PRZEWODNIK

IDENTYFIKACJA I UWIERZYTELNIENIE W USŁUGACH ELEKTRONICZNYCH

Związek Banków Polskich

Przewodnik powstał
w Związku Banków Polskich
w ramach prac Forum Technologii
Bankowych ZBP i Rady Bankowości
Elektronicznej ZBP.

Copyright © Związek Banków Polskich
All rights reserved
ISBN 978-83-950679-2-1

Warszawa 2020, wydanie I

ZESPÓŁ REDAKCYJNY
Maciej Kostro, *redaktor prowadzący*
Michał Tabor, *redaktor merytoryczny*

AUTORZY
Zbigniew Długosz
Marcin Jankowski
Marta Merta
Krzysztof Pycia
Marek Obuchowicz
Konrad Stolarski
Marcin Strzałek
Michał Tabor
Marcin Wolski
Tomasz Zając

PROJEKT GRAFICZNY
Voilà! Information Design Studio
www.voila-infographics.com

SPIS TREŚCI

1 Wstęp / 6

2 Nomenklatura pojęciowa / 7

3 Streszczenie / 20

4 Identyfikacja i uwierzytelnienie w standardach / 21

4.1 Rozporządzenie eIDAS / 21

4.1.1 Usługi zaufania i identyfikacja elektroniczna / 21

4.1.2 Podpis elektroniczny / 22

4.1.3 Pieczęć elektroniczna / 23

4.1.4 Infrastruktura klucza publicznego / 23

4.1.5 Znakowanie czasem / 24

4.1.6 Ważność podpisu i pieczęci / 24

4.1.7 Identyfikacja elektroniczna wg rozporządzenia eIDAS / 25

4.1.8 Rodzaje podpisów i pieczęci elektronicznych / 26

4.2 Podpisy elektroniczne w uregulowaniach krajowych / 30

4.3 Standardy ETSI / 31

4.4 Specyfikacja eIDAS / 32

4.5 Norma ISO 29115 / 35

4.5.1 Struktura i poziomy wiarygodności uwierzytelnienia / 35

4.5.2 Fazy w strukturze wiarygodności / 38

4.5.3 Wymagania organizacyjne i proceduralne / 41

4.5.4 Wymagania i środki sterowania bezpieczeństwem / 41

4.6 Standard NIST SP 800-63 / 42

4.6.1 SP 800-63A Rejestracja i weryfikacja tożsamości / 43

4.6.2 SP 800-63B Uwierzytelnianie i zarządzanie cyklem życia / 43

4.6.3 SP 800-63C Federacje i asercje / 44

4.6.4 Rodzaje urządzeń uwierzytelniających / 45

5 Przegląd koncepcji uwierzytelnienia / 47

5.1 Czynniki uwierzytelniania / 47

5.2 Dyrektywa PSD2 / 48

5.3 Uwierzytelnienie kryptograficzne / 49

5.3.1 Problem losowości przy generowaniu „haseł jednorazowych" / 49

5.3.2 Mechanizmy uwierzytelnienia oparte o kryptografię asymetryczną / 53

5.3.3 Podpis serwerowy / 53

5.3.4 Dowody niezaprzeczalności / 56

5.4 Uwierzytelnienie biometryczne / 57

5.4.1 Pojęcia i definicje / 57

5.4.2 Wstęp do biometrii / 58

5.4.3 Mechanizmy odporności na ataki / 63

5.4.4 Biometria jako metoda uwierzytelniania / 64

5.5 Uwierzytelnienie proceduralne / 66

5.6 Uwierzytelnienie oparte na wiedzy / 67

5.7 Uwierzytelnienie w oparciu o portale społecznościowe / 67

5.8 Uwierzytelnienie na podstawie danych bankowych właściciela rachunku / 68

5.9 Uwierzytelnienie na podstawie atrybutów / 69

5.10 Uwierzytelnienie z zachowaniem prywatności / 69

5.11 Zdalne potwierdzanie tożsamości / 72

5.11.1 Zalecenia KNF w zakresie zdalnego potwierdzania tożsamości / 72

5.11.2 Rozwiązania zdalnego potwierdzania tożsamości / 73

6 Przegląd rozwiązań technicznych / 75

6.1 Karty elektroniczne / 75

6.1.1 Rodzaje kart elektronicznych / 75

6.1.2 Kwalifikowane urządzenie do składania podpisu elektronicznego / 77

6.2 Narodowe dokumenty tożsamości / 77

6.3 Hasła jednorazowe / 78

6.4 Mechanizmy CAP/DPA / 80

6.5 3DSecure / 81

6.6 Metody push / 82

6.7 Mobile Connect / 82

6.8 Uwierzytelnienie a czytniki kart elektronicznych / 83

6.8.1 Rodzaje czytników / 83

6.8.2 Uwierzytelnienie terminala / 84

6.9 Zcentralizowane systemy potwierdzania tożsamości / 87

7 Aspekty prawne / 89

7.1 Zasady świadczenia usług zaufania / 89

7.2 Podpis elektroniczny a forma czynności prawnej / 90

7.3 Identyfikacja i Węzeł Krajowy / 92

7.4 Uwierzytelnianie w usługach płatniczych / 94

7.5 Identyfikacja TPP / 96

7.6 Dane osobowe a identyfikacja i uwierzytelnianie / 97

7.7 Identyfikacja i weryfikacja w rozumieniu przepisów AML / 98

8 Identyfikacja i uwierzytelnienie – stan obecny w Polsce / 100

8.1 Stan obecny sektora finansowego / 100

8.2 Dyrektywa PSD2 i definicja SCA / 102

8.3 SCA w Polsce w świetle NIST SP 800-63 / 104

8.4 Zapamiętany sekret / 104

8.5 Lista kodów / 106

8.6 Kody SMS/aplikacja mobilna / 106

8.7 Tokeny sprzętowe / 106

8.8 Inne / 106

8.9 Identyfikacja i uwierzytelnienie jako usługa bankowa / 107

8.10 Inne metody użycia danych bankowych / 110

ROZDZIAŁ 1.0

WSTĘP

Zachodzące w ostatnich latach zmiany w sposobie funkcjonowania banków i ich klientów szczególnie są widoczne w sposobie i rosnącej skali wykorzystania elektronicznych kanałów komunikacji. W tym zakresie ostatnie tygodnie wielokrotnie zwiększyły zarówno zainteresowanie jak i faktyczne użycie zdalnych kanałów dostępu zarówno do usług bankowych jak i innych dziedzin codziennego życie.

W tym kontekście szczególnego znaczenia nabiera kwestia właściwej identyfikacji, a następnie uwierzytelnienia użytkownika usług elektronicznych. Odpowiednie i wiarygodne mechanizmy potwierdzania tożsamości są kwestią krytyczną w obszarze bezpieczeństwa korzystania z kanałów zdalnych i realizowanych za ich pomocą usług.

Tematyka związana z identyfikowaniem i potwierdzaniem tożsamości obywateli i klientów cyfrowych znajduje coraz szersze odzwierciedlenie w licznych regulacjach prawnych zarówno na poziomie Unii Europejskiej jak i krajowym. Prawo w tym zakresie stara się nadążać za szybko zmieniającą się technologią w taki sposób, aby w maksymalny sposób zabezpieczyć i ograniczyć ryzyko nieuprawnionego korzystania z technologii cyfrowych. Rozporządzenia takie jak eIDAS czy PSD2 to sztandarowe przykłady określające ramy i standardy korzystania ze zdobyczy rozwiązań cyfrowych. Choć wiele aspektów zostało już prawnie i proceduralnie uregulowanych to nieustanny rozwój technologii nieustająco określa nowe potrzeby, które wymagają wyznaczania norm prawnych. Przykładem takiego obszaru jest wykorzystywanie biometrii.

Odpowiadając na tą zmieniającą się rzeczywistość pod patronatem Związku Banków Polskich przygotowany został przewodnik „Identyfikacja i uwierzytelnienie w usługach elektronicznych" będący praktycznym kompendium wiedzy na temat szeroko rozumianego potwierdzania tożsamości w usługach elektronicznych. Na przewodnik składają się zebrana terminologia, przegląd aktów prawnych, standardów oraz koncepcji uwierzytelniania jak również krótki opis praktycznych zastosowań w polskim sektorze bankowym.

Zaletą niniejszego przewodnika jest zebranie wraz z opisem w jednym miejscu szerokiego spektrum dostępnych rozwiązań dotyczących zdalnego potwierdzania tożsamości. Rozwiązania te prezentowane są z praktycznymi przykładami nie tylko polskimi ale także międzynarodowymi. Wszystko to zostało zaprezentowane w kontekście uregulowań prawnych obecnie obowiązujących z pokazaniem implikacji jakie te uregulowania niosą dla poszczególnych sposobów identyfikacji i uwierzytelnienia w kanałach elektronicznych.

Niewątpliwie rola i znaczenie kanałów elektronicznych będzie rosło w naszym życiu obejmując coraz to nowe obszary codziennego funkcjonowania. Łatwość z jaką możemy z nich korzystać musi iść w parze z odpowiednim i bezpiecznym sposobem ich użycia. Od tego zależeć będzie wiarygodność i skłonność do wykorzystywania usług zdalnych w bieżącym działaniu. Nie zapominajmy zatem o bezpieczeństwie. W tym ma także pomóc niniejszy przewodnik. Dobrej lektury.

Wojciech Pantkowski

Dyrektor Zespołu Systemów Płatniczych i Bankowości Elektronicznej

Związek Banków Polskich

ROZDZIAŁ 2.0

NOMENKLATURA POJĘCIOWA

Niniejszy rozdział został przygotowany na podstawie dokumentu „Opracowanie nomenklatury pojęciowej elektronicznej identyfikacji i usług zaufania", przygotowanego w ramach projektu Model krajowego schematu identyfikacji elektronicznej (eID) w Polsce z uwzględnieniem budowy państwowego brokera eID i wykorzystaniem usług zaufania, autorstwa: Miłosza Brakonieckiego, Tomasza Mielnickiego, Artura Miękiny, Michała Tabora, Daniela Wachnika.

identyfikacja elektroniczna

oznacza proces używania danych w postaci elektronicznej identyfikujących osobę, unikalnie reprezentujących osobę fizyczną lub prawną, lub osobę fizyczną reprezentującą osobę prawną;
[eIDAS art. 3 1)]

Zasadniczo jest to proces pozwalający na przekazanie danych identyfikujących do strony ufającej. W skrócie elektroniczną identyfikację nazywa się eID, mając na myśli nie tylko proces, ale także system lub środek identyfikacji. Zadaniem identyfikacji elektronicznej jest przekazanie danych identyfikujących osobę fizyczną, prawną lub osobę fizyczną reprezentującą osobę prawną na żądanie strony ufającej (zwanej w systemach identyfikacji usługodawcą). W przyjętym podejściu dostawca usługi identyfikacji jest adwersarzem procesu używania danych, dostarczając potwierdzenie (uwierzytelnienie) osoby posługującej się danymi identyfikującymi osobę.

środek identyfikacji elektronicznej

oznacza materialną lub niematerialną jednostkę zawierającą dane identyfikujące osobę i używaną do celów uwierzytelniania dla usługi online;
[eIDAS art. 3 2)]

Środek identyfikacji elektronicznej zawiera dane identyfikujące, np. Profil Zaufany, czy elektroniczny dowód tożsamości zawierający funkcję uwierzytelnienia. Środkiem identyfikacji elektronicznej w domenie publicznej (poza systemem identyfikacji elektronicznej) nie jest para login/hasło ponieważ nie zawiera danych identyfikujących, a jedynie dane dostępowe do środka identyfikacji elektronicznej, który znajduje się w systemie chronionym loginem i hasłem. Środek identyfikacji elektronicznej jest wydawany w ramach systemu (schematu) identyfikacji elektronicznej. Strony ufające będą otrzymywały dane identyfikujące osobę fizyczną, prawną, lub osobę reprezentującą osobę prawną w postaci krótkoterminowych środków identyfikacji elektronicznej wystawionych przez dostawcę tożsamości.

dane identyfikujące osobę

oznaczają zestaw danych umożliwiających ustalenie tożsamości osoby fizycznej lub prawnej, lub osoby fizycznej reprezentującej osobę prawną;
[eIDAS art. 3 pkt. 3)]

Dane identyfikujące osobę to zestaw danych, który jednoznacznie pozwala wskazać osobę fizyczną, prawną lub fizyczną reprezentującą osobę prawną. Danymi identyfikującymi osobę nie jest występujący samodzielnie numer telefonu o ile nie nastąpiło formalne powiązanie tego numeru z osobą – np. poprzez umowę, zobowiązanie itp. Na potrzeby krajowego schematu identyfikacji elektronicznej przyjęto, że danymi identyfikującymi osobę będą takie dane, które samodzielnie

(bez kontekstu systemowego) potrafią wskazać w sposób jednoznaczny konkretną osobę fizyczną lub prawną. W praktyce w Polsce jest to numer PESEL, a także numer dokumentu tożsamości.

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;
[eIDAS art. 3 pkt. 4)]

Należy przez słowo system rozumieć „schemat". Na ten schemat składa się wiele elementów m.in.: reguły, procedury, wymagania, dane, interfejsy, tokeny, systemy komputerowe. System identyfikacji elektronicznej wydaje środki identyfikacji elektronicznej i zapewnia obsługę procesu uwierzytelniania, tak aby strona ufająca mogła polegać na identyfikacji elektronicznej. Przykładowo, jeżeli schemat identyfikacji jest oparty o kartę dowodu osobistego to system identyfikacji elektronicznej obejmuje – procesy rejestracji związane z wnioskowaniem i wydawaniem dowodów, systemy bazodanowe obejmujące bazy osób, wydanych dowodów osobistych oraz bazę unieważnionych dowodów osobistych oraz system pozwalający na przeprowadzenie procesu uwierzytelnienia on-line w usługach wykorzystujących ten dowód.

uwierzytelnianie

oznacza proces elektroniczny, który umożliwia identyfikację elektroniczną osoby fizycznej lub prawnej, lub potwierdzenie pochodzenia oraz integralności weryfikowanych danych w postaci elektronicznej;
[eIDAS art. 3 pkt. 5)]

Uwierzytelnianie to proces, który jest realizowany przez stronę ufającą lub w imieniu strony ufającej, którego celem jest zapewnienie wiarygodności środków identyfikacji elektronicznej lub danych w postaci elektronicznej (np. podpisanego dokumentu elektronicznego lub opatrzenie pieczęcią elektroniczną).

Należy tu wyróżnić różne procesy uwierzytelniania:
• Uwierzytelnianie realizowane przez dostawcę tożsamości, który przed uwolnieniem danych identyfikujących osobę na podstawie żądania strony ufającej (usługodawcy) musi potwierdzić, na podstawie przyjętych w danym schemacie identyfikacji elektronicznej metod, że działa na podstawie i za zgodą osoby, której dane dotyczą.
• Uwierzytelnianie realizowane przez stronę ufającą mające na celu potwierdzenie, że może polegać na otrzymanych danych identyfikujących osobę (np. weryfikacja pieczęci pod danymi).
• Uwierzytelnianie realizowane przez stronę ufającą potwierdzające że może polegać na podpisie lub pieczęci elektronicznej.

W praktyce obecnie uwierzytelnie najczęściej występuje w systemach zamkniętych. Tzn. np. bank uwierzytelnia klienta na potrzeby dostępu tego klienta do usług bankowych oferowanych przez siebie. Dostawca tożsamości jest jednocześnie stroną ufającą.

strona ufająca

oznacza osobę fizyczną lub prawną, która polega na identyfikacji elektronicznej lub usłudze zaufania;
[eIDAS art. 3 pkt. 6)]

Stroną ufającą jest odbiorca uwierzytelnionej lub podpisanej informacji, bazujący na domniemaniu rzetelności dostawcy usług identyfikacji elektronicznej jak i usług zaufania. Strona ufająca powinna być szczególnie chroniona prawnie, ponieważ ona ponosi główne ryzyko związane z nierzetelnym działaniem usług.

W szczególności jest to osoba, która polega na wydanych przez dostawcę tożsamości środkach identyfikacji elektronicznej.

W kontekście identyfikacji elektronicznej strona ufająca będzie definiowana jako usługodawca – dostawca usługi bazującej na identyfikacji elektronicznej (np. podmiot publiczny świadczący e-usługi, sklep internetowy)

W przypadku usług zaufania „strona ufająca" to ta, która jest odbiorcą dokumentu z podpisem elektronicznym lub pieczęcią elektroniczną, gdzie zaufanie do podpisu lub pieczęci jest elementem jej procesu biznesowego.

Stroną ufającą jest także osoba korzystająca bezpośrednio z usługi zaufania
i oczekująca, że wynik tej usługi będzie zgodny z jej definicją – np. osoba korzystająca z usługi walidacji podpisu elektronicznego oczekuje, że walidacja potwierdzi ważność podpisu elektronicznego zapewniając bezpieczeństwo strony ufającej.

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;
[eIDAS art. 3 pkt. 7)]

Rozporządzenie eIDAS nakłada szereg obowiązków związanych z akceptacją identyfikacji elektronicznej, rozpoznawaniem podpisów, pieczęci i znaczników czasu przez podmioty sektora publicznego.

W preambule eIDAS pojawia się wielokrotnie także odwołanie do sektora prywatnego. Niniejsza definicja ma zapewnić odróżnienie sektora publicznego od prywatnego. W treści eIDAS następuje odwołanie do podmiotów innych niż podmioty sektora publicznego w zakresie modelu płatności za usługi identyfikacji elektronicznej.

podmiot prawa publicznego

oznacza podmiot zdefiniowany w art. 2 ust. 1 pkt 4 dyrektywy Parlamentu Europejskiego i Rady 2014/24/UE [eIDAS art. 3 pkt. 8)]

Podmiot prawa publicznego to podmiot, który posiada wszystkie poniższe cechy:
a) został utworzony w konkretnym celu zaspokajania potrzeb w interesie ogólnym, które nie mają charakteru przemysłowego ani handlowego;

b) posiada osobowość prawną; oraz
c) jest finansowany w przeważającej części przez państwo, władze regionalne lub lokalne lub inne podmioty prawa publicznego; bądź jego zarząd podlega nadzorowi ze strony tych władz lub podmiotów; bądź ponad połowa członków jego organu administrującego, zarządzającego lub nadzorczego została wyznaczona przez państwo, władze regionalne lub lokalne, lub przez inne podmioty prawa publicznego;

podpisujący

oznacza osobę fizyczną, która składa podpis elektroniczny;
[eIDAS art. 3 pkt. 9)]

Zgodnie z eIDAS podpis elektroniczny może być złożony jedynie przez osobę fizyczną. Komplementarną definicją jest definicja „składającego pieczęć elektroniczną".

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 art. 3 pkt. 10)]

Definicja podpisu elektronicznego jest bardzo szeroka i zapewnia neutralność technologiczną. Najważniejszym elementem definicji podpisu elektronicznego jest jego postać elektroniczna, oraz cel wykonania podpisu elektronicznego (intencja podpisującego), jakim jest podpisanie dokumentu lub treści. Definicja ta nie ogranicza podpisów do technik kryptograficznych, ani nie uzależnia uznania danych elektronicznych za podpis od cech technicznych lub funkcjonalnych, np. zapewnienia integralności lub autentyczności. W szczególności podpisem, zgodnie z tą definicją, jest imię i nazwisko umieszone przez podpisującego pod wiadomością poczty elektronicznej, użyte tam jako podpis. W takiej sytuacji wymaganiem weryfikacji tego dowodu może być weryfikowanie autentyczności i integralności takiej wiadomości.

zaawansowany podpis elektroniczny

oznacza podpis elektroniczny, który spełnia wymogi określone w art. 26;
[eIDAS art. 3 pkt. 11)]

Zaawansowany podpis elektroniczny to taki, który:
a) jest unikalnie przyporządkowany podpisującemu;
b) umożliwia ustalenie tożsamości podpisującego;
c) jest składany przy użyciu danych służących do składania podpisu elektronicznego, których podpisujący może, z dużą dozą pewności, użyć pod wyłączną swoją kontrolą; oraz
d) jest powiązany z danymi podpisanymi w taki sposób, że każda późniejsza zmiana danych jest rozpoznawalna.

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;
[eIDAS art. 3 pkt. 12)]

Uznanie podpisu elektronicznego za podpis elektroniczny kwalifikowany wymaga spełnienia przez niego łącznie następujących cech:
• jest podpisem zaawansowanym;
• jest składany za pomocą kwalifikowanego urządzenia do podpisu elektronicznego;
• opiera się na kwalifikowanym certyfikacie.
Kwalifikowanemu podpisowi elektronicznemu eIDAS przypisuje takie same skutki prawne jak podpisowi własnoręcznemu.

Uwaga! eIDAS wskazuje także na podpisy zaawansowane weryfikowane kwalifikowanym certyfikatem, które nie są kwalifikowanymi podpisami, gdyż nie są składane za pomocą kwalifikowanego urządzenia do podpisu elektronicznego.

dane służące do składania podpisu elektronicznego

oznaczają unikalne dane, których podpisujący używa do składania podpisu elektronicznego;
[eIDAS art. 3 pkt. 13)]

eIDAS nie definiuje czym są dane służące do składania podpisu elektronicznego. W przypadku podpisu zwykłego to może być np. ciąg liter. W przypadku podpisów opartych o kryptografię asymetryczną są to klucze kryptograficzne przechowywane w bezpiecznym urządzeniu

(karta kryptograficzna, HSM). W przypadku innych podpisów dane te mogą zawierać inne informacje, np. bazować na środkach identyfikacji elektronicznej, tj. danymi do złożenia podpisu zaufanego są między innymi dane zawarte w Profilu Zaufanym.

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;
[eIDAS art. 3 pkt. 14)]

Certyfikat jest rozwiązaniem zapewniającym zidentyfikowanie podpisującego poprzez wskazanie danych podpisującego (pseudonim lub imię i nazwisko) oraz wiążących dane pozwalające na weryfikację podpisu z podpisującym. Certyfikat podpisu elektronicznego służy do weryfikacji podpisu. Dostawca usługi zaufania wydawania certyfikatów podpisu elektronicznego posiada dane pozwalające na jednoznaczne zidentyfikowanie podpisującego nawet jeżeli certyfikat wskazuje pseudonim lub nie zawiera danych jednoznacznie identyfikujących podpisującego. Certyfikat elektroniczny zazwyczaj wydawany jest w formacie x.509

kwalifikowany certyfikat podpisu elektronicznego

oznacza certyfikat podpisu elektronicznego, który jest wydawany przez kwalifikowanego dostawcę usług zaufania i spełnia wymogi określone w załączniku I;
[eIDAS art. 3 pkt. 15)]

Wymogi dla kwalifikowanych certyfikatów podpisów elektronicznych określa Załącznik Nr I stanowiący integralną część rozporządzenia eIDAS 910/2014.

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;

[eIDAS art. 3 pkt. 16)]

Usługi zaufania nie stanowią listy zamkniętej i mogą być rozszerzane o inne usługi wykraczające poza zamknięty katalog. O otwartości tego katalogu świadczą motywy 25 i 26 preambuły eIDAS. Jednakże transgranicznie eIDAS wprowadza tylko zamknięty katalog usług zaufania, pozostawiając możliwość definiowania nowych usług na poziomie krajowym.

Usługi zaufania są realizowane przez dostawcę usługi, który ponosi odpowiedzialność za ich działanie zgodnie z polityką świadczenia usługi zaufania. Rozporządzenie nakłada szczególną odpowiedzialność na dostawców usług zaufania. Obecnie najbardziej znane w Polsce usługi zaufania (występujące pod nazwą usługi certyfikacyjne) to wydawanie certyfikatów oraz znakowanie czasem. Świadczenie tych usług nie zmienia się z wejściem w życie nowego prawa. Rozporządzenie eIDAS rozszerza katalog usług zaufania, jak wskazuje sama definicja. Za świadczeniem usług zaufana występuje odpowiedzialność i zazwyczaj odpłatność.

kwalifikowana usługa zaufania

oznacza usługę zaufania, która spełnia stosowne wymogi określone w niniejszym rozporządzeniu;
[eIDAS art. 3 pkt 17)]

Kwalifikowana usługa zaufania musi być świadczona przez kwalifikowanego dostawcę usług zaufania. Kwalifikowana usługa zaufania spełnia standardy określone w rozporządzeniu eIDAS oraz aktach implementujących eIDAS. Kwalifikowane usługi zaufania w kontekście eIDAS stanowią zamknięty katalog usług rozpoznawalnych pomiędzy krajami Unii Europejskiej. Kwalifikowane usługi zaufania korzystają z tzw. domniemania skuteczności prawnej, tzn. przyjmuje się, że wynik kwalifikowanej usługi zaufania jest rzetelny i ciężar dowodu odwrotnego spoczywa na stronie kwestionującej tę jakość. Każdy kraj członkowski może tworzyć tzw. kwalifikowane krajowe usługi zaufania, które mogą korzystać ze szczególnych przywilejów i warunków bezpieczeństwa na poziomie krajowym, ale nie muszą być uznawane pomiędzy krajami członkowskimi.

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;
[eIDAS art. 3 pkt 18)]

Ocena zgodności jest jednym z warunków uzyskania statusu kwalifikowanej usługi zaufania. Dostawcy usług mogą korzystać z krajowych lub zagranicznych jednostek oceniających zgodność. W Polsce obecnie brak jest takich jednostek, które zgodnie z normą EN 319403, mogłyby dokonać takiego audytu zgodności. Norma ta stawia wysokie wymagania dla m.in. w zakresie kompetencji personelu takiej jednostki.

dostawca usług zaufania

oznacza osobę fizyczną lub prawną, która świadczy przynajmniej jedną usługę zaufania, jako kwalifikowany lub niekwalifikowany dostawca usług zaufania;
[eIDAS art. 3 pkt 19)]

Dostawca usług zaufania stanowi zaufaną stronę trzecią zarówno dla osoby bezpośrednio korzystającej z usługi, jak i dla strony ufającej. W tym zakresie dostawcą usługi zaufania nie powinien być podmiot zabezpieczający transakcje na własne potrzeby. Rozporządzenie eIDAS nakłada szczególne wymagania jakościowe na świadczenie usług zaufania, niezależnie od tego czy są to usługi kwalifikowane, czy nie. Dostawcą usługi zaufania są np.: centra certyfikacji wydające certyfikaty lub świadczące usługi znakowania czasem. Przy czym należy pamiętać, że wymagania eIDAS nie dotyczą zamkniętych systemów.

kwalifikowany dostawca usług zaufania

oznacza dostawcę usług zaufania, który świadczy przynajmniej jedną kwalifikowaną usługę zaufania i któremu status kwalifikowany nadał organ nadzoru;
[eIDAS art. 3 pkt 20)]

Aktualnie w Polsce funkcjonuje 5 centrów certyfikacji wydających kwalifikowane certyfikaty. Na mocy eIDAS, od 1 lipca 2016 r., przez rok będą one dostawcami usług zaufania w zakresie wydawania kwalifikowanych certyfikatów podpisu elektronicznego. Rozpoczęcie świadczenia pozostałych kwalifikowanych usług zaufania wymaga audytu i rejestracji zgodnie z eIDAS w organie nadzoru.

produkt

oznacza sprzęt lub oprogramowanie lub odpowiednie komponenty sprzętu lub oprogramowania, które są przeznaczone do wykorzystania w świadczeniu usług zaufania;
[eIDAS art. 3 pkt 21)]

Może to być sprzęt lub oprogramowanie dla użytkownika końcowego lub też elementy środowiska dostawcy usług zaufania.

urządzenie do składania podpisu elektronicznego

oznacza skonfigurowane oprogramowanie lub skonfigurowany sprzęt, które wykorzystuje się do składania podpisu elektronicznego;
[eIDAS art. 3 pkt 22)]

Urządzeniem do składania podpisu elektronicznego jest w szczególności kara kryptograficzna. Rozporządzenie dopuszcza również alternatywnie, aby takim urządzeniem była np. aplikacja na telefonie komórkowym lub komputerze.

kwalifikowane urządzenie do składania podpisu elektronicznego

oznacza urządzenie do składania podpisu elektronicznego, które spełnia wymogi określone w załączniku II;
[eIDAS art. 3 pkt 23)]

Załącznik, stanowiący integralną część rozporządzenia eIDAS 910/2014, określa wymogi dla kwalifikowanych urządzeń do składania podpisu elektronicznego. Kwalifikowane urządzenie zabezpiecza dane służące do składania podpisu elektronicznego w całym cyklu ich życia tj. od momentu generacji, poprzez użycie, aż do zniszczenia. Kwalifikowane urządzenie do składania podpisu elektronicznego jest niezbędne do złożenia kwalifikowanego podpisu elektronicznego, który jest równoważny podpisowi odręcznemu.

podmiot składający pieczęć

oznacza osobę prawną, która składa pieczęć elektroniczną;
[eIDAS art. 3 pkt 24)]

Pieczęć elektroniczna jest przypisana do osoby prawnej, która jest źródłem pochodzenia pieczęci. Osoba prawna jako składający pieczęć powinna być rozumiana szeroko, w tym zakresie zastosowanie ma zapis motywu 68 preambuły eIDAS wskazujący, że jako „osoba prawna" należy rozumieć wszystkie podmioty ustanowione na mocy prawa niezależnie od ich formy prawnej.

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;
[eIDAS art. 3 pkt 25)]

Pieczęć elektroniczna nie jest podpisem elektronicznym osoby prawnej, nie jest także substytutem podpisu własnoręcznego osoby fizycznej. Na mocy eIDAS znaczenie prawne pieczęci ogranicza się do potwierdzenia autentyczności i integralności oznaczonego dokumentu. Natomiast skutki prawne pieczęci elektronicznej muszą zostać określone w osobnym przepisie prawa, umowie, oświadczaniu lub dokumentach wewnętrznych. Przykładem jest zapisane w eIDAS pieczęci elektronicznej do usługi zaufania znakowania czasem, które buduje zobowiązanie dostawcy tej usługi i stanowi dowód w postaci znacznika czasu.

zaawansowana pieczęć elektroniczna

oznacza pieczęć elektroniczną, która spełnia wymogi określone w art. 36;
[eIDAS art. 3 pkt 26)]

Zaawansowana pieczęć elektroniczna to taka pieczęć elektroniczna, która:
a) jest unikalnie przyporządkowana podmiotowi składającemu pieczęć;
b) umożliwia ustalenie tożsamości podmiotu składającego pieczęć;
c) jest składana przy użyciu danych służących do składania pieczęci elektronicznej, które podmiot składający pieczęć może, mając je z dużą dozą pewności pod swoją kontrolą, użyć do złożenia pieczęci elektronicznej; oraz
d) jest powiązana z danymi, do których się odnosi w taki sposób, że każda późniejsza zmiana danych jest rozpoznawalna.

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; [eIDAS art. 3 pkt 27)]

W Polsce nie były jeszcze świadczone takie usługi. Kwalifikowana pieczęć elektroniczna powinna mieć zastosowanie dla następujących obszarów usług administracji publicznej:

- automatyczne wydawanie odpisów z rejestrów i ewidencji;
- automatyczne potwierdzanie doręczeń;
- automatyczne potwierdzanie stanu lub działania;
- automatyczne potwierdzanie realizacji procesu biznesowego;
- zabezpieczanie dokumentacji występującej w systemach informacyjnych urzędów w momencie ich wyjścia na zewnątrz.

dane służące do składania pieczęci elektronicznej

oznaczają niepowtarzalne dane, które podmiot składający pieczęć wykorzystuje do złożenia pieczęci elektronicznej;
[eIDAS art. 3 pkt 28)]

eIDAS nie definiuje czym są dane służące do składania pieczęci elektronicznej. W szczególności może to być identyfikator umieszczany przez składającego pieczęć – tak jak to ma miejsce w przypadku wydawania odpisów KRS. W przypadku pieczęci opartych o kryptografię asymetryczną są to najczęściej klucze kryptograficzne przechowywane w bezpiecznym urządzeniu (karta kryptograficzna, HSM).

certyfikat pieczęci elektronicznej

oznacza poświadczenie elektroniczne, które łączy dane służące do walidacji pieczęci elektronicznej z osobą prawną i potwierdza nazwę tej osoby;
[eIDAS art. 3 pkt 29)]

Certyfikat pieczęci elektronicznej spełnia takie same wymagania jak certyfikat podpisu elektronicznego, nie ma także różnic w zakresie stosowanej technologii dla certyfikatów pieczęci.

kwalifikowany certyfikat pieczęci elektronicznej

oznacza certyfikat pieczęci elektronicznej, który jest wydawany przez kwalifikowanego dostawcę usług zaufania i spełnia wymagania określone w załączniku III;
[eIDAS art. 3 pkt 30)]

Załącznik III stanowiący integralną część rozporządzenia eIDAS 910/2014 określa wymogi dla kwalifikowanych certyfikatów pieczęci elektronicznej.

urządzenie do składania pieczęci elektronicznej

oznacza skonfigurowane oprogramowanie lub skonfigurowany sprzęt, które wykorzystuje się do składania pieczęci elektronicznej;
[eIDAS art. 3 pkt 31)]

Urządzeniem do składania podpisu elektronicznego jest w szczególności kara kryptograficzna lub urządzenie HSM. Rozporządzenie dopuszcza alternatywnie aby takim urządzeniem była np. aplikacja na serwerze firmowym, który dokonuje takiego poświadczenia.

kwalifikowane urządzenie do składania pieczęci elektronicznej

oznacza urządzenie do składania pieczęci elektronicznej, które spełnia odpowiednio wymogi określone w załączniku II;
[eIDAS art. 3 pkt 32)]

Załącznik II stanowiący integralną część rozporządzenia eIDAS 910/2014 określa wymogi dla kwalifikowanych urządzeń do składania podpisu elektronicznego.

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;
[eIDAS art. 3 pkt 33)]

Elektroniczny znacznik czasu potwierdza, że dane nim opatrzone istniały w momencie znakowania. Znacznik czasu zapewnia integralność dokumentu od momentu znakowania, a także potwierdza w przypadku znakowania podpisanego dokumentu, że podpis elektroniczny został złożony przed momentem znakowania czasem.

kwalifikowany elektroniczny znacznik czasu

oznacza elektroniczny znacznik czasu, który spełnia wymogi określone w art. 42;
[eIDAS art. 3 pkt 34)]

Kwalifikowany elektroniczny znacznik czasu to elektroniczny znacznik czasu, który:
a) wiąże datę i czas z danymi tak, aby w wystarczający sposób wykluczyć możliwość niewykrywalnej zmiany danych;
b) oparty jest na precyzyjnym źródle czasu powiązanym z uniwersalnym czasem koordynowanym; oraz
c) jest podpisany przy użyciu zaawansowanego podpisu elektronicznego lub opatrzony zaawansowaną pieczęcią elektroniczną kwalifikowanego dostawcy usług zaufania lub w inny równoważny sposób.

dokument elektroniczny

oznacza każdą treść przechowywaną w postaci elektronicznej, w szczególności tekst lub nagranie dźwiękowe, wizualne lub audiowizualne;
[eIDAS art. 3 pkt 35)]

eIDAS będąc prawem nadrzędnym w stosunku do prawa krajowego i mający zastosowanie bezpośrednie w prawie krajowym ustanawia obowiązującą definicję dokumentu elektronicznego. Niezależnie przewiduje się, że od września 2016 roku w kodeksie cywilnym będzie obowiązywała nowa definicja dokumentu. Dla dokumentów zidentyfikowanych jako elektroniczne zastosowanie będzie miała definicja pochodząca z rozporządzenia eIDAS.

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 jakiejkolwiek nieupoważnionej zmiany;
[eIDAS art. 3 pkt 36)]

Usługa taka jest świadczona przez stronę trzecią, co oznacza, że nie może być realizowana przez urząd lub inny podmiot na rzecz komunikacji ze swoimi klientami. Realizacja usługi przez stronę trzecią zapewnia niezależne źródło dowodu i skutek prawny wysłania i otrzymania danych przekazanych za pomocą usługi rejestrowanego doręczenia elektronicznego. Usługa doręczenia zapewnia ochronę danych przed utratą integralności i poufności – gwarantuje bezpieczeństwo.

kwalifikowana usługa rejestrowanego doręczenia elektronicznego

oznacza usługę rejestrowanego doręczenia elektronicznego, która spełnia wymogi określone w art. 44;
[eIDAS art. 3 pkt 37)]

Kwalifikowana usługa rejestrowanego doręczenia elektronicznego to usługa rejestrowanego doręczenia elektronicznego, która:
a) jest świadczona przez co najmniej jednego kwalifikowanego dostawcę usług zaufania;
b) z dużą dozą pewności zapewniają identyfikację nadawcy;
c) zapewnia identyfikację adresata przed dostarczeniem danych;
d) wysłanie i otrzymanie danych jest zabezpieczone zaawansowanym podpisem elektronicznym lub zaawansowaną pieczęcią elektroniczną kwalifikowanego dostawcy usług zaufania w taki sposób, by wykluczyć możliwość niewykrywalnej zmiany danych;
e) każda zmiana danych niezbędna do celów wysłania lub otrzymania danych jest wyraźnie wskazana nadawcy i adresatowi danych;
f) data i czas wysłania, otrzymania i wszelkiej zmiany danych są wskazane za pomocą kwalifikowanego elektronicznego znacznika czasu.

W przypadku przesyłania danych między co najmniej dwoma kwalifikowanymi dostawcami usług zaufania wymogi określone w lit. a)–f) mają zastosowanie do wszystkich kwalifikowanych dostawców usług zaufania.

certyfikat uwierzytelniania witryn internetowych

oznacza poświadczenie, które umożliwia uwierzytelnianie witryn internetowych i przyporządkowuje witrynę internetową do osoby fizycznej lub prawnej, której wydano certyfikat;
[eIDAS art. 3 pkt 38)]

Celem wprowadzenia certyfikatu uwierzytelniania witryn internetowych jest zbudowanie jednolitych w UE podstaw prawnych do stosowanych obecnie certyfikatów SSL.

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;
[eIDAS art. 3 pkt 39)]

Wprowadzone w eIDAS kwalifikowane certyfikaty uwierzytelniania witryn internetowych nie mają skutków prawnych leżących w eIDAS, natomiast zostały określone szczegółowe wymogi dla takich certyfikatów. Jednym z najważniejszych elementów Kwalifikowanego Certyfikatu Uwierzytelniania Witryn Internetowych jest jawne wpisanie w certyfikacie osoby fizycznej lub prawnej, której wydano certyfikat.

dane służące do walidacji

oznaczają dane używane do walidacji podpisu elektronicznego lub pieczęci elektronicznej; [eIDAS art. 3 pkt 40)]

W szczególności dane służące do walidacji są zawarte w certyfikacie podpisu lub pieczęci elektronicznej.

walidacja

oznacza proces weryfikacji i potwierdzenia ważności podpisu elektronicznego lub pieczęci. [eIDAS art. 3 pkt 41)]

Walidacja jest procesem formalnym zapewniającym potwierdzenie ważności podpisu lub pieczęci elektronicznej. Walidacja kwalifikowanych podpisów potwierdza ważność kwalifikowanego podpisuw sposób jednoznaczny. Walidacja realizowana z wykorzystaniem kwalifikowanej usługi walidacji kwalifikowanych podpisów lub kwalifikowanych pieczęci elektronicznych umożliwia stronie ufającej otrzymanie wyniku procesu walidacji.

węzeł transgraniczny (eIDAS Node)

zgodnie z rozporządzeniem wykonawczym Komisji 1501/2015, węzeł oznacza punkt przyłączenia będący częścią architektury systemu interoperacyjności identyfikacji elektronicznej, który jest wykorzystywany w procesie transgranicznego uwierzytelniania osób i który ma zdolność do rozpoznawania i przetwarzania lub przesyłania danych do innych węzłów poprzez umożliwienie sprzężenia krajowej infrastruktury identyfikacji elektronicznej jednego państwa członkowskiego z krajowymi infrastrukturami służącymi do identyfikacji elektronicznej innych państw członkowskich. [Rozp. 1501/2015]

Węzeł transgraniczny - eIDAS Node powstał w Instytucie Maszyn Matematycznych (IMM) w oparciu dorobek Connected Europe Freamework i produkty projektu transgranicznych cyfrowych usług publicznych STORK 2.0 (Secure Identity Across Borders Linked), w którego ramach wypracowano modele interoperacyjności czyli współpracy ze sobą różnych krajowych systemów informatycznych. W ramach projektu wypracowano m.in sfederowany model uwierzytelnienia i identyfikacji umożliwiający federację systemów dostawców tożsamości – model PEPS (Pan-European Proxy Services – Paneuropejskie usługi pośredniczące).

węzeł krajowy identyfikacji elektronicznej (węzeł krajowy)

[Ustawa o usługach zaufania Art. 21a]
rozwiązanie organizacyjno-techniczne umożliwiające uwierzytelnianie użytkownika systemu teleinformatycznego, korzystającego z usługi online, z wykorzystaniem środka identyfikacji elektronicznej wydanego w systemie identyfikacji elektronicznej przyłączonym do tego węzła bezpośrednio albo za pośrednictwem węzła transgranicznego. Funkcjonowanie węzła krajowego zapewnia minister właściwy do spraw informatyzacji.

Rozwiązanie, które pełni główną rolę zarządczą w sfederowanym modelu tożsamości w Polsce w zakresie uwierzytelniania w systemach admnistracji publicznej, w szczególności będzie skupiał wszystkie zgłoszone systemy identyfikacji w Polsce, a także będzie pośrednikiem między brokerami komercyjnymi a węzłem eIDAS Node

komercyjny węzeł identyfikacji

[Definicja ekspercka]

Punkt pośredniczący między systemami dostawców tożsamości a systemami podmiotów ufających danym tych systemów. Węzeł identyfikacji zapewnia techniczne interfejsy z dostawcami tożsamości oraz podmiotami ufającymi z wykorzystaniem kanałów zdalnych oraz rozliczalność transakcji uwierzytelnienia.

dostawca usługi

[Definicja ekspercka]

Dostawca usługi ang. Service Provider (SP) to system, rozwiązanie lub rola, która oferuje zdalną usługę użytkownikom w Internecie (inną niż identyfikacja i uwierzytelnienie). Dostawca usługi, na potrzeby realizowanych przez siebie usług, korzysta z mechanizmów pozwalających na identyfikację elektroniczną klientów. Dostawcą usługi może być podmiot publiczny lub prywatny, w szczególności są to: systemy e-administracji, sklepy internetowe lub portale usługowe.

dostawca atrybutów

[Definicja ekspercka]

Dostawca atrybutów ang. Attribute Provider (AP). Podmiot odpowiedzialny za dostarczanie brakujących i wymaganych atrybutów wykorzystywanych do świadczenia usługi zaufania. Potwierdzenie ich udostępnienia wykonywane jest w procesie identyfikacji elektronicznej. Dostawcami atrybutów są np. rejestry państwowe, w tym system KRS.

dostawca tożsamości / środka identyfikacji elektronicznej

[Definicja ekspercka]

Dostawca tożsamości – (w skrócie dostawca eID/ dostawca tożsamości/Identity Provider IdP) – podmiot odpowiedzialny za rejestrację osób i wydawanie im środków identyfikacji elektronicznej, uwalnianie danych potwierdzających tożsamości klientów dostawcy tożsamości.

Identity Provider (IDP). Podmiot zarządzający tożsamością i dostarczający osobie środki identyfikacji elektronicznej. Wydaje środki identyfikacji na określonych poziomach bezpieczeństwa (zaufania). Np. Ministerstwo Cyfryzacji wydające Profil Zaufany, czy bank wydający środki eID swoim klientom lub w inny sposób potwierdzający tożsamość swoich klientów na rynku komercyjnym.

dostawca usługi uwierzytelnienia

[Definicja ekspercka]

Podmiot odpowiedzialny realizujący proces uwierzytelnienia – zapewniający mechanizm chroniący dostępu dla użytkownika za pomocą haseł, kluczy, tokenów lub kart kryptograficznych.

poziom bezpieczeństwa (zaufania/wiarygodności)

poziomy bezpieczeństwa zgodnie z art. 8 rozporządzenia eIDAS.
[eIDAS art. 8]

Tzw. Level of Assurance. Poziomy te określają wiarygodność środka identyfikacji elektronicznej – zapewniając tym samym wymagane warunki ochrony. Rozporządzenie eIDAS określa 3 poziomy wiarygodności: niski (low), średni (substantial) i wysoki (high), przypisując każdemu z nich konkretne warunkach ochrony. Zastosowanie przez usługodawcę środków identyfikacji elektronicznej, opartych o jeden z wyżej wymienionych poziomów wiarygodności, powinno zostać poprzedzone analizą ryzyka.

identyfikowana osoba

[Definicja ekspercka]
Osoba fizyczna, osoba prawna lub osoba fizyczna reprezentująca osobę prawną, której dane są przekazywane w procesie identyfikacji elektronicznej. W niektórych opracowaniach stosowana jest nazwa – „Podmiot identyfikacji elektronicznej”

ROZDZIAŁ 3.0

STRESZCZENIE

Opracowanie „Identyfikacja i uwierzytelnianie w usługach elektronicznych", przygotowane z inicjatywy Forum Technologii Bankowych oraz Rady Bankowości Elektronicznej, ma za zadanie opisać w syntetyczny sposób problemy związane z tytułowymi obszarami, szczególnie w kontekście usług bankowych. Na przewodnik składa się: uporządkowana terminologia, przegląd przepisów prawa, standardów oraz koncepcji uwierzytelniania, a także krótki opis praktycznych zastosowań w polskim sektorze bankowym. W rozdziale poświęconym standardom, skupiono się na opisaniu podstaw prawnych, technicznych oraz znaczeniu standaryzacji dla rozwoju usług zaufania. Wskazano normy międzynarodowe, rekomendacje na poziomie Unii Europejskiej oraz krajowe, mające wpływ na świadczenie tego typu usług. Osią dla funkcjonowania usług zaufania w UE jest z pewnością rozporządzenie eIDAS, definiujące m.in.: zasady dotyczące podpisu elektronicznego oraz pieczęci elektronicznej, znakowanie czasem a także ich walidacji. eIDAS, wzbogacony o regulacje narodowe oraz standardy, opracowywane przez European Telecommunications Standards Institute (ETSI) oraz Connecting Europe Facility, normę ISO 29115, tworzy ramy dla rozwiązań stosowanych w różnych sektorach działalności, w tym publicznym i finansowym. Spójność systemów zarządzania identyfikacją, tożsamością oraz federacją tych tożsamości, zapewniana jest przez amerykański standard NIST SP 800-63, który jest rozpoznawany i wykorzystywany globalnie.

Przegląd koncepcji uwierzytelniania pozwala ustrukturyzować wiedzę na temat procesów i zasadniczych podziałów czynników uwierzytelniania, co staje się niezwykle istotne, np. w kontekście dyrektywy PSD2, posługującej się kategoriami wiedzy, posiadania oraz cechy. Właściwa definicja oraz zrozumienie tych kategorii to podstawa opracowania dobrze działających schematów silnego uwierzytelniania (tzw. SCA, Strong Customer Authentication) dla usług bankowości elektronicznej. W rozdziale opisano także mechanizmy oparte o uwierzytelnianie kryptograficzne, symetryczne i asymetryczne, aspekty losowości w kontekście haseł jednorazowych oraz bezpieczne protokoły komunikacyjne (SSL/TLS). Szczególną uwagę zwrócono na uwierzytelnianie biometryczne, prezentując jego dokładną charakterystykę oraz obszary zastosowań. Wspomniano także o uwierzytelnianiu proceduralnym oraz różnych przypadkach uwierzytelniania opartego o wiedzę, w tym m.in. w oparciu o dane bankowe właściciela rachunku – co znalazło np. zastosowanie w Profilu Zaufanym w Polsce. Poruszono problem zdalnego potwierdzania tożsamości wraz z opisem dostępnych rozwiązań w tym zakresie.

Wśród rozwiązań technicznych opisano m.in.: karty elektroniczne, kwalifikowane urządzenia, narodowe dokumenty tożsamości. Wyróżniono mechanizmy CAP/DPA, 3D Secure oraz stosowane powszechnie hasła jednorazowe czy notyfikacje push w aplikacjach mobilnych.

W rozdziale dotyczącym aspektów prawnych omówiono w szczególności polskie regulacje oraz implikacje z nich wynikające dla wdrażania procesów identyfikacji i uwierzytelniania w kanałach zdalnych.

Ostatni rozdział opracowania pokazuje przegląd rozwiązań z obszaru identyfikacji i uwierzytelniania stosowanych przez polskie banki, w tym także z obszaru usług publicznych (Profil Zaufany, rejestracja firmy w CEIDG).

Przewodnik będzie podlegał okresowym aktualizacjom, w przypadku zmian regulacyjnych oraz istotnych zmian rynkowych.

ROZDZIAŁ 4.0

IDENTYFIKACJA I UWIERZYTELNIENIE W STANDARDACH

Istnieje szereg uregulowań i standardów technicznych definiujących kwestie dotyczące identyfikacji, uwierzytelnienia oraz usług wspierających te procesy. W niniejszym rozdziale postaramy się wskazać zarówno podstawy prawne oraz standaryzacyjne dla stosowania mechanizmów zabezpieczających transakcje realizowane na odległość. Omówimy m.in.: obszar stosowania podpisów i pieczęci elektronicznych, identyfikacji elektronicznej oraz zastosowania różnego rodzaju mechanizmów uwierzytelniania. Zakres standaryzacji jest bardzo szeroki, począwszy od norm międzynarodowych, poprzez rekomendacje krajowe, a kończąc na aktach prawnych. Wszystkie te dokumenty częściowo się pokrywają, a częściowo uzupełniają. Celem niniejszego raportu jest przedstawienie syntezy tych opracowań i stworzenie jednego wspólnego wzorca jako kompletu dobrych praktyk, które powinny być brane pod uwagę przy budowie, obsłudze i utrzymaniu systemów zaufania, jakimi są systemy dostawców tożsamości, usług uwierzytelnienia elektronicznego, dostawców usług zaufania, a także szeroko pojętych systemów dostawców usług elektronicznych.

Najważniejszymi dokumentami, na których opiera się niniejszy raport, są:
1. akty prawne związane z podpisem elektronicznym, w szczególności:
• rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 910/2014 w sprawie identyfikacji elektronicznej i usług zaufania w odniesieniu do transakcji na rynku wewnętrznym oraz uchylające dyrektywę 1999/93/WE,
• ustawa z dnia 5 września 2016 r. o usługach zaufania oraz identyfikacji elektronicznej (Dz. U. 2016 poz.159 z poz. zm.),
• ustawa z dnia 6 sierpnia 2010 r. o dowodach osobistych (Dz.U. 2010 nr 167 poz 1131 z poz. zn.),
• ustawa z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (Dz. U. z 2017 r. poz. 570 z poz. zm).
2. dokumenty wytworzone w ramach projektu Connecting Europe Facility (CEF),
3. norma ISO 29115,
4. standard NIST SP 800-63,
5. standardy ETSI.

W dalszej części rozdziału opisane są najważniejsze z nich.

4.1
Rozporządzenie eIDAS

Jako wstęp do szczegółowej analizy mechanizmów uwierzytelniania i identyfikacji elektronicznej należy wskazać rozporządzenie eIDAS[1]– akt prawny, który definiuje prawne aspekty stosowania tych mechanizmów w Unii Europejskiej. eIDAS definiuje wymagania i skutki prawne stosowania usług zaufania oraz usług identyfikacji elektronicznej, a więc stanowi legalną podstawę dla zapewnienia bezpieczeństwa transakcji elektronicznych oraz potwierdzania tożsamości w usługach elektronicznych. Usługami zaufania są w szczególności usługi związane z podpisem elektronicznym i pieczęcią elektroniczną, w tym usługi wydawania certyfikatów, walidacji oraz konserwacji podpisów oraz pieczęci. Do usług zaufania należą także znakowanie czasem oraz usługa rejestrowanego doręczenia elektronicznego.

4.1.1
Usługi zaufania i identyfikacja elektroniczna

W tym miejscu warto zaznaczyć, że identyfikacja elektroniczna i usługi zaufania stanowią dwa różne obszary stosowania rozporządzenia eIDAS, które mogą być od siebie za-

1. *eIDAS - rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 910/2014 w sprawie identyfikacji elektronicznej i usług zaufania w odniesieniu do transakcji na rynku wewnętrznym oraz uchylające dyrektywę 1999/93/WE*

leżne i wykorzystywać siebie wzajemnie, ale stanowią całkowicie osobny obszar regulacji. Identyfikacja elektroniczna pozwala w sposób procesowy i zabezpieczony przekazać dane identyfikowanej osoby fizycznej lub prawnej, natomiast warunkiem koniecznym identyfikacji jest wcześniejsze uwierzytelnienie identyfikowanej osoby. Rozporządzenie wskazało, że obszar identyfikacji elektronicznej może być osobno regulowany w każdym kraju. W Polsce został ustanowiony krajowy schemat identyfikacji elektronicznej, który szerzej został opisany w kolejnych rozdziałach.

Usługi zaufania stanowią osobny obszar stosowania rozporządzenia eIDAS. Ich cechą wspólną jest to, że zazwyczaj są świadczone na komercyjnych zasadach a rozpoznawalność tych usług oraz ich skutki mają zastosowanie w całej Unii Europejskiej. Wynikiem najbardziej rozpoznawalnych usług zaufania są: podpis elektroniczny, pieczęć elektroniczna oraz znacznik czasu, zostaną one szczegółowo omówione w niniejszym rozdziale. Warto w tym miejscu wskazać, że podpis elektroniczny nie jest identyfikacją elektroniczną, natomiast identyfikacja elektroniczna może być wykorzystana w obszarze usług zaufania. Szczególną formą usług zaufania są usługi kwalifikowane, czyli takie, które podlegają szczególnej kontroli państw członkowskich, ale także są w całej Unii uznawane, za niezaprzeczalne źródło dowodowe w postępowaniach administracyjnych i sądowych.

Rozporządzenie eIDAS ma zastosowanie do publicznie dostępnych usług zaufania, natomiast nie niesie skutków w zakresie zamkniętych systemów np. usług wewnątrz pojedynczej organizacji lub dostępnego tylko dla wewnętrznych użytkowników systemu banku. Innymi słowy o podpisach elektronicznych, pieczęciach elektronicznych oraz rejestrowanym doręczeniu elektronicznym w rozumieniu rozporządzenia eIDAS można mówić tylko wtedy, gdy są one efektem usługi zaufania. Natomiast usługa zaufania jest świadczona przez niezależnego dostawcę - stronę trzecia, która na podstawie regulaminu i polityki usługi zaufania gwarantuje stronom z nich korzystającym bezstronność oraz bezpieczeństwo transakcji.

4.1.2
Podpis elektroniczny

Podpis elektroniczny stanowi najbardziej rozpoznawalny produkt rozporządzenia eIDAS, którego szerokie zastosowanie umożliwia realizację transakcji na odległość za pomocą różnego rodzaju środków komunikacji elektronicznej. Podpis odręczny, podpis papierowy lub bardziej generalnie podpis jest na tyle oczywistym elementem naszego funkcjonowania, że w praktyce nie jest on zdefiniowany ani w literaturze, ani w prawie. Definicja podpisu elektronicznego zawarta w eIDAS odnosi się do generalnego rozumienia podpisu jako bytu oczywistego. Podpis elektroniczny oznacza dane w postaci elektronicznej, które po dołączeniu przez podpisującego do podpisywanej treści elektronicznej służą właśnie jako podpis. Nieodłącznymi elementami podpisu elektronicznego są: elektroniczna postać tego podpisu oraz to, że powstał w wyniku intencji podpisującego złożenia podpisu. Zgodnie z rozporządzeniem eIDAS o podpisie elektronicznym możemy mówić tylko wtedy, gdy jest wynikiem zastosowania usługi zaufania.

ART. 3 10 rozporządzenia eIDAS, 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.

Taka definicja nie ogranicza technologicznie, w jaki sposób podpis ma być zaimplementowany, a więc z podpisem elektronicznym jest każda możliwa elektroniczna postać

podpisu, o ile spełnia wymagania samego rozporządzenia co do postaci, intencji podpisującego oraz powstała w wyniku wykorzystania usługi zaufania.

Najpowszechniejszy sposób składania podpisu elektronicznego opiera się na wykorzystaniu technologii podpisu cyfrowego, czyli kryptografii asymetrycznej, która jest określana w literaturze jako infrastruktura klucza publicznego (PKI). Istnieją także podpisy elektroniczne oparte o zabezpieczenie czynności przez system teleinformatyczny dostawcy usługi podpisu np. podpis zaufany.

Nieodłącznie z podpisem elektronicznym związana jest definicja certyfikatu podpisu elektronicznego, który stanowi dokument elektroniczny pozwalający na przypisanie konkretnego podpisującego do podpisu przez niego złożonego. Certyfikat jest wydawany podpisującemu przez dostawcę usługi zaufania, a pozwala każdemu weryfikującemu na walidację podpisu elektronicznego.

ART. 3 10 rozporządzenia eIDAS, 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;

4.1.3
Pieczęć elektroniczna

Pieczęć elektroniczna określona w rozporządzeniu eIDAS jest bardzo podobna pod względem definicji do podpisu elektronicznego, jednakże ma inne zastosowanie. Pieczęć elektroniczna jest przypisana do osoby prawnej, a skutki jej złożenia będą związane z potwierdzeniem autentyczności i integralności. Dokument oznaczony pieczęcią elektroniczna posiada dowody, że został utworzony przez podmiot identyfikowany tą pieczęcią oraz dowody, że nie zmienił swojej zawartości. Podobnie jak w podpisach elektronicznych pieczęć elektroniczna może być tworzona w różnych rozwiązaniach technologicznych, ale najczęściej jest realizowana za pomocą technologii podpisu cyfrowego.

ART. 3 10 rozporządzenia eIDAS, pieczęć elektroniczna oznacza dane w postaci elektronicznej dołączone do innych danych w postaci elektronicznej lub logicznie z nimi powiązane, aby zapewnić autentyczność pochodzenia oraz integralność powiązanych danych;

Podobnie jak w przypadku podpisu elektronicznego, z pieczęcią elektroniczna związany jest certyfikat pieczęci elektronicznej, który pozwala na jej walidację oraz wskazuje podmiot, który złożył daną pieczęć elektroniczną.

4.1.4
Infrastruktura klucza publicznego

Technologia podpisu cyfrowego[2] oparta jest o kryptografię asymetryczną, która wymaga istnienia dwóch komplementarnych kluczy A i B. Wiadomość zaszyfrowaną kluczem A można odszyfrować kluczem B i odwrotnie – zaszyfrowaną kluczem B daje się odszyfrować kluczem A. Użytkownik generuje więc parę kluczy (tych par jest w praktyce nieskończenie wiele) i jeden klucz chroni – będzie to jego klucz prywatny, za pomocą którego będzie składał podpis cyfrowy. Drugi klucz, komplementarny do prywatnego, jest publicznie znany – służy do weryfikacji złożonego podpisu cyfrowego. Klucz publiczny nazywany jest danymi do weryfikacji podpisu i jest obowiązkowym elementem certyfikatu podpisu elektronicznego lub certyfikatu pieczęci elektronicznej, jeżeli podpis lub

2. *Termin podpis cyfrowy jest używany przez ETSI do określenia technologii*

pieczęć elektroniczna zostały zrealizowane w oparciu o technologię podpisu cyfrowego. Ważnym elementem mechanizmu podpisu cyfrowego jest wykorzystanie do szyfrowania nie całości podpisywanego dokumentu, a jedynie jego reprezentacji nazywanej skrótem. Należy odnotować, że aktualnie zarówno podpisy elektroniczne jak i pieczęci elektroniczne najczęściej realizuje się za pomocą technologii podpisów cyfrowych.

Tak jak powiedziano wyżej, podpis cyfrowy jest wynikiem zaszyfrowania wartości funkcji skrótu danych podpisywanych za pomocą danych służących do złożenia podpisu cyfrowego (klucza prywatnego). Tym samym podpis cyfrowy nie istnieje „samodzielnie", tj. nie ma możliwości, aby go złożyć w oderwaniu od danych podpisywanych - uniemożliwia to brak danych, których dotyczyłby podpis. Wynikowa postać podpisu cyfrowego jest zmienna w zależności od treści danych podpisywanych. Jeżeli kluczem prywatnym zaszyfruje się identyczną treść, to wynik, w postaci podpisu cyfrowego, będzie zawsze taki sam. Natomiast opatrzenie podpisem cyfrowym danych o różnej treści zawsze da odmienną postać podpisu. Tak więc, mimo złożenia podpisu za pomocą tych samych danych służących do jego złożenia, podpis cyfrowy będzie miał zmienną postać elektroniczną. W przeciwieństwie do podpisu własnoręcznego cechą podpisu cyfrowego, która powoduje ograniczenie jego zastosowania, jest brak możliwości złożenia go in blanco. Jest to konsekwencją zalety tego narzędzia, która polega na zapewnieniu integralności podpisanych danych. Innymi słowy, jakakolwiek zmiana tych danych powoduje, że nie można ich powiązać z podpisem cyfrowym, a zatem pozbawia dowodu złożenia podpisu. Nie ma więc żadnego znaczenia czy dokument in blanco zostanie uzupełniony zgodnie z wolą stron, czy też nie. Podpis cyfrowy będzie można przyporządkować tylko do danych w postaci podpisanej pierwotnie.

4.1.5
Znakowanie czasem

Znacznik czasu jest wynikiem działania usługi zaufania – znakowania czasem. W wyniku działania tej usługi tworzone jest potwierdzenie, że oznakowana treść istniała w momencie jej znakowania, co więcej znakowanie czasem także potwierdza integralność oznakowanej nią treści.

ART. 3 33) rozporządzenia eIDAS, 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

Znakowanie czasem jest wykorzystywane do potwierdzenia istnienia treści, ale także wskazywania momentu, w którym nastąpiło podpisanie dokumentu oraz zabezpieczenie wartości dowodowej związanej z podpisem i pieczęcią elektroniczną. Podobnie jak podpis elektroniczny i pieczęć elektroniczna do znakowania czasem wykorzystywany jest technologia podpisu cyfrowego. Dostawca usługi znakowania czasem realizuje znakowanie w oparciu o przesłany mu skrót znakowanego dokumentu, dzięki czemu nie ma możliwości zapoznania się z jego treścią.

4.1.6
Ważność podpisu i pieczęci

Podpis elektroniczny i pieczęć elektroniczna są ważny bezterminowo, jeśli zostały złożone w okresie ważności certyfikatu służącego do ich weryfikacji. Jednakże, aby tak się stało, weryfikujący powinien dysponować dowodami, że podpis został złożony w okresie ważności certyfikatu. Zwykle dowodem czasu złożenia takiego podpisu jest znacznik

czasu. W przyszłości może się okazać, że aktualnie stosowane algorytmy szyfrowe zostaną złamane za kilka/kilkanaście lat i na podstawie klucza publicznego (ogólnie dostępnego) można będzie odtworzyć klucz prywatny, czyli dane służące do składania podpisu elektronicznego. Każdy, kto dysponuje kluczem prywatnym będzie mógł fałszować dane podpisy elektroniczne, tzn. składać je w imieniu kogoś innego. Posiadając dowód złożenia podpisu elektronicznego w postaci znacznika czasu i chcąc zapewnić sobie niezaprzeczalność podpisu w dłuższym okresie czasu rzędu kilku/kilkunastu lat, należy taki podpis (właściwie znacznik) „konserwować", czyli co 3-4 lata ponownie znakować czasem złożone podpisy elektroniczne i poprzednie znaczniki czasu. Zapewne kolejne znakowania będą wykonywane technikami bezpiecznymi w danym momencie i nie będzie miał wtedy istotnego znaczenia fakt kompromitacji techniki składania podpisu sprzed kilkunastu lat.

Cechy podpisu elektronicznego:

- podpis elektroniczny nie istnieje w postaci graficznej lub innej materialnej, choć może zawierać postać graficzną,
- podpisu elektronicznego nie można go złożyć w oderwaniu od podpisywanych danych,
- każdy podpis elektroniczny jest inny, nie ma możliwości powielenia podpisu elektronicznego
- okres jego bezpieczeństwa jest skończony, choć niezdefiniowany w momencie składania podpisu, a jego wydłużenie wymaga aktywnego utrzymania przez okresowe
- ponowne składanie podpisu z bieżącym znacznikiem czasu,
- podpis elektroniczny nie odzwierciedla cech fizycznych osoby,
- podpis elektroniczny jest tworzony w oparciu o usługę zaufania i zwykle składany za pomocą specjalistycznych urządzeń,
- podpisujący może posiadać więcej niż jeden certyfikat podpisu elektronicznego.

4.1.7 Identyfikacja elektroniczna wg rozporządzenia eIDAS

Identyfikacja elektroniczna w rozporządzeniu eIDAS nie jest usługą zaufania, a procesem, który może być obsługiwany zarówno przez dostawców usług identyfikacji jak i rozwiązania udostępniane przez administrację publiczną, np. dowód osobisty. Podpis elektroniczny i pieczęć elektroniczna nie jest produktem identyfikacji elektrycznej ani też identyfikacja elektroniczna nie jest usługą wynikającą z podpisu elektronicznego.

identyfikacja elektroniczna – oznacza proces używania danych w postaci elektronicznej identyfikujących osobę, unikalnie reprezentujących osobę fizyczną lub prawną, lub osobę fizyczną reprezentującą osobę prawną;

uwierzytelnianie – oznacza proces elektroniczny, który umożliwia identyfikację elektroniczną osoby fizycznej lub prawnej, lub potwierdzenie pochodzenia oraz integralności weryfikowanych danych w postaci elektronicznej;

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;

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;

Powodem oddzielnego uregulowania kwestii identyfikacji jest przypisanie wyłączanej decyzji w zakresie stosowania identyfikacji dla własnych obywateli przez państwa członkowskie Unii Europejskiej. W tym zakresie każdy kraj członkowski może utworzyć państwową usługę identyfikacji elektronicznej lub wykorzystać usługi sektora prywatnego. Aspekt identyfikacji i nierozerwalnie z tym związany problem dowodów tożsamości jest rozwiązywany przez każdy kraj oddzielnie na poziomie unijnym, skutkiem czego w krajach członkowskich ukształtowało się wiele odmiennych rozwiązań kwestii identyfikacji, w tym brak dowodów tożsamości, np. w Danii. Dopiero Traktat Lizboński, który wszedł

w życie w 2009 r., w art. 77 ust. 3 zawarł możliwość narzucenia jednolitych wymagań dot. m.in. dowodów tożsamości, ale tylko w zakresie swobody przemieszczania się osób.

W związku z powyższym, rozporządzenie eIDAS ma inne cele w stosunku do aspektów identyfikacji on-line, a inne do usług zaufania, których celem jest dostarczenie dowodów z komunikacji elektronicznej i oświadczeń woli. Jeśli chodzi o identyfikację to rozporządzenie nie ma na celu wprowadzenia jednolitego systemu eID w Unii, a jedynie wzajemne rozpoznawanie i uznawanie różnych schematów elektronicznej identyfikacji w aplikacjach narodowych. Natomiast w odniesieniu do podpisów elektronicznych rozporządzenie (i akty wykonawcze) narzuca jednolite ramy, które zapewniają transgraniczne uznawanie podpisów i pieczęci elektronicznych, szczególnie opartych o kwalifikowane certyfikaty.

Więcej informacji nt. rozporządzenia eIDAS zawartych jest w pkt. 4.5 raportu.

4.1.8
Rodzaje podpisów i pieczęci elektronicznych

Podpis elektroniczny i pieczęć elektroniczna występują w 3 różnych rodzajach: zwykłym, zaawansowanym i kwalifikowanym. Poniżej, na przykładzie podpisu elektronicznej, opisano czym jest kwalifikowany i zaawansowany podpis elektroniczny.

4.1.8.1
Zaawansowany podpis elektroniczny

Zaawansowany podpis elektroniczny zgodnie z rozporządzeniem eIDAS charakteryzuje się czterema cechami:

- jest unikalnie przyporządkowany podpisującym, czyli może go złożyć tylko jedna osoba podpisująca (tzn. nie jest on przywiązany do żadnej grupy osób, a jedynie do pojedynczego podpisującego),
- umożliwia ustalenie tożsamości podpisującego, poprzez wskazanie takich atrybutów jego tożsamości, które są dla niego unikalne,
- jest składany przy użyciu danych służących do składania podpisu elektronicznego, których podpisujący może, z dużą dozą pewności, użyć pod wyłączną swoją kontrolą. W rzeczywistości oznacza to, że jeżeli mamy do czynienia z dokumentem podpisanym kwalifikowanym podpisem elektronicznym, możemy zakładać, że nikt inny nie mógł go złożyć – tylko określony podpisujący,
- zapewnia, że podpisany dokument i związane z nim dane nie zostały zmienione po podpisaniu. W szczególności, że każda późniejsza zmiana podpisanych danych jest rozpoznawalna – a w efekcie jest zachowana integralność treści i podpisu.

4.1.8.2
Kwalifikowany podpis elektroniczny

Każdy kwalifikowany podpis elektroniczny jest zaawansowanym podpisem elektroniczny, który spełnia dodatkowe dwa warunki:

- jest składany za pomocą kwalifikowanego urządzenia do składania podpisu elektronicznego,
- opiera się na kwalifikowanym certyfikacie podpisu elektronicznego.

4.1.8.3
Kwalifikowany certyfikat podpisu elektronicznego

Podstawą funkcjonowania kwalifikowanego podpisu elektronicznego jest kwalifikowany

certyfikat podpisu elektronicznego. Certyfikat towarzyszy każdemu złożonemu podpisowi - jest włączony w strukturę złożonego podpisu, weryfikujący podpis ma wgląd w pełną zawartość certyfikatu. Certyfikat jest wydawany dla podpisującego i stanowi wzorzec służący do weryfikacji podpisów, z tego powodu jest jawny dla adresata podpisanego dokumentu.

Certyfikat jest wydawany przez kwalifikowanego dostawcę usługi zaufania - centrum certyfikacji. Pierwszą czynnością wykonywaną przez centrum certyfikacji przed wydaniem certyfikatu jest zweryfikowanie tożsamości osoby przyszłego posiadacza. Centrum certyfikacji ponosi pełną odpowiedzialność za prawidłową weryfikację tożsamości, a także innych danych, które znajdą się w certyfikacie. Certyfikat to w rzeczywistości elektroniczny dokument potwierdzający tożsamość osoby podpisującej.

Centrum certyfikacji po pozytywnej rejestracji posiadacza certyfikatu - późniejszego podpisującego, realizuje proces utworzenia danych do składania podpisu elektronicznego, czyli generuje dane do składania podpisu elektronicznego oraz dane do weryfikacji podpisu elektronicznego.

Każdy kwalifikowany certyfikat podpisu elektronicznego zawiera informację, potwierdzającą, że jest kwalifikowanym certyfikatem podpisu elektronicznego. Dodatkowo, każdy kwalifikowany certyfikat identyfikuje swojego wystawcę - kwalifikowaną usługę zaufania. Kwalifikowane usługi zaufania podlegają nadzorowi państw członkowskich Unii Europejskiej. Listy kwalifikowanych usług zaufania uprawnionych do wydania kwalifikowanego certyfikatu są publikowana na stronach komisji europejskiej pod adresem: https://ec.europa.eu/digital-single-market/en/eu-trusted-lists-trust-service-providers.W certyfikacie kwalifikowanym znajdują się obowiązkowo: identyfikator certyfikatu, dane osobowe podpisującego, okres ważności certyfikatu, a także dane pozwalające na weryfikację podpisu elektronicznego. Za prawidłowe umieszczenie i potwierdzenie danych zawartych w certyfikacie odpowiada dostawca usługi zaufania.

Kwalifikowany certyfikat zawiera:

- imię i nazwisko posiadacza – podpisującego,
- numer jednoznacznie identyfikujący podpisującego, może to być numer PESEL lub numer dokumentu tożsamości, ale może to być również inny numer unikalny w obrębie danego wystawcy certyfikatów,
- kraj, którego dotyczą powyższe informacje, czyli jeżeli użyto numeru PESEL do identyfikacji podpisującego, to będzie Polska; kraj wskazany w certyfikacie nie musi oznaczać obywatelstwa,
- może wskazywać firmę związaną z posiadaczem certyfikatu, w takim wypadku to powiązanie także jest weryfikowane przez centrum certyfikacji.

Certyfikat kwalifikowany zawiera także szereg dodatkowych atrybutów, które są automatycznie weryfikowane przez oprogramowanie. Ważnym atrybutem jest informacja o tym, czy podpisy weryfikowane tym certyfikatem zostały utworzone przy użyciu kwalifikowanego urządzenia do składania podpisu elektronicznego.

4.1.8.4
Kwalifikowane urządzenie do składania podpisu elektronicznego

Qualified Electronic Signature Creation Device (QSCD), czyli kwalifikowane urządzenie do składania podpisu elektronicznego jest obowiązkowym elementem koniecznym do złożenia kwalifikowanego podpisu elektronicznego.

Szczegółowe warunki prawne dla kwalifikowanego urządzenia określa załącznik II rozporządzenia eIDAS a są nimi:
• zagwarantowanie w racjonalny sposób poufności danych służących do składania podpisu elektronicznego użytych do złożenia podpisu elektronicznego;
• w praktyce tylko jednorazowe wystąpienie danych służących do składania podpisu elektronicznego użytych do złożenia podpisu elektronicznego;
• uniemożliwienie, z racjonalną dozą pewności, pozyskania danych służących do składania podpisu elektronicznego użytych do złożenia podpisu elektronicznego oraz skuteczną ochronę podpisu elektronicznego przed sfałszowaniem za pomocą aktualnie dostępnych technologii;
• możliwość skutecznej ochrony, przez osobę uprawnioną do składania podpisu, danych służących do składania podpisu elektronicznego użytych do złożenia podpisu elektronicznego, przed użyciem ich przez innych.

Szczegółowe warunki techniczne i normalizacyjne określone zostały w tzw. Protection Profile w normie CEN EN 419 211 Protection Profiles for SSCD.

Komisja Europejska cyklicznie publikuje listę wszystkich rodzajów kwalifikowanych urządzeń na stronie eIDAS Observatory: https://ec.europa.eu/futurium/en/eidas-observatory - lista ta stanowi kompletny wykaz wszystkich certyfikowanych urządzeń, które mogą być wykorzystywane jako kwalifikowane urządzenie do składania podpisu elektronicznego.

Podpisy weryfikowane kwalifikowanymi certyfikatem, ale złożone bez kwalifikowanego urządzenia, nazywane są zaawansowanymi podpisami elektronicznymi opartymi o kwalifikowanych certyfikat, natomiast nie są kwalifikowanymi podpisami elektronicznymi. Informację potwierdzającą, czy podpis został złożony za pomocą kwalifikowanego urządzenia można znaleźć w samym certyfikacie w postaci specjalnego atrybutu lub na zaufanych listach, gdzie wystawca certyfikatu oświadcza, że wszystkie wydane w ramach danej usługi certyfikaty potwierdzają, iż podpisy mogą być złożone jedynie z wykorzystaniem QSCD.

Co ważne, nie istnieje możliwość złożenia podpisu bez urządzenia QSCD, jeżeli certyfikat wskazuje, że dane do składania podpisu są osadzone na takim urządzeniu. Natomiast jeżeli kwalifikowany certyfikat nie wskazuje umieszczenia kluczy na QSCD, to nawet późniejsze umieszczenie danych do składania podpisu na takim urządzeniu nie czyni podpisu kwalifikowanym. Innymi słowy, już w momencie wydawania kwalifikowanego certyfikatu wiadomo, czy będzie on służył do składania podpisów kwalifikowanych, czy zaawansowanych.

Oprogramowanie używane do weryfikacji podpisu elektronicznego powinno jednoznacznie informować na podstawie weryfikacji certyfikatu, czy podpis jest kwalifikowanym podpisem elektronicznym, czy zaawansowanym podpisem elektronicznym.

4.1.8.5
Zdalne kwalifikowane urządzenie do składania podpisu elektronicznego

Przed wejściem rozporządzenia eIDAS składanie kwalifikowanego podpisu elektronicznego (bezpiecznego podpisu elektronicznego opartego na kwalifikowanym certyfikacie) było możliwe za pomocą karty kryptograficznej, czyli urządzenia do składania podpisu elektronicznego będącego w bezpośrednim posiadaniu użytkownika. Takie podejście dawało szereg atrybutów bezpieczeństwa, dając pewność, że jedynym sposobem złożenia podpisu jest posiadanie tej jednej karty. Posiadanie karty ma jednak zasadniczą wadę, konieczny jest każdorazowo czytnik umożliwiający przeczytanie karty, co jest szczególnie trudne w przypadku używania urządzeń mobilnych.

Rozwój mobilności spowodował wypracowanie nowych rozwiązań zdalnie dostępnych urządzeń do składania podpisu elektronicznego. Urządzenia te dostępne są po wykonaniu wieloczynnikowego bezpiecznego uwierzytelnienia, dzięki czemu gwarantują bezpieczeństwo porównywalne z tym przypisanym kartom kryptograficznym. W przypadku kwalifikowanego urządzenia do składania podpisu elektronicznego – takie zdalne urządzenie musi być utrzymywane przez kwalifikowanego dostawcę usług zaufania, który gwarantuje bezpieczeństwo całej usługi.

Schemat dostępu do zdalnego kwalifikowanego urządzenia do składania podpisu elektronicznego oparty jest zazwyczaj o dwie cechy tożsamości: token związany z telefonem komórkowym oraz hasło statyczne. W zależności od dostawcy rozwiązań token ten jest albo oparty o aplikację generującą tokeny czasowe, są także rozwiązania oparte o hasła SMS.

4.1.8.6
Ważność certyfikatu i czas złożenia podpisu

Certyfikat kwalifikowany zawiera oznaczenie ważności, tzn. dokładnego momentu, w którym uzyskał ważność i dokładnego momentu, w którym ją straci. W większości przypadków certyfikat rozpoczyna ważność w momencie jego generacji. Czas ważności jest w certyfikacie określony w sposób uniwersalny za pomocą czasu UTC –nie ma znaczenia, w jakiej strefie czasowej certyfikat został utworzony i w jakiej jest aktualnie weryfikowany. Ważność certyfikatu może naruszyć jego unieważnienie lub zawieszenie, które jest realizowane za pośrednictwem wystawcy certyfikatu. Wszyscy wystawcy certyfikatów kwalifikowanych udostępniają publiczną, darmową i dostępną w czasie rzeczywistym usługę pozwalającą na weryfikację ważności wystawionych przez siebie certyfikatów. Kwalifikowany podpis elektroniczny jest ważny, o ile został złożony w okresie ważności certyfikatu kwalifikowanego.

4.1.8.7
Rozpoznawanie certyfikatów zagranicznych

Kwalifikowany podpis elektroniczny oparty na kwalifikowanym certyfikacie wydanym w jednym państwie członkowskim jest uznawany za kwalifikowany podpis elektroniczny we wszystkich pozostałych państwach członkowskich Unii Europejskiej (por. art. 25 ust. 3 rozporządzenia eIDAS). To wymaganie przepisów unijnych nakłada na podmioty weryfikujące podpisy elektroniczne obowiązek stosowania rozwiązań pozwalających na rozpoznawanie nie tylko krajowych, ale także zagranicznych certyfikatów kwalifikowanych. Do realizacji tego służą zaufane listy, które publikowane są przez każde państwo członkowskie i zawierają wszystkie aktywne i historyczne kwalifikowane usługi zaufania.

Certyfikat, którego wystawca nie znajduje się na zaufanych listach, nie jest kwalifikowany, więc podpisy złożone za jego pomocą nie są kwalifikowanymi podpisami elektronicznymi.

4.1.8.8
Formaty podpisu

Kwalifikowany podpis elektroniczny nie musi być złożony w jakimś konkretnym formacie, aby był ważny. Rozporządzenie eIDAS w artykule 27 wskazuje pośrednio[3] na formaty podpisów, które muszą być rozpoznawane w usługach online podmiotów publicznych, ale złożenie podpisu w innym formacie nie powoduje, że nie mamy do czynienia z kwalifikowanym podpisem elektronicznym. Powyższa decyzja wykonawcza wskazała formaty podpisu elektronicznego określone normami w 2012 r. Od tego momentu nastąpiło wiele zmian w zakresie formatów podpisów i powstały też nowe normy, które zachowu-

ją zgodność z wcześniejszymi formatami. Należy więc uznać, że administracja publiczna, przyjmując dokumenty elektroniczne, w tym oferty w ramach zamówień publicznych, powinna rozpoznawać formaty podpisu elektronicznego, co zapewnia zgodność z wymaganiami decyzji wykonawczej 2015/1506 (patrz: „Standardy ETSI").

Ustalenie formatu kwalifikowanego podpisu elektronicznego, w którym są przyjmowane oferty, nie ogranicza konkurencyjności, ponieważ aplikacje umożliwiające złożenie podpisu kwalifikowanego w wyżej wymienionych formatach są ogólnie i bezpłatnie dostępne. Format podpisu nie jest związany z dostawcą certyfikatu kwalifikowanego i choć często podmioty wydające certyfikaty kwalifikowane dostarczają aplikacje do składania podpisu, to nie należy utożsamiać formatu podpisu elektronicznego z konkretnym dostawcą certyfikatu.

4.1.8.9
Zaawansowane i kwalifikowane pieczęci elektroniczne

Tak jak podpisy elektroniczne, pieczęci elektroniczne występują jako: zwykłe, zaawansowane i kwalifikowane. Zestaw wymagań opisanych w rozporządzeniu eIDAS dla zaawansowanej i kwalifikowanej pieczęci jest taki sam jak dla zaawansowanego i kwalifikowanego podpisu elektronicznego.

4.2
Podpisy elektroniczne w uregulowaniach krajowych

Wprowadzenie przez rząd RP w marcu 2019 r., nowego elektronicznego dowodu osobistego z nowymi, elektronicznymi funkcjonalnościami oraz nowelizacji ustawy o dowodzie osobistym, ukonstytuowało na rynku krajowym podpis osobisty. Jest to zaawansowany podpis elektroniczny, który użyty przez podpisującego w stosunku do podmiotu publicznego został zrównany z podpisem złożonym własnoręcznie. Ustawodawca zostawił obszar swobody co do zakresu uznania podpisu osobistego i jego mocy dowodowej w relacjach konsumenckich w stosunku do podmiotów spoza świata administracji publicznej. Podpis osobisty nie jest kwalifikowanym podpisem elektronicznym, a więc nie korzysta z domniemań prawnych oraz paneuropejskiego uznania.

Technicznie dowód osobisty zawiera warstwę elektroniczną (chip), który łącznie z oprogramowaniem jest wg informacji projektowych Ministra Cyfryzacji urządzeniem QSCD, czyli spełnia wymogi kwalifikowanego urządzenia do składania podpisu elektronicznego. Tym samym oznacza to, że urządzenie zostało certyfikowane do poziomu co najmniej EAL4+ w zakresie całości rozwiązania (certyfikacja odnośnie nośnika lub systemu operacyjnego może być nawet na wyższym poziomie wiarygodności, np. EAL5). Niestety, Ministerstwo Spraw Wewnętrznych odpowiedzialne za dowód osobisty nie udostępnia specyfikacji urządzenia ani certyfikatów potwierdzających spełnienie tych wymagań.

Polski dowód z warstwą elektroniczną, oprócz udostępnienia możliwości złożenia podpisu osobistego, adresuje także aspekt identyfikacji w wyniku wyposażenia warstwy elektronicznej również w certyfikat identyfikacji i uwierzytelnienia oraz w specyficzny certyfikat potwierdzenia obecności właściciela dokumentu w określonym czasie i miejscu. Warto także podkreślić, iż narodowy dokument tożsamości posiada mechanizmy zabezpieczające przed fałszerstwem i potwierdzające, że dokument został wydany przez uprawniony podmiot, że dane zawarte w warstwie elektronicznej są autentyczne i integralne, a także, że dokument nie został sklonowany (użycie Active, Passive i Chip authentication).

Drugim, obok podpisu osobistego, podpisem elektronicznym uregulowanym w krajowym systemie prawnym, jest podpis zaufany. Podpis osobisty jest podpisem zaawansowanym składanym z wykorzystaniem urządzenia do składania podpisu, natomiast podpis zaufany nie ma de facto przypisanego poziomu wiarygodności i nie jest podpisem zaawansowanym, zgodnie ze stanowiskiem Ministra Cyfryzacji. Podpis zaufany został wprowadzony w ustawie o informatyzacji działalności podmiotów realizujących zadania publiczne i również jego zastosowanie zostało ograniczone jedynie do świata administracji publicznej.

Podpisem zaufanym nazwany został podpis elektroniczny, którego autentyczność i integralność jest zapewniona przez pieczęć elektroniczną ministra właściwego ds. informatyzacji. Ponieważ zgodnie ze stanowiskiem ministra cyfryzacji, podpis zaufany nie jest podpisem zaawansowanym zgodnie z rozporządzeniem eIDAS to nie może on korzystać ani z domniemań prawnych ani własności podpisów zaawansowanych wynikających z rozporządzenia eIDAS. Dokumenty opatrzone podpisem zaufanym nie są rozpoznawane poza polską administracją publiczną.

Zastosowanie podpisu osobistego oraz zaufanego do podpisywania sprawozdań finansowych z działalności spółek zostało usankcjonowanie w ustawie o zmianie niektórych ustaw w celu ograniczenia obciążeń regulacyjnych, która została opublikowana w Dzienniku Ustaw w dniu 8 sierpnia 2019 r. poz. 1495.

Omawiając możliwości polskiego eDowodu należy także zwrócić uwagę, że nowe przepisy unijne (rozporządzenie PE i Rady (UE) 2019/1157) wprowadzające standard wzoru blankietu dokumentu tożsamości, definiują dla warstwy elektronicznej nowe wymagania dot. umieszczenia na chipie zakodowanych wzorców odcisków papilarnych palców właściciela dokumentu (drugiej obok zdjęcia cechy biometrycznej). Wymaganie to powoduje konieczność zmiany obecnego eDowodu i wydania nowego z nowymi funkcjonalnościami najpóźniej poczynając od 3 sierpnia 2021 r.

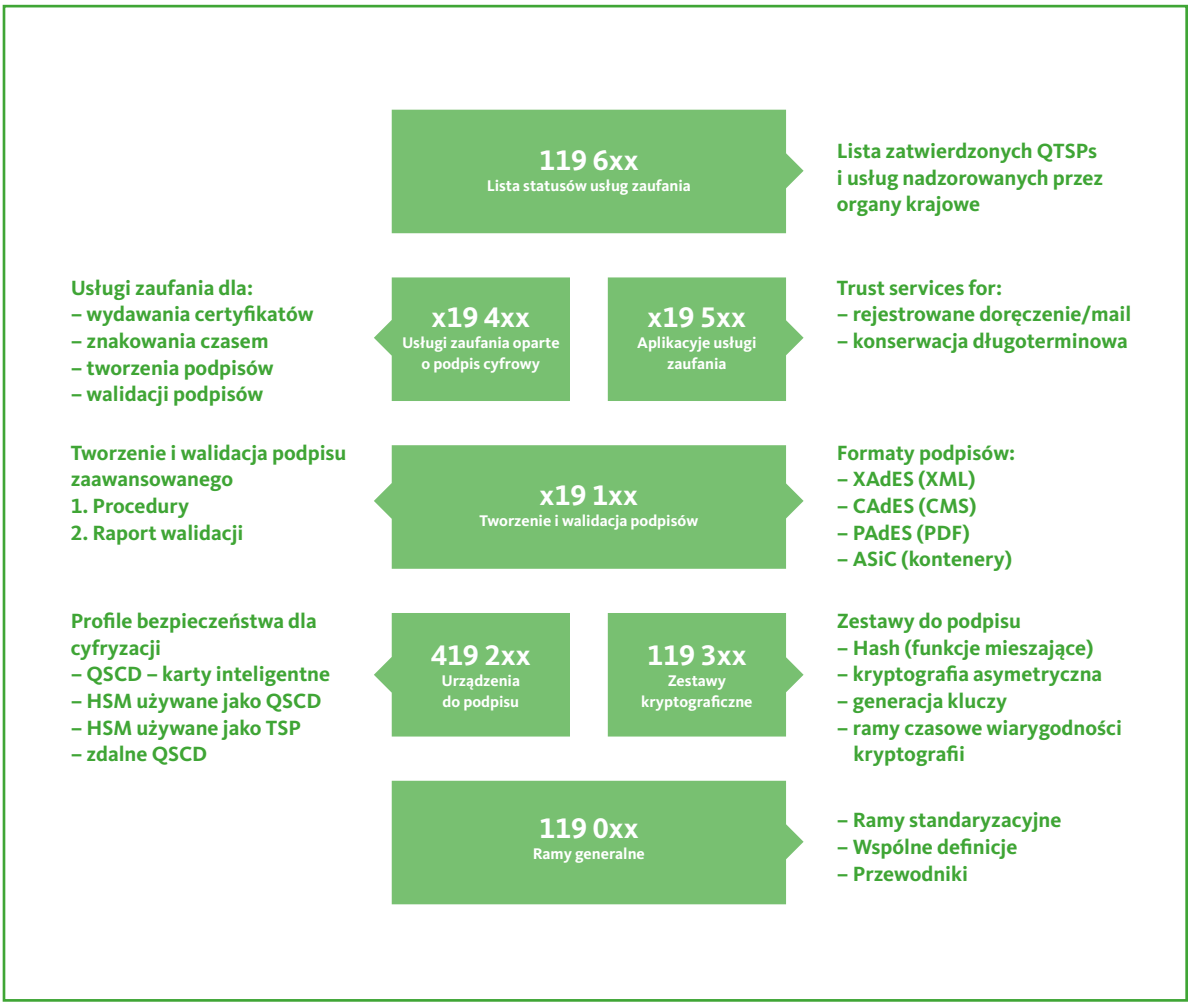
4.3
Standardy ETSI

W ramach implementacji rozporządzenia eIDAS Komisja Europejska zleciła Europejskiemu Instytutowi Norm Telekomunikacyjnych (ETSI) i Europejskiemu Komitetowi Normalizacyjnemu (CEN) opracowanie szeregu standardów. Analogiczne działanie było realizowane przez Komisję Europejską w ramach wdrażania dyrektywy o podpisach elektronicznych. Dokumenty normalizacyjne mają dawać wskazówki poprawnej implementacji eIDAS , a także niektóre z nich są elementem aktów wykonawczych (decyzji Komisji) wydanych na podstawie delegacji zawartych w eIDAS.

Za standaryzację, w ramach ETSI, wspierającą obecną i nadchodzącą technologię podpisów elektronicznych i powiązanych usług (np. zarejestrowaną dostawę elektroniczną, pieczęcie elektroniczne), a także infrastrukturę usług zaufania obsługującą takie usługi odpowiada komitet techniczny TC ESI. Jego działanie ma na celu wsparcie wymogów regulacyjnych, takich jak rozporządzenie eIDAS, a także ogólnych wymagań dla świadczenia usług komercyjnie.

ETSI wraz z CEN w ostatnich czterech latach opublikowało kilkadziesiąt standardów dotyczących obszaru funkcjonowania rozporządzenia eIDAS. W szczególności, są to standardy opisujące: zaufane listy, wymagania dla świadczenia usług zaufania, formaty podpisów, wymagania kryptograficzne oraz profile bezpieczeństwa dla urządzeń. Mapę standardów prezentuje poniższa ilustracja.

RYSUNEK 1. Ramy standaryzacyjne eIDAS. Opublikowane standardy



Ramy standaryzacyjne eIDAS

Standardami ETSI, które najbardziej wpływają na interoperacyjność podpisu elektronicznego i pieczęci elektronicznej są formaty podpisów. ETSI opublikowało 4 podstawowe formaty referencyjne dla standardowych dokumentów i danych:

XAdES – Format oparty o specyfikację XML,
ETSI EN 319 132-1 V1.1.1 (2016-04) – Electronic Signatures and Infrastructures (ESI); XAdES digital signatures; Part 1: Building blocks and XAdES baseline signatures;
PAdES – Format oparty o pliki PDF,
ETSI EN 319 142-1 V1.1.1 (2016-04) - Electronic Signatures and Infrastructures (ESI); PAdES digital signatures; Part 1: Building blocks and PAdES baseline signatures;
CAdES – Format dla danych binarnych oparty o specyfikację ASN.1,
ETSI EN 319 122-1 V1.1.1 (2016-04) - Electronic Signatures and Infrastructures (ESI); CAdES digital signatures; Part 1: Building blocks and CAdES baseline signatures;
ASiC – Format użycia pozostałych formatów w archiwum ZIP,
ETSI EN 319 162-1 V1.1.1 (2016-04) - Electronic Signatures and Infrastructures (ESI); Associated Signature Containers (ASiC); Part 1: Building blocks and ASiC baseline containers.

Aktualnie ETSI pracuje nad formatem JAdES, który będzie oparty o strukturę danych JSON.

4.4
Specyfikacja eIDAS

Wraz z wejściem w życie eIDAS działania dotyczące standaryzacji w zakresie identyfikacji elektronicznej z wcześniejszych projektów tj. IDABC i STORK 2.0 zostały przejęte przez inicjatywę Connecting Europe Facility (CEF) eID Building Block.

Moduł eID programu CEF przede wszystkim wspiera państwa członkowskie we wdrażaniu sieci eIDAS (infrastruktury technicznej łączącej krajowe systemy eID). CEF eID to zestaw usług (w tym oprogramowania, dokumentacji, szkoleń i wsparcia) świadczonych przez Komisję Europejską i zatwierdzonych przez państwa członkowskie, który pomaga administracjom publicznym i prywatnym dostawcom usług na rozszerzenie korzystania z ich usług online na obywateli z innych krajów europejskich. W Polsce, w oparciu o doświadczenia CEF powstał Krajowy Węzeł Identyfikacji elektronicznej oraz rozwiązanie Moje ID.

CEF eID opublikował zaktualizowaną wersję 1.2 specyfikacji technicznych dla ram interoperacyjności eIDAS w październiku 2019 roku. Wydanie specyfikacji technicznych dla identyfikacji elektronicznych jest przewidziane w rozporządzeniu eIDAS i art. 12 rozporządzenia wykonawczego nr 2015/1501. Zadaniem specyfikacji jest stworzenie platformy umożliwiającej praktyczną łączność między środkami eID z różnych państw członkowskich w celu wspierania interoperacyjności.

Specyfikacje zostały opracowane przez państwa członkowskie i Komisję Europejską współpracujące w podgrupie technicznej ds. eID sieci współpracy eIDAS. Komisja zapewnia również, w ramach usług CEF eID, przykładowe wdrożenie oparte na tych specyfikacjach technicznych, które państwa członkowskie mogą przyjąć jako wdrożenie „gotowe".

Obecna wersja składa się z czterech oddzielnych dokumentów, z których każdy dotyczy określonego obszaru:

- Format wiadomości eIDAS;
- Profil atrybutu eIDAS SAML;
- Wymagania kryptograficzne eIDAS;
- Architektura interoperacyjności eIDAS.

Obecna specyfikacja techniczna została zaktualizowana w porównaniu do poprzedniej wersji 1.1. Ta aktualizacja dotyczy w szczególności: stosowania niezgłoszonych schematów eID, identyfikacji stron ufających, poprawek w profilach atrybutów i wymagań kryptograficznych oraz ulepszeń w obsłudze metadanych.

Znaczącym elementem standardu eIDAS jest definicja niezbędnych składników interoperacyjności sieci eIDAS określona w dokumencie eIDAS Interoperability Architecture v.1.2. Zawiera ona składniki niezbędne do osiągnięcia interoperacyjności zgłoszonych systemów eID zgodnie z rozporządzeniem eIDAS [eIDAS].

Interesariuszami sieci eIDAS są:

- strony ufające, które wymagają autentyczności i integralności danych identyfikacyjnych osoby żądającej usługi. Najczęściej oczekiwanie tych danych jest związane z wypełnianiem obowiązków w zakresie ochrony danych i wymaga również poufności otrzymanych danych osobowych;
- obywatele, oczekujący poufności danych identyfikujących jego osobę oraz zapewnieniajego prywatności;
- operatorzy elementów sieci eIDAS - realizujący wymagania wynikające z wymagań strony ufającej i obywateli.

Aby spełnić te wymagania i zapewnić odpowiedzialność zgodnie z rozporządzeniem eIDAS, standard przyjął następujące priorytety:

- zapewnienie poufności danych identyfikujących osobę;
- zapewnienie autentyczności i integralności danych identyfikujących osobę;
- bezpieczną identyfikację i uwierzytelnianie punktów końcowych komunikacji.

W standardzie przyjęto następujące definicje:

- MS to odbierające państwo członkowskie, w którym ma siedzibę strona ufająca żądająca uwierzytelnienia osoby;
- eIDAS-Node to jednostka operacyjna zaangażowana w transgraniczne uwierzytelnianie osób. Węzeł może mieć różne role, które zostały wyróżnione w specyfikacji (eIDAS-Connector / eIDAS-Service, patrz poniżej);Łącznik-eIDAS: Węzeł eIDAS żądający transgranicznego uwierzytelnienia;
- Usługa- eIDAS: Węzeł eIDAS zapewniający transgraniczne uwierzytelnianie;
- eIDAS-Proxy-Service: usługa eIDAS obsługiwana przez wysyłające państwo członkowskie i zapewniająca dane identyfikacyjne identyfikowanej osoby;

• eIDAS-Middleware-Service: usługa eIDAS z uruchomionym oprogramowaniem pośrednim dostarczonym przez wysyłające państwo członkowskie, obsługiwana przez odbierające państwo członkowskie i zapewniająca osobiste dane identyfikacyjne.

Przyjęto dwa schematy uwierzytelniania w usługach opartych na specyfikacji:

• Schemat oparty na proxy: (e-notyfikowany) schemat eID, który zapewnia transgraniczne uwierzytelnianie za pośrednictwem usługi eIDAS-Proxy-Service;

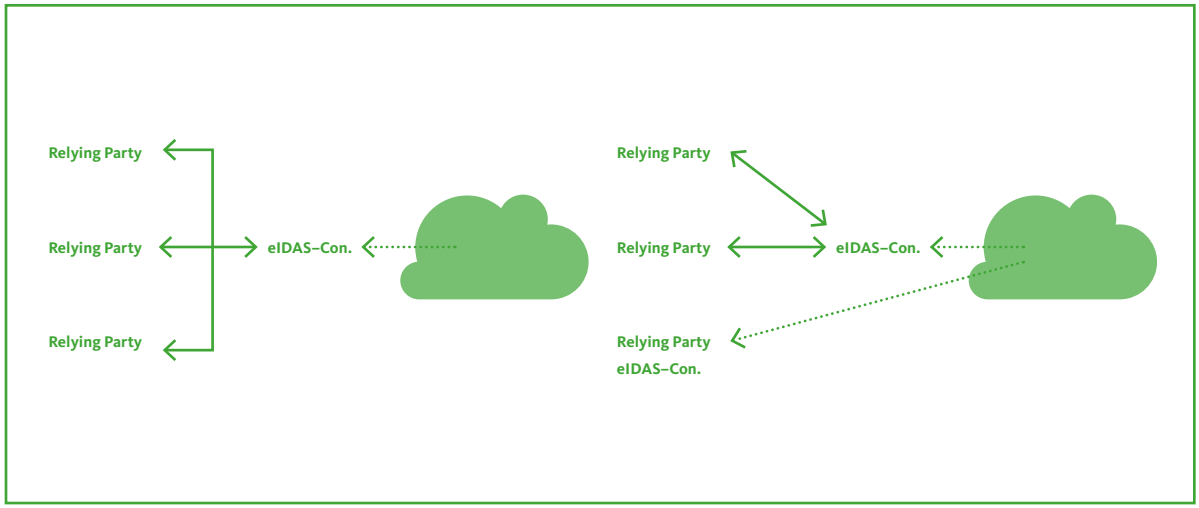
• Schemat oparty na oprogramowaniu pośrednim: (e-notyfikowany) schemat eID, który zapewnia transgraniczne uwierzytelnianie za pośrednictwem eIDAS-Middleware-Services.

W ramach omawianego standardu, interoperacyjność między różnymi schematami, osiągnięto poprzez zdefiniowanie technicznych interfejsów między łącznikami eID a usługami eIDAS, łącznie węzłami eIDAS.

Każde odbierające państwo członkowskie stosuje jeden lub więcej łączniki eIDAS, to od niego zależy decyzja o wdrożeniu łączników n szczeblu krajowym. Łączniki eIDAS nie muszą być obsługiwane przez samo państwo członkowskie, ale mogą być również obsługiwane przez publiczne lub prywatne strony ufające mające siedzibę w tym państwie członkowskim.

Państwo członkowskie działające dokładnie na jednym łączniku nazywane są scentralizowanymi MS, podczas gdy MS obsługujące kilka łączników nazywa się MS zdecentralizowanymi.

RYSUNEK 2. Scentralizowane i zdecentralizowane wdrożenie



Węzły eIDAS obsługują atrybuty tożsamości wyspecyfikowane w minimalnym zestawie danych, ale mogą obsługiwać dodatkowe atrybuty tożsamości.

Minimalny zestaw atrybutów tożsamości został wyspecyfikowany w dokumencie eIDAS SAML Attribute Profile.

TABELA 1. Obowiązkowe atrybuty osoby fizycznej

FamilyName	Nazwisko	cbc:FamilyName
FirstName	Imiona	cvb:GivenName
DateOfBirth	Data urodzenia	cvb:BirthDate
PersonIdentifier	Unikalny identyfikator	cva:Cvidentifier

TABELA 2. Dodatkowe atrybuty osoby fizycznej

BirthName	Imiona z urodzenia	cvb:BirthName
BirthName	Nazwisko z urodzenia	cvb:BirthName
PlaceOfBirth	Miejsce urodzenia	cva:BirthPlaceCvlocation
CurrentAddress	Adres	cva:Cvaddress
Gender	Płeć (Male,Female, Unspecified)	cva:Cvaddress

4.5
Norma ISO 29115

Niniejszy rozdział opisuje normę PN-ISO/IEC 29115:2017-07 - wersja angielska –Technika informatyczna – Techniki bezpieczeństwa – Ramy uzasadnionej pewności poziomów uwierzytelnienia.

W normie określono ramy zarządzania uzasadnioną pewnością uwierzytelnienia podmiotu w określonym kontekście. W szczególności, norma ta:

- określa cztery poziomy uzasadnionej pewności uwierzytelnienia podmiotu;
- określa kryteria i wytyczne do osiągnięcia każdego z czterech poziomów uzasadnionej pewności uwierzytelnienia podmiotu;
- zapewnia wytyczne do odwzorowania innych schematów uzasadnionej pewności uwierzytelnienia na cztery zdefiniowane poziomy;
- zapewnia wytyczne do wymiany wyników uwierzytelnienia, które wykorzystują koncepcję czterech poziomów; oraz
- zapewnia wytyczne w odniesieniu do zabezpieczeń, które są zalecane w celu zmniejszenia zagrożeń związanych z uwierzytelnianiem.

4.5.1
Struktura i poziomy wiarygodności uwierzytelnienia

Norma ISO/IEC 29115 (Information technology – Security techniques – Entity authentication assurance framework), która równolegle jest rekomendacją X.1254 organizacji ITU-T. Dokument ten tworzy ramy dla określania „jakości" uwierzytelnienia elektronicznego. Wiele transakcji elektronicznych, wewnątrz lub pomiędzy systemami ICT, cechują wymagania odnośnie bezpieczeństwa, które zależą od poziomu pewności co do tożsamości stron. Te wymagania mogą dotyczyć: ochrony zasobów przed nieuprawnionym dostępem, a także zapewniać rozliczalność, umożliwiać księgowanie lub pobieranie opłat. Standard określa sposób zapewnienia wiarygodności uwierzytelnienia jednostki (Entity Authentication Assurance), odnoszący się do zaufania jakim można „obdarzyć" wszystkie procesy, czynności zarządzania oraz technologie użyte do ustanowienia i zarządzania tożsamością w transakcjach uwierzytelnienia. Norma prezentuje zatem analogiczne podejście, jak zastosowane w projektach STORK i IDABC. Jednak norma ma charakter uniwersalny, może znaleźć zastosowania we wszystkich sektorach (projekty IDABC i STORK były nakierunkowane na usługi publiczne i w kontekście transgranicznym w UE). Zastosowanie normy ISO 29115 przez różnych dostawców usług uwierzytelniających (Credential Service Providers, CSP), a takimi mogą być np. banki i firmy komercyjne wydające tokeny dla klientów, pozwoli na porównanie i uzyskanie jednolitej klasyfikacji danych uwierzytelniających z różnych CSP. Ponadto norma uwzględnia uwierzytelnienie nie tylko osób, ale i urządzeń. W porównaniu z IDABC i STORK, norma ISO29115 wprowadza więcej obszarów, które są brane pod uwagę (dodatkowo wyszczególniony obszar zarządzania danymi uwierzytelniającymi, ang. credential management) i więcej czynników, które przedstawiono na rysunku.

RYSUNEK 3. Diagram poglądowy struktury wiarygodności uwierzytelnienia wg

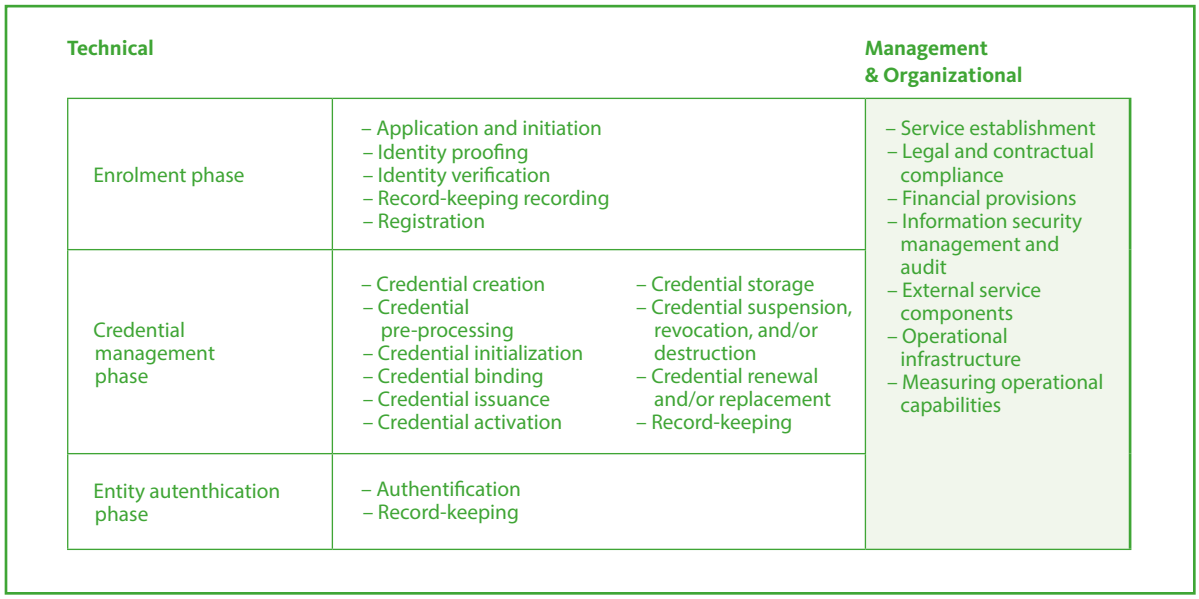


TABELA 3.

Potencjalny wpływ błędnego uwierzytelnienia	Poziom wiarygodności (Level of Assurance)			
	1	2	3	4
Niewygoda, dolegliwość lub uszczerbek na reputacji lub pozycji	niski	umiarkowany	znaczący	wysoki
Strata finansowa lub odpowiedzialność podmiotu*	niski	umiarkowany	znaczący	wysoki
Szkoda dla podmiotu, jego planów lub publicznych interesów	---	niski	umiarkowany	wysoki
Wyciek informacji wrażliwych lub nieuprawniony dostęp do nich	---	umiarkowany	znaczący	wysoki
Bezpieczeństwo osobowe	---	---	niski umiarkowany	znaczący wysoki
Naruszenie prawa cywilnego lub karnego	---	niski	znaczący	wysoki

** w oryginale „agency liability".*

Poziomy wiarygodności wg normy określane są jako Level of Assurance (LoA). Norma określa 4 poziomy w analogiczny sposób jak STORK QAA (por. 3.3). Wybór właściwego poziomu wiarygodności powinien nastąpić po ocenie ryzyka transakcji lub usługi, w ramach której jednostki (osoby i NPE) będą uwierzytelniane. Sam standard nie określa sposobu przeprowadzenia oceny ryzyka; można ją dokonać np. w oparciu o normę ISO/IEC 27005. Tabela 3 przedstawia potencjalny wpływ błędnego uwierzytelnienia, przy

czym siła każdego z czynników jest określona w ogólnej skali wartości: niski, umiarkowany, znaczący, wysoki[3]. Do organizacji należy określenie, jakie to są konkretne wartości (np. jaki poziom strat finansowych oznacza wpływ niski, umiarkowany itd.), bazując na ocenie ryzyka właściwej dla tej organizacji, jej działalności, sytuacji itp.

Należy dodać, iż norma dopuszcza zdefiniowanie przez organizację używającą standardu dodatkowych czynników (niewymienionych w Tabeli 3) natury biznesowej, adekwatnych dla danej organizacji i jej działalności. Przykładowo może istnieć usługa, której cel biznesowy jest łatwiej osiągalny z niższym LoA, np. z użyciem „tylko" hasła, gdy jednocześnie organizacja posiada inne procesy dla ograniczenia strat lub akceptuje zwiększone ryzyko. Druga ważna uwaga – dla danej organizacji lub usługi, może istnieć wiele rodzajów (klas) transakcji, z których każda może mieć inny poziom LoA (np. w zależności od wartości pieniężnej transakcji).

Przed przeprowadzeniem transakcji organizacja (dostawca usługi) powinna:
• zakomunikować stronie przeciwnej swoje wymagania co do poziomu wiarygodności (LoA);
• wdrożyć odpowiednie polityki i środki techniczne zapewniające utrzymanie określonego poziomu LoA systemu wykonującego transakcje;
• posiadać dane uwierzytelniające własnych podmiotów (osób i NPE) na wymaganym poziomie LoA.

Standard ISO 29115 wyróżnia następujących aktorów w strukturze wiarygodności uwierzytelnienia:
• podmiot uwierzytelniany (osoba lub NPE) ,
• dostawca danych uwierzytelniających (CSP, Credential Service Provider),
• urząd rejestracji (RA, Registration Authority),
• strona ufająca (RP, Relying Party),
• weryfikator,
• zaufana trzecia strona (TTP, Trusted Third Party).

Aktorzy mogą należeć do różnych, niezależnych organizacji.

CSP wydaje i/lub zarządza danymi uwierzytelniającymi lub sprzętem, oprogramowaniem i danymi, które mogą być użyte do stworzenia danych uwierzytelniających.

Przykładowymi CPS są:
• bank wydający tokeny do uwierzytelnienia klientów do internetowego konta,
• kwalifikowane centrum certyfikacji wydające certyfikaty elektroniczne,
• Ministerstwo Spraw Wewnętrznych wydające Profil Zaufany do uwierzytelnienia w ramach platformy ePUAP.

Urząd Rejestracji (RA) jest to urząd odpowiedzialny za rejestrację podmiotu (zebranie danych); RA ręczy za zebrane dane dotyczące tożsamości podmiotu i musi cieszyć się zaufaniem ze strony CSP. RA weryfikuje tożsamość wg określonych procedur (np. poprzez weryfikację dokumentu tożsamości, czy sprawdzenie danych w rejestrach). W procesie rejestracji podmiot uzyskuje unikalny identyfikator (jeden lub więcej).

Strona ufająca polega na deklarowanej tożsamości. Strona ufająca może wymagać uwierzytelnienia deklarowanej tożsamości; w tym celu może przeprowadzić uwierzytelnienie samemu lub powierzyć tą operację stronie trzeciej.

Weryfikator potwierdza informacje o tożsamości. Weryfikatorem może być strona ufająca lub inny podmiot cieszący się zaufaniem strony ufającej.

3. *na podstawie* [3].

Zaufana trzecia strona jest to urząd lub jego przedstawiciel (agent), posiadający zaufanie innych aktorów w zakresie czynności związanych z bezpieczeństwem procesu uwierzytelnienia. Przykładem zaufanej trzeciej strony jest centrum certyfikacji (CA), czy urząd znakowania czasem.

4.5.2
Fazy w strukturze wiarygodności

Norma ISO 29115 wyróżnia 3 fazy w strukturze wiarygodności uwierzytelnienia:
- faza rejestracji,
- faza zarządzania danymi uwierzytelniającymi,
- faza uwierzytelnienia podmiotu.

Faza rejestracji

Faza rejestracji składa się z czterech procesów: złożenie aplikacji i inicjalizacja, udowadnianie (proofing) tożsamości, weryfikacja tożsamości, ewidencja i rejestracja. Procesy te mogą się różnić w zależności od rygorów przyjętego poziomu LoA. Proces rejestracji może być zainicjalizowany na różne sposoby. Na przykład może być efektem złożenia żądania przez sam podmiot (np. poprzez internetowy formularz) lub też poprzez stronę trzecią w imieniu podmiotu lub bezpośrednio przez dostawcę danych uwierzytelniających CSP (np. wydanie karty zdrowia przez instytucję państwową). Udowodnienie tożsamości (proofing) jest procesem pozyskania i weryfikacji wystarczającej ilości informacji niezbędnej do zidentyfikowania podmiotu na określonym poziomie wiarygodności. Na przykład mogą to być informacje identyfikujące osobę na podstawie dokumentu (dokumentów) tożsamości, czy aktu urodzenia. Proces ten może zawierać czynność sprawdzenia oryginalności dokumentu tożsamości. Im wyższy poziom LoA, tym bardziej rygorystyczny powinien być proces, zgodnie z tabelą poniżej (przy czym proces z wyższym LoA spełniać musi także wszystkie wymagania dla niższych LoA).

TABELA 4. Wymagania procesu udowadniania tożsamości

LoA	Opis	Cel	Środki sterowania bezpieczeństwem	Metoda przetwarzania
LoA1 – low	Niskie zaufanie lub brak zaufania co do deklarowanej tożsamości	Tożsamość jest unikalna w danym kontekście	Własna deklaracja	Lokalnie lub zdalnie
LoA2 – medium	Pewne zaufanie co do deklarowanej tożsamości	Tożsamość jest unikalna w danym kontekście oraz jednostka, której dotyczy tożsamość, obiektywnie istnieje	Udowodnienie tożsamości poprzez użycie informacji o tożsamości z autorytatywnego źródła	Lokalnie lub zdalnie
LoA3 – high	Wysokie zaufanie co do deklarowanej tożsamości	Tożsamość jest unikalna w danym kontekście, jednostka, której dotyczy tożsamość, obiektywnie istnieje, tożsamość jest zweryfikowana i używana w innych kontekstach	Udowodnienie tożsamości poprzez użycie informacji o tożsamości z autorytatywnego źródła + weryfikacja	Lokalnie lub zdalnie
LoA4 – very high	Bardzo wysokie zaufanie co do deklarowanej tożsamości	Tożsamość jest unikalna w danym kontekście, jednostka, której dotyczy tożsamość, obiektywnie istnieje, tożsamość jest zweryfikowana i używana w innych kontekstach	Udowodnienie tożsamości poprzez użycie informacji o tożsamości z autorytatywnego źródła + weryfikacja + osobiste stawiennictwo	Wyłącznie lokalnie

Weryfikacja tożsamości to proces sprawdzenia uzyskanych w procesie udowadniania tożsamości informacji poprzez porównanie z innymi źródłami. Z kolei rezultatem procesu ewidencjonowania jest zapis (rekord) dotyczący przeprowadzonego procesu rejestracji, który powinien zawierać zebrane informacje i dokumenty oraz informacje o rezultacie poszczególnych kroków. Krokiem kończącym proces rejestracji jest złożenie żądania/wniosku dostępu do usługi lub zasobu. Może on być wykonany w trakcie lub zaraz po rejestracji lub też później.

Faza zarządzania danymi uwierzytelniającymi
Faza zarządzania danymi uwierzytelniającymi zawiera wszystkie istotne procesy związane z zarządzaniem cyklem życia danych uwierzytelniających lub środków do ich wytwarzania. Faza ta może zawierać wszystkie lub niektóre z następujących procesów:
- wytworzenie danych uwierzytelniających,
- wydanie danych uwierzytelniających lub środków do ich wytworzenia,
- przechowywanie danych uwierzytelniających,
- aktywacja danych uwierzytelniających,
- unieważnienie i/lub zniszczenie danych uwierzytelniających,
- odnowienie / zastąpienie danych uwierzytelniających, ewidencja czynności.

Wytworzenie danych uwierzytelniających
Proces ten może zawierać trzy podprocesy: przetwarzanie wstępne, inicjalizację i powiązanie. Niektóre dane uwierzytelniające lub środki do ich wytworzenia wymagają wykonania czynności wstępnych związanych z przypisaniem nośnika do określonego użytkownika (np. nadruk imienia i nazwiska na karcie elektronicznej).

Z kolei inicjalizacja zawiera wszystkie czynności niezbędne do „odblokowania" środków do wytworzenia danych uwierzytelniających w taki sposób, aby mogły spełniać swoją rolę (np. karta elektroniczna może zostać wydana w stanie zablokowanym i musi zostać odblokowana poprzez podanie numeru PIN przed użyciem).

Powiązanie jest procesem ustanowienia związku między danymi uwierzytelniającymi lub środków do wytworzenia danych uwierzytelniających a podmiotem, dla którego są one wydane. Sposób powiązania jest zależny od wymaganego poziomu LoA. Przykładowo, w przypadku procesu on-line może się to odbywać poprzez podanie na końcu procesu kodu aktywacyjnego przesłanego SMS'em.

Wydanie danych uwierzytelniających
Wydanie danych uwierzytelniających to proces, w którym następuje przekazanie danych uwierzytelniających (lub środków do ich wytworzenia) i ostateczne ich powiązanie z podmiotem. Złożoność tego procesu jest różna w zależności od wymaganego poziomu LoA.

Dla wyższych poziomów wiarygodności, proces ten może wymagać osobistego przekazania urządzeń sprzętowych (np. karty elektronicznej). W innych przypadkach może wystarczać dostarczenie hasła lub PIN pocztą elektroniczną lub tradycyjną.

Aktywacja danych uwierzytelniających
Jest to proces, po którym dane uwierzytelniające lub środki do ich wytworzenia są gotowe do użycia. Na przykład po wytworzeniu i inicjalizacji danych uwierzytelniających lub ich nośnika następuje ich zablokowanie do czasu wydania, celem zabezpieczenia przed nadużyciami. W takim przypadku odblokowanie może nastąpić np. poprzez podanie hasła. Proces aktywacji może także nastąpić po okresie zawieszenia ważności danych uwierzytelnienia.

Przechowywanie danych uwierzytelniających
Proces ten polega na bezpiecznym przechowywaniu danych uwierzytelniających lub środków do ich wytworzenia w sposób chroniący przed nieuprawnionym użyciem lub modyfikacją.

Zawieszanie, unieważnianie i/lub niszczenie danych uwierzytelniających
Unieważnienie jest procesem nieodwracalnego zakończenia ważności danych uwierzytelniających. Z kolei zawieszenie jest czasowym „zatrzymaniem" ich ważności. Unieważnienie powinno nastąpić w następujących przypadkach:
• dane uwierzytelniające lub środki do ich wytworzenia zostały zgłoszone jako zagubione lub skradzione lub w inny sposób skompromitowane,
• upłynęła ważność danych uwierzytelniających,
• ustała podstawa dla wydania danych uwierzytelniających (np. pracownik odszedł z pracy),
• dane uwierzytelniające zostały użyte do nieuprawnionych celów,
• zostały wydane inne dane uwierzytelniające celem zastąpienia poprzednich.

Okres pomiędzy powiadomieniem o wystąpieniu zdarzenia wymagającego unieważnienia / zawieszenia danych uwierzytelniających, a zakończeniem procesu unieważniania / zawieszania powinien być określony w polityce organizacji. Dla wyższych poziomów LoA, czas ten powinien być odpowiednio krótki. Niektóre dane uwierzytelniające mogą być zniszczone fizyczne (np. te przechowywane na kartach elektronicznych i innych tokenach sprzętowych).

Odnowienie / zastąpienie danych uwierzytelniających
Odnowienie polega na przedłużeniu ważności istniejących danych uwierzytelniających. Zastąpienie to proces wydania nowych danych uwierzytelniających lub środków do ich wytworzenia w miejsce unieważnionych danych uwierzytelniających. Rygory tych procesów mogą być różne w zależności od poziomu wiarygodności.

Ewidencja
Odpowiednie zapisy o przeprowadzonych czynnościach powinny być tworzone i przechowywane
w rejestrach poprzez cały cykl życia danych uwierzytelniających. Dane ewidencyjne powinny zawierać co najmniej następujące informacje:
• odnotowanie faktu stworzenia danych uwierzytelniających,
• identyfikator danych uwierzytelniających (jeśli stosuje się),
• podmiot dla którego dane zostały wydane (jeśli stosuje się),
• status danych uwierzytelniajcych (je[li stosuje si).

Faza uwierzytelnienia
W fazie uwierzytelnienia podmiot używa swoich danych uwierzytelniających do potwierdzenia tożsamości wobec strony ufającej. Proces uwierzytelnienia polega na ustanowieniu (lub nie) pewności co do tego stwierdzenia. Proces ten wykorzystuje określony protokół zademonstrowania posiadania i/lub kontroli nad danymi uwierzytelniającymi. Wymagania tego protokołu są różne w zależności od stosowanego poziomu wiarygodności. Na przykład, przy niskich LoA być może wystarczy użycie hasła. Z kolei dla wyższych LoA, niezbędne może być wykorzystanie protokołów kryptograficznych typu wezwanie – odpowiedź (ang. challenge – response). Dla wyższych poziomów wiarygodności wymagane jest użycie uwierzytelnienia wieloczynnikowego.

Podobnie jak dla innych faz, w fazie uwierzytelnienia wymagane jest prowadzenie ewidencji zdarzeń.

4.5.3
Wymagania organizacyjne i proceduralne

Przy określaniu poziomu wiarygodności należy brać pod uwagę nie tylko czynniki techniczne, ale także rozważyć wpływ otoczenia prawnego, umów i kwestii organizacji i zarządzania. Nawet najlepsze zabezpieczenia techniczne nie wystarczą, jeśli nie stoją za nimi kompetentni ludzie czy odpowiednie działania. Dlatego standard ISO 29115 formułuje pewne zalecenia w tym obszarze, przy czym nie określa konkretnych wymagań w tym zakresie dla poszczególnych poziomów LoA. Pierwszy aspekt jaki należy rozważyć, to status prawny organizacji dostarczającej usługi zaufania – na przykład dostawca usług zaufania zarejestrowany jako jednostka prawna (np. podmiot gospodarczy) na pewno daje większą wiarygodność, gdyż z założenia podlega pewnym ogólnym wymaganiom prawnym. Inna sprawa to kwestia zgodności prawnej, na przykład ze względu na przetwarzanie danych osobowych. Przy poziomie LoA2 lub wyższym organizacje w strukturze wiarygodności powinny posiadać udokumentowane polityki bezpieczeństwa informacji, stosować zarządzanie ryzykiem i inne środki kontrolne zapewniające stosowanie odpowiednich praktyk. Natomiast dla poziomu 3 i wyższych powinien być wdrożony system zarządzania bezpieczeństwem (np. wg ISO/IEC 27000). Ponadto dla poziomu 2 i wyższych powinny być przeprowadzane okresowe audyty bezpieczeństwa (wewnętrzne i zewnętrzne), weryfikujące stosowanie określonych praktyk.

Norma ISO 29115 wymaga także, aby organizacja wdrażająca strukturę uwierzytelnienia ustanowiła politykę (polityki) oraz procedury określające procesy w organizacji, pozwalające na spełnienie wymagań ustanowionych w tej normie. Polityki i procedury będą różnić się w zależności od roli jaką pełni dana organizacja w strukturze wiarygodności uwierzytelnienia.

4.5.4
Wymagania i środki sterowania bezpieczeństwem

W dalszej części norma opisuje rodzaje zagrożeń dla wszystkich trzech faz (rejestracji, zarządzania danymi uwierzytelniającymi i uwierzytelnienia) oraz wymagania w zakresie tzw. środków sterowania bezpieczeństwem (ang. controls), jakie są niezbędne w zależności od poziomu wiarygodności LoA. Poniżej przytoczone są tylko niektóre z nich; zainteresowanych czytelników, w szczególności tych, którzy chcą wdrażać system identyfikacji i uwierzytelnienia w oparciu o tą normę, odsyłamy do jej treści.

Faza rejestracji

Poziom wiarygodności fazy rejestracji jest odzwierciedlony przede wszystkim wymaganiami co do procesu weryfikacji tożsamości i wiarygodności zebranych danych identyfikacyjnych. Im wyższy poziomo LoA, tym naturalnie, więcej czynności weryfikujących musi być wykonanych. Wymagania te wynikają z przyjętych w normie środków zabezpieczających przed określonymi rodzajami zagrożeń.

Podczas gdy dla poziomu 1 dane identyfikujące osobę mogą być zgłoszone (zadeklarowane) samemu przez osobę rejestrowaną, to już dla poziomu 2 i wyższych musi być przedstawiony wiarygodny dokument tożsamości posiadający zdjęcie. Dla poziomu 3 (i wyżej) dodatkowo wymagane jest przedstawienie innego dokumentu identyfikującego (np. aktu urodzenia, ślubu) i jego weryfikacja poprzez porównanie z danymi zawartymi w rejestrach, na podstawie których dany dokument został wydany. Dodatkowo wymagana jest weryfikacja danych z dokumentu tożsamości ze zdjęciem, poprzez próbę skontaktowania się z osobą z pomocą tych danych. Dla najwyższego poziomu (LoA 4), oprócz wszystkich w/w wymagań, dodatkowo niezbędna jest weryfikacja dodatkowego dokumentu tożsamości, a także osobiste stawiennictwo osoby rejestrowanej.

Ponadto, bez względu na poziom wiarygodności, obowiązkowym jest publikacja (dokumentu) polityki w zakresie rejestracji (określającej sposób weryfikacji tożsamości, m.in. listę dopuszczonych rodzajów dokumentów tożsamości) oraz naturalnie przestrzeganie jej zasad.

Faza zarządzania danymi uwierzytelniającymi

W tej fazie występuje znacznie więcej wymagań co do środków sterowania bezpieczeństwem. Poniżej przedstawione są subiektywnie wybrane najistotniejsze z nich:

- bez względu na poziom LoA, wymagany jest sformalizowany i udokumentowany proces wytwarzania i wydawania danych uwierzytelniających,
- wszelkie moduły sprzętowe, takie jak karty elektroniczne - jeśli używane do przechowywania danych uwierzytelniających - powinny być przechowywane w sposób bezpieczny i kontrolowane (np. poprzez rejestrację numerów seryjnych),
- proces musi zapewniać, że dane uwierzytelniające lub środki do ich generowania (np. karta elektroniczna) są aktywowane przez zamierzoną jednostkę,
- dane uwierzytelniające są unieważniane lub niszczone (jeśli to możliwe) w określonym dla każdego poziomu czasie, zgodnie z polityką organizacyjną,
- dodatkowo dla poziomu LoA 4 wytwarzanie danych uwierzytelniających (np. kluczy kryptograficznych) musi odbywać się w „sprzętowym module kryptograficznym" (zgodnie z ISO/IEC 19790; np. na karcie elektronicznej lub HSM) oraz po wytworzeniu tych danych, powinny one zostać zablokowane do czasu przekazania użytkownikowi.

Faza uwierzytelnienia

W skład zagrożeń dla fazy uwierzytelnienia wchodzą zarówno zagrożenia związane z użyciem danych uwierzytelniających, jak i ogólne zagrożenia, które mogą wystąpić w tej fazie, takie jak: złośliwe oprogramowanie (wirusy, trojany itd.), ataki typu „Denial of Service", inżynieria społeczna, błędy użytkownika (słabe hasła, brak ochrony informacji) i inne. Norma ISO 29115, z pewnymi wyjątkami, zajmuje się jedynie zagrożeniami związanymi z użyciem danych uwierzytelniających.

Generalnie urządzenia przechowujące dane uwierzytelniające (np. karty elektroniczne) powinny być zabezpieczone przed fałszowaniem poprzez umieszczenie zabezpieczeń fizycznych (np. hologram, mikrodruk), przy czym standard nie podaje konkretów (tzn. jakie zabezpieczenia przy jakim poziomie) – powinno to wynikać z szacowania ryzyka dla danego przypadku. Powinien być także zaimplementowany mechanizm blokowania danych uwierzytelniających po określonej liczbie nieudanych prób użycia hasła odbezpieczającego te dane. Ponadto należy używać mechanizmów uwierzytelnienia, które nie transmitują haseł, a sesje powinny być szyfrowane.

Dla poziomów 3 i 4 bezwzględnie wymagane jest uwierzytelnienie wieloczynnikowe (np. coś co wiem i coś co mam). Ogólnie, co podkreśla norma, uwierzytelnienie wieloczynnikowe pozwala zapobiegać wielu ogólnym zagrożeniom (aczkolwiek nie wszystkim).

4.6
Standard NIST SP 800-63

Niezależnie od standardów europejskich powstaje wiele standardów światowych, które mają szeroki wpływ na stosowanie mechanizmów bezpieczeństwa, a także są włączane w standardy europejskiej. Od wielu lat prym w zakresie standardów bezpieczeństwa dla usług i rozwiązań elektronicznych wiedzie NIST. Omawiany w niniejszym rozdziale standard NIST SP 800-63 stanowi bazę dla wszystkich systemów zarządzania identyfikacją, tożsamością oraz federacji tych tożsamości.

Standard SP 800-63 zawiera przegląd ogólnych ram tożsamości z wykorzystaniem środków uwierzytelnienia, poświadczeń i asercji w systemie cyfrowym, a także oparty na ryzyku proces wyboru poziomów wiarygodności. SP 800-63 zawiera zarówno materiały normatywne, jak i informacyjne.

W ramach standardu wyróżnia się pakiet woluminów:
- SP 800-63A Enrollment and Identity Proofing,
- SP 800-63B Authentication and Lifecycle Management,
- SP 800-63C Federation and Assertions.

4.6.1
SP 800-63A Rejestracja i weryfikacja tożsamości

Standard NIST SP 800-63-A opisuje, w jaki sposób wnioskodawcy mogą udowodnić swoją tożsamość i zostać zarejestrowani jako ważni subskrybenci w systemie tożsamości. Zapewnia wymagania, według których wnioskodawcy mogą zarówno dowodzić tożsamości, jak i rejestrować się na jednym z trzech różnych poziomów ograniczania ryzyka zarówno w zdalnych, jak i stacjonarnych scenariuszach.

SP 800-63A ustala wymagania dla uzyskania danego poziomu wiarygodności tożsamości (IAL). Trzy poziomy odzwierciedlają opcje, które agencje mogą wybierać na podstawie profilu ryzyka i potencjalnej szkody wyrządzonej przez atakującego, który złoży fałszywe żądanie tożsamości.

Wyróżnia się następujące poziomy:

- Poziom wiarygodności tożsamości 1: Nie ma wymogu powiązania wnioskodawcy z konkretną tożsamością w świecie rzeczywistym. Wszelkie atrybuty podane w połączeniu z procesem uwierzytelniania są potwierdzane przez siebie lub powinny być traktowane jako takie (w tym atrybuty, które dostawca usług uwierzytelniających potwierdza stronie ufającej).
- Poziom wiarygodności uwierzytelnienia 2: Dowody potwierdzają istnienie deklarowanej tożsamości w świecie rzeczywistym i weryfikują, czy wnioskodawca jest odpowiednio powiązany z tą tożsamością w świecie rzeczywistym. Poziom 2 wprowadza potrzebę zdalnego lub fizycznego przedstawienia tożsamości. Atrybuty mogą zostać udostępnione stronie ufającej, aby wykonać anonimową identyfikację ze zweryfikowanymi atrybutami.
- Poziom wiarygodności uwierzytelnienia 3: Fizyczna obecność jest wymagana do potwierdzenia tożsamości. Identyfikujące atrybuty muszą zostać zweryfikowane przez upoważnionego i przeszkolonego przedstawiciela dostawcy usług uwierzytelniających. Podobnie jak w przypadku poziomu 2, atrybuty mogą zostać udostępnione stronie ufającej, aby wykonać anonimową identyfikację ze zweryfikowanymi atrybutami.

4.6.2
SP 800-63B Uwierzytelnianie i zarządzanie cyklem życia

SP 800-63B dostarcza zalecenia dotyczące procesów uwierzytelnienia, w szczególności wyboru środków uwierzytelnienia, które mogą być stosowane na różnych poziomach pewności uwierzytelnienia (AAL). Zawiera także zalecenia dotyczące cyklu życia środków uwierzytelniających, w tym odwołania w przypadku zagubienia lub kradzieży.

W przypadku usług, w których wymagane jest ponowne logowanie, udane uwierzytelnienie zapewnia uzasadnioną, opartą na ryzyku gwarancję, że sub-

skrybent uzyskujący dostęp do usługi w danym momencie jest taki sam, jak ten, który wcześniej uzyskał dostęp do usługi. Odporność tego zaufania opisuje kategoryzacja według poziomów pewności uwierzytelnienia. NIST SP 800-63B opisuje, w jaki sposób osoba może bezpiecznie uwierzytelnić się u dostawcy usług uwierzytelniających, aby uzyskać dostęp do usługi cyfrowej lub zestawu usług cyfrowych.

Trzy poziomy pewności uwierzytelnienia określają podzbiory opcji, które agencje mogą wybrać na podstawie ich profilu ryzyka i potencjalnej szkody wyrządzonej przez atakującego przejmującego kontrolę nad środkiem uwierzytelnienia i uzyskującym dostęp do systemów agencji.

Wyróżnia się następujące poziomy:

• Poziom pewności uwierzytelnienia 1: Zapewnia pewne zapewnienie, że strona uwierzytelniająca kontroluje środki uwierzytelnienia powiązane z kontem subskrybenta. Poziom 1 wymaga uwierzytelnienia jednoskładnikowego lub wieloskładnikowego przy użyciu szerokiej gamy dostępnych technologii uwierzytelniania. Pomyślne uwierzytelnienie wymaga, aby strona uwierzytelniająca udowodniła posiadanie i kontrolę nad środkami uwierzytelnienia za pomocą bezpiecznego protokołu uwierzytelniania.

• Poziom pewności uwierzytelnienia 2: Zapewnia dużą pewność, że strona uwierzytelniająca kontroluje środki uwierzytelnienia powiązane z kontem subskrybenta. Dowód posiadania i kontroli dwóch różnych czynników uwierzytelniania jest wymagany za pośrednictwem bezpiecznego protokołu (protokołów) uwierzytelnienia. Zatwierdzone techniki kryptograficzne są wymagane na poziomie 2 i wyższym.

• Poziom pewności uwierzytelnienia 3: Zapewnia bardzo dużą pewność, że strona uwierzytelniająca kontroluje środki uwierzytelnienia powiązanych z kontem subskrybenta. Uwierzytelnianie na poziomie 2 opiera się na dowodzie posiadania klucza za pomocą protokołu kryptograficznego. Uwierzytelnianie poziomi 3 MUSI używać sprzętowego urządzenia uwierzytelniającego i środka, które zapewnia odporność na podszywanie się pod weryfikatora; to samo urządzenie MOŻE spełniać oba te wymagania. W celu uwierzytelnienia na poziomie 3, wnioskodawcy MUSZĄ udowodnić posiadanie i kontrolę nad dwoma odrębnymi czynnikami uwierzytelniającymi za pomocą bezpiecznego protokołu (protokołów) uwierzytelnienia. Wymagane są zatwierdzone techniki kryptograficzne.

4.6.3
SP 800-63C Federacje i asercje

NIST SP 800-63C dostarcza wymagania przy korzystaniu ze sfederowanych architektur tożsamości i asercji w celu przekazania wyników procesów uwierzytelniania i odpowiednich informacji o tożsamości do wnioskującej agencji. Ponadto, oferuje techniki zwiększające prywatność w celu udostępniania informacji o ważnym, uwierzytelnionym podmiocie i opisuje metody, które pozwalają na silne uwierzytelnianie wieloskładnikowe (MFA), podczas gdy podmiot pozostaje anonimowy dla usługi cyfrowej SP 800-63C wskazuje na trzy poziomy pewności asercji (FAL):

• Poziom pewności asercji 1: Pozwala subskrybentowi na włączenie strony ufającej do otrzymania kolejnych asercji. Asercja jest podpisana przez dostawcę tożsamości przy użyciu zatwierdzonej kryptografii,

• Poziom pewności asercji 2: Dodaje wymóg szyfrowania asercji przy użyciu zatwierdzonej kryptografii, dzięki czemu strona ufająca jest jedyną stroną, która może ją odszyfrować,

• Poziom pewności asercji 3: Wymaga od subskrybenta przedsta-

wienia dowodu posiadania klucza kryptograficznego wymienionego w asercji oprócz samego artefaktu asercji. Asercja jest podpisana przez dostawcę tożsamości i zaszyfrowane wobec strony ufającej przy użyciu zatwierdzonej kryptografii.

4.6.4
Rodzaje urządzeń uwierzytelniających

SP 800-63B dostarcza mapowanie różnych urządzeń na poziom pewności uwierzytelnienia.

TABELA 5.

Poziom 1	Poziom 2	Poziom 3
Memorized secret	MF OTP Device	MF Crypto Device
Look-Up Secret	MF Crypto Software	SF Crypto Device plus memorized Secret
Out-of-band	MF Crypto Device or Memorized Secret plus:	SF OTP Device plus
SF OTP Device	Look-Up Secret	MF Crypto Device or Software;
MF OTP Device	Out-of-band	SF OTP Device plus SF Crypto Software plus Memorized Secret
SF Crypto Software	SF OTP Device	
SF Crypto Device	SF Crypto Software	
MF Crypto Software	SF Crypto Device	
MF Crypto Device		

1. Single–Factor OTP Device – urządzenie z kategorii sprzętu (np. token) bądź oprogramowania (zainstalowanego na telefonie), które generuje jednorazowy kod. Nie wymaga aktywacji za pomocą drugiego czynnika.
2. Multi-Factor OTP Device - urządzenie z kategorii sprzętu (np. token) bądź oprogramowania (zainstalowanego na telefonie), które wymaga aktywacji za pomocą drugiego czynnika (aktywowanego za pomocą biometrii palca bądź bezpośredniego interfejsu komputera za pomocą np. USB).
3. Single–Factor Crypto Software – jest to jednoskładnikowe uwierzytelnienie, którego klucz jest przechowywany na dysku, karcie bądź innym miękkim nośniku, które nie wymaga aktywacji za pomocą drugiego czynnika. Uwierzytelnianie odbywa się poprzez udowodnienie posiadania i kontroli klucza.
4. Multi-factor Crypto Software - jest to wieloskładnikowe uwierzytelnienie, którego klucz jest przechowywany na dysku, karcie bądź innym miękkim nośniku, które wymaga aktywacji za pomocą drugiego czynnika. Uwierzytelnianie odbywa się poprzez udowodnienie posiadania i kontroli klucza. Ten rodzaj uwierzytelnienia jest tym CO MASZ i aktywacja odbywa się za pomocą tego CO Wiesz orasz tego KIM JESTEŚ.
5. Single–Factor Crypto Device – jednoskładnikowe urządzenie kryptograficzne (np. klucz USB), które wykonuje operacje kryptograficzne przy użyciu chronionych kluczy kryptograficznych i zapewnia dane wyjściowe środka uwierzytelnienia poprzez bezpośrednie połączenie z punktem końcowym użytkownika. Urządzenie wykorzystuje osadzone symetryczne lub asymetryczne klucze kryptograficzne i nie wymaga aktywacji poprzez drugi czynnik uwierzytelnienia.
6. Multi-factor cryptographic device - wieloskładnikowe urządzenie kryptograficzne to urządzenie sprzętowe, które wykonuje operacje kryptograficzne przy użyciu jednego lub więcej chronionych kluczy kryptograficznych i wymaga aktywacji za pomocą drugiego czynnika uwierzytelniającego. Uwierzytelnianie odbywa się poprzez udowodnienie

posiadania urządzenia i kontroli klucza. Dane wyjściowe środka uwierzytelnienia są dostarczane przez bezpośrednie połączenie z punktem końcowym użytkownika i są w dużym stopniu zależne od konkretnego urządzenia kryptograficznego i protokołu, ale zazwyczaj jest to pewnego rodzaju podpisany komunikat. Wieloskładnikowe urządzenie kryptograficzne jest czymś:

- co masz (posiadanie),
- i MUSI być aktywowane przez coś, co znasz (wiedza) lub czymś, kim jesteś (cechy klienta).

W kontekście mechanizmów silnego uwierzytelnienia, które w założeniu dopuszcza stosowanie co najmniej dwóch elementów należących do kategorii: wiedza (coś, co wie wyłącznie użytkownik), posiadanie (coś, co posiada wyłącznie użytkownik) i cechy klienta (coś, czym jest użytkownik) możliwe jest zestawienie różnego rodzaju urządzeń, które zagwarantują zachowanie odpowiedniego poziomu pewności uwierzytelnienia. W szczególności można wskazać na kombinację:

- Coś co masz: telefon/karta SIM, token, aplikacja na telefonie,
- Coś co znasz: hasło lub coś kim jesteś (odcisk palca).

ROZDZIAŁ 5.0

PRZEGLĄD KONCEPCJI UWIERZYTELNIENIA

Wcześniejsze rozdziały dotyczyły zagadnień identyfikacji i uwierzytelnienia w bardzo szerokim aspekcie. Ten rozdział jest natomiast poświęcony omówieniu najczęściej spotykanych mechanizmów uwierzytelnienia w aspekcie technicznym i szczegółowych problemów z tym związanych.

Uwierzytelnianie jest procesem, w którym sprawdza się czy obiekt (osoba fizyczna lub maszyna) jest tym, za który się podaje i czy ma odpowiednie uprawnienia dostępu. W bankowości uwierzytelnianie jest stosowane w następujących procesach:

- Logowanie, które oznacza uzyskanie dostępu do konta bankowości internetowej lub mobilnej,
- Potwierdzenie transakcji w szczególności: przelewu, wniosku w bankowości internetowej lub transakcji e-commerce,
- Uwierzytelnienie usługodawców zapewniające budowanie bezpiecznego dostępu stron trzecich w procesach obsługi klienta. W szczególności uwierzytelnienie AIS (dostępu do informacji o koncie) PIS (usługi inicjacji płatności).

5.0

Proces uwierzytelnienia użytkownika realizowany jest w 4 etapach:

- Żądanie uwierzytelnienia – obiekt, który chce się uwierzytelnić wysyła żądanie uwierzytelnienia wraz z identyfikatorem,
- Przypisanie polityki - system uwierzytelniający odnajduje po identyfikatorze jaka polityka uwierzytelniania jest przypisana do tego obiektu a następnie wysyła żądanie podania czynników uwierzytelniających (ang. Authentication factors),
- Przekazanie czynników - obiekt przekazuje wskazane czynniki uwierzytelniające (np.: hasło, kod jednorazowy, cechy biometryczne) – czynnik te mogą być łączne,
- Weryfikacja - system sprawdza, czy czynniki uwierzytelniające są prawidłowe, a następnie dokonuje oceny ryzyka biorąc pod uwagę aktualne cechy obiektu (np. geolokalizacja, sposób pisania na klawiaturze itp.),

Dopiero tak zrealizowany proces pozwala na uwierzytelnienie użytkownika w usłudze. Niektóre z tych etapów realizowane są łącznie, np. w sytuacji gdy system uwierzytelniający realizuje tylko jedną politykę uwierzytelnienia.

5.1 Czynniki uwierzytelniania

Czynniki uwierzytelniania (ang. Authentcation factors) dzielą się na 3 grupy:

- co wiem – informacja dostępna tylko dla osoby uwierzytelnianej, oparta o jej wiedzę lub posiadane informacje np. hasło, PIN,
- co mam – informacja generowana przez obiekt będący w wyłącznym władaniu osoby uwierzytelnianej np.: PIN z tokenu sprzętowego lub programowego, kod jednorazowy SMS, karta zdrapka, token podłączany do urządzenia i komunikujący się bezpośrednio z aplikacją itp.,
- czym jestem – cechy fizyczne lub behawioralne jednoznacznie identyfikujące osobę, możliwe do porównania z wzorcem przy użyciu algorytmów biometrycznych lub przez wyszkolony personel.

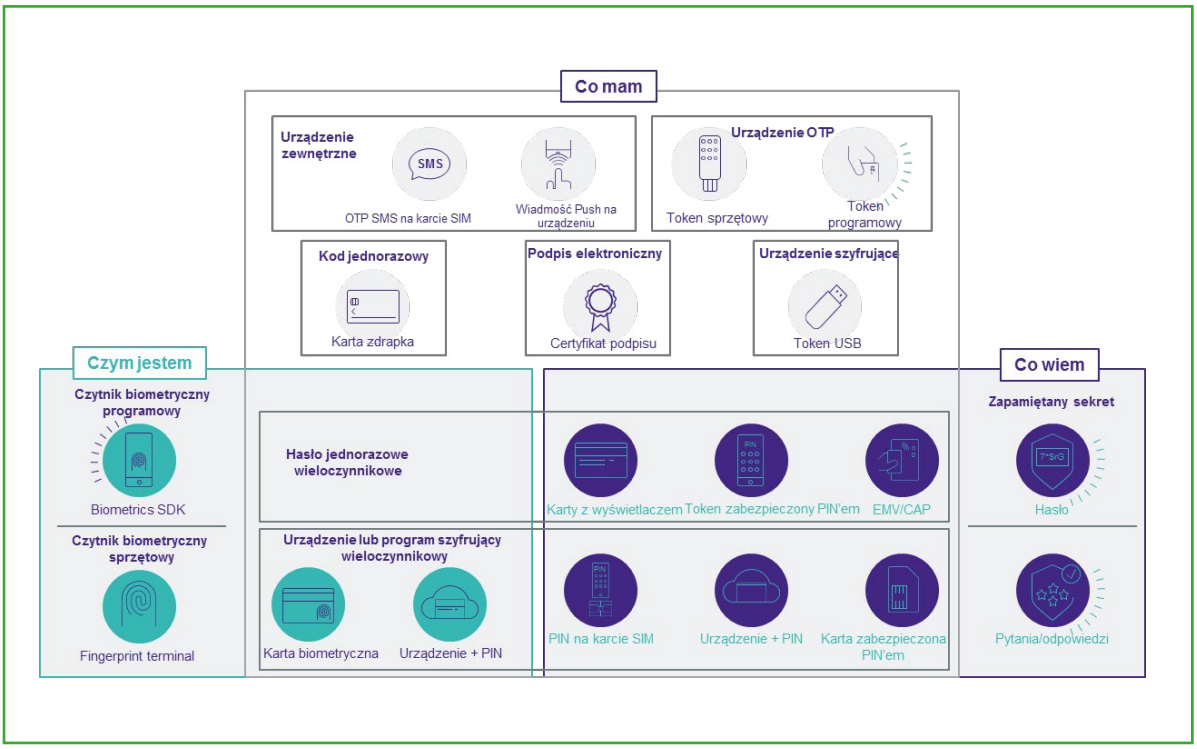
Kombinacja dwóch lub więcej czynników uwierzytelniania nazywana jest silną metodą uwierzytelniania. Co do zasady należy przyjąć, że nie istnieje jedna uniwersalna silna metoda uwierzytelniania, którą można zastosować we wszystkich przypadkach. W zależności od poziomu ryzyka związanego z wartością transakcji lub osobą uwierzytelnianą, oczekiwanej wygody użytkowania, dostępnych środków technicznych, kanałów komuni-

kacji oraz wymagań prawnych, do każdego procesu uwierzytelnienia oraz każdej uwierzytelnianej osoby należy indywidualnie dobrać odpowiednią metodę uwierzytelnienia. Informacje te są zapisywane w serwerze uwierzytelniającym.

Podobnie należy przyjąć, że nie istnieje metoda uwierzytelniania, którą będzie można stosować wiecznie. Zmiany technologiczne, coraz bardziej wyrafinowane metody ataków i nadużyć, zmiana przyzwyczajeń użytkowników oraz zmieniające się wymagania prawne, powodują konieczność ewolucji metod uwierzytelniania stosowanych przez instytucje finansowe i inne podmioty.

Warto zauważyć, ze niektóre cechy, jak np. odcisk palca nie zawsze będą miały tą samą wartość jako faktor bezpieczeństwa. Wyższą wartość ma, gdy podmiot ufający sam weryfikuje wzorzec biometryczny, a niższą, gdy tylko otrzymuje potwierdzenie z urządzania jakim jest np. smartfon. W tej drugiej sytuacji podmiot ufający dostanie takie samo potwierdzenie zgodności odcisku palca, bez względu jaka osoba go złożyła, w tej sytuacji odcisk palca jest deklaratywnie przypisany do osoby, bez weryfikacji podmiotu ufającego. Gdy np. kilka osób ma przypisany odcisk palca w telefonie dla np. banku, będzie to ta sama osoba. Jedyną stosowaną metodą jest konieczność ponownej aktywacji funkcji autoryzacji odciskiem palca bo dodaniu kolejnego wzorca, jednak jedynym potwierdzeniem, że wzorzec został dodany przez właściwego użytkownika jest jego deklaracja.

RYSUNEK 4. Przykłady czynników uwierzytelniania



5.2
Wymagania dyrektywy PSD2 dla uwierzytelniania

Obowiązująca od września 2019 dyrektywa PSD2 (Payment Service Directive 2) nałożyła na banki obowiązek – poza ściśle określonymi wyjątkami – stosowania silnego uwierzytelnienia (ang. SCA – Strong Customer Authentication) klientów przy ich kontakcie online z bankiem. SCA jest definiowane jako stosowanie przynajmniej dwóch, niezależnych od siebie czynników uwierzytelniających należących do różnych grup.

Wyjątkowo banki mogą zrezygnować z silnego uwierzytelnia w następujących przypadkach, gdy:
• analiza ryzyka transakcji (TRA – Transaction Risk Analysis) wykaże niskie ryzyko transakcji według kryteriów ściśle zdefiniowanych w PSD2,
• kwota transakcji jest niższa od ustalonego w PSD2 progu,
• transakcja jest powtarzalna,
• transakcja jest wykonywana na urządzeniu bez nadzoru np. opłaty parkingowe, opłaty za komunikację miejską.

Wymagania SCA nie są nowością dla banków, które już wcześniej stosowały powszechnie silne uwierzytelnianie transakcji (np. hasło + SMS OTP). Nowością jest jednak wymóg dynamic linking – dynamicznego wiązania kodu jednorazowego z danymi transakcji, co widać w migracji w bankach z komunikatów SMS z „samym" kodem na komunikaty rozbudowane, dobrze opisujące transakcję, której kod dotyczy. Dzięki temu minimalizowane jest ryzyko, że w przypadku ataku, klient poda kod do autoryzacji przelewu bez świadomości, że przelew dotyczy większej kwoty i na inny rachunek niż ma świadomość realizacji przelewu.

Szczególnym przypadkiem jest uwierzytelnienie transakcji typu e-commerce (płatność kartą płatniczą w sklepie internetowym). Ponieważ EBA (European Banking Assiciation) wydała interpretację mówiącą, że dane zamieszczone na karcie płatniczej (numer karty, data ważności, CVV itp.) nie są czynnikiem uwierzytelniającym, stosowany powszechnie system uwierzytelniania 3DS oparty na danych z karty (1-szy czynnik) i kodzie jednorazowym (2-gi czynnik) nie jest zgodny z wymaganiami PSD2. Ponieważ do chwili obecnej nie opracowano wygodnej i możliwej do zastosowania we wszystkich kanałach online metody uwierzytelniania transakcji e-commerce, EBA zgodziło się przesunąć termin obowiązywania PSD2 dla tego typu transakcji o rok, do września 2020.

Wskutek wejścia w życie PSD2 banki w Polsce wprowadziły w praktyce dwie alternatywne metody na dostęp wcześniej jednoskładnikowy do bankowości. Tzn. albo zachowały dostęp jednoskładnikowy i dopiero dostęp do historii transakcji płatniczych powyżej 90 dni wymaga dodatkowe uwierzytelniania, albo każde logowanie wymaga dwufaktorowego uwierzytelniania. W tym drugim przypadku jednak szeroko stosowaną praktyką jest możliwość dodania urządzenia (przeglądarki na danym urządzeniu do tzw. listy urządzeń zaufanych, przez co takie urządzenia staje jednym z faktorów – coś co mam).

5.3
Uwierzytelnienie kryptograficzne

Generalnie techniki kryptograficzne można podzielić na „symetryczne" i „asymetryczne". W tych pierwszych obie strony, tj. osoba dokonująca szyfrowania i osoba odszyfrowująca używają tego samego klucza algorytmu kryptograficznego. Najbardziej popularnym przykładem takiego algorytmu jest AES (ang. Advanced Encryption Standard). Natomiast algorytmy kryptografii asymetrycznej używają pary kluczy A i B. Są to klucze komplementarne w tym sensie, że po zaszyfrowaniu wiadomości kluczem A można ją odszyfrować przy pomocy klucza B i odwrotnie. Mechanizm ten jest nazywany podpisem cyfrowym i jest szczególnie użyteczny dla podpisu elektronicznego, o czym więcej można przeczytać w rozdziale 4.1.2.

Uwierzytelnianie oparte na kryptografii wykorzystuje również technologia Block-Chain.

5.3.1
Problem losowości przy generowaniu „haseł jednorazowych"

Ta technika uwierzytelnienia („haseł jednorazowych") bazuje na „wspólnym sekrecie", jaki muszą znać obie strony, czyli jest przykładem techniki „symetrycznej". W najprost-

szej wersji (bez jakiegokolwiek algorytmu kryptograficznego) tworzone są zestawy losowych haseł o długości rzędu 20-30 bitów (kilka znaków). Zestawy te znane są serwerowi (i muszą być przekazane w postaci elektronicznej), jak również są udostępniane klientowi (nośnik tradycyjny – papierowy powoli wychodzi z użycia, zastępuje go SMS oraz tokeny software'owe i sprzętowe). Bezpieczeństwo rozwiązania dotyczy dwóch najważniejszych aspektów: jakości generatora losowego oraz poufności procesu tworzenia, przechowywania i dystrybucji haseł.

Hasła jednorazowe muszą być nieprzewidywalne dla napastnika, który chciałby próbować podszyć się pod uprawnionego klienta. Stąd generator losowy musi tworzyć ciągi bitów, które spełniają wszystkie następujące wymagania:
• nie powinno być wykonalne odróżnienie wyjścia generatora od prawdziwych losowych bitów o rozkładzie równomiernym; innymi słowy wszystkie możliwe serie wyjść ukazują się z równym prawdopodobieństwem;
• dla danego ciągu bitów wyjściowych, nie powinien być znany sposób obliczenia lub przewidzenia, dowolnych innych bitów wyjściowych, ani przeszłych ani przyszłych;
• odpowiednio długi strumień wyjściowy (rzędu kilkudziesięciu bitów) nie powinien powtórzyć się w czasie życia generatora, chyba że zupełnie przypadkowo;
• z punktu widzenia atakującego, wyjście generatora nie powinno powodować wycieku informacji, takich jak jego stan wewnętrzny.

Równie istotna jest pewność, że implementacja generatora pracuje poprawnie, stąd poza powyższymi wymaganiami teoretycznymi należy również zagwarantować spełnienie następujących **wymagań, co do poprawności projektu implementacji i samego działania generatora:**
• implementacja powinna być tak zaplanowana, aby pozwoliła na walidację, łącznie ze specyficznymi założeniami projektowymi. Walidacja generatora oznacza, że zachowuje się on zgodnie z oczekiwaniami nie tylko podczas normalnej pracy, ale też dla przewidzianych granicznych warunków pracy (np. graniczne temperatury pracy). Odgałęzienia w kodzie związane z bezpieczeństwem, które sterują zachowaniem w warunkach wyjątkowych (np. inicjalizacja, nieudane testy itp.) powinny być zweryfikowane za pomocą przemyślanego wymuszenia wszystkich warunków błędu tak, aby wystąpiły podczas testów walidacyjnych;
• powinny istnieć dowody projektowe (teoretyczne, empiryczne lub oba) na poparcie wszystkich wymagań bezpieczeństwa generatora, łącznie z ochroną przed błędnym zachowaniem;
• po wykryciu błędu generator powinien przejść w stan błędu i przestać generować ciąg losowy, a odblokowanie z tego stanu wymaga dodatkowych testów poprawności działania, wywoływanych automatycznie i/lub na żądanie.

Decydując się na wykorzystanie konkretnego generatora losowego zasadnym jest postawienie wymagania, aby był on zgodny z polską normą PN ISO/IEC 18031 „Technika informatyczna – techniki bezpieczeństwa – generowanie bitów losowych". Zgodność z tą normą gwarantuje bowiem spełnienie powyższych wymagań, jednak musi być to potwierdzone za pomocą certyfikatu wydanego przez niezależną trzecią stronę lub przynajmniej za pomocą badań weryfikacyjnych wykonanych przez niezależny od producenta generatora zespół.

Ponieważ norma PN ISO/IEC 18031 została wycofana we wrześniu 2016 i nie została zastąpiona nową, zasadnym jest zatem odwołanie do normy FIPS 186-4 Digital Signature Standard, która wprowadza wymaganie stosowania wyłącznie certyfikowanych na zgodność z FIPS-140 generatorów bitów i liczb losowych.

W warunkach europejskich wystarczające będzie posiadanie przez RNG (ang. Random Number Generator) certyfikatu Common Criteria na poziomie EAL 5+.

Dobrze zaprojektowany i poprawnie używany generator losowy na nic się nie zda, gdy przeciwnik będzie miał dostęp do wygenerowanych losowych haseł. Decydując się na

ten typ uwierzytelnienia należy bezwzględnie sprawdzić na każdym etapie tworzenia i dystrybucji losowych sekretów czy, i ewentualnie kto, ma możliwość uzyskania wglądu do wygenerowanych haseł. Poza takimi aspektami, jak uprawnienia operatorów i administratorów systemów teleinformatycznych, musi być również rozważone ryzyko użycia przez napastnika dodatkowych narzędzi, np. kamer w pomieszczeniu drukującym hasła. W przypadku, gdy jakaś osoba ma legalne prawo dostępu do tworzonych haseł, np. w ramach inspekcji i potwierdzania poprawności działania systemu, należy rozważyć pracę takich osób w reżimie „dwóch-par-oczu" (nigdy nie pozostaje sama) i ryzyko podatności na korupcję i/lub szantaż.

Przechowywanie zestawów haseł na serwerze powinno odbywać się w taki sposób, aby nie można było uzyskać do nich dostępu na podstawie analizy zawartości plików tzw. backup'ów. Można to uzyskać za pomocą wykorzystania do przechowywania haseł dodatkowego urządzenia, zwykle określanego mianem HSM (ang. Hardware Security Module), albo z wykorzystaniem technik kryptograficznych (przechowywane na serwerze zestawy haseł są zaszyfrowane). W tym drugim przypadku jest dodatkowy problem z dostępem do klucza algorytmu szyfrującego, który musi być znany aplikacji działającej na serwerze.

Z kolei zabezpieczenie przygotowanych zestawów haseł po stronie klienta jest trudne do wykonania w przypadku technik tradycyjnych (papier, plastik). W praktyce stosuje się karty-zdrapki, które chronią przed atakiem niewykorzystującym dodatkowe narzędzia typu skaner prześwietlający, i pozwalają – w ograniczony sposób – na zapewnienie detekcji naruszenia zabezpieczenia.

W wersji bardziej zaawansowanej technika „haseł jednorazowych" wykorzystuje algorytm kryptograficzny w postaci tzw. jednokierunkowej funkcji skrótu. Funkcja ma tę właściwość, że dla pewnego argumentu można łatwo obliczyć wartość skrótu będącą liczbą 160-bitową (lub dłuższą), natomiast jest obliczeniowo niemożliwe dokonanie operacji odwrotnej. Tzn. mając wartość skrótu, i znając algorytm działania funkcji, nie jest możliwe odtworzenie argumentu. Ponadto dla dwóch różnych argumentów wyniki funkcji skrótu będą całkowicie różne, tj. nawet gdy argumenty różnią się tylko jednym bitem, ich skróty będą średnio różnić się na połowie pozycji (będą losowe). Przykładem takiej funkcji skrótu jest SHA (ang. Secure Hash Algorithm). W praktycznych zastosowaniach serwer pamięta tylko jedno „długie" losowe hasło „KEY" (zazwyczaj 256-bitowe), natomiast zestawy jednorazowych haseł klienta „H_i" są tworzone w oparciu o indywidualny numer konta klienta (NR_KONTA) i licznik (i), które to wartości – w odróżnieniu od haseł – nie muszą pozostawać poufne:

H_i = SHA (KEY || NR_KONTA || i), gdzie || oznacza konkatenację bitów.

W celu uwierzytelnienia klient przesyła hasło jednorazowe H_i, natomiast serwer jest w stanie niezależnie obliczyć to samo hasło w oparciu o przechowywane „swoje" hasło (KEY), numer konta klienta (NR_KONTA) i zapamiętaną liczbę ostatnich udanych prób uwierzytelnień (i). Jest również dopuszczalne przekazywanie jawnie w kanale łączności parametru „i" razem z hasłem jednorazowym H_i – dla bezpieczeństwa protokołu uwierzytelnienia nie ma to praktycznego znaczenia, o ile funkcja skrótu jest odpowiednio zaimplementowana i klucz KEY pozostaje nieznany atakującemu.

Zauważmy, że w scenariuszu z użyciem kryptograficznej funkcji skrótu w technice haseł jednorazowych można stosunkowo prosto zapewnić ochronę sekretów po stronie serwera – wystarczy jedno losowe hasło (KEY), które będzie przechowywane tylko

w urządzeniu HSM. Oczywiście, wymagania co do losowości tego hasła pozostają w mocy (patrz „Generator losowy"). Na rynku dostępne są również warianty tej metody uwierzytelnienia ze sprzętową ochroną haseł jednorazowych po stronie klienta. W takim przypadku klient dysponuje sprzętowym tokenem, który w niedostępnej do odczytu miejscu pamięci przechowuje klucz poufny (KEY_{NR_TOKEN}). Każdy token ma klucz indywidualny, który jest obliczany z klucza losowego serwera (KEY) wg następującego wzoru:

$$KEY_{NR_TOKEN} = SHA\ (KEY\ ||\ NR_TOKEN) \qquad (\&).$$

Natomiast hasło jednorazowe H_i jest generowane przez token w oparciu o aktualną datę i czas („jednorazowość" hasła klienta polega na tym, że zmienia się w każdej minucie) (DATA_TIME) z dokładnością do 1 minuty oraz klucz indywidualny tokena:

$$H_i = SHA\ (KEY_{NR_TOKEN}\ ||\ DATA_TIME) \qquad (\&\&).$$

W tym mechanizmie uwierzytelnienia serwer również pamięta tylko swój klucz losowy KEY i dysponuje tablicą powiązań „nazwa konta" – „nr tokenu". W celu sprawdzenia poprawności hasła H_i wykonuje dwie operacje: w pierwszej oblicza KEY_{NR_TOKEN} wg wzoru (&), a w drugiej hasło jednorazowe wg schematu (&&). Jednym z powszechnie używanych w Polsce tego typu rozwiązań haseł jednorazowych, ze sprzętową ochroną klucza po stronie klienta, jest produkt „SecurID" serii 700 firmy RSA Security. Strategia dostarczania i implementacji tego typu uwierzytelnienia zakłada, że producent samodzielnie generuje dla danej sieci klucz KEY i klucze tokenów KEY_{NR_TOKEN}. Po spersonalizowaniu tokenów ich klucze są kasowane, natomiast klucz KEY jest zapamiętywany przez producenta, gdyż ewentualne rozszerzenie zamówienia o dodatkową pulę tokenów w sieci wymaga jego znajomości. Reputacja RSA Security ostatnio znacznie ucierpiała, gdyż firma oznajmiła, że doszło do kradzieży kluczy i de facto kompromitacji ich aktualnie wdrożonych rozwiązań. Wynika z tego, że decydując się na konkretne rozwiązanie należy brać pod uwagę ryzyko ujawnienia sekretów po stronie producenta/dostawcy i raczej wybierać takie, które pozwalają na generację kluczy dopiero w miejscu eksploatacji.

Dodatkowe informacje nt. implementacji rozwiązań opartych o technikę haseł jednorazowych można znaleźć w rozdziale 5.3.1

5.3.1.1
SSL/TLS z mechanizmem „pre-shared key" lub certyfikatami X.509

Często mamy do czynienia z połączeniem on-line klienta (hostem) z serwerem aplikacyjnym. W „zwykłych" zastosowaniach protokół http jest wystarczający, natomiast wymaga się dwustronnego uwierzytelnienia między hostem i serwerem oraz zestawienia poufnego (szyfrowanego) połączenia. W takiej sytuacji można zastosować protokół https zamiast zwykłego http. Standardy przewidują kilka wariantów zestawiania takiego połączenia, a jednym z nich jest technika pre-shared key, gdzie - w celu wzajemnego uwierzytelnienia i ustanowienia klucza sesyjnego - obie strony połączenia wcześniej przekazują sobie wspólny sekret (hasło). W tym sensie jest to symetryczna technika kryptograficzna, w której obie strony dysponują tym samym kluczem, identycznie jak w przypadku połączeń WiFi opartych o parametr „PSK". Dobre praktyki IT wymagają, aby taki klucz nie był używany zbyt długo (np. nie dłużej niż kilka miesięcy) i był zawsze wymieniany w przypadku kompromitacji (lub nawet tylko podejrzenia, iż do niej doszło).

Dokumenty standaryzacyjne definiujące użycie techniki pre-shared key (PSK) w protokole SSL/TLS (RFC 4279, 4785 i 5487) określają, że ten typ symetrycznego uwierzytelnienia kryptograficznego może być połączony z algorytmami asymetrycznymi. Przykładem

jest wykorzystanie współdzielonego klucza PSK do uwierzytelnienia klucza sesyjnego uzgodnionego za pomocą protokołu Diffiego-Hellmana (algorytmu z rodziny „asymetrycznych") oraz wykorzystania klucza PSK tylko do uwierzytelnienia klienta, wykonując jednocześnie uwierzytelnienie serwera za pomocą certyfikatów klucza publicznego z algorytmem RSA.

5.3.2
Mechanizmy uwierzytelnienia oparte o kryptografię asymetryczną

Jak wspomniano wcześniej, asymetryczne algorytmy kryptograficzne używają pary kluczy: publicznego i prywatnego. Złożenie podpisu wymaga użycia klucza prywatnego, natomiast weryfikacja podpisu odbywa się z wykorzystaniem klucza publicznego, komplementarnego z prywatnym. W celu złożenia podpisu pod pewną wiadomością w postaci elektronicznej można byłoby teoretycznie całą wiadomość zaszyfrować kluczem prywatnym. Wykorzystując np. 2048-bitowy klucz algorytmu RSA należałoby wiadomość podzielić na 2 kB części i po kolei szyfrować. Jednak tego typu działanie byłoby bardzo mało efektywne, szczególnie, iż algorytmy asymetryczne szyfrują kilkaset razy wolniej niż algorytmy symetryczne. Stąd w praktycznych zastosowaniach, w celu podpisania wiadomości, dokonuje się tylko jednokrotnego szyfrowania przy pomocy klucza prywatnego. Nie szyfruje się bowiem po kolei poszczególnych partii pliku, a jedynie jego skrót obliczony przy pomocy „kryptograficznej funkcji skrótu", np. z rodziny SHA. Taka funkcja skrótu wykonuje się szybko (prędkość działania jest porównywalna z algorytmami symetrycznymi) i ma m.in. tą właściwość, że jest obliczeniowo niemożliwe stworzenie dwóch wiadomości, które miałyby ten sam skrót. Weryfikacja podpisu wymaga, aby stosowna aplikacja dokonała jeszcze raz obliczenia skrótu wiadomości i porównania, czy obliczony skrót zgadza się z ciągiem otrzymanym w wyniku odszyfrowania pola „podpis" przy pomocy klucza publicznego. Ta zgodność potwierdza tzw. matematyczną poprawność podpisu, natomiast „ważność prawna" podpisu zachodzi dopiero po zweryfikowaniu, że w momencie składania podpisu para kluczy podpisującego (prywatny i publiczny) była „ważna".

Jednak na jakiej podstawie weryfikujący podpis dokonuje powiązania klucza publicznego z konkretnym podmiotem (osobą, serwerem) i jak sprawdza ich „ważność"? Służą do tego „certyfikaty klucza publicznego" wydane w ramach infrastruktury PKI (ang. Public Key Infrastructure). W takiej infrastrukturze występuje urząd certyfikacji CA (ang. Certification Authority), który pełni rolę „zaufanej trzeciej strony". Wydawane przez CA certyfikaty, zgodne z normą X.509, to nic innego niż struktura danych w postaci elektronicznej, która zawiera m.in.: nazwę właściciela, jego klucz publiczny, datę ważności („nie wcześniej niż" i „nie później niż"), dopuszczalny sposób wykorzystania klucza, nazwę wystawcy i podpis wystawcy certyfikatu. Wystarczy więc zaufać kluczowi publicznemu CA, aby przy jego pomocy weryfikować podpisy pod certyfikatami kluczy publicznych użytkowników i w ten sposób uzyskiwać pewność, że podpisującym (właścicielem klucza publicznego) jest dana osoba.

Zauważmy, że używanie algorytmów asymetrycznych do uwierzytelnienia bez stosownej infrastruktury PKI, i tym samym wykorzystywania pewnych sformalizowanych struktur danych, czyni takie rozwiązanie podatnym na szereg ataków i nie powinno być stosowane. Inną kwestią jest natomiast odpowiedź na pytanie, czy tworzyć własną infrastrukturę PKI, czy skorzystać z już istniejącej na rynku? Problem ten wykracza poza ramy niniejszego opracowania.

Podpisy elektroniczne oparte o asymetryczne algorytmy kryptograficzne są metodą uwierzytelnienia powszechnie stosowaną w obecnych i przyszłych systemach teleinformatycznych. Ma ona szereg zalet, w tym stosunkowo proste wsparcie dla mechanizmów niezaprzeczalności (patrz pkt dot. normy PN ISO/IEC 13888). Jednak równocześnie należy brać pod uwagę zagrożenia wiążące się z tą technologią. Jednym z istotniejszych wśród nich jest aspekt poufności klucza prywatnego. Jego pozyskanie przez atakującego ma katastrofalne skutki – podpisy składane przez napastnika z wykorzystaniem skompromitowanego klucza prywatnego będą bowiem nierozróżnialne pod względem technicznym i prawnym od podpisów elektronicznych legalnego właściciela. Jeśli ma on świadomość kompromitacji swojego klucza prywatnego, powinien niezwłocznie unieważnić swój certyfikat, jednak do tego czasu napastnik może składać w jego imieniu oświadczenia woli. Podobnie jak z techniką haseł jednorazowych, o której mowa wyżej, istnieją dwa podstawowe warianty przechowywania klucza prywatnego algorytmu asymetrycznego: z i bez wykorzystania sprzętowego tokena.

5.3.2.1
PKI z tokenem programowym

W najprostszej i zarazem najtańszej wersji klucz prywatny służący do podpisów jest przechowywany w pliku dyskowym. Jednocześnie plik ten jest zaszyfrowany przy pomocy hasła, stąd zwykłe skopiowanie danych nie pozwala atakującemu na pozyskanie klucza. Aby tego typu ochrona dawała chociaż pewne podstawowe bezpieczeństwo przed niektórymi atakami, implementujący powinien wykorzystać sformalizowane struktury danych, w tym przede wszystkim standard PKCS#12 i PKCS#5. Niemniej jednak przechowywanie klucza w pliku dyskowym nierozerwalnie związane jest z koniecznością jego „eksportu" do aplikacji podpisującej, która dokonuje przekształceń matematycznych z jego udziałem. Stąd w takim rozwiązaniu zawsze zawiera się ryzyko, iż atakujący zainstaluje w środowisku teleinformatycznym podpisującego specjalny exploit, który skopiuje wyeksportowany do aplikacji klucz prywatny i prześle go napastnikowi.

Wariantem przechowywania klucza prywatnego w pliku dyskowym jest, wprowadzona przez regulację eIDAS, możliwość przechowywania kwalifikowanego certyfikatu podpisu elektronicznego w chmurze, pod warunkiem zachowania standardów bezpieczeństwa. Otwiera to całkiem nowe możliwości popularyzacji użycia kwalifikowanego podpisu elektronicznego, ponieważ jego certyfikat jest wówczas dostępny z każdego miejsca bez konieczności posiadania sprzętowego nośnika certyfikatu (karty podpisu) oraz komputera wyposażonego w czytnik kart.

5.3.2.2
PKI z tokenem sprzętowym

Bardziej bezpieczne rozwiązanie podpisów elektronicznych opartych o asymetryczne algorytmy kryptograficzne polega na przechowywaniu klucza prywatnego w specjalnym tokenie sprzętowym. Wykonywanie operacji matematycznych odbywa się również w tokenie, stąd klucz prywatny do podpisów nie jest eksportowany do aplikacji. W takim rozwiązaniu atakujący nie jest w stanie skopiować klucza i pozostają mu jedynie ataki obliczone na GUI (ang. Graphical User Interface – interfejs graficzny użytkownika), czyli „podmianę" interfejsu graficznego – podpisujący w dobrej wierze decyduje się złożyć np. pewne oświadczenie woli, którego treść widzi na ekranie, natomiast w rzeczywistości podpisuje coś innego.

Decydując się na użycie tokena sprzętowego najlepiej wybrać taki, który przeszedł ewaluację i posiada status „bezpiecznego urządzenia do składania podpisów elektronicz-

nych" w rozumieniu przepisów ustawy o podpisach elektronicznych (zob. rozdział 6.1.2). Taki sprzętowy token jest nieklonowalny, tj. nie jest możliwe, nawet przy wykorzystaniu specjalistycznego sprzętu, sporządzenie kopii klucza prywatnego służącego do składania podpisów.

Należy podkreślić, iż wg metodyk określania poziomów wiarygodności w dokumentach [2] i [3], zastosowanie kryptografii asymetrycznej i PKI wraz z tokenem sprzętowym pozwala na osiągnięcie najwyższego (4) poziomu.

5.3.3
Podpis serwerowy

W niniejszym pkt. opracowania zostaną omówione kwestie podpisów serwerowych, które są modyfikacjami standardowych rozwiązań PKI z tokenami programowymi lub sprzętowymi, a mianowicie:podpis zaufany, podpis w locie oraz popisy chmurowe". Podpis zaufany nie jest oparty o standardowe mechanizmy certyfikatu wydanego dla osoby podpisującej, jest rozwiązaniem czysto polskim. Podpis w locie oraz podpisy chmurowe są standardowymi rozwiązaniami podpisów cyfrowych opartymi o klucze przetwarzane w infrastrukturze dostawcy usługi podpisu.

5.3.3.1
Podpis zaufany

W standardowej implementacji podpisu cyfrowego każdy z podpisujących ma swoją parę kluczy asymetrycznego algorytmu kryptograficznego i przechowuje je w tokenie software'owym (programowym) lub sprzętowym. Jednocześnie podpisujący (i weryfikujący) musi uzyskać potwierdzenie, że jego podpisy są weryfikowane przy pomocy konkretnego klucza publicznego. To potwierdzenie ma postać certyfikatu zgodnego z normą X.509 i poza kluczem publicznym zawiera szereg dodatkowych informacji użytecznych dla aplikacji weryfikującej podpisy elektroniczne („podpisy cyfrowe" w przypadku logowania on-line).

Podpis zaufany nie należy do kategorii standardowej implementacji PKI. Otóż, w jego przypadku podpis jest oparty o zabezpieczenie integralności i autentyczności realizowane pieczęcią elektroniczną Ministra Cyfryzacji. Innymi słowy, podpis zaufany powstaje w systemie nadzorowanym przez Ministra Cyfryzacji poprzez uwierzytelnienie i identyfikację podpisującego, skompletowanie oświadczenia woli oraz zabezpieczenie danych identyfikujących podpisującego oraz treści oświadczenia woli za pomocą pieczęci elektronicznej przypisanej do Ministra Cyfryzacji. Dzięki takiemu podejściu podpis zaufany może powstać tylko i wyłączenie w systemie nadzorowanym przez MC oraz po realizacji określonej procedury utworzenia podpisu zaufanego.

W systemach zewnętrznych podpis zaufany jest widoczny jako pieczęć Ministra Cyfryzacji, natomiast atrybuty tej pieczęci określają szczegółowo osobę, która złożyła podpis zaufany oraz informację, że jest to podpis tej osoby. Podpis zaufany jest silnie związany z Profilem zaufanym, który stanowi środek identyfikacji elektronicznej dla podpisu zaufanego.

5.3.3.2
Podpis chmurowy

Podpis chmurowy jest standardowym rozwiązaniem podpisu cyfrowego opartym o asymetryczne klucze kryptograficzne. Różnica w stosunku do podpisów opartych o karty

kryptograficzne polega na tym, że klucze prywatne przechowywane są w infrastrukturze dostawcy usługi zaufania i dostępne są dla podpisującego po uprzednim uwierzytelnieniu. Ta technologia pozwala na rezygnację z kart kryptograficznych, oparcie uwierzytelnienia na telefonie komórkowym. Dodatkową zaletą podpisów chmurowych jest brak powiązania z urządzeniem, a co za tym idzie brak konieczności instalacji sterowników kart kryptograficznych i indywidualnej konfiguracji stacji roboczej do składania podpisu. Aktualnie podpisy chmurowe są bardzo rozwijane przez wielu dostawców usług zaufania, są także wspierane przez działania standaryzacyjne. W ostatnich latach powołano Cloud Signature Consortium, które skupia wielu dostawców usług zaufania oraz jednostki naukowe. Celem CSC jest rozwój podpisów serwerowych.

5.3.3.3
Podpis w locie

Podpis w locie jest w rzeczywistości podpisem chmurowym realizowanym w oparciu o certyfikat i dane identyfikacyjne użyte jednorazowo. Typowa struktura działania podpisu w locie obejmuje identyfikację elektroniczną, wydanie certyfikatu oraz złożenie podpisu w jednej iteracji z użytkownikiem. Podpisy w locie wymagają szybkiej i zdalnej identyfikacji elektronicznej, natomiast pozwalają na zmianę modeli biznesowych stosowania certyfikatu wydanego tylko na potrzeby pojedynczego oświadczenia woli lub pojedynczego procesu biznesowego. Technicznie certyfikat takiego podpisu elektronicznego może być wtedy wydany jako biznesowo krótkoterminowy, choć faktycznie byłby nie tyle jednorazowy, co udostępniony wyłącznie w określonym procesie (np. podpisania umowy) oraz z terminem ważności istotnie ograniczonym (np. 1 godzina).

5.3.4
Dowody niezaprzeczalności

Implementujący mechanizmy elektronicznego uwierzytelnienia powinien brać również pod uwagę aspekt posiadania dowodów w przypadku sporów z klientem, który może kwestionować w ogóle fakt wydawania jakichś dyspozycji w oparciu o wcześniej zrealizowany (ze skutkiem pozytywnym) proces elektronicznej identyfikacji i/lub uwierzytelnienia. Pozostawienie problemu dowodowego działowi IT, który z kolei będzie opierał się o ogólne zapisy rejestrów zdarzeń występujących w systemie teleinformatycznym firmy, może nie być wystarczające, albo bardzo trudno akceptowalne. Wynika to z tego, że w przypadku pominięcia problemu dowodów na etapie projektu, w konsekwencji zapewne trzeba będzie udostępniać biegłemu całe rejestry zdarzeń systemowych i obszerne opisy używanych rozwiązań. Jak wobec tego polepszyć swoją pozycję „dowodową" w przypadku ewentualnego sporu, co do skuteczności środków elektronicznego uwierzytelnienia? Wydaje się, że warto rozważyć zastosowanie mechanizmów, które będą zgodne z normą PN-ISO/IEC 13888 Technika informatyczna – Techniki zabezpieczeń – Niezaprzeczalność. „Niezaprzeczalność" wg tej normy wymaga wystawienia poświadczenia, które może być wykorzystywane w celu udowodnienia, że wystąpił określony rodzaj zdarzenia lub działania. Poświadczenia mogą być przechowywane (pod pewnymi warunkami) lub przekazywane w trakcie wymiany niezaprzeczalności pomiędzy zaangażowanymi podmiotami.

Norma składa się z trzech arkuszy:
- arkusz 1: Model ogólny,
- arkusz 2: Mechanizmy wykorzystujące techniki symetryczne,
- arkusz 3: Mechanizmy wykorzystujące techniki asymetryczne.

Techniki „asymetryczne” związane są z certyfikatami klucza publicznego X.509, natomiast „symetryczne” z tzw. bezpiecznymi kopertami, przy czym oba rozwiązania oparte są na kryptograficznej wartości kontrolnej zapewniającej integralność poświadczanych danych, czyli jeden
z podstawowych atrybutów bezpieczeństwa.

Norma przewiduje następujące tokeny niezaprzeczalności, odpowiadające poszczególnym rodzajom tradycyjnych „pieczęci”, stosowanych w realnym świecie (np. pieczątka „dziennik podawczy”):
• niezaprzeczalność pochodzenia,
• niezaprzeczalność dostarczenia,
• niezaprzeczalność przedłożenia,
• niezaprzeczalność przesłania.

Ogólny token niezaprzeczalności składa się z „odcisku wiadomości”, który zapewnia integralność poświadczanej wiadomości i poniższych danych (obligatoryjnych i fakultatywnych):
• identyfikatora polityki niezaprzeczalności, którą stosuje się do poświadczania,
• rodzaju świadczonej usługi niezaprzeczalności,
• identyfikatora wyróżniającego podmiotu poświadczenia,
• identyfikatora wyróżniającego wystawcy poświadczenia w przypadku, gdy nie jest on podmiotem poświadczenia,
• identyfikatora wyróżniającego podmiotu, współpracującego z podmiotem poświadczenia (np. nadawcy wiadomości, albo odbiorcy, dla którego przeznaczono wiadomość albo organu dostarczającego),
• identyfikatora wyróżniającego żądającego poświadczenie w przypadku, gdy nie jest on podmiotem poświadczenia,
• identyfikatorów wyróżniających pozostałych podmiotów, zaangażowanych w działanie (np. odbiorców, dla których przeznaczono wiadomość),
• daty oraz czasu wystawienia poświadczenia,
• daty oraz czasu zajścia zdarzenia lub podjęcia działania,
• danych opcjonalnych, które wymagają ochrony pochodzenia/integralności.

Tworzenie takich „tokenów niezaprzeczalności” pozwala na proste udowodnienie w sądzie, że działania firmy były zgodne z dyspozycjami klienta i będą mogły być selektywnie udostępniane w toku postępowania arbitrażowego.

5.4
Uwierzytelnienie biometryczne

5.4.1
Pojęcia i definicje

Biometria – dział informatyki dotyczący metod automatycznego rozpoznawania tożsamości z wykorzystaniem własności fizycznych (np. odcisk palca, układ żył krwionośnych w palcu lub dłoni) oraz zachowania (np. barwa głosu, podpis odręczny) człowieka.

Dane biometryczne – dane na dowolnym etapie przetwarzania będące wynikiem pomiaru biometrycznego (np.: dane surowe, czyli próbki biometryczne, cechy biometryczne, wzorce biometryczne).

Cechy biometryczne – liczby lub etykiety (np.: minucje odcisku palca, bity kodu żył krwionośnych palca lub dłoni, średnia prędkość składania podpisu odręcznego) wyzna-

czone na podstawie próbki biometrycznej i używane w porównywaniu biometrycznym.

Wzorzec biometryczny – zbiór cech biometrycznych wykorzystywany w bezpośrednim porównywaniu z cechami badanej próbki biometrycznej.

Biometryczne dane referencyjne – dane biometryczne (np. próbki lub cechy) przypisane do tożsamości i zachowane w systemie w celu późniejszego rozpoznawania tożsamości.

5.4.2
Wstęp do biometrii

Powszechnie uznaje się, że uwierzytelnienie następuje na podstawie tego:

co znamy:	hasło/PIN - ciąg liter/cyfr pamiętany przez petenta, nazwisko panieńskie matki itp.
co posiadamy:	kartę elektroniczną, certyfikat cyfrowy, dowód osobisty, paszport, legitymację, rekomendacje/listy polecające, urządzenie mobilne (np. smartfon, tablet)
czym naprawdę jesteśmy	biometrii

Dwie pierwsze metody nie uwierzytelniają konkretnej osoby, a jedynie kogoś, kto dysponuje określoną wiedzą lub posiada określone przedmioty; nie są w stanie odróżnić osoby uprawnionej od kogoś, kto wszedł w posiadanie wiedzy lub przedmiotów osoby uprawnionej. Aby nadać większą rangę prawną tym metodom stosuje się umowy, porozumienia lub odbiera oświadczenia o właściwym wykorzystywaniu tych metod.

Biometria jest najlepszą i najbardziej obiektywną metodą weryfikacji tożsamości, co zawdzięcza dwóm szczególnym cechom, jakich nie posiadają inne metody weryfikacji:
- cechy biometryczne nie zmieniają się z wiekiem danej osoby,
- nie ma dwóch osób o identycznych cechach biometrycznych.

Biometryczna weryfikacja tożsamości – uwierzytelnianie - to proces porównania typu „1 do 1" (1: 1) badanego wzorca biometrycznego odpowiadającego deklarowanej tożsamości (np. nr PESEL, nr klienta, nr karty kredytowej, nr telefonu, nr konta) z biometrycznymi danymi referencyjnymi zapisanymi w centralnej bazie danych lub na karcie elektronicznej, urządzeniu mobilnym względnie innym nośniku. System biometryczny weryfikuje i potwierdza tożsamość i najczęściej (głównie ze względów bezpieczeństwa) prezentuje swoją decyzję w formie binarnej (tak/nie).

Należy tu wyjaśnić różnicę pomiędzy identyfikacją a uwierzytelnianiem.

Identyfikacja jest procesem potwierdzania tożsamości poprzez wyszukanie jej w dostępnych bazach danych – przy użyciu biometrii jest stosowane zatem porównanie 1:n.

Uwierzytelnianie jest procesem potwierdzania tożsamości osoby uprzednio zidentyfikowanej – w taki przypadku trzeba tylko sprawdzić, czy osoba zidentyfikowana – np. przez login lub nazwę użytkownika – jest tą, za którą się podaje. Przy użyciu biometrii stosuje się tu porównanie 1:1.

Biometria to technika pomiaru istot żywych w celu automatycznego rozpoznawania osób. Metody biometryczne dzielą się na dwie podgrupy:
• badające cechy fizyczne / biologiczne,
• badające cechy zachowania (behawioralne).

Koncepcja tworzenia cech biometrycznych – twarzy i odcisku linii papilarnych.

Stosowane w biometrii cechy biologiczne to:
• linie papilarne – odciski palców,
(prawdopodobieństwo błędnej akceptacji lub odrzucenia 10^{-6}),
• geometria dłoni, twarzy (10^{-4}),
• DNA (trudno odróżnić bliźniaków),
• obraz siatkówki, tęczówki (10^{-7}),
• naczynia krwionośne palca (ang. Finger Vein) i dłoni (ang. Palm Vein).

Stosowane w biometrii cechy behawioralne to:
• podpisy - kształt i dynamika,
• głos,
• dynamika pisania na klawiaturze (ang. keystroke pattern),
• chód – sposób chodzenia (ang. gait), etc.

Metody biometryczne składają się z dwu etapów:
Rejestracji/akwizycji danych i właściwej identyfikacji/uwierzytelnienia.

Rejestracja/akwizycja danych (zapisywanie obrazu i/lub tworzenie bazy danych):
• pozyskanie wybranej cechy biometrycznej - czytnik biometryczny skanuje określoną cechę biometryczną osoby ubiegającej się o dostęp do systemu,
• przetwarzane do postaci cyfrowej, filtrowanie i tworzenie wzorca,
• zapisywanie wzorca w lokalnym lub centralnym repozytorium, lub przenośnym nośniku takim jak karta elektroniczna lub urządzenie mobilne.

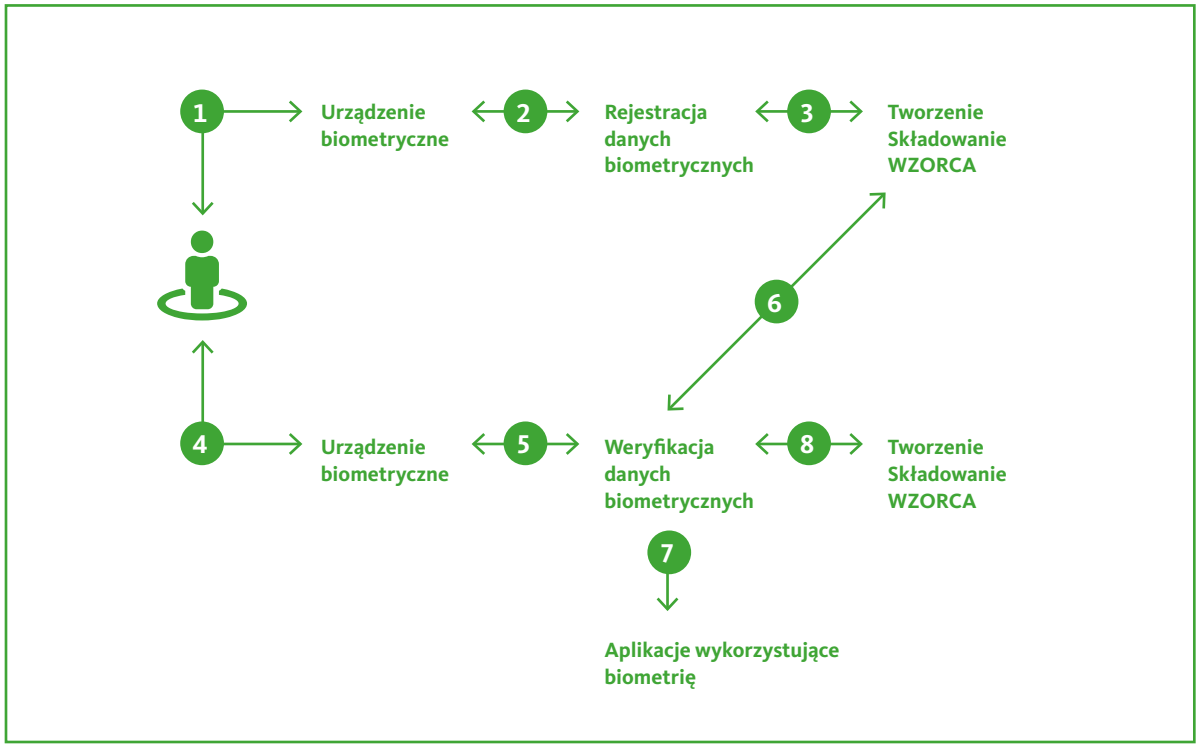
Właściwa identyfikacja/uwierzytelnienie (lub weryfikacja), zwana często fazą operacyjną:
• bieżące skanowanie cechy biometrycznej osoby chcącej uzyskać dostęp do systemu,
• przetwarzanie otrzymanych danych w sposób analogiczny jak na etapie akwizycji danych, aż do uzyskania formatu identycznego z formatem zakodowanego wcześniej wzorca,
• porównanie otrzymanych charakterystyk ze wzorcem,
• dostarczenie wyniku porównania do aplikacji biznesowej, która rozstrzyga o dopuszczeniu lub odrzuceniu potencjalnego użytkownika,
• zapisanie danych do audytu, zgodnie z wymaganiami.

Ilustracja 6 przedstawia schemat wykorzystania biometrii do uwierzytelnienia. Przebieg procesu jest następujący:
1. pozyskanie wybranej cechy biometrycznej - czytnik biometryczny skanuje określoną cechę biometryczną osoby ubiegającej się o dostęp do systemu;
2. przetwarzane do postaci cyfrowej, filtrowanie i tworzenie wzorca;
3. zapisywanie wzorca w lokalnym lub centralnym repozytorium lub przenośnym tokenie takim jak karta elektroniczna;
4. bieżące skanowanie cechy biometrycznej osoby chcącej uzyskać dostęp do systemu;
5. przetwarzanie otrzymanych danych w sposób analogiczny jak na etapie akwizycji danych, aż do uzyskania formatu identycznego z formatem zakodowanego wcześniej wzorca;

6. porównanie otrzymanych charakterystyk ze wzorcem;
7. dostarczenie wyniku porównania do aplikacji biznesowej, która rozstrzyga o dopuszczeniu lub odrzuceniu potencjalnego użytkownika;
8. zapisanie danych do audytu, zgodnie z wymaganiami.

Przetworzenie danych biometrycznych do postaci wzorca odbywa się za pomocą koderów. Otrzymane wzorce mogą być specyficzne dla producenta algorytmów biometrycznych lub uniwersalne, zgodne z przyjętymi normami.

RYSUNEK 5. Schemat wykorzystania biometrii do uwierzytelnienia.



RYSUNEK 6. Przetworzenie danych biometrycznych.

Poniższa tabela przedstawia zestawienie najpopularniejszych metod biometrycznych na rynku.

TABELA 6*.

Modalność biometryczna	Opis metody	Wybrani producenci urządzeń/rozwiązań
Odcisku palca	Bazuje na układzie punktów charakterystycznych (minucji) linii papilarnych	NEC, IDEMIA, Precise, Crossmatch, Thales
Tęczówki oka	Bazuje na cechach charakterystycznych tęczówki oka	Panasonic, IDEMIA, LG, IrisGuard
Naczyń krwionośnych palca	Bazuje na unikalnym wzorze układu naczyń krwionośnych wewnątrz palca	Hitachi (Hitachi Ltd., Hitachi Omron Terminal Solutions), NEC, Sony
Naczyń krwionośnych dłoni	Bazuje na unikalnym wzorze układu naczyń krwionośnych wewnątrz ludzkiej dłoni	Fujitsu
Rozpoznawanie twarzy	Bazuje na analizie obrazu twarzy	Aurora, IDEMIA, NEC, Innovatrics
Odcisku dłoni i jej elementów	Bazuje na odcisku całej dłoni, krawędzi dłoni lub innych jej elementów	IDEMIA
Geometria dłoni	Bazuje na cechach charakterystycznych kształtu dłoni	HandPunch,
Głosowa	Bazuje na analizie charakterystyki głosu	Nuance, EasyVoiceBiometrics, Salmat, SentryCom
Podpis odręczny	Bazuje na charakterystyce wizualnej podpisu (dwuwymiarowy obraz), ale także na sposobie, w jaki podpis został złożony, tj. dynamice ruchu pióra	Xyzmo, Wacom
Dynamika pisania na klawiaturze	Bazuje na unikalnym sposobie pisania na klawiaturze lub używania ekranu dotykowego smartfona/tabletu	TypingDNA, BioCatch,

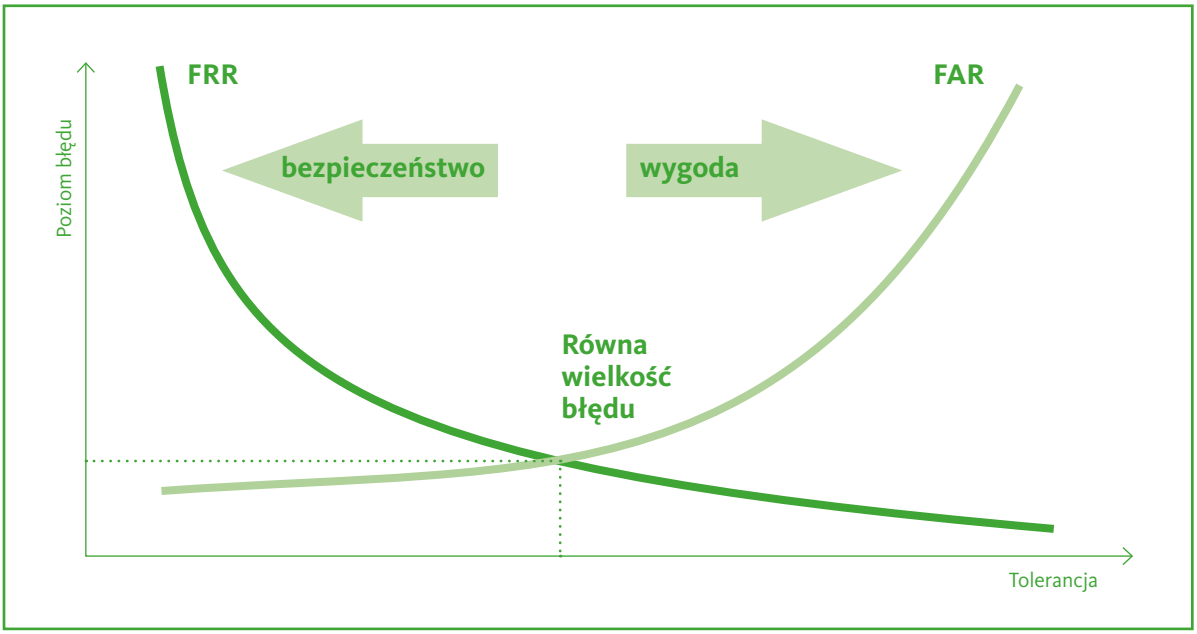
** Źródło RAPORT BIOMETRYCZNY 2.0 „Bankowość biometryczna" Grupa ds. Biometrii FTB.*

Niezawodność poszczególnych modalności biometrycznych warunkuje ich przydatność w różnych zastosowaniach. Niektóre algorytmy biometryczne znalazły w ostatnich latach szerokie zastosowanie w bankowości dzięki znacznej poprawie ich parametrów.

Niezawodność algorytmów biometrycznych opisuje się głównie przez podanie 2 podstawowych parametrów:
• Wskaźnik błędnego odrzucenia (ang. False Rejection Rate – FRR) – prawdopodobieństwo, że osoba uprawniona zostanie odrzucona,
• Wskaźnik błędnej akceptacji (ang. False Acceptance Rate – FAR) – prawdopodobieństwo, że osoba nieuprawniona zostanie zaakceptowana.

Oba wskaźniki są od siebie zależne, przy czy każdy opisuje inną cechę systemu biometrycznego:

RYSUNEK 7. Zależność błędnego odrzucenia i błędnej akceptacji.



Punkt pracy systemu, tj. decyzja czy bardziej istotny jest parametr FAR czy FRR (bezpieczeństwo czy wygoda) zależy od decyzji integratora systemu.

Należy też zauważyć, że na wynik porównania biometrycznego zasadniczy wpływ ma jakość pobranej próbki biometrycznej (zdjęcie twarzy, odcisku palca itp.) Podanie precyzyjnego parametru liczbowego niezawodności wymagałoby dokładnego określenia parametrów jakościowych próbki biometrycznej Poniższa tabela przedstawia wskaźniki niezawodności biometrycznej weryfikacji dla typowych dla bankowości jakości próbek biometrycznych:

TABELA 7*.

Porównanie 1:1	Twarz	Odcisk palca	Tęczówka
Wskaźnik błędnego odrzucenia (ang. False Rejection Rate – FRR) np. uprawniony, lecz niezaakceptowany (ang. Authorized but rejected)	0,6 – 2%	0,1 – 0.5%	0,1 – 2%
Wskaźnik błędnej akceptacji (ang. False Acceptance Rate – FAR) np. nieuprawniony, lecz zaakceptowany (ang. Unauthorized but accepted)	0,01% – 0,1%	1E-05% – 0,01%	1E-06% – 0,01%
Wskaźnik niemożności rejestracji (ang. Failure to Enroll Rate)	0%	0,1– 2%	0.5 – 2%

** Źródło (Source): National Institute of Standards and Technology report 2019.*

Przedstawione wskaźniki będą ulegać polepszeniu z poprawą technologii i poprzez użycie dwu lub więcej identyfikatorów biometrycznych – obecnie przy użyciu wizerunku twarzy i 4 odcisków palców uzyskuje się poprawność blisko 100%.

Dodatkowymi parametrami przydatnymi w ocenie algorytmu biometrycznego są:

- wielkość wzorca biometrycznego pojedynczej próbki – ma znaczenie przy konieczności przechowywania dużych baz danych. Najmniejsze obecnie wzorce biometryczne mają ok 500 bajtów,
- szybkość porównania biometrycznego – ma znaczenie przy konieczności przeszukiwania dużych baz danych. Najszybsze algorytmy osiągają obecnie ok 1 ms,
- szybkość kodowania (przetwarzania próbki biometrycznej we wzorzec) – ma znaczenie przy rejestracji dużych ilości nowych próbek – najlepsze obecnie wyniki to ok. 110 ms.

Dodatkowo warto podkreślić, że dla jakości danych biometrycznych kluczowa jest pewność od kogo zostały zebrane. Dlatego inną jakość będą miały odciski palca pobrane w banku czy urzędzie, a inną przypisanie wcześniej pobranych odcisków palca do aplikacji mobilnej na komputerze, gdzie dostawca aplikacji nie ma dostępu do odcisków palca ani do procesu pobranie tych odcisków. Przypisania cech bazujących na biometrii jest wyłącznie deklaratywne, nie zmienia to jednak wartości tej metody, kluczowa jest jednak edukacja klientów o znaczeniu nie rejestrowania odcisków palców innych osób na urządzeniach wykorzystywanych do czynności sensytywnych (np. bankowości).

5.4.3 Mechanizmy odporności na ataki

Najbardziej rozpowszechnioną metodą ataku jest próba użycia sztucznych obiektów do dostarczenia próbki biometrycznej. Inną, nieco mniej popularną, jest wykorzystanie czyjejś osoby bez jej wiedzy i zgody.

Poniższa tabela przedstawia przykłady narzędzi i metod ataków na systemy biometryczne:

TABELA 8.

Rodzaj ataku	Kategoria narzędzia ataku	Przykładowe narzędzia
Sztuczne obiekty	Całkowite	Sztuczny palec,
	Częściowe	Naklejka na palcu, okulary, szkła kontaktowe
Z wykorzystaniem czynnika ludzkiego	Martwe	Martwe ciało, odcięty palec/ręka
	Zmodyfikowane	Okaleczenie, chirurgiczna zmiana odcisków palców między palcami rąk i/lub nóg, chirurgiczna zmiana twarzy
	Niezgodne	Mimika, czubek lub krawędź palca
	Wymuszone	Wykorzystanie braku przytomności, wymuszenie groźbą lub podstępem
	Zgodne	Bliźniak, sobowtór

W celu zapobieżenia atakom producenci systemów biometrycznych stosują rozmaite techniki wykrywania żywotności (ang. Liveness detection). Techniki te można podzielić na:

- statyczne – polegają na analizie próbki biometrycznej pod kątem prawdopodobieństwa, że pochodzi ze sztucznego obiektu bądź została pobrana bez wiedzy i zgody właściciela,
- behawioralne – wymagają aktywnego udziału użytkownika, który wykonuje czynności zlecone przez system biometryczny.

Poniższa tabela przestawia wybrane techniki wykrywania żywotności:

TABELA 9.

	Wizerunek twarzy	Odcisk palca	Tęczówka oka
Metody statyczne	Analiza zdjęcia – tło, odbicia, spójność itp.	Pomiar Przewodności elektrycznej skóry palca Pomiar ciepła skóry palca Analiza odcisku palca za pomocą technik przetwarzania obrazu	Analiza zdjęcia – pomiar odbić Analiza zdjęcia w podczerwieni
Metody behawioralne	Analiza wykonania przez użytkownika losowo wybranych poleceń - ruchów gałek ocznych, ruchów głową, mrugania oczami, uśmiechu itp. Analiza tekstu wyświetlonego na ekranie i czytanego na głos przez użytkownika		

Bezpieczeństwo systemów biometrycznych pod kątem wykrywania żywotności określa norma ISO 30107.

5.4.4 Biometria jako metoda uwierzytelniania

W dobie wzrostu przestępczości, uwierzytelnienie tożsamości staje się pierwszorzędnym wyzwaniem. Stosowanie właściwych metod biometrycznych (czyli m.in. weryfikujących żywotność mierzonych obiektów) w połączeniu z nowoczesną kryptografią (np. podpis elektroniczny), pozwala na stworzenie bardzo solidnych mechanizmów uwierzytelniania, pozbawionych wad wyolbrzymianych w sensacyjnych filmach i krążących półprawdach.

Ta zasada – w środowisku specjalistów powszechnie uznawana za kanon – legła u podstaw podjęcia przez międzynarodowe organizacje decyzji o zastosowaniu tych metod do uwierzytelnienia osób w ruchu międzynarodowym i dokumenty (paszport, pozwolenie na pobyt, eID) oraz systemy tam stosowane obligatoryjnie wykorzystują te metody. Biometria jest powszechnie stosowana w europejskich systemach identyfikacji, np.: Eurodac, SIS II i VIS, e-paszport biometryczny. Po podjęciu tej decyzji w mediach pojawiło się szereg dywagacji na temat zagrożeń związanych z wykorzystaniem biometrii – związanych zwłaszcza z naruszeniem prywatności i możliwością fałszowania dokumentu. Jednakże dzisiaj po kilku latach od wprowadzenia paszportów (najpierw z jedną cechą biometryczną) żadne z wysuwanych wtedy zagrożeń nie urzeczywistniło się w praktyce. Ich wystąpienie jest jeszcze mniej prawdopodobne po wprowadzeniu paszportu z dwoma cechami biometrycznymi, gdyż znacznie zostały wzmocnione mechanizmy wzajemnego uwierzytelnienia się podmiotów (osoby i organu kontrolującego; dane biometryczne są przesyłane tylko do autoryzowanych czytników). Warto zapoznać się

z rozwiązaniami, opracowanymi przez międzynarodowe gremia specjalistów i wzorując się na nich stosować podobne rozwiązania w systemach komercyjnych.

Metody uwierzytelniana oparte o biometrię i kryptografię są coraz szerzej stosowane w ramach prowadzenia działalności gospodarczej, w szczególności w branży finansowej. Organizacje, które zastosowały silne mechanizmy uwierzytelnienia oparte o biometrię i kryptografię odnotowują znaczny spadek przestępstw związanych z tożsamością. Jednakże spadek przestępstw w tych organizacjach nie oznacza spadku przestępstw w ogóle. Oznacza to, że przestępcy uznając przełamywanie tych systemów za zbyt kosztowne i ryzykowne przenoszą swą działalność tam, gdzie te metody nie są stosowane. Wniosek nasuwa się sam: organizacje, które zaniechają rozwijania silnych mechanizmów uwierzytelniania muszą się liczyć z poniesieniem konsekwencji będących skutkiem przestępstw.

5.4.4.1
Obszary zastosowań uwierzytelnienia biometrycznego.
Uwierzytelnienie biometryczne jest stosowane zarówno w usługach oferowanych konsumentom dla zabezpieczenia wykonywanych przez nich operacji, jak również przez same te organizacje w wewnętrznych operacjach dla ich usprawnienia, czy uniknięcia przestępstw i ataków wykonywanych przez nieuczciwych pracowników.

Poniżej przedstawione są przykłady wykorzystania uwierzytelnienia biometrycznego po stronie konsumenta.

Uwierzytelnianie operacji bankomatowych w tym wypłat i wpłat w bankomatach z wykorzystaniem karty EMV z aplikacją biometryczną „match-on-card" i skanera biometrycznego wbudowanego w bankomat; w ten sposób biometria zwiększa bezpieczeństwo transakcji bankomatowych w ogromnym stopniu chroniąc przed tzw. skimmingiem.

Uwierzytelnianie transakcji w okienkach bankowych - biometria, jako najpewniejsza metoda uwierzytelniania przeciwdziała problemowi braku odpowiedniej identyfikacji osoby wykonującej operacje w okienkach bankowych.

Uwierzytelnianie transakcji bankowych (przelewów) w Internecie - biometria stanowi bezpieczniejsze narzędzie do autoryzacji transakcji internetowych w porównaniu ze zdrapkami, tokenami czy też kodami sms'owymi, gdyż bank uzyskuje blisko 100% gwarancję, że osoba potwierdzająca daną transakcję jest właścicielem konta.

Uwierzytelnienie przy kontakcie z call center banku przy użyciu biometrii głosowej.

Uwierzytelnianie dokumentów elektronicznych (dowody tożsamości, karty zdrowia, paszporty, karty kibica itd.) - biometria stanowi najlepszą metodę uwierzytelniania dokumentów elektronicznych. Powszechnie stosuje się biometryczne uwierzytelnianie paszportów i dowodów osobistych, na których przechowywane są dane biometryczne obywateli. Uwierzytelnianie pacjentów i lekarzy wystawiających diagnozę stanowi przełom w administracji i ochronie zdrowia. Biometria w kartach kibica stanowi rozwiązanie problemów z nielegalnym uczestnictwem osób niepożądanych na imprezach sportowych.

Uwierzytelnianie wypłat zasiłków dla bezrobotnych oraz rent i emerytur (np. poprzez bankomat bez potrzeby wykorzystania karty bankowej); wprowadzenie identyfikacji biometrycznej stanowi rozwiązanie dla wypłat zasiłków w lokalnych oddziałach banków;

osoby bezrobotne mogłyby w ten sposób, bez użycia karty lub stania w kolejkach w oddziałach, wypłacać swój zasiłek w bankomacie lub POS biometrycznym. Podobnie ma się sytuacja w wypłatą rent i emerytur (np. bankomat lub POS w oddziałach pocztowych).

Biometryczna kontrola dostępu do klucza prywatnego przy elektronicznym podpisywaniu dokumentów z wykorzystaniem certyfikatów kwalifikowanych. Biometria pozwala na zastąpienie numeru PIN podczas podpisywania dokumentów z wykorzystaniem certyfikatów kwalifikowanych.

Inne przykłady to:
- uwierzytelnianie płatności mobilnych – przez wbudowane do smartfonów skanery odcisku palca i wizerunku twarzy lub – rzadziej – tęczówki oka,
- uwierzytelnienie przy płatności kartą płatniczą w terminalach POS – karta ma wbudowany skaner odcisku palca, który zastępuje PIN,
- uwierzytelnianie transakcji w terminalach POS - Pay by Finger,
- kontrola dostępu do skrytek depozytowych w bankach i na poczcie.

5.0

Poniżej z kolei przedstawione są przykłady wykorzystania uwierzytelnienia biometrycznego po stronie wewnętrznej organizacji/przedsiębiorcy.
I. kontrola dostępu do pomieszczeń - biometria stanowi idealne rozwiązania do ochrony krytycznych stref w budynkach,
II. rejestracja czasu pracy - biometria pozwala na rzetelną kontrolę czasu pracy pracowników[4],
III. biometria podnosi poziom bezpieczeństwa logowania do zasobów sieciowych i systemów biznesowych,
IV. biometria uwierzytelnia operacje na komputerach PC (drukowanie, modyfikacje plików itd.),
V. biometria umożliwia wprowadzenie innowacji i ułatwień dla pracowników, np. biometryczna stołówka dla pracowników.
Zastosowania te są coraz bardziej popularne na świecie i będą powszechnie stosowanymi rozwiązaniami w niedalekiej przyszłości.

Szczegółowe informacje o biometrii, jej zastosowaniach, zaletach i wadach, jak i aspektach prawnoorganizacyjnych można uzyskać z RAPORTU BIOMETRYCZNEGO 2.0 „Bankowość biometryczna" opracowanego przez Grupę ds. Biometrii FTB, z którego treścią będzie się można zapoznać już niedługo na stronach Forum Technologii Bankowych Związku Banków Polskich.

5.5
Uwierzytelnienie proceduralne

Celem uwierzytelnienia jest potwierdzenie, że podmiot, którego to uwierzytelnienie dotyczy, jest tym, za kogo się podaje. Podstawową cechą odróżniającą uwierzytelnienie proceduralne od innych mechanizmów uwierzytelnienia jest to, że uwierzytelnienie to nie musi występować na początku procesu, natomiast jest warunkiem poprawnego zakończenia procesu. Uwierzytelnienie takie można wykorzystywać wszędzie tam, gdzie ryzyko nadużycia wynikające z braku uwierzytelnienia na początku procesu jest niewielkie lub powstaje w wypadku, gdyby całość procesu zakończyła się bez uwierzytelnienia.

Przykładem uwierzytelnienia proceduralnego może być np. wniosek do jednostki samorządu terytorialnego o wycięcie drzewa. W tym przypadku korzyść, czyli zgodę na wycięcie drzewa, otrzymać może wyłącznie wnioskodawca, będący właścicielem nieru-

4. W Polsce, zdaniem Urzędu Ochrony Danych Osobowych, obecnie obowiązuje całkowity zakaz wykorzystywania danych biometrycznych (np. linii papilarnych, skanów siatkówki oka itp.) pracowników dla celów ewidencji czasu pracy.

chomości, na której znajduje się drzewo i to on ponosi koszt wycięcia drzewa – decyzja ponadto wysyłana jest na adres właściciela nieruchomości. Wobec powyższego, na bazie analizy ryzyka, uwierzytelnienie wnioskodawcy następuje dopiero w momencie, w którym powstaje konieczność weryfikacji zgodnego z prawem wycięcia drzewa. W takim wypadku nawet, jeżeli o wycięcie wnioskowała osoba nieuprawniona lub właściciel nie zamierzał wycinać drzewa, zgoda będzie miała znaczenie dopiero w momencie wycięcia drzewa.

Z uwierzytelnieniem proceduralnym mamy także do czynienia w sytuacji, kiedy realizując proces na różnych jego etapach dokonujemy weryfikacji poszczególnych atrybutów uwierzytelnianego podmiotu i dopiero na zakończenie procesu zweryfikowane atrybuty dają wystarczające dla danego procesu prawdopodobieństwo, że osoba uwierzytelniająca się jest tą, za którą się podaje.

Zaletą uwierzytelnienia bazującego na procesie jest to, że mechanizm ten nie wymaga wcześniejszej rejestracji i wydania np. haseł osobie uwierzytelnianej. Jest on powszechnie stosowany przez administrację w procesach dokumentowych (przebiegających tradycyjnie na papierze), gdzie procedura administracyjna pozwala na zweryfikowanie atrybutów mających znaczenie dla sprawy realizowanej, np. na podstawie wniosku papierowego przesłanego pocztą.

5.6
Uwierzytelnienie oparte na wiedzy

Uwierzytelnienie oparte na wiedzy (ang. knowlage-based) polega na tym, że uwierzytelniający i uwierzytelniany posiadają wspólną wiedzę, której weryfikacja pozwala na przeprowadzenie procesu uwierzytelnienia. Strona uwierzytelniająca proszona jest o odpowiedź na pytanie lub serię pytań, i na tej podstawie następuje uwierzytelnienie. Uwierzytelnienie oparte na wiedzy jest najczęściej stosowanym mechanizmem dla osób fizycznych, gdzie hasło stanowi współdzielony atrybut uwierzytelnienia. Poza hasłami stosuje się także inne informacje, które uwierzytelniany posiada, a uwierzytelniający może zweryfikować, np.: fakty z życia, zawartość posiadanych dokumentów, historia transakcji.

W biznesie metoda ta jest z powodzeniem stosowana w bankach w celu uwierzytelnienia telefonicznego kanału kontaktu z klientem. Najczęściej stosowane są tutaj informacje podane do banku w momencie rejestracji konta.

W administracji publicznej najciekawszym przykładem zastosowania takiej metody uwierzytelnienia jest uwierzytelnienie oświadczenia podatkowego poprzez podanie kwoty podatku z poprzedniego okresu podatkowego. Rozwiązanie to adresuje podstawowe ryzyko złożenia deklaracji w imieniu innej osoby, przy uwzględnieniu faktu, że złożenie deklaracji jest obowiązkowe. Zabezpieczeniem tego rozwiązania jest procedura weryfikacji i ew. wyjaśniania w przypadku wpłynięcia np. dwóch deklaracji za ten sam okres podatkowy.

5.7
Uwierzytelnienie w oparciu o portale społecznościowe

Coraz popularniejszym sposobem uwierzytelniania w wielu serwisach internetowych jest wykorzystywanie tożsamości pochodzącej z portalu społecznościowego. Do najpopularniejszych metod należy uwierzytelnianie się za pomocą konta w serwisie społecznościowym Facebook oraz za pomocą tożsamości konta Google.

Stosowanie tej metody wymaga uwzględnienia ryzyka, że tożsamość na serwisach społecznościowych może być sfabrykowana, a duża liczba powiązań z innymi użytkownikami może nie wynikać z faktu rzeczywistego potwierdzenia znajomości danej osoby, a jedynie potwierdzać aktywność na danym portalu. Zagrożenia związane z korzystaniem z tej metody uwierzytelniania dotyczą zarówno uwierzytelniającego, jak i uwierzytelnianego. Uwierzytelniający musi uwzględnić ryzyko fałszywej tożsamości na portalu społecznościowym, natomiast uwierzytelniany - zezwalając na tę metodę - zgadza się na przekazywanie innych atrybutów tożsamości związanych z używanym portalem, np. aktywność i wpisy dokonywane na tym portalu. Ta metoda uwierzytelnienia jest przykładem wykorzystania idei federacji tożsamości (por. 3.8).

5.0

5.8
Uwierzytelnienie na podstawie danych bankowych właściciela rachunku

Metoda uwierzytelniania powszechnie używana w ecommerce to uwierzytelnienia na podstawie danych z przelewu bankowego. Przelew zawiera imię, nazwisko (lub nazwę dla firm), adres oraz unikatowy numer rachunku bankowego. Bardzo ważne znaczenie biznesowe ma metoda do ograniczenia ryzyk związanych z transakcjami realizowanymi zdalnie, gdzie uwierzytelnienie realizowane na podstawie danych bankowych jest dodatkowym zabezpieczeniem procesu.

W praktyce większość rachunków to rachunki posiadające jednego właściciela, a nawet w przypadku rachunku, do którego więcej niż jedna osoba ma dostęp, jest mało prawdopodobne wykorzystanie tego rachunki w celach fraudowych. Dzięki temu w momencie, gdy klient zdalnie deklaruje kim jest oraz posiadanie rachunku bankowego, to zgodność danych z przelewu jest faktorem bardzo wysoce uwiarygadniającym podane dane i do wielu zastosowań wystarczającym a jednocześnie wygodnym.

Wygoda jest zapewniana przez możliwość zlecenia przelewu w formule paybylink. Co ważne, przy stosowaniu tej metody zawsze pozostaje ślad jej użycia w historii rachunku bankowego (dane przelewu), a powszechnie wpisany jest tekst nawiązujący do charakteru transakcji w opisie przelewu (np. potwierdzenie tożsamości). Przyjętą kwotą takiego przelewu jest 1 złoty. Dzięki temu klient ma potwierdzenie wykonania takiej transakcji wprost w banku.

Dodatkowo Związek Banków Polskich prowadzi bazę, która pozwala odrzucić rachunki wcześniej założone na przelew, bez potwierdzonej face2face tożsamości. Dzięki temu metoda może być używana nie tylko na rynku ecommerce czy pożyczek, ale nawet do zakładania kont bankowych.

Ta metoda to także potwierdzenie numeru rachunku bankowego, co w wielu procesach biznesowych jest również ważne. Na rynku np. pożyczek nie tylko potwierdza się tożsamość osoby z użyciem tzw. przelewu weryfikacyjnego, ale także pozyskuje pewny numer rachunku bankowego, na który następuje wypłata pożyczki, tym samym pożyczka zostanie wypłacona (przy pozytywnej decyzji) wyłącznie na rachunek, którym może dysponować wnioskodawca.

Warto podkreślić, że ta metoda może i jest używana samodzielnie, lub może być połączona z np. weryfikacją danych ze zdjęcia dokumentu tożsamości. Wtedy zgodność danych uwiarygadnia, że przedstawiony zdalnie dokument był oryginalny.

Analogiczny zestaw danych można pozyskać dzięki usłudze AIS PSD2. Imię i nazwisko są wprost wskazane w PSD2 jako dane, które są przekazywane (o ile są dostępne w banko-

wości elektronicznej, ale w praktyce w każdym banku są dostępne przez serwisy internetowe). Dostęp do historii rachunku / rachunków pozwala z kolei pozyskać dane stron transakcji dla historycznych przelewów. W wypadku użycia AIS nie mamy jednak do czynienia z „opisem przelewu", który pozwalał określić cel realizacji przelewu i jest łatwo dostępny dla właściciela rachunku. Nie ma pewności i standardów, jak historia takich transakcji będzie prezentowana klientom w bankach.

5.9
Uwierzytelnienie na podstawie atrybutów

Typowym przykładem takiego uwierzytelnienia jest realizacja karty zdrapki celem zasilenia telefonu pre-paid. W tym procesie uwierzytelnienie dotyczy faktu, że osoba jest uprawniona (zakupiła) do zasilenia telefonu o ustaloną kwotę. Najczęściej metoda uwierzytelnienia opartego o atrybuty jest stosowana tam, gdzie uwierzytelnienie nie dotyczy bezpośrednio niezmiennych cech tożsamości, a jedynie tych, które są potrzebne do decyzji autoryzacyjnej.

Uwierzytelnienie oparte o atrybuty będzie miało zastosowanie dla zakupu alkoholu przez Internet, gdzie dla realizacji procesu nie jest konieczne poznanie danych osobowych kupującego alkohol, natomiast konieczne jest potwierdzenie jego pełnoletności. W niektórych implementacjach elektronicznego dokumentu tożsamości, dokument taki jest w stanie potwierdzić jedynie fakt pełnoletności, obywatelstwa, zamieszkiwania danego regionu czy przynależności zawodowej (zob. także rozdział 5.7).

5.10
Uwierzytelnienie z zachowaniem prywatności

W dobie dynamicznego rozwoju środków komunikacji elektronicznej, Internetu i e-usługi, coraz większym problemem staje się kwestia zachowania prywatności. Dotychczasowe zastosowanie PKI i innych technik uwierzytelnienia zakłada ujawnienie danych o tożsamości. Jest to w większości przypadków niezbędne do uzyskania dostępu do usługi ze względu na jej naturę (np. przy dostępie do danych medycznych, przy załatwianiu spraw urzędowych). Jednak można wyobrazić sobie pewne rodzaje usług, do których dostęp mógłby (lub powinien być) anonimowy, na przykład:

- głosowanie w wyborach, gdzie w procesie uwierzytelnienia weryfikuje się jedynie czy jesteśmy uprawnieni,
- anonimowy donos na policję,
- zakup artykułów dostępnych tylko dla osób dorosłych, gdzie wymagana jest jedynie weryfikacja wieku, a inne dane personalne są zbędne w procesie.

W zakresie elektronicznej identyfikacji i uwierzytelnienia ochronę prywatności rozumie się poprzez:
- zapewnienie anonimowości i braku możliwości dotarcia poprzez dane uwierzytelniające do rzeczywistych danych użytkownika (ang. untraceability),
- ujawnianie wyłącznie niezbędnych danych o tożsamości użytkownika,
- brak możliwości skojarzenia dwóch elektronicznych tożsamości (danych uwierzytelniających) z jedną osobą, nawet, jeśli te dane zostały wydane przez tego samego dostawcę tożsamości (ang. unlinkability),
- nieujawnianie dostawcy tożsamości (wydawcy danych uwierzytelniających) informacji \ o usłudze, z której użytkownik korzysta lub skorzystał.

W procesie ochrony prywatności w usługach elektronicznych występuje trzech aktorów: użytkownik, dostawca tożsamości (Identity Provider), dostawca usługi (Service Provider). Dostawca usługi określa kryteria dla swojej usługi, jakie musi spełnić użytkownik, aby uzyskać dostęp (czyli jakie atrybuty powinien posiadać użytkownik). Następnie

udziela dostępu do usługi po uzyskaniu potwierdzenia spełnienia tych kryteriów. Tymi kryteriami (atrybutami) mogą być np.: wiek, miejsce zamieszkania, przynależność do grupy społecznej czy zawodowej, posiadanie określonych uprawnień (np. do świadczeń medycznych). Dostawca tożsamości wydaje dane uwierzytelniające chroniące tożsamość (ang. privacy enabled credentials), certyfikuje/akredytuje dostawców usług spełniających określone wymagania ochrony prywatności oraz weryfikuje na żądanie i za zgodą użytkownika jego atrybuty.

Użytkownik zgłasza do dostawcy tożsamości żądanie weryfikacji atrybutów, a następnie przedstawia dostawcy usługi dane uwierzytelniające chroniące prywatność, czyli potwierdzające spełnienie kryteriów, ale nieujawniające innych danych i spełniające w/w kryteria ochrony prywatności.

Obecnie istnieje wiele inicjatyw mających na celu określenie norm i standardów w zakresie ochrony prywatności w dziedzinie usług elektronicznych i uwierzytelnienia. Jedna z inicjatyw podjęta została w ramach komitetu ISO/IEC JTC 1/ SC27, który jest odpowiedzialny za technologie informacyjne i bezpieczeństwo. Komitet SC 27 przoduje w tworzeniu i rozwoju standardów szyfrowania i bezpieczeństwa cyfrowego. Obecnie komitet ten opracowuje lub planuje opracować w przyszłości standardy dotyczące m.in. zarządzania tożsamością i prywatnością oraz protokołami kryptograficznymi.

W szczególności powstają następujące standardy:

ISO/CEI 20008 "Information technology — Security techniques -- Anonymous digital signatures" określający mechanizmy anonimowego podpisu cyfrowego,

ISO/CEI 18370 "Information technology — Security techniques — Blind digital signatures", opisujący tzw. ślepe podpisy cyfrowe, w których odbiorca otrzymuje podpis bez potrzeby przekazania przez podpisującego części lub jakiejkolwiek informacji związanej z podpisywaną wiadomością lub podpisanej wiadomości,

ISO/IEC 20009 "Information technology — Security techniques — Anonymous entity authentication", który opisuje mechanizm anonimowego uwierzytelnienia umożliwiającego ukrycie identyfikatora strony uwierzytelnianej,

ISO/IEC 24760 "Information technology — Security techniques — A framework for identity management" stanowiący ogólny zbiór wymagań dla systemów zarządzania tożsamością, m.in. w zakresie poszanowania prywatności,

ISO/IEC 29100 "Information Technology – Security Techniques – A privacy Framework", którego celem jest pomoc w implementacji w systemach ICT wymagań prawa w zakresie ochrony danych osobowych,

ISO/IEC 29134 "Information technology — Security techniques — Privacy Impact Assessment Methodology" opisujący metodykę przeprowadzania oceny stopnia ochrony prywatności przez systemy przetwarzające dane osobowe, tzw. Privacy Impact Assesment (PIA),

ISO/IEC 29191 "Information technology — Security techniques — Requirements on partially anonymous, partially unlinkable authentication", który stanowi przewodnik użycia podpisów grupowych i innych mechanizmów w celu minimalizacji ujawnianych danych o użytkowniku.

Inny komitet ISO/IEC, JTC1/SC17, jest z kolei odpowiedzialny m.in. za technologie kartowe i identyfikację osób. Komitet ten odpowiada za serię standardów dot. technologii kart procesorowych i ich interoperacyjności (m.in. ISO/IEC 7816). Grupa robocza WG4 tego komitetu zajmuje się tematem prywatności przy implementacji rozwiązań korzystających z technologii kartowych. Celem jest wypracowanie komend i niskopoziomowych protokołów zapewniających realizację prywatności wynikającą z regulacji narodowych lub europejskich, czy w szczególności implementację protokołów wypracowanych w ramach SC27.

Na poziomie technicznym istnieją dwie główne implementacje techniczne:
• protokół Modular Enhanced Role Authentication (mERA) opisany w standardzie EN 14890,
• protokół Restricted Identification (RI), opisany w niemieckim dokumencie BSI TR 03110 cz. 2, a następnie inkorporowany do normy EN 14890.

mERA stanowi model ochrony prywatności, w którym celem jest uzyskanie przez użytkownika dostępu do usługi elektronicznej (on-line) przy jednoczesnym zapobieżeniu ujawnienia dostawcy danych o użytkowniku tej usługi oraz uniemożliwieniu dostawcy tożsamości (IdP) pozyskania wiedzy na temat usługi. W modelu tym istnieje zaufana trzecia strona (dostawca tożsamości), która dostarcza dostawcy usługi dowodu, że użytkownik został odpowiednio uwierzytelniony i spełnia określone kryteria lub posiada określone atrybuty (np.: wiek, narodowość, przynależność do jakiejś grupy czy społeczności) określone przez dostawcę e-usługi.

Protokół mERA umożliwia implementację różnej architektury systemu w zależności od modelu biznesowego, czy polityki wydawcy identyfikatora elektronicznego: może to być architektura zarówno z dostawcą tożsamości (zaufaną trzecią stroną) jak i bez. Dzięki zastosowaniu protokołu anonimowego uwierzytelnienia mEAC („Privacy constrained Modular EAC", opisany w normie EN14890), chroniącego dane identyfikacyjne karty elektronicznej i jej użytkownika, trzecia strona staje się zbędna - zadanie weryfikacji kryteriów dostępu do usługi oraz wygenerowanie danych uwierzytelniających spoczywa wtedy na dostawcy usługi.

Protokół Restricted Identification (w tłumaczeniu „ograniczona identyfikacja") został opracowany w Niemczech na potrzeby niemieckiego dokumentu tożsamości (por. 9.3). Protokół ten opiera się na statycznym protokole Diffie'go – Hellman'a, który generuje sektorowy identyfikator mikroprocesora. Sektorem w tym przypadku jest grupa terminali (czytających kartę). Terminal danego sektora rozpoznaje mikroprocesor karty po jego sektorowym identyfikatorze (pseudonimie) przekazanym wcześniej przez mikroprocesor, bez potrzeby czytania z karty danych personalnych posiadacza. Przy czym przed wykonaniem protokołu ograniczonej identyfikacji, wymagane jest uwierzytelnienie terminala i procesora zgodnie z procedurą Extended Access Control v2 (więcej nt. EAC znajduje się w 6.5.2).

Poza w/w pracami, istnieją także **inne inicjatywy w zakresie uwierzytelnienia z ochroną prywatności**. Są to m.in.:
• Idemix – jest to technologia opracowana przez IBM, która umożliwia wydawanie i prezentację kryptograficznie zabezpieczonych deklaracji (claims) związanych z tożsamością; technologia ta wykorzystuje tokeny bazujące na tzw. „podpisach grupowych", zamiast wykorzystania standardowego podpisu;
• U-Prove – jest to technologia opracowana przez Microsoft do zarządzania tożsamością za pomocą kryptograficznie chronionych deklaracji (claims), które mogą być powiązane z użyciem karty elektronicznej; technologia

ta umożliwia silną ochronę prywatności m.in. dzięki zwiększonej kontroli użytkownika i zapobieganiu jego śledzeniu;
• U-PrIM (Usable Privacy-enhancing Identity Management) – jest to projekt badawczy uniwersytetu w Karlstad (KaU) w Szwecji w kooperacji z partnerami biznesowymi: Nordea Bank i Gemalto; celem projektu jest wypracowanie sposobów praktycznego wykorzystania metod ochrony prywatności przy zarządzaniu tożsamością z wykorzystaniem kart elektronicznych;
• ABC4Trust (Attribute-based Credentials for Trust) – jest to projekt badawczo-rozwojowy finansowany przez Unię Europejską, zajmujący się kwestiami zunifikowanej architektury ABC (Attribute-based Credentials) oraz otwartą implementacją referencyjną systemu ABC umożliwiającego, w ramach jakiejś ograniczonej wspólnoty, anonimowe wypowiedzi jej członków na temat tejże lub jej członków.

5.11
Zdalne potwierdzanie tożsamości

Standardowy model potwierdzenia tożsamości wymaga stawienia się w punkcie rejestracji, wylegitymowania na podstawie dokumentu tożsamości oraz potwierdzenia, że osoba opisana w dokumencie jest rzeczywiście tą, która zgłosiła się do punktu rejestracji. Taki model był dotychczas standardowy dla otwierania kont bankowych, wymagań dyrektywy przeciwdziałania praniu brudnych pieniędzy oraz wydawania kwalifikowanych certyfikatów. Model potwierdzania tożsamości bezpośredni ma dwie zasadnicze wady. Pierwsza jest oczywista i związana jest z faktem, że wymaga on fizycznego spotkania się weryfikowanego z osobą weryfikującą. Drugi dotyczy tego, że cały model bezpieczeństwa jest oparty o doświadczenie oraz umiejętności prawidłowego przeprowadzenia procesu przez weryfikującego. Model ten w związku z tym jest podatny na manipulacje oraz w rzeczywistości obarczony błędem skutecznej identyfikacji biometrycznej.

Oczekiwania rynku doprowadziły do wypracowania nowych – zdalnych modeli potwierdzania tożsamości wykorzystujących sieć Internet oaz kamerę zamieszczoną w telefonie lub komputerze identyfikowanego. W tym zakresie identyfikacja elektroniczna jest oparta o dwa modele – wideo-identyfikację oraz tzw. selfie-id czyli automatyczną identyfikację zdalną. Ze względu na popularyzację tych modeli oraz nowe zagrożenia z nimi związane instytucje nadzorcze wydały zalecenia dotyczące budowy i stosowania rozwiązań zdalnego potwierdzania tożsamości.

5.11 .1
Zalecenia KNF w zakresie zdalnego potwierdzania tożsamości

Dokument przedstawiony przez KNF zawiera dobre praktyki w zakresie wypełniania obowiązków wynikających z przepisów o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu. Przedstawione dobre praktyki dotyczą identyfikacji klienta i potwierdzania tożsamości w bankach oraz oddziałach instytucji kredytowych w oparciu o metodę wideo-weryfikacji.

Niezależnie od przedstawionych praktyk to na bankach ciąży wymóg ustalenia poziomu i profilu ryzyka klienta, a realizowany mechanizm identyfikacji i zastosowane środki zabezpieczające zależeć powinny od przeprowadzonej analizy ryzyka.

Dokument przedstawiony przez KNF wskazuje, że w zakresie potwierdzania tożsamości klienta bez jego fizycznej obecności – instrumentami najbardziej pewnymi w zastosowaniu są zdefiniowane w rozporządzeniu eIDAS środki identyfikacji elektronicznej oraz kwalifikowany podpis elektroniczny. Natomiast w przypadku braku możliwości wykorzystania powyższych środków identyfikacji elektronicznej lub kwalifikowanego podpisu

elektronicznego, bank powinien rozważyć zastosowanie wzmożonych środków bezpieczeństwa finansowego.

Najważniejszymi dobrymi praktykami wskazanymi przez KNF są:
• przeprowadzenie analizy ryzyka oraz opiniowanie i konsultacje w aspekcie przeciwdziałania praniu pieniędzy oraz finansowaniu terroryzmu;
• formalne wprowadzenie procedury dotyczącej procesu wideoweryfikacji;
• analizowanie przypadków odmowy nawiązania relacji z klientem przy pomocy wideoweryfikacji;
• przeprowadzanie szkoleń dla pracowników, w szczególności w zakresie identyfikacji i weryfikacji tożsamości oraz weryfikacji dokumentów tożsamości
• objęcie procesu systememem kontroli wewnętrznej oraz systememem informacji zarządczej;
• sprawdzenie klienta i informacji zawartych w jego dowodzie osobistym w bazach danych;
• stosowanie technik uzupełniających jak: weryfikacje biometryczne, OCR, weryfikacja kodu MRZ, ustanowienie czynników behawioralnych, wykonanie zdjęcia twarzy z poziomu aplikacji banku.

5.11.2 Rozwiązania zdalnego potwierdzania tożsamości

W zakresie rozwiązań zdalnego potwierdzenia tożsamości, zarówno jeżeli chodzi o pełną wideo-identyfikację z fizycznym udziałem operatora, jak również narzędzi automatycznych (self-ID), proces identyfikacji i weryfikacji tożsamości sprowadza się do następujących działań:
1. Sprawdzeniu rzeczywistego istnienia osoby fizycznej (mechanizmy liveness detecton służące wykryciu mowy, ruchu, reakcji);
2. Sprawdzeniu, czy dokument tożsamości należy do tej konkretnej osoby, która legitymuje się przed ekranem telefonu/komputera;
3. Sprawdzeniu i powiązaniu wizerunku osoby na zdjęciu dokumentu tożsamości z wizerunkiem twarzy na zdjęciu/wideo;
4. Sprawdzenie ważności prawnej dokumentu tożsamości (autentyczność dokumentu).

Wszystkie powyższe działania mają na celu potwierdzenie tożsamości osoby fizycznej na poziomie równym lub wyższym w odniesieniu do procesu weryfikacji tożsamości w punkcie fizycznym.

Na rynku europejskim jest szereg dostawców, którzy oferują usługi sefl-ID, jak również wideo-identyfikacji w oparciu o deklarację zgodności z wytycznymi KNF bądź BAFIN, w szczególności w odniesieniu do wymagań AML oraz eIDAS.

Rozwiązaniom rynkowym zdalnego potwierdzenia tożsamości można przypisać następujące funkcjonalności:
• dostępność w model SaaS oraz On-premise,
• wbudowane mechanizmy wykrywania żywotności (liveness detection) o różnych poziomach wykrywania potencjalnych ataku prezentacji (biometrii),
• interfejs dla użytkownika końcowego dostępny z poziomu aplikacji mobilnej lub przeglądarki www,
• narzędzia mające zastosowanie w szczególności w procesach: onboardingu klientów, zakładania rachunków bankowych, potwierdzeniu wieku, aktualizacji danych klientów na potrzeby wymagań KYC.

W zakresie dostępnych na rynku rozwiązań należy wskazać, że obecne są rozwiązania zarówno zagraniczne jak i krajowe. Rozwiązania te różnią się poszczególnymi cechami funkcjonalnymi i bezpieczeństwa, natomiast ważnymi aspektami, które powinny być brane pod uwagę w wyborze rozwiązania są:

- certyfikacja bezpieczeństwa lub zgodności z rozporządzeniem eIDAS,
- deklaracja spełnienia wymagań KNF,
- dostępność rozwiązań w urządzeniach mobilnych,
- zastosowanie technik weryfikacji żywotności,
- zakres dokumentów tożsamości dla których możliwa jest weryfikacja,
- przetwarzanie danych w europejskim obszarze gospodarczym,
- przedstawicielstwo w Polsce.

ROZDZIAŁ 6.0
PRZEGLĄD ROZWIĄZAŃ TECHNICZNYCH

6.1
Karty elektroniczne

6.1.1
Rodzaje kart elektronicznych

Karta elektroniczna (mikroprocesorowa) jest rodzajem tokena sprzętowego i jednym z podstawowych nośników danych uwierzytelniających jako tzw. bezpieczny komponent. Mikroprocesor karty to mały komputer realizujący protokoły kryptograficzne (symetryczne lub asymetryczne) oraz bezpiecznie przechowujący dane. Mikroprocesor posiada własny system operacyjny, interfejs programistyczny (w postaci zestawu komend APDU) i komunikacyjny (podstawowe dwa interfejsy to: stykowy zgodny z ISO 7816 oraz bezstykowy zgodny z ISO 14443).

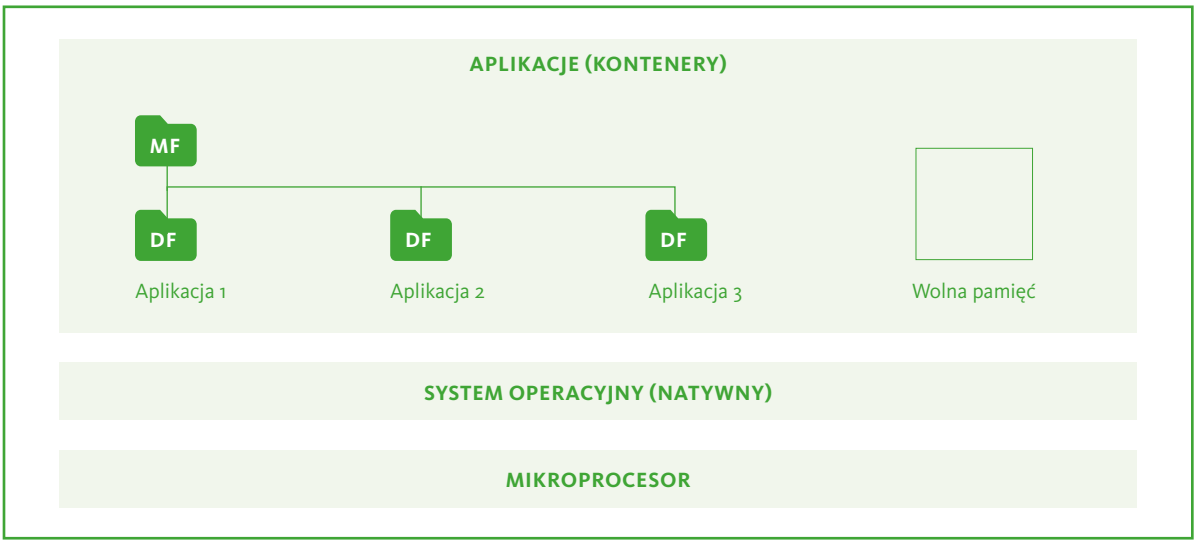
W przypadku kart elektronicznych wykorzystywanych do składania podpisów elektronicznych i uwierzytelnienia PKI, posiadają one koprocesor kryptograficzny do realizacji protokołów asymetrycznych (oraz symetrycznych). Zwykle karty takie mają możliwość generowania lub importu kluczy (par kluczy) oraz składania podpisu cyfrowego i elektronicznego (porównaj pkt 5.1.3.1), polegającego na zaszyfrowaniu kluczem prywatnym wyniku funkcji skrótu z podpisywanego dokumentu. Zatem bez względu na to, czy realizowany jest proces składania podpisu elektronicznego, uwierzytelnienia, czy szyfrowania asymetrycznego, z punktu widzenia karty elektronicznej jest to zawsze ta sama funkcja złożenia podpisu.

Karty realizujące kryptografię asymetryczną nazywa się potocznie kartami PKI lub bardzie poprawnie IAS (Identification, Authentication, Signature co oznacza w języku polskim identyfikację, uwierzytelnienie i podpis).

Wyróżnia się dwa podstawowe rodzaje kart elektronicznych (ze względu na technologię systemu operacyjnego):
- natywne,
- oparte o maszynę wirtualną (tzw. otwarte).

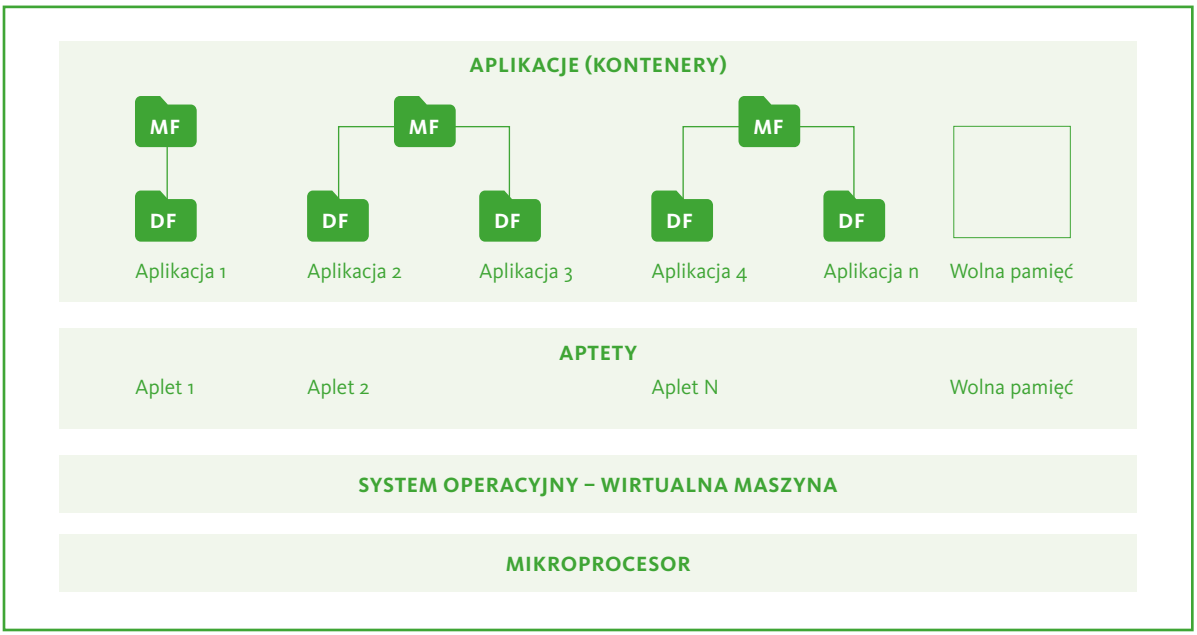
Karty natywne są to karty posiadające system operacyjny oparty o własne rozwiązanie danej firmy, którego kod umieszczany jest na stałe w pamięci trwałej mikroprocesora (ROM) w procesie produkcyjnym wytwórcy „silikonu" (tzw. maska). Wszelkie zmiany, a zatem i zmiany funkcjonalności karty natywnej, są niemożliwe – karta posiada tylko takie funkcje (algorytmy, protokoły, komendy), jakie zostały pierwotnie zaprojektowane i osadzone w krzemie. Odbiorca karty (użytkownik, nabywca, personalizator itp.) może jedynie umieszczać dane, nie ingeruje w „logikę" kodu wykonywanego. Karty takie mają bardzo ograniczone możliwości w zakresie zmian zawartości po wydaniu karty (personalizacji powydawniczej). Można jedynie aktualizować dane lub dodawać nowe dane. W przypadku chęci wprowadzenia zmian (np. dodania funkcji oprogramowania nieprzewidzianej na początku) trzeba wprowadzić nowy produkt i wyprodukować nowy „silikon" (nowa maska krzemowa). Dlatego karty te są nazywane czasem „zamkniętymi". Mają one zastosowanie przede wszystkim tam, gdzie nie przewiduje się powydawniczego zarządzania zawartością (lub w ograniczonym zakresie) i najczęściej dla rozwiązań jednoaplikacyjnych (paszport elektroniczny I i II generacji).

RYSUNEK 8. Uproszczony model warstwowy karty natywnej.



Nowoczesne rozwiązania kart elektronicznych posiadają systemy operacyjne oparte o maszynę wirtualną (idea analogiczna do maszyn wirtualnych na komputerach klasy PC). Rozwiązania takie posiadają system operacyjny dostarczający zunifikowane środowisko uruchamiania aplikacji (tzw. apletów w przypadku systemu Java lub kodletów – dla systemu Multos). Specyfikacje są otwarte, więc każdy może tworzyć kod aplikacji (czyli modyfikować funkcjonalność karty). Aplikacje te są kodem wykonywalnym i realizują funkcje logiczne, korzystając z funkcji podstawowych (API) systemu operacyjnego. Ponieważ aplety mogą być przechowywane i są uruchamiane w pamięci programowalnej (EEPROM), można je ładować i kasować, także po wydaniu karty. Ponadto na jednej karcie można umieszczać niezależnie różne aplikacje obok siebie. Można powiedzieć, że każdy z apletów działa jak jedna karta natywna. Stąd takie karty nazywa się wieloaplikacyjnymi. Tego typu karty często nazywa się otwartymi, gdyż nie tylko producent karty może tworzyć i modyfikować oprogramowanie karty oraz można dokonywać tego powydawniczo. Obecnie istnieją dwie implementacje kart z wirtualnymi maszynami: Java Card i Multos.

RYSUNEK 9. Uproszczony model warstwowy karty z maszyną wirtualną.



6.1.2
Kwalifikowane urządzenie do składania podpisu elektronicznego

Wymogi dla kwalifikowanych urządzeń do składania podpisu elektronicznego:

1. Kwalifikowane urządzenia do składania podpisu elektronicznego zapewniają dzięki właściwym środkom technicznym i proceduralnym co najmniej:
• zagwarantowanie w racjonalny sposób poufności danych służących do składania podpisu elektronicznego użytych do złożenia podpisu elektronicznego;
• w praktyce tylko jednorazowe wystąpienie danych służących do składania podpisu elektronicznego użytych do złożenia podpisu elektronicznego;
• uniemożliwienie, z racjonalną dozą pewności, pozyskania danych służących do składania podpisu elektronicznego użytych do złożenia podpisu elektronicznego oraz skuteczną ochronę podpisu elektronicznego przed sfałszowaniem za pomocą aktualnie dostępnych technologii;
• możliwość skutecznej ochrony, przez osobę uprawnioną do składania podpisu, danych służących do składania podpisu elektronicznego użytych do złożenia podpisu elektronicznego, przed użyciem ich przez innych.

2. Kwalifikowane urządzenia do składania podpisu elektronicznego nie zmieniają danych, które mają być podpisane, ani nie uniemożliwiają przedstawienia tych danych podpisującemu przed złożeniem podpisu.

3. Dane służące do składania podpisu elektronicznego mogą być generowane lub zarządzane w imieniu podpisującego wyłącznie przez kwalifikowanego dostawcę usług zaufania.

4. Bez uszczerbku dla pkt 1 lit. d) kwalifikowani dostawcy usług zaufania zarządzający danymi służącymi do składania podpisu elektronicznego w imieniu podpisującego mogą kopiować dane służące do składania podpisu elektronicznego wyłącznie w celu utworzenia kopii zapasowej, pod warunkiem że spełnione są następujące wymogi:
• bezpieczeństwo skopiowanych zbiorów danych musi być na tym samym poziomie co w przypadku oryginalnych zbiorów danych;
• liczba skopiowanych zbiorów danych nie przekracza minimum niezbędnego do zapewnienia ciągłości usługi.

Member States' notifications on: Designated Bodies under Article 30(2) and 39(2) of Regulation 910/2014 and Certified Qualified Signature Creation Devices under Article 31(1)-(2), and Certified Qualified Seal Creation Devices under Article 39(3) of Regulation 910/2014, and information from Member States on: Secure Signature Creation Devices benefiting from the transitional measure set in article 51(1) of Regulation 910/2014.

6.2
Narodowe dokumenty tożsamości

Dokumenty tożsamości zawierające mikroprocesor, wydawane przez rządy państw, same w sobie nie stanowią elektronicznej tożsamości ani środka identyfikacji elektronicznej. Rolę tę pełnią zawarte w nich dane – elektroniczne poświadczenia tożsamości. Najpowszechniejszą i najłatwiejszą metodą stworzenia z dokumentu tożsamości środka identyfikacji elektronicznej jest umieszczenie w nim certyfikatu elektronicznego PKI. Do tego jest potrzebne posiadanie przez dokument mikroprocesora kryptograficznego posiadające funkcję/aplikację IAS (ang. Identification, Authentication, Signature; pierwotnie zwane „PKI"), która umożliwia umieszczenie pary kluczy asymetrycznych wraz z certyfikatem elektronicznym. Certyfikat taki może być zarówno wydany przez państwo, jak też pochodzić z sektora komercyjnego (np. certyfikat kwalifikowany). Zwykle (szczególnie w UE), mikroprocesory elektronicznych dokumentów tożsamości z funkcją PKI/IAS spełniają wymagania odnoszące się do kart - urządzeń do składania podpisu kwalifikowanego (SSCD), a więc zgodnie z wymaganiami dla najwyższego poziomu wiarygodności uwierzytelnienia.

Zastosowanie narodowego dokumentu tożsamości jako nośnika elektronicznego identyfikatora jest o tyle interesujące, że umożliwia stosunkowo łatwe i tanie oraz masowe wyposażenie obywateli w środki do e-identyfikacji i uwierzytelnienia, gdyż i tak tego typu dokumenty są wydawane w większości krajów, najczęściej obowiązkowo. Rozwiązuje to problem „jajka i kury" – nie ma e-usług bez środków e-identyfikacji; nie ma środków e-identyfikacji, bo nie ma e-usług. Taki dokument niekoniecznie musi być odpowiednikiem dowodu osobistego. Równie skutecznie rolę tą spełni każdy inny dokument wydany przez państwo, np. prawo jazdy czy karta ubezpieczenia zdrowotnego, wyposażone w odpowiedni bezpieczny element w postaci certyfikowanego procesora kryptograficznego z oprogramowaniem wewnętrznym. Jednak standardem na świecie jest wykorzystanie do tego celu dowodów osobistych.

Polski eDowód oprócz funkcjonalności dokumentu podróży (ICAO) i możliwości odczytu zdjęcia biometrycznego właściciela dokumentu, posiada również bogaty zakres funkcjonalności z zakresu IAS, tj.:
• potwierdzenie obecności,
• identyfikację i uwierzytelnienie,
• podpis osobisty,
• opcjonalny kwalifikowany podpis elektroniczny
(wgrywany przez Dostawców Usług Zaufania).

Wykorzystanie funkcjonalności identyfikacji i uwierzytelnienia oraz podpisu osobistego jest konsekwentnie przez Rząd RP rozszerzane. Natomiast zastosowanie funkcji potwierdzenia obecności jest obecnie traktowane po macoszemu. Zgodnie z koncepcją Państwa, funkcjonalność ta miała być przede wszystkim wykorzystana w obszarze uszczelnienia systemu służby ochrony zdrowia poprzez potwierdzanie obecności pacjentów w placówkach zdrowia lub nawet potwierdzania zastosowanych procedur medycznych.

Certyfikat potwierdzenia obecności, który posiada każdy wydany eDowód może być także elementem potwierdzającym autentyczność dokumentu, obok zabezpieczeń zastosowanych w ramach funkcjonalności ICAO (active, pasive i chip Authentication).

W przyjętym w kraju federacyjnym modelem identyfikacji elektronicznej, źródło tożsamości którym jest eDowód z funkcją eID jest jedynym z ważniejszych elementów tego systemu. Istnieją jednak bariery dotyczące wykorzystania, tej funkcjonalności o najwyższym poziomie wiarygodności, jak np.
• niewielkie nasycenie rynku eDowodami (rocznie wydawanych jest ok. 3 mln szt. Dokumentów),
• konieczność użycia czytnika RFID lub NFC do odczytu danych i użycia eDowodu.

Dla sektora bankowego, połączenie rozwiązań opartych o zaawansowaną kryptografię z rozwiązaniami biometrycznymi jest wydaje się wysoce perspektywicznym i obiecującym rozwiązaniem, znacznie wzmacniającym bezpieczeństwo obrotu sektora finansowego i ograniczającym ryzyko ekspozycji na oszustwa i próby wyłudzeń w zakresie usług finansowych.

6.3
Hasła jednorazowe

Hasła jednorazowe (OTP – One-time Password) są powszechnie stosowane, jako mechanizm służący do uwierzytelniania podmiotów. Hasła jednorazowe dają możliwość

najprostszej i niewymagającej inwestycji infrastrukturalnych implementacji dwuczynnikowego uwierzytelnienia (ang. two-factor authentication), które składa się na czynnik wiedzy (czyli co użytkownika „wie") oraz czynnik posiadania (coś co użytkownik „ma"). Hasła jednorazowe są generowane po stronie uwierzytelniającego albo dostarczane do uwierzytelniającego alternatywnym kanałem komunikacji np. przez sieć telefoniczną.

Najczęściej wykorzystywane są następujące metody dostarczenia haseł generowanych po stronie dostawcy usługi są jednorazowe hasła przesyłane przez SMS, natomiast w praktyce zaprzestano już przesyłania pocztą karty zdrapki lub papierowej karty haseł jednorazowych.W przypadku generowania haseł po stronie uwierzytelniającego najczęściej stosowane są:
• tokeny kryptograficzne, zawierające czynnik losowy (ang. salt),
• aplikacje na telefony komórkowe.

Kluczowa zmiana jaka przyszła wraz PSD2 i wejściem w życie RTS dot. SCA to konieczność dynamicznego linkowania kodu OTP z danymi transakcji.

Do niedawna najpopularniejszą i zarazem najprostszą metodą dostarczania haseł jednorazowych do użytkownika była dystrybucja pre-generowanych haseł na kartach zdrapkach lub wydrukowanych na papierze. Metoda ta miała jednak wady, które ograniczały użyteczność takiego rozwiązania. Przede wszystkim użytkownik jest ograniczony co do ilości posiadanych haseł. W wypadku wykonywania wielu transakcji w krótkim czasie użytkownik może wyczerpać dostępną pulę haseł, ponadto użytkownicy podatni są na próby phishingu związanego z podawaniem kilku kolejnych haseł z listy, co wraz z kradzieżą danych uwierzytelniających, np. do konta bankowego, umożliwiało przestępcy wykonywanie dowolnych operacji. Hasła takie generowane były losowo (patrz pkt 5.1.1), najczęściej z wykorzystaniem jednokierunkowej funkcji skrótu, a przekazane użytkownikowi hasła musiały być przechowywane na serwerze. Ważne jest również zaufanie do kanału przesyłania haseł.

Wraz ze wzrostem dostępności telefonii komórkowej popularna stała się metoda przekazywania haseł jednorazowych przez SMS. Metoda ta ma wiele zalet nad metodami papierowymi i zdrapkami. Przede wszystkim jest zdecydowanie tańsza niż przesyłanie informacji pocztą tradycyjną. Ponadto, każde hasło jednorazowe jest przypisane do konkretnej transakcji (choć nie jest to konieczne), więc niemożliwe jest wykorzystanie niewykorzystanego hasła jednorazowego do innej transakcji niż ta, dla której zostało ono wygenerowane. Metoda ta nie uzależnia użytkownika od ilości posiadanych haseł, tak jak metoda papierowa. Hasła jednorazowe wysyłane SMSem posiadają również wady, które w niektórych przypadkach mogą dyskwalifikować tę metodę. Metoda zakłada bowiem przebywanie w zasięgu telefonii komórkowej w momencie potwierdzania transakcji hasłem jednorazowym, co w pewnych przypadkach nie jest spełnione.

Kolejną metodą dostarczenia hasła jednorazowego jest wykorzystanie sprzętowych tokenów. Token jest urządzeniem kryptograficznym, które np. na podstawie aktualnego czasu pochodzącego z wbudowanego w token zegara oraz losowego klucza kryptograficznego, umieszczonego w części elektronicznej tokenu, generuje co ustalony okres czasu numer, będący wynikiem operacji kryptograficznej, który może być wykorzystany jako hasło. Metoda ta, pomimo wysokiego stopnia bezpieczeństwa jest rzadko, w porównaniu z hasłami SMS, wykorzystywana przede wszystkim ze względu na wygodę użytkownika. Największym zagrożeniem dla tokenu jest jego utrata. Niektóre tokeny posiadają dodatkowe zabezpieczenie w postaci konieczności podania kodu PIN, co zabezpiecza go przed nieuprawnionym użyciem. Innym zabezpieczeniem, które kosztem

wygody użytkownika zwiększa bezpieczeństwo rozwiązania, jest częsty brak pośrednika między wystawcą tokena a użytkownikiem – użytkownik odbiera token osobiście.

Innym wariantem wykorzystania tokena jest użycie telefonu komórkowego z zainstalowanym na nim tokenem programowym. Stosowanie takiego tokena jest związane z wyższym poziomem ryzyka w stosunku do tokenów hardware'owych i nie zawsze wykorzystanie go jest możliwe.

Istnieją jeszcze inne metody realizacji idei dwuskładnikowego uwierzytelnienia, które są formą haseł jednorazowych. Jedną z nich jest wyświetlenie np. siatki obrazków, wśród których znajdują się obrazy zdefiniowane wcześniej przez użytkownika. Obrazy w siatce posiadają przypisane numery, które należy podać w odpowiednim miejscu. Uwierzytelnienie hasłem jednorazowym może również przybrać inną formę – np. w niektórych bankach dostęp do infolinii klientów jest chroniony poprzez hasło, którego nie wpisuje się jednak w całości, a podaje wyczytane przez automat pewne znaki np. 2, 5 i 7 znak hasła.

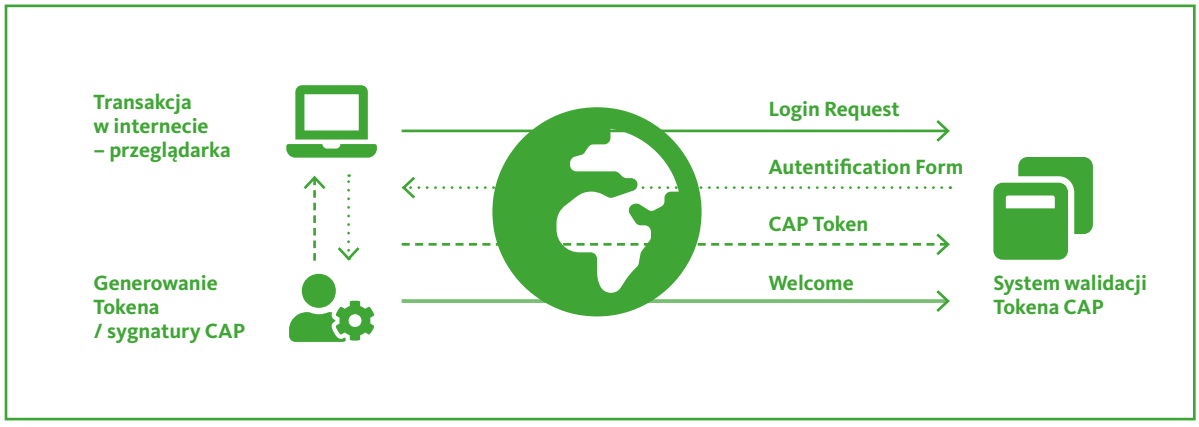
Najnowsze rozwiązania to komunikaty PUSH w aplikacjach mobilnych- klient zatwierdza transakcje na telefonie, widząc wszystkie istotne dane transakcji, bez konieczności przepisywania kodów, z zachowaniem dynamicznego linkowania. Podobnie jak SMS, usługa wymaga posiadania telefonu (smartfonu) oraz dostępu nie tyle do sieci telekomunikacyjnej, co dostępu do sieci Internet.

6.4
Mechanizmy CAP/DPA

Standard EMV, a w szczególności, jego dwie implementacje aplikacji stworzone przez MasterCard oraz Visa, znane jako CAP (MasterCard Chip Authentication Program - 2007) oraz jego najnowsza implementacja AA4C (Advanced Authentication for Chip - 2008) i DPA (Visa Dynamic PassCode Authentication) są aplikacjami uwierzytelnienia użytkownika w zdalnym dostępie do usług.

Aplikacja CAP/DPA realizuje transakcje, przez przygotowanie danych w innym systemie niż komputer użytkownika. Do komputera wprowadzany jest jedynie wynik współpracy karta – czytnik (token/sygnatura). Wszelkie obliczenia realizowane są w układzie aplikacja lokalna – czytnik, a następnie przenoszone są przez użytkownika do aplikacji komunikującej się z danym serwisem, uniemożliwiając ich „podmianę". W przypadku ataku, jedyne, co może grozić użytkownikowi to odrzucenie transakcji przez zdalny system, z powodu niezgodności tokena/sygnatury z przesłanymi danymi.

RYSUNEK 10. Typowy scenariusz wykorzystania aplikacji CAP/DPA.



Poniżej przedstawiono proces zdalnego uwierzytelnienia przy pomocy aplikacji CAP/DPA:

1. użytkownik, przy pomocy przeglądarki, łączy się ze stroną wybranego serwisu i - w zależności od przyjętej polityki bezpieczeństwa danego serwisu - postępuje zgodnie z oczekiwaną przez serwis metodą logowania lub realizacji transakcji,

2. użytkownik karty wkłada kartę zawierającą aplikację uwierzytelnienia (CAP/DPA) do podłączonego czytnika kart mikroprocesorowych,

3. w zależności od sposobu logowania, narzuconego przez dany serwis, czytnik generuje OTP (One Time Password) lub oczekuje na wprowadzenie danych wyświetlonych przez Serwer Uwierzytelnienia, przy metodzie Challenge – Respons (C/R),

4. użytkownik może wprowadzić dodatkowe informacje, np.: kwota, data transakcji itp.,

5. następnie użytkownik wprowadza PIN, jeśli jest zły, użytkownik proszony jest o ponowne wprowadzenie PIN lub sesja jest zakończona,

6. jeżeli wprowadzony PIN, jest poprawny, terminal przekazuje do karty żądanie wygenerowania kryptogramu,

7. na podstawie informacji zawartych w karcie, karta generuje kryptogram, który na podstawie odpowiedniego algorytmu, czytnik przekształca w token/sygnaturę, wyświetlany następnie przez czytnik.

Aplikacja CAP/DPA może – w zależności od wymagań – działać w trzech trybach pracy:
MODE 1 – tryb uwierzytelnienia użytkownika karty. Ten tryb używa techniki challenge-response i może dodatkowo korzystać z danych wprowadzonych przez użytkownika za pomocą klawiatury PCR, tj. kwoty transakcji, kodu waluty. Wartość generowanej liczby losowej oraz kwoty i kodu waluty wykorzystane są w procesie generacji kryptogramu AC (Application Cryptogram).
MODE 2 – tryb generowania OTP (One Time Password). W tym trybie nie wprowadza się żadnych danych z klawiatury PCR. Aplikacja CAP zapewnia, że każdy token, posiada unikalną wartość, dane wejściowe i klucz podpisujący dla danej operacji generacji tokena jest unikalny.
MODE 2 z Transaction Data Signing (TDS) - w tym opcjonalnym trybie rozszerzenia MODE 2, kryptogram (AC) używany jest jako klucz podpisujący dodatkowe dane wprowadzone przez użytkownika karty, związane z tą transakcją. Posiadacz ma możliwość prowadzenia 10 pól po 10 cyfr. Mogą to być np.: kwota i waluta transakcji, data i czas transakcji, nr rachunku itp.
MODE 3 Transaction Data Signing (TDS) – tryb umożliwiający wprowadzanie znaków alfanumerycznych.

6.5
3DSecure

Usługa 3D Secure to zabezpieczenie transakcji dokonywanych bez fizycznego użycia karty w Internecie. Usługa została wdrożona w pierwszej kolejności przez Visa pod marką „Verified by Visa/Visa Secure, a następnie kolejne organizacje płatnicze udostępniły usługę do swoich klientów: Mastercard, American Express, Discover oraz JCB International. Zabezpieczenie 3D Secure polega na dodatkowej autoryzacji transakcji kodem jednorazowym, wysyłanym klientowi SMS-em na numer podany jako numer kontaktowy z bankiem. Alternatywnie, zamiast SMS, możemy mieć do czynienia z innym drugim faktorem, takim jak komunikat push i akceptacja w bankowości mobilnej. Osoba dokonująca zakupu w sklepie internetowym, po wprowadzeniu niezbędnych danych karty

(numer, imię i nazwisko właściciela, datę ważności, kod CVC/CCV), otrzymuje SMS zawierający jednorazowe hasło lub akceptuje transakcje w bankowości internetowej lub mobilnej. Dopiero po wprowadzeniu kodu w odpowiednie pole dochodzi do ostatecznej autoryzacji.

Na poziom bezpieczeństwa wpływa również konieczność uwierzytelnienia obu stron transakcji, gdyż e-sklep (merchant) musi również obsługiwać technologię 3D Secure.

W roku 2016 ogłoszono nową wersję 3D Secure 2.0. Nowe, ulepszone rozwiązania miało na celu zmniejszenie liczby transakcji nieuprawnionych. 3-D Secure 2.0, dostarcza wydawcom kart i detalistom dodatkowych narzędzi umożliwiających dostosowanie procesu uwierzytelniania, w szczególności poprzez zapewnienie dodatkowych informacji nt. transakcji (np. rodzaj urządzenia czy adres dostawy). Pozwala to detalistom i instytucjom finansowym na bardziej precyzyjne uwierzytelnianie klienta w czasie rzeczywistym.

6.6
Metody push

Coraz większy udział aplikacji bankowych, jako narzędzia dostępu do zasobów finansowych przez klientów instytucji finansowych, sprzyja rozwojowi metody dynamicznych notyfikacji. Metoda push służy do autoryzacji zleceń np. przelewów lub potwierdzenia tożsamości w bankowości internetowej (jako dodatkowy czynnik uwierzytelniający). Metoda push (pojawiających się komunikatów w aplikacji mobilnej banku) może skutecznie zastąpić metodę jednorazowych kodów SMS w wielu zastosowaniach, jednak należy podkreślić, że kody SMS, nawet dla klientów korzystający z autoryzacji mobilnej nadal często są potrzebne, choćby do aktywacji aplikacji mobilnej.

Wyłącznie w gestii klienta jest podjęcie decyzji czy chce korzystać z metody uwierzytelnienia PUSH. Alternatywnie, klienci mogą wciąż wykorzystywać wyłącznie kody SMS.

6.7
Mobile Connect

Mobile Connect to standard stworzony przez GSM Association, który w swoim podstawowym założeniu nie wymaga urządzeń mobilnych posiadających dostęp do Internetu ani instalowania przez użytkowników dodatkowych aplikacji na danym urządzeniu. Mobile Connect oparty jest o rozwiązanie aplikacyjne na karcie SIM.

Usługa jest oferowane przez różnych operatorów telefonii komórkowych, a jej aktywacja sprowadza się do kilku kroków:
1. Zgłoszenie chęci uruchomienia usługi np. :
• na stronie internetowej operatora komórkowego lub w serwisie internetowym,
• w przypadku użycia w aplikacji wspierającej obsługę Mobile Connect, wystarczy podać swój numer telefonu komórkowego, a po chwili na jego ekranie pojawi się komunikat autoryzacyjny;
2. Potwierdzenie aktywacji Mobile Connect za pomocą komunikatu wyświetlonego na ekranie telefonu;Użytkownik dokonuje wyboru metody uwierzytelnienia (np. numer PIN lub potwierdzenie komunikatu push). O wyborze zastosowanej formy decyduje operator usługi.
3. Dane potwierdzające tożsamość użytkownika są zapisywane na karcie SIM. Numer telefonu jest odpowiednikiem loginu, natomiast PIN lub metoda push stanowi drugi czynnik uwierzytelnienia. W ramach Mobile Connect wszelka transmisja informacji może odbywać się w formie szyfrowanej.

6.8
Uwierzytelnienie a czytniki kart elektronicznych

6.8.1
Rodzaje czytników

Czytniki kart elektronicznych zasadniczo nie odgrywają szczególnej roli w procesie uwierzytelnienia do usług elektronicznych on-line. Czytniki stanowią jedynie środek „transportu" danych między komputerem i kartą elektroniczną, nie ingerując ani nie interpretując treści (działają w warstwie niższej w modelu warstwowym odniesienia OSI). Obecnie najbardziej rozpowszechnionym standardem protokołu komunikacyjnego czytników z komputerem jest PC/SC. Rozszerzeniem funkcji czytnika było dodanie klawiatury do wprowadzania kodów PIN (ang. PinPad).

Zastosowanie wbudowanej klawiatury wraz z Secure Messaging, pozwalają na bezpieczne użycie kodu PIN uruchamiającego funkcje kryptograficzne chipa, tj. w przypadku polskiego eDowodu, podpisu osobistego czy też funkcji identyfikacji i uwierzytelnienia.

Zdarza się jednak, że czytniki kart są elementem urządzenia (aplikacji) współpracującego z kartą. W szczególnych przypadkach mamy do czynienia ze specyficznymi czytnikami będących faktycznie terminalami wieloaplikacyjnymi. Terminal taki to komputer z aplikacją komunikującą się z kartą, wyposażony oczywiście w standardowy czytnik kart, posiadający określoną funkcję w systemie wykorzystującym karty elektroniczne. Terminal może być zbudowany jako zestaw urządzeń (komputer PC z systemem operacyjnym, aplikacją/aplikacjami i czytnikiem kart stanowiącym urządzenie zewnętrzne) lub jako jedno urządzenie integrujące wszystkie te elementy w jednej obudowie (zob. przykładowy terminal medyczny na poniższym rysunku). Zintegrowane terminale wieloaplikacyjne to komputery posiadające własne oprogramowanie systemowe (tzw. firmware), w którym można uruchamiać programy (aplikacje) realizujące określone czynności. Terminal taki posiada dwie „przestrzenie" – „otwartą", w której uruchamia się w/w aplikacje, oraz „zamkniętą", która realizuje krytyczne operacje z punktu widzenia bezpieczeństwa (np. dostęp do kart elektronicznych i klawiatury), podlegające ewaluacji w ramach certyfikacji bezpieczeństwa (jest częścią tzw. Target of Evaluation – TOE). Aplikacje z części otwartej nie mogą wykonywać w/w krytycznych operacji samodzielnie, a jedynie pośrednio, korzystając z funkcji zaimplementowanych w certyfikowanej (bezpiecznej) części zamkniętej.

Przykładowy terminal dwuszczelinowy, używany w systemach kart zdrowia.

Zastosowanie terminala jest uzasadnione: specyfiką systemu wykorzystującego karty, przypadków użycia karty i danymi na karcie. Terminal ma zwykle określoną rolę w systemie, jest pod kontrolą i posiada określone uprawnienia. Przykładowo, w systemach kart zdrowia czytnik może lub musi pracować w trybie off-line, a więc musi przenosić i uruchamiać w bezpieczny sposób aplikacje pracujące z kartami elektronicznymi (np. generującymi i podpisującymi elektronicznie plik transakcji medycznej). Ponadto może uzyskiwać dostęp do pewnych danych wrażliwych (np. odczyt i wyświetlenie na ekranie informacji medycznych) lub wykonywać krytyczne operacje kryptograficzne (np. zaszyfrowanie danych wrażliwych przed przesłaniem przez Internet), w sytuacji gdy z założe-

nia pracuje on w środowisku ICT, niebędącym pod kontrolą instytucji odpowiedzialnej za system karty zdrowia (np. w szpitalu). W takiej sytuacji czynnik jest elementem bezpieczeństwa, dlatego czytniki tej klasy posiadają certyfikację bezpieczeństwa wg Common Criteria, standardowo na poziomie EAL3.

Warto wskazać, że czytniki kart zastosowane przez administrację publiczną w procedurze aktywowania warstwy elektronicznej eDowodu, posiadają certyfikację na poziomie EALXX, i w pełni zabezpieczają użycie przez właściciela zarówno kodów PIN jak i PUK.

Nieco bardziej złożonym rozwiązaniem jest, oprócz zabezpieczenia komunikacji na drodze czytnik – karta, dodatkowe zabezpieczenie dostępu do mikroprocesora z wykorzystaniem odrębnego uwierzytelnienia. W tego typu zastosowaniach kart elektronicznych, dostęp do danych w mikroprocesorze i jego funkcji jest ograniczony tylko dla określonych, zaufanych terminali (np. w paszportach biometrycznych zawierających odciski palców, czy w kartach zdrowia zawierających dane medyczne). Zatem, terminal musi uwierzytelnić się za pomocą protokołów symetrycznych (wykorzystanie klucza symetrycznego) lub asymetrycznych (wykorzystanie certyfikatów CVC), zanim karta udzieli dostępu. W tym przypadku terminal musi posiadać własny tzw. bezpieczny element (czyli mikroprocesor), na którym może przechowywać klucze do uwierzytelnienia się wobec karty.

Najbardziej rozpowszechnionym jest wykorzystanie do tego celów certyfikatów CVC. Każdy terminal posiada swoją parę kluczy, dla których wydawany jest certyfikat CVC, zawierający m.in. informacje o uprawnieniach terminala. Terminal, zanim uzyska dostęp do danych lub funkcji mikroprocesora, musi się uwierzytelnić, tzn. udowadnia posiadanie klucza prywatnego oraz przesyła swój certyfikat, a karta elektroniczna weryfikuje jego ważność i uprawnienia.

Istnieją dwa podstawowe standardy dla uwierzytelnienia za pomocą CVC:
• norma EN 14890 – uniwersalny standard dla wszelkich kart kryptograficznych wykorzystujących algorytmy asymetryczne (typu IAS/PKI np. kart do podpisu elektronicznego, kart zdrowia),
• dokument Technical Report BSI 03110 Advanced Security Mechanisms for Machine Readable Travel Documents – dedykowany dla paszportów biometrycznych i kart pobytu.

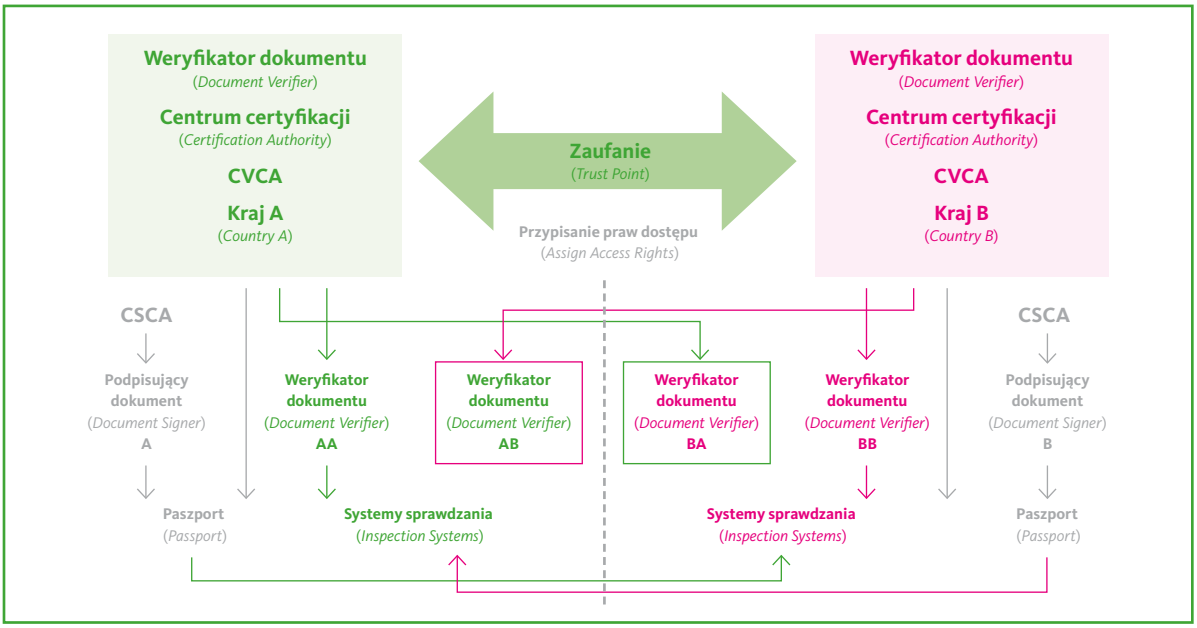
Obydwa standardy są bardzo zbliżone do siebie, wykorzystują te same mechanizmy i protokoły, natomiast różnią się m.in. profilami certyfikatów. Więcej na temat uwierzytelnienia terminali za pomocą CVC znajduje się w rozdziałach 6.5.2 i 9.3.

6.8.2
Uwierzytelnienie terminala

Prace ekspertów europejskich zaowocowały propozycją alternatywnego uwierzytelniania. Chodzi o uwierzytelnianie terminala (ang. terminal authentication) dzięki wykorzystaniu dodatkowej infrastruktury PKI, w której wydawane są certyfikaty dla weryfikujących dokumentów paszportowych.

Rozszerzona kontrola dostępu (Extended Access Control) jest wymagana dla dostępu do odcisków palca – uznawanych za dane wrażliwe – jako ochrona dodatkowa. Jest to opcjonalne wymaganie ICAO, jednakże UE przyjęła je jako obowiązkowe po wprowadzeniu do paszportów odcisków palców. Zakłada się, że kontrola dostępu do tych danych powinna być tak skuteczna, jak to możliwe. Struktury PKI dwu krajów i ich współdziałanie zostały przedstawione na poniższym rysunku.

RYSUNEK 11. Schemat struktur PKI do realizacji EAC.

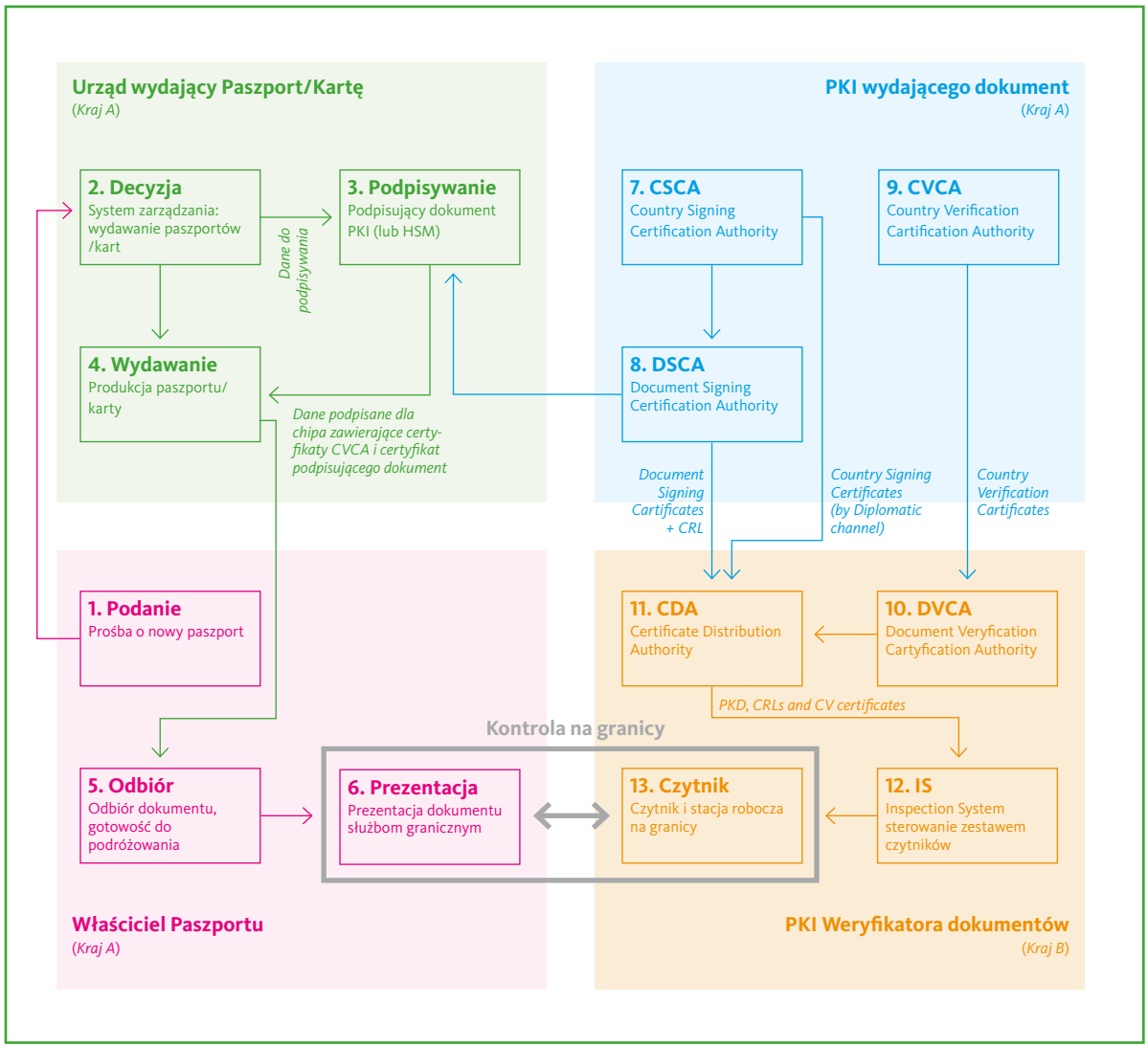


Sposób ten podnosi poziom bezpieczeństwa, zapewnia lepszą poufność danych, a w szczególności przeciwdziała odczytywaniu wrażliwych danych z warstwy elektronicznej paszportu przez nieupoważniony terminal. Najważniejszymi elementami tej struktury są krajowe centra certyfikacji. Istnieją dwa rodzaje narodowych centrów certyfikacji. Pierwsze z nich to CSCA (Country Signing Certificate Authority) czyli centrum, które obecnie wydaje certyfikaty dla wydawcy paszportu (DS - Document Signer). Wydawca paszportu przy ich pomocy podpisuje z kolei dane umieszczane w paszporcie w celu zapewnienia biernego uwierzytelnienia. Centrum to przekazuje swój autocertyfikat (samopodpisany) wszystkim odpowiednikom z pozostałych krajów. Drugie centrum to DVCA (Document Verifier Certificate Authority), czyli centrum, które będzie wydawać certyfikaty zarówno krajowym weryfikatorom dokumentów (DV - Document Verifier, np. Straży Granicznej), a ci z kolei będą wydawać certyfikaty dla systemu sprawdzania (Inspection System, np. systemom zainstalowanym na przejściach granicznych), ale również, a raczej przede wszystkim, wydawać będą certyfikaty wszystkim zagranicznym weryfikatorom dokumentów, aby można było zamknąć ścieżkę zaufania i zrealizować rozszerzoną kontrolę dostępu, co można by bardziej przystępnie określić jako nadawanie uprawnień zagranicznym służbom do czytania paszportów obywateli określonego kraju.

Cały system wydawania i użytkowania paszportów biometrycznych jest dosyć skomplikowany, bo obejmuje: gromadzenie danych, ich weryfikację, podsystem zabezpieczenia przed oszustwami i nieuprawnionym dostępem, produkcję dokumentów i ich dystrybucję, a w końcu weryfikację tych dokumentów i tożsamości ich właścicieli. W sposób schematyczny tę strukturę, i współdziałanie jej obiektów, obrazuje poniższy rysunek 12.

Kontrola na granicy z zastosowaniem paszportu biometrycznego nie została jeszcze określona w sposób dokładny, gdyż może być ona bardzo różnorodna, począwszy od np. wyświetlenia na ekranie zawartości wizerunku twarzy zapisanego w warstwie elektronicznej paszportu i porównanie go ze zdjęciem w paszporcie oraz twarzą podróżnego, do całkowicie zautomatyzowanej kontroli z wykorzystaniem procesu dopasowywania wzorców. W kontroli mogą być stosowane obie cechy biometryczne razem (podnosi to efektywność kontroli) lub każda z nich oddzielnie. Sposób kontroli będzie również uzależniony od środowiska, w którym będzie ona realizowana, inaczej będzie realizowa-

RYSUNEK 12. Proces związany z cyklem życia paszportów biometrycznych.

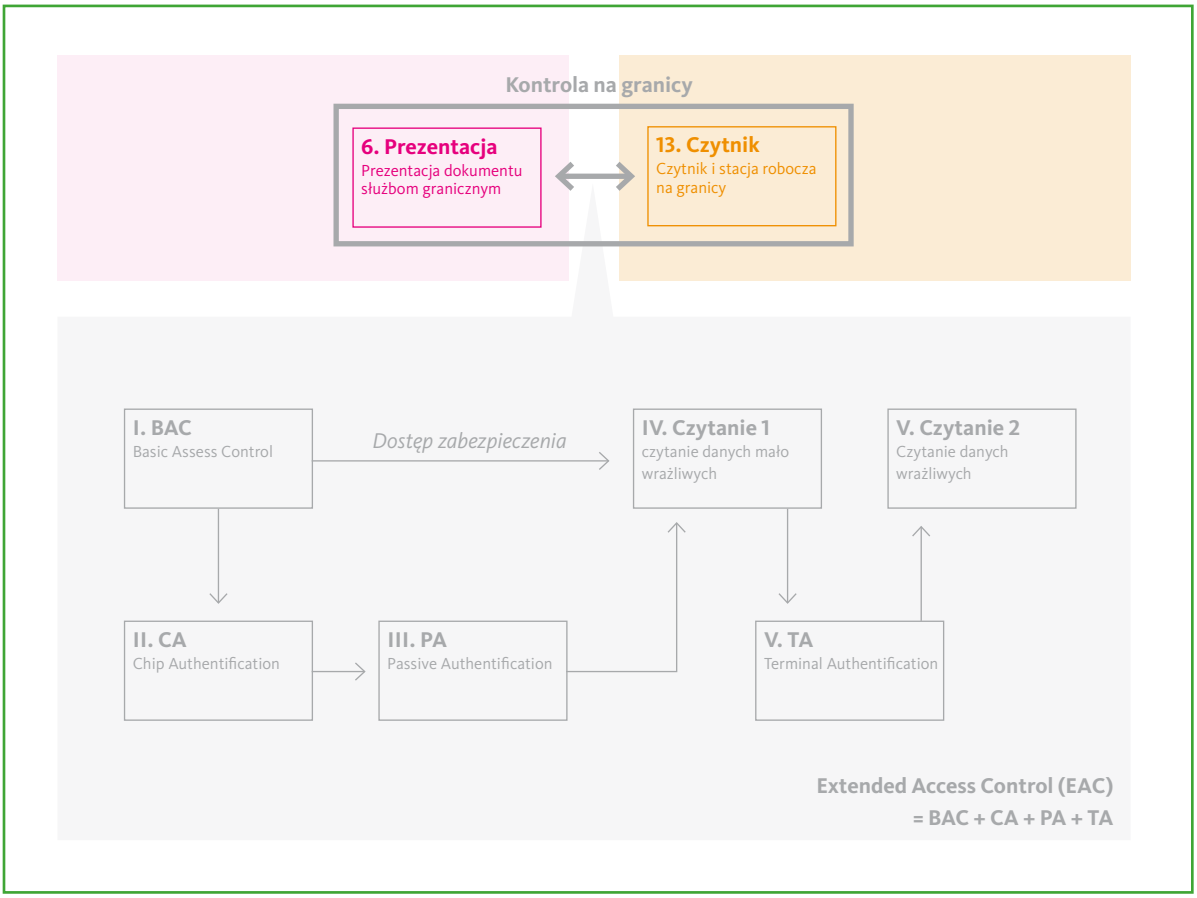


na kontrola w portach lotniczych i morskich, a inaczej w zatłoczonym pociągu lub na leśnym przejściu w niekorzystnych warunkach atmosferycznych (deszcz, śnieg, wiatr, mróz). Od narodowych ustaleń będzie zależało również, czy na pierwszej linii kontroli będzie realizowana tylko podstawowa kontrola dostępu (zdjęcie i podpis danych zapisanych w warstwie elektronicznej oraz opcjonalnie autentyczność paszportu), czy również rozszerzona kontrola dostępu, tj. dodatkowo odciski palców.

Na rysunku 13. przedstawiono schemat weryfikacji paszportu na granicy z możliwością wariantowego wykorzystania wyżej opisanych sposobów.

Podstawowym dokumentem zawierającym regulacje związane z działalnością tej struktury jest raport techniczny. Dokument ten został opracowany przez grupę roboczą ds. PKI i EAC Komitetu Artykułu 6, której Komitet Artykułu 6 nadał oficjalny status i która przyjęła nazwę Brussels Interoperability Group (BIG). Była ona odpowiedzialna za zapewnienie interoperacyjności paszportów wszystkich państw członkowskich UE oraz za opracowanie pewnych dokumentów. Grupa ta, po opracowaniu wszystkich niezbędnych dokumentów (polityk certyfikacji, profilów ochrony, specyfikacji testów itp.) oraz wdrożeniu do eksploatacji we wszystkich krajach członkowskich paszportów elektronicznych z dwoma cechami biometrycznymi, została rozwiązana w roku 2011.

RYSUNEK 13. Schemat weryfikacji paszportu na granicy.



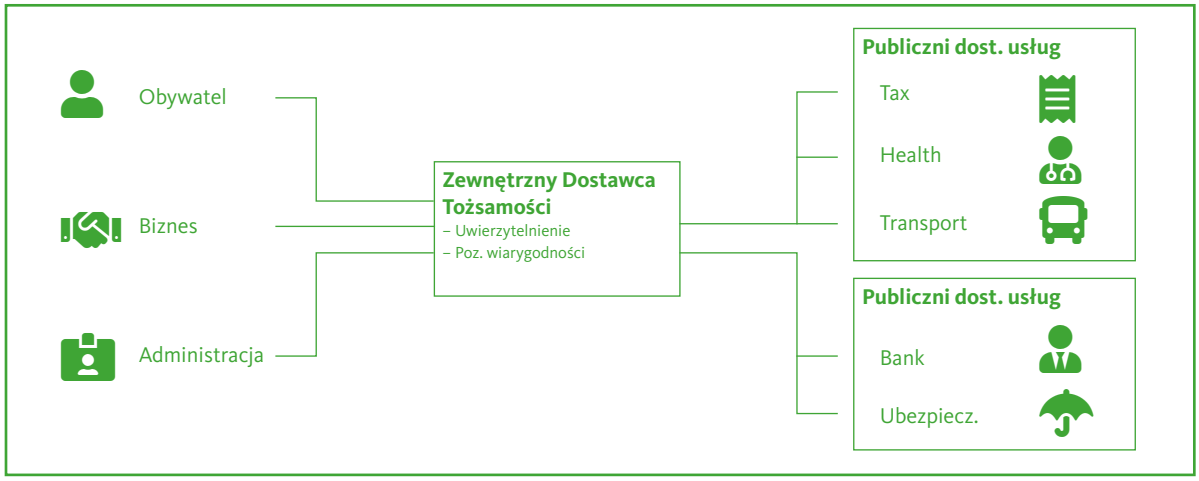
Dokument ten jest jednak nadal uzupełniany i aktualizowany przez kolejne grupy robocze specjalistów z poszczególnych krajów, powoływane doraźnie w tym celu.

6.9
Zcentralizowane systemy potwierdzania tożsamości

Obecnie na popularności zyskują zcentralizowane systemy dostarczające usługi uwierzytelnienia dla zewnętrznych usług elektronicznych. Zwykle jest to dostawca tożsamości (ang. Identity Provider), który wydaje swoje identyfikatory elektroniczne oraz oferuje usługi uwierzytelniania - staje się tzw. „Authentication Service Provider", czyli dostawcą usług uwierzytelnienia.

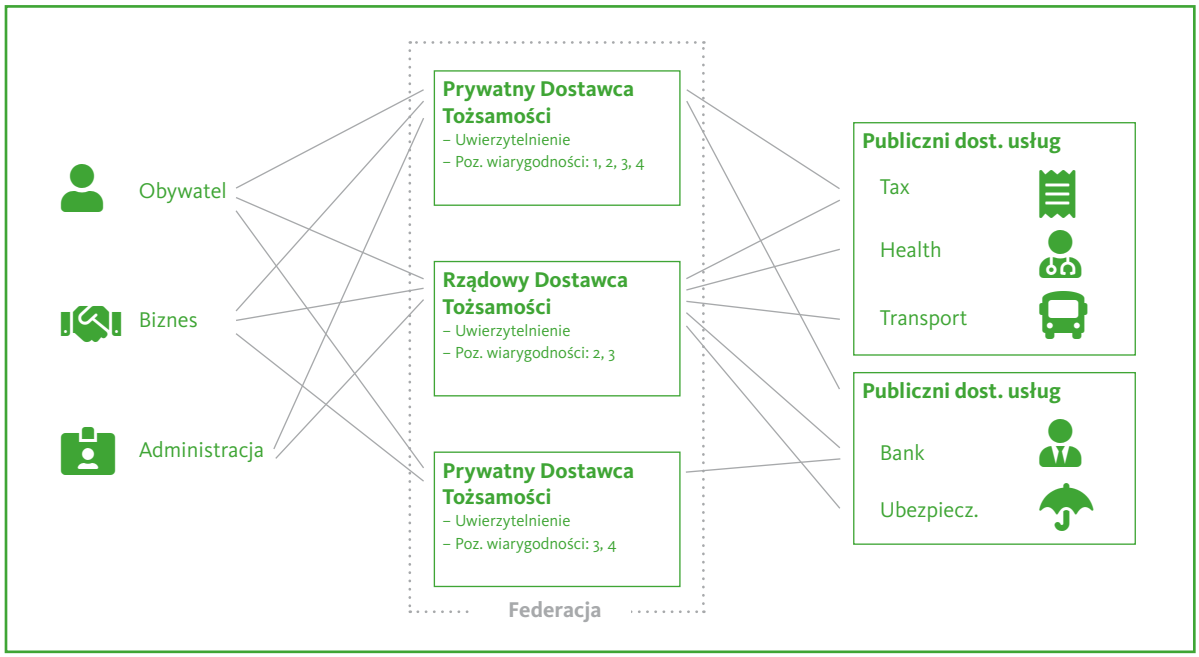
Działanie takich systemów opiera się na wykorzystaniu protokołów federacji tożsamości, takich jak SAML (najbardziej popularny), które umożliwiają współdzielenie w sposób bezpieczny i wiarygodny wyniku uwierzytelnienia. W takim przypadku dostawca e-usługi (np. bank) nie musi wydawać własnych środków do identyfikacji i uwierzytelnienia (np. kart elektronicznych z certyfikatami, czy tokenów OTP) swoim klientom (użytkownikom tej usługi), ani tworzyć własnych systemów IT do realizacji procesu uwierzytelnienia, co wiąże się z określonymi oszczędnościami. W zamian za to dostawca usługi może akceptować i wykorzystywać środki identyfikacji i uwierzytelnienia zewnętrznych dostawców (np. kwalifikowane certyfikaty elektroniczne wydawane przez kwalifikowane centrum certyfikacji, czy też dane uwierzytelniające zawarte w elektronicznym dowodzie osobistym wydanym przez państwo). Idea ta przedstawiona jest na poniższym rysunku.

RYSUNEK 14. Schemat przedstawiający ideę zewnętrznego dostawcy tożsamości.



Co więcej, możliwe jest współistnienie wielu dostawców tożsamości (publicznych i prywatnych), którzy mogą współdzielić swoje usługi z różnymi usługami elektronicznymi i między sobą. Uzyskuje się w ten sposób efekt federacji (wielu) tożsamości (elektronicznych), które są wzajemnie uznawane, przez co ograniczyć można liczbę elektronicznych identyfikatorów używanych przez jedną osobę. Ponadto można realizować funkcję tzw. „Single Sign On", w której uwierzytelnienie u jednego dostawcy tożsamości przy dostępie do jednej usługi automatycznie umożliwia dostęp do innych usług, bez powtarzania procesu uwierzytelnienia – pod warunkiem oczywiście, że poziom wiarygodności uwierzytelnienia jest zgodny z wymaganiem tej drugiej usługi. Idea ta przedstawiona jest na poniższym rysunku.

RYSUNEK 15. Ilustracja idei federacji tożsamości – w tym przykładzie występują dostawcy prywatni i publiczni, oferujące różne poziomy wiarygodności uwierzytelnienia.



Przykładem praktycznej implementacji idei zcentralizowanego systemu potwierdzania tożsamości (i federacji) jest np. system ePUAP w Polsce, a przykładem federacji tożsamości jest np. BankID w Szwecji (zob. więcej w 9.1), czy system zbudowany w ramach projektu STORK.

ROZDZIAŁ 7.0
ASPEKTY PRAWNE

7.1
Zasady świadczenia usług zaufania

Usługi zaufania oraz zasady ich świadczenia określone zostały w eIDAS oraz ustawie o usługach zaufania oraz identyfikacji elektronicznej z dnia 5 września 2016 r. („UoUZIE"), która uzupełnia przepisy rozporządzenia na poziomie krajowym. UoUZIE reguluje funkcjonowanie krajowej infrastruktury zaufania, działalność dostawców usług zaufania, tryb notyfikacji krajowego systemu identyfikacji elektronicznej, nadzór nad dostawcami usług zaufania, krajowy schemat identyfikacji elektronicznej oraz nadzór nad tym schematem. Przepisów ustawy oraz rozporządzenia nie stosuje się jednak do identyfikacji elektronicznej lub świadczenia usług zaufania wykorzystywanych wyłącznie w zamkniętych systemach wynikających z przepisów prawa, porozumień lub umów zawartych przez określoną grupę uczestników.

eIDAS ustanawia otwarty katalog usług zaufania, do którego zalicza m.in.: tworzenie, weryfikację i walidację podpisów elektronicznych oraz certyfikatów uwierzytelniania witryn internetowych czy konserwację elektronicznych podpisów, pieczęci lub certyfikatów powiązanych z tymi usługami (art. 3 pkt. 16 eIDAS). Z kolei katalog kwalifikowanych usług zaufania, które są rozpoznawalne pomiędzy państwami członkowskimi jest katalogiem zamkniętym. Świadczenie kwalifikowanych usług zaufania jest działalnością reglamentowaną i podlega wpisowi do rejestru prowadzonego przez Narodowy Bank Polski z upoważnienia ministra właściwego ds. informatyzacji (aktualnie Minister Cyfryzacji). Wpis do rejestru dostawców usług zaufania świadczących kwalifikowane usługi zaufania, zgodnie z art. 21 eIDAS, poprzedza zwrócenie się do jednostki oceny zgodności o przeprowadzenie audytu i zakontraktowanie oceny zgodności z eIDAS. Lista takich jednostek oceny zgodności umieszczona jest na stronie Komisji Europejskiej. Na dzień 28.11.2019 r., znajdowały się na niej podmioty z 11 państw, przy czym brak jest wśród nich jakichkolwiek podmiotów z Polski. Po otrzymaniu wpisu do rejestru kwalifikowany dostawca usług zaufania powinien dokonać również zgłoszenia do Narodowego Banku Polskiego (pełniącego funkcję Narodowego Centrum Certyfikacji), w celu wydania temu dostawcy certyfikatów usługi zaufania oraz wpisania go na listę kwalifikowanych dostawców (na dzień 13.03.2020 r. na liście tej znajduje się 5 podmiotów). W przypadku dostawców zamierzających świadczyć niekwalifikowane usługi zaufania wpis do rejestru nie jest obligatoryjny i dopuszczalne jest świadczenie takich usług również bez jego uzyskania. Obecnie, w rejestrze dostawców usług niekwalifikowanych, znajduje się jedynie 7 podmiotów.

Nadzór nad dostawcami usług zaufania sprawuje Minister Cyfryzacji. Do zakresu jego obowiązków należy m.in.: unieważnianie certyfikatów wydanych dostawcom usług zaufania, nakładanie kar pieniężnych, współpraca z organami nadzoru innych państw członkowskich i udzielanie im pomocy, analizowanie raportów z oceny zgodności oraz przekazywanie Komisji Europejskiej do dnia 31 marca każdego roku sprawozdania z jego głównych działań w poprzednim roku kalendarzowym wraz z zestawieniem notyfikacji dotyczących naruszeń otrzymanych od dostawców usług zaufania. UoUZIE przyznaje Ministrowi Cyfryzacji dodatkowe uprawnienia w odniesieniu do kwalifikowanych dostawców usług zaufania. Zgodnie z art. 30 UoUZIE, w przypadku prowadzenia przez kwalifikowanego dostawcę działalności niezgodnie z przepisami Minister Cyfryzacji

może wezwać go do: usunięcia stwierdzonych nieprawidłowości i doprowadzenia swojej działalności do stanu zgodnego z przepisami o usługach zaufania, zmiany polityki świadczenia usług lub innych dokumentów lub unieważnienia kwalifikowanych certyfikatów wydanych z naruszeniem polityki, a nawet wydać decyzję o odebraniu kwalifikowanemu dostawcy usług zaufania statusu kwalifikowanego lub odebraniu statusu kwalifikowanego świadczonej przez niego usłudze zaufania.

Co najmniej raz na 24 miesiące, kwalifikowani dostawcy usług podlegają audytowi (na swój własny koszt), celem potwierdzenia, że spełniają nałożone na nich wymogi. Dodatkowo, Minister Cyfryzacji może w każdym momencie przeprowadzić audyt lub zwrócić się do jednostki oceniającej zgodność o przeprowadzenie oceny (na koszt dostawcy) celem potwierdzenia, że zarówno dostawca, jak i świadczone przez niego kwalifikowane usługi zaufania, spełniają wymogi określone w eIDAS. W przypadku podejrzenia, że zostały naruszone przepisy dotyczące ochrony danych osobowych, Minister Cyfryzacji ma obowiązek poinformować o wynikach audytów Urząd Ochrony Danych Osobowych.

Należy również wspomnieć, że wraz z wejściem w życie UoUZIE, świadczenie usług zaufania, podobnie jak wydawanie środków identyfikacji elektronicznej, zostało zaliczone do określonego w art. 6 ustawy z dnia z dnia 29 sierpnia 1997 r. Prawo bankowe („PB") katalogu tzw. innej działalności bankowej,a więc uzyskało status działalności, która może być wykonywana przez bank.

7.2
Podpis elektroniczny a forma czynności prawnej

Korzystanie z usług zaufania niesie za sobą istotne implikacje na gruncie przepisów prawa. Szczególnie doniosłe występują przy tym w zakresie prawa cywilnego i są związane z praktyką stosowania podpisu elektronicznego. eIDAS wyróżnia podpisy: „zwykłe", zaawansowane oraz kwalifikowane (zob. art. 3 pkt 10, 11, 12 eIDAS).

Definicja podpisu elektronicznego jest szeroka i obejmuje każde dane w postaci elektronicznej, które są dołączone lub logicznie powiązane z innymi danymi w postaci elektronicznej i które użyte są przez podpisującego jako podpis. Wraz z wejściem w życie eIDAS zmianie uległa również koncepcja wykorzystania podpisu elektronicznego. Już z samej jego definicji wynika bowiem, że podpis elektroniczny nie służy identyfikacji podpisującego. Jest to jedna z kluczowych różnic w stosunku do definicji podpisu elektronicznego z nieobowiązującej już ustawy o podpisie elektronicznym z 2001 r., gdzie wyraźnie wskazywano na taką właśnie jego funkcję. Na gruncie eIDAS, warunkiem kwalifikacji podpisu jako elektronicznego jest natomiast użycie danych wyłącznie do celów wykonania podpisu, a więc na pierwszy plan wysuwa się uwierzytelnianie osoby, nie zaś jej identyfikacja.

Ponieważ podpis elektroniczny stanowi już samo dołączenie bądź logiczne powiązanie danych w postaci elektronicznej z innymi danymi w postaci elektronicznej, z reguły jego zastosowanie będzie związane ze składaniem oświadczeń woli w formie dokumentowej w rozumieniu przepisów ustawy z dnia 23 kwietnia 1964 r. Kodeks cywilny („KC"). Zgodnie z art. 77^2 KC, dla zachowania formy dokumentowej wystarczające jest złożenie oświadczenia woli w postaci dokumentu. Pojęcie dokumentu jest przy tym rozumiane szeroko i oznacza każdy nośnik informacji umożliwiający zapoznanie się z treścią dokumentu (art. 77^3).

Wprowadzony na gruncie eIDAS kwalifikowany podpis elektroniczny zastąpił natomiast dotychczas funkcjonujący bezpieczny podpis elektroniczny weryfikowany przy pomocy ważnego kwalifikowanego certyfikatu. Kwalifikowany podpis elektroniczny definiowany jest jako zaawansowany podpis elektroniczny, składany za pomocą kwalifikowanego urządzenia do składania podpisu elektronicznego i który opiera się na kwalifikowanym certyfikacie podpisu elektronicznego (zob. pkt. 4.1.8.3 Przewodnika). Kwalifikowane urządzenia do składania podpisu elektronicznego podlegają certyfikowaniu przez odpowiednie publiczne lub prywatne podmioty wyznaczone przez państwa członkowskie, podlegające notyfikacji Komisji Europejskiej (do tej pory na liście notyfikowanych podmiotów nie znajduje się jednak żaden podmiot z Polski). Skorzystanie z kwalifikowanego podpisu elektronicznego będzie związane ze składaniem oświadczeń woli w formie elektronicznej. Zgodnie z art. 78^1 § 1 KC forma taka występuje w przypadku złożenia oświadczenia woli w postaci elektronicznej i opatrzenia go właśnie takim kwalifikowanym podpisem elektronicznym. Co jednak szczególnie istotne, oświadczenie woli złożone w formie elektronicznej jest zgodnie z art. 78^1 § 2 KC równoważne z oświadczeniem woli złożonym w formie pisemnej. Przepis ten stanowi odzwierciedlenie art. 25 eIDAS, zgodnie z którym kwalifikowany podpis elektroniczny ma skutek prawny równoważny podpisowi własnoręcznemu.

W powyższym kontekście należy również nadmienić, że w ostatnim czasie, w ramach prac Grupy Roboczej ds. rejestrów rozproszonych i blockchain[5], pojawiła się koncepcja rozszerzenia dyspozycji przepisu art. 78^1 KC dodatkowo na kwalifikowaną pieczęć elektroniczną, co miałoby służyć zwiększeniu efektywności oraz zabezpieczenia cyfrowego obrotu gospodarczego. Pieczęć elektroniczna, w odróżnieniu od podpisu elektronicznego, służy zapewnieniu autentyczności pochodzenia oraz integralności danych w postaci elektronicznej, dodanych do innych danych w postaci elektronicznej lub logicznie z nimi powiązanych (zob. rozdział 4.1.3Przewodnika). Przede wszystkim jednak, w przypadku pieczęci elektronicznej, dysponentem klucza prywatnego (zob. rozdział 5.3.2 Przewodnika) może być osoba prawna. Celem więc proponowanego zabiegu ma być uporządkowanie statusu prawnego czynności realizowanych z faktycznym wyłączeniem lub zaangażowaniem czynnika ludzkiego oraz usprawnienie obrotu gospodarczego poprzez umożliwienie wykorzystywania pieczęci elektronicznej do składania oświadczeń woli w postaci elektronicznej. Rozwiązanie takie z jednej strony zwiększałoby bezpieczeństwo prawne kontrahentów przedsiębiorców wykorzystujących do składania oświadczeń zautomatyzowane systemy, a z drugiej wymuszałoby na przedsiębiorcach zwiększenie kontroli nad zautomatyzowanymi systemami wykorzystywanymi w ich działalności. Choć niewątpliwie takie rozwiązanie niesie za sobą wiele możliwości, które należy ocenić pozytywnie, to jednak wymaga ostrożnego rozważenia, gdyż może stwarzać również pewne problemy praktyczne. Dla przykładu wskazuje się, że wykorzystanie przez kontrahenta pieczęci elektronicznej przy składaniu oświadczenia woli może wysoce utrudnić instytucji obowiązanej wykonanie, wynikających z przepisów o przeciwdziałaniu praniu pieniędzy i finansowaniu terroryzmu, obowiązków z zakresu weryfikacji tożsamości osoby działającej w imieniu klienta[6]. Kontrowersyjne jest również to, czy rozszerzenie funkcji pieczęci elektronicznej poza samo zapewnianie autentyczności i integralności

5. *Działająca przy Ministerstwie Cyfryzacji Grupa robocza ds. rejestrów rozproszonych i blockchain jest platformą dyskusji na temat cyfryzacji różnych sektorów gospodarki i administracji z wykorzystaniem technologii blockchain, w skład której wchodzą specjaliści technologii blockchain będący przedstawicielami m.in.: biznesu, izb gospodarczych, kancelarii prawnych, uczelni wyższych oraz jednostek badawczo-rozwojowych.*

6. *Grupa robocza ds. rejestrów rozproszonych i blockchain, Koncepcja Rozszerzenia Znaczenia Prawnego Pieczęci Elektronicznej, 20.11.2019 r., s. 19-21.*

danych (tj. celem przyznania jej również funkcji oświadczenia woli), na gruncie prawa krajowego, nie spowodowałoby problemów praktycznych w obrocie unijnym, poprzez doprowadzenie do niejednolitej interpretacji w ramach UE pojęcia pieczęci elektronicznej oraz skutków prawnych jej zastosowania.

Odrębna regulacja w zakresie formy czynności prawnej, również związana ze stosowaniem podpisów elektronicznych, zawarta jest w przepisach PB. Zgodnie z art. 7 PB, oświadczenia woli związane z dokonywaniem czynności bankowych mogą być składane w postaci elektronicznej. Dodatkowo regulacja ta przewiduje, że jeżeli ustawa zastrzega dla czynności prawnej formę pisemną, uznaje się, że czynność dokonana w postaci elektronicznej spełnia wymagania formy pisemnej także wtedy, gdy została zastrzeżona pod rygorem nieważności. Warto przy tym dodać, że wraz z wejściem w życie UoUZIE, do PB dodany został również art. 7b, wskazujący, że oświadczenia woli związane ze świadczeniem przez bank usług zaufania mogą być składane w postaci elektronicznej.

Sposób tworzenia, utrwalania, przekazywania, przechowywania i zabezpieczania, w tym przy zastosowaniu podpisu elektronicznego, dokumentów związanych z czynnościami bankowymi sporządzonych na informatycznych nośnikach danych, określa obecnie rozporządzenie Rady Ministrów z dnia 26.10.2004 r. („Rozporządzenie z art. 7 PB"). Niestety, rozporządzenie to nie zostało dostosowane do regulacji eIDAS oraz UoUZIE, co może rodzić problemy w jego interpretacji i stosowaniu. Dla przykładu, Rozporządzenie z art. 7 PB posługuje się pojęciami podpisu elektronicznego i bezpiecznego podpisu elektronicznego, które to od momentu uchylenia ustawy o podpisie elektronicznym pozostają nieaktualne. Należy jednak zaznaczyć, że już obecnie w Rządowym Centrum Legislacyjnym dostępny jest projekt nowego rozporządzenia, mającego zastąpić Rozporządzenie z art. 7 PB. W dniu 11 marca zostało skierowane do podpisu przez Prezesa Rady Ministrów. Projekt ten opracowany jest już z zastosowaniem terminologii właściwej eIDAS, w szczególności w zakresie pojęć kwalifikowanego podpisu elektronicznego oraz kwalifikowanej pieczęci elektronicznej. Intersującą zmianą jest również wprowadzenie możliwości wykorzystywania technologii DLT/blockchain w celu przechowywania danych i dokumentów związanych z czynnościami bankowymi. Znowelizowane rozporządzenie wejdzie w życie po upływie 6 miesięcy od dnia jego ogłoszenia.

7.3
Identyfikacja i Węzeł Krajowy

Zarówno przepisy eIDAS, jak i UoUZIE, wprowadziły również nowe regulacje w zakresie systemów identyfikacji elektronicznej. Zgodnie z punktem 12 preambuły eIDAS, celem rozporządzenia nie jest ingerowanie w systemy zarządzania tożsamością elektroniczną i powiązane z nimi infrastruktury ustanowione w państwach członkowskich, a zapewnienie bezpiecznej elektronicznej identyfikacji i uwierzytelniania na potrzeby dostępu do transgranicznych usług online oferowanych przez państwa członkowskie. Jednym z kluczowych założeń eIDAS w zakresie identyfikacji elektronicznej jest zatem: doprowadzenie do wzajemnego uznawania środków identyfikacji elektronicznej przez państwa członkowskie, zniesienie, przynajmniej w przypadku usług publicznych, istniejących barier w transgranicznym stosowaniu środków identyfikacji elektronicznej w państwach członkowskich w celu uwierzytelniania, wypracowanie wspólnego podejścia w zakresie uznawania i sposobów notyfikowania systemów identyfikacji elektronicznej oraz określenie poziomów bezpieczeństwa i współpraca państw członkowskich w zakresie bezpieczeństwa i interoperacyjności systemów identyfikacji elektronicznej. Na mocy eIDAS systemy identyfikacji elektronicznej, które spełniają wymogi stawiane

im w rozporządzeniu, podlegają notyfikacji Komisji Europejskiej. Zgodnie z Dziennikiem Urzędowym Komisji Europejskiej (2019/C 425/6), dotychczas 13 państw dokonało notyfikacji swoich systemów, są to: Niemcy, Włochy (zgłoszone 2 systemy), Chorwacja, Estonia, Hiszpania, Luksemburg, Belgia (zgłoszone 2 systemy), Portugalia, Wielka Brytania, Czechy, Holandia, Słowacja oraz Łotwa.

Stosownie do wymogów UoUZIE w Polsce powstał krajowy schemat identyfikacji elektronicznej, w którego skład wchodzi: węzeł krajowy identyfikacji elektronicznej login.gov.pl („Węzeł Krajowy"), przyłączone do niego systemy identyfikacji elektronicznej, w których wydawane są środki identyfikacji elektronicznej, systemy teleinformatyczne, w których udostępniane są usługi online oraz węzeł wykorzystywany w procesie transgranicznego uwierzytelniania osób. Zgodnie z art. 21a ust. 2 UoUZIE Węzeł Krajowy jest rozwiązaniem organizacyjno-technicznym umożliwiającym uwierzytelnianie użytkownika systemu teleinformatycznego, korzystającego z usługi online, z wykorzystaniem środka identyfikacji elektronicznej wydanego w systemie identyfikacji elektronicznej przyłączonym do tego węzła bezpośrednio albo za pośrednictwem węzła transgranicznego. Przyłączenie systemu identyfikacji elektronicznej oraz systemu teleinformatycznego, w którym udostępniane są usługi do węzła krajowego, następuje na wniosek podmiotu odpowiedzialnego za ten system. Obecnie z wykorzystaniem Węzła Krajowego można skorzystać ze 121 portali oferujących usługi online[7].

Do Węzła Krajowego powinny być przyłączone systemy teleinformatyczne, w których świadczone są usługi spełniające następujące warunki:

1. są realizowane przez Internet,
2. są usługami świadczonymi przez podmiot publiczny,
3. wymagają uwierzytelnienia użytkownika za pomocą środka identyfikacji elektronicznej o określonym poziomie bezpieczeństwa (niskim, średnim lub wysokim), które może być realizowane za pośrednictwem tego węzła[8].

Użytkownik ma możliwość skorzystania z usług oferowanych poprzez Węzeł Krajowy za pomocą logowania z wykorzystaniem profilu zaufanego – usługi oferowanej przez Elektroniczną Platformę Usług Administracji Publicznej („ePUAP"). Oznacza to, że nie jest konieczne generowanie dla użytkownika nowych, dedykowanych danych uwierzytelniających, gdyż profil zaufany zostaje tworzony za pośrednictwem banku. Zgodnie z § 8 ust. 10 rozporządzenia Ministra Cyfryzacji z dnia 10 września 2018 r. w sprawie profilu zaufanego i podpisu zaufanego, jeżeli użytkownik posiada profil w ePUAP może on skorzystać z profilu zaufanego z wykorzystaniem czynników uwierzytelniania tożsamych z czynnikami służącymi do jego identyfikacji i uwierzytelniania w ePUAP. W praktyce oznacza to, że do logowania w profilu zaufanym użytkownik może wykorzystywać również swoje dane logowania do bankowości internetowej, oczywiście o ile dany bank zapewnia taką opcję swoim klientom. Możliwość ta wynika wprost z art. 19a ust. 2a ustawy z dnia 17.02.2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne. Zgodnie z tymi przepisami, Minister Cyfryzacji, na wniosek banku krajowego lub innego przedsiębiorcy, udziela zgody na nieodpłatne wykorzystywanie do identyfikacji i uwierzytelniania w ePUAP środków identyfikacji elektronicznej stosowanych do uwierzytelniania w systemie teleinformatycznym banku krajowego lub innego przedsiębiorcy. Innymi metodami, z wykorzystaniem których możliwe jest korzystanie z usług oferowanych poprzez Węzeł Krajowy są: e-Tożsamość oraz e-dowód (zob. rozdział 6.2 Przewodnika).

7. zob. oficjalna strona internetowa Węzła Krajowego, https://login.gov.pl/login/services, dostęp: 11.03.2020 r.
8. zob. załącznik nr 6 dokumentacji Ministerstwa Cyfryzacji dotyczącej integracji z Węzłem Krajowym, https://mc.bip.gov.pl/interoperacyjnosc-mc/wezel-krajowy-dokumentacja-dotyczaca-integracji-z-wezlem-krajowym.html), dostęp: 09.03.2020 r.

7.4
Uwierzytelnianie w usługach płatniczych

Zagadnienie uwierzytelniania odgrywa szczególnie istotną rolę w przepisach z zakresu usług płatniczych, gdzie doczekało się szczegółowego uregulowania w dyrektywie Parlamentu Europejskiego i Rady (UE) 2015/2366 z dnia 25 listopada 2015 r. w sprawie usług płatniczych w ramach rynku wewnętrznego („PSD2"), w implementujących tę dyrektywę przepisach ustawy z dnia 19 sierpnia 2011 r. o usługach płatniczych (dalej „UUP"), a także w rozporządzeniu delegowanym Komisji (UE) 2018/389 z dnia 27 listopada 2017 r. uzupełniającym PSD2, w odniesieniu do regulacyjnych standardów technicznych dotyczących silnego uwierzytelniania klienta i wspólnych i bezpiecznych otwartych standardów komunikacji („RTS").

Przepisy UUP definiują uwierzytelnianie jako procedurę umożliwiającą dostawcy usług płatniczych weryfikację tożsamości użytkownika lub ważności stosowania konkretnego instrumentu płatniczego, łącznie ze stosowaniem indywidualnych danych uwierzytelniających (art. 2 pkt 33b UUP). Szczególnym rodzajem uwierzytelniania definiowanym w UUP jest silne uwierzytelnianie użytkownika („SCA"), zdefiniowane (art. 2 pkt. 26aa UUP) jako uwierzytelnianie zapewniające ochronę poufności danych w oparciu o zastosowanie co najmniej dwóch elementów należących do kategorii:
- wiedza o czymś, o czym wie wyłącznie użytkownik,
- posiadanie czegoś, co posiada wyłącznie użytkownik,
- cechy charakterystyczne użytkownika.

będących integralną częścią tego uwierzytelniania oraz niezależnych w taki sposób, że naruszenie jednego z tych elementów nie osłabia wiarygodności pozostałych. Dodatkowo, szczegółowe wymagania odnoszące się do SCA zostały uregulowane w RTS, które adresują takie kwestie jak: zasady dokonywania przeglądu środków bezpieczeństwa, stosowanie kodu uwierzytelniającego i dynamicznego łączenia, wymogi dotyczące poszczególnych elementów należących do kategorii wiedza, posiadanie oraz cechy klienta, wymóg niezależności elementów, a także zasady dotyczące poufności i integralności indywidualnych danych uwierzytelniających.

Zgodnie z art. 32i ust. 1 UUP dostawcy usług płatniczych zobowiązani są do stosowania SCA, w przypadku gdy płatnik:
- uzyskuje dostęp do swojego rachunku w trybie on-line,
- inicjuje elektroniczną transakcję płatniczą,
- przeprowadza za pomocą kanału zdalnego czynność, która może wiązać się z ryzykiem oszustwa związanego z wykonywanymi usługami płatniczymi lub innych nadużyć.

Przepisy RTS ustanawiają jednak katalog przypadków, w których, na zasadzie wyjątku, dostawcy mogą odstąpić od stosowania SCA (art. 10 – 21 RTS). Wyłączenia takie dotyczą m.in.: niektórych sytuacji uzyskiwania dostępu do informacji o rachunku płatniczym, płatności zbliżeniowych w punktach sprzedaży, płatności w terminalach samoobsługowych służących uiszczaniu opłat za przejazd i opłat za postój, zaufanych odbiorców, transakcji cyklicznych, poleceń przelewu miedzy rachunkami będącymi w posiadaniu tej samej osoby fizycznej lub prawnej, transakcji niskokwotowych, czy transakcji, które dostawca usług płatniczych uzna za charakteryzujące się niskim poziomem ryzyka.

Pojęcie uwierzytelniania, jako procedury o charakterze weryfikacyjnym, której obowiązek przeprowadzenia obciąża dostawcę, immanentnie związane jest z pojęciem autoryzacji, odnoszącym się na gruncie przepisów UUP do działań podejmowanych przez użytkownika. Zgodnie z art. 40 ust. 1 UUP, transakcję płatniczą uważa się za autoryzo-

waną, jeżeli płatnik wyraził zgodę na wykonanie transakcji płatniczej w sposób przewidziany w umowie między płatnikiem a jego dostawcą. Autoryzację należy więc, na gruncie omawianych przepisów, rozumieć jako złożenie przez użytkownika konkretnego oświadczenia woli, w konkretny, przewidziany we właściwej umowie, sposób. Sposób ten najczęściej będzie sprowadzał się do właściwego posłużenia się wydanym płatnikowi przez dostawcę instrumentem płatniczym.

Definicja instrumentu płatniczego zawarta w przepisach UUP jest bardzo szeroka i obejmuje każde zindywidualizowane urządzenie lub uzgodniony przez użytkownika i dostawcę zbiór procedur, wykorzystywane przez użytkownika do złożenia zlecenia płatniczego (art. 2 pkt 10 UUP). Wydanie instrumentu płatniczego wiąże się z koniecznością przestrzegania przez dostawcę i użytkownika szeregu obowiązków mających na celu zapewnianie bezpieczeństwa korzystania z takiego instrumentu.

Użytkownik uprawniony do korzystania z instrumentu płatniczego jest obowiązany (art. 42 ust. 1 UUP):
- korzystać z instrumentu płatniczego zgodnie z umową ramową, w szczególności podejmować niezbędne środki służące zapobieżeniu naruszeniu indywidualnych danych uwierzytelniających, w szczególności jest obowiązany do przechowywania instrumentu płatniczego z zachowaniem należytej staranności oraz nieudostępniania go osobom nieuprawnionym, oraz
- zgłaszać niezwłocznie dostawcy lub podmiotowi wskazanemu przez dostawcę stwierdzenie utraty, kradzieży, przywłaszczenia albo nieuprawnionego użycia instrumentu płatniczego lub nieuprawnionego dostępu do tego instrumentu.

Dostawca wydający instrument płatniczy jest z kolei obowiązany do:
- zapewnienia, że indywidualne dane uwierzytelniające nie są dostępne dla osób innych niż użytkownik uprawniony do korzystania z tego instrumentu,
- niewysyłania niezamówionego instrumentu płatniczego, z wyjątkiem sytuacji, w których instrument płatniczy otrzymany przez użytkownika podlega wymianie,
- zapewnienia stałej dostępności odpowiednich środków pozwalających użytkownikowi na bezpłatne dokonanie zgłoszenia stwierdzenia utraty, kradzieży, przywłaszczenia albo nieuprawnionego użycia instrumentu płatniczego lub nieuprawnionego dostępu do tego instrumentu oraz procedur pozwalających na udowodnienie dokonania takiego zgłoszenia na wniosek złożony przez użytkownika w terminie 18 miesięcy od jego dokonania, a także do uniemożliwienia korzystania z instrumentu płatniczego po dokonaniu zgłoszenia,
- zapewnienia stałej dostępności odpowiednich środków pozwalających użytkownikowi na wystąpienie z wnioskiem o odblokowanie albo zastąpienie zablokowanego instrumentu płatniczego nowym, a także do nienakładania opłat w wysokości przekraczającej kosztów bezpośrednio związanych z wydaniem nowego instrumentu płatniczego.

Prawidłowe przeprowadzanie uwierzytelniania ma istotne znacznie nie tylko dla oceny wypełniania przez dostawcę nałożonych nie niego w tym zakresie obowiązków, ale również dla rozkładu odpowiedzialności dostawcy i użytkownika w przypadku wystąpienia nieautoryzowanych transakcji płatniczych (nazywanych też transakcjami oszukańczymi, czy bardziej potocznie fraudami). To bowiem, czy daną transakcję dostawca powinien uznać za autoryzowaną, zależy w szczególności od poprawnego zastosowania i wyniku procedury uwierzytelnienia. Podobnie, istotne znaczenie dla kwestii tej odpowiedzialności może mieć ocena wypełnienia przez użytkownika i dostawcę wskazanych powyżej obowiązków związanych z instrumentami płatniczymi.

W przypadku wystąpienia nieautoryzowanej transakcji płatniczej przepisy (art. 46 ust. 1 UUP) zasadniczo nakładają na dostawców obowiązek niezwłocznego zwrotu płatnikowi kwoty takiej transakcji (nie później niż do końca dnia roboczego następującego po dniu

stwierdzenia wystąpienia nieautoryzowanej transakcji, którą został obciążony rachunek płatnika, lub po dniu otrzymania stosownego zgłoszenia, z wyjątkiem przypadku, gdy dostawca płatnika ma uzasadnione i należycie udokumentowane podstawy, aby podejrzewać oszustwo, i poinformuje o tym w formie pisemnej organy powołane do ścigania przestępstw). UUP określa jednak pewne przypadki, w których odpowiedzialność za nieautoryzowane transakcje poniesie płatnik (art. 46 ust. 2 UUP).

Po pierwsze, płatnik odpowiada za nieautoryzowane transakcje płatnicze do wysokości równowartości w walucie polskiej kwoty 50 euro, jeżeli nieautoryzowana transakcja jest skutkiem:
• posłużenia się utraconym przez płatnika albo skradzionym płatnikowi instrumentem płatniczym lub
• przywłaszczenia instrumentu płatniczego.

Trzeba jednak dodać, że nawet tak niewielki kwotowo, jak wskazany powyżej, zakres odpowiedzialności płatnika nie ma zastosowania, gdy płatnik nie miał możliwości stwierdzenia utraty, kradzieży lub przywłaszczenia instrumentu płatniczego przed wykonaniem transakcji płatniczej (z wyjątkiem przypadku, gdy działał umyślnie), a także w przypadku, gdy utrata instrumentu płatniczego przed wykonaniem transakcji płatniczej została spowodowana działaniem lub zaniechaniem ze strony pracownika, agenta lub oddziału dostawcy płatnika lub podmiotu świadczącego na rzecz tego dostawcy usługi techniczne. Po drugie, płatnik odpowiada za nieautoryzowane transakcje płatnicze w pełnej wysokości, jeżeli doprowadził do nich umyślnie albo w wyniku umyślnego lub będącego skutkiem rażącego niedbalstwa naruszenia co najmniej jednego z omówionych już powyżej obowiązków użytkownika dotyczących korzystania z instrumentu płatniczego.

Co istotne, wskazane powyżej przypadki odpowiedzialności płatnika mają zastosowanie w sytuacjach, gdy stosowane są przez dostawcę zasady SCA. UUP stanowi bowiem, że w przeciwnym przypadku, gdy dostawca płatnika nie wymaga SCA, płatnik nie ponosi odpowiedzialności za nieautoryzowane transakcje płatnicze, chyba że działał umyślnie. Analogicznie, odpowiedzialność płatnika ograniczona jest do przypadków jego umyślności, w zakresie nieautoryzowanych transakcji płatniczych, do których doszło po dokonaniu przez płatnika zgłoszenia dostawcy (lub podmiotowi wskazanemu przez dostawcę) stwierdzenia utraty, kradzieży, przywłaszczenia albo nieuprawnionego użycia instrumentu płatniczego lub nieuprawnionego dostępu do tego instrumentu, a także w sytuacjach gdy dostawca nie zapewnia odpowiednich środków umożliwiających dokonanie w każdym czasie takiego zgłoszenia.

Warto jednak mieć na uwadze, że w przypadku użytkowników niebędących konsumentami istnieje możliwości uzgodnienia odmiennych niż wskazane powyżej zasad odpowiedzialności za nieautoryzowane transakcje płatnicze (art. 33 w zw. z art. 46 ust. 2-5 UUP).

7.5
Identyfikacja TPP

Przepisy PSD2 uzupełniły katalog usług płatniczych o dwie nowe usługi: inicjowania transakcji płatniczej oraz dostępu do informacji o rachunku. Świadczenie tych usług przez ich dostawców (tzw. Third Party Providers, „TPP") ma, zgodnie z przepisami RTS, odbywać się w oparciu o spełniający określone wymogi interfejs, którego obowiązek posiadania został nałożony na dostawców prowadzący rachunki płatnicze dostępne on-

-line („ASPSP"). Jedną z kluczowych, z punktu widzenia przepisów RTS, funkcjonalnością jaka powinna być zapewniona w takim interfejsie jest umożliwienie TPP zidentyfikowania się wobec ASPSP (art. 30 ust. 1 pkt a RTS). Z kolei, do celów takiej identyfikacji TPP, mogą wykorzystywać kwalifikowane certyfikaty pieczęci elektronicznych oraz kwalifikowane certyfikaty uwierzytelniania witryn internetowych (art. 34 ust. 1 RTS). RTS stawia przy tym wymóg, aby takie kwalifikowane certyfikaty zawierały dodatkowe szczególne atrybuty w stosunku do roli dostawcy, a także do nazwy właściwych organów, w których dostawca usług płatniczych jest zarejestrowany. Co istotne, stosowanie tych dodatkowych atrybutów nie powinno wpływać na interoperacyjność i uznawanie kwalifikowanych certyfikatów pieczęci elektronicznych lub kwalifikowanych certyfikatów uwierzytelniania witryn internetowych zgodnie z przepisami eIDAS[9].

Warto dodatkowo nadmienić, że w dniu 11.12.2018 r. Europejski Organ Nadzoru Bankowego („EBA") wydał opinie w zakresie wykorzystywania przez TPP wyżej wymienionych metod w celu identyfikowania się przed ASPSP[10]. EBA wskazał, że TPP mogą alternatywnie:

- stosować jednocześnie kwalifikowane certyfikaty pieczęci elektronicznych i kwalifikowane certyfikaty uwierzytelniania witryn internetowych – rozwiązanie to zostało uznane za najbezpieczniejsze,
- wykorzystywać wyłącznie kwalifikowane certyfikaty uwierzytelniania witryn internetowych – rozwiązanie o mniejszym stopniu bezpieczeństwa,
- wykorzystywać kwalifikowane certyfikaty pieczęci elektronicznych wraz z dodatkowymi elementami, które zapewnią bezpieczną komunikację – rozwiązanie mniej bezpieczne, o ile nie jest stosowany też drugi element, który zapewnia poufność przekazywanych danych.

Równocześnie jednak EBA w pkt. 15 opinii sugeruje, żeby właściwe organy nadzoru rekomendowały ASPSP, aby te wymagały od TPP stosowania rozwiązania opisanego w pkt. 1. W kontekście liczby wykorzystywanych do identyfikacji certyfikatów, EBA wskazuje, że jeżeli TPP korzysta z usług np.: agentów, dostawców usług technicznych bądź prowadzi działalność poprzez oddział, to pożądane jest stosowanie wielu certyfikatów – odrębnych dla każdego z podmiotów, z których TPP korzysta przy świadczeniu usług płatniczych.

7.6
Dane osobowe a identyfikacja i uwierzytelnianie

Stosowanie rozwiązań z zakresu identyfikacji i uwierzytelniania nierozerwalnie wiąże się z tematyką przetwarzania danych osobowych. Dlatego też przedsiębiorcy, w ramach przeprowadzania tych czynności, muszą pamiętać o stosowaniu regulacji z tego zakresu, w szczególności przepisów rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych („RODO"). Kluczowe zasady dotyczące przetwarzania danych osobowych zawiera art. 5 tego rozporządzenia. Należą do nich: zgodność z prawem, rzetelność i przejrzystość, ograniczenie celu, minimalizacja danych, prawidłowość, ograniczenie przechowywania, integralność i poufność danych osobowych oraz rozliczalności. Przepisy RODO określają także m.in.: zamknięty katalog podstaw do przetwarzania danych osobowych (art. 6 RODO), uprawnienia osób, których dane dotyczą, a także nakładają na administratora danych osobowych liczne obowiązki, w tym również o charakterze organizacyjnym.

9. *Można nadmienić, że analogiczne zasady dotyczą również zasad potwierdzania dostępność kwoty niezbędnej do wykonania transakcji płatniczej realizowanej w oparciu o tę kartę, zgodnie z art. 49a UUP.*
10. *zob. opinion of the European Banking Authority on the use of EIDAS certificates under the RTS on SCA and CSC (EBA-Op-2018-7).*

Związek przepisów dotyczących przetwarzania danych osobowych z przepisami z zakresu identyfikacji i uwierzytelniania widoczny jest m.in. na gruncie regulacji określających zasady stosowania SCA, w szczególności art. 2 oraz art. 18 RTS. Przepisy te, nakładają na dostawców usług płatniczych obowiązki w zakresie wykonywania analizy przeprowadzanych transakcji, celem wykrywania nieautoryzowanych lub nielegalnych transakcji płatniczych. Sprostanie wymogom określonym w tych przepisach wymaga uwzględnienia w prowadzonych analizach uwarunkowań takich jak: elementy typowe dla danego użytkownika czy też wzorców zachowań. Bez wątpienia więc, ich zastosowanie będzie związane z przetwarzaniem szerokiego zakresu istotnych danych osobowych użytkowników usług płatniczych.

Za inny, praktyczny przykład pokazujący, w jaki sposób przenikać się mogą zagadnienia z zakresu usług zaufania oraz danych osobowych, mogą posłużyć wątpliwości dotyczące ujawniania numeru PESELw związku z korzystaniem z kwalifikowanego podpisu elektronicznego. Prezes Urzędu Ochrony Danych Osobowych („PUODO") zwrócił uwagę, że o ile zasadne jest użycie numeru PESEL w procesie weryfikacji osoby wnioskującej o wydanie certyfikatu kwalifikowanego podpisu elektronicznego, to co najmniej wątpliwe jest ujawnienie tego numeru innym osobom jako konsekwencja użycia podpisu. Zdaniem PUODO, wykorzystanie numeru PESEL w kwalifikowanym podpisie elektronicznym nie jest bowiem wymogiem stawianym przez eIDAS, który w załączniku nr I wskazuje jedynie, że kwalifikowany certyfikat powinien zawierać m.in. kod identyfikacyjny certyfikatu, który musi być niepowtarzalny. Dodatkowo PUODO wskazuje, że ujawnianie numeru PESEL na szeroką skalę może ułatwiać dokonywanie kradzieży tożsamości[11].

7.7
Identyfikacja i weryfikacja w rozumieniu przepisów AML

Identyfikacja i weryfikacja klienta (a także beneficjenta rzeczywistego i osoby upoważnionej do działania w imieniu klienta) to środki bezpieczeństwa finansowego, stanowiące podstawowy element całego systemu przeciwdziałania praniu pieniędzy i finansowaniu terroryzmu. Mają one na celu dokonanie oceny narażenia instytucji obowiązanej (m.in.: banków, instytucji pożyczkowych, krajowych instytucji płatniczych) na wykorzystanie jej w procederze prania pieniędzy i finansowania terroryzmu oraz rozpoznanie ryzyka związanego ze stosunkami gospodarczymi i transakcjami okazjonalnymi, realizowanymi przez instytucję obowiązaną. Obowiązki w tym zakresie uregulowane zostały w szczególności w dyrektywie Parlamentu Europejskiego i Rady (UE) 2018/843 z dnia 30 maja 2018 r. zmieniającej dyrektywę (UE) 2015/849 w sprawie zapobiegania wykorzystywaniu systemu finansowego do prania pieniędzy lub finansowania terroryzmu oraz, w implementującej ją do prawa polskiego, ustawie z dnia 1 marca 2018 r. o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu („uAML").

W rozumieniu przepisów uAML, identyfikacja obejmuje proces ustalenia przez instytucję obowiązaną wskazanych w ustawie danych klienta (a także beneficjenta rzeczywistego i osoby upoważnionej do działania w imieniu klienta). W przypadku klienta będącego osobą fizyczną są to m.in.: imię i nazwisko, obywatelstwo, numer PESEL, a także seria i numer dokumentu stwierdzającego tożsamość. Weryfikacja polega zaś na potwierdzeniu ustalonych danych identyfikacyjnych klienta (a także beneficjenta rzeczywistego i osoby upoważnionej do działania w imieniu klienta) na podstawie: dokumentu stwier-

11. *zob. wystąpienie Prezesa Urzędu Ochrony Danych Osobowych do Ministra Cyfryzacji z 14.06.2019 r., ZSPU.023.97.2019.PM.*

dzającego tożsamość osoby fizycznej, dokumentu zawierającego aktualne dane z wyciągu z właściwego rejestru lub innych dokumentów, danych lub informacji pochodzących z wiarygodnego i niezależnego źródła (art. 37 uAML).

W praktyce weryfikacja danych klienta może odbywać się na wiele sposobów. Jednym z nich jest wykorzystanie kanałów zdalnych. Zarówno Generalny Inspektor Informacji Finansowej („GIIF"), jak i Komisja Nadzoru Finansowego ("KNF") zwróciły uwagę na fakt, że podczas nawiązywania stosunków gospodarczych lub przeprowadzania transakcji okazjonalnej, bez fizycznej obecności klienta, mogą się pojawić wątpliwości co do zakresu środków, jakich instytucja obowiązana może użyć w celu dokonania weryfikacji. Jako najbezpieczniejszą metodę wskazano środki identyfikacji elektronicznej określone w eIDAS, w tym kwalifikowany podpis elektroniczny[12]. Zgodnie z zaleceniami GIIF,w przypadku braku możliwości zastosowania takich metod, instytucja obowiązana powinna rozważyć zastosowanie wzmożonych środków bezpieczeństwa finansowego. Ocena, czy w danym przypadku występuje wyższe ryzyko prania pieniędzy lub finansowania terroryzmu, zgodnie z art. 33 uAML, ostatecznie spoczywa jednak zawsze na instytucji obowiązanej, która rozpoznaje ryzyko prania pieniędzy oraz finansowania terroryzmu, związane z danym stosunkiem gospodarczym lub transakcją okazjonalną oraz ocenia poziom rozpoznanego ryzyka. Instytucja obowiązana sama musi ustalić zatem, jakie: dokumenty, dane oraz informacje wykorzysta w celu weryfikacji tożsamości klienta[13]. KNF, w tym zakresie, wskazała na możliwość użycia w tym celu wideoweryfikacji przez banki oraz oddziały instytucji kredytowych. Muszą one jednak być zgodne ze standardami Rekomendacji D KNF dotyczącej zarządzania obszarami technologii informacyjnej i bezpieczeństwa środowiska teleinformatycznego w bankach oraz spełniać inne wymogi (zob. rozdział 5.11 Przewodnika).

Nad rozszerzeniem metod przeprowadzania identyfikacji klientów na potrzeby AML z wykorzystaniem środków cyfrowych pracuje również Financial Action Task Force („FATF"). W wydanych w marcu 2020 roku przez FATF wytycznych wskazano, że identyfikacja i weryfikacja klienta w oparciu o systemy identyfikacji cyfrowej, zawiera się w wymogu stosowania przez instytucje obowiązane danych lub informacji pochodzących z wiarygodnych i niezależnych źródeł. System identyfikacji cyfrowej wykorzystywany do prowadzenia costumer due diligance powinien przy tym opierać się na: technologii, odpowiednim zarządzaniu, procesach i procedurach, które zapewniają należyty poziom pewności, że system daje dokładne wyniki i adresuje ryzyka, takie jak adekwatne zabezpieczenie danych osobowych czy ochrona przed cyberatakami[14].

12.. *zob. wytyczne Generalnego Inspektora Informacji Finansowej w sprawie identyfikacji klienta instytucji obowiązanej i weryfikacji jego tożsamości w sytuacji braku jego fizycznej obecności, 22.08.2018 r.*
13. *zob. komunikat nr 4 w sprawie korekty komunikatu Generalnego Inspektora Informacji Finansowej z dnia 22 sierpnia 2018 r. w sprawie identyfikacji klienta instytucji obowiązanej i weryfikacji jego tożsamości, 18.04.2019 r.*
14. *zob. FATF, Guidance On Digital Identity, March 2020.*

ROZDZIAŁ 8.0

IDENTYFIKACJA I UWIERZYTELNIENIE – STAN OBECNY W POLSCE

8.1

Stan obecny sektora finansowego

W ciągu ostatnich lat bankowość elektroniczna stała się standardem, który jest stałym oczekiwaniem klientów. Potrzebują oni nie tylko zdalnej możliwości zarządzania finansami, ale przede wszystkim wygodnego i prostego w użyciu interfejsu, który spełni ich oczekiwania. Wraz z wejściem w życie rozporządzenia o ochronie danych osobowych (RODO, ang. General Data Protection Regulation, GDPR) elementem niezwykle istotnym dla użytkowników końcowych stało się bezpieczeństwo. Funkcjonalność ta była zawsze oczekiwana przez użytkowników, jednak wizja znaczących kar finansowych, które mogą zostać nałożone na organizacje niezapewniające odpowiedniego poziomu zabezpieczeń sprawił, że bezpieczeństwo stało się elementem niemal krytycznym. Ogólny obraz bankowości elektronicznej nie uległ znacznej zmianie – w dalszym ciągu aktualny jest podział na kanały dostępu oraz segmentację klientów. W dalszym ciągu zmienia się perspektywa klientów korporacyjnych, którzy dostrzegli łatwość wykorzystania kanałów bankowości elektronicznej i również chcą korzystać z ich benefitów. Zauważalna jest zmiana metod zarządzania rachunkiem firmowym oraz wykorzystywanych w tym celu interfejsów i kanałów dostępu. Dotychczasowe mechanizmy komunikacji klienta korporacyjnego z bankami niejednokrotnie są uznawane za przestarzałe i migrowane do bankowości elektronicznej. Z perspektywy kanałów dostępu, przeszły one w ostatnich latach znaczną metamorfozę, i to nie tylko ze względu na wejście w życie dyrektywy PSD2 (ang. Payment Services Directive 2, Dyrektywa Parlamentu Europejskiego i Rady (UE) 2015/2366 z dnia 25 listopada 2015 r. w sprawie usług płatniczych w ramach rynku wewnętrznego), ale również ze względu na rosnącą popularność wykorzystywania bankowości mobilnej.

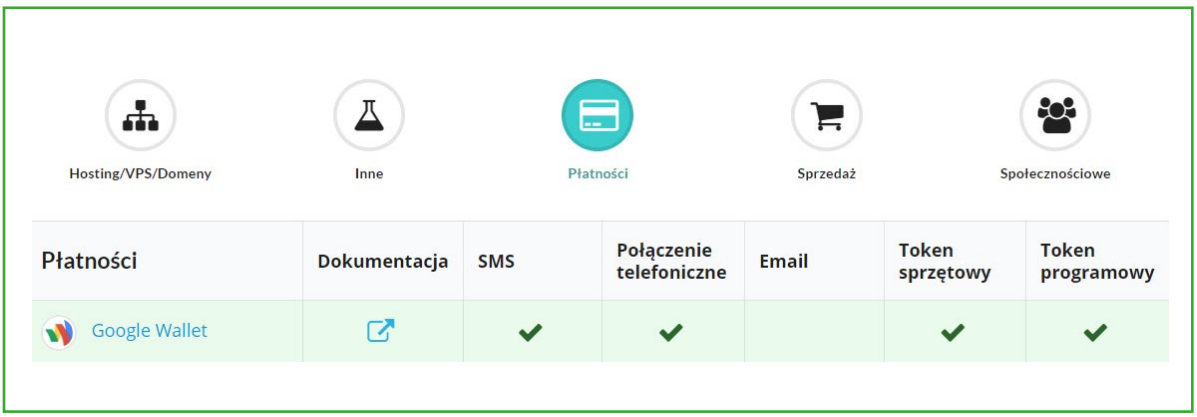
Zgodnie z raportem NetB@nk za II kwartał 2019 opublikowanym przez ZBP, liczba aktywnych klientów indywidualnych (czyli takich, którzy przynajmniej raz w miesiącu logują się do bankowości elektronicznej) bankowości internetowej wzrosła o 3,5% osiągając poziom ponad 18 mln. Liczba rachunków klientów indywidualnych z dostępem do bankowości internetowej przekroczyła 36,6 mln. Analogicznie, dla bankowości mobilnej liczba aktywnych klientów indywidualnych wzrosła o 5,5% osiągając poziom prawie 9,5 mln. W skali roku, liczba aktywnych użytkowników bankowości internetowej wzrosła o niecałe 8%, natomiast liczba aktywnych użytkowników bankowości mobilnej wzrosła o ponad 30%. Wartości te nie tylko potwierdzają, że klienci preferują wygodę oraz stały dostęp do swoich rachunków i finansów, ale także definiują dalszy kierunek zmian w bankowości elektronicznej. Ciągle najpopularniejszą formą dostępu do rachunku jest bankowość internetowa, jednak rosnąca popularność technologii mobilnych, a co za tym idzie, wzrost zainteresowania bankowością mobilną.

Wejście w życie dyrektywy PSD2 wprowadziło znaczne zmiany w zakresie identyfikacji i uwierzytelniania użytkowników bankowości elektronicznej, a w szczególności bankowości internetowej. Dotychczasowe rozwiązania najczęściej opierały się na wykorzystaniu indywidualnego dla klienta identyfikatora oraz statycznego hasła, które w zależności od organizacji musiało spełniać pewne założenia dotyczące złożoności. Warto również zaznaczyć, że w bankowości elektronicznej, hasło nie jest już najczęściej wprowadzane w postaci hasła maskowanego i w tym przypadku dość dużo się zmieniło na przestrzeni

ostatnich lat. Proces uwierzytelniania użytkowników bankowości korporacyjnej zwykle różnił się od bankowości indywidualnej i najczęściej wymagał, poza nazwą użytkownika i hasłem, podania drugiego składnika uwierzytelniającego (najczęściej kodu wygenerowanego na dedykowanym urządzeniu – tokenie sprzętowym, lub innego rodzaju hasła jednorazowego). Dyrektywa PSD2 wymaga wprowadzenia dodatkowych mechanizmów uwierzytelniających, które dotychczas były domeną klientów korporacyjnych, także dla klientów indywidualnych. Wynikiem jest zmiana procesu uwierzytelniania i wprowadzenie dodatkowych wymagań, które muszą zostać spełnione, aby użytkownik uzyskał dostęp do danych finansowych oraz historii transakcji.

Wykorzystanie dwuskładnikowego uwierzytelniania (ang. Two Factor Authentication, 2FA) staje się powoli standardem nie tylko w obszarze bankowości, ale wszystkich usług elektronicznych. Osoby, którym zależy na zapewnieniu wyższego poziomu bezpieczeństwa podczas dostępu do konta i wykorzystaniu dwuskładnikowego uwierzytelniania mogą skorzystać z popularnych platform przedstawiających listę stron z określeniem, czy i w jakim zakresie obsługują 2FA, przykładowo https://dwa-skladniki.pl/. W ramach drugiego składnika uwierzytelniającego, na wspomnianej stronie uwzględnione zostały obecnie najpopularniejsze rozwiązania: SMS, połączenie telefoniczne, email, token sprzętowy oraz token programowy.

RYSUNEK 16. Przykład wykorzystania dwuskładnikowego uwierzytelniania dla platformy Google Wallet[15].



W zakresie bankowości elektronicznej, nie uległo zmianie wykorzystanie drugiego składnika na potrzeby realizacji polityki autoryzacyjnej. W celu potwierdzenia, że wykonanie konkretnej, potencjalnie wrażliwej operacji zostało zlecone przez danego użytkownika. Najczęściej spotykaną sytuacją jest wysłanie przez bank kodu SMS do użytkownika w celu potwierdzenia zlecenia przelewu na rachunek nienależący do klienta. W takiej sytuacji klient jest proszony o dodatkowe potwierdzenie operacji poprzez przepisanie otrzymanego w wiadomości SMS kodu. Warto zaznaczyć, że rosnącą popularność zdobywa obecnie tzw. autoryzacja mobilna, która przeznaczona jest dla użytkowników posiadających smartfony i realizowana najczęściej w jeden z dwóch sposobów. Pierwszy polega na skorzystaniu z dedykowanej aplikacji instalowanej na telefonie lub komponentu zainstalowanej bankowej aplikacji mobilnej, która pozwala na wygenerowaniu kodu autory-

Przykład wiadomości push dla systemu operacyjnego iOS[16].

15. *Źródło: https://dwa-skladniki.pl/.*
16. *Źródło: https://www.mbank.pl/grafiki/inne/aktualne-grafiki2/17.jpg*

zacyjnego (token programowy). Drugi sposób to wykorzystanie tzw. powiadomień push (ang. push notifications) pozwalających na potwierdzenie operacji na telefonie poprzez otworzenie wyświetlonego komunikatu, który następnie przekierowuje użytkownika do aplikacji banku.

Użytkownicy dążą do uzyskania pełnej swobody podczas korzystania z usług elektronicznych i starają się unikać zapamiętywania wielu złożonych haseł do różnych serwisów. W związku z tym, coraz większą popularność zdobywają rozwiązania zintegrowane, które dają użytkownikowi możliwość jednorazowego zalogowania się do usługi i uzyskania dostępu do usług powiązanych. W środowiskach biurowych powszechnie wykorzystywane są rozwiązania typu single sign-on (SSO), natomiast w środowisku internetowym coraz popularniejsze stają się otwarte standardy autoryzujące. Najczęściej spotykanym obecnie standardem, wykorzystywanym przez największe światowe organizacje (np.: Amazon, Google, Microsoft, Facebook), jest OAuth, który polegając na zaufaniu do organizacji, gdzie użytkownik może już być zalogowany, pozwala na wykorzystanie tej informacji w innych serwisach i uzyskanie do nich dostępu.

Z perspektywy użytkownika bankowości elektronicznej, ostatnie lata przyniosły liczne zmiany w zakresie identyfikacji i uwierzytelniania, jednak w zdecydowanej większości, zmiany te były ukierunkowane na elementy bezpieczeństwa. Mechanizmy uzyskiwania dostępu nie zmieniły się znacząco. W dalszym ciągu, gdy wykorzystywany jest drugi składnik uwierzytelniający, najczęściej jest to kod przesłany w wiadomości SMS. Banki stosują spójne metody autoryzacji i uwierzytelnienia, wykorzystując bardzo zbliżone rozwiązania biznesowe i techniczne. Wprowadzenie dyrektywy PSD2 wymusza zapewnienie pewnego stopnia integracji pomiędzy bankami oraz definiuje określone zasady komunikacji. Wykorzystując specjalne interfejsy dostępowe, użytkownik otrzymuje większą swobodę w realizacji przynajmniej podstawowych funkcji dostępnych dotychczas jedynie z poziomu bankowości elektronicznej. W dalszym ciągu nie jest dostępny uniwersalny identyfikator, który pozwalałby na wygodne i efektywne korzystanie z bankowości elektronicznej różnych banków. Niezależnie jednak od wymagań wprowadzanych przez dyrektywę PSD2, rozwijane są dedykowane miejsca (huby), gdzie użytkownik będzie miał łatwy dostęp do usług bankowych oraz administracyjnych.

8.2
Dyrektywa PSD2 i definicja SCA

W dniu 14 września 2019 r. weszło w życie Rozporządzenie Delegowane Komisji Europejskiej w zakresie regulacyjnych standardów technicznych (tzw. RTS) dotyczące między innymi silnego uwierzytelnienia klienta. Głównym powodem wdrożonych rozwiązań jest zwiększenie bezpieczeństwa korzystania z usług płatniczych oferowanych drogą elektroniczną i tym samym ograniczenie możliwości wystąpienia oszustw związanych z tymi usługami. Rozporządzenie wprowadziło konieczność stosowania procedur silnego uwierzytelnienia, czyli minimum dwuskładnikowego potwierdzania tożsamości klientów.

Opiera się ono na zastosowaniu co najmniej dwóch składników należących do 3 kategorii:

- **Kategoria „wiedza”** – to kod (np. PIN), hasło lub inny element, który jest i powinien być znany tylko klientowi - posiadaczowi danego instrumentu płatniczego lub bankowości internetowej,
- **Kategoria „posiadanie”** – to element, który dany użytkownik ma w posiadaniu (np. karta plastikowa, telefon z kartą SIM) i który może zostać użyty w trakcie dokonywania płatności lub korzystania z bankowości internetowej,
- **Kategoria „cecha klienta”** – to specyficzna dla danego klienta cecha, którą tylko on dysponuje i która go jednoznacznie wyróżnia. Dobrym przykładem jest biometria w postaci np. odcisku palca, tęczówki oka czy układu żył.

Stosowanie procedur silnego uwierzytelnienia jest wymagane (nie licząc wyłączeń) przy dokonywaniu płatności w terminalach płatniczych (POS), płatnościach za zakupy w Internecie (e-commerce, m-commerce) oraz logowaniu i korzystaniu z bankowości internetowej czy mobilnej[17].

Niezwykle istotną cechą silnego uwierzytelnienia, która musi być spełniona jest to, aby poszczególne wyżej wymienione kategorie były od siebie niezależne w tym sensie, że naruszenie jednej z nich nie osłabia wiarygodności pozostałych. Należy dodatkowo pamiętać, że uwierzytelnianie musi być zaprojektowane w sposób zapewniający ochronę poufności danych uwierzytelniających.

Dostawca powinien wymagać silnego uwierzytelnienia klienta, co najmniej przy dokonywaniu przez użytkownika następujących czynności:

- uzyskiwaniu dostępu do rachunku płatniczego online (np. przez kanały bankowości internetowej lub mobilnej), o ile wyświetlana historia jest dłuższa niż 90 dni;
- inicjowaniu elektronicznej transakcji płatniczej do odbiorcy spoza białej listy;
- przeprowadzaniu za pomocą kanału zdalnego czynności, która może wiązać się z ryzykiem oszustwa płatniczego lub innych nadużyć;

Bardzo ważny jest także wymóg dynamicznego linkowania drugiego faktora z danymi transakcji (z transakcją).

Wdrożenie przez Unię Europejską nowej dyrektywy PSD2 wprowadza nie tylko wymóg silnego uwierzytelnienia, ale również możliwość oferowania nowych produktów i usług związanych nie tylko z rynkiem usług płatniczych. Zarówno podmioty będące obecne na tym rynku, takie jak banki, Spółdzielcze Kasy Oszczędnościowo-Kredytowe czy oddziały zagranicznych instytucji kredytowych, ale także nowe rodzaje podmiotów (dostawcy będący stroną trzecią, Third Party Providers, TPP) będą mogły wykorzystać możliwość oferowania nowych usług budowanych w oparciu o PSD2, akty wykonawcze (w tym Regulacyjne Standardy Techniczne – RTS) i akty prawa krajowego. Nowymi kategoriami usług są:

- Account Information Service (AIS) – usługa dostępu do informacji o rachunku, zdefiniowana w art. 67 PSD2;
- Payment Initiation Service (PIS) – usługa inicjowania transakcji płatniczej, zdefiniowana w art. 66 PSD2;

Confirmation of the Availability of Funds (CAF) – usługa potwierdzania dostępności na rachunku płatniczym płatnika kwoty niezbędnej do wykonania transakcji płatniczej, zdefiniowana w art. 65 PSD2[18].

W celu ułatwienia komunikacji i rozwoju innowacyjnych usług na rynku polskim ZBP wraz z przedstawicielami podmiotów pracujących razem z ZBP stworzyli wspólnie polski standard API, który odpowiada na wyzwania stawiane przez Dyrektywę. Standard ten dostępny jest na stronie projektu PolishAPI pod adresem https://polishapi.org/#docs.

17. *Por. https://www.zbp.pl/aktualnosci/wydarzenia/Silne-uwierzytelnianie-juz-od-14-wrzesnia.*

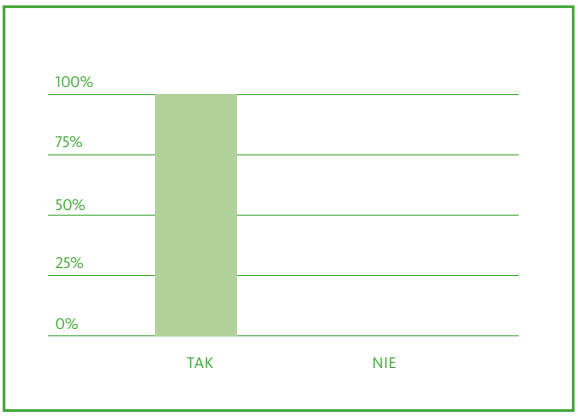
18. *Por. PolishAPI. Specyfikacja interfejsu na potrzeby usług świadczonych przez strony trzecie w oparciu o dostęp do rachunków płatniczych, 2 grudnia 2019, wersja 3.0. https://polishapi.org/#docs.*

8.3
SCA w Polsce w świetle NIST SP 800-63

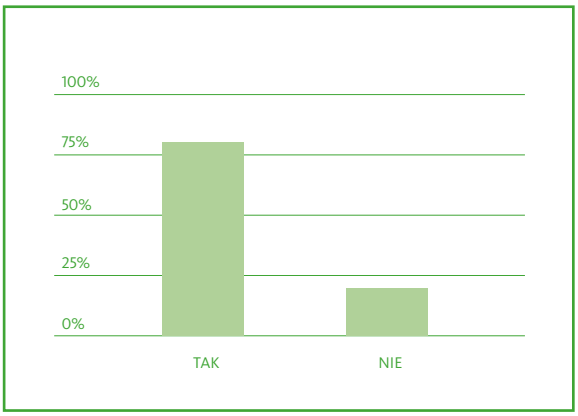
Porównanie wykorzystywanych mechanizmów implementujących SCA do najlepszych praktyk w zakresie identyfikacji i uwierzytelniania użytkowników w systemach teleinformatycznych, zostało przeprowadzone zgodnie z wymaganiami przedstawionymi w standardzie NIST SP 800-63 opublikowanym przez Narodowy Instytut Standaryzacji i Technologii (NIST, National Institute of Standards and Technology). Szczegółowy opis standardu został przedstawiony w rozdziale 4.6. Przeanalizowaliśmy mechanizmy implementujące SCA w 22 bankach w Polsce. Poniżej zostały przedstawione wyniki badania.

Dla każdego mechanizmu identyfikacji i uwierzytelnienia sprawdziliśmy, czy korzysta z bezpiecznego kanału komunikacji SSL/TLS oraz, czy wykorzystuje dodatkowy mechanizm HSTS (ang. HTTP Strict Transport Security). Wyniki prezentują poniższe tabele:

RYSUNEK 17. Wykorzystanie bezpiecznego kanału komunikacji SSL/TLS przy logowaniu



RYSUNEK 18. Wykorzystanie dodatkowego mechanizmu HSTS przy logowaniu



8.4
Zapamiętany sekret

Zapamiętany sekret (ang. memorized secret), jest to poufna wartość, która została zapamiętana przez użytkownika (zwykle hasło lub PIN). Zgodnie z rekomendacjami standardu NIST, sekret musi składać się przynajmniej z 8 znaków, a w przypadku gdy został losowo wygenerowany przez zaufaną stronę uwierzytelniającą – przynajmniej 6 znaków. NIST dopuszcza sytuację, w której sekret będzie się składał z pojedynczej grupy znaków, na przykład przy wykorzystaniu samych liter lub cyfr. Koniczna jest weryfikacja sekretu wprowadzanego przez użytkownika z listą niedozwolonych ciągów znaków (np. proste hasła, które mogą zostać łatwo odgadnięte przez potencjalnego atakującego). Zalecane jest także, aby maksymalna długość hasła była nie mniejsza, niż 64 znaki oraz aby akceptowalne były wszystkie drukowalne znaki ASCII[19]. Zgodnie z rekomendacjami standardu NIST, zabronione jest wykorzystywanie przez użytkowników podpowiedzi do haseł (tzw. hint) oraz niedozwolone jest wymaganie podawania odpowiedzi na pytania pomocnicze (np. „Jakie imię miał twój pierwszy pies?"). Nie jest zalecane określanie dodatkowych wymagań dotyczących złożoności haseł (np. różne grupy znaków: litery, cyfry, znaki specjalne), ani wymuszanie okresowej zmiany hasła (dopuszczalne jedynie w określonych wypadkach). Hasła użytkowników muszą być przesyłane przy pomocy uwierzytelnionego i chronionego kanału, który uniemożliwia podsłuchanie lub zmodyfikowanie przesyłanej wiadomości. Dodatkowo, standard NIST definiuje restrykcyjne

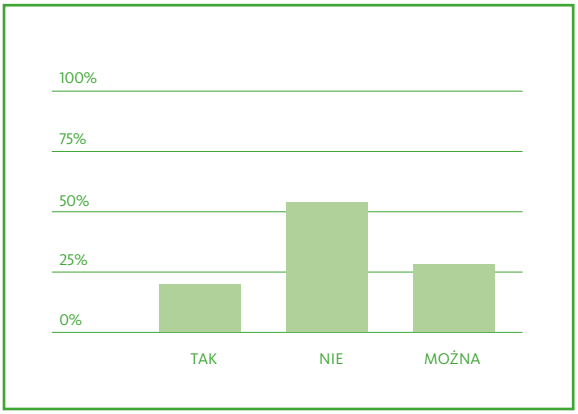
ą zostać spełnione podczas przechowywania sekretu

19. *https://pl.wikipedia.org/wiki/ASCII#Znaki_drukowalne*

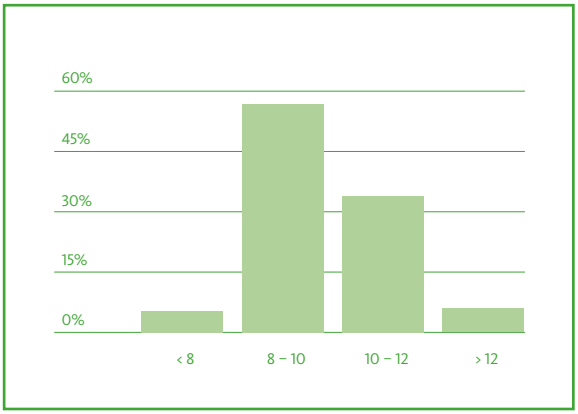
– zarówna w przypadku hasła, jak i kodu PIN.

W ramach analizy identyfikacji i uwierzytelniania w bankach zostały przeanalizowane następujące aspekty logowania:
1. Czy w celu uwierzytelniania bank wykorzystuje hasło maskowane?;
2. Jaka jest długość hasła akceptowalna przez bank?;
3. Czy bank wykorzystuje „obrazek bezpieczeństwa" przy procesie logowania?;
4. Czy bank wymaga dodatkowej informacji (poza dwuskładnikowym uwierzytelnieniem), np. numeru PESEL?

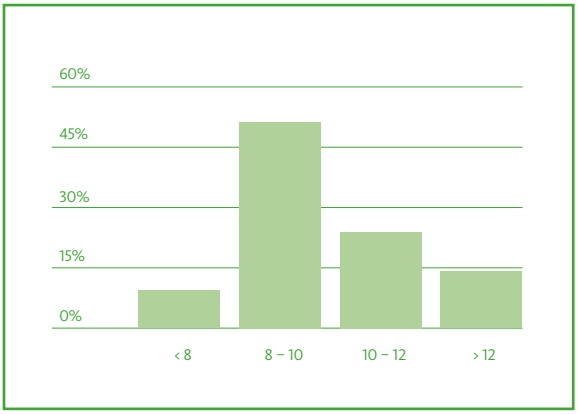
RYSUNEK 19. Wykorzystanie hasła maskowanego podczas logowania



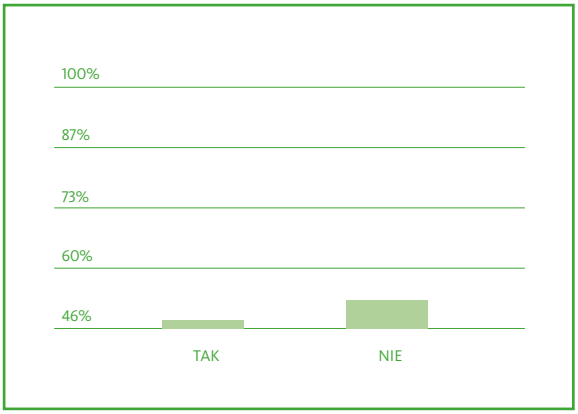
RYSUNEK 20. Wymagana przez banki minimalna długość hasła



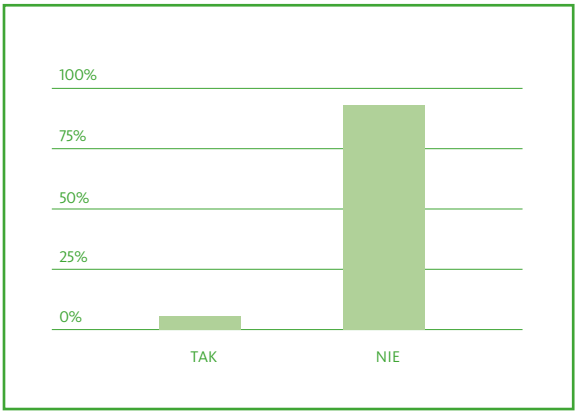
RYSUNEK 21. Wymagana przez banki maksymalna długość hasła



RYSUNEK 22. Wykorzystanie obrazka bezpieczeństwa podczas logowania

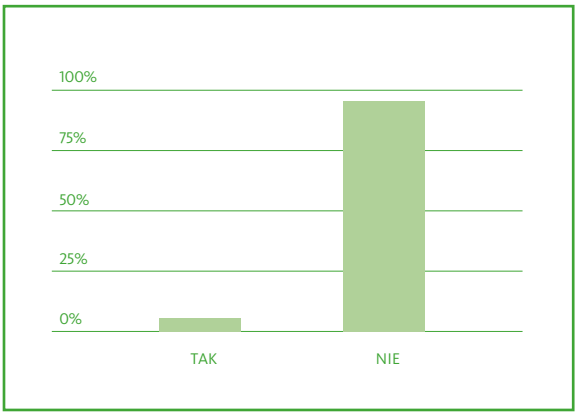


RYSUNEK 23. Wykorzystanie dodatkowego mechanizmu podczas logowania

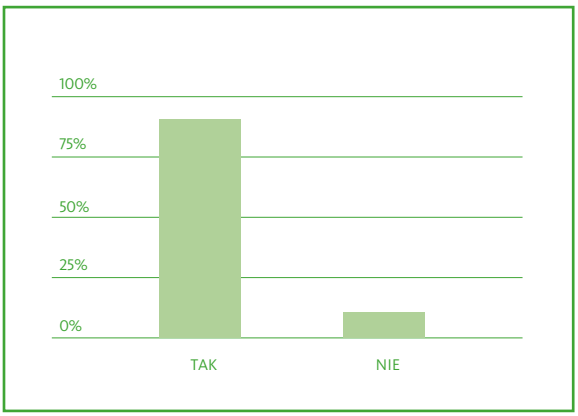


8.0

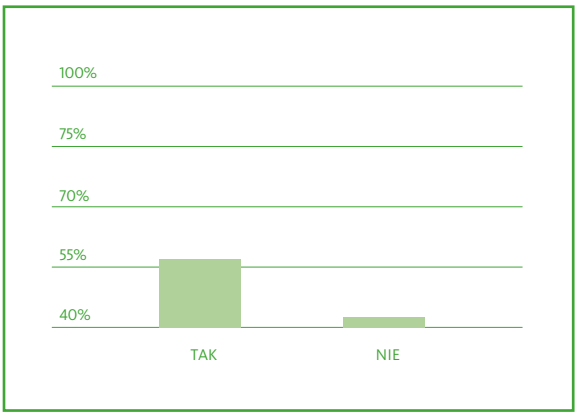
RYSUNEK 24. Wykorzystanie listy kodów przez banki podczas procesu logowania



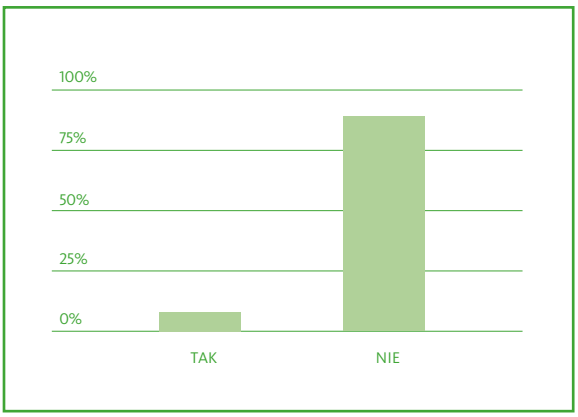
RYSUNEK 25. Wykorzystanie kodów przesyłanych za pomocą SMS jako jednego z czynników SCA



RYSUNEK 26. Wykorzystanie autoryzacji w aplikacji na urządzeniu mobilnym, jako jednego z czynników SCA



RYSUNEK 27. Wykorzystanie tokenu sprzętowego jako jednego z czynników SCA



Lista kodów

Lista kodów (Look-Up Secrets) jest to fizyczny lub elektroniczny zbiór sekretów wymieniony pomiędzy użytkownikiem, a stroną weryfikującą. Każdy kod z listy kodów może być wykorzystany tylko jeden raz. Po stronie banku sekret musi być przechowywany w formie hasza z solą przy użyciu powszechnie akceptowalnej funkcji haszującej. Sekrety wprowadzane prze użytkowników muszą być przesyłane przy pomocy uwierzytelnionego, chronionego kanału, który uniemożliwia podsłuchanie oraz modyfikację przesyłanej wiadomości.

8.6
Kody SMS/aplikacja mobilna

Wykorzystanie wiadomości SMS lub połączeń głosowych jest uważane za niewystarczające i zostanie wycofane w kolejnych edycjach dokumentu NIST. Strona uwierzytelniająca może korzystać z wiadomości typu „push", jeśli użytkownik korzysta z urządzeń, które to rozwiązanie wspierają. Jeśli proces uwierzytelniania nie zostanie zakończony w ciągu 5 minut, powinien zostać uznany za nieprawidłowy.

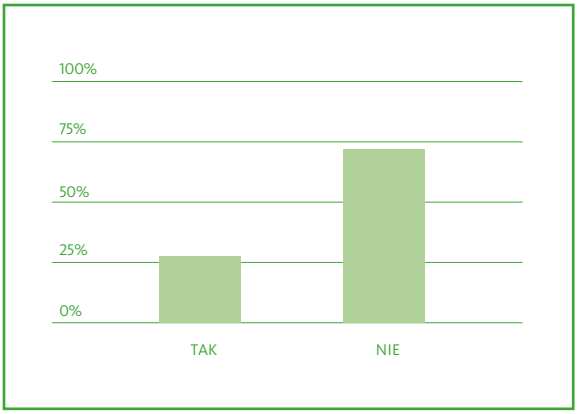
8.7
Tokeny sprzętowe

Dedykowane urządzenie, które pozwala na generowanie hasła jednorazowego. Dopuszczalne jest rozwiązanie, w którym wygenerowany kod składał się z 6 losowych cyfr. Każdy kod może być ważny nie dłużej niż 2 minuty.

8.8
Inne

Dodatkowym mechanizmem wykorzystywanym przez banki w celu podniesienia poziomu zabezpieczeń jest możliwość zapamiętania przeglądarki. Użytkownik podczas logowania ma możliwość dodania przeglądarki do zaufanych przeglądarek w swojej bankowości elektronicznej. Proces dodawania przeglądarki do przeglądarek

RYSUNEK 28. Zapamiętanie przeglądarki



zaufanych wymaga SCA ze strony klienta. Dzięki zastosowaniu tego podejścia banki przez kolejne 90 dni po tej operacji nie wymagają od klientów SCA dla celów podczas logowania do bankowości elektronicznej.

8.9
Identyfikacja i uwierzytelnienie jako usługa bankowa

Poziom bezpieczeństwa i zaufania do banków w Polsce oraz zaawansowane i innowacyjne rozwiązania w obszarze identyfikacji i uwierzytelniania klientów w kanałach elektronicznych rozwinęły rynek na usługi identyfikacji klienta przez bank. Głównym beneficjentem tych usług jest w tej chwili administracja państwowa jednak widać rosnące zainteresowanie ze strony firm komercyjnych.

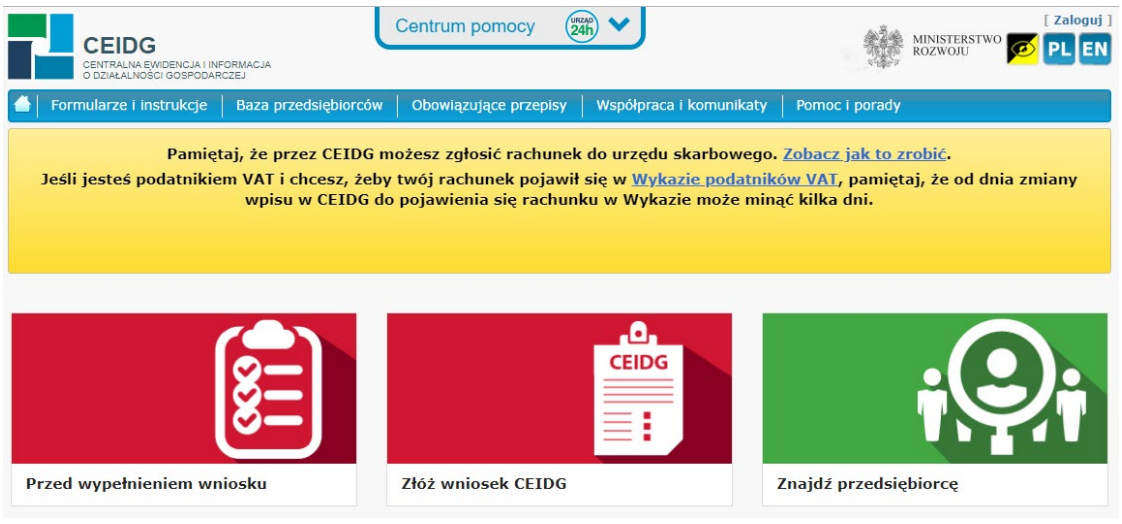
Przez ostatnie lata najbardziej popularną formą uwierzytelniania w elektronicznych usługach administracji publicznej za pomocą bankowości elektronicznej było korzystanie z Profilu Zaufanego, a dokładnie podpisu potwierdzonego profilem zaufanym. Profil zaufany pobiera informację dotyczącą tożsamości danego obywatela od banku po tym, gdy użytkownik potwierdził swoją tożsamość w kanale bankowości elektronicznej. Profil Zaufany, poza swoimi pewnymi wadami, jest przede wszystkim narzędziem dedykowanym dla administracji publicznej. Brakuje nadal w pełni funkcjonującego narzędzia inteoperacyjnego i niesilosowego, za pomocą którego użytkownik mógłby się uwierzytelniać we wszystkich kanałach elektronicznych. Rozporządzenie eIDAS, które szerzej zostało omówione w rozdziale 4.1, stworzyło podwaliny prawne, aby tego typu rozwiązania funkcjonowały nie tylko na rynku polskim, ale w całej Europie w ustandaryzowany sposób.

W tej chwili w Polsce istnieją już pierwsze rozwiązania, które w przyszłości mogą stanowić tego typu narzędzie wykorzystywane powszechnie do celów identyfikacji i uwierzytelniania. Jednym z nich jest węzeł krajowy stworzony zgodnie z wymaganiami eIDAS. Docelowa architektura węzła krajowego została zaprezentowana na poniższym rysunku. Kolejnymi rozwiązaniami są rozwiązania komercyjne czyli usługa mojeID proponowana przez KIR oraz usługa eID bankowego proponowana przez Blue Media. Warto podkreślić, że już wcześniej z pośrednictwem Blue Media można było potwierdzać telefony prepaid w bankach ING oraz Millennium, która to usługa została zaproponowana po wejściu obowiązku rejestracji kart SIM, i podobnie kluczowe w usłudze było potwierdzenie danych przez bank, co zostało wprost wskazane w prawie telekomunikacyjnym jako jedna z możliwości.

RYSUNEK 29. Docelowa architektura węzła krajowego[20]

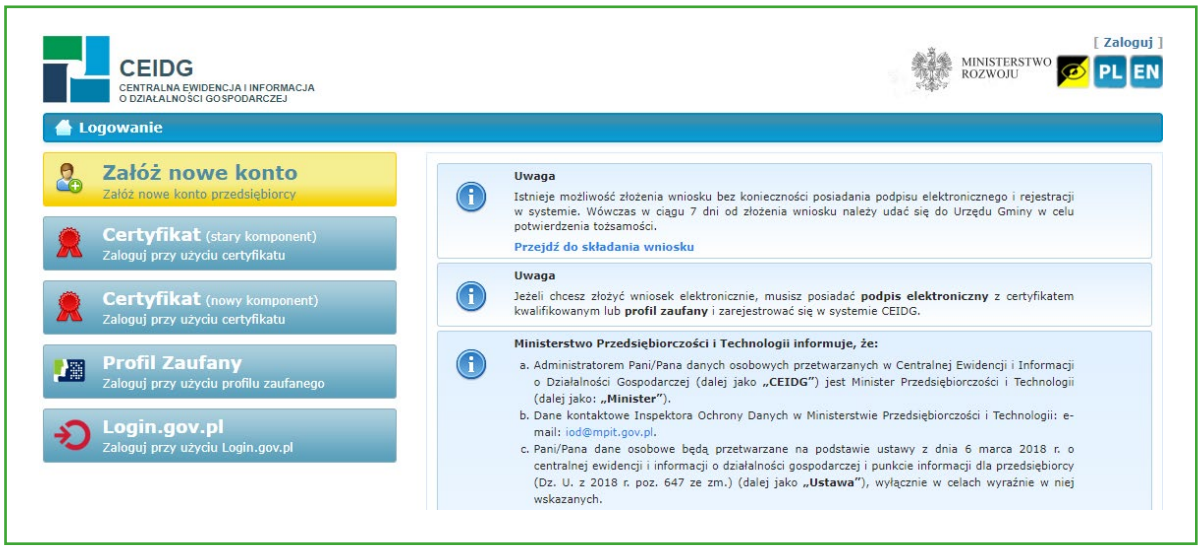
Jak wspomniano nie są to rozwiązania, które są powszechnie stosowane na rynku. Związane jest to przede wszystkim z dwiema przyczynami. Po pierwsze są to rozwiązania wdrożone niedawno. Węzeł Krajowy zaczął w pełni funkcjonować w sierpniu 2019 roku. Po drugie, rozwiązania te są powszechnie dostępne jedynie dla nielicznych użytkowników. Jako przykład niech posłuży próba zalogowania do CEIDG przez osobę fizyczną prowadzącą działalność gospodarczą. Poniższe wydruki z ekranów prezentują poszczególne kroki identyfikacji i uwierzytelnienia za pomocą Węzła Krajowego.

RYSUNEK 30. Krok 1 – Strona główna CEIDG. Wybieramy przycisk [Zaloguj]

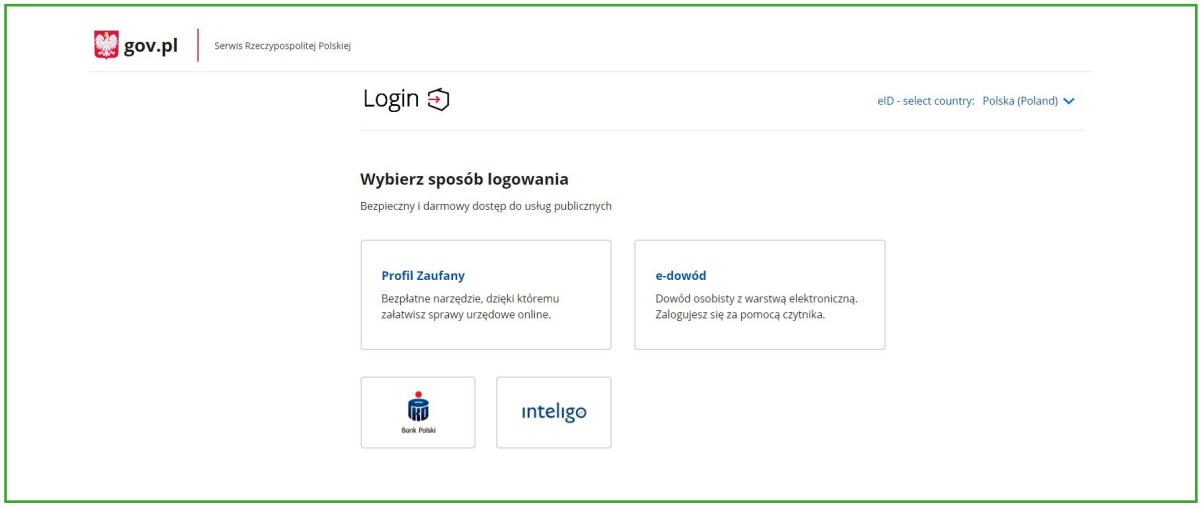


20. *https://www.gov.pl/web/cyfryzacja/budowa-krajowego-wezla-identyfikacji-elektronicznej.*

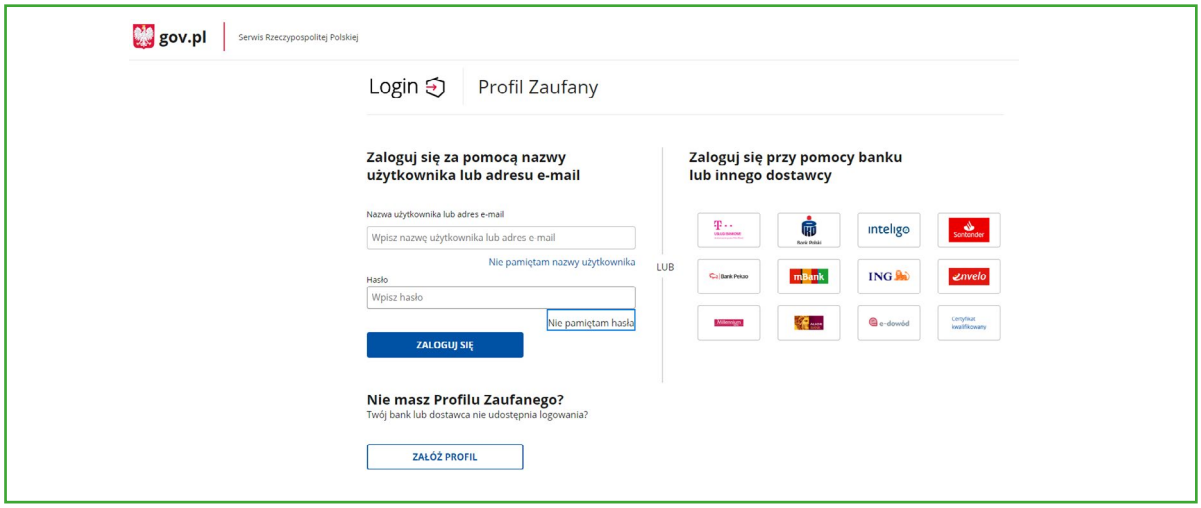
RYSUNEK 31. Krok 2 - Ekran logowania – wybieramy logowanie poprzez węzeł krajowy login.gov.pl



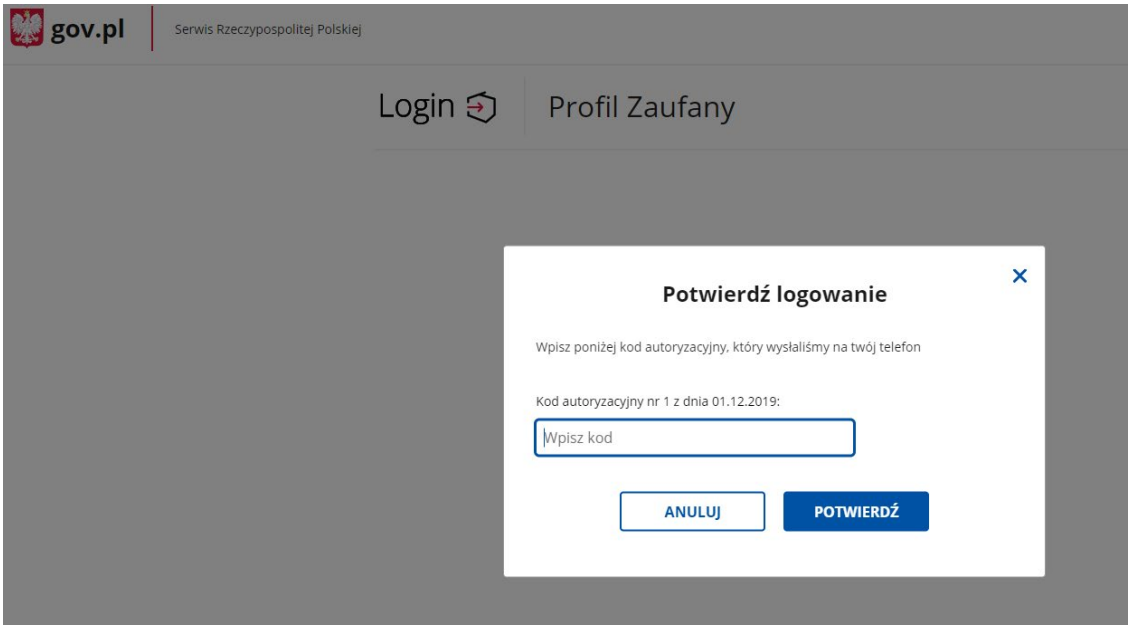
RYSUNEK 32. Krok 3 – Strona węzła krajowego. Zakładając, że nie jesteśmy klientem banków PKO BP ani Inteligo jesteśmy zmuszeni kliknąć Profil Zaufany



RYSUNEK 33. Krok 4 – wybieramy swój bank z listy (w tym PKO/Inteligo) i zostajemy przekierowani na jego stronę w celu wpisania loginu i hasła (Krok 5 i Krok 6) po czym zostajemy przekierowani z powrotem na stronę Profilu Zaufanego (alternatywnie korzystamy z założonego profilu zaufanego i używamy identyfikatora i hasła, podpisujemy się i potwierdzamy tożsamość podpisem kwalifikowanym, korzystamy z eDowodu lub z innego dostawcy tożsamości – envelo)



RYSUNEK 34. Krok 7 – Na stronie profilu zaufanego wpisujemy kod otrzymany przez wiadomość SMS z naszego banku



W kolejnym – ostatnim kroku 8 – jesteśmy przekierowani na stronę CEIDG. Jak widać z powyższego opisu węzeł krajowy jest rozwiązaniem, które wymaga jeszcze rozwinięcia niemniej jednak jest to niewątpliwie krok w dobrym kierunku.

8.10
Inne metody użycia danych bankowych

Metoda uwierzytelniania powszechnie używana w ecommerce to uwierzytelnienia na podstawie danych z przelewu bankowego. Przelew zawiera: imię, nazwisko (lub nazwę dla firm), adres oraz unikatowy numer rachunku bankowego.

W praktyce większość rachunków to rachunki posiadające jednego właściciela, a nawet w przypadku rachunku, do którego więcej niż jedna osoba ma dostęp jest mało prawdopodobne wykorzystanie tego rachunki w celach fraudowych. Dzięki temu w momencie, gdy klient zdalnie deklaruje kim jest oraz posiadanie rachunku bankowego, to zgodność danych z przelewu jest faktorem bardzo wysoce uwiarygadniającym podane dane i do wielu zastosowań wystarczającym, a jednocześnie wygodnym.

Wygoda jest zapewniana przez możliwość zlecenia przelewu w formule paybylink. Co ważne, przy stosowaniu tej metody zawsze pozostaje ślad jej użycia w historii rachunku bankowego (dane przelewu), a powszechnie wpisany jest tekst nawiązujący do charakteru transakcji w opisie przelewu (np. potwierdzenie tożsamości). Przyjętą kwotą takiego przelewu jest 1 złoty. Dzięki temu klient ma potwierdzenie wykonania takiej transakcji wprost w banku.

Dodatkowo Związek Banków Polskich prowadzi bazę, która pozwala odrzucić rachunki wcześniej założone na przelew, bez potwierdzonej face2face tożsamości. Dzięki temu metoda może być używana nie tylko na rynku ecommerce czy pożyczek, ale nawet do zakładania kont bankowych.

Ta metoda to także potwierdzenie numeru rachunku bankowego, co w wielu procesach biznesowych jest również ważne. Na rynku np. pożyczek nie tylko potwierdza się tożsamość osoby z użyciem tzw. przelewu weryfikacyjnego, ale także pozyskuje pewny numer rachunku bankowego, na który następuje wypłata pożyczki, tym samym pożyczka zostanie wypłacona (przy pozytywnej decyzji) wyłącznie na rachunek, którym może dysponować wnioskodawca.

Warto podkreślić, ze ta metoda może i jest używana samodzielnie, lub może być połączona z np. weryfikacją danych ze zdjęcia dokumentu tożsamości. Wtedy zgodność danych uwiarygadnia, że przedstawiony zdalnie dokument był oryginalny.

Analogiczny zestaw danych można pozyskać dzięki usłudze AIS PSD2. Imię i nazwisko są wprost wskazane w PSD2 jako dane, które są przekazywane (o ile są dostępne w bankowości elektronicznej, ale w praktyce w każdym banku są dostępne przez serwisy internetowe). Dostęp do historii rachunku / rachunków pozwala z kolei pozyskać dane stron transakcji dla historycznych przelewów. W wypadku użycia AIS nie mamy jednak do czynienia z „opisem przelewu", który pozwalał określić cel realizacji przelewu i jest łatwo dostępny dla właściciela rachunku. Nie ma pewności i standardów, jak historia takich transakcji będzie prezentowana klientom w bankach.

FinTaxLegal

Związek Banków Polskich

ZWIĄZEK BANKÓW POLSKICH
ul. Kruczkowskiego 8
00-380 Warszawa