



OBSERWATORIUM . BIZ

ISBN 978-83-954468-0-1

BIZNES BEZ PAPIERU

Komercjalizacja eID i usług zaufania w Polsce i Europie

RAPORT SPECJALNY

patron główny



EFPE

partner naukowy



partner społeczny



partner



partner



patron honorowy



MINISTERSTWO
PRZEDSIĘBIORCZOŚCI
I TECHNOLOGII



Drodzy Państwo!

Jako autorzy Raportu „BIZNES BEZ PAPIERU — Komerccjalizacja eID i usług zaufania w Polsce i Europie” wyrażamy swoje podziękowanie wszystkim Instytucjom i Osobom, które przyczyniły się do stworzenia tego dokumentu. Stanowi on stanowią już naszą trzecią w okresie dwóch lat publikację poświęconą temu ważnemu obszarowi gospodarki cyfrowej.

W pierwszym rzędzie dziękujemy Europejskiemu Forum Podpisu Elektronicznego, które pełni rolę Patrona Głównego Raportu, Patronom Honorowym, czyli Ministerstwu Cyfryzacji oraz Ministerstwu Przedsiębiorczości i Technologii, Partnerom Raportu – Asseco Data Systems SA oraz Krajowej Izbie Rozliczeniowej SA, jak również Patronowi Honorowemu – Polskiej Izbie Informatyki i Telekomunikacji oraz Patronowi Społecznemu – Fundacji Polska 5.0.

Dziękujemy przedstawicielom instytucji komercyjnych, aktywnie działających na rynku gospodarki cyfrowej, przedstawicielom administracji publicznej oraz niezależnym ekspertom rynkowym, którzy zgodzili się wesprzeć nasz projekt swoimi cennymi wypowiedziami i opiniami, które umieściliśmy w Raporcie.

Mamy nadzieję, że Raport przybliży Państwu specyfikę i stan bieżący polskiego rynku elektronicznej identyfikacji (eID) oraz usług zaufania, w szczególności na tle głównych trendów rynku europejskiego. Efektywne wdrożenie takich rozwiązań jak podpis elektroniczny w chmurze, pieczęć elektroniczna, elektroniczne doręczenie może doprowadzić do prawdziwego przełomu na rynku usług on-line i w połączeniu z tworzącym się w Polsce rynkiem elektronicznej identyfikacji, stanowić o kolejnym kroku w bezpiecznej i efektywnej cyfryzacji relacji między obywatelami, konsumentami, przedsiębiorcami, podmiotami gospodarczymi oraz administracją publiczną w naszym kraju.

Zapraszamy do lektury!

Obserwatorium.biz Sp. z o.o.





GŁÓWNE WNIOSKI RAPORTU - W PYTANIACH I ODPOWIEDZIACH

CO DAJE NAM ROZWÓJ I UPOWSZECHNIENIE ELEKTRONICZNEJ IDENTYFIKACJI (eID) I USŁUG ZAUFANIA?

Zawieranie umów – nawet tych najprostszych i związane z nimi płatności to podstawowe elementy krwioobiegu gospodarki. Cyfryzacja polskiej gospodarki w tych zakresach przebiega nierównomiernie. Płatności elektroniczne, realizowane przy pomocy kart, aplikacji czy smartfonów są już powszechne. Aby zawrzeć umowę, cały czas konieczna jest wizyta w placówce danej instytucji, co jest czasochłonne i nie przystaje do wymagań współczesności. Elektroniczne narzędzia eID i usługi zaufania adresują potrzeby zamykając poważną lukę w cyfryzacji polskiej gospodarki i społeczeństwa.

CO POKAZUJE NAM MAPA POLSKICH USŁUG eID I ZAUFANIA?

Mapa wskazuje na kilku dojrzałych dostawców usług zaufania – głównie podpisu elektronicznego, często oferujących usługi kwalifikowane. Jednocześnie coraz więcej podmiotów buduje systemy elektronicznej identyfikacji, często integrując kilku (np. bankowych) dostawców tożsamości. Pojawiają się również dostawcy pojedynczych usług zaufania jak walidacja podpisu czy e-delivery, którzy mają ambicje wdrażania usług kwalifikowanych. Integratorzy starają się budować szerszy zakres usług, wystawiając do ostatecznego usługodawcy cyfrowego, rozwiązanie ergonomiczne i wystandaryzowane – tak jak robią to integratorzy płatności wobec sklepów internetowych.

CO WIDZIMY PATRZĄC NA EUROPEJSKI RYNEK eID I USŁUG ZAUFANIA?

Widzimy rynek, który bardzo mocno się rozwija – blisko 200 podmiotów świadczy usługi kwalifikowane, notyfikowano już 17 schematów identyfikacji elektronicznej. Działające rozporządzenie eIDAS zapewnia standaryzację oraz transgraniczność budowanych rozwiązań. Z perspektywy Polski będziemy musieli otworzyć się na ekspansję zagranicznych narzędzi, które będą dostosowywane do naszego rynku, ale również nie uciekać od promocji naszych rozwiązań, czy wręcz budowy platform, które będą integrowane z dostawcami tożsamości (np. bankami) oraz usługodawcami cyfrowymi z innych krajów UE. Widzimy również dążenie do standaryzacji nowych narzędzi jak np. wideo weryfikacja przy on-boardingu do usług zaufania.



CO BĘDZIE KLUCZOWE DLA SUKCESU eID I USŁUG ZAUFANIA W PERSPEKTYWIE ROKU 2020

NARZĘDZIA:

- budowa rozwiązań odpowiadającym oczekiwaniom dzisiejszego klienta końcowego:
 - schemat identyfikacji oparty na funkcjonującej już tożsamości cyfrowej (np. bankowej lub pochodzącej od państwa) wykorzystywany jako wystarczający w procesach np. onboardingu lub potwierdzenia cech klienta (np. wieku);
 - kwalifikowany podpis elektroniczny dostępny on-line (wydawany np. na bazie wideo weryfikacji lub eID);
 - elektroniczne doręczenie jako alternatywa do listu polecanego, dostępne po wygodnym onboardingu np. na bazie eID;
 - walidacja podpisów elektronicznych dostępna do zintegrowania „plug&play” przez każdego usługodawcę cyfrowego.

USŁUGODAWCA CYFROWY I UŻYTKOWNIK:

- usługodawca (np. operator telekomunikacyjny wystawiający umowę do podpisu dla klienta elektronicznie) musi otrzymać skonfigurowany dla niego proces bazujący na eID i usługach zaufania – może to otrzymać od dostawcy lub integratora usług, edukacja usługodawcy, również od strony prawnej i bezpieczeństwa to „clue” sukcesu budowy szerokiej „sieci akceptacji” dla usług zaufania;
- końcowy użytkownik, nie musi rozumieć zawiłości eID i usług zaufania – przejdzie po-myślnie proces gdy zaufa marce usługodawcy (np. operatora telekomunikacyjnego), z którym podpisuje umowę on-line, a sam proces np. podpisu będzie nie mniej wygodny niż płatność elektroniczna w sklepie internetowym;

RYNEK I REGULATOR:

- budowa wspólnej przestrzeni dla wypracowywania nowych narzędzi i sposobów zastosowania eID i usług zaufania: wideo weryfikacji jako narzędzia onboardingu do usług zaufania, wykorzystania aplikacji mObywatel oraz e-dowodu do zastosowań komercyjnych, budowy publicznych i komercyjnych elektronicznych doręczeń;
- ścisła współpraca dostawców usług zaufania i integratorów tych usług z usługodawcami cyfrowymi, co pozwoli zrozumieć ich potrzeby i rozwijać tak usługi aby dostosowały się do oczekiwań ich oraz końcowych użytkowników - klientów indywidualnych i przedsiębiorców.



SPIS TREŚCI

WSTĘP	7
Rozdział 1 – MAPA eID i USŁUG ZAUFANIA W POLSCE	8
1.1 Wprowadzenie	8
1.2 Identyfikacja elektroniczna (eID)	10
1.3 Usługa podpisu elektronicznego	11
1.4 Usługa pieczęci elektronicznej	15
1.5 Usługa walidacji podpisów i pieczęci elektronicznych	16
1.6 Usługa znakowania czasem	17
1.7 Usługa uwierzytelniania witryn internetowych	18
1.6 Inne dodatkowe usługi niekwalifikowane	19
Rozdział 2 - PERSPEKTYWA EUROPEJSKA	22
2.1 Lokalny a międzynarodowy rynek usług	22
2.2 Notyfikowane schematy identyfikacji	23
2.3 Administracja publiczna w krajach UE oraz regulator na poziomie KE jako motor rozwojowy usług	24
2.4 Jednolitość rynku europejskiego	25
2.5 Kierunki zmian normalizacyjnych i certyfikacyjnych	27
Rozdział 3 – POTENCJAŁ KOMERCJALIZACJI eID ORAZ USŁUG ZAUFANIA	29
3.1 Wprowadzenie	29
3.2 eID jako podstawa sukcesu komercjalizacji usług cyfrowych	29
3.3 Potencjał komercjalizacji – warunki „higieniczne”	31
3.4 Potencjał komercjalizacji – wybrane obszary biznesowe	34
3.5 Komerccjalizacja eID i usług zaufania – wyniki badań	43
Rozdział 4 - SCENARIUSZE ROZWOJU RYNKU	48
4.1 Wprowadzenie	48
4.2 Rozwój narzędzi	48
4.3 Rozwój rynku usługobiorców i usługodawców (konsumentów, przedsiębiorców)	51
4.4 Rozwój rynkowy	52
Słownik pojęć	54
AUTORZY RAPORTU	57
PARTNERZY RAPORTU	58
Metodologia przygotowania raportu	59
Nota prawna	59

Mobilny Podpis Elektroniczny

 **SimplySign**
by **ASSECO**

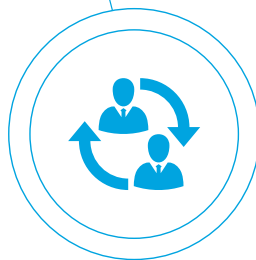


Uwolnij Moc Podpisu

Podpisuj co chcesz, kiedy chcesz,
bez ograniczeń!



Administracja



Biznes



Klienci

Dowiedz się więcej simplysign.pl Infolinia 801 540 340

ASSECO
DATA SYSTEMS



WSTĘP

Raport „BIZNES BEZ PAPIERU — Komerccjalizacja eID i usług zaufania w Polsce i Europie” jest kolejnym przygotowanym przez Obserwatorium.biz, szeroko dostępnym raportem rynkowym, który dotyczy obszarów elektronicznej identyfikacji oraz usług zaufania. Wcześniej, w roku 2017, przygotowane zostały dedykowane raporty „Raport eID – elektroniczna identyfikacja w Polsce” oraz „Przełom w usługach on-line – rozwój usług zaufania w Polsce”. Oba dokumenty stanowiły swoiste bazowe kompendium wiedzy o tym budującym się rynku, tłumaczyły podstawowe pojęcia, wskazywały pierwsze zastosowania w Polsce, przedstawiały perspektywę międzynarodową. Raporty unaoczniały, że eID oraz usługi zaufania mogą być pomocne zarówno w administracji publicznej, dla której zdalna identyfikacja obywatela i przedsiębiorcy była (i jest) bramą do skutecznego dostarczania e-usług przez państwo, jak i w świecie komercyjnym, który potrzebuje efektywnych procesów zdalnej akwizycji klientów, czy wiążącego pozyskania podpisu klienta pod umową w transakcji realizowanej zdalnie.

Wdrożone rok wcześniej przed publikacją raportów Rozporządzenie eIDAS, znalazło swój wyraz zarówno w uporządkowaniu tej sfery w polskim prawodawstwie (poprzez wdrożenie ustawy o usługach zaufania w 2016 roku, a następnie jej nowelizacji i rozszerzeniu nazewnictwa o elektroniczną identyfikację w roku 2018), jak i w większym zainteresowaniu tym rynkiem ze strony dostawców rozwiązań, podmiotów oferujących usługi cyfrowe oraz samych odbiorców końcowych, a w szczególności przedsiębiorców. Dlatego w bieżącym raporcie postanowiliśmy skupić się przede wszystkim na praktycznym zastosowaniu usług. W pierwszym rozdziale przedstawiona jest mapa polskich dostawców eID i usług zaufania – pozwala ona zorientować się jakie podmioty grają jakie role na tym rynku – kto jest, lub chce być dostawcą usług, usługobiorcą czy integratorem – co ciekawe niektóre podmioty, jak na przykład banki, mogą uczestniczyć w kilku rolach jednocześnie.

W kolejnym rozdziale wskazujemy na rozwój środowiska regulacyjnego oraz pokazujemy jak rozwijają się regulacje oraz sam rynek w tym zakresie w Europie. To ważne, nie tylko ze względu na możliwość inspiracji stosowanymi tam rozwiązaniami, ale również dlatego, że po pierwsze kreowane na poziomie międzynarodowym normy szczegółowe (np. kwalifikowanych usług doręczenia czy onboardingu video do usług zaufania) bezpośrednio wpływają na normy i kształt produktów na naszym rynku, a po drugie: gracze zagraniczni coraz odważniej wchodzą na polski rynek tych usług. W rozdziale trzecim przedstawiony został potencjał komercjalizacji wybranych sektorów rynku – unoacznia on chociaż wstępnie to, w jakich sektorach rynku komercyjnego (finansowego, HR, energetycznego i telekomunikacyjnego i innych) usługi zaufania będą mogły być skutecznie użyte i określa szacunkowo wartość tego rynku.

W ostatnim rozdziale przedstawione są warianty rozwoju rynku oraz scharakteryzowano główne główne kwestie i problemy, z którymi rynek i jego uczestnicy muszą się zmierzyć, aby w pełni skorzystać z potencjału eID i usług zaufania do realizacji procesów udanej transformacji cyfrowej gospodarki w Polsce.



Rozdział 1 –

MAPA eID i USŁUG ZAUFIANIA W POLSCE

1.1 Wprowadzenie

Istnieje duże grono dostawców rozwiązań z zakresu elektronicznej identyfikacji (eID) oraz dostawców usług zaufania, zarówno polskich, jak i zagranicznych, którzy oferują swoje produkty, starając się przekonać rynek, że to właśnie one są w stanie w sposób bezpieczny i wygodny zabezpieczyć rosnący wolumen wszelkiego rodzaju transakcji elektronicznych. Usługi te są przeznaczone zarówno dla obywateli, przedsiębiorców, jak i administracji publicznej, a ich podstawową korzyścią jest eliminacja „papierowych” procesów, przyspieszenie ich realizacji, jak również większa transparentność dla wszystkich uczestników rynku.

Ambicją tego raportu jest przedstawienie mapy eID i usług zaufania w Polsce według stanu na połowę roku 2019. W ocenie autorów raportu, ekosystem rodzimego rynku można podzielić na 5 głównych grup:

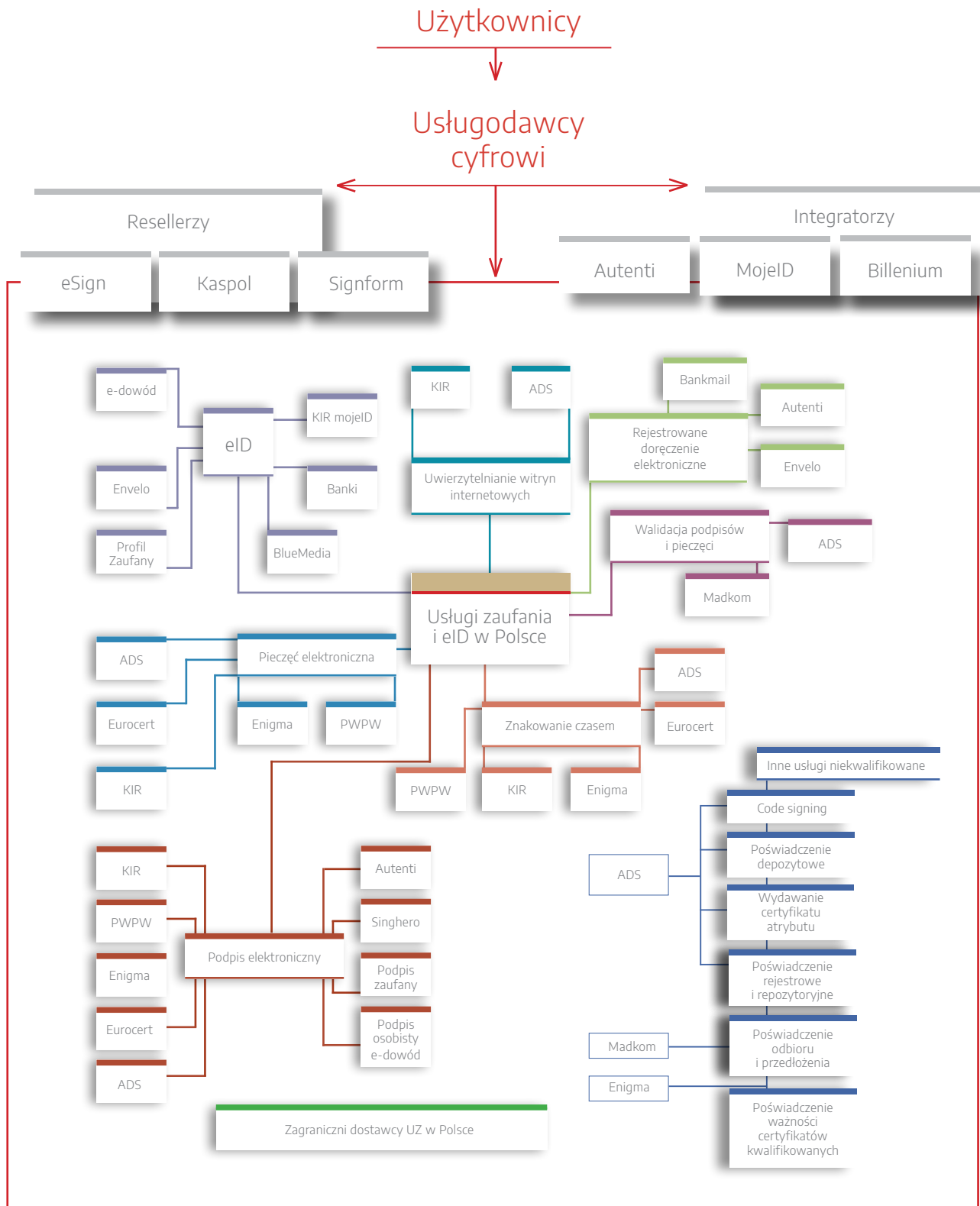
- krajowi i zagraniczni dostawcy usług zaufania i elektronicznej identyfikacji (eID);
- resellerzy usług zaufania i elektronicznej identyfikacji (eID);
- integratorzy usług zaufania i elektronicznej identyfikacji (eID);
- usługodawcy usług cyfrowych implementujący w swoich procesach powyższe rozwiązania;
- końcowi użytkownicy – w rolach indywidualnych lub przedsiębiorcy, będący ostatecznymi beneficjentami powyższych rozwiązań.

Należy wskazać, że na rynku dostępne są zarówno usługi kwalifikowane dostarczane przez kwalifikowanych dostawców (w pełni zgodne z rozporządzeniem eIDAS), jak i niekwalifikowane. Użycie danej usługi w wariantach kwalifikowanym bądź niekwalifikowanym jest zdeterminowane konkretnym przypadkiem użycia i zakresem obowiązujących regulacji prawnych, w których domenie znajduje się dany proces (czyli oprócz samej Ustawy o usługach zaufania i elektronicznej identyfikacji, również na przykład — odpowiednio — Prawo telekomunikacyjne czy po prostu Kodeks Cywilny).

Warunki funkcjonowania rynku eID i usług zaufania na jednolitym rynku cyfrowym Unii Europejskiej, określa Rozporządzenie eIDAS, które weszło w życie w lipcu 2016 r. Od tego czasu rynek rozwija się przy bardziej jednolitych i wystandardyzowanych zasadach, ale dynamiczny rozwój, połączony z szerokim komercyjnym wykorzystaniem swojego potencjału, ma jeszcze zdecydowanie przed sobą.



MAPA eID i USŁUG ZAUFANIA W POLSCE



Rozdział 1 –
MAPA eID i USŁUG ZAUFANIA

Wyjaśnienia skrótów:

ADS = Asseco Data Systems SA

KIR = Krajowa Izba Rozliczeniowa SA

PWPW = Polska Wytwórnia Papierów Wartościowych SA



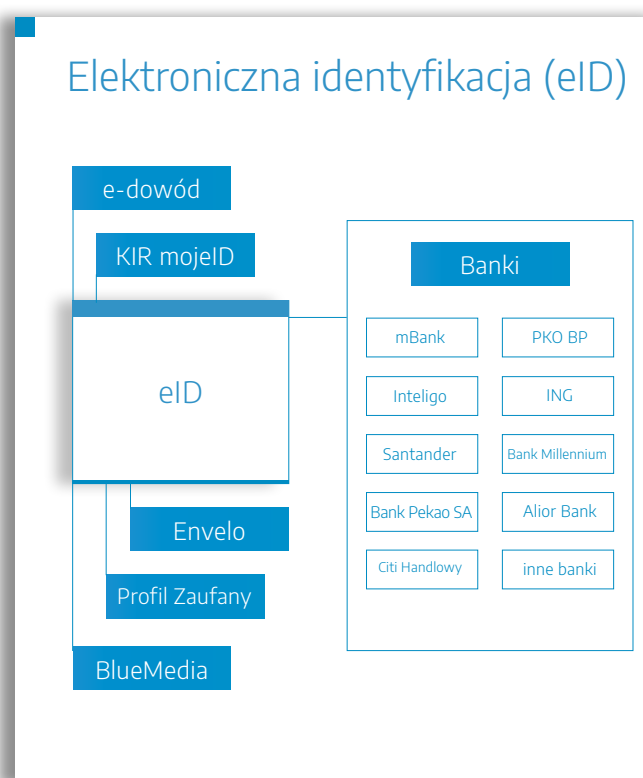
1.2 Identyfikacja elektroniczna (eID)

Usługi elektronicznej identyfikacji stanowią niezbędny warunek dla realizacji procesów transakcyjnych w świecie cyfrowym, w sposób bezpieczny dla obu stron. Coraz więcej spraw jako konsumenci czy obywatele możemy załatwić drogą elektroniczną. Występujemy wówczas jako konkretne osoby – „z imienia i nazwiska”. Dlatego podczas takiego procesu – założenia rachunku bankowego przez Internet, umówienia wizyty u lekarza przez aplikację mobilną czy złożenia deklaracji podatkowej – kluczowe dla obu stron transakcji jest, aby tożsamość składającego była rozpoznana w sposób właściwy, bezpieczny i ergonomiczny.

W Polsce występuje już wiele środków identyfikacji elektronicznej pozwalających na posługiwanie się elektroniczną tożsamością w Internecie, począwszy od najnowszego rozwiązania e-dowodu, przez Profil Zaufany, środki bankowe, po Envelo czy MojID KIR.

Rozwój systemu identyfikacji elektronicznej pozwala przenieść do cyfrowego świata procesy, które dotychczas wymagały od klienta osobistej wizyty w punkcie obsługi, urzędzie lub umawiania się z kurierem. Na przykład wdrażana przez Krajową Izbę Rozliczeniową (KIR) usługa mojID umożliwia użytkownikom zdalne potwierdzanie tożsamości w oparciu o dane pochodzące od zaufanych podmiotów określanych jako dostawcy tożsamości, np. banki. Wykorzystując mechanizmy uwierzytelniania w bankowości internetowej uzyskujemy zatem efekt „jednego okienka” – szybki, łatwy i bezpieczny dostęp do komercyjnych i publicznych usług on-line.

Jednak nie w każdym przypadku identyfikacja elektroniczna procesów online jest wystarczająca do zabezpieczenia transakcji online. Często dopiero połączenie obu elementów (eID + usługa zaufania) pozwala na pełną cyfryzację wszystkich procesów w świecie komercyjnym oraz administracji publicznej.





Potencjał identyfikacji elektronicznej

Cyfrowa tożsamość umożliwia rozwój nowoczesnych, zdalnych usług zaufania (np. podpis elektroniczny w chmurze), które wymagają zaadresowania kwestii kompleksowego mechanizmu zdalnego uwierzytelniania. Zgodnie z rozporządzeniem eIDAS rejestracja użytkownika w takiej usłudze może zostać zrealizowana w oparciu o identyfikację elektroniczną o poziomie wiarygodności średnim lub wysokim, o ile pierwotne potwierdzenie tożsamości było bezpośrednie. Dzięki wykorzystaniu mechanizmu identyfikacji elektronicznej użytkownik chcący korzystać z kwalifikowanej usługi nie musi osobiście stawić się w punkcie rejestracji, a całość usługi może zostać wykonana zdalnie. Także inne usługi zaufania, o ile wymagają inicjalnej rejestracji użytkownika, będą korzystały z mechanizmów identyfikacji elektronicznej.

1.3 Usługa podpisu elektronicznego

Bez wątplenia najlepiej znaną i rozumianą usługą zaufania jest podpis elektroniczny (w szczególności o statusie kwalifikowanym). Warto jednak wskazać, że obecnie na rynku występuje kilka rodzajów podpisu elektronicznego: kwalifikowany, zaawansowany oraz zwykły.



Od szeregu lat w prawie polskim, ale także w prawie europejskim, dopuszczalne jest zawieranie umów na odległość z wykorzystaniem środków komunikacji elektronicznej. W wielu przypadkach do tego celu wystarczające jest złożenie zwykłego podpisu elektronicznego, czyli niebędącego ani podpisem zaawansowanym, ani kwalifikowanym. Podpis elektroniczny „oznacza dane w postaci elektronicznej, które są dołączone lub logicznie powiązane z innymi danymi w postaci elektronicznej i które użyte są przez podpisującego jako podpis.” – eIDAS nie ogranicza technologii zapewniającej to dołączenie lub powiązanie.

Zaawansowany podpis elektroniczny technicznie nie różni się od kwalifikowanego podpisu elektronicznego. Kwalifikowany podpis elektroniczny jest zaawansowanym podpisem elektronicznym, jednak zasadniczą różnicą jest fakt, iż podpis jest złożony za pomocą kwalifikowanego



urządzenia do składania podpisu oraz jest weryfikowany kwalifikowanym certyfikatem. Kwalifikowany podpis elektroniczny ma w całej Unii Europejskiej skutek równoważny skutkowi podpisu własnoręcznego.

KWALIFIKOWANY PODPIS ELEKTRONICZNY = PODPIS WŁASNORECZNY -> UE

Podpis elektroniczny może być skutecznym dowodem w postępowaniach sądowych, nawet jeżeli nie jest to zaawansowany lub kwalifikowany podpis elektroniczny. W przypadku kwalifikowanych podpisów elektronicznych sąd jednak nie musi badać wiarygodności źródła takiego podpisu.

Usługi podpisu elektronicznego w Polsce i ich dostawcy



W zakresie podpisów kwalifikowanych na rynku dostępne są rozwiązania chmurowe (klucze przechowywane są przez kwalifikowany podmiot), a także rozwiązania tradycyjnych podpisów z czytnikami kart i kartami kryptograficznymi.

Podpis zaufany jest dedykowany dla posiadaczy profilu zaufanego do podpisywania podań i wniosków składanych do podmiotów publicznych.

Z kolei podpis elektroniczny, zwany podpisem osobistym, to rozwiązanie zaawansowanego podpisu elektronicznego. Użycie podpisu osobistego będzie wywoływało dla podmiotu publicznego w Polsce taki sam skutek, jak podpis własnoręczny. Z kolei dla podmiotu innego niż podmiot publiczny, taki sam skutek będzie osiągnięty, jeżeli obie strony wyrażą na to zgodę. W przypadku podpisów zwykłych, identyfikuje się dostawców platform www (Autenti, Signhero), którzy udostępniają serwisy www do składania podpisów oraz podglądu wartości dowodowej. Na podstawie danych agregowanych przez Ministerstwo Cyfryzacji, dostarczanych przez kwalifikowanych dostawców usług zaufania danych na początku maja bieżącego roku, w Polsce funkcjonowało blisko 565 tys. aktywnych certyfikatów kwalifikowanych.

Koncepcja podpisu w chmurze ma szansę zrewolucjonizować podejście do stosowania podpisu elektronicznego i upowszechnić tę usługę szczególnie wśród osób fizycznych. Przewagą podpisu w chmurze jest brak konieczności posiadania czytnika czy tokena oraz udostępnienie podpisu z wykorzystaniem zdalnej identyfikacji. Do kwalifikowanego e-podpisu w chmurze mogą być dodawane kolejne elementy, takie jak np. elektroniczny znacznik czasu.



Gdzie jest wykorzystywany podpis elektronicznie obligatoryjnie?

- podpisywanie sprawozdań finansowych przez przedsiębiorców
- raportowanie plików JPK VAT

Zastosowanie podpisu kwalifikowanego:

- składanie formularzy do KIO (Krajowej Izby Odwoławczej) (esp.uzp.gov.pl),
- składanie pism procesowych w sądowym postępowaniu upominawczym,
- kontakty drogą elektroniczną z Zakładem Ubezpieczeń Społecznych (ZUS), np.: podpisanie wniosku o wydanie zaświadczenia o niezaleganiu ze składkami na ubezpieczenie społeczne, podpisanie deklaracji,
- pozyskiwanie wypisów elektronicznych dotyczących wszystkich podmiotów gospodarczych wpisanych do Krajowego Rejestru Sądowego (KRS) (pdi.cors.gov.pl),
- podpisywanie urzędowej korespondencji z podmiotami administracji publicznej za pośrednictwem elektronicznej skrzynki podawczej,
- wystawianie faktur w formie elektronicznej,
- uczestniczenie w aukcjach i przetargach elektronicznych (np. www.e-przetarg.pl),
- podpisywanie raportów do Generalnego Inspektora Informacji Finansowej (GIIF),
- zgłaszanie drogą elektroniczną zbiorów danych osobowych do Generalnego Inspektora Ochrony Danych Osobowych (GIODO),
- składanie e-deklaracji do Ubezpieczeniowego Funduszu Gwarancyjnego (UFG),
- wszędzie tam, gdzie prawo wymaga formy pisemnej oświadczenia woli (np. umowy leasingu, umowy na kredyty konsumenckie, oświadczenia o przekazaniu praw autorskich).

Zastosowanie podpisu elektronicznego zwykłego:

- kontrakty z klientami
- umowy o dzieło, zlecenia
- wnioski pracownicze
- protokoły odbioru
- umowy najmu
- umowy o zachowaniu poufności



EKSPERT RAPORTU

Robert Trętowski
Wiceprezes Zarządu KIR

Popularność elektronicznego podpisu (kwalifikowanego i niekwalifikowanego) rośnie i będzie rosła wraz z pojawianiem się nowych możliwości jego zastosowania, jak i wprowadzaniem obowiązków posługiwania się nim przy określonych czynnościach. Wymóg składania sprawozdania finansowego w formie elektronicznej z kwalifikowanym podpisem to tylko najnowszy przykład.

Potencjał użycia e-podpisu w coraz większym stopniu dotyczy dziś nie tylko biznesu, lecz także użytkowników prywatnych. Jak pokazało badanie, przeprowadzone przez Kantar TNS dla Związku Banków Polskich i KIR, aż 74 proc. respondentów chciałoby podpisywać elektronicznie umowy na usługi telekomunikacyjne, 62 proc. – usługi bankowe, 57 proc. – usługi użyteczności publicznej, 51 proc. – usługi ubezpieczeniowe, zaś 50 proc. – usługi medyczne. W związku z tym widzimy bardzo duży potencjał w usłudze, nad którą pracujemy – mSzafir: kwalifikowany podpis elektroniczny wykorzystujący technologię chmurową.

Bezpieczne i wygodne potwierdzanie tożsamości jest dziś kwestią kluczową dla dalszego rozwoju usług cyfrowych – tak w sferze administracji publicznej, jak i po stronie komercyjnej. Jako podmiot zapewniający od wielu lat infrastrukturę umożliwiającą bezpieczną wymianę wrażliwych informacji drogą cyfrową, jesteśmy aktywnym uczestnikiem tego procesu, rozwijając produkty odpowiadające na zapotrzebowanie rynku. Takim przykładem jest mojeID, usługa umożliwiająca zdalne potwierdzanie tożsamości w Internecie z zachowaniem najwyższych standardów bezpieczeństwa.

Zarówno mSzafir, jak i mojeID to rozwiązania, których celem jest wspieranie procesów wdrażania rozwiązań cyfryzujących gospodarkę.



1.4 Usługa pieczęci elektronicznej

Kolejną usługą jest pieczęć elektroniczna, która jest wykorzystywana do pieczętowania dokumentów, danych oraz korespondencji elektronicznej. Pieczęć elektroniczna działa zasadniczo tak samo jak podpis elektroniczny, przy czym:

- Składającym pieczęć jest podmiot prawny, firma, urząd lub organizacja
- Pieczęć nie jest podpisem organizacji, czyli nie jest związana z reprezentacją i nie służy do składania oświadczeń woli w imieniu organizacji
- Potwierdza autentyczność dokumentu — dokument nią opatrzony został wystawiony przez daną organizację

Usługa dostarcza gwarancję integralności danych, identyfikuje podmiot, który jest autorem dokumentu oraz dodaje element niezaprzeczalności w świetle przepisów prawa. Dokumenty opieczętowane elektronicznie są bezpieczniejsze niż ich papierowe odpowiedniki, gdyż jakkolwiek ich zmiana jest natychmiast wykrywana.

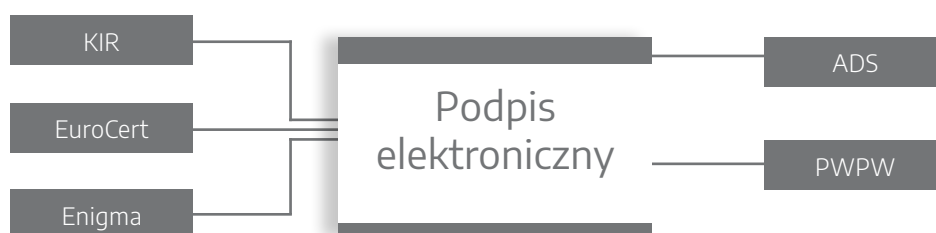
Na rynku są dostępne głównie pieczęci kwalifikowane (PWPW, ADS, Enigma, KIR, Eurocert), które zachowują pełną moc prawną i wartość dowodową w świetle przepisów prawa.

Analogicznie jak w przypadku usługi podpisu elektronicznego, na rynku dostępne są rozwiązania pieczęci w chmurze (online), jak również tradycyjne rozwiązania w oparciu o czytnik oraz kartę kryptograficzną.

Pieczęć elektroniczna pozwala na automatyzację procesów elektronicznych, w szczególności opatrywanie nią:

- Dokumentów bankowych i potwierdzeń zawarcia transakcji
- Faktur elektronicznych
- Automatycznych potwierdzeń zawarcia transakcji w usługach on-line
- Automatycznego wydawania zaświadczeń urzędowych
- Zabezpieczenia dokumentacji podpisanej w systemie teleinformatycznym – np. potwierdzenia skład złożonego za pomocą profilu zaufanego
- Wydawanie biletów elektronicznych, które mogą zostać zweryfikowane pod względem autentyczności przez każdego

Usługi pieczęci elektronicznej w Polsce i jej dostawcy





1.5 Usługa walidacji podpisów i pieczęci elektronicznych

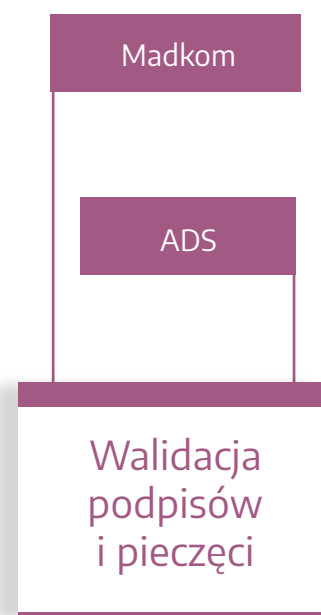
Walidacja oznacza proces weryfikacji i potwierdzenia ważności podpisu elektronicznego lub pieczęci.

Na polskim rynku istnieje obecnie jedna kwalifikowana usługa walidacji kwalifikowanych podpisów oraz pieczęci elektronicznych dostarczana przez firmę Asseco Data Systems. Dodatkowo, istnieje także dostawca usługi niekwalifikowanej (Madkom).

W przypadku usługi kwalifikowanej proces walidacji zakończony jest wydaniem poświadczenia zrealizowanej walidacji, które posiada wartość dowodową i może być wykorzystywane przy rozstrzyganiu sporów sądowych. Usługa walidacji zdejmuję obowiązek samodzielnej weryfikacji podpisu lub pieczęci i daje gwarancję, że została wykonana prawidłowo.

Wszędzie tam, gdzie ryzyko poprawnej weryfikacji może naruszyć bezpieczeństwo transakcji, np. przy wartościowych umowach na znaczące sumy, wieloletnich zobowiązaniach czy postępowaniach przetargowych w zamówieniach publicznych, wykorzystanie walidacji ma zasadnicze znaczenie i zapewnia bezpieczeństwo podmiotu akceptującego dokumenty podpisane lub podpczętowane.

Usługi walidacji podpisów i pieczęci elektronicznej w Polsce i jej dostawcy



Zastosowanie usługi walidacji:

- przyjmowanie oświadczeń i zobowiązań o podwyższonym ryzyku
- postępowania w zakresie zamówień publicznych
- zobowiązania długoterminowe lub wartościowe
- protokoły odbioru
- umowy najmu
- brak narzędzi do weryfikacji podpisu po stronie ufającej

Usługa walidacji może być dostarczana w różnych formach, w zależności od potrzeb klienta:

- Dostęp przez przeglądarkę www
- Dostęp przez integrację API
- Dostęp przed dedykowany serwer
- Walidacja przez skrzynkę e-mail



1.6 Usługa znakowania czasem

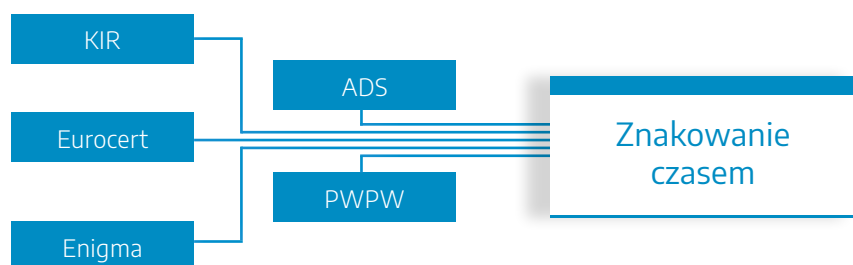
Na polskim rynku dostępne są zarówno usługi zarówno kwalifikowanego, jak i niekwalifikowanego znacznika czasu. Usługa jest przeznaczona dla wszystkich, którzy chcą uzyskać potwierdzenie istnienia e-dokumentu w czasie oznaczenia, a także dodatkowe zabezpieczenie momentu złożenia podpisu kwalifikowanego. W obu wariantach usługa dostarcza wiarygodne oznaczenie czasu przez zaufaną trzecią stronę.

Cechą wyróżniającą kwalifikowany znacznik czasu jest wywołanie skutków prawnych daty pewnej. Kwalifikowane znakowanie czasem jest realizowane tylko przez kwalifikowanego dostawcę usługi zaufania, a sąd uznaje dowody z kwalifikowanego znakowania czasem jako wiarygodne.

Wszędzie tam, gdzie wiarygodność czasu wykonania transakcji i powstania dokumentu ma zasadnicze znaczenie, tam wykorzystuje się znacznik czasu.

Obecnie na rynku jest kilku przedstawicieli kwalifikowanej usługi znakowania czasem (ADS, PWPW, Enigma, KIR, EuroCert).

Usługa znakowania czasem w Polsce i jej dostawcy



Zastosowanie znacznika czasu:

- zawieranie umów (bankowe, ubezpieczenia)
- faktury
- dokumentacja medyczna
- dokumentacja elektroniczna przepływająca wewnątrz firmy
- logi systemowe (IT)



1.7 Usługa uwierzytelniania witryn internetowych

Usługa uwierzytelniania witryn internetowych polega na wydawaniu przez zaufaną trzecią stronę certyfikatu, który umożliwia uwierzytelnianie witryn internetowych i przyporządkowuje witrynę internetową do osoby fizycznej lub prawnej, której wydano certyfikat. Usługa pozwala zestawiać szyfrowane połączenie SSL pomiędzy serwerami posiadającymi takie certyfikaty, a także udostępniać bezpieczne logowanie klientom.

W praktyce usługa działa tak samo, jak dzisiaj stosowane certyfikaty SSL. Kwalifikowany certyfikat uwierzytelnienia stron internetowych ustanawia prawne reguły dla potwierdzania wystawców takich stron.

Obecnie w Polsce jedynym dostawcą kwalifikowanej usługi uwierzytelniania witryn internetowych jest KIR. W przypadku usługi niekwalifikowanej jedynym dostawcą jest firma ADS.

Usługi uwierzytelniania witryn internetowych w Polsce i jej dostawcy

KIR

ADS

Uwierzytelnianie witryn internetowych

W ramach dyrektywy PSD2 dostawcy usług są zobowiązani do korzystania z kwalifikowanych certyfikatów uwierzytelniania stron internetowych – zarówno banki, jak i dostawcy usług płatniczych (TPP).



1.8 Usługa Rejestrowanego Doręczenia Elektronicznego

Usługa rejestrowanego doręczenia elektronicznego oznacza usługę umożliwiającą przesłanie danych między stronami trzecimi drogą elektroniczną i zapewniającą dowody związane z posługiwaniem się przesyłanymi danymi, w tym dowód wysłania i otrzymania danych, oraz chroniącą przesyłane dane przed ryzykiem utraty, kradzieży, uszkodzenia lub jakiegokolwiek nieupoważnionej zmiany.

W rejestrowanym doręczeniu dostawca usługi zaufania — świadczy ją na rzecz podmiotów trzecich, zapewnia identyfikację nadawcy dokumentu, identyfikację odbiorcy dokumentu, poufność i integralność dokumentu w procesie jego przekazywania, a także dowody nadania i doręczenia.

Obecnie na polskim rynku brak jest dostawców kwalifikowanej usługi Rejestrowanego Doręczenia Elektronicznego. W toku prac legislacyjnych i organizacyjnych toczy się projekt e-Doręczenia, który może przynieść wymierne korzyści w celu elektronicznej usług doręczeń.

Istnieją jednak dostawcy usługi Rejestrowanego Doręczenia Elektronicznego. Na ten moment identyfikuje się następujące platformy, które umożliwiają przekazywanie przesyłek elektronicznych, które wystawiają dowody nadania i odebrania, a także identyfikują nadawców i odbiorców:

| Envelo | Autenti | Bankmail

EKSPERT RAPORTU

Adam Ptasiwicz
Ekspert ds. e-Usług
Pion Sprzedaży Poczta Polska S.A.

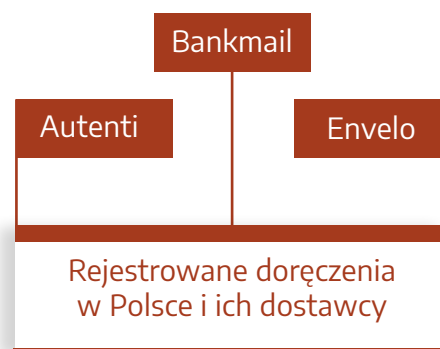
Niezbędnym elementem rozwoju usług zaufania jest ich powszechna dostępność oraz przyjęte regulacje prawne.

W Polsce wprowadzono kluczowe zmiany wraz z przyjęciem ustawy o usługach zaufania (...); aktualnie czekamy na ustawę o elektronicznej doręczeń. Jest ona szczególnie istotna ze względu na upowszechnienie i udostępnienie wszystkim obywatelom elektronicznej formy dokumentów. Do zwiększenia dynamiki rozwoju komercyjnych, jak i publicznych usług zaufania niezbędne są trzy czynniki:

- dostępność usług jako możliwość i łatwość korzystania w życiu codziennym
- edukacja jako przekonanie o bezpieczeństwie dokumentów przesyłanych elektronicznie
- interoperacyjność w zakresie współpracy różnych systemów oraz ich zdolność do wymiany danych i ich wykorzystania

Bez wątpienia nowa usługa publiczna będzie miała pozytywny wpływ na przybliżenie zalet usług zaufania w powszechnym zastosowaniu.

Usługi elektronicznego doręczenia w Polsce i ich dostawcy





1.9 Inne dodatkowe usługi niekwalifikowane

Rejestr niekwalifikowanych usług zaufania, a także dostawcy usług zaufania wskazują na istnienie oprócz powyżej omówionych bazowych usług zaufania — następujących usług zaufania, które umożliwiają zabezpieczanie danych i procesów:

- code signing (ADS)
- poświadczenie depozytowe (ADS)
- wydawanie certyfikatu atrybutu (ADS)
- poświadczenia rejestrowe i repozytoryjne (ADS)
- poświadczenia odbioru i przedłożenia (Madkom)
- poświadczenia ważności certyfikatów kwalifikowanych (Enigma)

EKSPERT RAPORTU

Mariusz Janczak
Kierownik Produktów
Pion Usług Bezpieczeństwa i Zaufania, Asseco Data Systems

Wdrożenie pełnej identyfikacji elektronicznej w procesach biznesowych i administracyjnych to technologiczny i procesowy skok w przyszłość. W Polsce taki system wciąż jest brakującym ogniwem transformacji w kierunku e-gospodarki, ale coraz więcej sygnałów z rynku pozwala nam sądzić, że wkrótce się to zmieni.

Elektroniczna identyfikacja osób fizycznych wraz z funkcjonalnością usług zaufania, szczególnie w postaci mobilnego podpisu cyfrowego, stanowią kluczowe instrumenty prawne pozwalające na realizację wszelkich procesów transakcyjnych w bezpiecznym świecie cyfrowym. To system, który radykalnie zmieni relacje usługodawców z klientami oraz usprawni procesy biznesowe.

Mobilny kwalifikowany e-podpis dostępny z poziomu aplikacji mobilnej na smartfona jest milowym krokiem stymulującym innowacyjność usług zaufania. Optymalizuje UX z perspektywy użytkowników końcowych, pozwalając tworzyć nowe usługi, produkty czy też modele biznesowe. Jest to podstawowy czynnik sukcesu wielu globalnych firm z sektora ICT. Upowszechnienie użycia tych narzędzi nie tylko przyspieszy rozwój biznesu, ale również znacząco usprawni ergonomię rozwiązań świadczonych przez administrację publiczną oraz dostawców usług komercyjnych m.in. z sektora finansowego, telekomunikacyjnego, ubezpieczeniowego czy medycznego.



myślimy cyfrowo

Opracowujemy oraz dostarczamy innowacyjne i niezawodne rozwiązania, odpowiadające wyzwaniom związanym z rozwojem technologii i zmianami prawnymi na poziomie krajowym i europejskim.

Wspomagamy sprawne funkcjonowanie sektora bankowego w Polsce, branży płatniczej, e-commerce i administracji publicznej. Wykorzystując doświadczenie i dojrzałość operacyjną, podejmujemy działania służące budowie nowoczesnej, cyfrowej gospodarki.



Rozdział 2 –

PERSPEKTYWA EUROPEJSKA

2.1 Lokalny a międzynarodowy rynek usług

Rynek europejski to 191 firm świadczących kwalifikowane usługi zaufania. Wszystkie kwalifikowane usługi świadczone w jednym z krajów UE powinny być rozpoznawane we wszystkich innych krajach UE. W szczególności podpisy i pieczęci elektroniczne oparte na kwalifikowanych certyfikatach wydanych przez kwalifikowane podmioty w innych krajach Unii Europejskiej muszą być rozpoznawane przez podmioty publiczne oraz podmioty świadczące usługi dla konsumentów. Takie konkurencyjne podejście obowiązkowego rozpoznawania certyfikatów kwalifikowanych z innych krajów ma być motorem rozwoju usług, a z danych zebranych z list zaufania, w ostatnich latach widać bardzo duży wzrost kwalifikowanych usług zaufania w krajach Europy Zachodniej.

Kwalifikowana usługa zaufania	Europa	Polska	Niemcy	Włochy	Hiszpania	Francja
Razem usługodawców	191	6	10	35	26	22
Wydawanie certyfikatów	167	6	8	35	23	14
Znakowanie czasem	92	5	5	14	14	9
Konserwacja	1				1	1
Rejestrowane doręczenie elektroniczne	11		2		3	4
Walidacja podpisów i pieczęci	13	1			2	1

Zestawienie kwalifikowanych usług zaufania w Europie - stan na maj 2019r.

W pierwszych dwóch latach obowiązywania rozporządzenia eIDAS głównymi usługami wpisywanymi na listy były usługi wydawania certyfikatów, natomiast w ostatnim roku zaczęły się pojawiać usługi nowe takie jak konserwacja i walidacja podpisów i pieczęci, oraz rejestrowane doręczenie elektroniczne.

Dostawcy usług zaufania podlegają obowiązkowym okresowym audytom w zakresie zgodności z rozporządzeniem eIDAS oraz są nadzorowane przez krajowe organy nadzoru. O ile poszczególne kraje nie mogą ograniczać dostępności zagranicznych kwalifikowanych usług zaufania, to mogą nakładać dodatkowe obowiązki na krajowe kwalifikowane usługi zaufania, lub wspierać np. zapewniając dostęp do krajowych rejestrów dokumentów tożsamości. O tym na ile krajowe prawo i organ nadzoru ogranicza lub wspiera kwalifikowanego dostawcę świadczy dostępność jego usług na rynkach zagranicznych, znaczącym przykładem jest opisana poniżej możliwość kwalifikowanych certyfikatów w oparciu o wideo weryfikację.



Rozporządzenie eIDAS pozwala na wydawanie certyfikatów kwalifikowanych w oparciu o potwierdzenie tożsamości w inny sposób niż bezpośrednio. Na podstawie tych przepisów kilkunastu dostawców kwalifikowanych usług zaufania wprowadziło mechanizm pozwalający na wydawanie certyfikatów na podstawie wideo weryfikacji, dzięki czemu wydanie certyfikatu kwalifikowanego nie wymaga spotkania z przedstawicielem centrum certyfikacji. Takie podejście nie tylko daje łatwość pozyskania certyfikatów kwalifikowanych, ale w rzeczywistości umożliwia świadczenie usług międzynarodowo.

Dodatkowym rozwiązaniem, które jeszcze nie jest oferowany na polskim rynku a dostępny u zewnętrznych kwalifikowanych dostawców usług jest kwalifikowany podpis jednorazowy. Certyfikat dla takiego podpisu jest wydawany na potrzeby pojedynczej transakcji lub grupy transakcji, nie wymaga pamiętania haseł i dodatkowych dostępów, nie wymaga także oferowania usługi unieważnienia certyfikatu. Takie podejście umożliwia znaczące uproszczenie w stosowaniu kwalifikowanego podpisu elektronicznego w usługach biznesowych, gdzie trzeba go zastosować do pojedynczej transakcji, a koszty wydania certyfikatu i jego użycia pokrywa usługodawca.

2.2 Notyfikowane schematy identyfikacji

Ważnym aspektem umiędzynarodowienia omawianych w tym raporcie usług jest umożliwienie wykorzystania środków identyfikacji elektronicznej pomiędzy krajami Unii Europejskiej. Państwa członkowskie są zobowiązane do uznawania w usługach online notyfikowanych środków identyfikacji elektronicznej, o ile spełniają one ustalony poziom wiarygodności (bezpieczeństwa). Notyfikacja oznacza wskazanie krajowego środka identyfikacji jako dostępnego w całej UE. Notyfikacja jest przeprowadzana na poziomie unijnym i poprzedzona jest zgłoszeniem do notyfikacji środka przez państwo członkowskie, które bierze odpowiedzialność za bezpieczeństwo tego środka identyfikacji. Na dzień publikacji niniejszego raportu opublikowano 17 schematów identyfikacji elektronicznej notyfikowanych i prenotyfikowanych - obejmujących różne środki identyfikacji. Najczęściej notyfikowanym środkiem jest karta identyfikacyjna (dowód tożsamości), niektóre kraje notyfikowały środki identyfikacji oparte o narzędzia mobilne. Ciekawostką jest notyfikowanie przez Włochy i Wielką Brytanię środków identyfikacji opartych o komercyjnych usługodawców.

Aktualnie Polska nie notyfikowała, ani nie zgłosiła do notyfikacji żadnego środka identyfikacji elektronicznej, natomiast oczekiwana jest notyfikacja profilu zaufanego na poziomie średnim oraz profilu osobistego (nowego dowodu osobistego z warstwą elektroniczną - tzw. e-dowodu) na poziomie wysokim.

Dostępność notyfikowanych środków identyfikacji elektronicznej będzie miał także duże znaczenie dla usług zaufania. Wydanie kwalifikowanego certyfikatu podpisu elektronicznego oraz realizacja kwalifikowanego rejestrowanego doręczenia może być oparta o środki identyfikacji elektronicznej o określonym bezpieczeństwie na poziomie średnim (*substantial*), a notyfikacja jest rzeczywistym potwierdzeniem jakości środka identyfikacji i jego prawnemu potwierdzeniu przez organ nadzoru w kraju, w którym jest prowadzona usługa.



Kraj	Środki identyfikacji	Poziom	Status	Data
Portugalia	Klucz mobilny	High	PEER REVIEWED	10. 2018
Słowacja	Karta identyfikacyjna Karta pobytu		PRE-NOTIFIED	04. 2019
Portugalia	System uprawnień profesjonalistów		PRE-NOTIFIED	05. 2018
Belgia	Aplikacja mobilna itsme®		PRE-NOTIFIED	04. 2019
Portugalia	Karta identyfikacyjna	High	NOTIFIED	02. 2019
Niemcy	Karta identyfikacyjna Karta pobytu	High	NOTIFIED	09.2017
Estonia	Karty identyfikacyjne Narzędzia mobilne	High	NOTIFIED	11. 2018
Włochy	Karta identyfikacyjna	High	PRE-NOTIFIED	11. 2018
Litwa	Karta identyfikacyjna		PRE-NOTIFIED	02.2019
Holandia	Środki identyfikacji przeznaczone dla biznesu		PRE-NOTIFIED	12. 2018
Czechy	Karta identyfikacyjna		PRE-NOTIFIED	12. 2018
Hiszpania	Karta identyfikacyjna	High	NOTIFIED	11. 2018
Chorwacja	Karta identyfikacyjna	High	NOTIFIED	11. 2018
Belgia	Karta identyfikacyjna Karta pobytu	High	NOTIFIED	12. 2018
Wielka Brytania	Środki identyfikacji elektronicznej zarządzane przez 5 firm i weryfikowane przez GOV.UK	Low, Substantial	NOTIFIED	05. 2019
Luksemburg	Karta identyfikacyjna	High	NOTIFIED	11. 2018
Włochy	Środki identyfikacji elektronicznej zarządzane przez 8 firm prywatnych	Low, Substantial, High	NOTIFIED	09. 2018

Zestawienie statusu notyfikacji schematów identyfikacji elektronicznej w Europie - stan na maj 2019r.

2.3 Administracja publiczna w krajach UE oraz regulator na poziomie KE jako motor rozwojowy usług

Podmioty realizujące zadania publiczne (*rynek usług publicznych*) są zobowiązane do rozpoznawania kwalifikowanych i zaawansowanych podpisów opartych o kwalifikowany certyfikat we wszystkich usługach online. Obowiązek ten dotyczy podpisów opartych o certyfikat kwalifikowany wydany w dowolnym państwie Unii Europejskiej, o ile same podpisy zostały utworzone w formatach referencyjnych.

Wiele dokumentów, nawet tych biznesowych jest tworzonych po to, aby w efekcie były one dowodami w sprawach urzędowych lub sądowych. To właśnie rozpoznawanie tych dokumentów przez administrację publiczną stanowi pierwszy krok do pełnego wykorzystania narzędzi elektronicznych przez biznes i osoby fizyczne. Z tego powodu rozporządzenie eIDAS skupiło się na usługach zaufania, które z założenia są komercyjnie dostępnymi rozwiązaniami podlegającymi normalnym prawom rynku, także z tego powodu państwa członkowskie nie powinny wprowadzać narzędzi i rozwiązań własnych, które naruszają konkurencyjność.



Swoboda przepływu usług zaufania na poziomie europejskim jest ogromną szansą rozwojową, ale też stanowi bardzo duży problem technologiczny w szczególności dla podmiotów publicznych w zakresie rozpoznawania certyfikatów kwalifikowanych. W tym zakresie podstawę stanowią listy usług zaufania, obejmujące wszystkie aktywne kwalifikowane usługi zaufania i publikowane przez poszczególne państwa. Listy usług zaufania za sprawą Komisji Europejskiej są dostępne z jednego miejsca – w postaci listy list. Listy te pozwalają w sposób automatyczny zweryfikować, czy kwalifikowany certyfikat jest wydany przez kwalifikowanego dostawcę usługi zaufania.

Komisja Europejska uruchomiła także program finansowania rozwiązań wspierających interoperacyjność podpisu elektronicznego. W postaci kodu dostępnego publicznie udostępnione zostały biblioteki pozwalające na weryfikację kwalifikowanych podpisów i pieczęci elektronicznych w dowolnych formatach ETSI.

2.4 Jednolitość rynku europejskiego

Celem rozporządzenia eIDAS jest osiągnięcie jednolitego rynku europejskiego rozumianego jako wzajemne rozpoznawanie podpisów i pieczęci elektronicznych opartych o certyfikaty kwalifikowane wydane w dowolnym kraju Unii Europejskiej. Aktualnie powszechnie dostępne są mechanizmy pozwalające na weryfikowanie takich podpisów kwalifikowanych. Natomiast nadal ogromne znaczenie mają dostawcy lokalni (krajowi), którzy wydają certyfikaty po rejestracji odbywającej się w sposób bezpośredni (wizyta u przedstawiciela centrum certyfikacji). Coraz więcej centrów certyfikacji udostępnia usługę wydania certyfikatu kwalifikowanego na podstawie identyfikacji zdalnej (wideo identyfikacji).

Rozporządzenie poza usługami związanymi z podpisami i pieczęciami elektronicznymi wyróżnia usługę rejestrowanego doręczenia elektronicznego. Usługa ta mimo oczywistej przydatności w relacjach pomiędzy administracją, biznesem i osobami fizycznymi jest rozwijana tylko krajowo w poszczególnych krajach Unii i nie jest stosowana szerzej. Dostępne kwalifikowane usługi rejestrowanego doręczenia elektronicznego są świadczone przez dostawców tylko w 5 krajach, a ich zasięg w rzeczywistości jest ograniczony do przekazywania dokumentów krajowo. Powodem tak wolnego rozwoju usługi doręczania jest brak obowiązku akceptacji przesyłek w ten sposób przychodzących przez podmioty publiczne, a także fakt, że normy techniczne określające warunki funkcjonowania tych usług zostały przez komitet normalizacyjny przyjęte dopiero na przełomie 2018 i 2019 roku. Ustalenie jednolitych zasad akceptacji kwalifikowanego elektronicznego doręczenia głównie przez podmioty publiczne oraz podmioty świadczące usługi konsumentom będzie motorem rozwoju tej usługi w całej Unii.



Poniżej przedstawiono tabelę porównawczą różnych rozwiązań podpisu elektronicznego - szczególnie istotnym jest cecha rozpoznawalności, która odpowiada kwestii zapewnienia jednolitości na rynku europejskim

Cecha	Kwalifikowany Podpis Elektroniczny	Osobisty Podpis Elektroniczny	Zaufany Podpis Elektroniczny
Wiarygodność	Podpis kwalifikowany	Podpis zaawansowany	Podpis zwykły
Rozpoznawalność	Paneuropejska	Polska	Polska
Weryfikowalność	Automatyczna np. Adobe czy usługach walidacji	Ręczna - wymaga konfiguracji	Ręczna - wymaga konfiguracji
Zastosowanie	Administracja Biznes	Administracja Opcjonalnie biznes	Administracja
Podpisujący	Obywatel Urzędnik	Obywatel	Obywatel
Podpis zdalny	Opcjonalnie	Nie - tylko karta	Tak
Równoważność formie pisemnej (forma elektroniczna)	TAK	NIE	NIE
Sposób rejestracji	Stacjonarny/zdalny	Stacjonarny	Stacjonarny/zdalny



2.5 Kierunki zmian normalizacyjnych i certyfikacyjnych

Aktualnie istnieją normy techniczne dla każdego obszaru usług zaufania. Zarówno wydawanie certyfikatów, składanie podpisów i znaczników czasu, a także pozostałe usługi zaufania zostały dobrze opisane za pomocą norm technicznych. W ostatnim roku opracowano i opublikowano normy dla podpisów zdalnych oraz dla rejestrowanego doręczenia elektronicznego.

Usługi	Normy
Dla dostawców usług	ETSI EN 319 401 General policy requirements for trust service providers
Wydawanie certyfikatów	ETSI EN 319 411-1 Part 1: General Policy and security requirements for TSPs issuing public key certificates ETSI EN 319 411-2 Part 2: EU qualified certificates
Składanie podpisów	ETSI TR 119 100 Guidance on the use of standards for signatures creation and validation ETSI TS 119 101 Policy and security requirements for applications for signature creation and signature validation ETSI TS 119 102 Procedures for Creation and Validation of AdES <ul style="list-style-type: none">Part 1: Signature creation and validationPart 2: Signature Validation Report
Zdalne podpisy	ETSI TS 119 431-1 Policy and Security Requirements for TSP Service Components Operating a Remote QSCD / SCD ETSI TS 119 431-2 Policy and Security Requirements for TSP Service Components Supporting AdES Digital Signature Creation ETSI TS 119 432 Protocols for Remote Digital Signature Creation
Znakowanie czasem	ETSI EN 319 421: Policy and Security Requirements for Trust Service Providers issuing Time-Stamps ETSI EN 319 422: Time-stamping protocol and time-stamp token profiles
Konserwacja	ETSI TS 119 511 Policy and security requirements for trust service providers providing long-term preservation of digital signatures or general data using digital signature techniques (draft) ETSI TS 119 512 Protocols for trust service providers providing long-term data preservation services (draft)
Rejestrowane doręczenie elektroniczne	ETSI EN 319 522 Electronic Registered Delivery Services (ERDS) ETSI EN 319 532 Registered Electronic Mail (REM) Services ETSI EN 319 521 Policy and Security Requirements for Electronic Registered Delivery Service Providers ETSI EN 319 531 Policy and Security Requirements for Registered Electronic Mail Service Provider
Walidacja podpisów i pieczęci	ETSI TS 119 441 Policy requirements for TSP providing signature validation services ETSI TS 119 442 Protocol profiles for trust service providers providing AdES digital signature validation services
Listy zaufania	ETSI TS 119 612: Trusted lists



EKSPERT RAPORTU

Michał Tabor

Partner, Członek Zarządu Obserwatorium.biz

W ciągu ostatnich 3 lat rynek usług zaufania w UE urósł do ponad 190 firm świadczących kwalifikowane usługi zaufania rozpoznawane przez instytucje publiczne i sądy wszystkich krajów członkowskich. Aktualnie większość tych usług to wydawanie kwalifikowanych certyfikatów podpisów i pieczęci elektronicznych. W dalszym rozwoju rynku spodziewam się, że będą następowały dwa równoległe działania, po pierwsze pojawi się więcej usług kwalifikowanych innych niż wydawanie certyfikatów, w szczególności widzę ogromny potencjał w rozwoju elektronicznych doręczeń i usług walidacji podpisów elektronicznych. Po drugie coraz większe znaczenie będą mieli dostawcy usług zaufania operujący na wielu rynkach jednocześnie i oferujący szeroki zakres usług zaufania. Efektem będzie zwiększenie konkurencji na rynkach lokalnych, które dotychczas były podzielone pomiędzy krajowych dostawców usług zaufania, a konkurencja wymusi lepszą ofertę produktową i łatwiejszy dostęp do usług.

EKSPERT RAPORTU

prof. dr hab. Dariusz Szostek

Partner Kancelarii Szostek & Bar

Końcówka drugiej dekady XXI wieku, w gospodarce cyfrowej ale także gospodarce wykorzystującej nowe technologie, w krajach rozwiniętych, w coraz większym stopniu wykorzystuje rozwiązania chmurowe, oraz paperless. Już nie tylko obieg dokumentów następuje w postaci elektronicznej, ale w ramach procesów biznesowych następuje pełen odwrót od tradycyjnego obiegu dokumentów na rzecz obiegu informacji, i to w pełni w postaci cyfrowej. W coraz większym zakresie państwa (jak Estonia, Dubaj itd.) rezygnują z obiegu tradycyjnego danych, informacji a co za tym idzie także dokumentów, na rzecz pełnego obiegu cyfrowego, coraz częściej sięgając do rozwiązań technologicznych opartych o tokeny, smart contracts, DLT oraz blockchain. Tak zwana rewolucja cyfrowa 3.0 w pełni opiera się o cyfrowy obieg i zapis informacji. Nie bez znaczenia w UE mają także regulacje unijne wspierające, a czasami wręcz wymuszające w sposób pośredni lub bezpośredni obieg elektroniczny. Przykładem może być chociażby RODO, gdzie przy masowości umów, koszt tradycyjnego funkcjonowania w zakresie dokumentów, w związku z obowiązkami informacyjnymi, czy prawem do bycia zapomnianym faktycznie promuje i wymusza paperless. Regulacje prawne w ramach projektu Europa Cyfrowa 2020 w pełni umożliwiają takie działania.



Rozdział 3 –

POTENCJAŁ KOMERCJALIZACJI eID ORAZ USŁUG ZAUFANIA

3.1 Wprowadzenie

W rozdziale poświęconym bieżącej sytuacji na rynku elektronicznej identyfikacji oraz usługom zaufania zostały już wstępnie wskazane ich bieżące obszary zastosowań – na przykład użycie kwalifikowanych podpisów elektronicznych w relacji z administracją publiczną. W tej części raportu spróbujemy się przyjrzeć przede wszystkim procesom biznesowym, w których aktualnie usługi eID oraz zaufania nie są wykorzystywane, lub są wykorzystywane

w ograniczonym zakresie. Niewątpliwe zalety eID i usług zaufania wynikające z ich wystandaryzowania, przejrzystej bazy prawnej, mocy wynikającej z ich dowodowego charakteru, restrykcyjnego procesu certyfikacji podmiotów kwalifikowanych, dają tytuł do tego aby znalazły one zastosowanie jako alternatywa do bieżących stosowanych rozwiązań cyfrowych lub wręcz były mocnym argumentem na rzecz strategicznej migracji danych procesów do kanałów elektronicznych (lub projektowaniu ich od razu z założeniem pełnej cyfryzacji „end-to-end”).

Usługi elektronicznej identyfikacji oraz zaufania mają przewagę nad innymi narzędziami wykorzystywanymi w budowie biznesowych procesów on-line – działają na bazie jednoznacznej wykładni prawnej i są wystandaryzowane pod względem spełniania wymogów bezpieczeństwa.

3.2 eID jako podstawa sukcesu komercjalizacji usług cyfrowych

Podobnie jak w poprzednich publikacjach (wydane w roku 2017 Raporty „Elektroniczna identyfikacja w Polsce” oraz „Przełom w usługach online – rozwój usług zaufania w Polsce”), autorzy stawiają tezę, że umasowienie narzędzi elektronicznej identyfikacji (eID) jest warunkiem niezbędnym do sukcesu komercjalizacji usług biznesowych z wykorzystaniem usług zaufania.

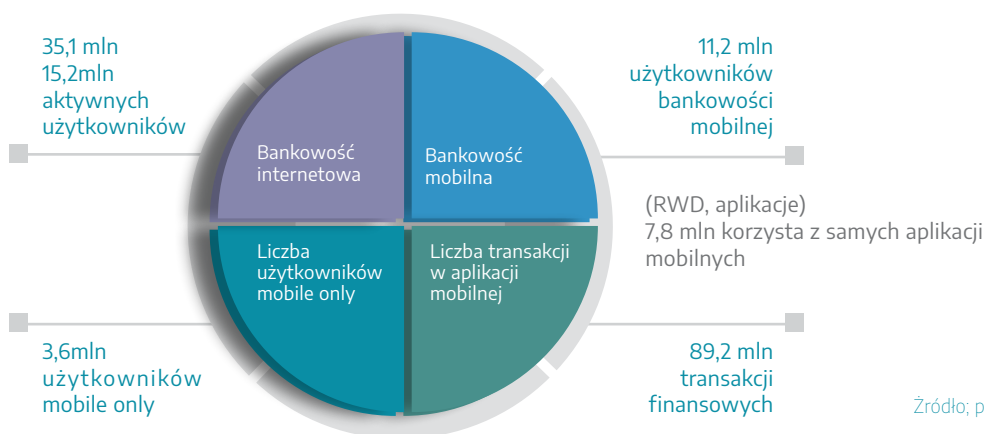
I ponownie wskazujemy na potencjał sektora bankowego, który posiada największą liczbę aktywnych użytkowników kanałów cyfrowych (ponad 15 mln. aktywnych klientów bankowości internetowej), którzy najpierw przeszli bezpieczną i zgodną z wymogami prawnymi identyfikację – najczęściej w kanale oddziałowym. Systematyczny kontakt z bankiem wyzwala również potrzebę odpowiedniej higieny cyfrowej to jest właściwego zarządzania dostępem do haseł i aplikacji przez użytkowników, które dzięki temu mogą służyć jako narzędzie dostępu do usług elektronicznych administracji rządowej – jakim jest Profil Zaufany czy mTożsamość do której

Upowszechnienie usług elektronicznej identyfikacji to podstawa sukcesu usług zaufania w Polsce.



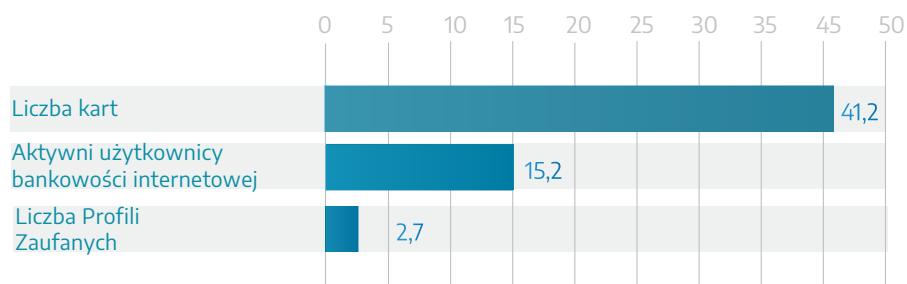
dostęp możliwy jest za pomocą aplikacji mObywatel. Warto zwrócić uwagę również na potencjał kart płatniczych, których powszechność oraz szeroka infrastruktura akceptacji, wskazuje, że również mogą być uznawane za jedno z docelowych nośników elektronicznej identyfikacji, również bazujących na bankach.

Liczba klientów elektronicznych kanałów dostępu do bankowości – kl. indywidualni”



Źródło: prnews.pl, Bankier.pl

Porównanie liczby Profili Zaufanych, liczby kart płatniczych i aktywnych użytkowników bankowości internetowej (w mln – 2018r.)



Ze względu na wczesny stan wdrożenia, wspomnianego już we wcześniejszym rozdziale, dowodu z warstwą elektroniczną (e-dowodu) oraz zakładany plan migracji, który będzie trwał do 10 lat, trudno określić potencjał wykorzystania tego narzędzia do procesów komercyjnych na tym etapie jego rozwoju.



3.3 Potencjał komercjalizacji – warunki higieniczne

Z perspektywy biznesowej usługi eID oraz usługi zaufania powinny stanowić swoistą „skrzynkę z narzędziami”, do której może sięgnąć menedżer czy decydet podejmujący wysiłki w celu budowy nowych procesów biznesowych czy też modyfikujący bieżące procesy – na przykład w celu ich optymalizacji czy cyfryzacji.

W naszej opinii aktualnie w naszym kraju istnieją poniższe, „higieniczne” warunki, niezbędne dla upowszechnienia elektronicznej identyfikacji (eID) oraz usług zaufania:

1. Świadomość eID oraz usług zaufania wśród usługodawców cyfrowych

2. Dostępność i ergonomia użycia eID oraz usług zaufania dla użytkowników

3. Stabilność i wsparcie środowiska regulacyjnego

4. Atrakcyjny model biznesowy użycia eID oraz usług zaufania

1. Świadomość eID oraz usług zaufania dla wśród usługodawców cyfrowych

Aktualnie firmy posiadają świadomość obecności różnego rodzaju narzędzi pozwalających na zdalną identyfikację klienta lub usługi zaufania (w tym zakresie przede wszystkim jedynie kwalifikowany podpis elektroniczny, który uważany jest generalnie i stereotypowo za narzędzie nieergonomiczne i drogie). Jednak podejmują próbę budowy tych procesów samodzielnie. Istotne jest więc, aby budować świadomość menedżerów opowiadających za transformację cyfrową swoich firm, czy obszar sprzedaży i transakcji elektronicznych („e-commerce”), żeby wiedzieli oni jak wbudowywać usługi zaufania w transformowane lub budowane od nowa procesy, aby zyskały one cechę cyfryzacji „end-to-end”.

IDEA – integrator eID oraz usług zaufania działający a’la integrator płatności.

Aktualnie gdy powstaje nowy sklep internetowy wdraża – niezbędne do efektywnego funkcjonowania na tym rynku – płatności elektroniczne. Aby nie budować własnego rozwiązania, co jest nieuzasadnione z przyczyn ekonomicznych, integruje się z jednym z dostępnych na rynku integratorów płatności. Jeżeli rynkowo „dorobimy się” takich analogicznych integratorów dla usług eID oraz zaufania, do których usługodawcy będą mogli się podłączyć praktycznie w modelu „plug&play” to dowód na upowszechnienie i sukces komercyjny tego typu usług.



2. Dostępność i ergonomia użycia eID oraz usług zaufania dla użytkowników

Dostępność w tym przypadku rozumiemy jako powszechność narzędzi, które są niezbędne użytkownikowi do realizacji procesów eID i usług zaufania. Jak wskazaliśmy wcześniej wierzymy, że kluczem do popularności usług zaufania będzie oparcie ich na elektronicznej identyfikacji, która z kolei może bazować na narzędziach ogólnie dostępnych jak dostęp do dowodu osobistego (z warstwą elektroniczną lub bez), bankowych kanałów elektronicznych, kart płatniczych czy nawet Profilu Zaufanego.

IDEA - elektroniczna identyfikacja oraz usługi zaufania powinny być proste w użyciu jak przelew przez internet typu „pay by link” („to co robi >>każdy<<”)

3. Stabilność i wsparcie środowiska regulacyjnego

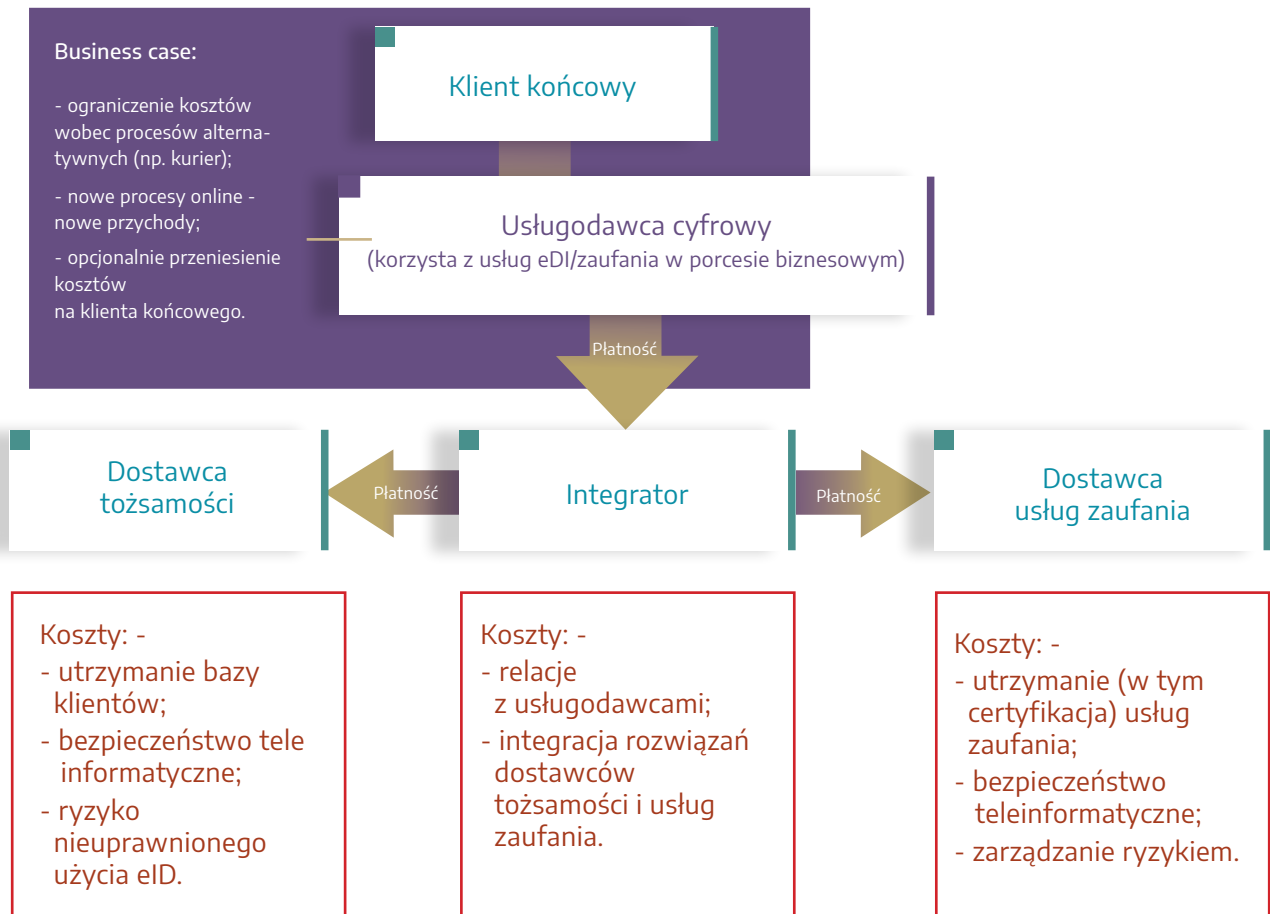
Dzięki przyjętej w UE formule przepisów dotyczących usług identyfikacji elektronicznej oraz usług zaufania bazującej na obowiązującym wszyskie kraje jednocześnie rozporządzeniu eIDAS zagwarantowano stabilność prawa. Na początek wspólne zobowiązania instytucji państwowych dotyczą akceptacji kwalifikowanych podpisów i pieczęci elektronicznych. Objęcie usług zaufania obowiązkiem notyfikacji prawa krajowego do pozostałych państw wspiera kontrolę nad lokalnymi rozwiązaniami, które naruszałby konkurencyjność rynku, choć cały czas obserwujemy w Polsce kolejne działania mające na celu ograniczenie konkurencyjności rynku i wprowadzenie krajowych rozwiązań - tak jak nadanie szczególnych praw podpisowi osobistemu w stosunkach krajowych.

4. Atrakcyjny model biznesowy użycia eID oraz usług zaufania

Wypracowanie odpowiedniego modelu biznesowego, który jest atrakcyjny dla wszystkich uczestników łańcucha transakcji jaką są usługi eID oraz usługi zaufania jest kluczowym warunkiem udanej komercjalizacji tego rynku. Brak wypracowania modelu i zrozumienia oczekiwań poszczególnych graczy może spowodować wieloletni paraliż rozwojowy rynku, nawet mimo gotowości prawnej, technologicznej i potencjalnemu korzystnemu przyjęciu przez klientów, którzy oczekują rozwiązań tego typu.



Docelowy model biznesowy usług eID i zaufania



W zarysowanym powyżej modelu biznesowym usług eID oraz zaufania, mamy znany z obszaru płatności schemat, w którym usługodawca płaci dostawcom eID i zaufania – poprzez integratora biznesowo-technologicznego (lub ewentualnie bezpośrednio), wynagrodzenie za użycie tych usług w swoich procesach biznesowych, które z kolei udostępnia swoim klientom końcowym (konsumentom czy przedsiębiorcom). Na potrzeby poniższych analiz przyjęliśmy że jednostkowa wartość „transakcji” wynosi 10 zł. jako suma wynagrodzenia płaconego integratorowi przez usługodawców w przypadku procesów wykorzystujących usługę eID i zaufania (np. użycie kwalifikowanego podpisu „w locie” na bazie identyfikacji elektronicznej pochodzącej z banku), w przypadku eDelivery kwotę ustalono na 1 zł. W obu przypadkach kwota wynika z możliwych referencji rynkowych tj. kosztów alternatywnych, które trzeba podjąć – przy wysłaniu kuriera identyfikującego klienta, z dokumentacją zwrotną, a w przypadku poczty – wysyłka listu poleconego priorytetowego z potwierdzeniem odbioru.

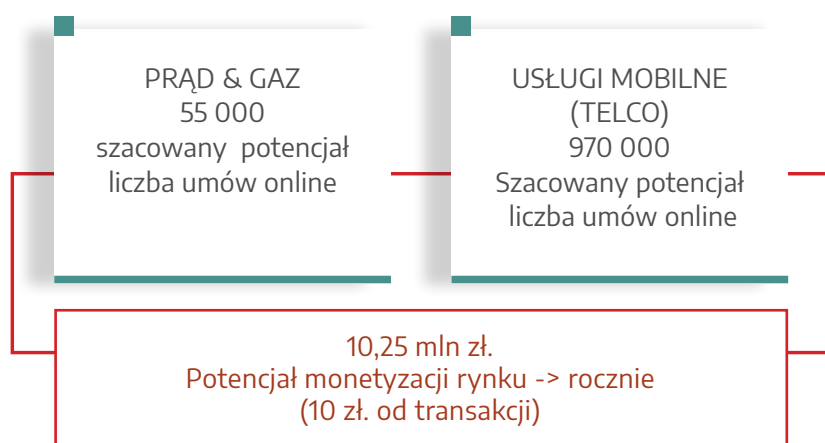


3.4 Potencjał komercjalizacji – wybrane obszary biznesowe

3.4.1 Zawierania umów / składanie oświadczeń woli

Flagowym przykładem możliwego wykorzystania eID do dalszej – zdalnej, obsługi podpisów i transakcji online są wszelkiego rodzaju umowy o korzystanie z usług, w szczególności usług / mediów dla domu lub małej firmy, gdzie jedną stroną jest konsument lub przedsiębiorca (najczęściej prowadzący własną działalność gospodarczą), a z drugiej dostawca tych usług – prądu, gazu, internetu i telefonu stacjonarnego czy operator telefonii komórkowej (ale można sobie wyobrazić, zawieranie w ten sposób również usług ochrony mienia czy ubezpieczeń majątkowych).

Potencjał rynku – operatorzy energii i gazu oraz usług mobilnych



Szacuje się, że w Polsce zmiany dostawcy prądu oraz gazu przez klientów indywidualnego oraz firmy (jednoosobowe działalności gospodarcze, MŚP) realizowanych jest 184 tysiące rocznie. Stosując współczynnik cyfryzacji wynoszący 30%, można przyjąć, że potencjał realizacji tych czynności w formule zdalnej, to jest gdzie identyfikacja oraz podpis realizowany jest drogą elektroniczną – poza siedzibą oddziału dostawcy czy jego agenta, wynosi 55 tys. sztuk rocznie. W przypadku umów o usługi telekomunikacyjne, szacunek zmian operatora wynosi 3,105 mln klientów indywidualnych oraz firmowych (jednoosobowe działalności gospodarcze, MŚP) rocznie (nie dotyczy odnawiania usług u tego samego operatora, której to czynności można często wykonać zdalnie, wykorzystując kanał telefoniczny lub nawet e-bok (mobilny lub internetowy), zapewniony przez dostawcę, więc potencjał biznesowy wykorzystania tutaj e-ID oraz usług zaufania, należy uznać za ograniczony). I ponownie stosując współczynnik rzędu 30%, kreuje się potencjał rzędu 970 tys. umów o mobilne usługi telekomunikacyjne, które mogą być uruchomione przez klientów poprzez wykorzystanie narzędzi eID i wystawionych na tej bazie usług zaufania (a konkretnie podpisu elektronicznego).



Potencjał dochodowy rynku, z uwzględnieniem wyjaśnionego powyżej „wskaźnika monetyzacji transakcji” wynosi zatem 10,25 mln zł. w skali roku.

W zakresie prawnym - oparcie o obowiązujące regulacje dotyczące elektronicznej identyfikacji – eIDAS oraz ustawę o usługach zaufania, oraz ustawy „domenowe” tj. prawo telekomunikacyjne, energetyczne. W przypadku sektora telekomunikacyjnego, w grudniu 2018 roku została wprowadzona ważna zmiana, umożliwiającą wykorzystanie formy dokumentowej i skuteczne zawarcie umowy, na bazie identyfikacji bankowej.

Można wskazać również potencjał wykorzystania eID w procesach podpisywania umów w kanałach tradycyjnych. W tym przypadku może udanie zacząć funkcjonować identyfikacja drogą elektroniczną, przy użyciu karty płatniczej wydanej przez polski bank, czy nowy dowód osobisty z warstwą elektroniczną (tzw. e-dowód). Proces ten może zmniejszać ryzyko użycia sfałszowanego dokumentu tożsamości oraz ułatwiać depapieryzację zawieranej umowy, na przykład z wykorzystaniem podpisu biometrycznego składanego na tablecie w miejscu sprzedaży lub poprzez autoryzację sms.

EKSPERT RAPORTU

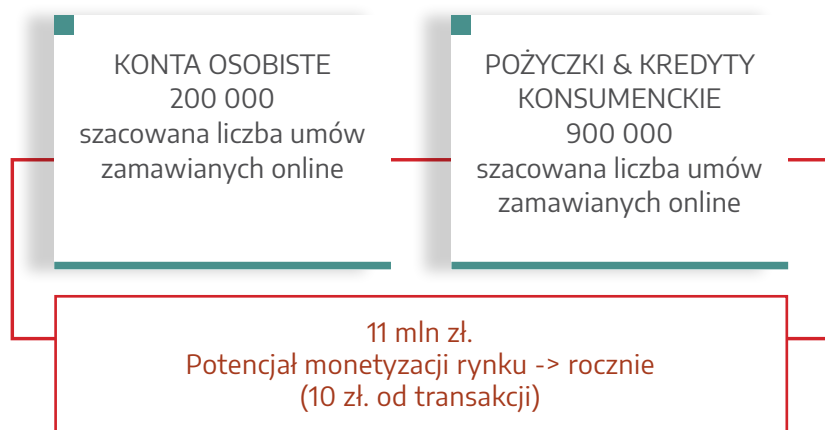
Dagmara Malinowska
General Manager, Rachuneo.pl

W Polsce nadal istnieją branże, które skutecznie opierają się cyfryzacji lub nie myślą o niej, jak o szansie na rozwój biznesu i redukcję kosztów działalności. Podczas projektowania porównywarki cen mediów dla domu - Rachuneo - przeprowadziliśmy kilkadziesiąt wywiadów i badań, z których jednoznacznie wynika, że klienci oczekują udogodnień znanych z innych branż. Jeśli można kupić online ubezpieczenie czy wycieczkę, otworzyć rachunek bankowy online, dlaczego nie można podpisać online umowy na dostawę prądu, gazu, TV i Internetu? Co znamienne, ta niechęć w przeważającej mierze dotyczy dużych państwowych podmiotów, choć chlubnym wyjątkiem jest tu PGE, której spółka - córka Lumi PGE właśnie udostępniła klientom możliwość podpisywania dokumentów podpisem elektronicznym. Prywatni sprzedawcy chętniej oferują klientom wygodę podpisywania umów online. W ten sposób redukują też koszty sprzedaży i obsługi umów. Cyfryzacja w tym obszarze jest więc rozwiązaniem, na którym wszyscy korzystają.

W Rachuneo naszą ambicją jest aby wszystkie procesy zawarcia umów z dostawcami mediów - energii, gazu, usług telekomunikacyjnych, były na naszej platformie realizowane cyfrowo. Jesteśmy w tym zakresie otwarci na współpracę z wszystkimi dostawcami tych usług jak i podmiotami wspierającymi budowę tych procesów - na przykład dostawcami eID i usług zaufania.



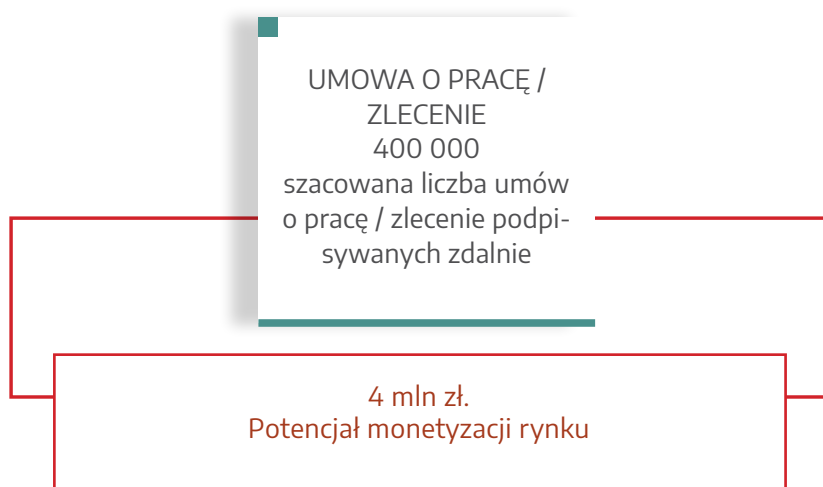
Potencjał rynku – usługi finansowe



Rynek usług finansowych jest jednym z tych rynków, który najszybciej przeszedł transformację cyfrową. Powtarzalne czynności jak wpłaty, wypłaty i przelewy realizowane są już w ponad 95% w kanałach zdalnych jak bankomaty czy systemy bankowości internetowej i mobilnej, poza oddziałami banków. Również sprzedaż produktów – depozytowych czy kredytowych i wynikające z niej podpisywanie umów między bankiem a konsumentem odbywa się w kanałach elektronicznych. Obszarem, w którym cały czas dominuje kanał tradycyjny jest tzw. onboarding, czyli pozyskiwanie nowego klienta, co najczęściej jest tożsame z założeniem konta osobistego, wraz z pakietem usług dodatkowych (płatniczych, dostępem do kanałów elektronicznych etc.). Szacujemy, że ok. 200 tys. kont osobistych jest zakładanych aktualnie w formule zdalnej – przede wszystkim z użyciem narzędzi typu „przelew autoryzacyjny”, wideo weryfikacji czy standardowym podpisie umowy przy kurierze dostarczającym dokumentację klientowi. Jest to więc miejsce do wykorzystania bezpieczniejszych i zestandaryzowanych usług eID oraz podpisu elektronicznego – pod warunkiem, że będzie to proces nie odstający od strony ergonomii od bieżących rozwiązań. Drugim obszarem, ilościowo znacznie większym są pożyczki gotówkowe. W ostatniej dekadzie stawały się coraz bardziej popularne, stanowiąc również coraz istotniejszą alternatywę dla banków, które z pewnym opóźnieniem wdrażały rozwiązania pozwalające na sprzedaż kredytów gotówkowych czy kart kredytowych w czystej formule „na klik”. Szacujemy, że nawet 900 tys. umów rocznie jest otwieranych w kanałach elektronicznych (strony internetowe, aplikacje mobilne). Zbiorczo, uwzględniając określony powyżej współczynnik monetyzacji, ten segment rynku elektronicznej identyfikacji i usług zaufania, może być warty nawet 11 mln zł. Innymi obszarami biznesowymi, które mogłyby wykorzystać określony wyżej mechanizm byłby również procesy onboardingowe dla firm (np. zakładania rachunków bieżących) oraz mechanizm, byłoby onboardingowe dla podmiotów typu fundusze inwestycyjne (pierwsze nabycie jednostek w funduszu z uwzględnieniem ankiety MIFID), firmy ubezpieczeniowe (np. nabycie ubezpieczeń na życie), czy platformy FX/Trade.

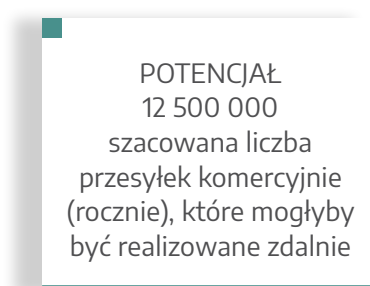


3.4.2 Zawieranie umów o pracę



Kolejnym obszarem, w którym mogą znaleźć zastosowanie usługi eID oraz usługi zaufania jest podpisywanie umów o pracę i zlecenie. Znowelizowane od stycznia 2019 wprowadziło więcej przestrzeni na cyfryzację dokumentacji pracowniczej. Szacujemy, że ok. 400 tys. umów tego typu jest podpisywanych zdalnie, co daje potencjał monetyzacji rynku eID oraz usług zaufania w tym zakresie na poziomie ok. 4 mln zł.

3.4.3 Elektroniczne doręczenia (e-delivery)



Rozwój publicznego procesu elektronicznych doręczeń, zapowiadany min. przez Ministerstwo Cyfryzacji, ma szansę otworzyć rynek również dla e-doręczeń komercyjnych, głównie w obszarze korespondencji komercyjnej (B2B), w której potwierdzenie otrzymania korespondencji jest istotne ze względu na konsekwencje wynikające z konkretnych umów między podmiotami życia gospodarczego. Wdrożenie rozwiązań o charakterze usług kwalifikowanych – czyli „elektronicznego listu poleconego z potwierdzeniem nadania i odbioru” usprawniłoby i przyspieszyłoby szereg procesów gospodarczych. Rozwiązanie te mogłyby być dostarczane przez komercyjnych dostawców kwalifikowanych usług zaufania, w oparciu o obowiązujące regulacje dotyczące elektronicznej identyfikacji i elektronicznego doręczenia – eIDAS oraz ustawę o usługach zaufania, jednocześnie pogłębiona analiza dla poszczególnych domen gospodarki mogłaby wskazywać na konieczność wprowadzenia odpowiednich zmian w KPA.



3.4.4 Wariant wykorzystania eID – potwierdzanie wybranych danych

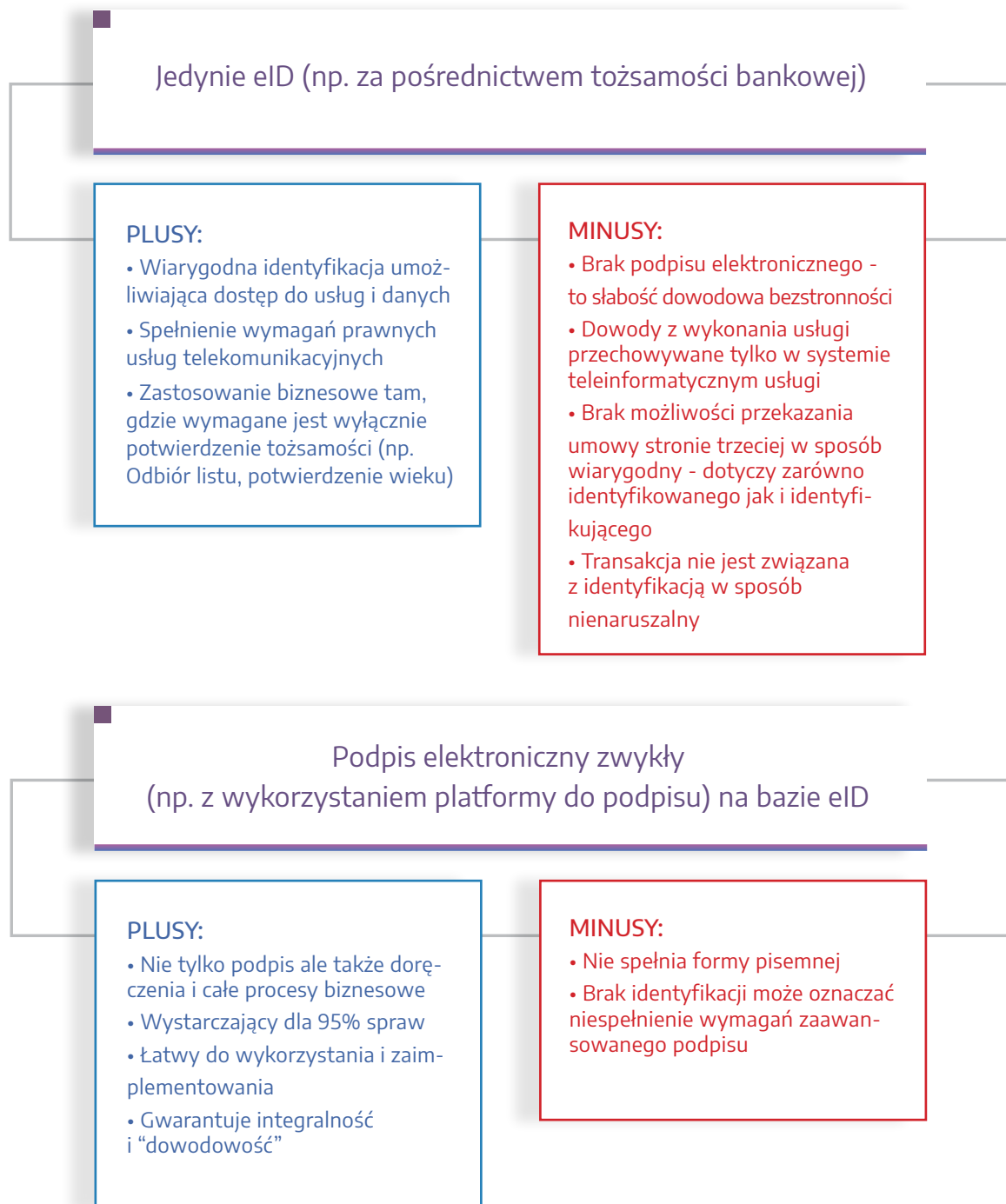
Narzędzia eID mogą również być przydatne w procesach, gdzie regulacje prawne lub sam charakter biznesowy usługi wymagają potwierdzenia przez zewnętrzny, zaufany podmiot wybranych cech klienta. Potwierdzenie pełnoletności jest jednym z tych możliwych scenariuszy użycia – dostępne narzędzie eID – wykorzystywane czy to on-line czy to w środowisku fizycznym może pomóc w potwierdzeniu wieku przy zakupie alkoholu, wizyt w punkcie bukmacherskim czy klubach, które chcą ograniczyć dostęp do swoich usług osobom niepełnoletnim. Również eID może stać się pożądaną optymalizacją w wybranych procesach e-handlu czy odbioru przesyłek (np. w tzw. paczkomatach), aby dodatkowo potwierdzić odbiór przesyłki przez uprawnioną do tego osobę (tzw. „elektroniczne doręczenie do rąk własnych”). Zyskująca cały czas na znaczeniu ochrona danych klientów (*RODO*) i idąca za nią świadomość tych ostatnich o swoich prawnych, również może udanie wspierać wykorzystanie usług eID, gdyż można wyobrazić sobie procesy, w których usługodawca – np. wypożyczalnia sprzętu narciarskiego – uzyskuje za pośrednictwem narzędzia typu karta płatnicza, identyfikacyjna czy e-dowód potwierdzenie tożsamości danego klienta – bez zbędnego przetwarzania danych u siebie i realizacji niepożądanych praktyk w postaci kserowania dokumentów tożsamości. Innym przykładem są Pracownicze Programy Kapitałowe, w których proces onboardingu rejestracji zarówno decydentów w firmach przystępujących do programu w poszczególnych instytucjach obsługujących programy jak i wśród klientów finalnych – pracowników, może być zbudowany w sposób wykorzystujący efektywność i bezpieczeństwo prawne eID i usług zaufania.



3.4.5 Wybór narzędzi eID oraz usług zaufania do wykorzystania w poszczególnych procesach komercyjnych

Poniżej wskazano na mocne (plusy) i słabe (minusy) strony wykorzystania różnych kompozycji elektronicznej identyfikacji (eID) i usług zaufania. Zestawienie te zostały wykonane w założeniu, że wykorzystanie poszczególnych narzędzi jest realizowane na potrzeby transakcji biznesowej, w ramach której powstaje zobowiązanie strony zidentyfikowanej lub potwierdzenie wykonanych przez nią czynności.

MOŻLIWE SCENARIUSZE ZASTOSOWANIA USŁUG eID ORAZ USŁUG ZAUFANIA:





Podpis elektroniczny kwalifikowany (np. „w locie”) na bazie eID

PLUSY:

- Równoważność formie pisemnej
- Rozpoznawalne jednakowo w całej UE
- Jednoznaczny dowód w postępowaniach sądowych
- Łatwość implementacji dla osób posługujących się identyfikacją
- Dostępność w przeglądarkach i systemach online, a także za pomocą aplikacji mobilnych
- Ryzyko oparte na transakcji.
- W przypadku podpisu w locie opłata może być ponoszona wyłącznie za złożony podpis - brak potrzeby zakupu podpisu na konkretny okres czasu

MINUSY:

- Rozwiązanie przywiązane do oferującego usługę - niezależne od klienta
- Opłata jest ponoszona przy każdej transakcji (przez klienta lub usługodawcę cyfrowego)
- Wymagana jest identyfikacja przy każdej transakcji.
- Koszt wydania certyfikatu kwalifikowanego
- Brak funkcjonujących rozwiązań polskich dostawców
- Wymaga każdorazowo akceptacji wniosku o wydanie certyfikatu (przy każdym złożeniu podpisu)

Tylko podpis elektroniczny zwykły (np. z wykorzystaniem platformy do podpisu)

PLUSY:

- Wystarczający dla 95% spraw
- Łatwy do wykorzystania i zaimplementowania
- Gwarantuje integralność i “dowodowość”
- Identyfikuje podpisującego i zapewnia powiązanie transakcji z tą osobą

MINUSY:

- Nie jest równy formie pisemnej
- W przypadku procesów dowodowych to strona skarżąca musi udowodnić, że jest on skutecznym podpisem



EKSPERT RAPORTU

Marcin Szulga
Department Director
Security and Trust Services Division
Trust Services Research and Development Department

Jaka jest strategia rynkowa Certum?

Utrzymanie pozycji lidera rynku usług zaufania w Polsce i zdobywanie rynku europejskiego wymaga realizacji zaawansowanych technologicznie planów rozwojowych. Myślimy przede wszystkim o rozwoju ukierunkowanym na segment dużych przedsiębiorstw. Oczekują one przede wszystkim wysokiej dostępności i stabilności usług, w połączeniu z niespotykaną na rynku detalicznym i MŚP wydajnością i skalowalnością. Realizacja tego wyzwania jest możliwa dzięki połączeniu naszej eksperckiej wiedzy analitycznej z wykorzystaniem nowych technologii. To dzięki niemu już dziś jesteśmy w stanie realizować ponad 3 miliony dziennych transakcji podpisu mobilnego SimplySign.

Ekspansję rynkową realizujemy także rozwiązując problemy biznesowe klientów poprzez rozbudowę funkcjonalności naszych produktów. Dla certyfikatów kwalifikowanych wprowadzamy nowe metody onboardingu przy pomocy tabletów i podpisów biometrycznych. Pracujemy nad wideoidentyfikacją i rejestracją na podstawie wiarygodnych baz tożsamości dostawców usług finansowych, bez konieczności stawienia się w punkcie rejestracji. To umożliwi nam dalszą ekspansję na rynkach zagranicznych.

Wprowadzamy także usługę podpisu „w locie”, która daje możliwość rozliczania pojedynczych transakcji.

Rozwijamy narzędzia wspierające skalowanie procesów „paperless”. W tym obszarze stawiamy na rozbudowę aplikacji do podpisu nowej generacji, w szczególności systemu Signer, który integruje wszystkie usługi zaufania Certum, opakowując je w intuicyjny, zintegrowany interfejs.



EKSPERT RAPORTU

Tomasz Sekutowicz
SignHero

Przeprowadziliśmy setki rozmów z przedsiębiorcami na podstawie tych doświadczeń wciąż uważam, że na pierwszym miejscu jest mentalność na drugim edukacja.

Dlaczego mentalność? Często to uwarunkowania historyczne, ale też pewna bariera strachu przed nowym. Przedsiębiorcy szczególnie z segmentu MŚP to w Polsce grupa szczególnie narażona na ciągłe zmiany w prawie, ale też mocno uwikłana w codzienną rzeczywistość oraz brak czasu. Codziennosc jest taka, że pismo na papierze z własnoręcznym podpisem stanowi wciąż wyznacznik w kontaktach pomiędzy przedsiębiorcami, ale też kontrolujący ich urzędnicy, pierwsze o co proszą to o... „segregatory z dokumentami”. Jak można te stereotypy i mentalność przełamywać? Według mnie tylko rzetelną edukacją. Właściwie cały rynek szeroko pojętych usług cyfrowych, gospodarki bez papieru powinien zjednoczyć się w celu właściwej edukacji rynku. Wtedy właśnie zwracając uwagę przedsiębiorcom z różnych branż, ale także konsumentom wyrobimy oddolną potrzebę cyfryzacji, braku strachu przed nowym, lecz także przed wciąż wszechwładnym kontrolerem proszącym o segregatory. Konsument oraz przedsiębiorca, który wie, że może podpisać umowę z kontrahentem za pomocą platformy do podpisywania, certyfikatu kwalifikowanego czy zwykłego maila będzie działał sprawniej w bardzo konkurencyjnej gospodarce. Będzie wiedział, że urzędnicy czy sądy muszą uznawać określone dowody elektroniczne. Podejście do cyfryzacji zmienia się są branże, nowe biznesy, startupy które od początku stawiają na cyfryzację oraz procesy „bez papieru” jako swoiste biznesowe DNA. Trend jest już bardzo widoczny w korporacjach, energetyce czy telekomunikacji.

Integracja platformy do podpisywania SignHero z platforma edukacyjną Lingroom. Stanowi ona ciekawy przykład łączenia środowisk, przełamywania barier mentalnych oraz wspomnianej już edukacji. Dzięki tej inicjatywie uczniowie mogą korzystać z nowoczesnych zdalnej cyfrowej nauki języków obcych. Nauczyciel może wyjść z szarej strefy dostając legalny zarobek podpisując umowę a wszystko bez drukowania w zgodzie z najnowszą literą prawa o działalności nieewidencjonowanej.

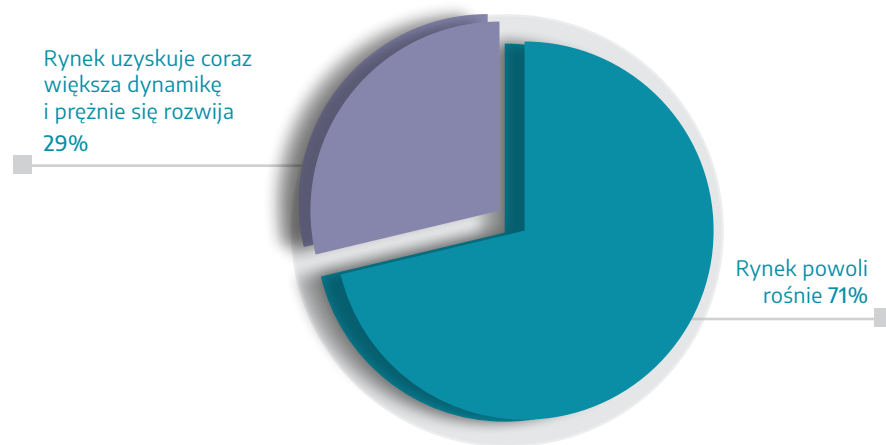


3.5 Komerccjalizacja eID i usług zaufania – wyniki badań

W ramach prac nad raportem zaprosiliśmy do współpracy dostawców usług eID i usług zaufania, jak również usługodawców cyfrowych, którzy dokonali oceny obecnego stanku rynku oraz wskazali perspektywy na okres 12 miesięcy.

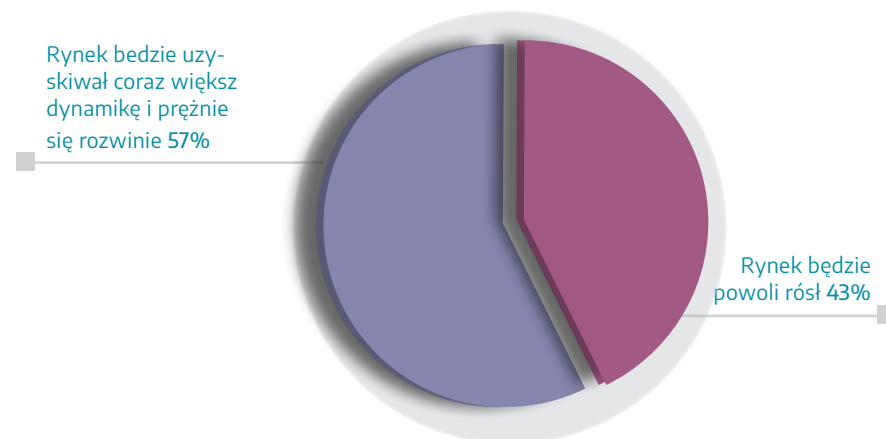
Wszyscy respondenci pozytywnie ocenili rozwój rynku eID i usług zaufania, zauważając jednak, że nie ma on dużej dynamiki.

Ocena biecej sztuacji na rznku eID i usug zaufania



W perspektywie najbliższych 12 miesięcy ankietowani dostrzegają szansę dynamicznego rozwoju rynku.

Ocena rozwoju rynku w perspektywie najbliższych 12 m-cy





Przedstawiciele dostawców usług wypowiedziłi się także na temat potencjału komercjalizacji usług zaufania oraz eID w wybranych sektorach, w szczególności energetyki, telekomunikacji, usług medycznych, IT, administracji publicznej czy finansowym.

Zdecydowanie najwyższy potencjał dla komercjalizacji dostrzegany jest w sektorze finansowym, co można uzasadnić dobrym przyjęciem obecnych już w sektorze rozwiązań, jego otwartością na nowości oraz potencjałem biznesowym dla eID i usług zaufania.

Potencjał komercjalizacji w sektorze finansowym:

Średnia (1-10):	8.71
Dominanta:	10

Wysoki potencjał

Uzasadnienie:

Duża świadomość, dużo kontaktów B2C, dobry start obecnych rozwiązań

Wysoko oceniany jest także potencjał w sektorze telekomunikacyjnym – respondenci zwrócili uwagę, że zastosowanie eID i usług zaufania pomogłoby zwiększyć konkurencyjność, wspomnieli także o konieczności podpisywania wielu dokumentów oraz nacisku na zdalny onboarding klienta.

Potencjał komercjalizacji w sektorze telekomunikacji:

Średnia (1-10):	7.71
Dominanta:	9

Wysoki potencjał

Uzasadnienie:

Duży potencjał do wprowadzenia ze względu na „zdalny charakter” procesu sprzedażowego, ponadto – procesy rejestracji SIM

Potencjał komercjalizacji w sektorze usług medycznych:

Średnia (1-10):	7.07
Dominanta:	5

Dość wysoki potencjał

Uzasadnienie:

Z jednej strony częsty kontakt biznes-klient i dużo dokumentów do podpisania, z drugiej - problemy legislacyjne i niska presja klientów na „cyfryzację” usług medycznych, istnienie konkurencyjnych usług publicznych



W rankingu wysoko uplasował się również sektor usług medycznych. Respondenci zwracają uwagę na potrzeby przetwarzania dużej liczby dokumentów w procesach medycznych, które wymagają stosowania podpisów. Z drugiej strony zagrożeniem dla komercjalizacji, jest kwestia sfery wrażliwych danych co może przełożyć się na niskie oczekiwania klientów co do cyfryzacji usług medycznych.

W dalszej kolejności uplasował się sektor administracji publicznej. W dużej mierze dlatego, że w ramach rozwiązań publicznych istnieją już narzędzia bezpłatne (np. podpis zaufany, podpis osobisty), które można wykorzystywać na co dzień w kontaktach z administracją publiczną.

Potencjał komercjalizacji w administracji publicznej:

Średnia (1-10):	6.71
Dominanta:	9

Dość wysoki potencjał

Uzasadnienie:

Z jednej strony państwo samo tworzy rozwiązania, z drugiej ma duży potencjał do ich popularyzacji. Dominacja narzędzi bezpłatnych

Dość wysoki potencjał wskazuje się w sektorze usług IT ze względu na rosnące zainteresowanie obszarem bezpieczeństwa, z czym z całą pewnością usługi zaufania są zbieżne.

Potencjał komercjalizacji w sektorze usług IT:

Średnia (1-10):	6.71
Dominanta:	9

Dość wysoki potencjał

Uzasadnienie:

Rosnące zainteresowanie i nacisk na bezpieczeństwo, jednak rzadkie kontakty B2C, nasycenie rynku

Potencjał komercjalizacji w domenie zarządzania zasobami ludzkimi:

Średnia (1-10):	6.29
Dominanta:	7

Potencjał niewysoki, ale wyższy od przeciętnego

Uzasadnienie:

Potencjał w umowach, ale niskie zapotrzebowanie



Potencjał komercjalizacji niewysoki bądź niewielki wskazuje się w domenie zarządzania zasobami ludzkimi, w sektorze obrotu nieruchomościami oraz w sektorze energetyki. Jako główne przyczyny niskiej oceny potencjału wskazywane są:

- Nieskie zapotrzebowanie użytkowników końcowych na usługi zaufania (np. obszar rekrutacji)
- Brak świadomości usługobiorców w zakresie istnienia usług zaufania i elektronicznej identyfikacji (obszar obrotu nieruchomościami)
- Niska konkurencyjność rynku, rzadkie zmiany dostawców – sektor energetyki

Potencjał komercjalizacji w sektorze obrotu nieruchomościami:

Średnia (1-10):	5.86
Dominanta:	3

Niewielki potencjał komercjalizacji

Uzasadnienie:

Brak świadomości, jest potencjał, ale wymaga zmiany postrzegania eID i usług zaufania. Ryzyko.

Potencjał komercjalizacji w sektorze energetyki:

Średnia (1-10):	5.71
Dominanta:	9

Niewielki potencjał komercjalizacji

Uzasadnienie:

Uzależnienie od wpływu państwa, rzadkie zmiany dostawcy, niska konkurencyjność



EKSPERT RAPORTU

Tomasz Chomicki
Przewodniczący Komitetu Administracji Cyfrowej
Polska Izba Informatyki i Telekomunikacji

W ostatnich latach można zaobserwować gwałtowny rozwój usług zaufania na Świecie. Ostatnio celebrowaliśmy dwadzieścia lat podpisu elektronicznego w Polsce, który pokazał nam nowy obraz współczesnego świata. Czas w którym żyjemy ciągle się zmienia i stawia firmom technologicznym coraz to nowe cyfrowe wyzwania. Powstają nowe usługi i rozwiązania w których kładzie się nacisk na mobilność, bezpieczeństwo danych oraz szybkość i elastyczność nowych rozwiązań. Cyber bezpieczeństwo stało się podstawą działania rynku „Cyfrowej Tożsamości”. Ważne jest aby nie zapomnieć, że rozwiązania, których kluczowym komponentem są dane wrażliwe podlegały procesowi certyfikacji w oparciu o normy tj. Common Criteria.

Cieszymy się, że na rynku polskim powstają opracowania takie jak Komerccjalizacja eID i usług zaufania w Polsce i Europie tworzony przez grono unikalnych ekspertów z dziedziny usług zaufania.



Rozdział 4 –

SCENARIUSZE ROZWOJU RYNKU

4.1 Wprowadzenie

W poprzednich rozdziałach opisano szereg rozwiązań i usług, które mają dostarczyć mechanizmy bezpieczeństwa dla usług dostępnych on-line oraz zapewnić zawieranie transakcji na odległość. Zweryfikowano potencjał komercjalizacji poszczególnych obszarów biznesowych, jak również wskazano na główne kierunki rozwoju rynku, które określili wypowiadający się eksperci. Zarówno przepisy prawa jak i dojrzałość usług oferowanych usług pozwalają postawić tezę, że będzie rosła zarówno świadomość użytkowników jak i wykorzystanie tych usług. Wskażmy jednocześnie jakie są scenariusze rozwoju tego rynku w zakresie transformacji jego:

- narzędzi;
- usługobiorców i usługodawców (konsumentów, przedsiębiorców);
- rozwoju biznesowego.

4.2 Rozwój narzędzi

Czy wygrają usługi zaufania powiązane z eID?

Tak – usługi eID są potrzebne do rejestracji w usługach zaufania, są pierwszym elementem wydania certyfikatu i obowiązkowym elementem elektronicznego doręczenia. Elektroniczna identyfikacja w sposób jednolity i uznany prawnie pozwala potwierdzić tożsamość, a więc wymagany także dla usług kwalifikowanych. Już dziś mamy środki identyfikacji elektronicznej, których poziom wiarygodności potwierdził Minister Cyfryzacji dopuszczając je do zakładania profilu zaufanego – wykorzystanie ich w usługach kwalifikowanych jest tylko kwestią czasu.

Narzędzia elektronicznej identyfikacji – dowód osobisty, wideoweryfikacja,

Dla funkcjonowania usług zaufania niezbędna jest dostępność usług identyfikacji elektronicznej, której pierwotnym źródłem są rejestry państwowe i wydawane na ich podstawie dokumenty tożsamości. Nowy elektroniczny dowód osobisty docelowo przyczyni się automatyzacji procesu rejestracji w usługach zaufania, ale zanim każdy będzie miał go w swoim portfelu minie jeszcze kilka lat. Na dziś najszybszym sposobem potwierdzania tożsamości dostępnym powszechnie w innych krajach jest wideo weryfikacja, umożliwia ona w szczególności wydanie certyfikatu



kwalfikowanego bez konieczności wizyty w punkcie potwierdzania tożsamości. Rozwiązania bazujące na wideo weryfikacji w najbliższych latach będą głównym mechanizmem weryfikacji, dla bezpieczeństwa będzie ona wspomagana innymi technikami, docelowo zaś elektroniczny dowód osobisty ma szansę stać się głównym rozwiązaniem do potwierdzania tożsamości obywatela w tych najważniejszych procesach elektronicznych.

Biometria cały czas budzi bardzo dużo emocji, choć bardzo powszechnie weszła w użycie w telefonach komórkowych, gdzie za pomocą odcisku palca i weryfikacji twarzy odblokowywany jest dostęp do telefonu, a także realizacja funkcji płatniczych. Wszystkie mechanizmy biometrii, które bez zbytej ingerencji w użyteczność będą wspomagały uwierzytelnienie użytkownika będą miały zastosowania dla usług zaufania, a w zależności od jego bezpieczeństwa będą głównym elementem zabezpieczeń lub mechanizmem wspomagającym bezpieczeństwo. W tym drugim kontekście coraz większe znaczenie będzie miała biometria behawioralna, która bazując na analizie zachowania użytkownika będzie dostarczała dodatkowej informacji, pozwalającej ocenić ryzyko transakcyjne przy identyfikacji elektronicznej oraz składaniu podpisów elektronicznych.

Nośniki i narzędzia dla usług zaufania

Gdy kilkanaście lat temu pierwsze kwalifikowane certyfikaty wchodziły do użycia karta stanowiła podstawę rozwiązań oferowanych przez wszystkich dostawców na rynku. Na przestrzeni lat główne udogodnienie dotyczyło zmniejszenia karty i udostępnienia jej w postaci klucza USB. Karta ma wadę polegającą na konieczności instalowania jej sterowników w środowisku, w którym ma być używana. Realizując generalną tendencję wirtualizacji rozwiązań aktualnie także w Polsce dostępne są rozwiązania podpisu kwalifikowanego umożliwiające zdalne złożenie podpisu kwalifikowanego. Tego typu rozwiązań jest coraz więcej i docelowo wyprą one kartę w zastosowaniach konsumentów, a sama karta zostanie jako rozwiązanie przeznaczone, tam gdzie osoba fizyczna składa każdego dnia wiele podpisów, w swoim dobrze określonym środowiskiem.

Nowy e-dowód – czy zmieni rynek

Nowy dowód osobisty z warstwą elektroniczną, wdrożony w marcu 2019r., wprowadził 4 główne funkcje elektroniczne: Przekazanie potwierdzonych danych posiadacza dowodu, Potwierdzenie obecności, Identyfikacja elektroniczna i Podpis Osobisty. Wszystkie te elementy będą miały coraz większe zastosowanie w zabezpieczaniu zarówno kontaktu bezpośredniego jak i elektronicznego obywatela z urzędami, bankami i firmami. W pierwszej fazie znaczenie dowodu będzie największe tam, gdzie warstwa elektroniczna zabezpiecza dzisiejsze funkcje weryfikacji dowodu np. przy udzieleniu kredytu. Dowód powinien mieć ogromną rolę w identyfikacji



obywatela w usługach publicznych, ale także w usługach zaufania i finansowych, natomiast dowód ze względu na swoje znaczenie dla prywatnych spraw każdego obywatela nie powinien stać się narzędziem służącym do składania podpisów i potwierdzeń w imieniu firm i urzędów, ponieważ w efekcie może stanowić to znakomite narzędzie do naruszenia bezpieczeństwa samego posiadacza dowodu.

Trwały nośnik a elektroniczne doręczenie

Institucja trwałego nośnika powstała ze względu na brak rejestrowanych elektronicznych doręczeń, docelowo trwały nośnik powinien zostać zastąpiony przez tego typu rozwiązania, które nie tylko będą gwarantowały niezmiennosc treści, ale także dostarczały dowody nadania i odebrania danych przekazywanych konsumentowi.

Głównym hamulcem rozwoju usług elektronicznego doręczenia w Polsce jest brak prawnych mechanizmów pozwalających na przyjmowanie w ten sposób dokumentów przez administrację publiczną. Ograniczenie się w zakresie wymiany dokumentów do własnych rozwiązań poszczególnych urzędów oraz portalu ePUAP nie wpływa na rozwój usług elektronicznych w Polsce. Doręczenia zdobywają coraz większe uznanie w krajach Unii Europejskiej i także w Polsce należy spodziewać się w niedługim czasie rozwoju tych usług. Projektowana ustawa o elektronicznych doręczeniach w zależności od swojej konstrukcji może dać podstawy do równoległego funkcjonowania i rozpoznawania przez administrację publiczną kwalifikowanych usług rejestrowanego doręczenia elektronicznego lub wprowadzając jeden model dotychczasowej usługi publicznej doręczenia elektronicznego powielić błędy ePUAP. W tym momencie w Polsce jest niewiele usług elektronicznych doręczeń, realizują je Envelo, Bankmail oraz Autenti, nie są to usługi kwalifikowane i każda realizuje doręczenie wg własnych standardów. W krajach członkowskich UE także jest tylko 11 kwalifikowanych usług RDE, ale należy zauważyć, że normy wskazujące jak zrealizować takie usługi zostały opublikowane w ciągu ostatniego pół roku.

Pieczeći elektroniczne

Stosowanie pieczęci elektronicznej we wszystkich usługach dostępnych on-line znacząco ułatwia procesy zarówno administracyjne jak i firmowe. Ogromne usprawnienie dałoby wprowadzenie do przepisów prawa możliwości wydawania decyzji i innych dokumentów przez urzędy, które zamiast podpisu zawierałyby kwalifikowaną pieczęć urzędu. Pieczęć nie wyeliminuje podpisów, które służą do składania oświadczeń woli, ale wszędzie tam, gdzie jest potrzebny automatyzm wydania dokumentu oraz mechanizm pozwalający na potwierdzenie źródła jego pochodzenia jest rozwiązaniem najlepszym. W tym zakresie o ile nastąpią planowane przez Ministra Cyfryzacji zmiany pieczęć elektroniczna stanie się podstawowym atrybutem pisma urzędowego.



4.3 Rozwój rynku usługobiorców i usługodawców (konsumentów, przedsiębiorców)

Perspektywa usługobiorcy i usługodawcy

Usługobiorca – czyli klient, który korzysta z usługi, aby zrealizować swoją potrzebę. Nauczony został, że wszystkie usługi on-line dostępne są od razu, bez zbędnego oczekiwania, bez konieczności wykonywania żadnych dodatkowych czynności. Badania nad użytecznością i doświadczeniem użytkownika pozwalają na znaczące podniesienie ergonomii korzystania z usług. Przyjazny interfejs, dostępność usług z telefonu komórkowego, łatwe płatności, brak konieczności wypełniania pisanych formularzy to główne cechy oczekiwanego rozwiązania usługowego w internecie. Ten przebieg jest bardzo prosty dla usług płatnych, które nie są obciążone dodatkowym ryzykiem transakcyjnym lub dodatkowymi wymaganiami prawnymi. Z tego powodu usługi operatorów energetycznych, telekomunikacyjnych i często ubezpieczeniowe wymagają spotkania z przedstawicielem lub przynajmniej popisania umowy za pośrednictwem kuriera. Nie jest to bardzo duże obciążenie, ale skutecznie wydłuża czas pomiędzy oczekiwaniem rozpoczęcia działania usługi, a jej realizacją.

Usługodawca – rozumiany jako firma, która realizując cele biznesowe chce zwiększać dostępność swoich usług dla klientów, pozyskiwać ich szybciej oraz jednocześnie optymalizować koszty. Optymalizacja kosztów jest najczęstszym powodem rozpoczynania projektów transformacji cyfrowej procesów biznesowych z papierowych na elektroniczne. Warunki brzegowe dla rozpoczęcia projektu depapieryzacji to zapewnienie niezmnieszonego dostępu klientów do usługi oraz zapewnienie kosztów nie większych niż w obrocie papierowym. Zazwyczaj zyski długoterminowe oraz wychodzące poza obszar pojedynczego procesu biznesowego nie są brane pod uwagę, w szczególności koszty przechowywania, wyszukiwania, przewożenia oraz obsługi w istniejących oddziałach nie są uwzględniane.

Dalszy rozwój rynku zależy od świadomości zarówno usługobiorcy jak i usługodawcy. Nowe innowacyjne pojawiające się usługi na pewno wpływają na konkurencyjność usług a to w efekcie podnosi świadomość i oczekiwanie klientów. Świadomość będzie rosła, za pojawiać się będą nowe oczekiwania usługobiorców, którym sprostać będą chcieli usługodawcy, w tym zakresie wykorzystanie usług identyfikacji elektronicznej jak i usług zaufania będzie coraz większe, o ile będą one oferowane w sposób zapewniający łatwość i przyjazność ich użytkowania.

Oczywiście dla dalszego rozwoju rynku występują też zagrożenia, które mogą całkowicie lub czasowo zahamować wykorzystanie elektronicznych usług w transakcjach online. Pierwsze zagrożenie to szeroko pojęte bezpieczeństwo, rozumiane zarówno jako gotowość dostawców usług zaufania i identyfikacji elektronicznej do sprostania pojawiającym się atakom i przyszłym próbom fraudów realizowanych w oparciu o te technologie. Popularyzacja rozwiązań identyfikacji elektronicznej, podpisów elektronicznych i usług zaufania będzie niosła za sobą coraz większe zainteresowanie przestępców, w tym zakresie dotychczasowe doświadczenie sektora bankowego wydaje się nieocenione.



Kolejnym zagrożeniem jest stanowienie prawa, które z jednej strony zostało zdefiniowane na poziomie europejskim, co gwarantuje jego stabilność w zakresie założeń, ale przepisy krajowe dają wskazania i narzędzia do rozpoznawania usług zaufania w usługach publicznych i ich rzeczywistego wykorzystania w tym sektorze. Prawne wprowadzanie lokalnych rozwiązań, może zaburzać konkurencyjność rynku a więc także i potencjalny jego rozwój.

4.4 Rozwój rynkowy

Kwalifikowani dostawcy usług zaufania dostarczają rozwiązania na najwyższym poziomie bezpieczeństwa, wymaganym przez przepisy prawa, normy techniczne oraz potwierdzone w okresowych audytach. Adresowanie biznesowych potrzeb klientów stoi poniekąd w sprzeczności z restrykcyjnymi wymaganiami bezpieczeństwa, z tego powodu bardzo duże znaczenie dla rozwoju rynku mają integratorzy usług zaufania oraz specjalizowane w tych usługach firmy konsultingowe. To te podmioty znając ograniczenia i możliwości usług kwalifikowanych oraz oczekiwania rynkowe są w stanie dostarczyć rozwiązania pozwalające

na realizację potrzeb biznesowych obu grup. Konsulting wokół procesów biznesowych dużych korporacji i realizacja cyfrowej transformacji ich biznesu pozwala na zaproponowanie optymalnych narzędzi dopasowanych do kultury organizacyjnej zmieniającej się instytucji. Integratorzy poza zaoferowaniem szerokiego wachlarza różnych usług zaufania i połączenia ich z innymi usługami biznesowymi są w stanie dostarczyć rozwiązania spełniające oczekiwania dotyczące ergonomii. Integratorzy są w stanie dobrać rozwiązania dla klientów z sektora MŚP – można sobie wyobrazić tu rozwiązania modułowe czy sektorowe – np. dedykowaną ofertę dla agencji pracy, prywatnych ośrodków zdrowia, szkół czy lokalnych dostawców usług wodociągowych, zarządzania odpadami itd.

Rynek usług zaufania, którego podstawowe usługi, potencjał i uwarunkowania działania przedstawiliśmy powyżej stoi aktualnie w bardzo ważnym momencie. Zapotrzebowanie na migrację procesów biznesowych, konsumenckich oraz administracyjnych jest wysokie i wszystko wskazuje na to, że będzie tylko dynamicznie rosnąć. Zabezpieczenie dowodowe i odpowiednie umocowanie w regulacjach, również pozostaje bardzo istotne. Instytucje komercyjne i publiczne szukają metod aby kolejne swoje procesy móc w pełni scyfrzować i udostępnić jak najszerszej rzeszy klientów. Jednocześnie końcowy użytkownicy deklarują, że chcieliby jak najwięcej czynności wykonywać on-line – analogicznie jak to robią aktualnie, gremialnie korzystając z usług finansowych online.

Przy rozwoju rynku niezbędne jest wspólne działanie na rzecz współpracy z regulatorem na rzecz wypracowywania odpowiednich zmian w prawie dających przestrzeń do bezpiecznego funkcjonowania eID i usług zaufania. Niezbędna jest również współpraca poszczególnych graczy na rynku, aby przekraczając swoją konkurencyjność, mogli dostrzec potencjał kooperacji – przy wspomnianej współpracy z regulatorem, przy oddziaływaniu na usługodawców cyfrowych, aby wspólnie przekonywać ich do korzystania z usług zaufania, przy wspólnych działaniach edukacyjnych wobec rynku. Jako autorzy niniejszego raportu, mamy przeświadczenie, że właśnie ten projekt jest dowodem na to, że rynek jest gotowy na taką, szeroką współpracę, w imię wspólnego celu – budowy przyjaznej klientom, obywatelom, przedsiębiorcom - Polski cyfrowej.



EKSPERT RAPORTU

Aleksander Naganowski, Director
Business Development, Partnerships and Innovation Poland
Mastercard

Cyfrowa tożsamość to nie innowacja na miarę przyszłości. To już całkiem aktualna potrzeba wielu kontrahentów biznesowych. W świecie, w którym wszelkie produkty i usługi możemy zamawiać cyfrowo, a najłatwiejszy kontakt z klientem zapewniają urządzenia mobilne, nieodzowna jest jednoznaczna identyfikacja komunikujących się stron.

Dlatego też Mastercard podjął wyzwanie budowy standardu tożsamości cyfrowej, który ma globalny zasięg, a jednocześnie zapewnia, że prawdziwym właścicielem zgromadzonych danych jest sam użytkownik, a nie organizacje, które informacje o nim zebrały. Przywrócenie zaufania między stronami kontaktującymi się w cyfrowym świecie to wizja Mastercard, którą budujemy z partnerami na całym świecie już teraz.

EKSPERT RAPORTU

Paweł Stosik,
Prezes Zarządu Fundacji Polska 5.0

Wiele, nie tylko polskich, przedsiębiorstw widzi podobne bariery związane z transformacją cyfrową. Jednym z problemów jest fakt, że nie wszystkie firmy traktują cyfryzację jako proces, działanie długofalowe. Brak im spójnej strategii oraz osób odpowiedzialnych za przebieg transformacji. Cyfryzacja pojedynczych procesów na zasadzie ad hoc może prowadzić do powstania chaosu informacyjnego nie tylko wewnątrz, ale również na zewnątrz firmy. Drugą niezwykle istotną, chyba najczęściej wskazywaną przez przedsiębiorców barierą są przestarzałe systemy oraz infrastruktura. Wiele z nich budowano latami, z każdą wprowadzaną zmianą zwiększając poziom skomplikowania. Modernizacja tych systemów, od której często zależy sukces cyfryzacji całego przedsiębiorstwa, może być niezwykle trudna i kosztowna.

„Elektroniczna identyfikacja i usługi zaufania są jednym z budzących największą nadzieję narzędzi na kompleksowe zaadresowanie tych wyzwań. Podczas prac Fundacji Polska 5.0 chcemy identyfikować największe bariery w cyfryzacji procesów na styku obywatela, konsumenta, przedsiębiorcy z państwem i usługodawcami komercyjnymi. Upowszechnienie wygodnych i bezpiecznych usług eID i zaufania mogą być pomocne w likwidacji tych barier.”



Słownik pojęć

„identyfikacja elektroniczna (eID)”	oznacza proces używania danych w postaci elektronicznej identyfikujących osobę, unikalnie reprezentujących osobę fizyczną lub prawną, lub osobę fizyczną reprezentującą osobę prawną;
„środek identyfikacji elektronicznej”	oznacza materialną lub niematerialną jednostkę zawierającą dane identyfikujące osobę i używaną do celów uwierzytelniania dla usługi online;
„dane identyfikujące osobę”	oznaczają zestaw danych umożliwiających ustalenie tożsamości osoby fizycznej lub prawnej, lub osoby fizycznej reprezentującej osobę prawną;
„system identyfikacji elektronicznej”	oznacza system identyfikacji elektronicznej, w ramach którego wydaje się środki identyfikacji elektronicznej osobom fizycznym lub prawnym, lub osobom fizycznym reprezentującym osoby prawne;
„uwierzytelnianie”	oznacza proces elektroniczny, który umożliwia identyfikację elektroniczną osoby fizycznej lub prawnej, lub potwierdzenie pochodzenia oraz integralności weryfikowanych danych w postaci elektronicznej;
„strona ufająca”	oznacza osobę fizyczną lub prawną, która polega na identyfikacji elektronicznej lub usłudze zaufania;
„podmiot sektora publicznego”	oznacza organ państwowy, regionalny lub lokalny, podmiot prawa publicznego lub stowarzyszenie utworzone przez jeden lub kilka takich organów lub jeden lub kilka takich podmiotów prawa publicznego, lub jednostkę prywatną, której co najmniej jeden z tych organów, podmiotów lub jedno z takich stowarzyszeń udzieliły upoważnienia do świadczenia usług publicznych, gdy działa ona na podstawie takiego upoważnienia;
„podmiot prawa publicznego”	oznacza podmiot zdefiniowany w art. 2 ust. 1 pkt 4 dyrektywy Parlamentu Europejskiego i Rady 2014/24/UE ⁽¹⁵⁾ ;
„podpisujący”	oznacza osobę fizyczną, która składa podpis elektroniczny;
„podpis elektroniczny”	oznacza dane w postaci elektronicznej, które są dołączone lub logicznie powiązane z innymi danymi w postaci elektronicznej, i które użyte są przez podpisującego jako podpis;
„zaawansowany podpis elektroniczny”	oznacza podpis elektroniczny, który spełnia wymogi określone w art. 26;
„kwalifikowany podpis elektroniczny”	oznacza zaawansowany podpis elektroniczny, który jest składany za pomocą kwalifikowanego urządzenia do składania podpisu elektronicznego i który opiera się na kwalifikowanym certyfikacie podpisu elektronicznego;
„dane służące do składania podpisu elektronicznego”	oznaczają unikalne dane, których podpisujący używa do składania podpisu elektronicznego;
„certyfikat podpisu elektronicznego”	oznacza poświadczenie elektroniczne, które przyporządkowuje dane służące do walidacji podpisu elektronicznego do osoby fizycznej i potwierdza co najmniej imię i nazwisko lub pseudonim tej osoby;



„kwalifikowany certyfikat podpisu elektronicznego”	oznacza certyfikat podpisu elektronicznego, który jest wydawany przez kwalifikowanego dostawcę usług zaufania i spełnia wymogi określone w załączniku I;
„usługa zaufania”	oznacza usługę elektroniczną zazwyczaj świadczoną za wynagrodzeniem i obejmującą: a) tworzenie, weryfikację i walidację podpisów elektronicznych, pieczęci elektronicznych lub elektronicznych znaczników czasu, usług rejestrowanego doręczenia elektronicznego oraz certyfikatów powiązanych z tymi usługami; lub b) tworzenie, weryfikację i walidację certyfikatów uwierzytelniania witryn internetowych; lub c) konserwację elektronicznych podpisów, pieczęci lub certyfikatów powiązanych z tymi usługami;
„kwalifikowana usługa zaufania”	oznacza usługę zaufania, która spełnia stosowne wymogi określone w niniejszym rozporządzeniu;
„jednostka oceniająca zgodność”	oznacza jednostkę określoną w art. 2 pkt 13 rozporządzenia (WE) nr 765/2008, która jest akredytowana zgodnie z tym rozporządzeniem jako właściwa do przeprowadzania oceny zgodności kwalifikowanego dostawcy usługi zaufania i świadczonych przez niego kwalifikowanych usług zaufania;
„dostawca usług zaufania”	oznacza osobę fizyczną lub prawną, która świadczy przynajmniej jedną usługę zaufania, jako kwalifikowany lub niekwalifikowany dostawca usług zaufania;
„kwalifikowany dostawca usług zaufania”	oznacza dostawcę usług zaufania, który świadczy przynajmniej jedną kwalifikowaną usługę zaufania i któremu status kwalifikowany nadał organ nadzoru;
„produkt”	oznacza sprzęt lub oprogramowanie lub odpowiednie komponenty sprzętu lub oprogramowania, które są przeznaczone do wykorzystania w świadczeniu usług zaufania;
„urządzenie do składania podpisu elektronicznego”	oznacza skonfigurowane oprogramowanie lub skonfigurowany sprzęt, które wykorzystuje się do składania podpisu elektronicznego;
„kwalifikowane urządzenie do składania podpisu elektronicznego”	oznacza urządzenie do składania podpisu elektronicznego, które spełnia wymogi określone w załączniku II;
„podmiot składający pieczęć”	oznacza osobę prawną, która składa pieczęć elektroniczną;
„pieczęć elektroniczna”	oznacza dane w postaci elektronicznej dodane do innych danych w postaci elektronicznej lub logicznie z nimi powiązane, aby zapewnić autentyczność pochodzenia oraz integralność powiązanych danych;
„zaawansowana pieczęć elektroniczna”	oznacza pieczęć elektroniczną, która spełnia wymogi określone w art. 36;
„kwalifikowana pieczęć elektroniczna”	oznacza zaawansowaną pieczęć elektroniczną, która została złożona za pomocą kwalifikowanego urządzenia do składania pieczęci elektronicznej i która opiera się na kwalifikowanym certyfikacie pieczęci elektronicznej;
„dane służące do składania pieczęci elektronicznej”	oznaczają niepowtarzalne dane, które podmiot składający pieczęć wykorzystuje do złożenia pieczęci elektronicznej;
„certyfikat pieczęci elektronicznej”	oznacza poświadczenie elektroniczne, które łączy dane służące do walidacji pieczęci elektronicznej z osobą prawną i potwierdza nazwę tej osoby;



„kwalifikowany certyfikat pieczęci elektronicznej”	oznacza certyfikat pieczęci elektronicznej, który jest wydawany przez kwalifikowanego dostawcę usług zaufania i spełnia wymogi określone w załączniku III;
„urządzenie do składania pieczęci elektronicznej”	oznacza skonfigurowane oprogramowanie lub skonfigurowany sprzęt, które wykorzystuje się do składania pieczęci elektronicznej;
„kwalifikowane urządzenie do składania pieczęci elektronicznej”	oznacza urządzenie do składania pieczęci elektronicznej, które spełnia odpowiednio wymogi określone w załączniku II;
„elektroniczny znacznik czasu”	oznacza dane w postaci elektronicznej, które wiążą inne dane w postaci elektronicznej z określonym czasem, stanowiąc dowód na to, że te inne dane istniały w danym czasie;
„kwalifikowany elektroniczny znacznik czasu”	oznacza elektroniczny znacznik czasu, który spełnia wymogi określone w art. 42;
„dokument elektroniczny”	oznacza każdą treść przechowywaną w postaci elektronicznej, w szczególności tekst lub nagranie dźwiękowe, wizualne lub audiowizualne;
„usługa rejestrowanego doręczenia elektronicznego”	oznacza usługę umożliwiającą przesłanie danych między stronami trzecimi drogą elektroniczną i zapewniającą dowody związane z posługiwaniem się przesyłanymi danymi, w tym dowód wysłania i otrzymania danych, oraz chroniącą przesyłane dane przed ryzykiem utraty, kradzieży, uszkodzenia lub jakiegokolwiek nieupoważnionej zmiany;
„kwalifikowana usługa rejestrowanego doręczenia elektronicznego”	oznacza usługę rejestrowanego doręczenia elektronicznego, która spełnia wymogi określone w art. 44;
„certyfikat uwierzytelniania witryn internetowych”	oznacza poświadczenie, które umożliwia uwierzytelnianie witryn internetowych i przyporządkowuje witrynę internetową do osoby fizycznej lub prawnej, której wydano certyfikat;
„kwalifikowany certyfikat uwierzytelniania witryn internetowych”	oznacza certyfikat uwierzytelniania witryn internetowych, który jest wydawany przez kwalifikowanego dostawcę usług zaufania i spełnia wymogi określone w załączniku IV;
„dane służące do walidacji”	oznaczają dane używane do walidacji podpisu elektronicznego lub pieczęci elektronicznej;
„walidacja”	oznacza proces weryfikacji i potwierdzenia ważności podpisu elektronicznego lub pieczęci.



AUTORZY RAPORTU



Miłosz Brakoniecki –
członek zarządu Obserwatorium.biz sp. z o.o.



Michał Tabor –
członek zarządu Obserwatorium.biz sp. z o.o.



Marcin Wolski –
ekspert Obserwatorium.biz sp. z o.o.



Marcin Żywicki –
analityk Obserwatorium.biz sp. z o.o.



patron główny



EFPE

partner naukowy



partner społeczny



partner



partner



patron honorowy



MINISTERSTWO
PRZEDSIĘBIORCZOŚCI
I TECHNOLOGII



Metodologia przygotowania raportu

Raport „Biznes bez papieru. Komerccjalizacja eID i usług zaufania w Polsce i Europie”, został przygotowany w oparciu o wiedzę partnerów i pracowników Obserwatorium.biz oraz przeprowadzone przez nich analizy rynku polskiego i zagranicznego w zakresie usług zaufania i elektronicznej identyfikacji oraz ich zastosowania w biznesie oraz administracji publicznej.

Dodatkowo zrealizowano badania przy wykorzystaniu techniki CAWI (ankiety na stronie WWW) wykonane w pierwszym kwartale 2019 - próba objęła osoby bezpośrednio związane z rynkiem eID i usług zaufania. W raporcie wypowiedzieli się również przedstawiciele następujących instytucji: Krajowa Izba Rozliczeniowa S.A., Asseco Data Systems S.A., Kancelaria Prawna Szostek & Bar, Poczta Polska S.A., Rachuneo, Sighnero, Polska Izba Informatyki i Telekomunikacji.

Nota prawna

Opinie zawarte w raporcie wydane zostały na podstawie wiedzy pozyskanej z badania rynku i doświadczenia autorów raportu. Autorzy nie biorą odpowiedzialności za decyzje podjęte na podstawie opinii wydanych w ramach raportu „Biznes bez papieru. Komerccjalizacja eID i usług zaufania w Polsce i Europie”

