dokumentów czy też ograniczać komukolwiek, w tym nadawcy, prawa dostępu do dokumentu.

Dotychczas wykorzystywane narzędzia informatyczne – czy oparte o regulacje polskiego prawa bankowego, czy też eIDAS – pozwalały na spełnienie powyższych wymogów dla dokumentów 1.0 i 2.0. Rozporządzenie eIDAS2, wprowadza nowe narzędzia, przede wszystkim prawne (bo technologicznie funkcjonujące od lat) dla zastosowania powyższych wymogów dla dokumentu 3.0, umożliwiające szerokie i powszechne stosowanie DLT lub blockchain jako technologii z zachowaniem wymogów RODO, w tym możliwość usuwalności danych.

Spory wpływ na eIDAS2 i koncepcję szerokiego zastosowania dokumentu 3.0 miał dokument przygotowany dla Parlamentu Europejskiego: *Blockchain and GDPR. Can distributed ledgers be squared with European data protection law?* (STOA PE 634.445)[28], w którym zaproponowano, aby dane osobowe były zapisywane w odrębnych bazach będących pod wyłączną kontrolą użytkownika, tj osoby, której dane osobowe dotyczą, w sposób umożliwiający ich usunięcie poprzez np. „odcięcie" od treści dokumentu, zarządzenie tymi danymi, a także anonimizację i możliwość wykorzystania tzw. dowodu zerowej wiedzy (o czym szerzej w dalszej części). Wyodrębnienie danych osobowych z blockchain, na rzecz funkcjonalnego połączenia z blokiem w taki sposób, aby w czasie wymaganym przez prawo istniała możliwość zapoznania się z dokumentem oraz danymi osobowymi w nim zawartymi, jest możliwe wyłącznie w ramach dokumentu 3.0 – niemożliwe w dokumencie 1.0 czy 2.0, gdzie konieczne są działania anonimizujące dokument po upływie wymaganego przez RODO czasu lub usunięcie całego dokumentu.

Dane osobowe, przede wszystkim tożsamość osoby fizycznej, ale także i innych podmiotów jest kluczowa w obrocie gospodarczym, ale także w kontaktach czy czynnościach eGoverment. Narzędzia dotychczas wykorzystywane do potwierdzania tożsamości elektronicznej, jak kwalifikowany podpis elektroniczny czy inne notyfikowane w EU na podstawie art. 9 eIDAS (Polski Profil Zaufania czy mObywatel) są odpowiednie dla dokumentu 2.0 i nie stanowią odpowiedniego narzędzia dla dokumentu 3.0. Stąd konieczność zmian, systemowa koncepcja nie tylko nowej zintegrowanej tożsamości cyfrowej, ale całego ekosystemu dla dokumentu 3.0, który już w niedługim czasie (bo maksymalnie w 2027 r.) musi zostać wprowadzony i zaakceptowany także przez instytucje bankowe.

[28] https://www.europarl.europa.eu/RegData/etudes/STUD/2019/634445/EPRS_STU(2019)634445_EN.pdf. Pobrano 3 sierpnia 2024r.

Nowe usługi zaufane i ich wpływ na dokument 3.0 w rozporządzeniu Rady Unii Europejskiej i Parlamentu Europejskiego z 30 kwietnia 2024 r. eIDAS2

3.1. Wprowadzenie

W ramach pakietu regulacji dotyczących rynku cyfrowego jako jedne z ostatnich w poprzedniej kadencji Parlamentu Europejskiego przyjęto AI Act[29] oraz rozporządzenie Parlamentu Europejskiego i Rady (UE) 2024/1183 z dnia 11 kwietnia 2024 r. w sprawie rozporządzenia (UE) nr 910/2014 w odniesieniu do ustanowienia europejskich ram tożsamości cyfrowej[30] (eIDAS2). Już sam tytuł rozporządzenia wskazuje na istotę jego treści. Rozporządzenie stanowi istotny element łączący unijne akty prawne nakładające obowiązki związane z bezpieczeństwem w środowisku cyfrowym jak NIS2 czy DORA. Już w konkluzjach z 1-2 października 2020 r. Rada Europejska wezwała Komisję do opracowania ogólnounijnej bezpiecznej publicznej identyfikacji elektronicznej, w tym interoperacyjnych podpisów cyfrowych przede wszystkim, aby zapewnić pełną kontrolę obywatelom Unii Europejskiej oraz rezydentom nad ich tożsamością oraz ich danymi w Internecie, a także aby umożliwić dostęp do publicznych, ale również prywatnych i transgranicznych usług cyfrowych. W polityce „Droga ku Cyfrowej Dekadzie do 2030" jednym z celów jest zapewnienie oraz wprowadzenie na szeroką skalę zaufanej, dobrowolnej, ale co najważniejsze, kontrolowanej w pełni i wyłącznie przez użytkownika tożsamości cyfrowej, uznawanej w całej Unii oraz umożliwiając każdemu użytkownikowi zarządzanie swoimi danymi w interakcjach online. Podobnie w „Europejskiej deklaracji praw i zasad cyfrowych w cyfrowej dekadzie"[31] przyjętej wspólnie przez Parlament Europejski, Radę i Komisję, gdzie w punkcie 7 podniesiono, że każdy powinien mieć dostęp online do kluczowych usług publicznych w Unii Europejskiej. Nikt nie powinien być proszony o podanie danych, aby uzyskać dostęp do cyfrowych usług publicznych i korzystać z tych usług częściej, niż jest to konieczne. W dokumencie tym przyjęto zobowiązanie do zapewnienia osobom mieszkającym w Europie możliwość dobrowolnego skorzystania z dostępnej, bezpiecznej i godnej zaufania tożsamości cyfrowej, która pozwala na dostęp do szerokiego wachlarza usług online. Zobowiązano się także do ochrony interesów ludności, przedsiębiorstw i instytucji publicznych przed ryzykami w cyberprzestrzeni i cyberprzestępczością, w tym przed naruszeniami ochrony danych i kradzieżą tożsamości lub manipulowaniem tożsamością, co obejmuje przede wszystkim wymogi w zakresie cyberbezpieczeństwa dla produktów skomunikowanych, wprowadzanych do obrotu na jednolity rynek. Prawo to obejmuje także kontrole tego, jak dane są wykorzystywane i komu są udostępniane. Dotychczasowe regulacje, w tym RODO, wymagają uzupełnienia o nowe narzędzia. Aktualne, będące podstawą dla dokumentu 1.0 a przede wszystkim 2.0 nie dają pełnej kontroli obywatelom UE nad własnymi danymi, w tym danymi osobowymi czy też tożsamością. Są statyczne a nie dynamiczne, czego wymagają nowoczesne usługi, w tym usługi zaufane.

W preambule do eIDAS2 wskazano, iż bardziej zharmonizowane podejście do identyfikacji elektronicznej powinno zmniejszyć ryzyko i koszty wynikające z obecnej fragmentacji spowodowanej stosowaniem rozbieżnych rozwiązań krajowych lub – w niektórych państwach członkowskich – brakiem takich rozwiązań w zakresie identyfikacji elektronicznej. Nowe podejście powinno wzmocnić rynek wewnętrzny, umożliwiając obywatelom i rezydentom unii, a także przedsiębiorcom identyfikowanie się i uwierzytelnianie swojej tożsamości online oraz offline w sposób bezpieczny, godny zaufania, przyjazny dla użytkownika, wygodny, w dostępnym i zharmonizowanym w całej Unii nowym narzędziu, jakim jest europejski portfel tożsamości cyfrowej, który zapewni zharmonizowany środek identyfikacji elektronicznej, umożliwiający uwierzytelnienie, ale co ważne, także udostępnienie danych związanych z tożsamością. Wskazuje się na konieczność bezpiecznego dostępu do usług publicznych i prywatnych za pomocą ulepszonego systemu usług zaufania i zweryfikowanych dowodów potwierdzających tożsamość oraz elektronicznych poświadczeń atrybutów, stanowiących podwalinę dokumentu 3.0. Jest to o tyle istotne, iż aktualnie funkcjonujące systemy w zakresie tożsamości cyfrowej nie są dostępne dla całej populacji, często uniemożliwiają dostęp transgraniczny i głównie funkcjonują krajowo czy też lokalnie. Według danych Komisji UE[32] tylko 14% kluczowych dostawców usług publicznych we wszystkich państwach wspólnoty pozwala na transgraniczne uwierzytelnienie za pomocą systemu e-ID, a wzrost wolumenu zdarzeń identyfikacji pomiędzy krajami jest bardzo powolny, praktycznie niewpływający na szersze transgraniczne operacje. Należy stwierdzić, iż tożsamość cyfrowa na rynku europejskim głównie odnosi się do działań lokalnych i do kontaktów z administracją. W wielu przypadkach, jak np. w Polsce, częsta, wręcz notoryczna jest wadliwość uwierzytelniania, czego przykładem jest mObywatel, gdzie prawidłowa weryfikacja dokumentu i jego uwierzytelnienie dokonywane jest najczęściej przez instytucje finansowe i podmioty zaufania publicznego (jak

[29] Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2024/1689 z dnia 13 czerwca 2024 w sprawie ustanowienia zharmonizowanych przepisów dotyczących sztucznej inteligencji oraz zmiany rozporządzeń nr 300/2008, nr 167/2013, 168/2013, 2018/858, 2018/1139 i 2019/2144 oraz dyrektyw 2014/90/UE, 2016/797 i 2020/1828 (akt w sprawie sztucznej inteligencji). Dz.Urz UE L 12.7.2024 2024/1689

[30] Dz.Urz UE L 30.4.2024 2024/1183

[31] Dz.Urz C 23.1.2023 2023/C 23/01

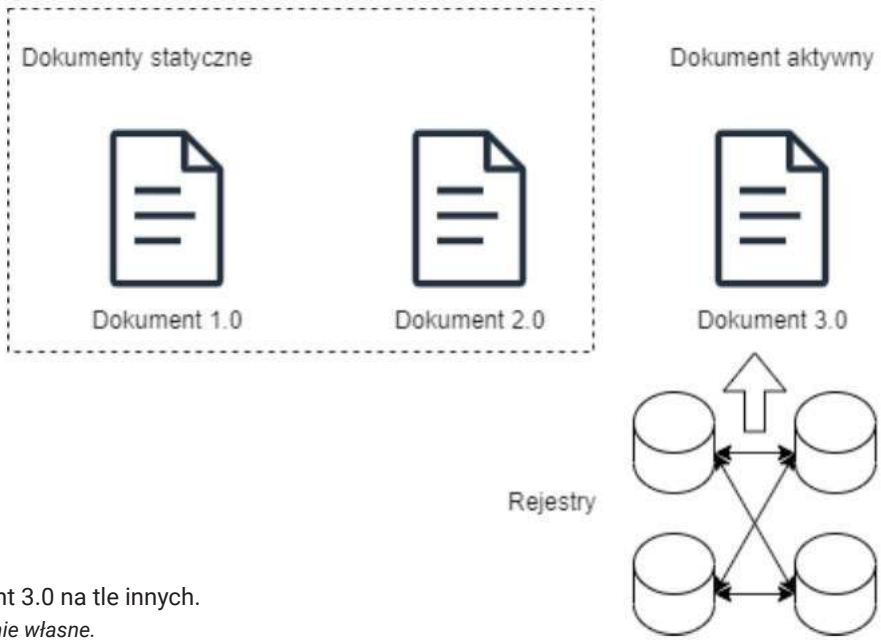
[32] https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/ europe-fit-digital-age/european-digital-identity_en Pobrano 5 sierpnia 2024

notariusze) ale już nie przez urzędy czy nawet służby policji, dla których często wystarczy okazanie dokumentu i to offline (brak szkoleń i wiedzy beneficjentów), bez jakiegokolwiek dalszego uwierzytelniania.

Równocześnie w obrocie prywatnym, dla bardzo wielu usług cyfrowych europejscy obywatele oraz rezydenci identyfikują się poprzez prywatne narzędzia i identyfikatory, jak Google, Facebook czy inne, tracąc przy tym kontrolę nad przekazywanymi danymi, praktycznie bez możliwości zarządzania nimi. Pokazuje to z jednej strony potrzebę utworzenia jednolitego europejskiego, transgranicznego narzędzia uwiarygodniającego tożsamość i umożliwiającego zarządzania danymi, z drugiej strony pokazuje olbrzymią akceptację dla takich rozwiązań, wręcz powszechność ich wykorzystania.

Tradycyjny dokument 1.0 czy 2.0 ujęty jest w zamkniętą całość. Różna jest moc dowodowa takiego dokumentu, może być też w różnej formie w zależności od sposobu jego sporządzenia, podpisania, uczestnictwa podmiotów zaufania publicznego itd. Treść tradycyjnego dokumentu składa się z różnych elementów – przykładowo tożsamość sporządzającego dokument, tożsamość stron czynności prawnych, tożsamość adresata dokumentu i podmiotu go wydającego (np. decyzja), treść oświadczenia lub stwierdzonego faktu, uprawnienia poszczególnych stron (np. licencje, pełnomocnictwa) dołączane do dokumentu tradycyjnego lub stwierdzenie ich faktu w treści itd. Całość jednak stanowi integralną całość, ewentualnie z załącznikami. W zależności od dokumentu może on być w formie dokumentowej, pisemnej, elektronicznej itp. – ale także jako całość. Jeżeli jest powiązany z domniemaniami prawnymi – także jako całość.

Dokument 3.0 jako dokument aktywny funkcjonuje w obrocie gospodarczym odmiennie niż 2.0 i 1.0. Składa się z wielu, łączących się w systemie elementów. Każdy z nich może podlegać pod inny rygor prawny, być powiązany z innymi domniemaniami, ulegać zmianie w czasie. Ważne, aby była możliwość zarządzania tymi danymi, ale także możliwość sięgnięcia po dane i informacje wcześniejsze, historyczne. W przypadku dokumentów 1.0 i 2.0 w związku ze zmianami faktów, danych itd. należało/należy wydać/dostarczyć nowy dokument zawierający bardziej aktualne dane. Dlatego też z niektórymi dokumentami 1.0 oraz 2.0 domniemania czy też skutki prawne powiązane są czasowo, co powoduje konieczność dostarczenia, nowych „świeżych" dokumentów czy to do banku, urzędu, notariusza itd. Aktualne dane, czy też „w miarę aktualne" dane funkcjonują w rejestrach, bazach, danych i archiwach. Dokumenty 1.0 czy też 2.0 są nośnikiem tychże danych tworzących informację, ale w sposób statyczny. Dokument 3.0 także jest nośnikiem, jednakże aktywnym, co oznacza, iż zmiana któregoś z elementów dokumentu (np. utrata uprawnień strony czy też zmiana adresu, stanu statusu majątkowego małżeńskiego) w chwili dokonania tejże zmiany, a właściwie zapisana w systemie czy części systemu składającego się na dokument 3.0 jest od razu odnotowywalna, a co za tym idzie – weryfikowalna, a co ważne dla usług cyfrowych od razu może na nią wpływać (Rys. 2). Rozporządzenie eIDAS2 ambitnie stawia za cel rozwój nowoczesnych interaktywnych usług cyfrowych, w tym usług zaufania, a co szczególnie istotne dla banków kwalifikowanych usług zaufania. Ich zbudowanie wymagać będzie jednak sporo czasu, a także zmiany podejścia wielu podmiotów, w tym goverment, na który nałożono szereg obowiązków, w tym wydawanie atrybutów



Rys. 2. Dokument 3.0 na tle innych.
Źródło: Opracowanie własne.

i kwalifikowanych atrybutów potwierdzających prawa czy też uprawniania podmiotów. Dla sukcesu powyższego procesu konieczne jest zbudowanie całego systemu dla dokumentu 3.0, w którym istotną i ważną rolę przyjmują banki, które do 2027 r. mają wprowadzić zmiany w systemach uwzględniające tożsamość cyfrową eIDAS2 jako silne uwierzytelnienie.

Dokument 3.0 to inaczej dokument rozproszony. A przepisy eIDAS2, szczególnie wydane na ich podstawie przepisy wykonawcze, stanowią podstawę standaryzacji tego systemu, obok innych jak dotyczące RODO, AML itd.

3.2. EU Wallet – Europejski portfel tożsamości cyfrowej

3.2.1. Portfele tożsamości cyfrowej – założenia ogólne[33]

Rozporządzenie eIDAS1 dało podstawy prawne do wprowadzenia identyfikacji tożsamości cyfrowej w całej UE poprzez krajowe narzędzia identyfikacji notyfikowane przez Komisję Europejską na podstawie art. 9. Wprowadzone narzędzia weryfikacji tożsamości poprzez węzły krajowe nie do końca spełniły oczekiwania w zakresie rozwoju, ale przede wszystkim transgraniczności tożsamości cyfrowej. Dlatego w eIDAS2 zaproponowano rozwiązanie oparte o koncepcję Self Sovereign Identity (SSI) – nowoczesne narzędzie nie tylko identyfikacji, ale także zarządzania nią. Model SSI pozwala samodzielnie użytkownikom (obywatelom UE oraz rezydentom) przekazywać swoje dane do usługodawców gwarantując wysoki poziom prywatności oraz bezpieczeństwa, ale – co istotne – samodzielną kontrolę swoich danych, możliwość nimi zarządzania, a także możliwość weryfikacji, komu dane zostały udostępnione i czy dalej ma do nich dostęp. Dotychczasowe i aktualnie funkcjonujące narzędzia identyfikacji elektronicznej i tożsamości cyfrowej nie pozwalały na taką kontrolę. Przepisy RODO pozwalają nam wprawdzie na kontrolę, zmianę oraz żądanie usunięcia danych osobowych, jednakże nie dają narzędzia do zarządzania nimi. Cóż z tego, iż mam prawo do żądania usunięcia danych, gdy (co jest bardzo częstym przypadkiem w odniesieniu do konsumentów) nawet nie pamiętamy, iż w ramach danej usługi online czy offline danemu podmiotowi swoje dane przekazano.

SSI należy zdefiniować jako system zarządzania tożsamością stworzony do działania niezależnie od podmiotów publicznych lub prywatnych, oparty na zdecentralizowanych architekturach technologicznych i zaprojektowany tak, aby priorytetowo traktować bezpieczeństwo użytkownika, prywatność, indywidualną autonomię i usamodzielnienie[34].

Powyższa koncepcja została opracowana jako wyraz osobistej suwerenności cyfrowej przez Christophera Allena w 2016 r. Wykorzystał ją do opisania opartych na zasadach ram, które stworzyłyby zdecentralizowany system zorientowanych na użytkownika, samozarządzających się, interoperacyjnych tożsamości cyfrowych. System ten opiera się na dziesięciu fundamentalnych zasadach, zgodnie z Prawami Tożsamości Kima Camerona (2005 r.): 1) istnienie, 2) kontrola, 3) dostęp, 4) przejrzystość, 5) trwałość, 6) przenośność, 7) interoperacyjność, 8) zgoda, 9) minimalizacja, 10) ochrona, które miałyby stanowić (brakującą) „warstwę tożsamości" w Internecie[35].

„Techniczny wymiar SSI był do tej pory zakotwiczony w zdecentralizowanych identyfikatorach (DID), weryfikowalnych roszczeniach (VC) i innych powiązanych standardach World Wide Web Consortium (W3C), tej samej organizacji zajmującej się standardami internetowymi, która stoi za powszechnymi protokołami internetowymi, które znamy dzisiaj, takimi jak HTML i HTTPS. Te zdecentralizowane standardy tożsamości są zestawem standardów technicznych służących do łączenia i kojarzenia danych dotyczących podmiotu tożsamości w trwały i uniwersalny sposób, tak aby podmiot tożsamości nie tylko miał kontrolę nad sposobem łączenia i wykorzystywania informacji, ale także był właścicielem profilu, a nie zewnętrznym dostawcą usług. W ten sposób zestaw powiązanych danych, zwanych poświadczeniami lub oświadczeniami, może być globalnie przenośny. Poświadczenia mogą obejmować dane uwierzytelniające, które przyznają podmiotowi tożsamości prawa dostępu lub przywileje, lub mogą obejmować weryfikację informacji, takich jak link do dokumentów tożsamości, certyfikatów zawodowych, historii kredytowej lub innych danych lub informacji. Każde poświadczenie powiązane z podmiotem tożsamości musi być podpisane cyfrowo przez inny podmiot tożsamości.

W ramach unikalności dwie osoby nie powinny mieć tego samego identyfikatora (unikalność), przy czym identyfikator nie może odnosić się do więcej niż jednego podmiotu tożsamości. Warunek ten można spełnić poprzez zastosowanie kryptografii, tj. matematyczne zapewnienie, że wydawane są tylko unikalne identyfikatory i zapobieganie ich ponownemu wydaniu.

[33] Szerzej Tożsamość cyfrowa – regulacje europejskie. Raport opracowany na zlecenie Programu Analityczno-Badawczego Fundacji Warszawski Instytut Bankowości, Warszawa 2024, PAB WIB 9/2024

[34] https://policyreview.info/glossary/self-sovereign-identity#footnote1_iruxuus Pobrano 6 sierpnia 2024r.

[35] https://www.lifewithalacrity.com/article/the-path-to-self-sovereign-identity/ Pobrano 6 sierpnia 2024r.

Ogólnie rzecz biorąc, SSI jest wdrażane jako systemy zarządzania tożsamością powiązane z blockchain, ale niezależne od blockchain, które kierują się podstawową zasadą projektowania zorientowanego na użytkownika, wykorzystując standardy techniczne, które umożliwiają generowane przez użytkowników i kontrolowane przez użytkowników zdecentralizowane identyfikatory, powiązane dane uwierzytelniające i poświadczenia"[36].

W praktyce portfel tożsamości funkcjonuje w oparciu o weryfikowalne poświadczenia, które użytkownicy uzyskują od różnych podmiotów. Mogą to być podmioty prywatne, ale dla pewności obrotu i wysokiego poziomu wiarygodności większe znaczenie mają poświadczenia wydawane przez instytucje goverment czy też banki. Zresztą w tym kierunku zmierza eIDAS2, o czym poniżej. Self-Sovereign Identity na wysokim poziomie opiera się na cyfrowych odpowiednikach tradycyjnych dokumentów i nie tylko tych dotyczących tożsamości. Weryfikowalne poświadczenia umożliwiają użytkownikom wykazywanie, a nawet udawadnianie określonych danych czy informacji bez konieczności ujawniania wszystkich, czy też dodatkowych danych osobistych. Nie jest to jednakże odpowiednik naszych dokumentów w mObywatelu czy też statyczna wizualizacja dokumentu tradycyjnego, tylko znacznie bardziej złożony system umożliwiający zautomatyzowaną weryfikację, ale i także tokenizację usług. SSI opiera się na decentralizacji eliminując potrzebę centralnych węzłów tożsamości i usług identyfikacji, jakiego dzisiaj wymaga mObywatel czy polski Profil Zaufany. W chwili obecnej SSI opiera się o mechanizm Verifable Credentials[37], gdzie istotnym elementem jest Verifiable Data Registery[3839]. To posiadacz portfela decyduje, które dane są udostępniane weryfikatorom, a stosując technologię tzw. zerowej wiedzy (*zero knowladge proofs*) pozwalają na udowodnianie posiadania poświadczenia (czyli udowadnianie uprawnień, np. osiągniętego wieku) bez konieczności ujawniania danych, informacji czy w ogóle poświadczenia. Weryfikowalne poświadczenia są także odporne na fałszerstwa, co stanowi solidne podstawy dla dokumentu 3.0.

3.2.2. EU Wallet[40]

W ramach projektu Europejskich Ram Tożsamości Cyfrowej wypracowany został koncept Europejskiego Portfela Tożsamości Cyfrowej oparty o SSI i umocowany w przepisach eIDAS2. Obok założeń Self Severeign Identity ma umożliwiać składanie kwalifikowanych podpisów elektronicznych i pieczęci elektronicznych (por. definicja i aspekty prawne w punkcie niżej). Zgodnie z zasadą neutralności technologicznej, EU Wallet będzie funkcjonował zarówno jako Edge wallet jak także jako cloud wallet, czyli zarówno jako rozwiązanie mobilne na telefonach czy też tabletach, ale także jako aplikacja deskopowa oraz cloud. Odmiennie od dotychczasowej identyfikacji opartej o eIDAS1, oprócz osób fizycznych EU Wallet będzie funkcjonował jako narzędzie pozwalające na identyfikację osoby prawnej, ale także osoby reprezentującej osobę prawną. Celem Komisji jest utworzenie zestandaryzowanego, interoperacyjnego i na wysokim poziomie bezpieczeństwa (NIS2) narzędzia pozwalającego na zarządzanie danymi, w tym tożsamością przez obywateli, rezydentów i inne podmioty, w tym osoby prawne z siedzibą w UE.

Jednolity standard jest gwarancją transgraniczności rozwiązania. Każde państwo samo może wydawać swoje portfele lub wskazać portfel, który będzie wykorzystywało (czy to dostawcy komercyjnego, prywatnego, czy też innego państwa), dzięki czemu będzie on akceptowalny w całej UE, a dane mogą być przenaszalne z jednego portfela do innego.

Security wymagane dla EU Wallet odnosi się do wysokiego poziomu bezpieczeństwa, zarówno w odniesieniu do potwierdzania tożsamości (zgodnie z art. eIDAS2), jak i atrybutów, ale także wymogów NIS2 dla podmiotów krytycznych i implementacji dyrektywy w krajowych porządkach prawnych.

Bezpieczeństwo jest powiązane z pełną **kontrolą użytkownika** nad swoimi danymi zgodnie z założeniami SSI, zwiększając prywatność i jeszcze głębiej realizując wymagania RODO. EU Wallet będzie służyć jako

[36] https://policyreview.info/glossary/self-sovereign-identity#footnote1_iruxuus pobrano 6 sierpnia 2024r.

[37] Verifiable Credentials Data Model v2.0; https://www.w3.org/TR/vc-data-model-2.0/ pobrano 6 sierpnia 2024r. Na szczególną uwagę zasługuje zdefiniowana terminologia oraz schematy oraz normy działania.

[38] Szerzej Tożsamość cyfrowa – regulacje europejskie. Raport opracowany na zlecenie Programu Analityczno-Badawczego Fundacji Warszawski Instytut Bankowości, Warszawa 2024, PAB WIB 9/2024

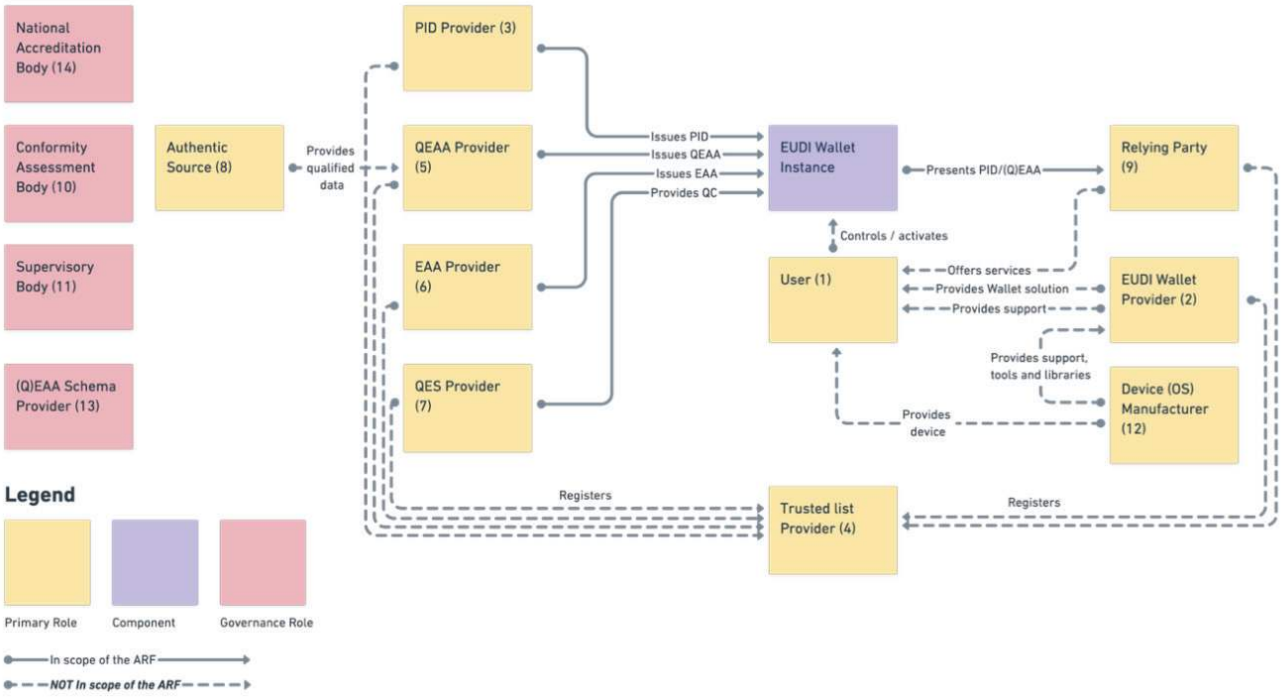
[39] Wykorzystywane w chwili obecnej są dwa typy portfeli – krawędziowy (edge wallet) i portfel w chmurze (cloud wallet). Edge wallet jest oprogramowaniem zainstalowanym na urządzeniu końcowym użytkownika. Dane, w tym klucze przechowywane są lokalnie na urządzeniu użytkownika. Podobnie jak tradycyjny portfel zawiera nasze dowody osobiste, prawo jazdy itd., ma on pełną kontrolę nad danymi, może także funkcjonować offline. Ale to na użytkowniku leży pełna odpowiedzialność zarówno za bezpieczeństwo aplikacji jak i urządzenia. Cloud Wallet przechowuje dane w chmurze. Uniezależnia to użytkownika od urządzenia. Ma dostęp do portfela z dowolnego urządzenia. Nie ma więc ryzyka, jakie jest związane z utratą urządzenia w systemie edge wallet. Z drugiej strony uzależniają od dostawcy oraz wymagają dostępu do sieci. Szerzej https://decentralized-id.com/development/wallets/ pobrano 6 sierpnia 2024 r.

[40] Niniejszy punkt jest skrótem analizy przedstawionej i przygotowanej dla WIB w Tożsamość cyfrowa – regulacje europejskie. Raport opracowany na zlecenie Programu Analityczno-Badawczego Fundacji Warszawski Instytut Bankowości, Warszawa 2024, PAB WIB 9/2024

narzędzie pozwalające na dostęp dla szerokiej gamy usług, zarówno goverment (do 2030 roku większość usług goverment ma być dostępna online), jak i prywatnych, komercyjnych jak i niekomercyjnych, **a od 2027 roku do usług bankowych, także gdy przepisy wymagają silnej identyfikacji**. Inaczej ujmując ma być narzędziem **interoperacyjnym**. Portfel EU Wallet ma na celu ułatwienie spełnienia wymogów silnego uwierzytelniania klienta. Zgodnie ze strategią Komisji w zakresie płatności detalicznych przypadek użycia zostanie opracowany w ścisłej współpracy z grupami doradczymi państw członkowskich ds. płatności detalicznych i branży finansowej[41].

Przepisy eIDAS2 wymagają **dostępności** do europejskiej tożsamości cyfrowej zarówno **online** dla usług cyfrowych, jak także umożliwiają uwierzytelnienie **offline**, zarówno w ramach uwierzytelnienia lokalnego (krajowego) jak i transgranicznego, z czym do tej pory nie mieliśmy do czynienia w ramach eIDAS1.

EU Wallet ma opierać się o zestaw narzędzi[42] uzgodniony wspólnie przez państwa członkowskie. Europejskie ramy tożsamości zostają wprowadzone w oparciu o kompleksową architekturę techniczną i ramy odniesienia, zestaw wspólnych norm technicznych i dokumentów referencyjnych oraz zestaw wytycznych i opisów najlepszych praktyk w obszarach: funkcje dla europejskich portfeli tożsamości cyfrowej dla użytkownika, w tym podpisywanie przy pomocy kwalifikowanych podpisów elektronicznych, interfejsy i protokoły, poziom zaufania, zgłaszanie stron ufających i weryfikacja ich autentyczności, elektroniczne poświadczanie atrybutów, mechanizmy weryfikacji ważności elektronicznych poświadczeń atrybutów i danych identyfikujących osoby, certyfikacja, publikacja wykazu europejskich portfeli tożsamości cyfrowej, przekazywanie informacji o naruszeniach bezpieczeństwa, weryfikacja tożsamości i atrybutów przez dostawców kwalifikowanych usług zaufania w zakresie elektronicznych poświadczeń atrybutów, kojarzenie tożsamości, minimalny wykaz atrybutów



1. End Users of EUDi Wallets
2. EUDI Wallet Providers
3. Person identification Data Providers
4. Trusted Lists providers
5. Qualifield Electronic Attestation of Attributes (QEAA) Providers
6. Non-qualifield Electronic Attestation of Attributes (EAA) Providers
7. Qualifield and non-quafield certificate for electronic signature/seal Providers
8. Authentic Sources
9. Relying Parties
10. Conformity Assessment Bodies (CAB)
11. Supervisory bodies
12. Device manufacturers and related subsystems providers
13. (Q)EAA Schema Providers
14. National Accreditation Bodies

Rys. 3. Przegląd ról portfela EUDI.
Źródło: https://eu-digital-identity-wallet.github.io/eudi-doc-architecture-and-reference-framework/1.1.0/arf/

[41] Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on a Retail Payments Strategy for the EU COM/2020/592 final.

[42] https://eur-lex.europa.eu/legal-content/PL/TXT/HTML/?uri=CELEX:32021H0946 pobrano 6 sierpnia 2024r.; https://www.intesigroup.com/en/wp-content/uploads/sites/4/2023/02/ARF-v1.0.0-final.pdf pobrano 6 sierpnia 2024r.

z autentycznych źródeł, takich jak adresy, wiek, płeć, stan cywilny, skład rodziny, obywatelstwo, wykształcenie i kwalifikacje zawodowe, tytuły i licencje, inne zezwolenia oraz dane dotyczące płatności, katalog atrybutów i systemy poświadczania atrybutów oraz procedury weryfikacji na potrzeby kwalifikowanych elektronicznych poświadczeń atrybutów[43].

3.2.3. EU Wallet w eIDAS2 – aspekty prawne i ich wpływ na dokument 3.0

3.2.3.1. Wprowadzenie

Europejski portfel tożsamości cyfrowej (EU Wallet) jest prawną podstawą dla unijnej koncepcji SSI, będąc swoistym „integratorem" danych w ramach dokumentu 3.0 umożliwiającym zarządzanie danymi, a co za tym idzie – narzędziem pozwalającym na zarządzanie tożsamością, ale także zarządzaniem dokumentami.

Zgodnie z art. 3 pkt. 42 przez europejski portfel tożsamości cyfrowej należy rozumieć środek komunikacji elektronicznej, który umożliwia użytkownikowi bezpieczne przechowywanie i walidację danych identyfikujących osobę i elektronicznych poświadczeń atrybutów oraz bezpieczne zarządzanie tymi danymi i poświadczeniami na potrzeby udostępniania ich stronom ufającym oraz innym użytkownikom europejskich portfeli tożsamości cyfrowej, i który umożliwia składanie kwalifikowanych podpisów elektronicznych lub kwalifikowanych pieczęci elektronicznych. Na potrzeby eIDAS zdefiniowano „środek identyfikacji elektronicznej" jako materialną i – co istotne w aspekcie dokumentu 3.0 – niematerialną jednostkę zawierająca dane identyfikujące osobę i używaną do celów uwierzytelniania dla usługi online lub, w stosownych przypadkach, dla usługi offline, gdzie uwierzytelnianie oznacza proces elektroniczny, który umożliwia potwierdzenie identyfikacji elektronicznej osoby fizycznej lub prawnej, lub potwierdzenie pochodzenia integralności danych w postaci elektronicznej.

Warto już w tym miejscu zwrócić uwagę, iż w chwili obecnej pomimo wypowiedzi niektórych polityków mObywatel nie spełnia wymogów definicji dla europejskiego portfela tożsamości, jest co najwyżej notyfikowanym środkiem identyfikacji elektronicznej na podstawie art. 9 eIDAS.

Europejskie portfele tożsamości cyfrowej mają ułatwiać stosowanie zasady jednorazowości, a co za tym idzie zmniejszać obciążenie administracyjne, a także wspierać transgraniczną mobilność obywateli i rezydentów unii oraz przedsiębiorców w całej Unii, a także sprzyjać rozwojowi interoperacyjnych usług administracji elektronicznej. W tym celu mają cechować się transgranicznością w zakresie wymiany danych oraz interoperacyjnością.

Zgodnie z preambułą wszystkie europejskie portfele tożsamości cyfrowej powinny umożliwiać użytkownikom elektroniczne identyfikowanie się i uwierzytelnianie online i w trybie offline w kontekście transgranicznym na potrzeby dostępu zarówno do usług publicznych, jak i prywatnych bez uszczerbku dla prerogatyw państw członkowskich w zakresie identyfikacji ich obywateli oraz rezydentów. Europejskie portfele tożsamości cyfrowej mogą także zaspokajać potrzeby instytucjonalne danej administracji publicznej, organizacji międzynarodowych oraz instytucji, organów jednostek organizacyjnych Unii. Obok uwierzytelnienia online dostępne ma być uwierzytelnienie offline – w szczególności w tych sektorach, gdzie usługi są często świadczone w ramach kontaktu osobistego, a jest konieczna weryfikacja tożsamości tudzież autentyczności atrybutów w oparciu o wysoki poziom bezpieczeństwa dla systemów identyfikacji elektronicznej (także wynikający z NIS2). Europejskie portfele tożsamości cyfrowej powinny wykorzystywać potencjał, jaki oferują rozwiązania zabezpieczające przed manipulacją, takie jak secure elements, w celu zapewnienia zgodności z wymogami bezpieczeństwa wynikającymi zarówno z rozporządzenia eIDAS jak i DORA czy dyrektywy NIS2 oraz przepisów implementowanych na jej podstawie. EU Wallet jest narzędziem umożliwiającym składanie kwalifikowanych podpisów elektronicznych domyślnie, ale – co istotne – nieodpłatnie i bez konieczności przechodzenia jakichkolwiek dodatkowych procedur uwierzytelniania czy procedur administracyjnych. Spowoduje to zmianę w zakresie onboardingu przy usłudze kwalifikowanego podpisu elektronicznego. Europejski portfel tożsamości cyfrowej ma umożliwić korzystanie z upoważnień, ale także pełnomocnictw w postaci elektronicznej. Państwa członkowskie mają obowiązek zapewnienia niezakłóconej interoperacyjności, w tym transgraniczności oraz odpowiedniego podniesienia bezpieczeństwa informatycznego, wzmocnienia na cyberataki, a tym samym znaczącego zmniejszenia potencjalnego ryzyka związanego z postępującą cyfryzacją dla obywateli i rezydentów Unii oraz, co jest nowością w stosunku co do eIDAS1, także dla przedsiębiorstw. EU Wallet jest elementem zgodnym z wysokim poziomem bezpieczeństwa określonym w Dyrektywie NIS2, a podmioty wydające europejski portfel tożsamości cyfrowej są uznawane za podmiot krytyczny, podlegający

[43] https://www.intesigroup.com/en/wp-content/uploads/sites/4/2023/02/ARF-v1.0.0-final.pdf pobrano 12 sierpnia 2024r. Patrz także Raport opracowany na zlecenie Programu Analityczno-Badawczego Fundacji Warszawski Instytut Bankowości, Warszawa 2024, PAB WIB 9/2024.

najwyższym wymogom w zakresie cyberbezpieczeństwa[44].

3.2.3.2. Ramy prawne

3.2.3.2.1. Zapewnienie Europejskiego portfela tożsamości

Państwa członkowskie, zgodnie z art. 5a eIDAS2, są zobligowane do zapewnienia swoim obywatelom co najmniej jeden EU Wallet w terminie najpóźniej do 21 listopada 2026 r., co z punktu ujęcia prac technologicznych oraz ewentualnie implementacyjnych eIDAS do krajowych porządków prawnych jest bardzo krótkim okresem. Dobrze by było, aby banki oraz inne instytucje finansowe przygotowały swoją infrastrukturę na EU Wallet i europejską tożsamość cyfrową w tym samym terminie. Do dnia 21 listopada 2024 na podstawie delegacji z art. 5a ust. 23 oraz art. 5c ust. 6 zostaną opublikowane przepisy wykonawcze, normy i architektura dla portfela.

Państwa mogą zapewnić portfel europejski samodzielnie przez siebie (takie wstępne zapowiedzi podnosiła także Polska), od innego państwa na podstawie upoważnienia tego państwa (lub konsorcjum państw tworzących europejski portfel tożsamości cyfrowej) lub utworzony zgodnie z przepisami wykonawczymi przez podmiot trzeci, lecz zaakceptowany i uznany przez państwo lub przez państwa członkowskie. Istotne m.in. dla dostosowania systemów bankowych do tożsamości cyfrowej i EU Wallet jest zapewnienie rozporządzeniem licencji otwartego oprogramowania dla kodu źródłowego komponentów oprogramowania użytkowego EU Wallet. Dotyczy to kodu źródłowego zainstalowanego na urządzeniach użytkownika. Odnośnie innych komponentów państwa członkowskie z uzasadnionych powodów (głównie bezpieczeństwa, chociaż nie tylko) mogą odmówić ujawnienia (art. 5a ust.3).

3.2.3.2.2. Zarządzanie europejskim portfelem tożsamości

Do momentu wejścia w życie eIDAS2 możliwość zarządzania swoimi danymi przez obywateli bądź rezydentów UE była dosyć ograniczona (de facto ograniczała się do możliwości zawieszenia lub unieważnienia środków identyfikacji elektronicznej). Koncepcja Self Severeign Identity zmienia tę sytuację. EU Wallet musi umożliwić użytkownikowi, w sposób jasny, przejrzysty a co za tym idzie – zrozumiały i identyfikowalny dla użytkownika (art. 5a ust.4):

1. możliwość bezpiecznego (zgodnie z NIS2 i wymogami dla podmiotów krytycznych) żądania, otrzymywania, wybierania, łączenia, przechowywania, usuwania, udostępniania i prezentacji i to pod wyłączną kontrolą użytkownika (bez możliwości kontroli przez podmioty trzecie, w tym dostawcę komponentu EU Wallet) danych identyfikujących osobę;

2. możliwość bezpiecznego (zgodnie z NIS2 i wymogami dla podmiotów krytycznych) żądania, otrzymywania, wybierania, łączenia, przechowywania, usuwania, udostępniania i prezentacji, pod wyłączną kontrolą użytkownika, w stosownych przypadkach, w połączeniu z poświadczeniami atrybutów[45], uwierzytelniania tożsamości wobec stron ufających[46] w trybie online oraz w stosownych przypadkach w trybie offline, w celu uzyskania dostępu do usług publicznych lub prywatnych;

3. możliwość selektywnego ujawniania danych (wybór wyłącznie przez użytkownika);

4. możliwość generowania pseudonimów, możliwość wykorzystywania ich do wybranych usług i przechowywanie ich w postaci zaszyfrowanej, także w sposób lokalny (chociaż dopuszcza się także rozwiązania dodatkowe, np. chmurowe) w europejskim portfelu tożsamości;

5. możliwość bezpiecznego uwierzytelniania EU Wallet innej osoby;

6. możliwość otrzymywania i udostępniania z portfela innej osoby danych identyfikujących tę osobę (w tym także osobę prawną);

7. możliwość otrzymywania i udostępniania elektronicznych poświadczeń atrybutów[47] w bezpieczny sposób pomiędzy dwoma portfelami tożsamości cyfrowej;

8. możliwość dostępu do rejestru wszystkich transakcji przeprowadzonych z wykorzystaniem europejskiego portfela tożsamości cyfrowej za pomocą panelu zarządzania, w tym:

   a) możliwość przeglądania aktualnej listy stron ufających[48], z którymi użytkownik ustanowił połączenie, oraz w stosownych przypadkach wszystkich udostępnionych tymże podmiotom danych z portfela. Ta funkcja pozwoli zarówno na weryfikację, czy dany podmiot

[44] Szerzej rozdział 7 niniejszego raportu.

[45] Na temat poświadczonych atrybutów patrz pkt. 3.5.1.

[46] Na temat pojęcia stron ufających patrz pkt. 3.3.

[47] Na temat pojęcia atrybutu i kwalifikowanego atrybutu patrz podrozdział 3.5.

[48] Szerzej na temat stron ufających patrz podrozdział 3.3.

w dalszym ciągu jest podmiotem ufającym, ale także informacje historyczne. Funkcja ta jest bardzo istotna w aspekcie dokumentu 3.0, gdzie interoperacyjność wymaga dla użytkownika informacji, jakim podmiotom udostępnił czy też dalej udostępnia dane i jaki jest status tychże podmiotów. Czy są to strony ufające w znaczeniu eIDAS2, a więc podlegające pod regulacje tegoż rozporządzenia, czy też inne podmioty. W dokumencie 2.0 czy też 1.0 dane widnieją w treści dokumentu (są w nim zamknięte), w dokumencie 3.0 będą widoczne na panelu zarządzania portfelem;

b) umożliwienie w sposób łatwy od strony użytkownika trwałego usunięcia danych osobowych, zgodnie z artykułem 17 RODO (a więc gdy dane nie są już niezbędne do celów, w którym zostały zebrane lub w inny sposób przetwarzane, gdy wniesiono sprzeciw na podstawie art. 21 ust. 1 RODO, gdy cofnięto zgodę, na której opiera się przetwarzanie – przy czym w naszej ocenie żądanie usunięcia danych z panelu EU Wallet należy uznać za żądanie cofnięcia zgody). Portfel ma umożliwić bezpośrednią możliwość kontaktu i wysłania żądania z poziomu panelu zarządzania portfelem. Łatwość tej oraz poniższej funkcji należy oceniać według kryterium średnio wykształconego użytkownika;

c) umożliwienie w sposób łatwy zgłaszania strony ufającej właściwemu krajowemu organowi ochrony danych, w przypadku otrzymania przypuszczalnie niezgodnego z prawem lub podejrzanego żądania udostępnienia danych. Inaczej ujmując w przypadku podejrzenia naruszenia RODO EU Wallet ma umożliwić z poziomu panelu zarządzania portfelem natychmiastowe i łatwe dokonanie zgłoszenia.

9. Możliwość składania kwalifikowanych podpisów elektronicznych i – co ważne – kwalifikowanych pieczęci elektronicznych. Dostawcy kwalifikowanej usługi podpisu elektronicznego czy też pieczęci elektronicznej muszą dostosować swoje systemy do możliwości podpisywania z poziomu portfela tożsamości cyfrowej (na wzór możliwości podpisywania np. w Adobe). Ponieważ EU Wallet służą nie tylko do zarządzania tożsamością osoby fizycznej, ale także i prawnej, stąd możliwość składania kwalifikowanych pieczęci elektronicznych (które mogą używać wyłącznie inne podmioty niż osoby fizyczne). Ta funkcja ma zintegrować wszelkie działania dotyczące dokumentu, w tym dokumentu 3.0 w jednym miejscu;
10. Umożliwienie pobierania danych użytkownika, w tym poświadczeń atrybutów i konfiguracji, przy czym opcja ta jest uzależniona techniczną wykonalnością (np. z portfela do portfela). Standardem jest natomiast udostępnianie dostępu do danych i ich weryfikacja dla podmiotów ufających;
11. Swoboda w korzystaniu z portfela. Użytkownik ma mieć pełną swobodę w wyborze portfela tożsamości cyfrowej, także jako użytkownik. Rozporządzenie wprowadza prawo dla użytkownika do przenoszenia danych do innego portfela w każdej chwili, także do portfela innego państwa, czy też wskazanego lub akceptowalnego przez inne państwo, wprowadzając tym samym otwartość w wykorzystywaniu portfeli. Celem jest utworzenie wspólnego jednolitego rynku cyfrowego w całej UE, a nie rozwiązania lokalnego. Inaczej ujmując banki i instytucje finansowe są zobligowane do integracji swoich systemów nie z polskim, lokalnym (jeżeli taki zostanie przez nasze państwo wydany) portfelem, ale powinny się przygotować na akceptację danych, atrybutów itd. niezależnie od tego, w jakim portfelu się znajdują. Tym bardziej, iż klienci banków i instytucji finansowych, w każdej chwili mogą te dane przenieść na inny portfel.

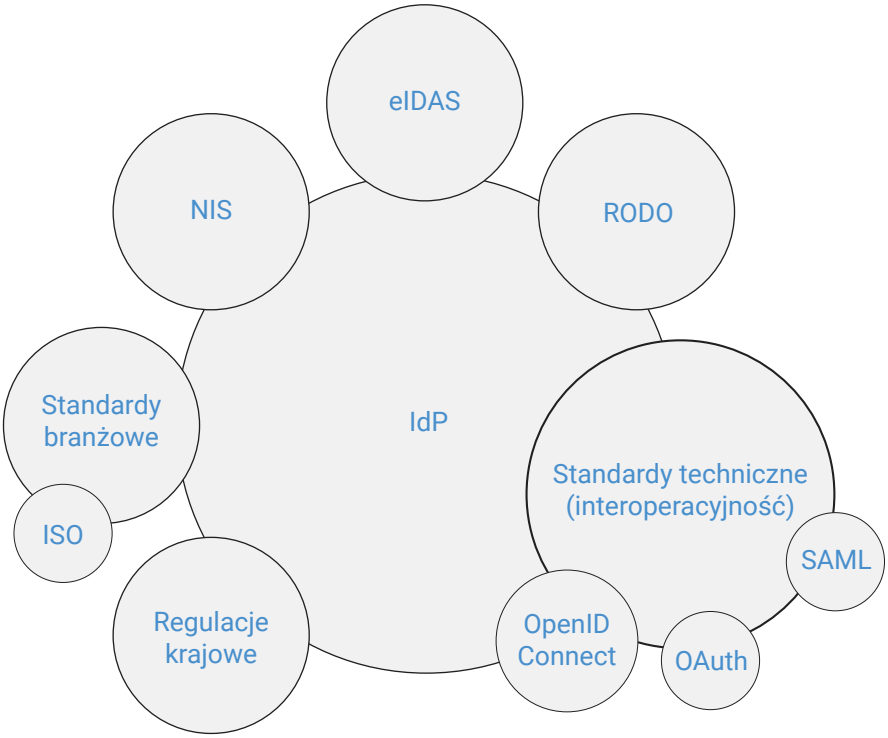
3.2.3.2.3. Zgodność EU Wallet z interfejsami

Dokument 3.0 mocno odbiega od jego odpowiedników wersji 2.0 i 1.0. Wymaga interakcji z wieloma systemami, pozyskiwania danych z różnych źródeł i baz. Podstawą dla jego skutecznego funkcjonowania jednolicie na rynku europejskim jest zgodność protokołów i interfejsów. Przykładem może tu być Google czy też Facebook, które jako podmioty prywatne umożliwiają weryfikację tożsamości w wielu systemach właśnie na zasadzie jednolitego standardu interfejsów i protokołów, za pomocą idei zaufanej trzeciej strony. Dostawca tożsamości (IdP) to system lub usługa do zarządzania tożsamością (Rys. 3).

Rozporządzenie eIDAS2 wprowadza obowiązek (art. 5 pkt 5) wprowadzenia przez dostawców EU Wallet zgodności ze wspólnymi protokołami i interfejsami (przepisy wykonawcze zostaną opublikowane w listopadzie 2024 r.):

– do celów wydawania danych identyfikujących osobę;

– do celów wydawania kwalifikowanych i niekwalifikowanych elektronicznych poświadczeń atrybutów lub kwalifikowanych i niekwalifikowanych certyfikatów do europejskiego portfela tożsamości cyfrowej;



Rys. 4. Ramy funkcjonowania IdP.
Źródło: Opracowanie własne.

- do integracji i na potrzeby stron ufających do celów żądania danych identyfikujących osobę elektronicznego poświadczenia atrybutów oraz ich walidacji. Inaczej ujmując, strony ufające – w tym banki i instytucje finansowe – integrując, według przepisów wykonawczych do eIDAS2, swoje systemy z EU Wallet, będą miały możliwość pozyskiwania jako strona ufająca danych identyfikujących, atrybuty oraz możliwość ich walidacji;

- na potrzeby udostępniania i prezentacji stron ufającym danych identyfikujących osobę, elektronicznych poświadczeń atrybutów lub selektywnie ujawnionych powiązanych danych w trybie online, oraz w stosownych przypadkach, w trybie offline. Interfejsy i protokoły mają umożliwić udostępnianie i prezentację całych danych, jak także (zgodnie z rozporządzeniem) selektywnie wybranych (wskazanych przez stronę ufającą lub przez użytkownika) selektywnych, wybranych danych (np. tylko wiek itd.). Tryb online jest obligatoryjny, offline w określonych przypadkach (m.in. ze względu na ograniczoną funkcjonalność trybu offline);

- do integracji z interfejsami i protokołami umożliwiającymi możliwość wyświetlenia unijnego znaku zaufania dla danego portfela;

- do bezpiecznej rejestracji użytkownika przy użyciu środka identyfikacji elektronicznej w europejskim portfelu tożsamości cyfrowej zgodnie z wysokim poziomem bezpieczeństwa albo ze średnim poziomem bezpieczeństwa w połączeniu z dodatkowymi procedurami zdalnej rejestracji, które łącznie spełnią wymogi dotyczące wysokiego poziomu bezpieczeństwa. W Polsce w chwili obecnej rejestrację do EU Wallet umożliwi Profil Zaufany lub mObywatel. **Warto w tym miejscu podjąć rozmowy, aby rejestracja mogła odbywać się także poprzez bankowe systemy identyfikacji tożsamości**.

- EU Wallet umożliwia otrzymywanie, walidowanie oraz udostępnianie danych identyfikujących osobę oraz elektroniczne poświadczenia atrybutów z innego europejskiego portfela tożsamości drugiego (innego) użytkownika. Konieczna jest zatem zgodność interfejsów i protokołów portfeli, aby takie dane w bezpieczny sposób przekazywać, udostępniać oraz walidować;

- UE Wallet jest narzędziem umożliwiającym składanie kwalifikowanego podpisu elektronicznego oraz kwalifikowanej pieczęci elektronicznej, w związku z tym wprowadza się zgodność interfejsów i protokołów dla ich składania poprzez

portfel za pomocą kwalifikowanych urządzeń do składania podpisów elektronicznych lub pieczęci elektronicznych,

– konieczna jest zgodność z interfejsami oraz protokołami dla funkcjonowania oraz możliwości realizowania wymogów z eIDAS2 przez podmioty ufające czy też w związku z ich funkcjonowaniem (także banki i instytucje finansowe) – w tym celu wymagana jest zgodność:

– dla możliwości przez ten podmiot automatycznego weryfikowania autentyczności i ważności europejskich portfeli tożsamości,

– dla możliwości zażądania przez użytkownika do strony ufającej usunięcia danych osobowych zgodnie z art. 17 RODO,

– dla możliwości zażądania przez użytkownika zgłoszenia strony ufającej (w tym banku lub instytucji finansowej) właściwemu krajowemu organowi ochrony danych osobowych w przypadku otrzymania niezgodnego z prawem lub podejrzanego żądania udostępniania danych. Ponieważ zarówno użytkownicy, jak i strony ufające mogą funkcjonować w odniesieniu do wszystkich podmiotów UE, w każdym kraju oznacza to konieczność wprowadzenia mechanizmu zgłaszania do wszystkich unijnych organów kontroli danych osobowych przez wszystkich użytkowników EU Wallet.

Powyższe wymogi interoperacyjności a także zgodności z interfejsami i protokołami odnoszą się do poziomu wspólnotowego i są jednolite dla wszystkich państw, dostawców EU Wallet, użytkowników czy też stron ufających. Państwa członkowskie, ponad powyższy obowiązek zgodnie z art. 5a ust. 7 (bez uszczerbku dla art. 5f czyli transgraniczności EU Wallet) mogą przewidzieć zgodnie z prawem krajowym dodatkowe funkcje dla europejskich portfeli tożsamości, w tym interoperacyjność z istniejącymi środkami identyfikacji elektronicznej, jednakże po spełnieniu wszystkich wymogów dla bezpieczeństwa interfejsów i protokołów dla EU Wallet.

3.2.3.2.4. Uprawnienia użytkownika europejskiego portfela tożsamości

EU Wallet jest dobrowolnym narzędziem dla użytkownika. W chwili obecnej ani przepisy unijne, ani krajowe nie nakładają na żadną ze stron, w szczególności na osoby fizyczne, obowiązku posiadania czy też używania europejskiego portfela tożsamości. Brak przymusu ustawowego, jaki jest związany chociażby z koniecznością posiadania dowodu tożsamości wskazuje, iż w pierwszym etapie wdrażania będzie to dodatkowy środek dla uwierzytelniania tożsamości, a nie jedyny. Jest to związane ze sporym wykluczeniem cyfrowym społeczeństw. W dalszym ciągu równolegle będą funkcjonowały tradycyjne dowody tożsamości. Osobom fizycznym, ale także prawnym, które nie korzystają z europejskiego portfela tożsamości nie można w żaden sposób ograniczyć ani utrudniać dostępu do usług publicznych, ale także prywatnych. Szczególnie istotne jest ostatnie ograniczenie, wskazujące na niemożność dla podmiotów prywatnych, które staną się stronami ufającymi, funkcjonowania wyłącznie w oparciu o tożsamość z EU Wallet. Muszą dopuścić tradycyjne metody weryfikacji tożsamości. Nie można też dla osób niekorzystających z EU Wallet ograniczać lub utrudniać dostępu do rynku pracy czy też swobody prowadzenia działalności gospodarczej.

Każdy użytkownik portfela musi mieć pełną kontrolę nad jego używaniem oraz nad znajdującymi się w nim danymi. Żaden z dostawców europejskiego portfela tożsamości nie ma prawa gromadzić informacji na temat używania portfela ani łączyć danych identyfikujących osobę lub jakichkolwiek innych danych osobowych przechowywanych w związku z jego używaniem z danymi osobowymi pochodzącymi z jakichkolwiek innych usług oferowanych przez tego dostawcę lub usług osób trzecich, które nie są niezbędne do świadczenia usługi portfela tożsamości cyfrowej. Łączenie tych danych jest jednakże możliwe, ale wyłącznie wtedy, gdy tego zażąda użytkownik (art. 5a ust. 14). Decyzja jest tutaj wyłączna po stronie użytkownika i nie można na nim tego wymuszać dla świadczenia usługi.

Dla bezpieczeństwa, ale także komfortu używania i zarządzania – dane osobowe związane z dostarczaniem europejskiego portfela tożsamości cyfrowej muszą być całkowicie i logicznie oddzielone od wszystkich innych danych będących w posiadaniu dostawcy danego EU Wallet.

Nakłada się obowiązek udostępniania europejskich portfeli tożsamości do użytku osobom z niepełnosprawnościami na równi z innymi użytkownikami. Zastosowanie ma tutaj także dyrektywa Parlamentu Europejskiego i Rady (UE) 2019/882 w sprawie wymogów dostępności produktów i usług, ale także jej implementacje. W aspekcie banków i instytucji finansowych dostępność dla osób z niepełnosprawnością dotyczy min.: terminali płatniczych, bankomatów, usług bankowości detalicznej, usług opartych o aplikacje mobilne.

3.3. Strony ufające

Zgodnie z art. 3 pkt.6 rozporządzenia eIDAS2 „stroną ufającą" jest osoba fizyczna lub prawna, która polega na identyfikacji elektronicznej, europejskich portfelach tożsamości cyfrowej lub innym środku identyfikacji elektronicznej lub usłudze zaufania. Banki już w dniu dzisiejszym korzystają z środków komunikacyjnych identyfikacji oraz z usług zaufania (które to pojęcie w eIDAS2 zostaje znacznie rozszerzone). Jednakże w przypadku zamiaru polegania na europejskim portfelu tożsamości cyfrowej na potrzeby świadczenia usług (zarówno dotyczy to usług publicznych, jak i prywatnych) za pomocą cyfrowej interakcji (w ocenie autorów zarówno online jak offline) strona ufająca musi się zarejestrować w państwie członkowskim w którym ma siedzibę jako strona ufająca. Po rejestracji może świadczyć usługi w całej UE.

Dla rejestracji konieczne jest przekazanie przez stronę ufającą:

1. informacji niezbędnych do uwierzytelnienia w EU Walletach użytkowników obejmujących: państwo członkowskie, w którym strona ufająca ma siedzibę, nazwę strony ufającej (np. Banku), wymagane przepisami numery rejestrowe (takie jak w Polsce KRS czy CEIDG), dane kontaktowe strony ufającej.

2. Istotne, i nowością w odniesieniu do dokumentu 2.0 i 1.0 w procesie rejestracji, konieczne jest wskazanie danych, które strona ufająca będzie pozyskiwała z portfela, pod rygorem zgłoszenia przez użytkownika krajowemu organowi nadzoru danych osobowych nadmiarowego żądania danych. Wyraźnie w art. 5b ust.3 wskazano, że nie wolno żądać przez stronę ufającą jakichkolwiek innych danych niż wpisane w rejestrze.

Informacje z rejestru są udostępniane przez państwa członkowskie publicznie, w sposób pozwalający na automatyczne ich przetwarzanie. Wszelkie zmiany podlegające rejestracji muszą być niezwłocznie przekazywane państwom członkowskim.

Strony ufające są uwierzytelniane w EU Wallet w sposób umożliwiający identyfikację oraz muszą potwierdzić swoją tożsamość.

W praktyce, w przypadku korzystania przez użytkownika z EU Wallet będzie informacja, iż dany podmiot, np. bank będący stroną ufającą, zamierza pozyskać dane tożsamości lub atrybut użytkownika. Uzyska on w tym momencie wszelkie informacje identyfikujące i uwierzytelniające ten bank oraz zgodność żądania danych z tym, co zrejestrowano w rejestrze stron ufających. Wszelkie żądania pozyskania danych zostają odnotowane w EU Wallet, zarówno gdy dojdzie do usługi, jak także gdy nie dokonano transakcji. Strona ufająca jest natomiast odpowiedzialna za przeprowadzenie na potrzeby usługi, przy interakcji online, uwierzytelnienia, ale też walidacji danych identyfikujących użytkownika europejskiego portfela tożsamości cyfrowej, ale także gdy korzysta z atrybutów – weryfikacji poświadczenia atrybutów.

Strona ufająca nie może przy usłudze elektronicznej odmówić używania pseudonimu lub pseudonimów użytkownika EU Wallet, w przypadkach, gdy identyfikacja nie jest wymagana na podstawie unijnych lub krajowych przepisów prawa. W odniesieniu do banków oraz instytucji finansowych, na potrzeby usług – a tym samym dokumentu 3.0 – z reguły identyfikacja użytkownika jest konieczna.

3.4. Transgraniczność EU Wallet

Podstawowym celem Polityki UE Cyfrowa Dekada 2030 jest utworzenie jednolitego rynku cyfrowego. Z wyżej przedstawionych dokumentów oraz analiz wynika, że jedną z dotychczasowych barier była faktyczna (bo nie prawna) niemożność dokonywania czynności zarówno w odniesieniu do prawa publicznego, jak i usług cyfrowych prywatnych w oparciu o dotychczasowe środki identyfikacji elektronicznej. Środki te zadziałały głównie w odniesieniu do usług lokalnych i powiązanych z Goverment.

Końcówka kadencji poprzedniego Parlamentu Europejskiego to szereg aktów prawnych regulujących rynek cyfrowy, jak DSA, MiCA, NIS2 itd. Wszystkie mają charakter transgraniczny.

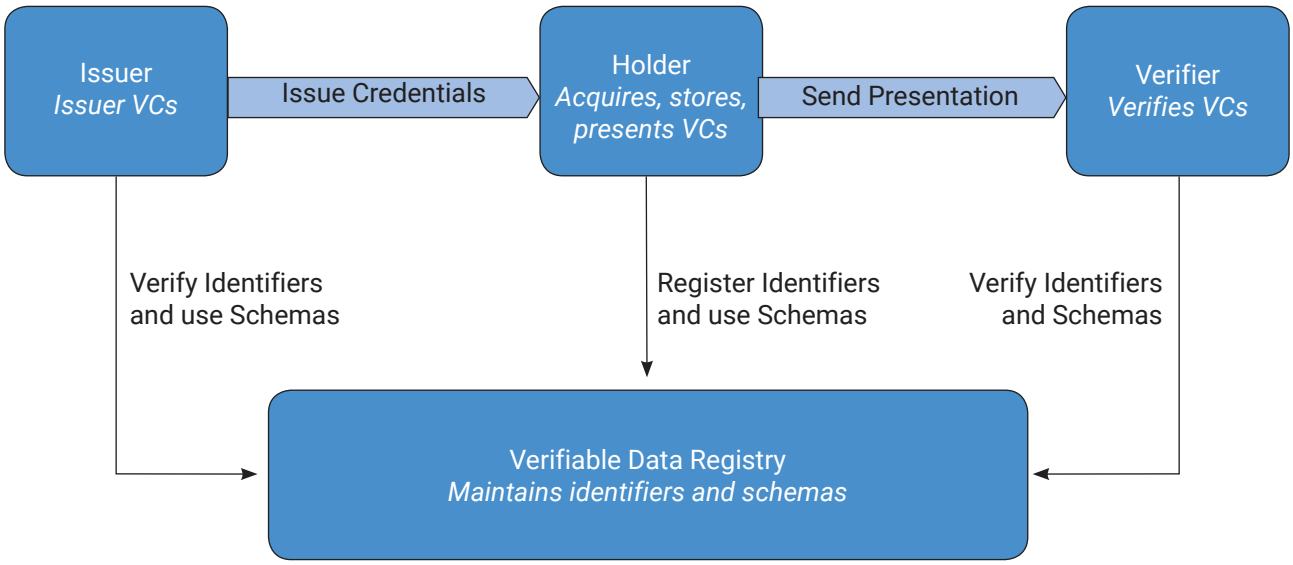
eIDAS2 poprzez portfel tożsamości cyfrowej, ale też i inne narzędzia niejako spina jednolitość europejskiego rynku cyfrowego. W art. 5 f pkt.1 wyraźnie wskazano, że w przypadku, gdy państwa członkowskie wymagają identyfikacji elektronicznej oraz uwierzytelnienia w celu dostępu do usługi online świadczonej przez podmiot sektora publicznego, muszą akceptować wszystkie europejskie portfele tożsamości cyfrowej, które są zgodne i wydane na podstawie eIDAS2. Koresponduje to z możliwością przenoszenia danych przez użytkownika z portfela do portfela, także wydanego czy też akceptowanego przez państwo inne niż miejsce zamieszkania użytkownika.

Naszym zdaniem, dla sukcesu europejskiego portfela tożsamości konieczna jest spora ilość usług cyfrowych wykorzystujących tożsamość cyfrową. Obok usług publicznych, ważny jest rozwój usług sektora prywatnego. Ważnym obszarem są usługi opierające się o silne uwierzytelnienie użytkowników do celów

identyfikacji elektronicznej (zarówno, gdy wymagają tego przepisy wspólnotowe, krajowe jak także wynika to z umów). Cyberbezpieczeństwo, ale także wymogi m.in. DORA, NIS2 są kluczowe w dzisiejszych usługach cyfrowych, w szczególności w odniesieniu do obszarów ważnych lub kluczowych jak transport, energia, bankowość i usługi finansowe, zabezpieczenie społeczne, zdrowie, woda pitna, usługi pocztowe, infrastruktura cyfrowa, edukacja czy telekomunikacja. Zgodnie z art. 5f pkt.2 podmioty świadczące te usługi (z reguły będą to prywatne podmioty ufające) są zobligowane w terminie 36 miesięcy od wydania przepisów wykonawczych do EU Wallet (czyli najpóźniej 21 maja 2026 r.) do akceptacji EU Wallet jako silnego środka uwierzytelnienia – jednakże na zasadzie dobrowolności (ze strony użytkownika) i wyłącznie na jego wniosek. Zgodnie z zasadą transgraniczności należy uznawać wszystkie europejskie portfele tożsamości cyfrowej. Do 21 listopada 2024 r. Komisja w drodze aktów wykonawczych ustanowi wykaz norm referencyjnych oraz odpowiednie specyfikacje i procedury. Banki i instytucje finansowe powinny jak najszybciej rozpocząć prace nad ich przystosowaniem do swoich systemów.

3.5. Atrybut w EU Wallet jako element dokumentu 3.0

W ramach obiegu dokumentów, procedur, ale także dla możliwości świadczenia usług – w tym usług cyfrowych – konieczne są bardzo często dodatkowe informacje, czy wręcz dowody na uprawnienia użytkownika dla dokonywania konkretnej czynności, czy też korzystanie z usługi – w tym usługi cyfrowej. Przykładowo do poruszania się pojazdami konieczne jest odpowiednie prawo jazdy, do pływania jachtami patent żeglarski, do świadczenia pomocy prawnej profesjonalnej ukończona aplikacja adwokacka, radcowska, notarialna itd. Dla korzystania z usług finansowych odpowiednie pełnomocnictwo (w przypadku osób prawnych). Dotychczas dokument stwierdzający odpowiednie uprawnienia najczęściej był dokumentem 1.0 lub 2.0. Atrybut stanowi element dla dokumentu 3.0. Parlament Europejski i Rada ustanawiając atrybuty uwzględniła (o czym wyraźnie mowa w motywie 62 preambuły eIDAS2) potrzeby sektora finansów, wskazując iż bezpieczna identyfikacja elektroniczna oraz dostarczanie poświadczeń atrybutów powinny zapewniać dodatkową elastyczność oraz rozwiązania właśnie dla tego sektora, umożliwiające identyfikację klientów i wymianę specjalnych atrybutów niezbędnych do spełnienia, na przykład unijnej staranności wobec klienta wynikających z przyszłego rozporządzenia ustanawiającego Urząd ds. Przeciwdziałania Praniu Pieniędzy, wymogów dotyczących odpowiedniego zachowania wynikających z przepisów dotyczących ochrony inwestorów lub do spełnienia wymogów silnego uwierzytelnienia klienta w odniesieniu do identyfikacji elektronicznej na potrzeby logowania się na konto i inicjowania transakcji w dziedzinie usług płatniczych.



Rys. 5. Wygląd podstawowego procesu, w jaki sposób weryfikowalne jest poświadczenia z rejestru (np. blockchain), które umożliwiają zaufane, suwerenne ramy weryfikacji .

Źródło: W. Abramson, A. J. Hall, P. Papadopoulos, N. Pitropakis, W. J. Buchanan, A Distributed Trust Framework forPrivacy-Preserving Machine Learning, arXiv:2006.02456v1.

3.5.1. Definicja

Pojęcie atrybutu oraz ich poświadczenia jest nowym, nieznanym w dotychczasowym prawie europejskim pojęciem. Definicja atrybutu jest bardzo ogólna oraz pojemna. Zgodnie z art. 3 ust. 43 „atrybut" oznacza cechę charakterystyczną, właściwość, prawo lub zezwolenie osoby fizycznej, prawnej lub przedmiotu. Zakres podmiotowy jest wyjątkowo pojemny. Obejmuje zarówno osoby fizyczne, jak i prawne (przykładem atrybutu osoby prawnej może być poświadczenie wpisu do odpowiedniego rejestru, pełnomocnictwa, prokury itd.). Zaskakujące jest rozszerzenie zakresu także na przedmioty. Jednakże, gdy uwzględnimy m.in. NIS2 i konieczność zapewnienia i udowodnienia bezpieczeństwa i ciągłości bezpieczeństwa produktu czy usługi, atrybut przedmiotu staje się ciekawym rozwiązaniem. „Zwykłe" atrybuty może zgodnie z eIDAS 2 wydawać każdy.

Dla rynku usług cyfrowych, w szczególności świadczonych przez banki i instytucje finansowe, o wiele istotniejsze jest „elektroniczne poświadczenie atrybutów", którym zgodnie z art. 3 ust. 44 jest poświadczenie w postaci elektronicznej, które umożliwia uwierzytelnienie atrybutów oraz „kwalifikowane poświadczenie atrybutów", którym jest poświadczenie wydawane przez kwalifikowanego dostawcę i spełnia wymogi załącznika V eIDAS.

Musi ono zawierać:

1. wskazanie w postaci nadającej się do automatycznego przetwarzania, że dane poświadczenie zostało wydane jako kwalifikowane elektroniczne poświadczenie atrybutów,

2. zestaw danych identyfikujących kwalifikowanego dostawcę usługi zaufania wydającego kwalifikowany atrybut,

3. zestaw danych jednoznacznie reprezentujących podmiot, do którego poświadczenia atrybutu się odnoszą (np. konkretna osoba fizyczna, prawna, gdy jest to pseudonim – musi to być wyraźnie określone),

4. zakres atrybutu (np. uprawnienie do kierowania samochodem osobowym a nie ciężarowym, uprawnienie do czynności płatniczych np. do kwoty x, itd.),

5. dane dotyczące początku i końca poświadczenia,

6. kwalifikowany podpis elektroniczny lub kwalifikowana pieczęć elektroniczna dostawcy usług zaufania,

7. miejsce, w którym nieodpłatnie jest dostępny certyfikat towarzyszący kwalifikowanemu podpisowi elektronicznemu lub pieczęci elektronicznej, aby można je było zweryfikować,

8. informacje na temat ważności kwalifikowanego poświadczenia lub miejsce usług, w którym można dowiedzieć się o statusie ważności kwalifikowanego poświadczenia.

W praktyce jest to odpowiednik wytycznych wydanych w 2014 r. w odniesieniu do kwalifikowanego podpisu elektronicznego. A kwalifikowane poświadczenie atrybutu jest zbliżone (ale nie tożsame) do poświadczenia dokumentu przez osobę uprawnioną do tego odpowiednimi przepisami (jak poświadczenie dokumentu przez pełnomocnika procesowego), ale też jako dokument wydany przez podmiot prywatny (np. bank).

Kwalifikowane elektroniczne poświadczenie atrybutu może zostać unieważnione po wydaniu, traci ono ważność z chwilą unieważnienia i nie może być przywrócony jego poprzedni status (art. 45 d).

Takie poświadczenie może służyć np. osobie X, która jest pracownikiem banku Y (X nie jest pełnomocnikiem, ani też nie jest przedstawicielem, bo takiego statusu nie mają pracownicy w placówkach), albo też osoba X prowadzi sprzedaż w imieniu banku Y (pośrednicy agencji itd.).

Innym przykładem poświadczenia jest numer IBAN – dostarczany przez bank dla klientów, głównie jako atrybut poprawiający wygodę (nie trzeba ciągu znaków przepisywać. W zaawansowanej formie może on jednak służyć do uwiarygodnienia właściciela poprzez IBAN, co bywa używane podczas oszustw polegających na podmianie numeru konta.

Rozporządzenie eIDAS obok „zwykłego atrybutu", który może wydawać każdy, kwalifikowanego poświadczenia, wydawanego przez kwalifikowany podmiot świadczący usługi zaufane, wprowadza trzecią grupę: „elektroniczne poświadczenie atrybutów wydane przez podmiot sektora publicznego odpowiedzialnego za źródło autentyczne lub przez podmiot sektora publicznego, który jest wyznaczony przez państwo do wydawania takich poświadczonych atrybutów w imieniu podmiotów sektora publicznego odpowiedzialnego za źródła autentyczne zgodnie z art. 45f eIDAS i załącznikiem VII".

Przez źródło autentyczne rozumie się repozytorium lub system za prowadzenie którego odpowiedzialny jest podmiot sektora publicznego lub podmiot prywatny, które zawiera i udostępnia atrybuty dotyczące

osoby fizycznej lub prawnej lub przedmiotu i które uważa się za podstawowe źródło tych informacji lub uznaje za autentyczne zgodnie z prawem UE lub prawem krajowym, w tym praktykami administracyjnymi.

Przykładowo takim atrybutem jest poświadczony, elektroniczny odpis KRS wydawany przez MS, a źródłem autentycznym system informatyczny KRS.

3.5.2. Skutki prawne elektronicznego poświadczenia atrybutów

Podobnie jak w 2014 roku wprowadzono skutki prawne dla podpisu elektronicznego i kwalifikowanego podpisu elektronicznego jednolite w całej UE, tak samo dekadę później postąpiono odnośnie atrybutu.

Wyraźnie i literalnie w eIDAS2 wskazano (art. 45b), iż elektronicznemu poświadczeniu atrybutów nie można odmówić skutku prawnego ani dopuszczalności jako dowodu w postępowaniu sądowym wyłącznie z tego powodu, że ma postać elektroniczną lub że nie spełnia wymogów dotyczących kwalifikowanych poświadczeń atrybutów.

W ujęciu interesów i potrzeb sektora finansów istotniejsze są skutki prawne kwalifikowanego elektronicznego poświadczenia atrybutów oraz poświadczenia atrybutów wydane przez podmiot sektora publicznego odpowiedzialny za źródło autentyczne lub w jego imieniu, gdyż zgodnie z art. 45b ust.2 ma taki sam skutek, jak poświadczenie wydane zgodnie z prawem w postaci papierowej (tradycyjnej, a więc jako dokument 1.0). Równoważność tychże atrybutów i dokumentu papierowego jest istotnym elementem dla budowania dokumentu 3.0.

Dla sektora finansowego i dokumentu 3.0 wykorzystywanego w tym sektorze kluczowe znaczenie mają skutki prawne elektronicznego poświadczenia atrybutów wydawane przez podmiot sektora publicznego. Państwa członkowskie na podstawie art. 45e muszą w terminie do 21 listopada 2026 r. wprowadzić środki umożliwiające kwalifikowanym dostawcom usług zaufania, którzy dostarczają kwalifikowane elektroniczne poświadczenia atrybutów, ich weryfikację na żądanie użytkownika (zgodnie z prawem UE lub krajowym) w zestawieniu z odpowiednim źródłem autentycznym w sektorze publicznym na poziomie krajowym, co najmniej w odniesieniu do atrybutów (minimalny zakres, jaki każde państwo ma udostępniać w EU Wallet):

1. adres;
2. wiek;
3. płeć;
4. stan cywilny;
5. skład rodziny;
6. narodowość lub obywatelstwo;
7. wykształcenie, tytuły i licencje;
8. kwalifikacje zawodowe, tytuły i licencje;
9. pełnomocnictwa i upoważnienia do reprezentowania osób fizycznych lub prawnych;
10. publicznoprawne zezwolenia i licencje;
11. i co ciekawe, a także zaskakujące w odniesieniu do osób prawnych, dane finansowe i dane dotyczące przedsiębiorstwa.

Banki i instytucje będą mogły opierać swoje działania, w tym zawieranie umów i same usługi, w oparciu o atrybuty zawierające powyższe dane ze źródeł autentycznych w sposób identyczny, jak w dniu dzisiejszym opierają się o dokument 1.0 lub 2.0.

Dla praktyki bankowej istotna jest **transgraniczność** poświadczenia atrybutów, w szczególności wydawanych przez podmiot sektora publicznego odpowiedzialnego za źródło autentyczne, który uznaje się na podstawie art. 45b we wszystkich państwach członkowskich.

3.5.3. Jak to będzie działało?

Podstawowym narzędziem dla obywateli UE i rezydentów jest EU Wallet. Sposób funkcjonowania europejskich portfeli tożsamości cyfrowej został szerzej omówiony w raporcie WIB 9/2024: Tożsamość cyfrowa. Regulacje europejskie (str. 45 i nast.). To w nim zawarte są dane uwierzytelniające tożsamość użytkownika, ale także atrybuty, w tym kwalifikowane oraz poświadczone przez podmioty publiczne. Portfele mają być podstawowym narzędziem dla korzystania z usług online, z zapewnieniem wysokiego poziomu bezpieczeństwa, jak i pełnej kontroli użytkownika nad danymi i nad tym, komu udostępnia atrybuty.

Dostawcy elektronicznych poświadczeń atrybutów muszą zapewnić użytkownikom EU Wallet możliwość żądania, a co za tym idzie „ściągnięcia" do portfela atrybutu, przechowywania na nim, niezależnie czy w wersji mobilnej, cloud czy w urządzeniu, ale co najważniejsze zarządzania nim, niezależnie od państwa członkowskiego, w którym zapewniany jest europejski portfel tożsamości. To użytkownik decyduje, które atrybuty zamierza przechowywać w portfelu, które udostępnia stronie ufającej i na jakich zasadach. Ma wgląd do tego komu i na jaki czas udostępnił atrybut lub informacje dotyczącą posiadania danego atrybutu. Może nimi w pełni zarządzać – analogicznie jak danymi osobowymi. Strona ufająca dla usługi online musi wskazać, które z atrybutów będą konieczne, ale to użytkownik ostatecznie decyduje, czy i jakie udostępni. Dostawcy kwalifikowanych

i niekwalifikowanych usług elektronicznego poświadczenia atrybutów nie mogą łączyć danych osobowych ze świadczeniem tych usług z danymi osobowymi pochodzącymi z jakichkolwiek innych usług oferowanych przez nich lub przez ich partnerów handlowych. Dane osobowe związane ze świadczeniem usług elektronicznego poświadczenia atrybutów muszą logicznie być oddzielone od wszelkich innych danych przechowywanych przez dostawcę elektronicznego poświadczenia.

Inaczej ujmując – dane osobowe i atrybuty muszą być od siebie oddzielone. Nie mogą być wykorzystywane ani przez dostawcę europejskiego portfela tożsamości, ani przez inne podmioty. To użytkownik decyduje, jakie atrybuty przechowuje w portfelu, jakie udostępnia i komu, ma na tym kontrolę i nadzór. Może je udostępnić online dla usług online świadczonych przez podmioty ufające, zgodnie z danymi określonymi przez te podmioty w procesie rejestracji jako podmiot ufający. Może także zgłaszać do właściwych krajowych organów kontroli naruszenia związane z udostępnianymi danymi.

Drugą możliwością, jaką daje portfel, jest przekazywanie wskazanych przez użytkownika danych bezpośrednio z portfela do drugiego portfela w sposób zapewniający bezpieczeństwo na wysokim poziomie, ale także z odnotowaniem tego faktu w portfelu w sposób umożliwiający nadzór nad tym, komu dane lub atrybuty są przekazywane.

Przykłady

Bank zawiera umowę o rachunek bankowy. W chwili obecnej, w przypadku osoby prawnej wymagane jest pozyskanie wielu danych, w tym danych z KRS lub CEiDG, ewentualne pełnomocnictwa do zawarcia umowy, dowód tożsamości lub inny dokument osoby reprezentującej zawierającego umowę z bankiem itd. Procedurę tę można przeprowadzić za pomocą dokumentów 1.0 lub 2.0, często poprzez pozyskanie danych z KRS lub CEiDG. Użytkownik uzyskuje pakiet dokumentów (w tym umowę w postaci dokumentu 1.0 lub 2.0).

Wykorzystując EU Wallet bank jako podmiot ufający określa jakie dane (osobowe) oraz atrybuty będzie wymagał. Klient wchodzi na panel zarządzania EU Wallet, zaznacza dane oraz atrybuty, które udostępnia lub wyraża zgodę na udostępnienie danych lub atrybutów oznaczonych w systemie na wniosek podmiot ufającego. Dane zostają udostępnione, pozostając jednocześnie pod kontrolą użytkownika.

W jednostce banku umowa jest zawierana w sposób tradycyjny. Klient oznacza dane, które udostępnia bankowi, w tym atrybuty i przekazuje bezpośrednio do EU Wallet banku (bez konieczności drukowania i potwierdzania czegokolwiek). Dane pozostają przy tym równocześnie pod kontrolą użytkownika. Opcja – przekazania danych EU Wallet-EU Wallet

Klient zamierza dokonać płatności lub innej usługi finansowej, dla której wymagane jest silne uwierzytelnienie. Dokonuje tego uwierzytelnienia w EU Wallet zarówno, gdy usługa dokonywana jest online, w siedzibie banku czy też przy terminalu.

Oczywiście banki już w dniu dzisiejszym stosują odpowiednie metody silnego uwierzytelnienia, najczęściej w swoich dedykowanych aplikacjach lub z użyciem alternatywnej metody sms. Za dwa lata będą mogły korzystać z uwierzytelnienie w EU Wallet, które stanie się powszechnym uwierzytelnieniem dla wielu usług cyfrowych, w sposób łatwy i intuicyjny dla użytkownika. Stworzy także możliwości świadczenia wielu innych niż dotychczas usług, w tym finansowych.

3.6. Czy aplikacja mObywatel to EU Wallet?

Polska aplikacja mObywatel funkcjonuje w oparciu o przepisy ustawy z 26 maja 2023 r. o aplikacji mObywatel (Dz.U. Poz 1234 oraz z 2024 r poz. 854). Nie wchodząc w szczegóły ustawy i funkcjonującego rozwiązania (mObywatel jako oprogramowanie przeznaczone dla urządzeń mobilnych, w którym są udostępniane usługi lub świadczone przez podmioty publiczne) mimo wypowiedzi niektórych polityków, nie jest ono w chwili obecnej EU Wallet w znaczeniu eIDAS2, co zresztą wskazano też w przytoczonym projekcie Strategii opracowanej przez Ministerstwo Cyfryzacji w podrozdziale 1.2. Nie może być chociażby z tego powodu, iż w chwili obecnej nie ma jeszcze przepisów wykonawczych co do kodów dla europejskich portfeli tożsamości, które muszą spełniać wysokie kryteria w zakresie cyberbezpieczeństwa i podlegać w tym zakresie certyfikacji (a aktualny nie spełnia tego wymogu) i który musi być zgłoszony jako EU Wallet do Komisji Europejskiej, ponadto należy spełnić wiele wymogów dodatkowych wynikających z eIDAS2 i przepisów wykonawczych. Już więc tylko z powodów formalnych mObywatel nie może być w chwili obecnej europejskim portfelem tożsamości.

Nie spełnia także szeregu wymogów merytorycznych. Dane osobowe nie są oddzielone od innych danych

– a tego w EU Wallet wymaga eIDAS2. Zakres i wybór dokumentów i innych danych, które umieszczane są w mObywatelu, jest w wyłącznym władztwie ustawodawcy, a umieszczone dokumenty nie są kwalifikowanymi poświadczeniami atrybutów ani poświadczonymi atrybutami wydawanymi przez podmiot publiczny zgodnie z eIDAS2. Nie ma możliwości udostępnienia danych osobowych do dokumentu 3.0, co najwyżej jako 2.0. Brak możliwości zarządzania danymi, zgłaszania naruszeń do organów kontroli, nie ma możliwości przenoszenia atrybutów między „mObywatelami" itd. A także nie ma możliwości przenoszenia danych i dokumentów do innych portfeli. Jest to aplikacja w pełni i wyłącznie zależna od systemów państwa.

Aplikacja mObywatel jest natomiast w chwili obecnej środkiem identyfikacji elektronicznej notyfikowanym Komisji Europejskiej na podstawie art. 9 eIDAS.

Dowód z dokumentu 3.0

4.1. Wprowadzenie

Jedną z podstawowych funkcji dokumentu jest funkcja dowodowa. W przypadku sporu to na stronie wywodzącej skutki prawne leży obowiązek stwierdzenia faktu. W odniesieniu do dokumentu 1.0 czy też 2.0 mamy ugruntowane zasady, domniemania prawne oraz reguły procesowe, w tym wieloletnią praktykę w przeprowadzaniu dowodu z dokumentu.

Dokument 3.0 nie jest jednolitym dokumentem w znaczeniu dokumentu 1.0 czy też 2.0. Jest dokumentem aktywnym podlegającym zmianom w osi czasu. Przeprowadzenie dowodu z takiego dokumentu wymaga nowych narzędzi, ale także nowych praktyk procesowych, z równoczesnym oparciem się o dotychczasowe przepisy procesowe.

Europejskie ujęcie dokumentu 3.0 wymaga jednolitych wspólnotowych narzędzi, w tym jednolitych domniemań prawnych uznawanych w każdej z europejskich jurysdykcji, ale według lokalnej procedury postępowania.

Kwestię, czy dokument 3.0 jest dokumentem w znaczeniu prawnym (a nie np. usługą dostępu do danych, informacji) przesądza na gruncie prawa europejskiego definicja dokumentu elektronicznego z art. 3 pkt 35, zgodnie z którym „dokument elektroniczny" oznacza każdą treść przechowywaną w postaci elektronicznej, w szczególności tekst, nagranie dźwiękowe, wizualne lub audiowizualne. Dotychczas w literaturze odnoszono się głównie do drugiej części zdania. Dokument 3.0 opiera się na multimedialności, ale także interfejsach, czasami na tokenizacji, ale każdorazowo jest to treść przechowywana w postaci elektronicznej, możliwa do absorpcji przez człowieka, chociaż czasami w sposób pośredni wymagający urządzeń technicznych, co jest już znaną praktyką odnośnie dokumentu 2.0. Wskazana europejska definicja koresponduje z polską lokalną zawartą w k.c w art. 77(3) – „dokumentem" jest nośnik informacji umożliwiający zapoznanie się z jej treścią.

Różnicą dla dokumentu 3.0 jest niemożność wydruku (co jest częste w odniesieniu do dokumentu 2.0), poświadczenia w tradycyjny sposób przez pełnomocnika procesowego, a także sposób przedłożenia w sądzie (często jako dostęp do dokumentu w systemie informatycznym podlegający zapoznaniu się przez sędziego na gruncie 243(1) – odnośnie dokumentów zawierających tekst oraz umożliwienie ustalenia ich wystawców lub na gruncie 308 k.p.c.

Drugą istotną różnicą z punktu widzenia praktyki jest to, iż poszczególne części składowe dokumentu 3.0 mogą być „wydawane" przez różne podmioty, pozyskiwane z różnych miejsc, wpisane w różne rejestry podlegające różnym domniemaniom prawnym.

Przykładem może być dokument 3.0, w którym dane osobowe udostępnianie są poprzez EU Wallet, a token inteligentej umowy zawierający część treści merytorycznej umowy wpisany jest do kwalifikowanego archiwum elektronicznego, pozostała jednak część w odrębnych rejestrach niebędących archiwum elektronicznym.

Na gruncie eIDAS dane osobowe będą podlegały pod domniemania prawne wynikające z przepisów odnoszących się do cyfrowej tożsamości, token i treść w nim wpisana pod domniemania prawne związane z kwalifikowanym archiwum elektronicznym, reszta pod klasyczne reguły dowodowe.

W konsekwencji, do poszczególnego elementu dokumentu 3.0 zastosowanie mogę mieć różne przepisy prawa, różne domniemania prawne, różna moc dowodowa poszczególnych fragmentów dokumentów. Atutem jest natomiast „osadzenie" dokumentu na linii czasu z możliwością analityki zmian poszczególnych składowych w czasie (np. zmiana danych osobowych, utrata uprawnień itd).

Dla praktyki procesowej istotne są domniemania prawne powiązane z dokumentem 3.0.

4.2. Domniemania prawne dla dokumentu 3.0

4.2.1. Domniemania prawne wynikające z eIDAS

Rozporządzenie eIDAS już od 10 lat wprowadza szereg domniemań prawnych, mających znaczenie i skutki procesowe. Do dotychczasowych powiązanych z usługami zaufania, takimi jak „podpis elektroniczny", „kwalifikowany podpis elektroniczny", „pieczęć elektroniczna", „kwalifikowana pieczęć elektroniczna", „doręczenie elektroniczne" jak i „kwalifikowane doręczenie elektroniczne" dochodzą nowe, dedykowane zarówno dla dokumentu 2.0, jak i 3.0: „archiwizacja elektroniczna", „kwalifikowana archiwizacja elektroniczna", „rejestr elektroniczny" oraz „kwalifikowany rejestr elektroniczny". Nowe narzędzia (w powiązaniu z domniemaniami prawnymi) stanowią podstawę dla dokumentu 3.0 i ułatwienia dowodowego dla faktów w nim zawartych, i to zarówno w odniesieniu do użytkownika EU Wallet, jak i strony ufającej.

Znaczenie oraz możliwości wykorzystania nowych narzędzi eIDAS2 jest o wiele szersze niż tylko dokument 3.0 oparty o dane z EU Wallet. Nowe narzędzia mogą mieć zarówno zastosowania do dokumentów

wytwarzanych w oparciu o europejski portfel tożsamości cyfrowej i poświadczone atrybuty czy też kwalifikowane poświadczone atrybuty, ale także do innych danych i innych dokumentów 3.0 wykorzystujących inne, czasami lokalne systemy informatyczne. Nie ma przeszkód, aby banki lub instytucje finansowe korzystały z tych narzędzi w odniesieniu do swoich danych czy też systemów już teraz, bez integracji z EU Wallet.

4.2.2. Archiwizacja elektroniczna i kwalifikowana usługa archiwizacji elektronicznej

4.2.2.1. Definicja

Przez „archiwizację elektroniczną" rozumie się usługę zapewniającą odbiór, przechowanie, pobieranie i usuwanie danych elektronicznych i dokumentów elektronicznych w celu zapewnienia ich trwałości i czytelności, a także zachowania integralności, poufności i dowodu pochodzenia przez cały okres ich przechowywania (art. 3 ust. 48 eIDAS). Natomiast przez kwalifikowaną usługę archiwizacji elektronicznej rozumie się usługę archiwizacji elektronicznej, która jest świadczona przez kwalifikowanego dostawcę usług zaufania i spełnia wymogi określone w rozporządzeniu eIDAS (art. 3 ust. 49 eIDAS).

Rozporządzenie eIDAS2 wraz z innymi w niedawnym czasie wydanymi wspólnotowymi aktami prawnymi, ma na celu utworzenie jednolitego, transgranicznego europejskiego rynku cyfrowego. W chwili obecnej wiele państw członkowskich wprowadziło krajowe wymogi dotyczące usług zapewniających bezpieczną i wiarygodną archiwizację elektroniczną. Reguły te jednak są lokalne i wymagają od przedsiębiorców zarówno wiedzy, jak i ponoszenia kosztów związanych z odrębnymi zasadami elektronicznej archiwizacji w poszczególnych systemach prawnych. W preambule do rozporządzenia eIDAS2 wskazano, że aby zapewnić pewność prawa, zaufanie i harmonizację we wszystkich państwach członkowskich, konieczne są wspólne ramy prawne dla archiwizacji elektronicznej, ale przede wszystkim kwalifikowanej archiwizacji elektronicznej, wzorowane na sprawdzonych ramach dla innych usług zaufania lub kwalifikowanych usług zaufania od lat znanych w eIDAS.

Ramy te mają oferować zarówno dostawcom usług zaufania, jak i użytkownikom skuteczny zestaw narzędzi obejmujący wymogi funkcjonalne, ale także jasne skutki prawne w przypadku korzystania z kwalifikowanej usługi archiwizacji elektronicznej i być jednolite w całej UE. Zgodnie z art. 45 j pkt. 2 do dnia 21 maja 2025 r. komisja, w drodze aktów wykonawczych, sporządzi wykaz norm referencyjnych oraz w razie potrzeby ustanowi specyfikacje i procedury w odniesieniu do kwalifikowanych usług archiwizacji elektronicznej. Poprzez spełnienie przez kwalifikowaną usługę archiwizacji elektronicznej tychże norm, specyfikacji i procedur domniemywa się zgodność z wymogami dla kwalifikowanych usług archiwizacji elektronicznej. W konsekwencji w przypadku sporu to strona przeciwna będzie musiała wykazać, iż archiwizacja nie spełnia wymogów eIDAS, a co za tym idzie – nie wywołuje skutków prawnych dla kwalifikowanej usługi archiwizacji. Daje to sporą przewagę procesową dla podmiotu, który korzysta z kwalifikowanej usługi.

4.2.2.2. Skutki prawne usług archiwizacji elektronicznej

Na podstawie art. 45i pkt. 1 eIDAS danym elektronicznym oraz elektronicznym dokumentom przechowywanym przy użyciu usługi archiwizacji elektronicznej nie można odmówić skutku prawnego ani dopuszczalności jako dowodu w postępowaniu sądowym wyłącznie z tego powodu, iż dane te mają postać elektroniczną lub że nie są przechowywane przy użyciu kwalifikowanej usługi elektronicznej. Przepis ten, jak i kolejny – dotyczący kwalifikowanej usługi – jest wzorowany na mającym ponad dekadę przepisie dotyczącym podpisu oraz kwalifikowanego podpisu elektronicznego i niedopuszczalności ich uznawalności.

Usługa archiwizacji elektronicznej może być dokonywana bez ograniczeń, przez każdy podmiot, zarówno działający na terytorium UE, jak i poza, jednakże z nakierowaną usługą na terytorium UE. Usługa ta może być świadczona także przez osoby fizyczne. Archiwizacji podlegają dane, zarówno będące elementem 3.0, jak i inne dane, w tym osobowe jak i nieosobowe, odnośnie których zastosowanie mają odpowiednie przepisy jak RODO czy dotyczące danych nieosobowych, w tym wszelkie zakazy i nakazy, a także kary. Rozporządzenie eIDAS wprowadza „jedynie" jednolite skutki prawne, nie ogranicza w żadnej mierze innych przepisów unijnych dotyczących danych.

Przedmiotowo usługa archiwizacji elektronicznej obejmuje swoim zakresem nie tylko dane będące podstawą dla dokumentu 3.0, ale także dokumenty elektroniczne w znaczeniu dokumentu 2.0.

Na potrzeby bezpieczeństwa obrotu oraz dokumentów elektronicznych, w tym jako dowód w postępowaniu dowodowym, istotna jest kwalifikowana postać usługi archiwizacji elektronicznej, którą powiązano z dodatkowym domniemaniem prawnym. Zgodnie z art. 45i pkt.2 eIDAS dane elektroniczne oraz elektroniczne dokumenty przechowywane przy użyciu

kwalifikowanej usługi archiwizacji elektronicznej korzystają z domniemania ich integralności i pochodzenia przez cały okres przechowywania przez kwalifikowanego dostawcę usług zaufania.

Reguła ta jest kalką zaufanej usługi kwalifikowanego podpisu elektronicznego lub pieczęci elektronicznej, których skutkiem prawnym od 10 lat jest zapewnienie autentyczności i integralności danych opatrzonych kwalifikowanym podpisem lub pieczęcią. Od 20 maja 2024 r., a właściwie to z chwilą, gdy pierwsze kwalifikowane usługi archiwizacji elektronicznej pojawią się na rynku, integralność oraz autentyczność (a co za tym idzie – domniemanie „oryginału"), zapewnia nowa usługa.

Rozporządzenie eIDAS nakłada szereg wymogów:

- musi być świadczona przez kwalifikowanych dostawców zaufania,
- musi wykorzystywać procedury i technologie umożliwiające zapewnienie trwałości i czytelność danych elektronicznych i dokumentów elektronicznych poza technologiczny okres ważności i co najmniej na cały okres prawnego lub umownego okresu przechowywania, przy jednoczesnym zachowaniu integralności i autentyczności pochodzenia,
- musi zapewnić przechowanie danych elektronicznych i dokumentów elektronicznych w taki sposób, aby były zabezpieczone przed utratą i modyfikacją, z wyjątkiem zmian dotyczących zmian nośnika lub formatu elektronicznego,
- oraz musi umożliwiać upoważnionym stronom ufającym otrzymanie w automatyczny sposób raportu potwierdzającego, że dane elektroniczne i dokumenty elektroniczne pobrane z kwalifikowanego archiwum elektronicznego korzystają z domniemania integralności danych od początku przechowywania do momentu pobrania.

Zgodnie z preambułą przepisy wykonawcze mają pozwalać na przenoszenie danych i dokumentów na inne nośniki i inne (nowe) formaty w celu przedłużenia ich trwałości oraz czytelności poza technologiczny okres ważności. Ponadto mają być stosowane technologie, gdy dokument lub dane przekazywane do kwalifikowanego archiwum zawierają co najmniej jeden kwalifikowany podpis lub pieczęć, umożliwiające w oparciu o technologie usług zaufania przedłużenie ich wiarygodności na okres przechowywania. Czyli inaczej ujmując mają automatycznie dokonywać konserwacji kwalifikowanego podpisu elektronicznego lub kwalifikowanej pieczęci elektronicznej.

Funkcja ta jest wyjątkowo istotna, ze względu na to, iż nie wszystkie podmioty dbają, konserwują, a co za tym idzie – przedłużają domniemania związane z kwalifikowanym podpisem elektronicznym lub kwalifikowaną pieczęcią elektroniczną.

Kwalifikowaną usługę archiwizacji elektronicznej może świadczyć wyłącznie kwalifikowany podmiot zaufania (analogicznie jak usługi kwalifikowanego podpisu elektronicznego, pieczęci czy też kwalifikowanego doręczenia) w znaczeniu art. 3 eIDAS, podlegający kontroli podmiotom nadzorującym i okresowym audytom. Archiwizacja elektroniczna rozszerzyła katalog usług zaufanych z art. 3 ust. 16.

Dla banków i innych instytucji finansowych szczególnie ciekawa jest ostatnia funkcja dająca gwarancje i domniemanie prawnej autentyczności i integralności przechowywanych danych przez cały okres archiwizacji, w tym danych dokumentu 3.0. Swoboda przepływu usług, w tym usług cyfrowych, pozwala na korzystanie z usługi kwalifikowanej archiwizacji od kwalifikowanych podmiotów zaufania bez jakichkolwiek ograniczeń na terytorium całej UE. Państwa członkowskie nie mogą dyskryminować dostawców usługi z innego kraju UE.

Korzystanie z EU Wallet dla silnego uwierzytelnienia, w połączeniu z kwalifikowaną usługą archiwizacji przerzuca w pełni odpowiedzialność banku na kwalifikowany podmiot zaufany zarówno w zakresie utraty, modyfikacji danych, jak i ich autentyczności i integralności oraz konserwacji kwalifikowanego podpisu elektronicznego oraz kwalifikowanej pieczęci elektronicznej. W takim przypadku zarówno podmiot finansowy, jak i podmiot zaufany, jako dostawca usługi, podlegają pod DORA.

Omawiane przepisy dotyczą zarówno dokumentów wytworzonych pierwotnie w postaci elektronicznej, wtórnie po digitalizacji, będące dokumentem elektronicznym 2.0, jak także danych stanowiących podstawę dokumentu 3.0.

Ten ostatni składa się z wielu danych, wpisanych w różne rejestry, w różne archiwa. Należy więc zwrócić uwagę, iż opisywanymi domniemaniami będą objęte tylko te „części" dokumentu 3.0, które są wpisane w kwalifikowane archiwum. W pozostałym zakresie albo zastosowania będą miały domniemania prawne z innych podstaw prawnych lub ogólne reguły dowodowe.

4.2.3. Rejestr elektroniczny i kwalifikowany rejestr elektroniczny

4.2.3.1. Definicja

Rozporządzenie eIDAS definiuje pojęcie „rejestru elektronicznego" i „kwalifikowanego rejestru elektronicznego" w art. 3 pkt. 52 i pkt. 53. „Rejestr elektroniczny" oznacza sekwencję elektronicznych wpisów danych zapewniającą integralność tych wpisów i prawidłowość ich chronologicznego uporządkowania. Natomiast „kwalifikowany rejestr elektroniczny" to rejestr świadczony przez kwalifikowanego dostawcę usług zaufania i spełnia wymogi art. 45l eIDAS.

Przepisy wykonawcze, analogicznie jak w odniesieniu do usługi archiwum elektronicznego, w tym normy referencyjne, specyfikacje i procedury zostaną opublikowane najpóźniej do 21 maja 2025 r.

Inaczej ujmując rejestry elektroniczne to sekwencje elektronicznych wpisów danych zapewniające integralność tych wpisów danych oraz dokładność ich chronologicznego uporządkowania. W preambule eIDAS wskazano, że w połączeniu z innymi technologiami powinny się one przyczyniać do opracowywania rozwiązań na rzecz bardziej efektywnych i transformacyjnych usług publicznych, takich jak głosowanie elektroniczne, transgraniczna współpraca organów celnych, transgraniczna współpraca instytucji akademickich oraz rejestrowanie własności nieruchomości w zdecentralizowanych rejestrach gruntów. Z uwagi na ich specyfikę, na przykład sekwencyjne uporządkowanie chronologiczne wpisu danych, rejestry elektroniczne powinny odróżniać się od innych usług. Proces tworzenia i aktualizacji rejestru elektronicznego zależy od rodzaju wykorzystanego rejestru, to znaczy czy jest on scentralizowany, czy rozproszony. Rozporządzenie zapewnia neutralność technologiczną i nie faworyzuje ani nie dyskryminuje jakiejkolwiek technologii rejestrów elektronicznych.

Stanowi podstawę prawną dla zapisu w rejestrze rozproszonym DLT oraz dla dokumentu 3.0. Usługa ta pozwala na osi czasu wykazywać zmiany zachodzące w dokumencie 3.0, wykazywać je i przedstawiać w sądzie jako dowód. W rejestrze mogą być zapisywane wszelkie dane, zarówno osobowe jak i nieosobowe.

4.3.2.2. Skutki prawne rejestru elektronicznego

Zgodnie z art. 45k rejestrowi elektronicznemu nie można odmówić skutku prawnego ani dopuszczalności jako dowodu w postępowaniu sądowym wyłącznie z tego powodu, że rejestr ten ma postać elektroniczną lub że nie spełnia wymogów dla kwalifikowanych rejestrów elektronicznych. Ze „zwykłym" rejestrem elektronicznym nie są powiązane żadne nowe dodatkowe domniemania prawne.

Te dotyczą kwalifikowanego rejestru elektronicznego, który korzysta z domniemania ich niepowtarzalnego i dokładnego sekwencyjnego uporządkowania chronologicznego i ich integralności. Usługę „zwykłego rejestru" może świadczyć każdy, „kwalifikowanego" wyłącznie kwalifikowany podmiot zaufany, którego rejestry muszą spełniać następujące wymogi:

- być tworzone i zarządzane przez co najmniej jednego kwalifikowanego dostawcę usług zaufanych,
- muszą ustalać pochodzenie wpisów danych w rejestrze,
- muszą zapewnić niepowtarzalne sekwencje uporządkowane chronologicznie wpisów w danym rejestrze,
- oraz rejestrować dane w taki sposób, że każda późniejsza zmiana danych jest natychmiast wykrywalna, co zapewnia ich integralność w czasie.

Wprowadza się ponadto dodatkowe domniemanie – w przypadku, gdy rejestr elektroniczny spełnia normy, specyfikacje i procedury określone w eIDAS i przepisach wykonawczych domniemywa się ich zgodność dla kwalifikowanych rejestrów elektronicznych.

Inaczej ujmując domniemanie obejmuje kolejność wpisu i jego niezmienność, a spełnienie norm przez kwalifikowany podmiot świadczący usługi zaufane, jest związane z domniemaniem prawidłowości rejestru. Rejestr elektroniczny jest kolejną, uzupełniającą eIDAS usługą wymaganą na rynku cyfrowym. Może ona funkcjonować niezależnie, jak i wspólnie z innymi usługami, w tym archiwum elektronicznym. Analogicznie jak usługa konserwacji kwalifikowanego podpisu elektronicznego funkcjonuje niezależnie od niego samego.

Dla banków i innych instytucji finansowych jest to optymalne narzędzie, powiązane z domniemaniem chronologii zdarzenia i wpisu, idealne narzędzie prawno–technologiczne do zapisu w rejestrze rozproszonym DLT w ramach dokumentu 3.0.

Podobnie jak przy archiwizacji w przypadku dokumentu 3.0 domniemaniem objęte są te części dokumentu, które wpisane są w kwalifikowany rejestr elektroniczny.

4.4. Domniemania prawne powiązane z atrybutami

Elektronicznemu poświadczeniu atrybutów nie można odmówić skutku prawnego ani dopuszczalności jako dowodu w postępowaniu sądowym wyłącznie z tego powodu, że ma postać elektroniczną lub że nie spełnia wymogów dla kwalifikowanych elektronicznych poświadczeń atrybutów. Te ostatnie oraz poświadczenia atrybutów wydane przez podmiot sektora publicznego odpowiedzialnego za źródło autentyczne lub w jego imieniu ma ten sam skutek prawny, jak poświadczenie wydane zgodnie z prawem w postaci papierowej. Wzajemnie uznaje się poświadczenie atrybutów wydane przez podmiot sektora publicznego odpowiedzialnego za źródło autentyczne wydane w jego imieniu w jednym z państw członkowskich za poświadczenie we wszystkich państwach członkowskich (art. 45b eIDAS).

Przepis ten jest odpowiednikiem przepisu dotyczącego równoważności kwalifikowanego podpisu elektronicznego z podpisem własnoręcznym. Kwalifikowane poświadczenie atrybutu lub poświadczenie atrybutu przez podmiot publiczny odpowiedzialny za źródło autentyczne jest równoważne z dokumentem papierowym tradycyjnym. Inaczej ujmując – prawo jazdy w postaci tradycyjnej, jak i poświadczone jako atrybut, czy też tradycyjny dyplom wykazujący wykształcenie, jak i jako atrybut, są sobie równoważne i nie można odmawiać ich skuteczności i ważności. Muszą być uznawane transgranicznie w całej UE. Tym też różnią się dokumenty w polskim mObywatelu od atrybutów, iż mają zastosowanie lokalnie wyłącznie w Polsce na podstawie prawa polskiego.

Poświadczone atrybuty mogą funkcjonować jako dokument 2.0 jak i 3.0. Ponadto, jeżeli są wpisane do kwalifikowanego archiwum elektronicznego lub kwalifikowanego rejestru elektronicznego, korzystają z domniemań prawnych związanych z tymi narzędziami.

Odnośnie atrybutów funkcjonujących jako dokument 2.0 zastosowanie mają także klasyczne reguły i domniemania prawne. Niezależnie od przepisów wspólnotowych i domniemań prawnych powiązanych z eIDAS poświadczenie atrybutów wydane przez podmiot sektora publicznego odpowiedzialnego za źródło autentyczne jest dokumentem urzędowym podlegającym pod art. 244 k.p.c, zgodnie z którym dokumenty urzędowe sporządzone w przepisanej formie przez powołane do tego organy władzy publicznej i inne organy państwowe w zakresie ich działania, stanowią dowód tego, co zostało w nich urzędowo poświadczone. Przepis ten stosuje się odpowiednio do dokumentów urzędowych sporządzanych przez organizacje zawodowe, samorządowe, spółdzielcze i inne organizacje pozarządowe w zakresie zleconym im przez ustawę spraw z dziedziny administracji publicznej.

Regulacja eIDAS nakłada na państwa członkowskie minimalny, aczkolwiek bardzo obszerny zakres atrybutów, jakie są zobligowane wydać obywatelom. Zrównanie dokumentu urzędowego z poświadczonym atrybutem przez podmiot publiczny odpowiedzialny za źródło autentyczne, w aspekcie przepisów administracyjnych, ale także dotyczących postępowania dowodowego z dokumentem urzędowym w zakresie procedury cywilnej pozwala, aby praktycznie wszystkie atrybuty papierowe wydawane przez urzędy były w postaci elektronicznej.

Drugim, w aspekcie dokumentu 3.0 sposobem pozyskiwania danych z atrybutów jest ich walidacja jako usługa zaufana w znaczeniu eIDAS i zapisywanie w dokumencie 3.0 tylko wyników walidacji, bez pobierania całości atrybutu, który pozostaje w EU Wallet. Dotyczy to atrybutów z wbudowaną regułą ujawniania, z zezwoleniem dla strony ufającej dostępu do poświadczenia.

Regulacja ta ma istotne znaczenie dla banków, które w sposób zautomatyzowany jako strony ufające mogą pozyskiwać atrybuty, także atrybuty osób prawnych, w tym pełnomocnictwa itd. łącząc je w dokument 3.0 z możliwością kwalifikowanej archiwizacji i kwalifikowanego rejestrowania sekwencji zmian.

ROZDZIAŁ V

Forma – podpis kwalifikowany w EU Wallet

Rozporządzenie eIDAS 2 wprowadza wiele zmian odnośnie dokumentów, ich archiwizacji, rejestrowania danych, atrybutów itd. Stanowi podwalinę dla dokumentu 3.0.

Należy żałować, iż nie wprowadzono, jak w niektórych systemach prawnych reguły, że wpis do kwalifikowanego rejestru elektronicznego, po uwierzytelnieniu w EU Wallet tożsamości użytkownika jest równoznaczny ze spełnieniem formy pisemnej.

W zakresie formy rozporządzenie eIDAS nie wprowadza na poziomie europejskim żadnych zmian pozostawiając aktualne status quo, niejako dokładając kolejne nowe elementy czy też narzędzia w powiązaniu z domniemaniami prawnymi.

Ustawodawca europejski podejmuje działania mające na celu upowszechnienie kwalifikowanych usług zaufanych wprowadzając do europejskiego portfela tożsamości nie tylko możliwość składania kwalifikowanego podpisu elektronicznego i kwalifikowaną pieczęć elektroniczną, ale także ich weryfikację. Europejski rynek cyfrowy ma opierać się o narzędzia na wysokim poziomie bezpieczeństwa. A takim narzędziem w zakresie potwierdzania tożsamości i autentykacji jest kwalifikowany podpis elektroniczny. Rozporządzenie nakłada obowiązek wprowadzenia mechanizmu do EU Wallet, aby oferować wszystkim osobom fizycznym możliwość składania kwalifikowanych podpisów elektronicznych domyślnie i – co istotne dla użytkownika – nieodpłatnie.

Nie oznacza to, iż będzie on nieodpłatny w ogóle, ile nieodpłatny dla użytkownika będącego osobą fizyczną. Ustawodawca nie przesądza o mechanizmie odpłatności – czy będzie kwalifikowany podpis elektroniczny refinansowany przez państwo, czy też będzie funkcjonował podobnie jak karta płatnicza, która jest nieodpłatna dla klienta, a koszty jej użycia przerzucone są na przedsiębiorcę. Nie ma przeszkód, aby koszt użycia kwalifikowanego podpisu elektronicznego został przerzucony na stronę ufającą.

Wprowadzenie do EU Wallet nieodpłatnego podpisu elektronicznego przyczyni się do jego upowszechnienia i traktowania jako podstawowego narzędzia składania oświadczeń woli w formie elektronicznej. Przyczyni się także do bezpieczeństwa transakcji.

Kwalifikowany podpis elektroniczny sprawdził się w aspekcie dokumentu 2.0. Jego istotą było obejmowanie całości treści dokumentu 2.0 algorytmem szyfrującym połączonym z domniemaniem autentyczności i integralności podpisywanego dokumentu. Zastępując na gruncie eIDAS podpis własnoręczny – kwalifikowanym podpisem elektronicznym, a na gruncie prawa materialnego równoważąc formę pisemną i elektroniczną (m.in. w Polsce).

Dokument 3.0 jako dokument aktywny składa się z wielu komponentów i nie wszystkie będą opatrywane kwalifikowanym podpisem elektronicznym. Tylko te, które będą nim opatrzone – będą w formie elektronicznej w znaczeniu k.c. – pozostałe komponenty w formie dokumentowej. Nie jest to jakaś nowa praktyka. Od lat w środowisku bankowym, ale nie tylko funkcjonują regulaminy, wzorce umowne, OWP i nie mają one wpływu na skuteczność składanych oświadczeń woli, gdy jest dla nich wymagana forma szczególna.

Automatyzacja oświadczeń woli banku a dokument 3.0

Rozwój koncepcji Dokumentu 3.0 to również pytanie o stymulujący go rynek DLT[49], który tworzy podwaliny pod tak zwany FINTERNET[50]. W ocenie autorów FINTERNET to miejsce, gdzie odbywać się będzie integracja dokumentu 3.0 na potrzeby tożsamości cyfrowej i umów bankowych. Dzięki takiemu zestawieniu, tj. dokumentowi 3.0 i pomysłów wykorzystania możliwości technicznych na bazie DLT, możliwe jest oferowanie nowych usług w bankowości. Sam finternet jest dążeniem do upowszechnienia usług na bazie tokenizacji, i dostarczenia tychże tokenów do zainteresowanych użytkowników poprzez ujednolicony rejestr[51]. Proces ten jest efektem odejścia od papierowych rejestrów (ksiąg rachunkowych) poprzez cyfryzację i dematerializację pieniądza. Kolejnym etapem tych głębokich zmian jest tokenizacja[52].

Jak podkreśla H. S. Shin tokenizacja nie jest synonimem decentralizacji, a jej przyszłościowy kierunek to nie DeFi na bazie kryptowalut, a tokenizacja aktywów ze świata rzeczywistego[53]. W takim ujęciu tokenizacja to proces rejestrowania roszczeń do aktywów rzeczywistych lub finansowych (**informacji**) na **programowalnej platformie**[54]. Taka platforma bazuje na tokenach i nie potrzebuje scentralizowanej warstwy aplikacyjnej, której rdzeniem jest rejestr będący bazą danych, jak w tradycyjnym rozwiązaniu (Rys. 5). Tradycyjne bazy nie byłyby też potrzebne w kontekście dostępu do danych użytkowników. Tak skonstruowana platforma mogłaby być zgodna z wcześniej opisanymi kwestiami tożsamości cyfrowej. Automatyczna weryfikacja atrybutu przez platformę pozwalałaby użytkownikowi na dostęp do usług finansowych w sposób szybki, z wykorzystaniem środków na odległość i bezpieczny. Z perspektywy banku z kolei – zgodny z obowiązującymi przepisami. Taka platforma mogłaby być usługą dodatkową do UE Wallet. Oferowałaby też nowy poziom automatyzacji.

Termin „programowalny" związany jest z możliwością wykorzystania **inteligentnych umów** i odpowiednią złożonością rejestru, co jest z kolei następstwem wykorzystania zaawansowanych rozwiązań technicznych[55]. Zgodnie ze wskazaniem M. Świerczyńskiego taką umowę charakteryzuje to, że jest to: „(...) oprogramowanie służące do automatycznego wykonywania określonych zadań, gdy zostaną spełnione z góry określone warunki". Jest to stanowisko zgodne z definicją legalną w Rozporządzeniu Parlamentu Europejskiego i Rady (UE) 2023/2854 z dnia 13 grudnia 2023 r. w sprawie zharmonizowanych przepisów dotyczących sprawiedliwego dostępu do danych i ich wykorzystywania oraz w sprawie zmiany rozporządzenia (UE) 2017/2394 i dyrektywy (UE) 2020/1828 (dalej: Akt w sprawie danych). Przy czym definicja legalna podkreśla również rolę danych, a jej pełne brzmienie w art. 2 pkt. 39 jest następujące: „(...) program komputerowy stosowany do automatycznego wykonywania umowy lub jej części, używający sekwencji **elektronicznych rekordów danych** i zapewniający ich **integralność** i **dokładność ich chronologicznego uporządkowania**"[56]. Należy podkreślić, że definicja legalna w akcie w sprawie danych nie spotkała się z przychylnym przyjęciem przez środowisko DLT, szczególnie tych podmiotów, które związane są z **Ethereum Blockchain**. Zarzucono prawodawcy zbyt szeroką definicję, która obejmie wszystkie inteligentne umowy swoimi restrykcyjnymi ograniczeniami[57].

Nie zmienia to jednak faktu, że Blockchain Ethereum jako pierwszy rejestr umożliwił tworzenie inteligentnych umów. Oferuje też standardy techniczne, na bazie których można projektować i emitować tokeny[58]. To właśnie upowszechnienie się emisji tokenów spowodowało, że konieczne były działania regulatora[59]. Warto dodać, że regulator europejski nie zdecydował się na wprowadzenie definicji legalnej tokenów. Termin ten pojawia się w Rozporządzeniu Parlamentu Europejskiego i Rady (UE) 2023/1114 z dnia 31 maja 2023 r. w sprawie rynków kryptoaktywów oraz zmiany rozporządzeń (UE) nr 1093/2010 i (UE) nr 1095/2010 oraz dyrektyw 2013/36/UE i (UE) 2019/1937, ale w przypadku definicji jest on tłumaczony tylko w formie nazw złożonych, które odnoszą się do pewnych

[49] Dokument 3.0 to koncepcja zapisu informacji w oparciu o nowe rozwiązania takie jak DLT. Dariusz Szostek, "Dokument 3.0" [w:] J. Gołaczyński (red.) "Prawo Nowych Technologii. Księga z okazji jubileuszu 20-lecia działalności Centrum Badań Problemów Prawnych i Ekonomicznych Komunikacji Elektronicznej i Studenckiego Koła Naukowego – Blok Prawa Komputerowego", 2022, Warszawa, el.

[50] A. Cartens, N. Nilekani, *Finternet: the financial system for the future*, "BIS Working Papers", No 1178, 2024, pp.

[51] I. Aldaroso, S. Doerr, L. Gambacorta, R. Garratt, P. K. Wilkens, *The tokenisation continuum*, "BIS Bulletin", 2023, No. 72, pp. 2.

[52] H. S. Shin, *Tokenisation for the real world*, "BIS speech", 2024, dostępne on-line: https://www.bis.org/speeches/sp240209.htm pobrano 6 sierpnia 2024r.

[53] Tamże.

[54] I. Aldaroso, S. Doerr, L. Gambacorta, R. Garratt, P. K. Wilkens..., pp. 2.

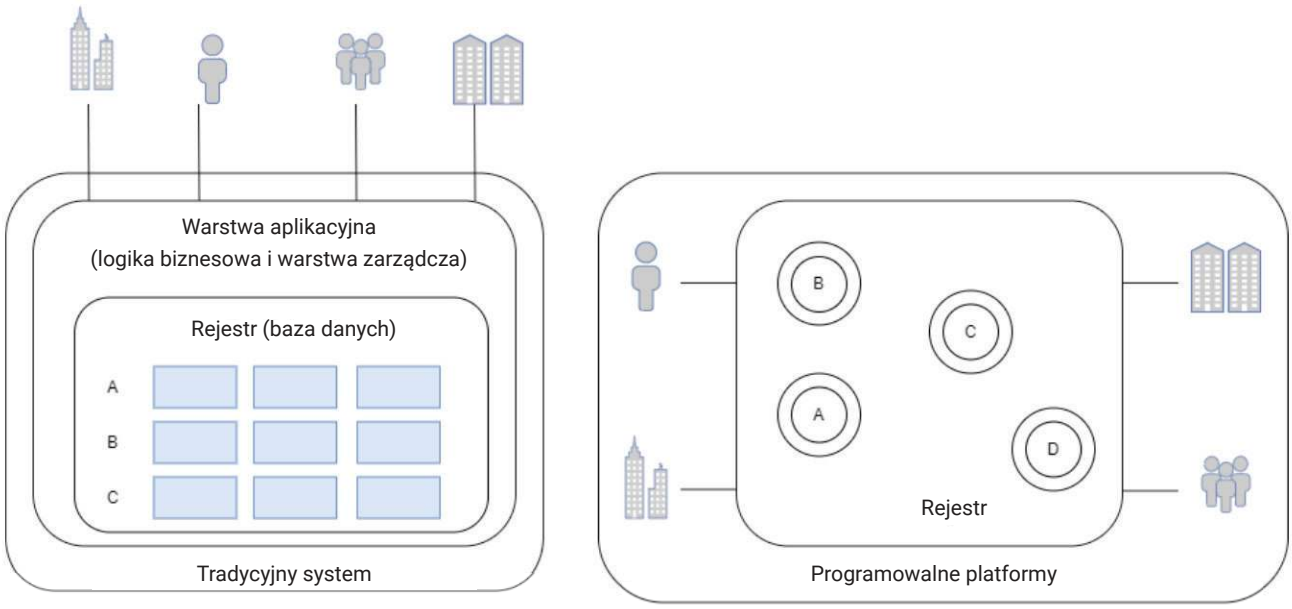
[55] M. Świerczyński, „Przełomowe technologie informatyczne w prawie prywatnym międzynarodowym", 2024, Warszawa, el.

[56] Dostępne on-line: https://eur-lex.europa.eu/legal-content/PL/TXT/HTML/?uri=OJ:L_202302854&qid=1723543094241 pobrano 6 sierpnia 2024r.

[57] Dostęp: https://data-act.info/joint-statement/ pobrano 6 sierpnia 2024r.

[58] V. Butterin, *Biała ksiega Ethereum*, dostęp: https://ethereum.org/pl/whitepaper/ pobrano 6 sierpnia 2024r; I. Aldaroso, S. Doerr, L. Gambacorta, R. Garratt, P. K. Wilkens..., pp. 2.

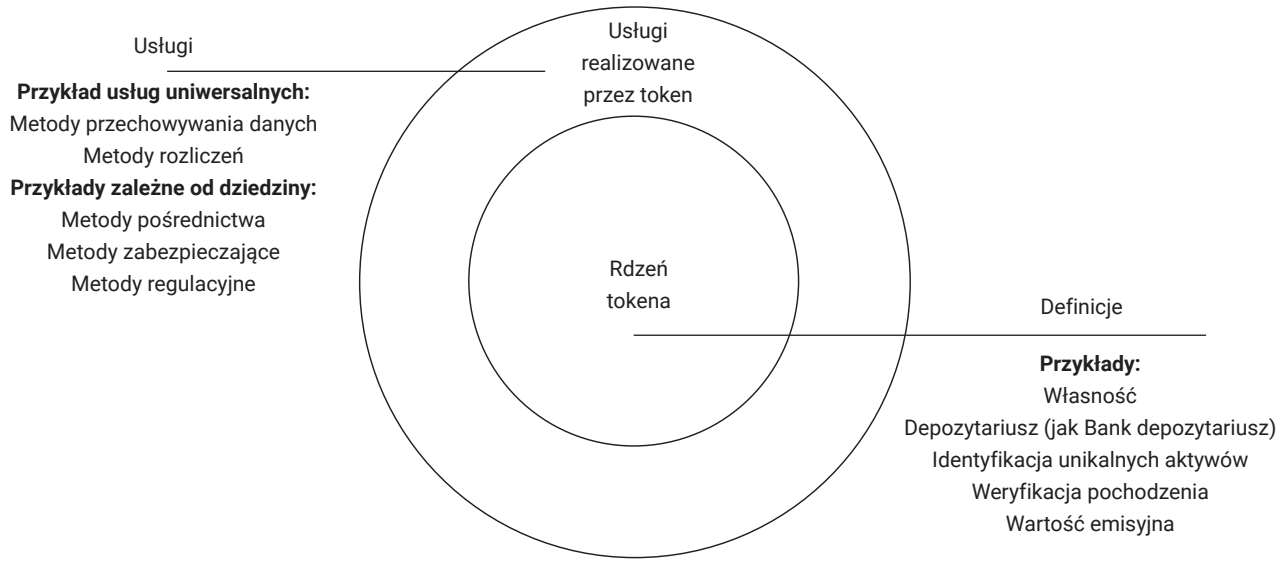
[59] Autorzy już pisali o tym w innych publikacjach – zob.. D. Szostek, "Blockchain and law", Baden-Baden, 2019, dostępne on-line: https://www.nomos-shop.de/nomos/titel/blockchain-and-the-law-id-95162/ obrano 6 sierpnia 2024r; R. Prabucki, „Kryptoaktywa w bankowości" [w:] K. Szpyt (red.), „FinTech. Nowe technologie w sektorze bankowym", 2024, Warszawa, el.



Rys. 6. Różnica pomiędzy programowalną platformą a tradycyjnym systemem.Źródło: Opracowanie własne.
Źródło: I. Aldaroso, S. Doerr, L. Gambacorta, R. Garratt, P. K. Wilkens, The tokenisation continuum, "BIS Bulletin", 2023, No. 72, pp. 2.

szczególnych tokenów[60]. Takie działanie należy uznać za właściwe – ramy prawne dla rynku kryptoaktywów odnoszą się do rozwiązań DLT i podobnych. Nie definiując tokenu prawodawca unijny dał sobie swobodę operowania tym terminem również przy rozwiązaniach innych, aniżeli DLT, co jest możliwe do zrealizowania[61].

Autorzy I. Aldaroso, S. Doerr, L. Gambacorta, R. Garratt, P. K. Wilkens opisują w swoim warsztacie badawczym kwestie tokenów w formule odniesienia się do „Usługi" i „Podstawy" (Rys. 6). Usługi odnoszą się do metod działania, a podstawy do tego, czym token jest. Konkludując: tokenizacja to **proces przekształcenia aktywa w token** z warstwami podstawowymi i usługowymi



Rys. 7. Czym jest token?
Źródło: I. Aldaroso, S. Doerr, L. Gambacorta, R. Garratt, P. K. Wilkens, The tokenisation continuum, "BIS Bulletin", 2023, No. 72, pp. 3.

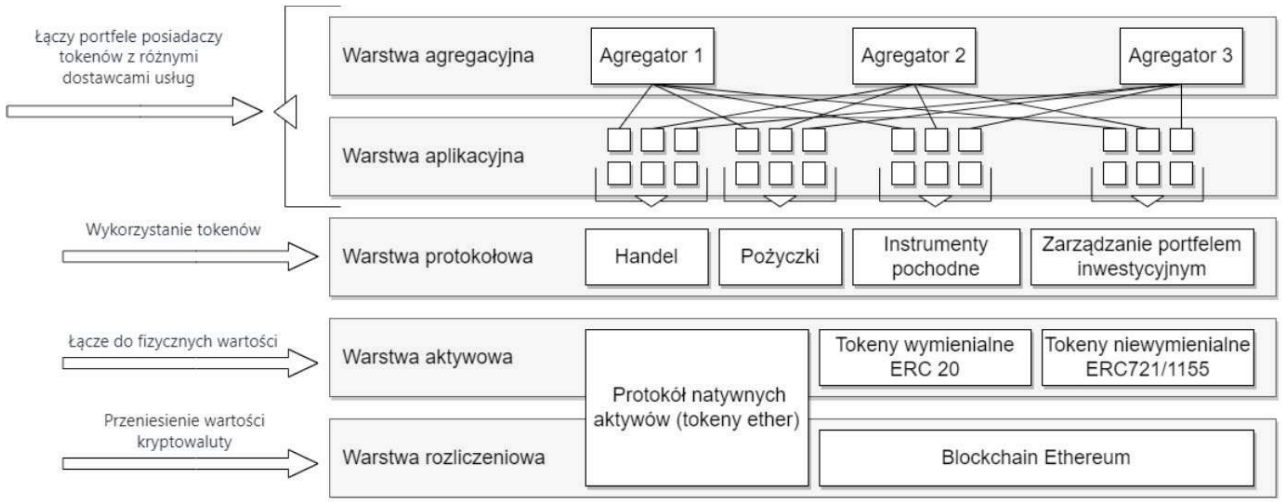
[60] Dostęp: https://eur-lex.europa.eu/legal-content/PL/TXT/?uri=-CELEX:32023R1114 pobrano 6 sierpnia 2024r.
[61] R. Garratt, H. S. Shin, *Stablecoins versus tokenised deposits: implications for the singleness of money*, "BIS Bulletin", 2023, no 73.

w pełnej zgodności z zasadami importującej programowalnej platformy (np. blockchain Ethereum).

Zaprezentowaną budowę tokenu można przedstawić też na płaszczyźnie konkretnego DLT. Jak już wskazano, blockchain Ethereum posiada odpowiednie standardy, które regulują od strony technicznej emisję tokenów. Sam mechanizm działania tego rozwiązania bazuje na tokenie natywnym (zwanym też z punktu widzenia doktryn polityczno-prawnych **kryptowalutą**), który pełni warstwę rozliczeniową. Odpowiednie ujęcie wszystkich kwestii w warstwach nakreśla nam, jak mogłoby wyglądać praktyczne wdrożenie tokenizacji na takiej platformie (przy czym sam token natywny to przykład tokenizacji). Całość rozwiązań technicznych jest łączona w tak zwany „stos", który tworzy niezależne środowisko finansowe oparte na różnych warstwach – DeFi (Rys. 7). Technika wyznacza też zasady, które są wyrażone w samym działaniu DLT, co przekłada się w przypadku emisji tokenów na ujednolicone, w przypadku blockchain Ethereum, w normach technicznych ERC reguły – tak, aby każdy wybrał takie, które odpowiadają jego pomysłowi na wykorzystanie tokenów.

Główny rdzeń standaryzacyjny dla tokenów w blockchain Etehreum to ERC-20 i ERC-721, bądź ERC-1155. ERC-20 ustanawia, że tokeny działają tak, jak token natywny, czyli ether – są wymienialne. Jest to norma opracowana przez F. Vogelstellera w 2015 roku. Jej zadaniem jest implementowanie API dla tokenów w inteligentnych umowach. Dzięki temu możliwy jest proces tokenizacji (tokeny emitujemy poprzez napisanie programu na ich emisję w inteligentnej umowie). ERC-721 to standard dedykowany tak zwanym NFT – tokenom niewymienialnym. Analogicznie, standard dla NFT implementuje API dla tokenów w ramach inteligentnych umów. Inność tokenów w tym standardzie polega na nadaniu im unikalności – są nieidentyczne i niezamienne. W związku z tym są rozróżnialne i można śledzić własność każdego z nich osobno. ERC-1155 to standard, który umożliwia emisję obu rodzajów tokenów w ramach jednej inteligentnej umowy[62]. Powyższa egzemplifikacja jest wskazaniem, jak wygląda cały proces na konkretnym działającym DLT.

Należy podkreślić, że optymalnym warunkiem rozwoju tokenizacji jest włączenie w cały proces banków i aktywów, które już występują w świecie realnym. Wskazane środowiska na bazie DLT i podobnych rozwiązań pełnić mają rolę platform, a cała technika za nimi stojąca ma pozwolić na stworzenie programowalnego rejestru, będącego programowalną platformą. Różnicą między DeFi a takim podejściem jest zbudowanie połączenia pomiędzy tradycyjnym rejestrem a rejestrem programowalnym – tak zwanej **rampy**. Dzięki rampom użytkownicy otrzymują nie tylko usługi w ramach DeFi, ale też usługi z katalogu tradycyjnych finansów z wszystkimi benefitami obracania nimi na bazie programowalnego rejestru. W związku z tym, że każda platforma programowalna może działać na innych zasadach, istotny jest też proces „**owijania** poprzez **most**". Proces ten pozwala na wykorzystanie kilku platform oferujących różne reguły działania dla tokenów (Rys. 8), co pozostaje



Rys. 8. Tak zwany stos DeFi.

Źródło: D. A. Zetzsche, R. P. Buckley, D. W. Arner, M. C. van Ek, Remaining regulatory challenges in digital finance and cryptoassets after MiCA, "Study Requested by the ECON Committe", 2023, pp. 27.

[62] Autorzy poruszali te zagadnienia w innych publikacjach np. R. Prabucki, "Mała encyklopedia rewolucji, co dalej?" [w:] R. Prabucki, R Wielki, K. Mucha (red.) Kryptowaluty: Perspektywa kryminologiczna i kryminalistyczna, 2024.

w zgodzie z wnioskami z poprzednich rozdziałów. Inne rozwiązanie można wykorzystać w takiej sytuacji dla tożsamości cyfrowej, a inne dla usługi finansowej.

Przerzucone dane z tradycyjnych rejestrów (baz danych) do rejestrów programowalnych otwierają drogę do ujednoliconych rejestrów, które oferują nowe możliwości. Nowe rejestry bazują od strony cywilistycznej na koncepcji **dokumentu 3.0**. Dzięki rampom banki i inne instytucje finansowe mogą korzystać z nowych rozwiązań na bazie danych. Niemniej ważny w tym aspekcie jest kontekst prawny. Korzystanie z dokumentu 3.0 wymaga odpowiedniego uregulowania tworzenia środowisk na bazie DLT, nadania rynkowi kryptoaktywów odpowiednich ram prawnych, a także uwzględnienia wątku cyberbezpieczeństwa dla podmiotów oferujących usługi na bazie **kryptoaktywów**, jak i reguł dla wykorzystania danych na poziomie prawa. Jak zauważa K. Szpringer, powstanie regulacji pozwoliłoby wypchnąć środek ciężkości rozwoju z DeFi na wdrożenia w postaci tokenizacji na rynku finansowym[63]. Stymulowałoby to w ocenie autorów rozwój tego, co współcześnie rozumiemy pod pojęciem „portfel" – zarówno na rynku DeFi, jak i tradycyjnym, z UE Wallet. Portfele na rynku DeFi służą do dostępu do tokenów i są rozwiązaniem ściśle technicznym bazującym na kryptografii[64]. Na rynku tradycyjnych finansów są to aplikacje mobilne, które analogicznie pozwalają na płatności (przesyłanie wartości), a także przechowują informacje, np. o biletach lub kartach lojalnościowych[65]. Przy powstaniu UE Wallet wszystkie te benefity niezależnie rozwijającego się rynku „portfeli", będą usługami dodatkowymi dla oferowanego w UE obywatelom narzędzia.

Brak regulacji powodował, że zainteresowanie współczesnej bankowości nowymi rozwiązaniami było nikłe. Łączenie tożsamości cyfrowej ze stokenizowanym rynkiem otwiera drogę do nowych usług. Do 2022 roku, gdy wskutek braku regulacji miały miejsce kolejne na rynku kryptoaktywów zdarzenia deprymujące ten obszar inwestycyjny, ESMA zauważyła, że aktywa kryptowalutowe stanowią **mniej niż 1% całkowitej kapitalizacji rynkowej** w tradycyjnych klasach aktywów[66]. W związku z tym powiązań pomiędzy zamkniętym środowiskiem z tokenami natywnymi a rynkiem finansowym nie było wiele. Jednak już w 2023 roku Europejski Bank Inwestycyjny opracował swoją pierwszą obligację cyfrową, która wykorzystywała kombinację DLT (prywatnych i publicznych blockchainów). Dostępność tych rozwiązań była możliwa za pośrednictwem platformy do tokenizacji – HSBC Orion. Takie działanie możliwe było dzięki wprowadzeniu odpowiednich ram prawnych przez Luksemburg[67]. Przykład ten pokazuje również, że tokenizacja i owijanie może być realnie wdrożone dla stworzenia ujednoliconych platform. Konkludując, dobrodziejstwo dokumentu 3.0 w bankowości zależy od właściwych regulacji i ich kompleksowości.

W perspektywie unijnych regulacji stymulujących wykorzystanie dokumentu 3.0 w aspekcie DLT i rynku kryptoaktywów należy zaliczyć:

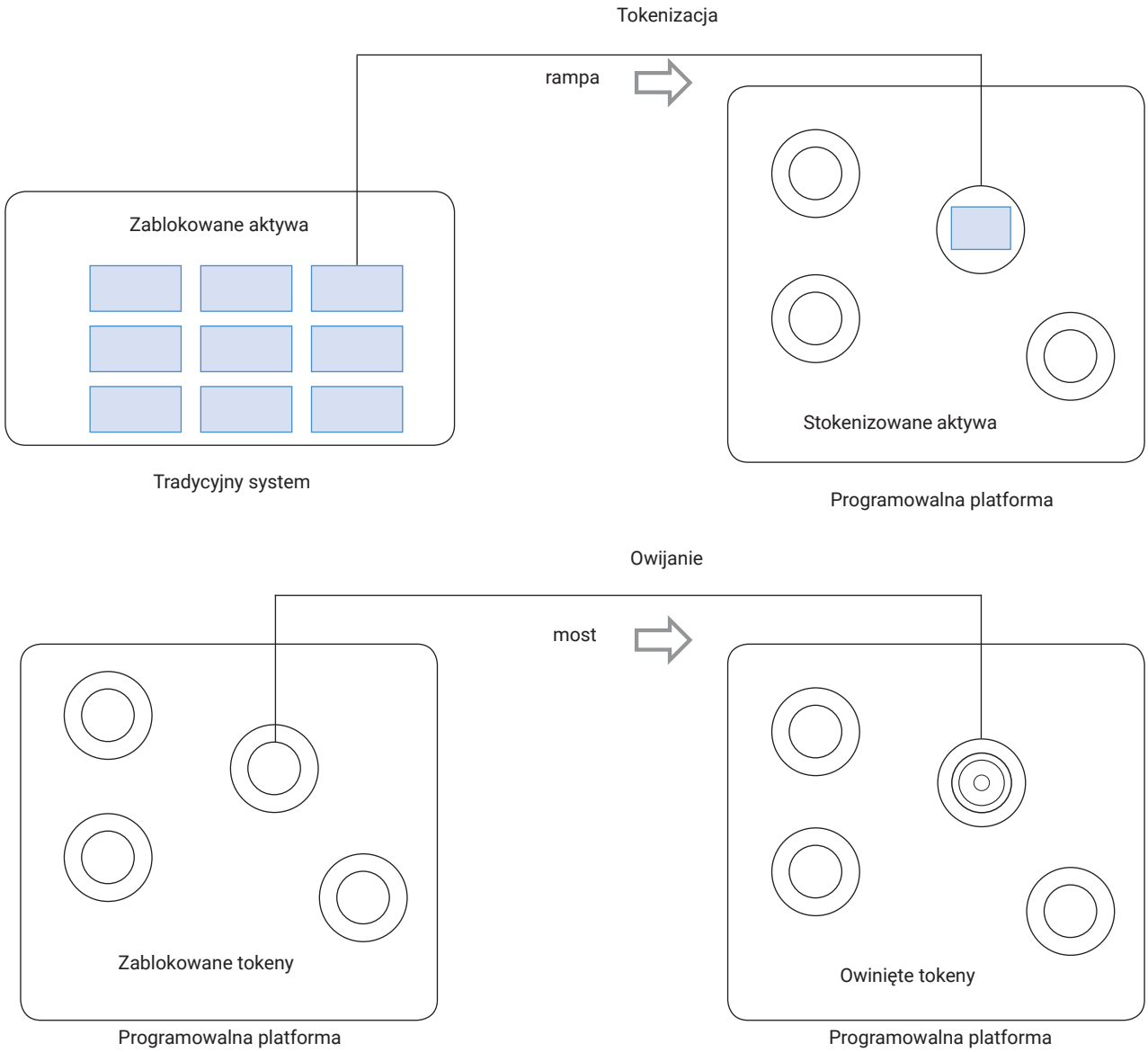
1. Rozporządzenie parlamentu europejskiego i rady (UE) 2022/858 z dnia 30 maja 2022 r. w sprawie systemu pilotażowego na potrzeby infrastruktur rynkowych opartych na technologii rozproszonego rejestru, a także zmiany rozporządzeń (UE) nr 600/2014 i (UE) nr 909/2014 oraz dyrektywy 2014/65/UE (dalej **DLT Pilot),**

2. Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2023/1114 z dnia 31 maja 2023 r. w sprawie rynków kryptoaktywów oraz zmiany rozporządzeń (UE) nr 1093/2010 i (UE) nr 1095/2010 oraz dyrektyw 2013/36/UE i (UE) 2019/1937 (Dalej MiCAR).

Mimo podobieństw należy podkreślić, że oba akty prawne pokrywają inne obszary kryptoaktywów[68]. Oba zostaną omówione w rozdziale 7.

Jak już zasygnalizowano, istotnym elementem całego procesu tokenizacji jest inteligentny kontrakt (umowa). Pojawienie się definicji inteligentnej umowy, zgodnie z pkt. 63 dokumentu o tytule: „Najczęściej zadawane pytania – Akt o Danych", nie oddziałuje na krajowe prawo umów. W opracowaniu wskazano, że: „definicja „inteligentnej umowy" jasno wskazuje, że to tylko programy komputerowe wykorzystywane do wykonywania umów – a nie umowy jako takie – są regulowane przez rozporządzenie o danych"[69]. Samo brzmienie definicji pozwala objąć swoim zastosowaniem zarówno opisane z Ethereum Blockchain **smart contracts**, jak i inne rozwiązania. Oddziaływanie to może być też negatywne, przez zapisy, które wprowadzają wymogi niemożliwe do zrealizowania w rozwiązaniach DLT bazujących na otwartych

[63] K. Szpringer, *Czy tokenizacja ma przyszłość*, „Monitor Prawa Bankowego" 2024, pp. 26.
[64] D. Zetzsche, A. Nikolakopoulou, *Crypto Custody and Crypto Wallets – An Empirical Assessment* –, 2024, Dostęp: https://blogs.law.ox.ac.uk/oblb/blog-post/2024/05/crypto-custody-and-crypto-wallets-empirical-assessment pobrano 6 sierpnia 2024r.
[65] FCA, PSR, *Call for information. Big tech and digital wallets*, CP24/9, 2024.
[66] ESMA, *Opening statement*, 2022, Dostęp: (02.08.2024).
[67] EIB, *EIB issues its first ever digital bond in pound sterling*, 2023, Dostęp: https://www.eib.org/en/press/all/2023-030-eib-issues-its-first-ever-digital-bond-in-british-pounds (02.08.2024).
[68] F. Annunziata, *Some reflections on the Proposed MiCA Regulation*, [w:] S. Leo, I. C. Panetta (red.), The Role of Distributed Ledger Technology in Banking. From Theory to Practice, Cambidge 2024, pp. 84.
[69] European Commission, *Frequently Asked Questions Data Act*, ver. 1.1, 2024 pp. 35.



Rys. 9. Tokenizowanie z wykorzystaniem rampy i owijanie poprzez most.
Źródło: I. Aldaroso, S. Doerr, L. Gambacorta, R. Garratt, P. K. Wilkens, The tokenisation continuum, "BIS Bulletin", 2023, No. 72, pp. 4.

rozwiązaniach blockchain. Zgodnie ze wskazanymi przepisami transakcje należy móc przerwać lub zmienić (tak zwany wymóg „*kill switch*"). W ocenie przedstawicieli rynku kryptoaktywów, pojęcie „smart contracts" jest niefortunne, ponieważ wedle nich intencją prawodawcy nie było wcale wykorzystanie tego pojęcia. Mimo sugestii o zmianę „smart contracts" na „digital contracts" prawodawca unijny pozostał nieugięty, wprowadzając definicję legalną inteligentnych umów[70]. W ocenie autorów istotnym jest motyw 105 z preambuły rozporządzenia o danych, które jasno wskazuje, że obostrzenia stosowane są w ściśle określonych warunkach: „zasadnicze wymagania powinny mieć zastosowanie wyłącznie do sprzedawców inteligentnych umów, jednak nie w przypadku, gdy opracowują oni inteligentne umowy wewnątrz przedsiębiorstwa wyłącznie na użytek wewnętrzny. Zasadnicze wymaganie polegające na zapewnieniu, by wykonywanie inteligentnych umów mogło być zawieszane i by inteligentne umowy mogły być rozwiązywane, zakłada wzajemną zgodę stron umowy o dzielenie się danymi. Stosowanie inteligentnych umów do automatycznego wykonywania umów o dzielenie się danymi pozostaje bez wpływu lub powinno pozostawać bez wpływu na stosowanie do umów o dzielenie się danymi stosownych przepisów prawa cywilnego, prawa zobowiązań i prawa ochrony konsumentów". W ocenie autorów prawodawca chciał i dążył do uregulowania szerokiego spektrum inteligentnych umów. Jest to

[70] https://data-act.info/joint-statement/ (02.08.2024).

definicja zgodna z ogólnymi założeniami Nicka Szabo. Odrzucono też w ten sposób blockchain czy też DLT jako niezbędny nośnik. Ponadto istotnym jest też kryterium, jakim jest identyfikowanie sprzedawców i innych osób, których działalność obejmuje wdrażanie inteligentnych umów dla innych, poprzez **sprzedaż** takich programów komputerowych. W przypadku braku elementu sprzedaży, nie ma konieczności spełnienia wymagań[71].

W kontekście omawianych zagadnień należy podkreślić ważne spostrzeżenia, które zostały zasygnalizowane przez Hennemann, Ebner, Karsten, Lienemann, Wienroeder. Inteligentne umowy są przedstawiane jako potencjał w zakresie ułatwiania zautomatyzowanego udostępniania i łączenia danych na dużą skalę przy jednoczesnym egzekwowaniu ograniczeń użytkowania. Te cechy powodowały, że Komisja przedstawiała je jako narzędzie techniczne wysokiego szczebla od samego początku inicjatywy rozporządzenia o danych. Szczególnie w kwestii długoterminowych porozumień (inaczej mówiąc, umów licencyjnych na dane) między posiadaczami danych a odbiorcami danych regularnie udostępniającymi dane, zauważono potencjał na wykorzystanie inteligentnych umów. W takich okolicznościach przewiduje się, że inteligentne umowy obniżą koszty transakcji (motyw 47 preambuły rozporządzenia o danych). Kwestia inteligentnych kontraktów jest poruszona (i skonkretyzowana) przede wszystkim w art. 36 rozporządzenia o danych. Pojawiają się one również w dwóch innych kontekstach regulacyjnych. Po pierwsze, przy kwestiach środków ochronnych opisanych w art. 11 ust. 1 rozporządzenia o danych. Rola inteligentnej umowy jako środka ochrony miałaby polegać na przeciwdziałaniu przed nieuprawnionym ujawnieniem przy wdrażaniu udostępniania łatwo dostępnych danych zgodnie z art. 4 i następnymi w rozporządzeniu o danych. Po drugie, inteligentne umowy wskazuje się jako przedmioty wymogów interoperacyjności w celu umożliwienia automatycznego wykonywania umów licencyjnych dotyczących danych, w przestrzeniach danych zgodnie z art. 33 ust. 1 lit. d) rozporządzenia o danych[72].

Ponadto warto zauważyć, że istnieje jeszcze jeden istotny element umieszczenia inteligentnych umów w rozporządzeniu o danych. Taka konstrukcja pozwala na domniemanie zgodności z zasadniczymi wymogami dla inteligentnych kontraktów, które spełniają normy zharmonizowane lub odpowiednie części Rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 1025/2012 z dnia 25 października 2012 r. w sprawie normalizacji europejskiej, zmieniające dyrektywy Rady 89/686/EWG i 93/15/EWG oraz dyrektywy Parlamentu Europejskiego i Rady 94/9/WE, 94/25/WE, 95/16/WE, 97/23/WE, 98/34/WE, 2004/22/WE, 2007/23/WE, 2009/23/WE i 2009/105/WE oraz uchylające decyzję Rady 87/95/EWG i decyzję Parlamentu Europejskiego i Rady nr 1673/2006/WE. W przypadku braku zharmonizowanych norm Komisja może podjąć kroki w celu ich opracowania i przyjęcia. Stwarza to realną szansę na promowanie ich interoperacyjności poprzez ustanowienie zasadniczych wymogów dla profesjonalistów.

Pozostaje pytanie o kwestie domniemania w kwestii samej inteligentnej umowy w aspekcie prawa. Należałoby założyć (domniemywać), że inteligentna umowa jest po prostu klasyczną umową napisaną w innym języku. W związku z tym, gdybyśmy stworzyli do niej klasyczną umowę, to prawo właściwe dla umowy oraz inteligentnej umowy jest takie samo. Teoretycznie, jak wskazuje El Harrak, można wyobrazić sobie sytuację, w której treść klasycznej umowy i inteligentnej umowy są rozbieżne. W takiej sytuacji, z czym zgadzają się autorzy raportu, pierwszeństwo powinna mieć klasyczna umowa. Jest to zgodne z zasadą zaproponowaną przez instytut ELI, na którą wskazuje też El Harrak. Zasada ta brzmi: „Off-chain przeważa nad on-chain". Stanowi ona, że „w przypadku, gdy umowa lub elementy umowy zawarte poza blockchainem są tłumaczone na kod [...], warunki umowy zawartej poza blockchainem mają pierwszeństwo przed wszelkimi warunkami zakodowanymi w blockchainie, chyba że strony wyraźnie uzgodniły inaczej poza blockchainem"[73].

Nie ulega jednak wątpliwości, że inteligenta umowa stała się narzędziem do wykorzystania przy projektowaniu bezpieczeństwa od strony technicznej.

[71] M. Hennemann, G. K. Ebner, B. Karsten, G. Lienemann, M. Wienroeder, *Data Act. An Introduction*., 2024, pp. 135-136.
[72] Tamże.
[73] M. El Harrak, Do Smart Contracts Need New Conflict-of-Laws Rules? [w:] *Blockchain and Private International Law*, A. Bonomi, M. Lehmann, S. Lalani (red.), 2023,

Dokument 3.0 regulacje dotyczące bezpieczeństwa

Bezpieczeństwo w aspekcie dokumentu 3.0 i prawa zostało podzielone w tym rozdziale na dwie płaszczyzny – bezpieczeństwo rynku kryptoaktywów oraz cyberbezpieczeństwo. Pierwsza płaszczyzna dotyczy podmiotów i działania z kryptoaktywami. Regulacje na tym poziomie tworzą ramy dla podmiotów, które oferowałyby usługi istotne z punktu widzenia omawianych zagadnień w zakresie krytpoaktywów. Opisane wcześniej tokeny, na bazie których działają lub mogą działać usługi, znalazły się w nowych ramach prawnych.

W kontekście powyższych istotnym jest zacząć od przykładu DLT Pilot. Kryptoaktywa nie istnieją w próżni regulacyjnej. Oznacza to, że te, które przyjmą na bazie obowiązujących ram prawnych np. postać instrumentów finansowych, będą podlegać pod Dyrektywę Parlamentu Europejskiego i Rady 2014/65/UE z dnia 15 maja 2014 r. w sprawie rynków instrumentów finansowych oraz zmieniająca dyrektywę 2002/92/WE i dyrektywę 2011/61/UE (dalej **MFiD**) oraz ich implementację. W takiej sytuacji obrót nimi znajdzie się w silnie uregulowanym obszarze, co może powodować uniemożliwienie rozwoju takiej innowacji. W związku z tym prawodawca unijny zdecydował się wprowadzić DLT Pilot, które ma **opcjonalnie** pozwalać regulować takie kryptoaktywa, zwalniając pewne podmioty stosujące wybrane systemy z wymogów stawianych przez unijne prawo finansowe (Rys. 9). Jak sama nazwa wskazuje, akt prawny jest działaniem **pilotażowym**, a ustanowione w ten sposób ramy mają działać 3 lata z możliwością rozciągnięcia ich w czasie przez Komisję Europejską o kolejne lata. Tak określony charakter próby ma na celu umożliwienie również ESMA i właściwym organom zdobycie doświadczenia w zakresie konkretnych możliwości i zagrożeń związanych z technologiami rozproszonego rejestru w usługach transakcyjnych i potransakcyjnych.

Zakres pilotażowego systemu DLT jest ograniczony do warunków mających zastosowanie do działania infrastruktur rynkowych opartych na **DLT**, zezwoleń na ich wykorzystanie oraz nadzoru i koordynacji właściwych organów i ESMA. Pod względem podmiotowym rozporządzenie ma zastosowanie do firm inwestycyjnych, operatorów rynku i CDPW[74]. Jest to też element bezpieczeństwa. Ponadto ESMA publikuje też listę infrastruktury rynkowej opartej na DLT wraz z innymi kluczowymi informacjami.

Należy też podkreślić, że opcjonalność stosowania DLT Pilot nie wpływa na inne systemy rynku finansowego, takie jak wielostronne platformy obrotu (MTF), zorganizowane platformy obrotu (OTF), centralne depozyty papierów wartościowych (CSD) i centralnych kontrahentów (CCP), co umożliwia poprzez te systemy prowadzenie działalności transakcyjnych i potransakcyjnej w zakresie kryptoaktywów, które kwalifikują się jako instrumenty finansowe zgodnie z prawodawstwem finansowym UE.

Drugim istotnym aktem jest **MiCAR**. Regulacja ta ma za zadanie wprowadzić kompleksowe ramy regulacyjne ustanowione przez Unię Europejską, mające na celu stworzenie jednolitych zasad dla kryptoaktywów i powiązanych z nimi usług. Kluczowe aspekty MiCAR z punktu widzenia omawianych zagadnień obejmują[75]:

1. Autoryzację dla dostawców usług związanych z kryptoaktywami (**CASP**): MiCAR wymaga, aby dostawcy usług CASP uzyskali zgodę do działania w UE. Obejmuje to między innymi usługi takie jak przechowywanie, handel i doradztwo związane z kryptoaktywami,

2. **Zakres i ograniczenia:** MiCAR dotyczy nieuregulowanych kryptoaktywów, ale wyłącza te, które są już regulowane na mocy istniejącego ustawodawstwa finansowego UE.

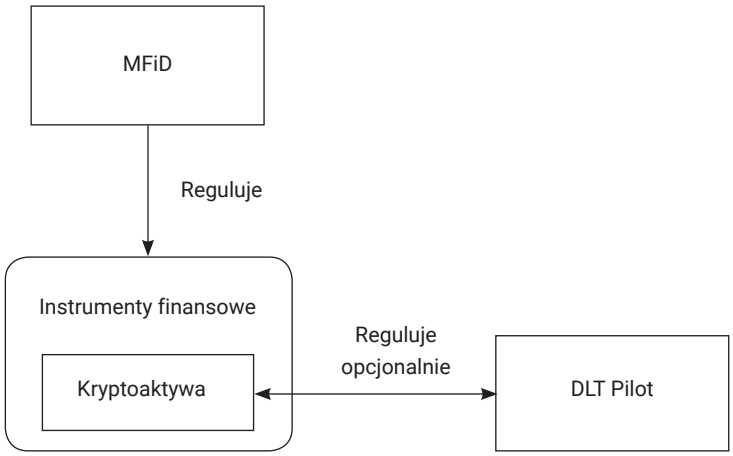
Na podstawie powyższego opisu kluczowych elementów uznać należy, że MiCAR uzupełnia obowiązujące już ustawodawstwo w zakresie tych tokenów, które nie znajdowały się w zakresie już obowiązującego prawa finansowego UE. Zgodnie z wytycznymi ESMA przeprowadza się test na bazie MiCAR i innych regulacji, aby sprawdzić, pod które przepisy podchodzą kryptoaktywa, które stosujemy (Rys. 10).

Problematycznym elementem testu są tak zwane tokeny **NFT**. Nazwa ta jest skrótowcem od *non-fungible tokens*, co odnosić się ma do unikalnych, nieustandaryzowanych aktywów lub tokenów, które wcześniej wskazano w ramach standardów Ethereum. Ich wykorzystanie może wykraczać poza produkty finansowe oferujące też inne nowe modele biznesowe[76]. Niekiedy tokeny te są nazywane „niepodzielnymi". Należy też podkreślić, że co do zasady MiCAR wyłącza NFT spod swojego zakresu w art. 2 ust. 3: „niniejsze rozporządzenie nie ma zastosowania do kryptoaktywów, które są unikalne i nie są zamienne z innymi kryptoaktywami". Trendy rynkowe ujawniają jednak modele biznesowe, gdzie NFT mogą być przedmiotem obrotu na rynkach, mogą być gromadzone spekulacyjnie i wykorzystywane jako środek wymiany. Możliwości

[74] Zgodnie z art 2 pkt. 14 DLT Pilot: „(...) oznacza centralny depozyt papierów wartościowych zdefiniowany w art. 2 ust. 1 pkt 1 rozporządzenia (UE) nr 909/2014.".

[75] K. F. Skorpen, *The Principle of Reverse Solicitation Under the Markets in Crypto Assets Regulation (MiCA)*, "European Union Law Working Papers" No. 80, 2023, pp. 11-12.

[76] M. Langer, P. Pinior, *Tokenizacja praw udziałowych w spółkach osobowych*, „Przegląd ustawodawstwa gospodarczego" nr 10, 2023, pp. 11.



Rys. 10. Relacja MFiD do DLT Pilot.
Źródło: Opracowanie własne.

te są ograniczone ze względu na techniczne parametry NFT, ale zastosowanie takich tokenów jako instrumentów finansowych jest możliwe. Co więcej, teoretyczna część NFT (ułamkowe) powodują brak unikalności. Reasumując – samo przypisanie unikalnego identyfikatora do pewnej wartości kryptograficznej nie powinno być zatem wystarczające do sklasyfikowania jej jako unikalnej lub niewymienialnej[77].

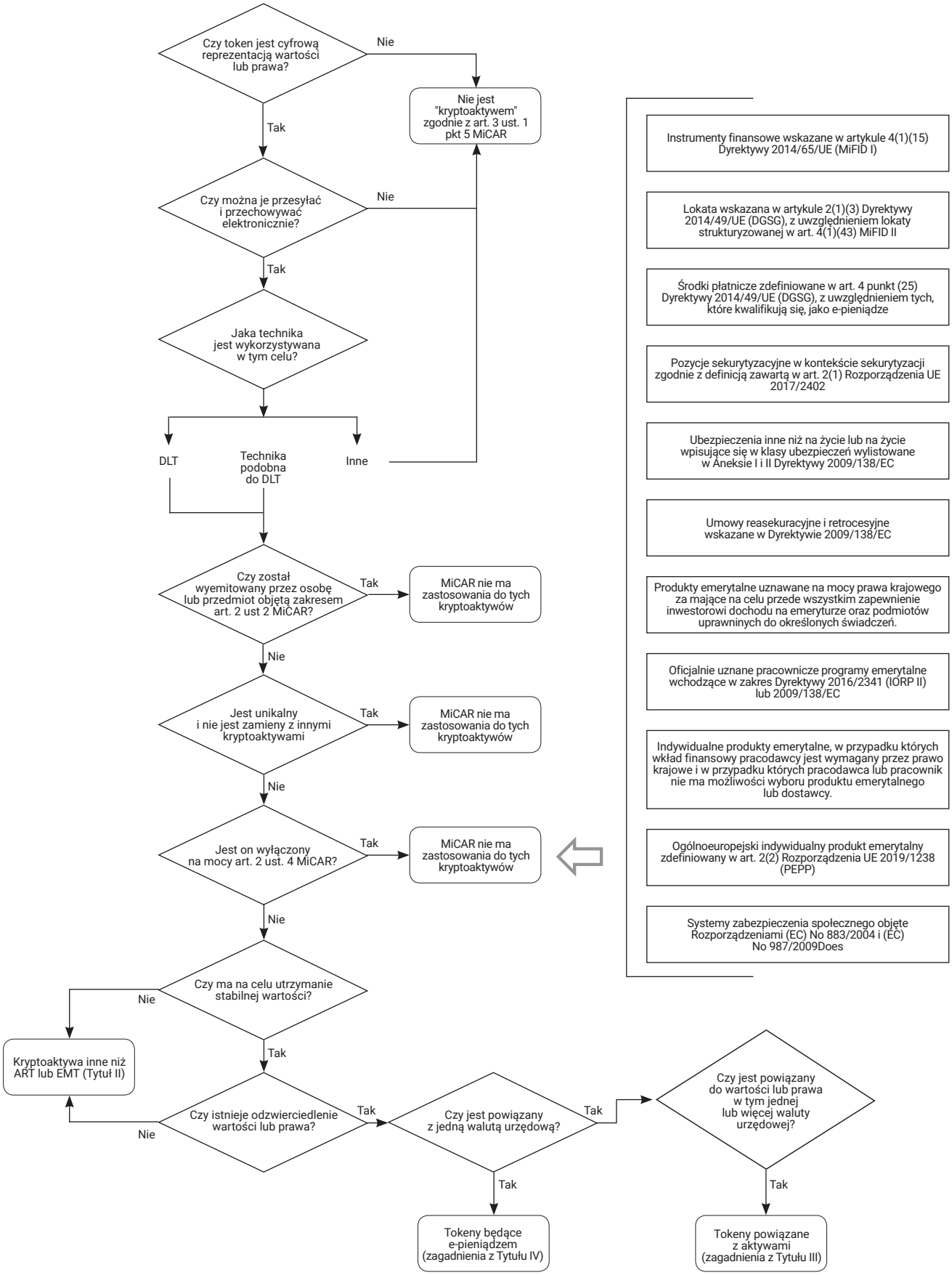
Kolejnym elementem jest zbudowanie połączenia pomiędzy MiCAR, a **DORA**. Powiązanie to polega na wskazaniu, że podmioty oferujące usługi w zakresie kryptoaktywów znajdują się w ramach obowiązywania MiCAR. Wskazanie to jest wyrażone w art. 3 ust. 1 pkt. 16 MiCAR. Usługa w zakresie kryptoaktywów opisana jest poprzez katalog enumeratywnie wskazanych usług lub rodzajów działalności związanych z kryptoaktywami, których jest łącznie 10 (Rys. 11). Następnie w DORA w art. 2 ust. 1 lit. f wskazano, że rozporządzenie ma zastosowanie dla: „dostawców usług w zakresie kryptoaktywów, którzy uzyskali zezwolenie na mocy rozporządzenia Parlamentu Europejskiego i Rady w sprawie rynków kryptoaktywów oraz zmieniającego rozporządzenia (UE) nr 1093/2010 i (UE) nr 1095/2010 oraz dyrektywy 2013/36/UE i (UE) 2019/1937 (zwanego dalej „rozporządzeniem w sprawie rynków kryptoaktywów") i emitentów tokenów powiązanych z aktywami". W ten sposób podmioty oferujące usługi w zakresie tokenów, które mieszczą się w ramach MiCAR, podlegają też restrykcyjnym przepisom w kwestii cyberbezpieczeństwa. DORA wprowadza ten sam poziom cyberbezpieczeństwa i odporności cyfrowej dla wszystkich podmiotów finansowych we wszystkich krajach UE. W ten sposób cyberbezpieczeństwo i ciągłość działania banków, firm ubezpieczeniowych, podmiotów oferujących usługi w zakresie kryptoaktywów i innych organizacji finansowych będą takie same we wszystkich krajach UE.

Do najważniejszych elementów DORA należy zaliczyć:

1. wskazanie bardzo szczegółowych wymogów dotyczących zarządzania ryzykiem ICT,
2. przedstawienie uproszczonych ram zarządzania ryzykiem ICT dla mniejszych podmiotów finansowych,
3. wskazanie klasyfikacji i raportowania incydentów i zagrożeń,
4. określenie zasad testowania cyfrowej odporności operacyjnej, w tym testy penetracyjne,
5. ustalenie zarządzania ryzykiem związanym z zewnętrznymi dostawcami ICT,
6. wskazanie wymagań dla dostawców usług ICT i ich nadzoru,
7. określenie zasad udostępniania informacji o zagrożeniach cybernetycznych,
8. wskazanie organów rządowych (właściwe organy) odpowiedzialnych za egzekwowanie DORA,
9. ustalenie kar dla organizacji finansowych i zewnętrznych dostawców ICT,

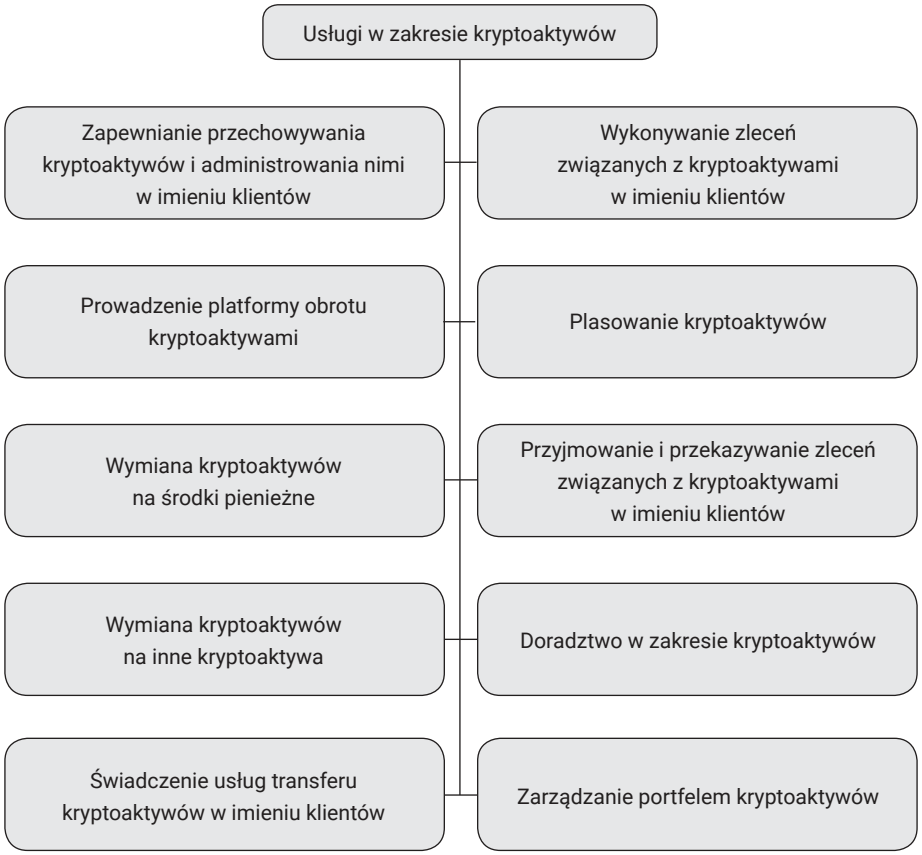
DORA, jak i zresztą NIS2, adresują kwestie „bezpieczeństwa sieci i systemów informatycznych", co

[77] EUBlockchain, *NFT-Legal Token Classification*, 2021. Dostęp: https://ssrn.com/abstract=3891872 (02.08.2024).



Rys. 11. Test na kryptoaktywa.

Źródło: ESMA, Consultation paper: Draft Guidelines on templates for explanations and opinions, and the standardised test for the classification of crypto-assets, under Article 97(1) of Regulation (EU) 2023/1114, 2024, pp. 34.



Rys. 12. Usługi w zakresie kryptoaktywów opisane w MiCAR.
Źródło: Opracowanie własne.

oznacza zdolność sieci i systemów informatycznych do przeciwstawienia się, przy określonym poziomie zaufania, wszelkim zdarzeniom, które mogą zagrozić dostępności, autentyczności, integralności lub poufności przechowywanych, przesyłanych lub przetwarzanych danych lub usług oferowanych przez te sieci i systemy informatyczne lub dostępnych za ich pośrednictwem. Należy jednak podkreślić, że NIS2 mimo iż wymienia „bankowość" i „infrastrukturę rynku finansowego" jako sektory, które muszą być zgodne z NIS2, to jednak zgodnie z art. 4 NIS2, DORA i inne regulacje sektorowe mają pierwszeństwo przed NIS2. W ocenie autorów w takiej sytuacji wszelkie podmioty finansowe, które są objęte zakresem DORA, nie muszą przestrzegać NIS2. Tym samym w przeciwieństwie do podmiotów wskazanych w NIS2, podmioty finansowe z DORA zobligowane są do cyfrowej odporności operacyjnej, a nie stricte cyberbezpieczeństwa (Tab. 1).

Tab. 1. Różnica między cyberbezpieczeństwem w NIS2, a cyfrową odpornością operacyjną w DORA.

	NIS2	DORA
Najważniejsze zagadnienie	„cyberbezpieczeństwo" oznacza działania niezbędne do ochrony sieci i systemów informatycznych, użytkowników takich systemów oraz innych osób dotkniętych cyberzagrożeniami	„cyfrowa odporność operacyjna" oznacza zdolność podmiotu finansowego do budowania, zapewniania i weryfikowania swojej integralności operacyjnej i niezawodności poprzez zapewnienie, bezpośrednio lub pośrednio poprzez korzystanie z usług świadczonych przez dostawców usług będących osobami trzecimi w zakresie ICT, pełnego zakresu zdolności związanych z ICT niezbędnych do zapewnienia bezpieczeństwa sieci i systemów informatycznych, z których korzysta podmiot finansowy i które wspierają nieprzerwane świadczenie usług finansowych i ich jakość, w tym przez cały czas trwania zakłóceń

Jednym z najważniejszych elementów DORA jest zarządzanie ryzykiem ICT. Podmioty finansowe (inne niż mikroprzedsiębiorstwa) muszą:

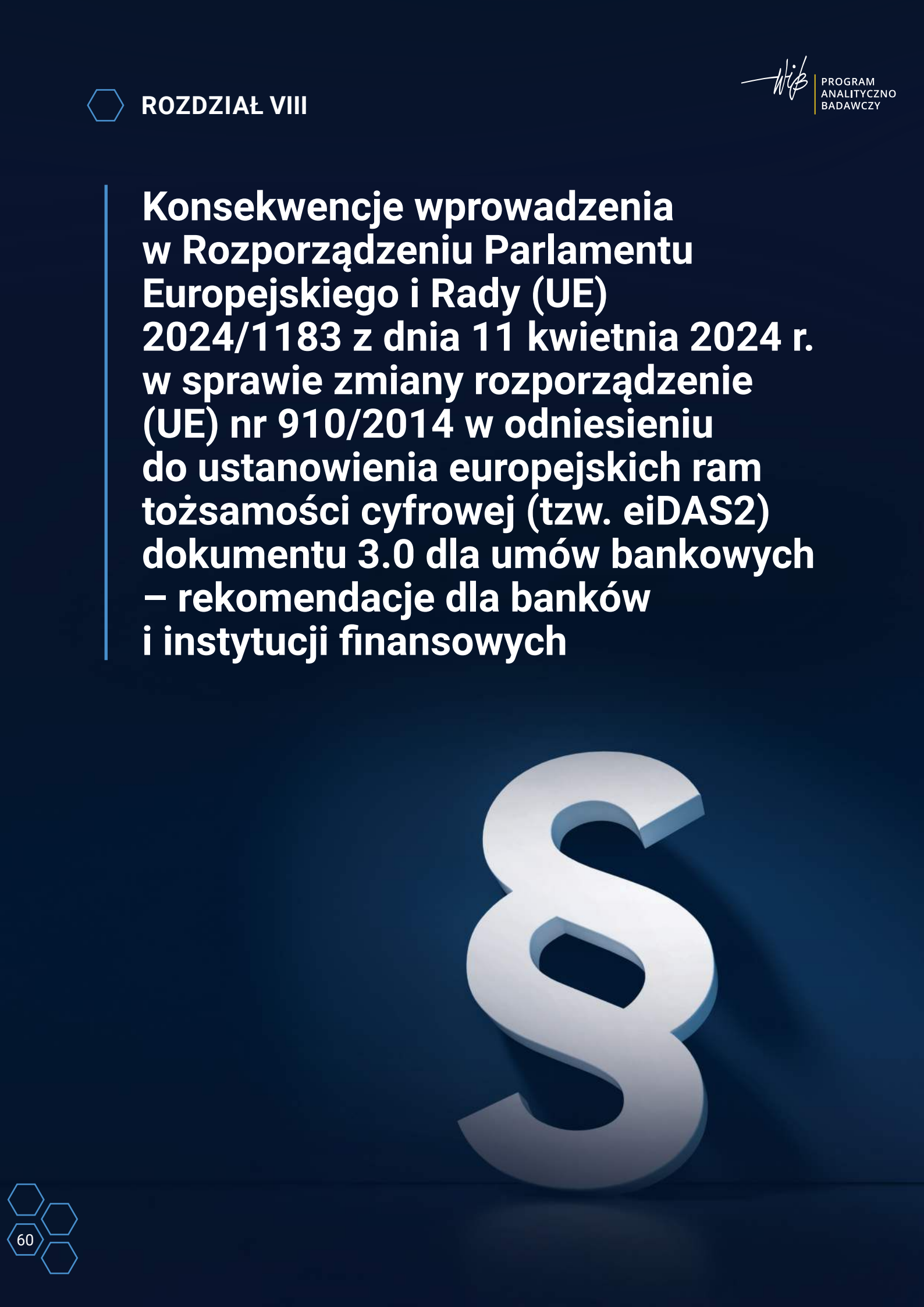
- posiadać wewnętrzne środki zarządzania i kontroli, które zapewnią skuteczne i ostrożne zarządzanie ryzykiem związanym z ICT,
- zapewniać, aby ich organ zarządzający określał, zatwierdzał, nadzorował i odpowiadał za wszystkie stosowne ustalenia,
- posiadać solidne, kompleksowe i dobrze udokumentowane ramy zarządzania ryzykiem i dobrze udokumentowane ramy zarządzania ryzykiem ICT wraz z niezbędnymi strategiami, politykami, procedurami, protokołami i narzędziami umożliwiającymi szybkie i skuteczne reagowanie ,
- stosować i utrzymywać zaktualizowane systemy, protokoły i narzędzia ICT, które są odpowiednie, niezawodne, odporne technologicznie i mają wystarczające możliwości oraz wystarczającą pojemność,
- zidentyfikować, sklasyfikować i odpowiednio udokumentować wszystkie wspierane przez ICT funkcje biznesowe, role i obowiązki oraz dokonywać przeglądu scenariuszy,
- stale monitorować bezpieczeństwo i działanie systemów i narzędzi, aby zminimalizować wpływ wszelkich zagrożeń teleinformatycznych,
- szybko wykrywać anomalie i identyfikować potencjalne punkty awarii,
- wdrożyć kompleksową politykę ciągłości działania ICT wraz z odpowiednimi planami, procedurami i mechanizmami ,
- opracowywać i udokumentować zasady tworzenia kopii zapasowych oraz procedury przywracania i odzyskiwania danych,
- rozmieszczać zasoby i personel w celu oceny słabych punktów i zagrożeń cybernetycznych, incydentów związanych z zagrożeniami cybernetycznymi, incydentów związanych z ICT, w szczególności cyberataków, oraz ich potencjalny wpływ na cyfrową odporność operacyjną podmiotu,
- opracowywać plany komunikacji kryzysowej w celu ujawniania co najmniej poważnych incydentów lub słabości związanych z ICT klientom, kontrahentom i opinii publicznej.

DORA powoduje też, co istotne z punktu widzenia dostarczania usług bankom, zarządzanie ryzykiem ICT ze strony osób trzecich. W związku z tym podmioty finansowe powinny:

- zarządzać ryzykiem stron trzecich jako integralnym elementem ich ogólnego ryzyka ICT,
- posiadać ustalenia umowne dotyczące usług ICT w celu prowadzenia działalności gospodarczej w pełnej zgodności z odpowiednimi przepisami,
- uwzględniać charakter, skalę, złożoność i znaczenie zależności związanych z ICT oraz wszelkie potencjalne zagrożenia,
- rozważyć korzyści i koszty alternatywnych rozwiązań przy identyfikacji i ocenie wszelkich związanych z tym ryzyk,
- uwzględniać w umowie prawa i obowiązki każdej ze stron oraz umowy o świadczenie usług.

Od podmiotu dostarczającego usługę zaufania wymaga się, aby spełniał wymogi w NIS2 i jej implementacji do systemu krajowego, czyli w przypadku Polski – nowelizacji UKSC. Kwalifikowani Dostawcy Usług Zaufania są w rozumieniu dyrektywy NIS2 podmiotami kluczowymi, a niekwalifikowani – ważnymi. W przypadku współpracy z bankiem, tj. bycia dostawcą usług ICT, będzie tego typu podmiot, co do zasady, podlegał pod DORA – z zastrzeżeniem, że niekoniecznie jako dostawca kluczowy.

Konsekwencje wprowadzenia w Rozporządzeniu Parlamentu Europejskiego i Rady (UE) 2024/1183 z dnia 11 kwietnia 2024 r. w sprawie zmiany rozporządzenie (UE) nr 910/2014 w odniesieniu do ustanowienia europejskich ram tożsamości cyfrowej (tzw. eiDAS2) dokumentu 3.0 dla umów bankowych – rekomendacje dla banków i instytucji finansowych



Jesteśmy świadkami istotnych zmian w zakresie technologii wykorzystywanych nie tylko przez banki i instytucje finansowe, ale także przez wiele innych nowoczesnych podmiotów. W ostatnich trzech latach Unia Europejska podjęła szereg działań legislacyjnych w zakresie uregulowania rynku cyfrowego w UE, tworząc podwaliny pod nowoczesną Europę cyfrową. Jego podstawą jest oparcie się o dane, a w konsekwencji, w ujęciu przedmiotu raportu, jest danatyzacja dokumentu i stworzenie podwalin prawnych pod dokument 3.0.

Rozporządzenie eIDAS2 wprowadza szereg zmian i nowych narzędzi prawno-technicznych powiązanych z nowymi domniemaniami prawnymi, istotnymi z punktu widzenia interesów banków i mającymi na celu realizację Polityki UE Cyfrowa Dekada 2030, która ma spowodować istotne zwiększenie kompetencji cyfrowych zarówno konsumentów banków, jak i przedsiębiorców (w tym MŚP, którzy stanowią istotną grupę klientów banków). A także zwiększyć dostępność usług online, a co za tym idzie spowodować zwiększenie zainteresowania usługami online banków i instytucji finansowych.

Rozporządzenie eIDAS wprowadza szereg nowych narzędzi pozwalających w większym zakresie, także w zakresie umów, opierać się o dokument 3.0. W chwili obecnej większość umów, głównie ze względów dowodowych, zawieranych jest w postaci dokumentu 1.0 lub 2.0.

W naszej ocenie w pierwszym okresie funkcjonowania eIDAS2 i uruchamiania nowych narzędzi sytuacja ta nie ulegnie diametralnej zmianie. Po pierwsze ze względów bezpieczeństwa procesowego, ale także ze względu na konieczność akceptacji czy też zainteresowania nowymi narzędziami rynku – w tym konsumentów. Z drugiej strony obserwując zainteresowanie aplikacją mObywatel (w ciągu 3 lat ponad 10 mln zainstalowanych aplikacji) można wnioskować, iż europejski portfel tożsamości cyfrowej upowszechni się w bardzo szybkim czasie.

Pomimo, iż nie nałożono na banki obowiązku stania się stroną ufającą w znaczeniu rozporządzenia eIDAS trudno, aby nowoczesne instytucje finansowe nie wdrożyły i akceptowały narzędzi, jakie daje nowelizacja rozporządzenia. Czas przygotowania banków i instytucji pod nową regulację nie jest odległy, dlatego poniżej przedstawiamy syntetycznie rekomendacje i kalendarz wdrożeń dla banków.

Rekomendacje dla banków

1. Analiza narzędzi eIDAS pod kontem potrzeb i celów banku, a co za tym idzie analiza procesów związanych z umowami w aspekcie nowej regulacji. Analiza ryzyka na osi czasu. W naszej ocenie nowe narzędzia, w szczególności kwalifikowane usługi zaufane, przenoszą sporą odpowiedzialność banku na kwalifikowane podmioty zaufane. Niemniej powodują też, że dostawcy usług zaufanych tym samym podlegają pod DORA (o ile świadczą usługi dla podmiotów finansowych – w przeciwnym razie ograniczają się do zgodności z NIS2/UKSC).

2. Przepisy eIDAS2 oraz nowe narzędzia nie zastępują dotychczasowych metod weryfikowania i uwierzytelniania tożsamości cyfrowej czy to osób fizycznych, czy też prawnych a także atrybutów. Są dodatkowymi metodami współistniejącymi z dotychczasowymi. Konieczne jest więc utrzymanie dotychczasowych procedur dotyczących weryfikowania i uwierzytelniania tożsamości klientów banków oraz instytucji finansowych oraz innych dokumentów stanowiących atrybuty. W takiej sytuacji jednak zmienić należy działanie mObywatela. Zmiany powinny objąć sposób przechowywania i przekazywania danych, zgodnie z referencyjną wersją europejskiego portfela. Udostępnione repozytoria znajdują się na https://github.com/eu-digital-identity-wallet. Tak korowana jest *European Digital Identity Architecture and Reference Framework*, dokument obejmujący architekturę techniczną, zestaw wspólnych norm i specyfikacji oraz wytycznych i najlepszych praktyk (dalej dokument ARF).

3. Rekomendujemy, aby banki przeanalizowały, ale też wykorzystały możliwości, jakie im daje możliwość stania się stroną ufającą w znaczeniu eIDAS2. Naszym zdaniem to, jak szybko EU Wallet stanie się podstawowym narzędziem dla zawierania umów, w dużej mierze zależy od tego, czy banki włączą się w środowisko europejskiego portfela tożsamości cyfrowej.

4. EU Wallet naszym zdaniem, ale co istotniejsze – zdaniem Komisji Europejskiej – będzie podstawowym jednolitym narzędziem uwierzytelniania tożsamości w szybkim czasie wypierając zainteresowanie takimi narzędziami, jak mObywatel czy Profil Zaufany w Polsce oraz inne unijne notyfikowane środki komunikacji elektronicznej (szerzej na temat tych narzędzi Raport WIB SYGN. PAB/WIB 9/2024 Tożsamość cyfrowa. Regulacje europejskie).

5. Ryzykiem dla polskiego rynku bankowego jest, w przypadku sukcesu EU Wallet w skali europejskiej, w braku jego wdrożenia przez polskie instytucje finansowe, przesunięcie młodej, nowoczesnej klienteli do zagranicznych instytucji finansowych oferujących nowoczesne usługi online. EU Wallet i silne uwierzytelnienie tożsamości zasadniczo zmieni sytuację w zakresie łatwości zawierania umów z zagranicznymi bankami i instytucjami finansowymi online. Z drugiej strony ułatwi pozyskiwanie klientów zagranicznych dla nowoczesnych usług.

6. Rekomendujemy intensywne włączenie się w prace i uzgodnienia ZBP w zakresie interfejsów i protokołów umożliwiającą zdalną i automatyczną identyfikację i uwierzytelnienie tożsamości oraz atrybutów z EU Wallet. Przepisy wykonawcze, wykaz norm referencyjnych oraz specyfikacje i rekomendacje zostały w trybie roboczym opublikowane już w chwili obecnej. Komisja Europejska jest zobligowana do ich wydania do 21 listopada 2024 r.

7. Rekomendujemy analizę systemów bankowych, procesów dla uwzględnienia tożsamości cyfrowej z EU Wallet i możliwości pobierania atrybutów jako dokumentu 2.0.

8. Od 21 maja 2027 EU Wallet i uwierzytelnienie tożsamości cyfrowej powinno być akceptowane przez banki jako silne uwierzytelnienie.

9. W związku z darmowym kwalifikowanym podpisem elektronicznym w EU Wallet dla osób fizycznych rekomendujemy analizę szerszego jego wykorzystania (w związku z jego upowszechnieniem) obok aktualnych procedur zawierania umów bankowych opartych o art. 7 prawa bankowego.

10. Rekomendujemy przy audytach bezpieczeństwa (NIS2, DORA) i analizie ryzyka, weryfikację potencjalnych korzyści z narzędzi eIDAS2 i kwalifikowanych usług zaufanych w aspekcie cyberbezpieczeństwa i ryzyka banku.

11. Rekomendujemy analizę sytemu banku pod kontem wdrożenia dokumentu 3.0 w tym akceptacji atrybutów, kwalifikowanych atrybutów wydawanych przez podmioty publiczne odpowiedzialne za źródło.

12. Rekomendujemy szersze wykorzystanie przez banki i instytucje finansowe kwalifikowanej usługi archiwizacji elektronicznej powiązanej z domniemaniem integralności i pochodzenia zapisanych w kwalifikowanym archiwum elektronicznym danych.

13. Rekomendujemy, w przypadku wdrożenia przez bank tokenizacji procesów, oparcie dokumentu 3.0 o zapis danych w kwalifikowanym rejestrze elektronicznym dla ułatwienia dowodu z sekwencji zdarzeń.

14. Rekomendujemy wykorzystywanie procesów tokenizacyjncyh w taki sposób, aby wykorzystywać różne DLT i rozwiązania zbliżone zgodnie z ich najlepszymi możliwościami, mieszając różne techniki, w zależności od modelu biznesowego.

15. Konieczne jest jak najszybsze zakończenie prac nad dokumentem ARF, który jest elementem krytycznym w znaczeniu dostępu do dobrej jakości dokumentacji technicznej. Znaczące wyprzedzenie dokończenia dokumentu ARF przed momentem integracji pozwoli bankom przygotować się na zmiany.

16. Postulujemy też realizację potrzeby sektorowej, w postaci zmapowania prac z Ministerstwem Cyfryzacji i ustalenia priorytetów wdrożeń kolejnych funkcjonalności.

Kalendarium wdrożenia eIDAS2

11 kwietnia 2024 r. – uchwalenie Rozporządzenia Parlamentu Europejskiego i Rady 2024/1183 w sprawie zmiany rozporządzenia (UE) nr 910/2014 w odniesieniu do europejskich ram tożsamości Dz.U. L 2024/1183 z 30 kwietnia 2024 r.

20 maja 2024 r. – wejście w życie rozporządzenia eIDAS2.

21 listopada 2024 r. – Komisja Europejska sporządzi wykaz norm referencyjnych oraz specyfikacje i procedury odnośnie interfejsów i protokołów EU Wallet i ich wdrożenia

21 listopada 2024 r. – Komisja Europejska sporządzi wykaz norm referencyjnych, specyfikacje i procedury dotyczące rejestracji użytkowników w EU Wallet za pomocą środków identyfikacji elektronicznej zgodnych z wysokim poziomem bezpieczeństwa albo środków identyfikacji średniego poziomu bezpieczeństwa w połączeniu z dodatkowymi procedurami zdalnej rejestracji, które łącznie spełnią wymogi wysokiego poziomu bezpieczeństwa.

21 listopada 2024 r. – Komisja Europejska ustanowi specyfikacje techniczne i procedury dla rejestracji stron ufających

21 listopada 2024 r. – Komisja Europejska ustanowi wykaz norm referencyjnych oraz specyfikacje i procedury dla certyfikacji europejskich portfeli tożsamości

21 listopada 2024 r. – Komisja Europejska ustanowi normy referencyjne, specyfikacje i procedury w zakresie bezpieczeństwa portfeli tożsamości cyfrowej

21 listopada 2024 r. – Komisja Europejska ustanowi normy referencyjne, specyfikacje i procedury dotyczące kwalifikowanych elektronicznych atrybutów oraz atrybutów wydawanych przez podmioty publiczne odpowiedzialne za źródło

21 maja 2025 r. – Komisja Europejska ustanowi normy referencyjne, specyfikacje i procedury dotyczące kwalifikowanych usług archiwizacji elektronicznej

21 maja 2025 r. – Komisja Europejska ustanowi normy referencyjne, specyfikacje i procedury dotyczące kwalifikowanych rejestrów elektronicznych

21 listopada 2026 r. – konieczność wydawania przez państwa członkowskie atrybutów określonych w załączniku nr VI eIDAS2

21 listopada 2027 r. – strony ufające, które świadczą usługi i zobowiązane na podstawie prawa UE lub krajowego do stosowania silnego uwierzytelnienia (a więc banki oraz instytucje finansowe) do celów identyfikacji elektronicznej na dobrowolny i wyłączny wniosek użytkownika EU Wallet, akceptują europejskie portfele tożsamości cyfrowej.

Raport przygotowany na zlecenie Fundacji
Warszawski Instytut Bankowości

PROGRAM
ANALITYCZNO
BADAWCZY