



ZWIĄZEK BANKÓW POLSKICH



IDENTYFIKACJA I UWIERZYTELNIENIE W USŁUGACH ELEKTRONICZNYCH

Przewodnik

Forum Technologii Bankowych przy Związku Banków Polskich

Warszawa, 2013

Autorzy

Zespół redakcyjny:

Tomasz Mielnicki (przewodniczący), Franciszek Wołowski, Marek Grajek, Piotr Popis

Współautorzy:

Piotr Łuczak, Michał Tabor, Miłosz Brakoniecki

Pozostałe osoby, które wsparły merytorycznie tworzenie dokumentu:

Marek Wądołek, Bohdan Grzegorski, Beata Bińkowska-Artowicz, Teresa Kamińska, Paweł Domański

1	<u>WSTĘP</u>	6
2	<u>TERMINOLOGIA</u>	8
3	<u>SYNTEZA I ZALECENIA</u>	12
3.1	CO TO JEST IDENTYFIKACJA I UWIERZYTELNIENIE?	12
3.2	PROCESY ZWIĄZANE Z ELEKTRONICZNĄ TOŻSAMOŚCIĄ	13
3.3	POZIOMY WIARYGODNOŚCI	13
3.4	STRUKTURA WIARYGODNOŚCI UWIERZYTELNIENIA	15
3.5	WYBÓR MODELU	16
3.6	USŁUGI ZAUFANIA I ICH DOSTAWCY	19
3.7	UWIERZYTELNIENIE W SEKTORZE PUBLICZNYM I PRYWATNYM	20
3.8	UWIERZYTELNIENIE AUTONOMICZNE I SFEDEROWANE	22
3.9	UWIERZYTELNIENIE TRANSGRANICZNE	23
3.10	POLITYKI I PROCEDURY	24
4	<u>IDENTYFIKACJA I UWIERZYTELNIENIE W STANDARDACH</u>	25
4.1	PODPIS ELEKTRONICZNY	25
4.1.1	PODOBIENSTWA I RÓŻNICE MIĘDZY PODPISEM ELEKTRONICZNYM I TRADYCYJNYM (WŁASNORĘCZNYM)	26
4.1.2	RODZAJE PODPISU ELEKTRONICZNEGO WG DYREKTYWY 93/99/EC	28
4.1.3	RODZAJE PODPISU ELEKTRONICZNEGO WG PROJEKTU ROZPORZĄDZENIA EIDAS	29
4.2	STANDARZY ETSI I CWA	31
4.3	IDABC	34
4.4	STORK	42
4.5	ROZPORZĄDZENIE „EIDAS”	48
4.6	NORMA ISO 29115	51
4.6.1	STRUKTURA I POZIOMY WIARYGODNOŚCI UWIERZYTELNIENIA	51
4.6.2	FAZY W STRUKTURZE WIARYGODNOŚCI	54
4.6.3	WYMAGANIA ORGANIZACYJNE I PROCEDURALNE	58
4.6.4	WYMAGANIA I ŚRODKI STEROWANIA BEZPIECZEŃSTWEM	58
4.7	STANDARD NIST SP 800-53	60
5	<u>PRZEGLĄD KONCEPCJI UWIERZYTELNIENIA</u>	62
5.1	UWIERZYTELNIENIE KRYPTOGRAFICZNE	62

Identyfikacja i uwierzytelnianie w usługach elektronicznych

5.1.1	PROBLEM LOSOWOŚCI PRZY GENEROWANIU „HASEŁ JEDNORAZOWYCH”	62
5.1.2	MECHANIZMY UWIERZYTELNIENIA OPARTE O KRYPTOGRAFIĘ ASYMETRYCZNA	66
5.1.3	PODPIS SERWEROWY.....	68
5.1.4	DOWODY NIEZAPRZECZALNOŚCI	72
5.2	UWIERZYTELNIENIE BIOMETRYCZNE	73
5.2.1	POJĘCIA I DEFINICJE	73
5.2.2	WSTĘP DO BIOMETRII.....	74
5.2.3	BIOMETRIA JAKO METODA UWIERZYTELNIANIA	78
5.2.4	OBSZARY ZASTOSOWAŃ UWIERZYTELNIENIA BIOMETRYCZNEGO.....	79
5.3	UWIERZYTELNIENIE PROCEDURALNE	80
5.4	UWIERZYTELNIENIE OPARTE NA WIEDZY.....	81
5.5	UWIERZYTELNIENIE W OPARCIU O PORTALE SPOŁECZNOŚCIOWE	81
5.6	UWIERZYTELNIENIE NA PODSTAWIE ATRYBUTÓW	82
5.7	UWIERZYTELNIENIE Z ZACHOWANIEM PRYWATNOŚCI	82
6	<u>PRZEGLĄD ROZWIĄZAŃ TECHNICZNYCH.....</u>	86
6.1	KARTY ELEKTRONICZNE.....	86
6.1.1	RODZAJE KART ELEKTRONICZNYCH	86
6.1.2	KARTY DO KWALIFIKOWANEGO PODPISU ELEKTRONICZNEGO - SSCD	88
6.2	NARODOWE DOKUMENTY TOŻSAMOŚCI	91
6.3	HASŁA JEDNORAZOWE	91
6.4	CAP/DPA	93
6.5	UWIERZYTELNIENIE A CZYTNIKI KART ELEKTRONICZNYCH	94
6.5.1	RODZAJE CZYTNIKÓW	94
6.5.2	UWIERZYTELNIENIE TERMINAŁA	96
6.6	ZCENTRALIZOWANE SYSTEMY POTWIERDZANIA TOŻSAMOŚCI	100
7	<u>ASPEKTY PRAWNE.....</u>	102
7.1	PRZESTĘPSTWA PRZECIWKO TOŻSAMOŚCI	102
7.2	OCHRONA DANYCH OSOBOWYCH.....	103
7.3	IDENTYFIKACJA I UWIERZYTELNIENIE.....	106
7.3.1	UWIERZYTELNIENIE DOKUMENTU	107
7.3.2	UWIERZYTELNIENIE OSOBY	108
7.3.3	IDENTYFIKACJA.....	109
8	<u>IDENTYFIKACJA I UWIERZYTELNIENIE – STAN OBECNY W POLSCE.....</u>	111

Identyfikacja i uwierzytelnianie w usługach elektronicznych

8.1	PRAKTYKA SEKTORA FINANSOWEGO	111
8.2	DOSTĘPNE POWSZECHNE NARZĘDZIA IDENTYFIKACJI I UWIERZYTELNIENIA	112
8.2.1	CERTYFIKATY ELEKTRONICZNE	112
8.2.2	EPUAP	112
8.2.3	PROFIL ZAUFANY	113
8.3	KWESTIA NARODOWEGO IDENTYFIKATORA.....	114
9	<u>STUDIUM PRZYPADKÓW</u>	<u>116</u>
9.1	BANK ID (SZWECJA)	116
9.2	NEMID (DANIA).....	117
9.3	NIEMIECKI EID (NPA)	120
9.4	MOBILEID (FINLANDIA)	126
9.5	OPENID	128
10	<u>LITERATURA</u>	<u>130</u>
11	<u>ZAŁĄCZNIK - POLITYKA BEZPIECZEŃSTWA WG NIST SP 800-53</u>	<u>132</u>

1 Wstęp

Ostatnia dekada upłynęła na dynamicznym rozwoju usług świadczonych zdalnie i przenoszeniu różnych transakcji do świata wirtualnego, do Internetu. Tradycyjny model polegający na bezpośrednich kontaktach personalnych dostawcy i odbiorcy usługi, wymianie papierowych dokumentów, jest wypierany przez usługi realizowane drogą elektroniczną i w czasie rzeczywistym („on-line”). Wiele czynności wymaga obustronnej interakcji stron, co z kolei wymusza zastosowanie odpowiednich metod i technik zapewniających między innymi skuteczność, niezaprzeczalność, rozliczalność i wiarygodność transakcji.

Jednym z najistotniejszych elementów, jeśli nie najważniejszym, każdej zdalnej transakcji elektronicznej jest właściwe zidentyfikowanie stron oraz ich uwierzytelnienie, w sposób adekwatny (czyli z właściwym poziomem pewności) do realizowanej usługi. W zasadzie jest to coś zupełnie oczywistego, bo te elementy występują także w przypadku transakcji tradycyjnych. Jednak w świecie elektronicznym te pojęcia nabierają nowego wymiaru. Tematyka ta jest obecna już od wielu lat, jednak standaryzacja i normalizacja w tym zakresie postępuje z opóźnieniem w porównaniu z powstającymi nowymi technologiami i ich wdrożeniami. Tradycyjnie sektor bankowy stanowi awangardę w dziedzinie nowych rozwiązań identyfikacji i uwierzytelnienia. Niemniej obecnie w Polsce dostawcy usług elektronicznych zwykle polegają na własnych standardach i rozwiązaniach, budując własne „silosy” w zakresie zarządzania elektroniczną tożsamością swoich klientów – użytkowników e-usług. Skutkuje to stosowaniem modelu silosowego a w tego typu rozwiązaniach uwierzytelnienia nie mają wspólnej podstawy i są „uszyte” jedynie na potrzeby i na miarę danej organizacji i świadczonych przez nią usług. W takim modelu każdy z dostawców e-usług jest zarazem dostawcą tożsamości (ang. *Identity Provider*), a użytkownik zmuszony jest posiadać wiele tożsamości elektronicznych, wiele identyfikatorów elektronicznych i różnych środków uwierzytelnienia. Dotyczy to zarówno sektora komercyjnego, jak i publicznego.

Ważnym impulsem zmian w podejściu do identyfikacji i uwierzytelnienia były i są rozwiązania proponowane przez rządy państw. Poruszając się w kontekście europejskim, pierwszym kamieniem milowym było opracowanie i wprowadzenie, także do obiegu prawnego, uniwersalnej metody identyfikacji w świecie elektronicznym – podpisu elektronicznego, w oparciu o technologie infrastruktury klucza publicznego (PKI), w szczególności tak zwanego podpisu kwalifikowanego, mającego szczególną moc prawną (równoważną z podpisem odręcznym). Siłą tego rozwiązania jest jego uniwersalizm – możliwość stosowania powszechnie przez obywateli, do wszelkich usług elektronicznych (także komercyjnych) i na obszarze całej Unii Europejskiej, podobnie jak w świecie fizycznym korzysta się z dowodów tożsamości wydanych przez państwo. Idea napotkała trudności w praktycznej realizacji, niemniej, przynajmniej w teorii, dała możliwość ograniczenia modelu silosowego oraz wprowadzenia standaryzacji w zakresie identyfikacji i uwierzytelnienia elektronicznego. Z kolei wdrożenie elektronicznych dokumentów tożsamości (dokumentów z mikroprocesorem) wydatnie wsparło rozpowszechnienie idei w większości krajów, gdzie się na ten krok zdecydowano – uzyskano bowiem efekt powszechności i łatwej dostępności elektronicznych środków identyfikacji.

Inne inicjatywy Unii Europejskiej, takie jak IDABC, STORK, Netcards, stanowią kolejne ważne kroki milowe dla praktycznej realizacji paneuropejskiego modelu uwierzytelnienia. I chociaż dotyczą przede wszystkim aspektu transgranicznego (wykorzystania środków identyfikacji elektronicznej wydanych w jednym kraju do realizacji e-usług w innym kraju), to wypracowane tam podejście ma silny aspekt uniwersalny – modele procesów, aspekty bezpieczeństwa, czy klasyfikacja wiarygodności różnych metod

Identyfikacja i uwierzytelnianie w usługach elektronicznych

uwierzytelnienia, mogą być zastosowane praktycznie dla każdego rodzaju usługi. Ponadto projekty te upowszechniają i realizują ideę federacji tożsamości, dzięki której możliwe jest wykorzystanie jednej elektronicznej tożsamości w wielu obszarach (ograniczając liczbę elektronicznych identyfikatorów posiadanych przez jedną osobę), czy współdzielenia wyniku uwierzytelnienia (tzw. *Single-Sign-On*).

W końcu, na dzień dzisiejszy istnieje już odpowiednia podstawa normatywna dla procesu uwierzytelnienia do usług elektronicznych. Oprócz standardu amerykańskiego NIST SP 800-53, istnieje także (od tego roku) pierwsza norma międzynarodowa, ISO 29115, umożliwiająca standaryzację podejścia do uwierzytelnienia elektronicznego w skali globalnej.

Niniejszy przewodnik ma na celu przedstawienie aktualnego stanu wiedzy w zakresie identyfikacji i uwierzytelnienia elektronicznego zwłaszcza do usług świadczonych zdalnie. Prezentuje w sposób syntetyczny tematykę uwierzytelnienia, począwszy od terminologii, poprzez procesy, wymagania, najlepsze praktyki, stan standaryzacji i regulacji prawnych. Praca ta dokonuje również przeglądu najważniejszych metod uwierzytelnienia oraz przykładów praktycznego ich wykorzystania, a także przedstawia i promuje nowoczesne trendy. Przewodnik przeznaczony jest dla szerokiego grona menedżerów i specjalistów technicznych i nietechnicznych, związanych ze świadczeniem e-usług. Dla czytelnika chcącego w syntetycznym skrócie poznać najważniejsze aspekty uwierzytelnienia (np. menedżera IT, CIO) przeznaczony jest rozdział 3. Dodatkowo polecane są także: rozdział 8, opisujący stan obecny w Polsce, czy rozdział 9 opisujący przykłady realizacji. Osoby wdrażające usługi elektroniczne i systemy informatyczne je wspierające (specjaliści ICT, architekci systemów, projektanci procesów) mogą z kolei zagłębić się w szczegóły zawarte w rozdziałach 4, 5 i 6. Z kolei lektura rozdziału 7 pozwala na poznanie najważniejszych aspektów prawnych, w oderwaniu od których żadne rozwiązanie techniczne nie może funkcjonować.

2 Terminologia

Najbardziej istotnymi terminami w dziedzinie identyfikacji elektronicznej, uwierzytelnienia i usług zaufania są następujące pojęcia: **tożsamość, identyfikator, uwierzytelnianie, dane uwierzytelniające** (ang. **credentials**), **autoryzacja, autentyczność**.

Pojęcia te są definiowane w kilku normach. W definicjach tych jednak występują różnice, dlatego w raporcie są prezentowane wszystkie definicje tych pojęć, przy czym przy definicjach uznanych przez zespół redakcyjny za najważniejsze umieszczono komentarz „termin rekomendowany”. W ten sposób czytelnik będzie mógł sobie wyrobić własne zdanie w kwestii terminologii stosowanej w rozważanej przez raport dziedzinie. W przypadku, gdy dostępna była norma w języku angielskim podano pojęcie i jego definicję w oryginale oraz dodano tłumaczenie polskie.

Termin	Źródło	Definicja	Komentarz	Przykład
Tożsamość (ang. identity)	PN-I-02000 3.4.093	Element danych przypisany podmiotowi (3.9.074) ¹ i wykorzystywany do jego identyfikowania (3.1.031).	termin rekomendowany	Nazwisko imię, data i miejsce urodzenia.
Identyfikacja (ang. identification)	CWA 15264	Proces pozyskania informacji o deklarowanej tożsamości (strony) bez uwzględnienia wiarygodności tej informacji ²	termin rekomendowany	
Identyfikacja (ang. identification)	PN-I-02000 3.1.031	Proces zautomatyzowanego rozpoznania określonego użytkownika (3.1.110) w systemie, możliwy do zrealizowania dzięki zastosowaniu		

¹ To jest oznaczenie pozycji w normie, pod którą zdefiniowano pojęcie. W tym przypadku pod oznaczeniem (3.9.074) znajduje się definicja pojęcia „podmiot”.

² tłumaczenie

Identyfikacja i uwierzytelnianie w usługach elektronicznych

		unikalnych nazw.		
Uwierzytelnianie				
Uwierzytelnienie kryptograficzne (ang. cryptographic authentication)	PN-I-02000 3.3.103	Wykorzystanie technik związanych z szyfrowaniem (3.3.083) do przeprowadzenia uwierzytelnienia (3.4.104).		
Uwierzytelnienie podmiotów (ang. entity authentication)	PN-I-02000 3.3.104	Potwierdzenie, że podmiot (3.9.074) jest tym, za kogo się podaje.		
Uwierzytelnianie (ang. authentication)	PN-ISO/IEC 2382-8 luty 2001 08.01 .11	Działanie weryfikowania deklarowanej tożsamości jednostki.	termin rekomendowany	Potwierdzenie hasłem, cechą biometryczną lub metodami kryptograficznymi, deklarowanej tożsamości.
Uwierzytelnianie	ISO 11166-1	Proces stosowany między nadawcą a odbiorcą dla zapewnienia integralności danych i uwierzytelnienia źródła ich pochodzenia.		
Identyfikator				
Identyfikator wyróżniający (ang. distinguishing Identifier)	PN-I-02000 3.4.021	Informacja jednoznacznie wyróżniająca podmiot (3.9.074) w procesie uwierzytelniania (3.4.061)	termin rekomendowany	NIP, PESEL

Identyfikacja i uwierzytelnianie w usługach elektronicznych

Identyfikator (ID) użytkownika	PN-ISO/IEC 2382-8 luty 2001 08.04.22	Ciąg znaków lub wzorzec, który jest używany przez system przetwarzania danych do identyfikowania użytkownika.		
Identyfikator wyróżniający (ang. distinguishing name)	ISO/IEC 11770-2	Informacja, która jednoznacznie wyróżnia dany podmiot.		
Autoryzacja				
Autoryzacja (ang. authorization)	PN-I-02000	Nadanie praw, które obejmują przyznanie dostępu (3.1.026) na podstawie praw dostępu (3.1.086) [PN-ISO/IEC 2382-8:2001] ³ . UWAGA - Proces przyznania podmiotowi całkowitego lub ograniczonego dostępu do zasobu.	termin rekomendowany	Na podstawie podanego identyfikatora (deklaracja tożsamości) i uwierzytelnienia tej deklaracji hasłem bank dopuszcza klienta do wykonania operacji określonych w umowie na rachunku tego klienta.
Autoryzacja (uprawnienie)	PN-ISO 8908	Zezwolenie na nabycie lub wykonanie usługi.		
Autentyczność				
Autentyczność	PN-I-02000	Właściwość polegająca na tym, że pochodzenie lub zawartość obiektu (3.9.062) informatycznego są		

³ Polska norma PN-ISO/IEC 2382-8:2001 „Technika informatyczna - Terminologia – Bezpieczeństwo”

Identyfikacja i uwierzytelnianie w usługach elektronicznych

		takie, jak deklarowane.		
Autentyczność	TR 13335-1	Właściwość zapewniająca, że tożsamość podmiotu lub zasobu jest taka, jak deklarowana. Autentyczność dotyczy takich podmiotów jak: użytkownicy, procesy, systemy i informacja.	termin rekomendowany	Potwierdzenie przez upoważniony organ, że przedstawiony dokument został rzeczywiście wydany przez uprawniony do tego podmiot.
Dane uwierzytelniające				
Dane uwierzytelniające (ang. credentials)	PN-ISO/IEC 2382-8 luty 2001 08.01 .14	Dane, które są przekazywane w celu ustalenia deklarowanej tożsamości jednostki		
Dane uwierzytelniające (inaczej: referencje, poświadczenie, insygnia, kwalifikacje)	Identity and Access Management: Assurance and Authentication Guidelines Michael Locatis Chief Information Officer for the State Of Colorado – OIT- Office of IT	Obiekt, który autorytatywnie wiąże tożsamość (i ewentualnie, dodatkowe atrybuty) z tokenem posiadanym przez osobę i będącym pod jej kontrolą.		Certyfikat elektroniczny

Z uwagi na istnienie bardzo wielu różnych definicji podstawowych pojęć związanych z identyfikacją i uwierzytelnieniem, wybrano definicje z norm dot. technik informatycznych, nie dokonując żadnych zmian. W pracach grupy podjęto próbę ujednoczenia tych definicji, lecz rezultaty nie uzyskały konsensusu. Taki zresztą konsensus nie jest możliwy, gdyż do poszczególnych pojęć (np. uwierzytelnienia) inaczej podchodzi naukowiec kryptolog, inaczej technolog informatyk tworzący aplikacje, inaczej prawnik, a jeszcze inaczej użytkownik końcowy.

3 Synteza i zalecenia

Niniejszy rozdział rysuje podstawowe pojęcia i procesy związane z identyfikacją i uwierzytelnieniem w usługach świadczonych drogą elektroniczną w ujęciu czysto funkcjonalnym, nieco abstrahującym od podstaw prawnych, standardów technicznych oraz implementacji. Oznacza to, że można potraktować go jako streszczenie raportu przeznaczone dla osób, które pragną zapoznać się z najważniejszymi praktycznymi wnioskami wynikającymi z raportu, unikając jednocześnie szczegółowej analizy uwarunkowań prawnych i technicznych. Na użytek odbiorców, którzy po lekturze syntezy zdecydują się na pogłębienie analizy, zamieszczono odsyłacze do sekcji raportu zawierających bardziej systematyczną prezentację zagadnień.

3.1 Co to jest identyfikacja i uwierzytelnienie?

Istnieje wiele niezrozumienia co do znaczenia pojęć typu: identyfikacja, uwierzytelnienie, autoryzacja. Często te terminy są mieszane, używane zamiennie lub jako tożsame. Istnieje też wiele, nie zawsze spójnych definicji (vide rozdział 2 „Terminologia”). Dlatego zanim przejdzie się do dalszych części tego rozdziału i raportu, należy zaakcentować, co w praktyce oznaczają te słowa i jak są one rozumiane przez autorów niniejszego raportu. Usługi elektroniczne zakładające interakcję z użytkownikiem wymagają zwykle identyfikacji użytkownika i jego uwierzytelnienia. Zgodnie z terminologią, identyfikację rozumie się jako nadanie (przypisanie) identyfikatora do osoby oraz deklarację (stwierdzenie) tożsamości osoby poprzez przedstawienie identyfikatora. Taki identyfikator jednoznacznie tą osobę identyfikuje i stanowi elektroniczną tożsamość użytkownika w tymże środowisku. Sama identyfikacja pozwala zatem na stwierdzenie „o kogo chodzi”, ale nie potwierdza, że użytkownik danej e-usługi jest faktycznie tą osobą, która została zadeklarowana i zidentyfikowana. Do tego potwierdzenia służy właśnie uwierzytelnienie, polegające na dostarczeniu dowodów, że użytkownik jest właśnie tą zidentyfikowaną osobą (nikt się nie podszywa). W szczególnych przypadkach identyfikacja i uwierzytelnienie może przebiegać jednocześnie (np. gdy nasz identyfikator jest tajny, stanowiąc jednocześnie „hasło”), ale zasadniczo są to dwa różne procesy. Z kolei pod pojęciem autoryzacji (często mylonej z uwierzytelnieniem i niepoprawnie nazywanej „autentykacją”) rozumie się proces nadania określonych uprawnień, z których następnie poprawnie zidentyfikowana i uwierzytelniona osoba będzie mogła korzystać.

Techniki uwierzytelnienia można generalnie podzielić na trzy grupy, oparte na weryfikacji:

- a) „co znasz” (login, hasło/PIN),
- b) „co posiadasz” (sprzętowy token, np. karta elektroniczna),
- c) „co masz” lub „czym jesteś” (cecha biometryczna).

Zdarzają się także techniki „mieszane” - użycie sprzętowego tokena do identyfikacji wymaga jego odblokowania poprzez podanie kodu PIN lub danych biometrycznych, które są weryfikowane przez procesor tokena. Powszechnie uznaje się, że uwierzytelnienie jednoczynnikowe oparte jest na jednym elemencie: „co znasz” albo „co posiadasz”, natomiast kombinacja tych obu elementów to „uwierzytelnienie wieloczynnikowe” (ang. *multifactor authentication*). Uwierzytelnienie wieloczynnikowe, obok opartego na podaniu cechy biometrycznej („co masz” lub „czym jesteś”), należą do kategorii „silnego uwierzytelnienia” (ang. *strong authentication*).

3.2 Procesy związane z elektroniczną tożsamością

Bez względu na sposób ujęcia problemu tożsamości i uwierzytelnienia, pojęcie elektronicznej tożsamości zawsze występuje w kontekście podobnych procesów biznesowych. W każdym z formalnych standardów uwierzytelnienia (opisanych w rozdziale 4) można wyróżnić trzy podstawowe procesy:

- **proces rejestracji**, czyli pozyskania i weryfikacji atrybutów tożsamości fizycznej⁴, konstytuujących tożsamość elektroniczną w sposób wiążący ją możliwie jednoznacznie i wiarygodnie z tożsamością fizyczną;
- **proces zarządzania danymi uwierzytelniającymi**, zawierający m.in. proces wydania danych uwierzytelniających (po raz pierwszy), odnowienia, unieważnienia, zawieszenia;
- **proces uwierzytelnienia**.

Warto zwrócić uwagę, że realizacja każdego z wymienionych procesów nie ma charakteru w pełni deterministycznego, tj. w wyniku realizacji danego procesu uzyskujemy rezultat, który jedynie z zadany­m prawdopodobieństwem (z pewnym poziomem wiarygodności) odzwierciedla faktyczny związek pomiędzy tożsamością fizyczną i elektroniczną. Ponieważ na łączny poziom wiarygodności procesu uwierzytelnienia wpływają wszystkie wymienione procesy, rozwiązania techniczne lub organizacyjne, związane z realizacją dowolnego z nich i obniżające jego wiarygodność, z natury rzeczy wpływają na obniżenie efektywnej wiarygodności produktu końcowego - uwierzytelnienia.

Wspomniane procesy w sposób najbardziej kompleksowy i uniwersalny opisuje norma ISO 29115 (por. 0). Warto zauważyć, że odnosi się ona także do kwestii uwierzytelnienia „jednostek nieosobowych” (ang. „Non-Person Entity”), np. jednostek organizacyjnych lub systemów technicznych, co wyróżnia ją spośród innych standardów (np. ustanowionych w IDABC i STORK). Wiele przedstawionych poniżej koncepcji oparto na rozwiązaniach przywołanej normy.

3.3 Poziomy wiarygodności

Wiele elektronicznych usług wymaga identyfikacji i uwierzytelnienia użytkownika, jednak nie wszystkie te usługi potrzebują takiego samego poziomu bezpieczeństwa. Inne wymagania odnoszą się do dostępu do wrażliwych danych medycznych, inne do pobierania formularzy urzędowych. W zależności od rodzaju usługi i wymaganego poziomu bezpieczeństwa zastosowane powinny być adekwatne metody i techniki uwierzytelnienia o określonej wiarygodności. W związku z tym dla każdej usługi powinien zostać określony (na podstawie analizy ryzyka) poziom wiarygodności wymagany dla procesu uwierzytelnienia. Poziom wiarygodności określa stopień zaufania dopuszczalny i akceptowalny biorąc pod uwagę straty, jakie mogą być poniesione w przypadku błędnego uwierzytelnienia. Dla ułatwienia porównań usług i metod uwierzytelnienia oraz uzyskania interoperacyjności powstały różne klasyfikacje standaryzujące poziomy wiarygodności i ich interpretację, wraz z wymaganiami co do procesów i technik w zakresie identyfikacji i uwierzytelnienia, opisane w rozdziale 4. Wspomniany wyżej projekt normy ISO 29115

⁴ Zgodnie z nomenklaturą przedstawioną w rozdziale 2 – *dane uwierzytelniające*.

zapewni podejście spójne co do zasady z zastosowanym w projektach IDABC i STORK (por. 4.3 oraz 4.4).

We wspomnianych dokumentach określone zostały 4 poziomy wiarygodności (od 1 do 4), gdzie poziom 1 oznacza poziom najniższy (minimalna wiarygodność lub jej brak), a poziom 4 – najwyższy (wymagania podobne jak dla certyfikatów kwalifikowanych). Dostarczają one wytycznych pozwalających określić poziom wiarygodności danej usługi oraz metody (procesy, środki, techniki) jego osiągnięcia. Przypomnijmy, że przy określaniu poziomu wiarygodności uwierzytelnienia w konkretnym modelu należy wziąć pod uwagę pełen proces; począwszy od akwizycji i zarządzania danymi uwierzytelniającymi (rejestracja, generowanie, wydanie, zarządzanie cyklem życia, nośnik / sposób przechowywania itp.), po właściwy proces uwierzytelnienia, a także czynniki organizacyjne (m.in. otoczenie prawne, infrastrukturę, bezpieczeństwo, w tym bezpieczeństwo informacji, systemów IT itp.). Zgodnie z normą ISO 29115 poziomy wiarygodności zostały określone w opisany poniżej sposób:

LoA⁵ 1 – minimalna wiarygodność lub jej brak. Nie wymaga użycia kryptografii. Przykładowo, poziom może mieć zastosowanie w serwisach internetowych, do których użytkownik sam się rejestruje, dane uwierzytelniające to login i hasło, a usługa polega na udostępnieniu pewnych materiałów, np. wiadomości czy dokumentacji produktu. Z kolei dla uwierzytelnienia urzędnika wystarczającym identyfikatorem może być adres MAC.

LoA 2 – ograniczona wiarygodność deklarowanej tożsamości. Nie wymaga użycia kryptografii. Na tym poziomie wystarcza uwierzytelnienie jednoczynnikowe, jednak zastosowany być powinien bezpieczny protokół uwierzytelnienia, redukujący wpływ podsłuchania (ang. *eavesdropping*) i ataków polegających na zgadywaniu. Przechowywane dane uwierzytelniające muszą być chronione. Przykładem usługi na tym poziomie może być serwis instytucji ubezpieczeniowej, umożliwiający zmianę adresu zamieszkania.

LoA 3 – wysoka wiarygodność deklarowanej tożsamości. Poziom ten wymaga uwierzytelnienia wieloczynnikowego oraz użycia kryptografii. Przykładem może być usługa polegająca na zgłoszeniu patentu do urzędu patentowego lub też dostęp do rachunku inwestycyjnego.

LoA 4 – bardzo wysoka wiarygodność deklarowanej tożsamości. Ten poziom jest zbliżony do LoA 3, ale dodatkowo wymaga fizycznej obecności przy rejestracji osoby oraz użycia odpornych na manipulacje tokenów sprzętowych (np. kart elektronicznych z mikroprocesorem) przechowujących sekrety lub kryptograficzne klucze prywatne. Protokół uwierzytelnienia musi chronić kryptograficznie wszelkie dane identyfikujące osobę i inne wrażliwe dane. Przykładem usługi wymagającej tego poziomu, może być serwis umożliwiający aptekarzowi wydanie leków lub też zatwierdzenie przez osobę z zarządu przedsiębiorstwa dużego transferu pieniędzy z firmowego konta bankowego. W przypadku uwierzytelnienia urządzeń czy systemów (tzw. NPE - *Non Person Entity*), wymagane jest użycie certyfikatów elektronicznych (np. X.509 czy CVC).

Na podstawie normy ISO 29115 proponuje się także wyznaczenie wymaganego poziomu wiarygodności dla danej e-usługi. Czynność ta polega na określeniu wpływu ewentualnego błędu w uwierzytelnieniu na wielkość straty finansowej, stopień utraty reputacji, niewygody, czy wycieku

⁵ LoA – ang. *Level of Assurance*, poziom wiarygodności.

informacji wrażliwych. W zależności od oszacowanej wielkości straty (niska, umiarkowana, znacząca, wysoka) dana usługa zakwalifikuje się do określonego poziomu LoA (zob. tabela Tabela 5). To, co oznacza dla danej organizacji stratę niską, wysoką itd. należy do oceny przez tę organizację.

Przykładowo: przyjmijmy, że wyciek danych medycznych (stanowiących informację wrażliwą) można uznać za stratę „wysoką”. Zatem wymagany poziom wiarygodności uwierzytelnienia będzie najwyższy – 4. Zatem dostawca tożsamości, system uwierzytelnienia i cała tzw. struktura wiarygodności uwierzytelnienia powinny spełniać wymagania jak dla tego poziomu, czyli m.in. dane uwierzytelniające powinny być wydawane wyłącznie na tokenie sprzętowym, powinna być wykorzystywana kryptografia, a w fazie rejestracji wymaga się fizycznej obecności osoby.

Metodyka oceny ryzyka oraz wymagań dotyczących poziomu wiarygodności nie jest przedmiotem przywołanych powyżej standardów - nie istnieje jeden powszechnie uznany model oceny wiarygodności i skala jej poziomów. W zależności od dziedziny zastosowania, organizacji i/lub infrastruktury można tworzyć własne modele, w szczególności definiując własną skalę, dysponującą większą liczbą poziomów wiarygodności. Jednak dla zapewnienia interoperacyjności zaleca się mapowanie różnych skal na jedną, np. określoną w ISO 29115. Taka czynność została przeprowadzona np. w ramach projektu STORK: różne kraje posiadały własne skale, o różnej liczbie poziomów, toteż stworzono wspólną skalę, na którą zmapowano skale krajowe (por. rys. Rysunek 6 w rozdz. 4.4). Ponadto zaleca się publikowanie zastosowanej metodyki, co umożliwi dokonanie mapowania innym dostawcom, rozważającym sfederowanie z systemem, w którym jest ona stosowana. Alternatywnie sfederowania usług uwierzytelnienia można dokonać przez mapowanie rozbieżnych modeli na wspólny model referencyjny, np. ISO 29115 lub STORK.

3.4 Struktura wiarygodności uwierzytelnienia

Struktura wiarygodności uwierzytelnienia jest to zestaw wszystkich, technicznych i organizacyjnych czynników wpływających na całkowity poziom wiarygodności uwierzytelnienia. Końcowy wynik zawsze jest równy najniższemu poziomowi osiągniętemu przez któryś z czynników (zasada „najsłabszego ogniwa”).

W strukturę wiarygodności wchodzi przede wszystkim opisane w rozdz. 3.2 procesy związane z elektroniczną tożsamością. W ramach tych procesów istnieją liczne podprocesy i czynniki wchodzące w strukturę wiarygodności. Na przykład w fazie rejestracji (ang. *enrolment*) wyróżnia się oprócz samego procesu rejestracji osoby, także złożenie aplikacji (formularza), udowadnianie i weryfikację tożsamości, czy rejestrację (zapis) i archiwizację przebiegu procesu. Z kolei w fazie zarządzania danymi uwierzytelniającymi wyróżnia się m.in. procesy tworzenia (generowania) danych uwierzytelniających, inicjalizacji, powiązania z tożsamością, wydanie (przekazanie) osobie, aktywacji (po przekazaniu), przechowywania i zarządzania stanem (zawieszanie, odwoływanie, odnowienie).

Oprócz elementów technicznych, w strukturze wiarygodności występują także czynniki organizacyjne i zarządcze, takie jak sposób/forma prowadzenia usługi (np. forma działalności gospodarczej), otoczenie prawne, uwarunkowania kontraktowe, stan finansowy, bezpieczeństwo informacji itp.

Jednocześnie cała struktura wiarygodności nie stanowi zbioru zamkniętego – jeżeli istnieją istotne inne czynniki (nie wymienione np. w ISO 29115) wpływające na wiarygodność uwierzytelnienia, to powinny one być włączone do struktury i wzięte pod uwagę. Więcej informacji na ten temat znajduje się w rozdziale 4, w szczególności w podrozdziale 0 (dotyczącym normy ISO 29115).

3.5 Wybór modelu

Sposób klasyfikacji skali wiarygodności w przytoczonych wcześniej standardach nie jest tożsamy, zatem może zaistnieć problem, który standard wybrać. Na pewno norma ISO jest dokumentem najbardziej uniwersalnym, mającym charakter globalny. Natomiast w kontekście europejskim najistotniejszy jest model STORK, wypracowywany przez ostatnie lata (stąd też widoczna zbieżność poziomów określonych w eIDAS z poziomami STORK QAA). Zasadniczo we wszystkich modelach idea podziału jest identyczna, ale określone w nich poziomy nie są równoważne - wymagania dotyczące poszczególnych poziomów różnią się wzajemnie (uproszczone porównanie poziomów znajduje się w tabeli

Tabela 1). Niemniej są to różnice niewielkie i przy stosunkowo niedużych uzupełnieniach można osiągnąć zgodność między nimi. Jedyna istotna różnica tkwi w podejściu do wymagań poziomu najwyższego (4). W podejściu europejskim (STORK i eIDAS), poziom najwyższy osiągnąć można stosując jedynie „kwalifikowane” narzędzia (np. certyfikat kwalifikowany), wydane przez podmiot kwalifikowany (zgodnie z podejściem zastosowanym w dyrektywie 99/93/EC dot. podpisu elektronicznego). Norma ISO jest mniej restrykcyjna w tym zakresie (pozostawia więcej swobody decyzjom wynikającym z szacowania ryzyka). Oczywiście osiągnięcie poziomu 4 STORK oznacza osiągnięcie tegoż poziomu wg skali ISO.

Inną ewentualnością jest stworzenie własnej skali, na przykład poprzez modyfikację wybranego modelu. W szczególności może to być celowe, aby uzyskać strukturę wiarygodności ze skalą mapowalną (zgodną) zarówno z modelami europejskimi (STORK i eIDAS), jak i ISO. Przykładowo można stworzyć skalę pięciopoziomową, w której poziom 4 odpowiadałby poziomowi 4 wg ISO, a poziom 5 odpowiadałby poziomowi 4 wg STORK. W takim przypadku byłoby możliwe zmapowanie własnej klasyfikacji zarówno na model ISO (poziom 4 i 5 łącznie odpowiadałby poziomowi 4 ISO), jak i na model STORK (poziom 5 odpowiadałby poziomowi 4 wg STORK, a poziomy 3 i 4 razem odpowiadałyby poziomowi 3 wg STORK).

Tabela 1. Uprozczone porównanie poziomów wiarygodności w różnych modelach

	STORK	ISO29115	eIDAS (proj.) ⁶
Poziom 1	Zdalnie Deklaracja własna tożsamości Login-hasło/PIN	Zdalnie Deklaracja własna tożsamości Wymagane procedury Login-hasło	—
Poziom 2	Rejestracja zdalna Weryfikacja tożsamości przez operatora rejestracji Zgoda rządu Silne hasło/PIN	Rejestracja zdalna Udowodnienie tożsamości przez osobę deklarującą (np. przedstawienie dokumentu identyfikacyjnego) Procedury Polityka bezp. informacji Audyty bezpieczeństwa	—
Poziom 3	Rejestracja zdalna Weryfikacja tożsamości przez operatora procesu rejestracji Osobiste stawiennictwo warunkowe (w zależności od środków weryfikacji) Akredytacja lub nadzór przez instytucję państwową Certyfikat programowy, token OTP, certyfikat niekwalifikowany na tokenie sprzętowym Zapewnione bezpieczeństwo uwierzytelnienia	Rejestracja zdalna Udowodnienie tożsamości przez osobę deklarującą (np. przedstawienie dokumentu identyfikacyjnego) Weryfikacja tożsamości przez operatora procesu rejestracji (np. poprzez okazanie dodatkowego dokumentu identyfikacyjnego) Procedury Polityka bezpieczeństwa informacji Audyty bezpieczeństwa System zarządzania bezpieczeństwem Uwierzytelnienie wieloczynnikowe	Rejestracja zdalna Weryfikacja tożsamości przez operatora procesu rejestracji z wykorzystaniem oficjalnych środków (określonych w prawie, np. dokumentów wydanych przez państwo) Akredytacja/nadzór państwa Certyfikat, token OTP
Poziom 4	Osobiste stawiennictwo przy wydawaniu danych uwierzytelniających Certyfikat kwalifikowany Token sprzętowy certyfikowany Zapewnione bezpieczeństwo uwierzytelnienia równoważne z Common Criteria min. EAL4+ (Spełnienie wszystkich wymagań wynikających z aktów prawnych dot. podpisu elektronicznego)	Osobiste stawiennictwo Udowodnienie i weryfikacja tożsamości Procedury Polityka bezp. informacji Audyty bezpieczeństwa System zarz. bezpieczeństwem Token sprzętowy Uwierzytelnienie wieloczynnikowe	Osobiste stawiennictwo Weryfikacja dokumentu identyfikacyjnego wydanego przez państwo Weryfikacja tożsamości w rejestrach państwowych Dane uwierzytelniające wydane przez instytucję publiczną lub kwalifikowanego dostawcę usług zaufania Certyfikat kwalifikowany Token sprzętowy certyfikowany

⁶ Wg stanu projektu rozporządzenia na dzień 25.10.2013; klasyfikacja może ulec zmianie

3.6 Usługi zaufania i ich dostawcy

W obecnym stanie prawnym i faktycznym jedyną powszechnie uznaną i uregulowaną usługą zaufania w kraju jest działalność urzędów certyfikacji (ang. *certification authority*, CA) potwierdzających tożsamość posiadaczy podpisu elektronicznego. W polskiej rzeczywistości prawnej skala realizacji tej usługi jest ograniczona w stosunku do zakresu wynikającego z dyrektywy 1999/93/EC. Implementując postanowienia dyrektywy w prawie krajowym ustawodawca zdecydował się przenieść doń jedynie koncepcje kwalifikowanego podpisu elektronicznego i jego dostawcy, rezygnując z implementacji zaawansowanego podpisu elektronicznego⁷. Można jedynie spekulować, w jakiej mierze niepełna implementacja dyrektywy przyczyniła się do ograniczenia potencjału rozwoju infrastruktury zaufania w Polsce i związanych z nią usług.

Taki stan rzeczy ulegnie zapewne zasadniczej odmianie w niezbyt odległej przyszłości w wyniku przyjęcia projektu rozporządzenia w sprawie identyfikacji elektronicznej i usług zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznym (COM(2012)⁸ 238; por. rozdział 4.5). W obecnej wersji projektu do podpisu elektronicznego bazującego na przepisach dyrektywy 1999/93/EC⁹ dodano szereg nowych usług zaufania oraz realizujących je podmiotów – dostawców usług zaufania. Usługi zaufania i realizujący je dostawcy obejmują wg projektu rozporządzenia osoby fizyczne lub prawne świadczące jedną lub więcej usług zaufania, rozumianą jako elektroniczną usługę polegającą na tworzeniu, kontroli, weryfikacji i przechowywaniu:

- podpisów elektronicznych,
- pieczęci elektronicznych,
- elektronicznych znaczników czasu,
- dokumentów elektronicznych,
- usług przekazu elektronicznego,
- usług uwierzytelniania witryn internetowych,
- certyfikatów elektronicznych, w tym certyfikatów podpisów elektronicznych i pieczęci elektronicznych.

Należy zauważyć, że UE zdecydowała się na zastąpienie wymagającej czasochłonnej implementacji do prawa krajowego dyrektywy przez obowiązujące powszechnie, z chwilą jego opublikowania, rozporządzenie. Wydaje się, że zastosowane podejście jest wynikiem świadomości narastającej luki pomiędzy potrzebami rozwijającego się rynku elektronicznego i koniecznością zapewnienia „transgraniczności” na obszarze UE oraz istniejącej infrastruktury prawnej i normatywnej.

Jak wynika z definicji usługi zaufania, rozporządzenie będzie dotyczyło wielu (większości?) dostawców usług elektronicznych obecnie już funkcjonujących, których działalność na dzień dzisiejszy nie ma związku z ustawą o podpisie elektronicznym i dyrektywą 1999/93/EC, i które nie podlegają pod specjalne rygory, jakie są nałożone np. na dostawców kwalifikowanych usług certyfikacyjnych (będący odpowiednikiem „kwalifikowanego dostawcy usług zaufania” wg rozporządzenia). Nowa regulacja prawna

⁷ W 2001 r. nie była znana decyzja Komisji nr 511 z 2003 r., która wprowadziła wymagania dla „kwalifikowanych” i „zwykłych” podmiotów; w trakcie prac parlamentarnych nad ustawą o podpisie przeważał pogląd, że wymagania i skutki prawne będą tylko dla kwalifikowanych usług, natomiast do „zwykłych” usług (bez ich różnicowania np. na „zaawansowane”) odnosił się będzie art. 8.

⁸ Dalej – rozporządzenie eIDAS.

⁹ Dyrektywa 1999/93/EC utraci moc prawną z chwilą wejścia w życie przywołanego rozporządzenia.

Identyfikacja i uwierzytelnianie w usługach elektronicznych

wyraźnie podkreśla bowiem zasadę: jeśli jakiś podmiot świadczy usługę, której skutki prawne wynikają z rozporządzenia, to jednocześnie musi spełnić wymagania zawarte w tymże rozporządzeniu. Zatem nowa regulacja wprowadzi pewne nowe wymagania dla całej masy podmiotów prywatnych i publicznych, w tym ich odpowiedzialność prawną za usługi zaufania, jakie wg rozporządzenia będą dostarczać. W sektorze prywatnym wymagania są formalnie dobrowolne, jednak jeśli podmiot nie spełnia wymagań, to nie może powoływać się na przepisy dot. skutków prawnych. Wymagania wynikają m.in. z art. 9 aktualnej wersji projektu:

Dostawca usług zaufania odpowiada za wszystkie bezpośrednie szkody poniesione przez osobę fizyczną lub prawną w wyniku niedopełnienia zobowiązań [...].

Z kolei w dalszej części projektu (art. 15) narzucone są wymagania co do bezpieczeństwa, wg których dostawcy usług zaufania:

- przyjmują odpowiednie środki techniczne i organizacyjne w celu zarządzania ryzykiem,
- zapewniają poziom bezpieczeństwa dostosowany do stopnia ryzyka,
- podejmują środki zapobiegające incydentom związanym z bezpieczeństwem lub minimalizujące ich wpływ,
- informują zainteresowane strony o negatywnych skutkach takich incydentów,
- zgłaszają bezzwłocznie wszelkie przypadki naruszenia bezpieczeństwa lub utraty integralności – które mają znaczący wpływ na świadczoną usługę zaufania i zawarte w niej dane osobowe:
 - właściwemu organowi nadzorczemu;
 - właściwemu organowi krajowemu ds. bezpieczeństwa informacji;
 - innym odpowiednim stronom trzecim, takim jak organy ds. ochrony danych.

W niektórych przypadkach, zwłaszcza gdy naruszenie bezpieczeństwa lub utrata integralności będzie dotyczyć dwóch lub większej liczby państw członkowskich, organ nadzorczy będzie powiadamiał organy nadzorcze w pozostałych państwach członkowskich oraz Europejską Agencję ds. Bezpieczeństwa Sieci i Informacji (ENISA), jak również może podać zaistniałe fakty do wiadomości publicznej, jeżeli uzna, że ujawnienie naruszenia leży w interesie publicznym. Ponadto wg intencji wnioskodawców, do rozporządzenia będzie dołączona lista norm i standardów technicznych, które będą obowiązywały dostawców usług zaufania. Warto jeszcze nadmienić, iż nowe rozporządzenie rozróżnia i oddzielnie traktuje kwestię dostawców usług zaufania i wydawców tzw. środków identyfikacji elektronicznej (por. 3.7). Oznacza to, że nie każdy dostawca tożsamości jest dostawcą usług zaufania.

3.7 Uwierzytelnienie w sektorze publicznym i prywatnym

Dotychczasowa infrastruktura prawna i normatywna uwierzytelnienia i zaufania skupiała się wokół usług realizowanych przez sektor komercyjny. Zgodnie z regulacjami UE obowiązkiem państw członkowskich jest notyfikowanie do Komisji Europejskiej projektów norm i standardów technicznych oraz projektów aktów prawnych zawierających przepisy techniczne. Odbywa się to w oparciu o tzw. dyrektywę notyfikacyjną (dyrektywa 83/189/EWG, zmieniona przez dyrektywę 98/34/WE). Należy dodać, że dyrektywa 98/48/WE rozszerzyła system notyfikacji tak, by obejmował również „usługi społeczeństwa informacyjnego”. Z obowiązku notyfikacji zwolnione jednak pozostają *explicite* te akty prawne, które odnoszą się do działań państwa w ramach jego wyłącznej domeny aktywności. Oznacza to, że o ile infrastruktura prawna i normatywna usług zaufania świadczonych przez sektor prywatny podlega

Identyfikacja i uwierzytelnianie w usługach elektronicznych

procesowi obligatoryjnej harmonizacji w ramach UE, harmonizacja analogicznych usług świadczonych przez administrację publiczną krajów członkowskich realizowana jest wyłącznie wskutek implementacji programów i projektów, w których ich udział jest dobrowolny (np. IDABC lub STORK). W rezultacie osiągnięto w skali UE harmonizację technicznych standardów usług zaufania świadczonych przez sektor prywatny, wyrażającą się w szczególności w postaci list TLS - Trusted List of supervised/accredited Certification Service Providers oraz szczegółowych wymogów technicznych, jakim muszą odpowiadać urządzenia wykorzystywane do przechowywania i składania kwalifikowanego podpisu elektronicznego. Listy TLS zawierają certyfikaty urzędów certyfikacji funkcjonujących w krajach UE i zarejestrowanych jako wystawcy certyfikatów kwalifikowanego podpisu elektronicznego. Wydawane przez nie certyfikaty kwalifikowanego podpisu elektronicznego winny być uznawane w skali całej UE, co przynajmniej w teorii gwarantuje realizację traktatowej zasady swobody przepływu usług.

Rozwiązania stosowane przez rządy państw UE w zakresie usług zaufania świadczonych na rzecz, w ramach lub przez sektor publiczny nie zdołały osiągnąć porównywalnego poziomu unifikacji i akceptacji. Specyfika rozwiązań stosowanych przez i w krajach UE w zakresie usług zaufania w sektorze publicznym sprawia, że nie są one akceptowane w innych krajach członkowskich na podstawie ogólnie obowiązujących standardów prawnych i technicznych. Oznacza to w praktyce brak realizacji traktatowej zasady swobody przepływu osób – obywatele kraju członkowskiego UE z reguły nie mają możliwości łatwej realizacji elektronicznych usług publicznych na terenie innego kraju. Próba rozwiązania problemu interoperacyjności usług zaufania w sektorze publicznym była realizacja - pod auspicjami UE - projektów IDABC (por. 4.3) oraz STORK (por. 4.4). Najbardziej istotnym produktem obu projektów jest zdefiniowanie i implementacja struktury brokera tożsamości tłumaczącego żądania uwierzytelnienia złożone w ramach jednego systemu krajowego i dotyczące tożsamości potwierdzonej w ramach innego systemu, na format właściwy dla kraju pochodzenia okaziciela. Obecnie realizowany jest projekt STORK2, stanowiący kontynuację projektu STORK. W jego ramach realizowane są pilotażowe zastosowania o znacznej skali infrastruktury zaprojektowanej w ramach poprzedniego etapu.

Projekt rozporządzenia eIDAS zasadniczo zmienia opisany stan rzeczy, a jednocześnie sankcjonuje rzeczywistość, w której rozwiązania stosowane w poszczególnych krajach UE podążyły w kierunkach na tyle rozbieżnych, że oparcie ich na wspólnych standardach technicznych wydaje się obecnie nieracjonalne i niewykonalne. Jedną z podstawowych nowości wnoszonych przez projekt eIDAS jest zasada wzajemnego uznawania i akceptowania środków identyfikacji elektronicznej dla tych usług, w przypadku których identyfikacja elektroniczna jest wymagana, aby można było uzyskać dostęp na szczeblu krajowym. Obowiązki zgłoszenia (oraz innym obowiązkom przewidzianym w projekcie) podlegają środki identyfikacji elektronicznej wydawane przez państwo członkowskie, w jego imieniu lub co najmniej na jego odpowiedzialność. W praktyce, w ramach specyfiki uregulowań prawnych funkcjonujących w Polsce, oznacza to wyrażone nie wprost uznanie, że baza infrastruktury usług zaufania zostanie przeniesiona w znaczącym stopniu z sektora prywatnego do publicznego. Wynika to z oczywistego faktu, że prowadzenie rejestrów pozwalających powiązać tożsamość, w tym elektroniczną, z osobą fizyczną jest jednym z podstawowych zadań realizowanych w Polsce przez administrację publiczną. Projekt rozporządzenia jednoznacznie określa, że *(p)ństwa członkowskie muszą zapewnić jednoznaczne powiązanie między danymi związanymi z identyfikacją elektroniczną a osobą, której identyfikacja ta dotyczy. Ten obowiązek nie oznacza, że jedna osoba nie może korzystać z kilku środków identyfikacji elektronicznej, lecz wszystkie takie środki muszą być powiązane z tą samą osobą. I dalej: (p)ństwa członkowskie muszą przyjąć odpowiedzialność za jednoznaczność powiązania (tj. za to, aby dane identyfikacyjne przypisane jednej osobie nie zostały przypisane żadnej innej osobie) i za mechanizm uwierzytelniający (tj. za możliwość sprawdzenia ważności danych związanych z identyfikacją*

elektroniczną). Tak zdefiniowane obowiązki państw członkowskich w praktyce najłatwiej zrealizować powierzając desygnowanej instytucji publicznej realizację usług zaufania obejmujących potencjalnie wszystkich obywateli kraju i traktując emitowane przez nią *dane związane z identyfikacją elektroniczną* osoby jako referencyjne dla funkcjonowania innych usług zaufania, w tym świadczonych przez sektor prywatny usług o wartości dodanej, jeżeli rynek zasygnalizuje popyt na takie usługi.

Powstanie takiego popytu jest zależne przede wszystkim od statusu prawnego i skali dopuszczalnego zastosowania poświadczeń tożsamości emitowanych przez sektor publiczny. Należy zwrócić uwagę, że art. 9 projektu rozporządzenia przewiduje odpowiedzialność dostawcy usług zaufania *za wszystkie bezpośrednio szkody poniesione przez osobę fizyczną lub prawną w wyniku niedopełnienia zobowiązań (...), chyba że dostawca usług zaufania może udowodnić, iż działał z zachowaniem należytej staranności*. Przyjmując założenie, że dostawcą usługi zaufania jest instytucja publiczna, odpowiedzialność za ew. szkody spoczywa na państwie. Znając rezerwę państwa wobec przyjmowania zobowiązań i odpowiedzialności można spodziewać się, że ewentualne świadczone przez usługi zaufania zostaną obwarowane ograniczeniami zastosowania poza sektorem publicznym lub zastosowania te zostaną sformułowane w sposób wykluczający odpowiedzialność państwa. W takim przypadku emitowane przez państwo poświadczenia tożsamości będą mogły służyć jedynie jako dane referencyjne dla innych systemów elektronicznej tożsamości, w których dostawcą usługi zaufania nie będzie instytucja publiczna.

3.8 Uwierzytelnienie autonomiczne i sfederowane

W obecnym stanie prawnym jedyną obowiązującą w Polsce metodą uwierzytelnienia o walorze powszechnej użyteczności jest kwalifikowany podpis elektroniczny. Inne metody uwierzytelnienia, reprezentujące lepszy bilans kosztu do wiarygodności i ryzyka, mają znaczenie ograniczone z reguły do jednego wystawcy i zarazem podmiotu akceptującego. Tymczasem w świecie trend do federacji usług dostawców tożsamości zaznacza się jako jedna z najbardziej istotnych i aktualnych tendencji w zakresie elektronicznej tożsamości. Wydaje się, że zarówno rynek, jak i administracja publiczna przyjęły do wiadomości, że modele uwierzytelnienia zalecane do tej pory zarówno w warstwie prawnej, jak obowiązujących standardach technicznych, zostały jedynie w ograniczonym stopniu zaakceptowane przez potencjalnych odbiorców. Skutkiem takiego stanu rzeczy jest rozwój nowych modeli uwierzytelnienia, funkcjonujących bez wystarczających podstaw prawnych lub normatywnych, jednak rozwijających się dzięki temu, że dobrze odpowiadają potrzebom swych twórców i odbiorców. W opisanej sytuacji trzeba się liczyć z rozwojem różnorodnych, nowych modeli i form uwierzytelnienia, o naturze na tyle rozbieżnej, że trudne okaże się objęcie ich wspólnymi standardami prawnymi lub technicznymi. Zjawisko to z jednej strony pobudza kreatywność i konkurencję prowadząc do ukształtowania efektywnych modeli uwierzytelnienia. Z drugiej jednak strony prowadzi do segmentacji rynku usług zaufania i braku interoperacyjności różnych modeli uwierzytelnienia. Odpowiedzią rynku na zarysowane zjawisko jest federacja usług zaufania, sprowadzająca się do uznawania przez potencjalnych odbiorców usług różnych modeli uwierzytelnienia o zbliżonym profilu ryzyka, w tym także usług świadczonych przez podmioty trzecie. Klasycznym przykładem takiego modelu biznesowego jest coraz powszechniejsza w serwisach internetowych możliwość uwierzytelnienia z wykorzystaniem mechanizmów najbardziej popularnych portali społecznościowych.

Opisany stan rzeczy jest silnie odczuwany w Unii Europejskiej, gdzie podziały natury technicznej nakładają się na mozaikę jurysdykcji prawnej tworząc znaczące bariery dla rozwoju wspólnego rynku.

W wyniku realizacji projektów IDABC oraz STORK (por. 4.3 oraz 4.4) UE zyskała techniczne możliwości federacji usług zaufania, jednak nierozwiązana pozostała bariera natury prawnej: większość spośród usług zaufania dostępnych w krajach członkowskich ma moc prawną wiążącą jedynie w kraju pochodzenia. O ile można dopuścić ich wykorzystanie w innych krajach dla udostępnienia usług o wyłącznie informacyjnym charakterze, brak możliwości ich użycia związanego ze składaniem oświadczeń woli. Zapewne między innymi z tego właśnie powodu UE podjęła prace nad projektem rozporządzenia w sprawie identyfikacji elektronicznej i usług zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznym - eIDAS. Jedną z zasadniczych nowości w projekcie jest próba stworzenia podstaw prawnych dla systemu usług zaufania o zasięgu ogólnoeuropejskim. Kwestie związane z transgranicznymi usługami zaufania zostaną omówione w kolejnym punkcie, niniejszy poświęcony jest federacji usług zaufania na poziomie krajowym. Jak zasygnalizowano w rozdziale 3.4 projekt rozporządzenia eIDAS przewiduje możliwość świadczenia usług zaufania, które wcześniej nie były regulowane (co najmniej na poziomie prawa UE), a w konsekwencji ich status prawny był nieokreślony poza obszarem, dla którego strony uznały je kontraktowo za wiążący. Wejście w życie rozporządzenia eIDAS sprawi, że liczne usługi zaufania zyskają wiążący charakter z mocy prawa. Sam ten fakt będzie stanowić przesłankę dla ich federacji – wzajemnego uznawania przez różnych dostawców usług i/lub emisji poświadczeń tożsamości na podstawie poświadczeń wydanych przez innego dostawcę usług zaufania (zob. także w 6.6)

3.9 Uwierzytelnienie transgraniczne

Jedyną formą transgranicznego uznania poświadczeń tożsamości w obecnej rzeczywistości prawnej jest wspomniana wyżej harmonizacja z wykorzystaniem list TLS. Projekt eIDAS wprowadza w tym zakresie zasadę rynku wewnętrznego (*[p]rodukty spełniające wymagania niniejszego rozporządzenia dopuszcza się do swobodnego obrotu na rynku wewnętrznym*) oraz zasadę wzajemnego uznania (*[j]eżeli zgodnie z prawem krajowym lub praktyką administracyjną dostęp do usługi online wymaga identyfikacji elektronicznej przy użyciu środka identyfikacji elektronicznej oraz uwierzytelnienia, na potrzeby dostępu do tej usługi uznaje się i akceptuje wszystkie środki identyfikacji elektronicznej wydane w innym państwie członkowskim i objęte systemem uwzględnionym na liście publikowanej przez Komisję zgodnie z procedurą, o której mowa w art. 7*) wszystkich usług zaufania objętych zakresem rozporządzenia.

Dla zapewnienia realizacji tych zasad przewidziano wymóg zgłaszania opisanych środków identyfikacji elektronicznej Komisji Europejskiej, której przysługuje prawo weryfikacji ich zgodności z przepisami projektowanego rozporządzenia. Należy zauważyć, że obowiązek zgłaszania systemów identyfikacji elektronicznej dotyczy systemów wydanych *przez zgłaszające państwo członkowskie, w jego imieniu lub na jego odpowiedzialność*. Wymóg ten jednoznacznie odzwierciedla intencję nowego aktu prawnego, zgodnie z którą fundamentem infrastruktury zaufania na wspólnym rynku będą usługi zaufania świadczone raczej przez państwa członkowskie, a nie, jak do tej pory, przez instytucje sektora prywatnego. Równouprawnienie instytucji sektora prywatnego w dostępie do usług zaufania świadczonych przez instytucje publiczne gwarantuje przepis, zgodnie z którym *zgłaszające państwo członkowskie gwarantuje dostępność mechanizmów uwierzytelniania online w dowolnym czasie i nieodpłatnie, tak aby wszystkie strony ufające mogły dokonać weryfikacji danych identyfikujących osobę otrzymanych w formie elektronicznej*. Wymóg ten obowiązuje bez różnicowania stron ufających reprezentujących różne sektory (publiczny lub prywatny) i państwa członkowskie. Możliwość nieodpłatnej

i ciągłej weryfikacji danych identyfikujących osobę w połączeniu z gwarancją, że *dane osobowe związane z identyfikacją są jednoznacznie przypisywane do osoby fizycznej lub prawnej* otwiera drzwi do pełnej federacji usług zaufania w skali wspólnego rynku krajów UE. Co więcej, dzięki produktom projektu STORK UE dysponuje narzędziami technicznymi eliminującymi najważniejszą słabość opisanego sposobu federalizacji usług zaufania – konieczność organizacji sieci *many-to-many*. Produkty STORK pozwalają na stosunkowo łatwą organizację pan-europejskiego brokera tożsamości, tłumaczącego żądania weryfikacji pochodzące z jednego systemu krajowego na protokoły właściwe dla kraju pochodzenia weryfikowanego poświadczenia tożsamości.

Nie oznacza to, że propozycje zawarte w projekcie eIDAS są wolne od potencjalnych słabości. Projekt przewiduje procedurę zgłoszenia KE systemów identyfikacji elektronicznej, nie przewiduje jednak w obecnej formie jakiegokolwiek procedury weryfikacji, czy zgłaszane systemy odpowiadają wymogom rozporządzenia i wynikającym z innych aktów prawnych wymogom bezpieczeństwa i poufności. Każde państwo członkowskie jest zobowiązane do wyznaczenia organu sprawującego nadzór nad działającymi na jego terenie dostawcami kwalifikowanych usług zaufania. Zważywszy jednak, że systemy zgłaszane na podstawie przepisów rozporządzenia są z definicji systemami wydanymi *przez zgłaszające państwo członkowskie, w jego imieniu lub na jego odpowiedzialność*, nadzór sprawowany przez jeden organ państwa nad działalnością innego organu – dostawcy usług zaufania, może okazać się niewystarczająco skuteczny. Wydaje się, że w projekcie rozporządzenia brakuje elementu audytu zgłaszanych systemów przez agencję niezależną od zgłaszającego państwa.

Niezależnie od opisanej słabości projekt rozporządzenia eIDAS dostarcza podstaw prawnych dla budowy pan-europejskiego systemu elektronicznej identyfikacji i usług zaufania. Będą w nim jednak uczestniczyć jedynie obywatele i osoby prawne z tych krajów członkowskich, które zbudują i zgłoszą zgodnie z przepisami rozporządzenia skuteczne, krajowe systemy elektronicznej identyfikacji.

3.10 Polityki i procedury

Ważnym elementem budowania zaufania do usługi uwierzytelnienia jest istnienie odpowiedniej dokumentacji dotyczące prowadzonej działalności, a dostępnej publicznie, dla wszystkich interesariuszy w procesie identyfikacji i uwierzytelniania, w szczególności dla strony ufającej. Instytucja (jednostka) dostarczająca takie usługi powinna opracować i opublikować co najmniej politykę oraz regulamin (ang. *practice statement*) i/lub procedury - podobnie jak ma to miejsce w przypadku świadczenia usług certyfikacyjnych zgodnie z dyrektywą 1999/93/EC i polskiej ustawy o podpisie elektronicznym.

W polityce identyfikacji i uwierzytelnienia określa się m.in. cel i zakres działań, role i odpowiedzialność pracowników, zasady zapewnienia zgodności i bezpieczeństwa. W regulaminie i procedurach określa się sposób osiągnięcia w/w celów. Dokumenty te powinny być przeglądane i aktualizowane cyklicznie.

Takie podejście jest prezentowane zarówno w standardach dot. podpisu elektronicznego (standardy ETSI związane z dyrektywą 99/93/EC) i usług zaufania (nowe standardy ETSI związane z rozporządzeniem eIDAS), jak i w nowej normie ISO 29115, czy amerykańskim standardzie NIST SP 800-53.

4 Identyfikacja i uwierzytelnienie w standardach

Kwestia standaryzacji obszaru elektronicznej identyfikacji i uwierzytelnienia doczekała się co najmniej kilku znaczących opracowań, które mogą (i powinny) stanowić podwaliny budowanych informatycznych systemów realizujących usługi drogą elektroniczną. Te opracowania ustanawiają standardy, ale należą do różnych kategorii: 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, uwierzytelnienia elektronicznego i szeroko pojętych systemów dostawców usług elektronicznych.

Najważniejszymi dokumentami, na których opiera się niniejszy raport, są:

- akty prawne związane z podpisem elektronicznym, w szczególności:
 - dyrektywa UE 93/99/EC;
 - polska ustawa o podpisie elektronicznym;
 - rozporządzenie Rady Ministrów 1094 z dnia 7 sierpnia 2002 r. w sprawie warunków technicznych i organizacyjnych dla kwalifikowanych podmiotów;
 - Decyzja Komisji 2003/511/EC,
 - rozporządzenie Parlamentu Europejskiego i Rady w sprawie identyfikacji elektronicznej i usług zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznym rozporządzenia Komisji Europejskiej (projekt),
- dokumenty wytworzone w ramach projektu Komisji Europejskiej IDABC,
- dokumenty wytworzone w ramach projektu STORK,
- norma ISO 29115,
- standard NIST SP 800-53,
- opracowanie „Identity and Access Management: Assurance and Authentication Guidelines” rządu Stanu Kolorado w USA,
- standardy ETSI,
- standardy CWA (CEN Workshop Agreement).

W dalszej części rozdziału opisane są najważniejsze z nich.

4.1 Podpis elektroniczny

Według definicji zawartej w art. 3 ustawy o podpisie elektronicznym, podpis elektroniczny to:

„dane w postaci elektronicznej, które wraz z innymi danymi, do których zostały dołączone lub z którymi są logicznie powiązane, służą do identyfikacji osoby składającej podpis elektroniczny”.

Przytoczona definicja opiera się na podobnej, zawartej w dyrektywie 99/93/UE; podpis elektroniczny w rozumieniu art. 2 pkt 1 Dyrektywy oznacza

Identyfikacja i uwierzytelnianie w usługach elektronicznych

„dane w formie elektronicznej dodane do innych danych elektronicznych lub logicznie z nimi powiązane i służące jako metoda uwierzytelnienia”.

Jak wynika z definicji ustawowej podpisem elektronicznym jest każda możliwa elektroniczna forma identyfikacji osób fizycznych, w tym np. e-mail, która ujawniałaby dane personalne osoby nadawcy. Podpisem elektronicznym w rozumieniu ustawy są oprócz podpisów opartych na kryptografii symetrycznej lub asymetrycznej, np.: dane personalne załączone do listu w poczcie elektronicznej, hasło jednorazowe¹⁰ wraz z innymi danymi przekazywanymi podczas logowania do serwera bankowego. Warto dodać, że sam PIN nie spełnia warunku niepowtarzalności zawartego w definicji ustawowej danych służących do składania podpisu elektronicznego (*niepowtarzalne i przyporządkowane osobie fizycznej dane, które są wykorzystywane przez tę osobę do składania podpisu elektronicznego*), jednak stosowany jest zwykle z kartą, która posiada walor unikalności (numer seryjny) w związku z czym PIN użyty razem z kartą płatniczą jest pewnym rodzajem podpisu elektronicznego. Podobnie imię i nazwisko zapisane na końcu tekstu e_mail'a nie spełnia warunku „unikalności” zapisanego w definicji danych służących do składania podpisu elektronicznego. Osoba polegająca na takim „podpisie elektronicznym” musi dysponować dodatkowymi danymi, które pozwoliłyby na jednoznaczną identyfikację autora. Za podpis elektroniczny nie będzie można uznać również samego pliku video, z którego można poznać tożsamość osoby, konieczne jest bowiem, aby podpis elektroniczny był dołączany lub powiązany z danymi podpisywanymi.

Najpowszechniejszy sposób składania podpisu elektronicznego opiera się na kryptografii asymetrycznej. Systemy takie wymagają istnienia dwóch komplementarnych kluczy A i B. Wiadomość zaszyfowaną kluczem A można odszyfrować kluczem B i odwrotnie – zaszyfowaną 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 elektroniczny. Drugi klucz, komplementarny do prywatnego, jest publicznie znany – służy do weryfikacji złożonego podpisu elektronicznego. Należy odnotować, że aktualnie podpisy elektroniczne, zarówno *zwykłe*, jak i *bezpieczne* („kwalifikowane”), są implementowane z wykorzystaniem infrastruktury klucza publicznego (PKI) i technik kryptografii asymetrycznej. W wielu publikacjach i wypowiedziach autorzy upatrują różnice między „zwykłymi” i „kwalifikowanymi” podpisami elektronicznymi tylko w tym, że do złożenia „zwykłego” podpisu nie zastosowano kryptograficznej karty elektronicznej i/lub kwalifikowanego certyfikatu. Takie podejście - bardzo często spotykane, również w dokumentach UE - jest zawężeniem definicji ustawowej w stosunku do „zwykłego” podpisu. W dalszej części tego rozdziału pojęcie *podpisu elektronicznego* będzie właśnie tożsamy z zastosowaniem technik kryptografii asymetrycznej opartych o PKI.

4.1.1 Podobieństwa i różnice między podpisem elektronicznym i tradycyjnym (własnoręcznym)

Podpis elektroniczny jest najczęściej wynikiem zaszyfrowania wartości funkcji skrótu¹¹ danych podpisywanych za pomocą danych służących do złożenia podpisu elektronicznego (klucza prywatnego). Tym samym podpis elektroniczny 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 elektronicznego opartego o technologię cyfrową jest zmienna w zależności od

¹⁰ Niezależnie czy generowane ad hoc przez tzw. token, czy pochodzące z tzw. zdrapki.

¹¹ Por. rozdział 0.

Identyfikacja i uwierzytelnianie w usługach elektronicznych

treści danych podpisywanych. Jeżeli danymi służącymi do składania podpisu elektronicznego zaszyfruje się identyczną treść, to wynik, w postaci podpisu elektronicznego, będzie zawsze taki sam¹². Natomiast opatrzenie podpisem danych o różnej treści zawsze da odmienną postać podpisu elektronicznego. Tak więc, mimo złożenia podpisu elektronicznego za pomocą tych samych danych służących do jego złożenia, podpis będzie miał zmienną postać elektroniczną. W przeciwieństwie do podpisu własnoręcznego cechą podpisu elektronicznego, która powoduje pewne niewielkie ograniczenie jego zastosowania, jest brak możliwości złożenia go *in blanco*. Jest to konsekwencją zalety tego narzędzia, która polega na zapewnieniu integralności podpisywanych danych. Innymi słowy jakkolwiek zmiana tych danych powoduje, że nie można ich powiązać z podpisem elektronicznym, 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 elektroniczny będzie można przyporządkować li tylko do danych w postaci podpisanej pierwotnie. Podpis elektroniczny jest ważny bezterminowo jeśli został złożony w okresie ważności certyfikatu służącego do jego weryfikacji. Zwykle jednak dowodem czasu złożenia takiego podpisu jest znacznik czasu, który *de facto* jest też pewnego rodzaju podpisem elektronicznym i podlega tym samym ograniczeniom związanym z postępem technologicznym. 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 podpisu elektronicznego i poprzednich znaczników 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.

Podobieństwa między podpisem własnoręcznym i podpisem elektronicznym:

- służą do identyfikacji/uwierzytelnienia osoby,
- zwykle stanowią dowód złożenia oświadczenia woli.

Odmienności podpisu elektronicznego:

- podpis elektroniczny nie istnieje w postaci graficznej lub innej materialnej,
- nie można go złożyć w oderwaniu od podpisywanych danych,
- jest zmienny,
- 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,
- nie odzwierciedla cech fizycznych osoby,
- jest składany za pomocą specjalistycznych urządzeń,
- można posiadać więcej niż jeden „podpis elektroniczny”.

¹² Istnieją techniki kryptograficzne, które do szyfrowania dodają pewien element losowy, niezależny od treści szyfrowanych danych

4.1.2 Rodzaje podpisu elektronicznego wg dyrektywy 93/99/EC

Jak wspomniano na wstępie tego rozdziału dyrektywa UE posługuje się pojęciem „uwierzytelnienia”, natomiast polska ustawa odwołuje się do „identyfikacji”. Ta pozorna rozbieżność wynika z faktu, że inne dokumenty Europejskiego Komitetu Normalizacyjnego¹³ określają cztery podstawowe funkcje podpisu elektronicznego, gdzie **identyfikacja** jest najszerszą z możliwych:

- 1) identyfikacja (ang. *identification*),
- 2) uwierzytelnienie (ang. *authentication*),
- 3) oświadczenie wiedzy (ang. *declaration of knowledge*),
- 4) oświadczenie woli (ang. *declaration of will*).

Podpisy składane w celu **identyfikacji** (*Signatures for Identification*) służą wyłącznie do udowodnienia posiadania klucza prywatnego, tzw. *proof-of-possession of the private key*. Podpisy i certyfikaty służą w tym przypadku tylko do uwierzytelnienia w systemie i identyfikacji osoby starającej się o dostęp, np. do serwera, bazy danych itp. Identyfikacja opiera się na podpisaniu losowych danych przesłanych przez żądający identyfikacji serwer i weryfikacji tak złożonego podpisu cyfrowego. W przypadku poprawności żądający uwierzytelnienia ma pewność, że zweryfikował osobę, która posiada dany klucz prywatny. Unikalność klucza oraz jego poufność pozwalają przyjąć, że zweryfikowanym jest uprawniona osoba. Taka metoda uwierzytelnienia może zostać uznana za wystarczającą do celów identyfikacji, ale nie do celów oświadczenia woli. Podpisujący bowiem z reguły podpisuje dane całkowicie dla niego niezrozumiałe i mające charakter losowy, nie zawierające żadnego oświadczenia woli. Niestety istnieje ryzyko, że przesłane do podpisu dane, zamiast być całkowicie losowe, reprezentują jakąś zrozumiałą treść, w tym w szczególności oświadczenie woli niekorzystne dla podpisującego, choć nieznanie podpisującemu. Celem ograniczenia tego niebezpieczeństwa zwykle stosuje się inną parę kluczy (i tym samym inny certyfikat) do „identyfikacji” on-line, a inną do pozostałych rodzajów podpisu elektronicznego. Konieczność korzystania z dwóch oddzielnych certyfikatów może wydawać się uciążliwa, jednak w przypadku korzystania z tego samego urządzenia nie powinno to sprawiać żadnych kłopotów. Ponadto jest zasadne ze względu na bezpieczeństwo obrotu prawnego. Należy również dodać, że decyzja 511 Komisji Europejskiej z 14 lipca 2003 roku rekomenduje nielączenie certyfikatów wskazujących na podpisy elektroniczne jako oświadczenie woli z jakimikolwiek innymi zastosowaniami, np. „identyfikacji”.

Podpisy składane w celu **uwierzytelnienia** (*Signatures for Authentication*) są składane całkowicie automatycznie bez świadomości i ingerencji osoby składającej i nie służą do składania oświadczeń woli. Są to podpisy składane przez urządzenia, więc nie występują w krajach takich jak Polska, gdzie obowiązujące obecnie prawo łączy „podpis” z osobą fizyczną.

Podpisy składane jako **oświadczenie wiedzy** (*Signatures for declaration of knowledge*) nie służą do składania oświadczeń woli. Podpis ten służy, np. do potwierdzenia zapoznania się z dokumentem, czy odebrania dokumentu, nie stanowi jednak dowodu, że został on zatwierdzony, czyli że zawiera treść zaakceptowaną przez podpisującego. Tak więc błąd, podstęp, czy groźba przy jego składaniu nie mają większego znaczenia, gdyż podpisanie się na danym dokumencie stanowi jedynie dowód, że podpisujący miał go w posiadaniu. Służy więc m.in. do potwierdzenia prawdziwości dokumentu. Ten rodzaj podpisu ma zastosowanie np. w sytuacji elektronicznego notariatu. Notariusz nie składa bowiem podpisu na akcie notarialnym celem złożenia oświadczenia woli, lecz tylko celem uwiarygodnienia podpisanego dokumentu

¹³ Pkt. 4.2.2 CWA 14365 „Guide on the use of Electronic Signatures”

i potwierdzenia, że zostały dopełnione wszelkie wymagania przewidziane prawem. Zgodnie z aktualnym trendem ten typ podpisu nie będzie osiągany poprzez modyfikację treści rozszerzenia certyfikatu *extKeyUsage* i wskazanie typu np. „niezaprzeczalność dostarczenia”. Można się spodziewać, że zapewne będzie wdrażany poprzez odpowiednie doprecyzowanie w *atrybucie podpisu* lub poprzez informacje zawarte w samej treści podpisywanego dokumentu. Należy podkreślić, że atrybut podpisu może być automatycznie wprowadzany przez system teleinformatyczny.

Podpisy składane pod **oświadczeniem woli** (*Signatures as declaration of will*) stanowią dowód złożenia oświadczenia woli. Co oczywiste, winny być składane po zaznajomieniu się z treścią podpisywanego dokumentu oraz zgodne z intencją jego podpisania, a także pod pełną kontrolą podpisującego. Podpisy te są składane, m.in. w oparciu o certyfikat, który w polu *keyUsage* zawiera tylko bit *contentCommitment*¹⁴.

Jak wynika z powyższego każdy rodzaj podpisu elektronicznego może stanowić dowód, ale tylko nieliczne mogą potwierdzać oświadczenie woli. Tak więc podpis celem identyfikacji może stanowić dowód uzyskania dostępu do danej bazy danych przez konkretną osobę dysponującą kluczem prywatnym w określonym czasie. Podpis celem uwierzytelnienia stanowi dowód zapoznania się z treścią dokumentu. Każdy z tych podpisów powinien zostać dopuszczony do postępowania sądowego zgodnie z art. 5 ust. 2 dyrektywy UE i art. 8 ustawy o podpisie elektronicznym. **Fakt, że podpis elektroniczny nie będzie stanowił dowodu oświadczenia woli, nie oznacza, że nie może stanowić dowodu na inną okoliczność, np. integralność, czy dystrybucję nielegalnych kopii oprogramowania.**

Mając na uwadze powyższe należy pamiętać, że skutki prawne podpisu elektronicznego muszą być oceniane uwzględniając m.in. kontekst jego złożenia. Takie podejście zostało wdrożone np. w rozporządzeniu Ministra Edukacji Narodowej i Sportu z dnia 18 lipca 2005 r. w sprawie dokumentacji przebiegu studiów (Dz. U. nr 149, poz. 1233). Załącznik nr 3 tego rozporządzenia zawiera szczegóły elektronicznych struktur danych zapisanych w legitymacji studenckiej, która jest elektroniczną kartą procesorową. Dla potrzeb weryfikacji elektronicznej dane studenta są podpisywane bezpiecznym podpisem elektronicznym w rozumieniu ustawy o podpisie elektronicznym, upoważnionej przez władze uczelni osoby. Nie jest ten podpis związany z oświadczeniem woli, a jego charakter ujawnia obligatoryjny atrybut podpisu zawierający „rodzaj zobowiązania” (ang. *commitmentType*) z identyfikatorem obiektu { 1 2 840 113549 1 9 16 6 5 }, wskazującym, że „podpisujący zaaprobował podpisywane dane”.

Należy również zauważyć, że powyższe rodzaje podpisu elektronicznego nie odbiegają od zastosowań podpisu własnoręcznego, choć słusznie zauważa się, że zastosowanie podpisu elektronicznego może być dużo szersze niż podpisu własnoręcznego. Podpis elektroniczny nie jest bowiem zawsze stosowany tylko do składania oświadczeń woli.

4.1.3 Rodzaje podpisu elektronicznego wg projektu rozporządzenia eIDAS

W świetle doprecyzowań funkcji podpisu elektronicznego zawartych w dokumencie CWA 14365 należy stwierdzić, że zarówno definicja podpisu elektronicznego zawarta w dyrektywie 93/99/EC, jak i zastosowana w polskiej ustawie o podpisie elektronicznym, nie uwzględnia wszystkich rodzajów podpisów elektronicznych. Definicja ta powinna być mniej więcej następująca:

¹⁴ wcześniej *nonRepudiation*

podpis elektroniczny – dane w postaci elektronicznej, które wraz z innymi danymi, do których zostały dołączone lub z którymi są logicznie powiązane, służą do identyfikacji osoby składającej podpis elektroniczny, uwierzytelnienia tej osoby lub składania przez nią różnego rodzaju oświadczeń.

Nowe rozporządzenie eIDAS oparte jest na całkowicie nowym podejściu do kwestii funkcji podpisów elektronicznych w rozumieniu dyrektywy 93/99/EC. W projekcie eIDAS oddzielono funkcję „identyfikacji” do osobnej kategorii, a pozostałe rodzaje podpisów elektronicznych podzielono na „podpis elektroniczny”, który jest zawsze składany przez osobę fizyczną i „pieczęć elektroniczną”, która jest składana przez osobę prawną („automatycznie” przez sprzęt i/lub oprogramowanie):

- **identyfikacja elektroniczna** – oznacza proces używania danych identyfikujących osobę w formie elektronicznej, w sposób jednoznaczny reprezentujący osobę fizyczną lub prawną;
- **uwierzytelnianie** – oznacza proces elektroniczny, który umożliwia weryfikację identyfikacji elektronicznej osoby fizycznej lub prawnej lub pochodzenia i integralności danych elektronicznych;
- **podpis elektroniczny** – oznacza dane w formie elektronicznej dodane do innych danych elektronicznych lub logicznie z nimi powiązane i służące podpisującemu do składania podpisu;
- **pieczęć elektroniczna** – oznacza dane w formie elektronicznej dodane do innych danych elektronicznych lub logicznie z nimi powiązane, aby zagwarantować pochodzenie i integralność powiązanych danych.

Powodem oddzielnego uregulowania kwestii identyfikacji nie jest inna interpretacja norm i standardów przez autorów projektu eIDAS, a jedynie kwestie formalnoprawne w Unii Europejskiej. Otóż aspekt identyfikacji i nierozzerwalnie z tym związany problem dowodów tożsamości, przez wiele lat nie były w ogóle rozpatrywane na poziomie UE. Skutkiem tego 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:

„Jeżeli działanie Unii okazuje się niezbędne do ułatwienia wykonywania prawa, o którym mowa w artykule 20 ustęp 2 litera a) (swobodnego przemieszczania się i przebywania na terytorium Państw Członkowskich – przyp. red.), a Traktaty nie przewidują stosownych uprawnień do działania w tym zakresie, Rada, stanowiąc zgodnie ze specjalną procedurą ustawodawczą, może przyjąć przepisy dotyczące paszportów, dowodów tożsamości, dokumentów pobytowych lub jakichkolwiek innych podobnych dokumentów. Rada stanowi jednomyślnie po konsultacji z Parlamentem Europejskim.”

W związku z powyższym rozporządzenie eIDAS ma inne cele w stosunku do aspektów identyfikacji on-line, a inne do funkcji podpisów elektronicznych, rozumianych jako składanie oświadczeń lub zapewniających gwarancję pochodzenia i integralności danych. 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) narzuci jednolite formaty, które zapewnią transgraniczne uznawanie podpisów elektronicznych, szczególnie ich „kwalifikowanych” wersji, czyli opartych o kwalifikowane certyfikaty.

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

4.2 Standardy ETSI i CWA

W ramach implementacji dyrektywy Parlamentu Europejskiego i Rady 1999/93/WE z dnia 13 grudnia 1999 r. w sprawie wspólnotowych ram w zakresie podpisów elektronicznych Komisja Europejska zleciła Europejskiemu Instytutowi Norm Telekomunikacyjnych (ETSI) i Europejskiemu Komitetowi Normalizacyjnemu (CEN) opracowanie szeregu standardów. Dokumenty te z jednej strony miały dawać rządowi wskazówki poprawnej implementacji dyrektywy do systemu prawnego danego kraju, a z drugiej strony niektóre z nich są elementem aktów wykonawczych (decyzji Komisji) wydanych na podstawie delegacji zawartych w dyrektywie. Należy odnotować, że rozporządzenie eIDAS zawiera analogiczne rozwiązanie, tj. szczegółowe wymagania zostaną narzucone w formie aktów wykonawczych, które będą opierały się na normach i standardach.

„Specyfikacje techniczne” ETSI (ang. *Technical Specification* - TS) i „uzgodnienia robocze” CEN (ang. *CEN Workshop Agreement* – CWA) to łącznie kilkadziesiąt dokumentów. Omówienie wszystkich przekracza ramy niniejszego raportu, natomiast należy odnotować, że oba gremia standaryzacyjne w niektórych aspektach technicznych stworzyły zapisy, które są niekomplementarne. W związku z tym przede wszystkim trzeba brać pod uwagę te dokumenty, których obligatoryjność została narzucona decyzją Komisji 2003/511/EC, czyli:

- CWA 14169 – wymagania dla bezpiecznych urządzeń do składania podpisu elektronicznego¹⁵;
- CWA14167-1 – wymagania dla podmiotów świadczących usługi certyfikacyjne¹⁶;
- CWA 14167-2 – profil zabezpieczeń dla modułów sprzętowych stosowanych przez CA przy świadczeniu usług certyfikacyjnych¹⁷

Zwraca się uwagę, że standard CWA 14167-1 definiuje szczegółowe wymagania dla podmiotów świadczących usługi certyfikacyjne, zarówno dla wydających kwalifikowane, jak i „zwykłe” certyfikaty. Praktycznie rozciąga on wymagania dla „kwalifikowanych podmiotów” również na „zwykłe podmioty”, a wyłączenia wymagań dla „zwykłych” CA mają charakter drugorzędny i są następujące:

1. Każde centrum certyfikacji (CA) musi zapewnić obsługę systemów teleinformatycznych przez personel, którego role są następujące:

- 1) "Inspektor Bezpieczeństwa";
- 2) "Inspektor do spraw Rejestracji";
- 3) "Administrator Systemu";
- 4) "Operator Systemu";
- 5) "Inspektor do spraw Audytu".

„Zwykły” podmiot musi rozdzielić funkcje 1) i 5), natomiast „kwalifikowany” musi rozdzielić dodatkowo 1 z 2, 3 z 1 oraz 3 z 5.

¹⁵ CWA 14169: secure signature-creation devices

¹⁶ CWA 14167-1: security requirements for trustworthy systems managing certificates for electronic signatures — Part 1: System Security Requirements

¹⁷ CWA 14167-2: security requirements for trustworthy systems managing certificates for electronic signatures — Part 2: cryptographic module for CSP signing operations — Protection Profile (MCSO-PP)

Identyfikacja i uwierzytelnianie w usługach elektronicznych

2. „Kwalifikowane” CA musi zapewnić synchronizację swoich zegarów z dokładnością do 1 sekundy w stosunku do UTC, natomiast „zwykłe” CA musi zapewnić wiarygodny czas, bez doprecyzowania synchronizacji z UTC. Synchronizacja jest z kolei obowiązkowa w przypadku każdego podmiotu świadczącego usługę znakowania czasem.

3. Wydając kwalifikowany certyfikat musi być zapewnione zapisanie momentu stworzenia zgłoszenia certyfikacyjnego oraz musi być wskazany sposób zweryfikowania ważności certyfikatu, umożliwiającą właścicielowi kontrolę statusu certyfikatu.

4. Wszystkie certyfikaty muszą zawierać:

- nazwę właściciela lub pseudonim (ewentualne użycie pseudonimu musi być wyraźnie wskazane);
- klucz publiczny właściciela;
- bezpieczny podpis elektroniczny wydawcy;
- numer seryjny i nazwę wyróżniającą wydawcy;
- okres ważności (“nie wcześniej niż” oraz “nie później niż”);
- wskazanie polityki certyfikacji, w ramach której certyfikat został wydany.

„Kwalifikowany” certyfikat musi dodatkowo być zgodny z profilem określonym w specyfikacji technicznej ETSI TS 101 862.

Warto też odnotować, że dokument ten nakazuje, zarówno „zwykłym”, jak i „kwalifikowanym” podmiotom:

- utrzymywać w sprawności usługi związane z odwoływaniem certyfikatów na poziomie 99.9% czasu pracy i to w odniesieniu do okresów miesięcznych. Przyjmując, że typowo miesiąc ma 30 dni dostajemy maksymalny czas niedostępności systemu CA na poziomie niecałej jednej godziny,
- zapewnić alternatywne systemy teleinformatyczne w przypadku katastrof,
- używać do składania podpisów elektronicznych na certyfikatach HSM-ów spełniających te same wysokie wymagania oraz tylko algorytmów szyfrowych i ich parametrów opisanych w tzw. ALGO¹⁸,
- samo użycie autocertyfikatu nie jest wystarczające do dystrybucji „punktu zaufania” dla początku ścieżki certyfikacji,
- tworzyć dzienniki zdarzeń i przechowywać je w celu zapewnienia funkcji kontrolnych, w tym archiwizować wszystkie wydane certyfikaty, CRL-e i ARL-e,
- wydając certyfikat (zarówno „zwykły” jak i „kwalifikowany”) inspektor ds. rejestracji musi sprawdzić zgodnie z prawem krajowym tożsamość właściciela certyfikatu oraz inne atrybuty osoby, które byłyby zawarte w certyfikacie,
- umożliwić odwołanie certyfikatu, przy czym maksymalny czas potrzebny na opublikowanie informacji o zmianie statusu certyfikatu nie może być dłuższy niż 24 godz. Baza danych związana z CRL-ami i/lub OCSP musi być aktualizowana nie rzadziej niż raz dziennie nawet gdy nie ma zmiany,
- stosując usługę OCSP¹⁹ podmiot musi zapewnić bezpieczny kanał do przesyłania informacji i zapewnić odporność na ataki typu „*denial of service attacks*” i „*replay attacks*”, jak również

¹⁸ ETSI TS 102 176 - Electronic Signatures and Infrastructures (ESI); Algorithms and Parameters for Secure Electronic Signatures

¹⁹ On-line Certification Status Protocol

Identyfikacja i uwierzytelnianie w usługach elektronicznych

zawrzeć w odpowiedzi oznaczenie czasu wg którego należy rozpatrywać status danego certyfikatu. Warto zaznaczyć, że podmiot stosujący OCSP musi archiwizować wszystkie zapytania i odpowiedzi związane z tą usługą.

Polska ustawa o podpisie elektronicznym i rozporządzenie 1094, zawierające szczegółowe wymagania dla podmiotów świadczących kwalifikowane usługi certyfikacyjne, nie są sprzeczne z decyzją Komisji 2003/511/EC, ale przepisy unijne zawierają więcej wymagań, szczególnie w odniesieniu do „zwykłych” usług. Innymi słowy polskie uregulowania nie zawierają przepisów, które byłyby w sprzeczności z decyzją Komisji, ale implementujący musi mieć świadomość, że w Polsce, od 1 maja 2004 r. (data wejście RP do Unii) obowiązują również decyzje i rozporządzenia UE, które są bezpośrednią implementacją prawa unijnego na obszarze wspólnoty.

Jeśli chodzi o standardy ETSI to dla aspektów identyfikacji i podpisów elektronicznych najważniejsze są specyfikacje techniczne określające tzw. formaty podpisanych wiadomości:

- ETSI TS 101 903 (XAdES),
- ETSI TS 101 733 (CAdES),
- ETSI TS 102 778 (PAdES),

oraz profil (format) certyfikatu kwalifikowanego – ETSI TS 101 862.

Formaty podpisanych wiadomości są dodatkowo doprecyzowane w decyzji Komisji 2011/130/UE²⁰. Tworzenie aplikacji zgodnych z tymi formatami jest bardzo pożądane, aczkolwiek formalnie formaty te jeszcze nie są obligatoryjne. Wynika to z faktu, że art. 1 ust. 2 tej decyzji zawiera możliwość zastosowania innych rozwiązań:

Państwa członkowskie, których właściwe organy podpisują dokumenty, o których mowa w ust. 1 (XAdES, CAdES i PAdES – przyp. red.), przy użyciu innych formatów podpisu elektronicznego niż formaty, o których mowa w tym samym ustępie, powiadają Komisję o istniejących możliwościach weryfikacji, za pomocą których pozostałe państwa członkowskie mogą weryfikować otrzymane podpisy elektroniczne w trybie online, nieodpłatnie i w sposób zrozumiały dla osób niebędących rodzimymi użytkownikami języka, chyba że niezbędne informacje są już zawarte w dokumencie, w podpisie elektronicznym lub w elektronicznym nośniku dokumentu. Komisja udostępni te informacje wszystkim państwom członkowskim.

Natomiast profil certyfikatu kwalifikowanego jest obligatoryjny, gdyż jest wskazany jako obowiązkowy w CWA 14167-1, czyli jest narzucony decyzją Komisji 2003/511/EC. Jest bardzo prawdopodobne, że rozporządzenie eIDAS, a właściwie akty wykonawcze do tego rozporządzenia, również narzuci obowiązek stosowania jednego z kilku, zdefiniowanych w specyfikacjach technicznych ETSI, formatów podpisanych wiadomości bez możliwości odstępstw (kwestia interoperacyjności i transgraniczności rozwiązań).

Na zakończenie przeglądu norm i standardów warto dodać informację odnoszącą się do formalnej obligatoryjności tychże. Otóż w polskim porządku prawnym, w ogólności, zgodność z normami i standardami nie jest obligatoryjna – jest fakultatywna. Natomiast norma lub standard przywołane

²⁰ decyzja z dnia 25 lutego 2011 r. w sprawie ustalenia minimalnych wymagań dotyczących transgranicznego przetwarzania dokumentów podpisanych elektronicznie przez właściwe organy zgodnie z dyrektywą 2006/123/WE Parlamentu Europejskiego i Rady dotyczącą usług na rynku wewnętrznym

w akcie prawnym typu decyzja lub rozporządzenie, stają się częścią tego aktu i obowiązują w zakresie, w jakim ustanowiona jest obligatoryjność tego aktu prawnego. Stąd generalnie zgodność ze standardami ETSI i CEN należy uznać za „dobre praktyki”, natomiast część dokumentów CWA i ETSI, które są przywołane w decyzji Komisji 2003/511/EC (bezpośrednio lub pośrednio) mają charakter obligatoryjny – jeśli dany podmiot powołuje się na zapisy dyrektywy UE 93/99/EC lub polskiej ustawy o podpisie elektronicznym, to jednocześnie musi spełniać wymagania zawarte m.in. w standardzie CWA 14167-1.

4.3 IDABC

IDABC (*Interoperable Delivery of European eGovernment Services to public Administrations, Business and Citizens*) jest programem interoperacyjnego świadczenia ogólnoeuropejskich usług eGovernment dla administracji publicznej, przedsiębiorstw i obywateli. IDABC jest następcą programu IDA, prowadzonego w latach 2000-2004. IDA była zbiorem tzw. projektów wspólnego zainteresowania (ang. PCI – *Project of common interest*) i środków horyzontalnych (ang. HM – *horizontal measures*). IDABC wykorzystuje możliwości oferowane przez technologie informacyjne i komunikacyjne, aby wspierać międzynarodowe usługi sektora publicznego dla obywateli i przedsiębiorstw w zjednoczonej Europie. Pomaga on również zwiększyć efektywność i poziom współpracy pomiędzy europejskimi administracjami publicznymi. W wyniku tych działań Europa staje się coraz bardziej atrakcyjnym miejscem do mieszkania, pracy oraz inwestowania. Założone cele IDABC osiąga poprzez wydawanie rekomendacji oraz proponowanie rozwiązań, które umożliwiają krajowym i europejskim administracjom wydajną komunikację elektroniczną i oferowanie coraz bardziej nowoczesnych usług dla obywateli i przedsiębiorstw. Program zapewnia również finansowanie projektów spełniających warunek usprawniania komunikacji między administracjami.²¹

W ramach programu IDABC przeprowadzony został projekt eID *Interoperability for Pan-european eGovernment Services (PEGS)* którego celem było rozwiązanie problemów technicznych związanych z interoperacyjnością zarządzania tożsamością w krajach Unii Europejskiej. Kraje członkowskie Unii Europejskiej wprowadzają zaawansowane sposoby zarządzania tożsamością, ale poszczególne kraje wdrażają różne rozwiązania. Celem projektu „eID Interoperability for PEGS” było zaproponowanie ogólnej architektury, która biorąc pod uwagę istnienie różnych modeli krajowych, pozwoli na uzyskanie interoperacyjności.²² Projekt posiadał trzy fazy: studia i ocena obszaru zarządzania tożsamością, opracowanie raportów na temat sytuacji w krajach uczestniczących w projekcie oraz stworzenie - na podstawie pierwszych dwóch faz - wspólnej specyfikacji interoperacyjności pomiędzy istniejącymi lub planowanymi rozwiązaniami służącymi do uwierzytelnienia do elektronicznych usług publicznych (tzw. e-administracja) w krajach członkowskich. Projekt zakończył się zatem opracowaniem wielu dokumentów w zakresie identyfikacji i uwierzytelnienia w kontekście elektronicznych usług publicznych (eGovernment), z których jednym z najważniejszych dla niniejszego opracowania jest dokument *Common specifications for eID interoperability in the eGovernment context*. Pojęcie interoperacyjności w tym dokumencie oznacza, że użytkownik ma możliwość bezpośredniego użycia swojego narodowego systemu uwierzytelnienia (posiadając dane uwierzytelniające wydane w swoim kraju), do uwierzytelnienia

²¹ <http://www.eadministracja.pl/program-idabc-isa>

²² IDABC eID *Interoperability for PEGS, Common specifications for eID interoperability in the eGovernment context*

Identyfikacja i uwierzytelnianie w usługach elektronicznych

w innym kraju, bez potrzeby uzyskania lokalnych tokenów lub danych uwierzytelniających (na przykład certyfikat PKI z kraju A może być użyty do uwierzytelnienia w kraju B).

Wg w/w specyfikacji, dla zapewnienia funkcjonalności wiarygodnego uwierzytelnienia transgranicznego, narodowe infrastruktury powinny oferować odpowiednie gwarancje i funkcjonalności:

- rzetelne dane identyfikacyjne – dane identyfikacyjne dostarczane przez infrastrukturę (rejstry państwowe, certyfikaty PKI na kartach elektronicznych, czy komercyjne bazy danych używane w usługach e-government) muszą być wiarygodne,
- niezaprzeczalność i rozliczalność w procesie uwierzytelnienia – chociaż podstawową kwestią jest ochrona integralności danych identyfikujących, to bardzo ważne są także kwestie niezaprzeczalności i rozliczalności procesów (np. poprzez zbieranie tzw. logów z transakcji uwierzytelnienia) w celu uzyskania możliwości badania naruszeń bezpieczeństwa,
- rzetelne mechanizmy uwierzytelnienia – aplikacje korzystające z uwierzytelnienia powinny spełniać określone wymagania bezpieczeństwa, ustanowione przez kraje członkowskie,
- konsensus w odniesieniu do poziomów bezpieczeństwa – krajowe rozwiązania uwierzytelnienia powinny podlegać jednolitej klasyfikacji w zakresie poziomu bezpieczeństwa,
- wspierać komercyjne rozwiązania uwierzytelnienia (zobowiązanie do niedyskryminacji) – kraje powinny zezwolić na używanie nie-narodowych systemów uwierzytelnienia w zastosowaniach narodowych, pod warunkiem, że oferują one wymagany poziom bezpieczeństwa, nie niższy niż dla systemów narodowych.

Z kolei uwierzytelnienie transgraniczne powinno spełniać następujące wymagania:

- bez względu na aplikację transgraniczny system uwierzytelnienia powinien umożliwiać posiadaczom aplikacji uzyskanie wymaganego zestawu danych identyfikujących, przy czym zestaw ten powinien:
 - być minimalny (najmniejszy zestaw danych potrzebny do identyfikacji jednostki);
 - być uniwersalny (dostępny we wszystkich krajach);
 - być technologicznie neutralny (co zasadniczo oznacza, że nie może być narzucone korzystanie wyłącznie z PKI),
- umożliwiać kontrolę przez użytkownika w celu poszanowania prywatności (preferowane rozwiązania, które umożliwiają użytkownikowi weryfikację, które jego dane są prezentowane właścicielowi aplikacji lub właściciel aplikacji może przetwarzać tylko te dane, które są niezbędne w danej aplikacji; w każdej sytuacji użytkownik powinien być informowany o zakresie jego danych osobowych przetwarzanych przez aplikację),
- powinien podlegać abstrakcyjnej klasyfikacji w zakresie bezpieczeństwa, a dostawcy aplikacji powinni stosować rozwiązania oferujące określony poziom bezpieczeństwa (lub wyższy), w zależności od poziomu krytyczności.

Poza samym procesem uwierzytelnienia, transgraniczny system uwierzytelnienia powinien spełniać określone wymagania w zakresie standardów komunikacji z aplikacjami (przesyłać dane identyfikujące zgodnie z przyjętymi konwencjami w zakresie składni, technicznych standardów i mechanizmów bezpieczeństwa) oraz komunikacji pomiędzy systemami zarządzania tożsamością (IDMS) tak, aby właściciel aplikacji mógł polegać na informacji identyfikującej, którą otrzymuje poprzez możliwość weryfikacji źródła pochodzenia danych, czy posiadania informacji nt. gwarancji i słabości danego systemu uwierzytelnienia.

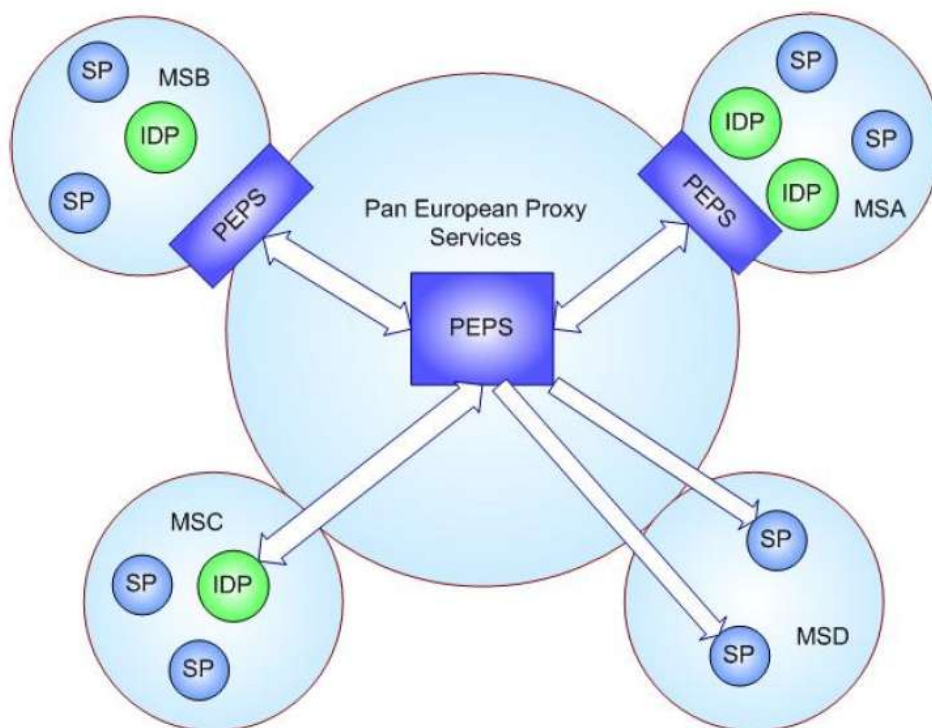
Identyfikacja i uwierzytelnianie w usługach elektronicznych

Jako rezultat prac w programie IDABC opracowana została koncepcja stworzenia architektury federującej lokalne (narodowe) systemy zarządzania tożsamości (IDMS). Opiera się ona o serwisy pośredniczące (brokerzy), tzw. PEPS (ang. *Pan European Proxy Services*), mogące działać na dwóch szczeblach: centralnym (europejskim) i lokalnym (krajowym). Rolą PEPS jest dostarczanie dostawcom usług (ang. *Service Provider*, SP) podstawowych funkcji, takich jak identyfikacja lokalnego dostawcy tożsamości (ang. *Identity Provider*, IDP), uzyskanie atrybutów tożsamości i przesłanie ich do dostawcy usług (SP). Akronim „PEPS” jest więc ogólnym opisem pakietu usług, które muszą być dostarczane.

W ogólności PEPS może być zrealizowany jako:

- jedna - centralna, europejska infrastruktura, poprzez którą wszystkie żądania uwierzytelnienia muszą być przesyłane,
- struktura rozproszona - poprzez budowę lokalnych (krajowych) PEPS, które przetwarzają żądania dotyczące dostawców tożsamości (IDP) z własnych krajów (ten model jest także nazywany modelem “middleware”, gdyż PEPS działa w tym przypadku, z punktu widzenia dostawców usług, jak middleware dostarczający ustandaryzowane funkcje (usługi) uwierzytelnienia, bez względu na metodę uwierzytelnienia),
- struktura mieszana - łącząca dwa powyższe modele, gdzie niektóre kraje posiadają swój własny PEPS, a inne korzystają z centralnego PEPS.

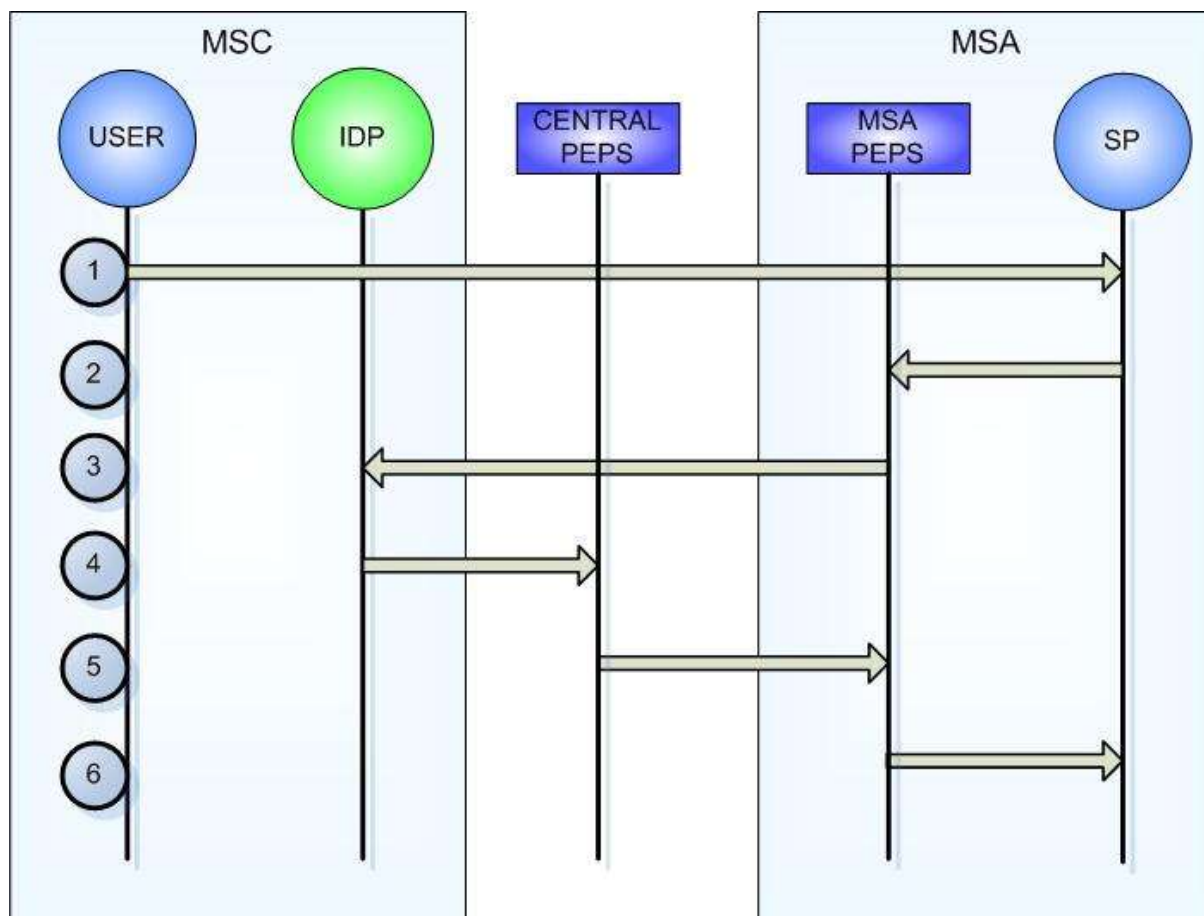
Bez względu na sposób implementacji, PEPS muszą realizować uwierzytelnienie obywatela wspierając różne metody, oferujące różny poziom bezpieczeństwa (hasła, hasła jednorazowe, PKI) i dostarczając informacji o poziomie wiarygodności uwierzytelnienia związanego z użytą metodą, wg ustandaryzowanej klasyfikacji. Rysunek 1 przedstawia wysokopoziomowy model architektury PEPS. Należy podkreślić, że model ten może być całkowicie zcentralizowany (tzn. istnieje tylko centralny PEPS, bez lokalnych) lub całkowicie zdecentralizowany (istnieją tylko lokalne PEPS, po jednym w każdym kraju) lub też mieszany. Rysunek przedstawia model, w którym w niektórych krajach istnieją lokalne PEPS, natomiast pozostałe kraje korzystają z centralnego PEPS.



Rysunek 1. Ogólny model architektury PEPS; legenda: PEPS – Pan European Proxy Services; IDP (Identity Provider) – dostawca tożsamości; SP (Service Provider) – dostawca usług; MS (Member State) – kraj członkowski (na podst. [1]).

Rysunek 2 przedstawia proces uwierzytelnienia obywatela w kraju C (MSC) do usługi w kraju A (MSA). Proces ten przebiega następująco:

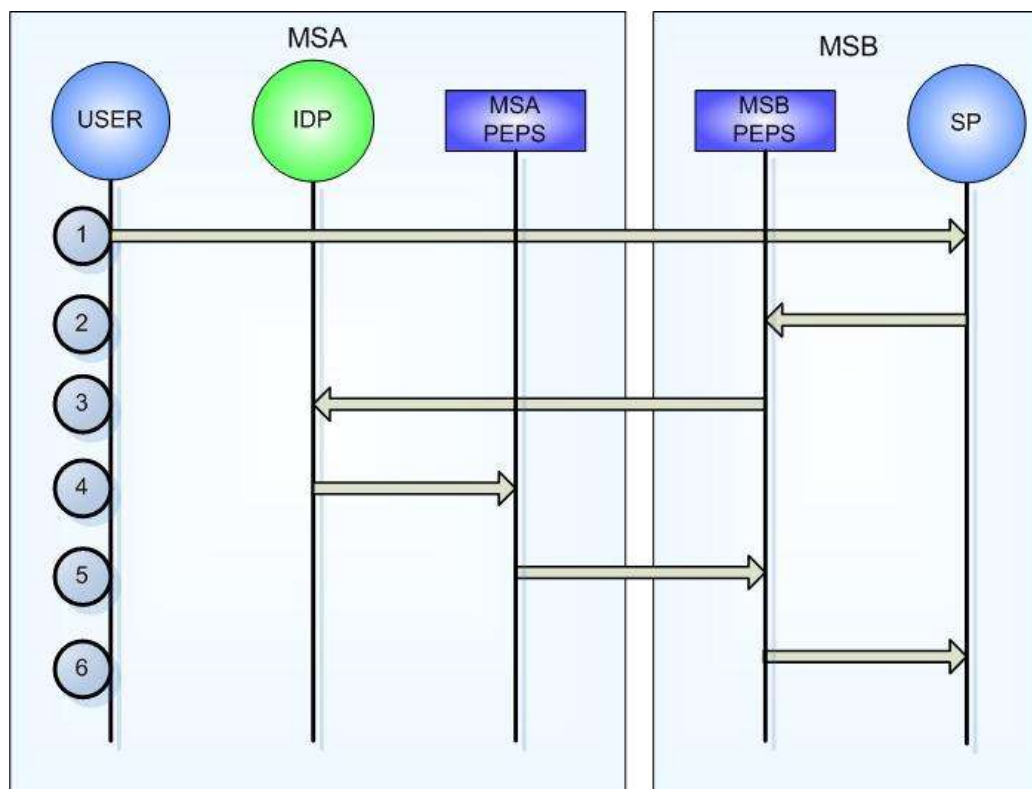
- 1) użytkownik (obywatel kraju C) łączy się z e-usługą w kraju A (oferowaną przez dostawcę usługi – SP),
- 2) użytkownik jest przekierowywany do PEPS kraju A, gdzie dokonywane jest rozpoznanie dostawcy tożsamości (IDP) użytkownika,
- 3) użytkownik jest przekierowany do właściwego dostawcy tożsamości (w jego kraju macierzystym) celem uwierzytelnienia,
- 4) wynik uwierzytelnienia jest przesyłany do centralnego PEPS, gdzie następuje jego podpisanie,
- 5) wynik uwierzytelnienia jest przesyłany z centralnego PEPS do PEPS kraju A, gdzie następuje jego ponowne podpisanie,
- 6) wynik uwierzytelnienia jest przesyłany do usługi (do SP), gdzie następuje weryfikacja podpisów i w przypadku pozytywnej weryfikacji wynik uwierzytelnienia oraz usługa są udostępnione użytkownikowi.



Rysunek 2. Proces uwierzytelnienia z wykorzystaniem centralnego PEPS w sytuacji, gdy jeden z krajów nie posiada własnego (lokalnego) PEPS (na podst. [1]).

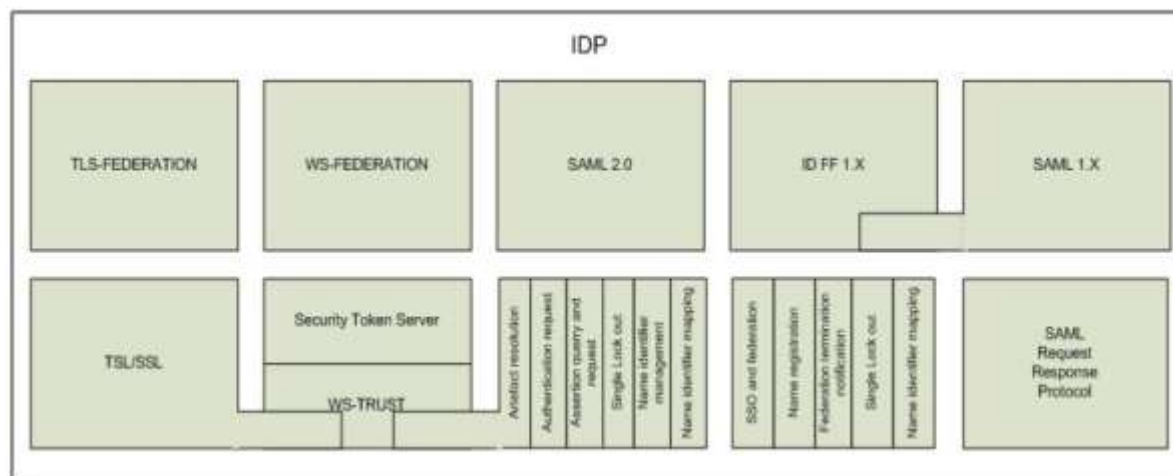
Z kolei Rysunek 3 przedstawia proces uwierzytelnienia w sytuacji, gdy oba kraje posiadają własny PEPS (uwierzytelnienie odbywa się bez udziału centralnego PEPS). Proces ten przebiega następująco:

- 1) użytkownik (obywatel kraju A) łączy się z e-usługą w kraju B,
- 2) użytkownik jest przekierowywany do PEPS kraju B, gdzie wykonywana jest usługa rozpoznania dostawcy tożsamości użytkownika,
- 3) użytkownik jest przekierowany do właściwego dostawcy tożsamości (w jego kraju macierzystym) celem uwierzytelnienia,
- 4) wynik uwierzytelnienia jest przesyłany do PEPS kraju A, gdzie następuje jego podpisanie,
- 5) wynik uwierzytelnienia jest przesyłany z PEPS kraju A do PEPS kraju B, gdzie następuje jego ponowne podpisanie,
- 6) wynik uwierzytelnienia jest przesyłany do usługi (do SP), gdzie następuje weryfikacja podpisów i w przypadku pozytywnej weryfikacji wynik uwierzytelnienia oraz usługa są udostępnione użytkownikowi.

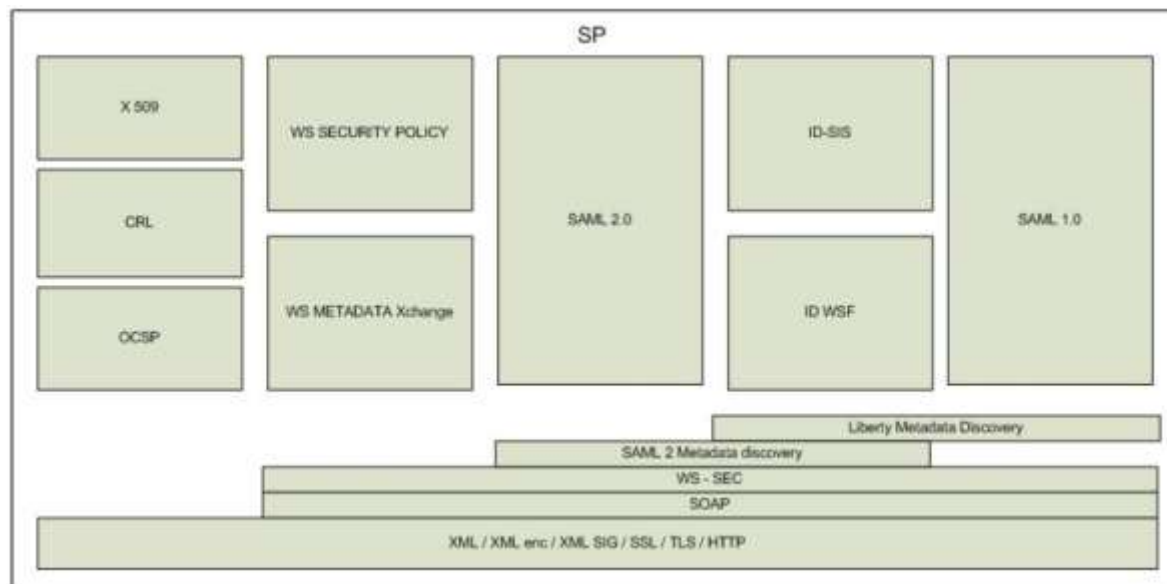


Rysunek 3. Proces uwierzytelnienia w sytuacji, gdy oba kraje posiadają własne (lokalne) PEPS (na podst. [1]).

Wynikiem końcowym programu IDABC jest opracowanie wspólnej specyfikacji systemów IDM, SP oraz PEPS. Poniższe dwa rysunki przedstawiają standardy potencjalnie mające zastosowanie w zarządzaniu tożsamością: rys. Rysunek 4 przedstawia standardy na poziomie dostawcy tożsamości (IDP), natomiast rys. Rysunek 5 – standardy na poziomie dostawcy usług (SP).



Rysunek 4. Standardy dla dostawcy tożsamości (na podst. [1]).



Rysunek 5. Standardy dla dostawcy usług (na podst. [1]).

Kluczową rolę w uzyskaniu interoperacyjności odgrywają metadane. W projekcie IDABC uznano, że protokół SAML jest standardem „de-facto” i przyjęto wersję SAML 2.0 jako podstawowy protokół federacji tożsamości, przy czym systemy krajowe wykorzystujące inne protokoły (jak TLSFederation, WS-Federation, Liberty Alliance) również mogą być włączone do systemu pan-europejskiego. Ponadto analizując poszczególne rozwiązania uwierzytelnienia w krajach członkowskich, dostrzeżono różnorodność używanych tokenów do uwierzytelnienia. Dlatego na potrzeby programu IDABC opracowano tzw. poziomy wiarygodności („levels of assurance”) związane z poszczególnymi tokenami (zob. tabela Tabela 2).

Poziom 4 oznacza najwyższy poziom wiarygodności, poziom 1 – najniższy. Zastosowanie określonego poziomu wiarygodności dla określonej usługi zależy od jej rodzaju i wymaganego poziomu bezpieczeństwa (rozumianego jako poziom akceptowanego ryzyka i konsekwencji spowodowanych błędnym uwierzytelnieniem). Po określeniu, na podstawie analizy ryzyka, wymaganego poziomu wiarygodności procesu uwierzytelnienia danej usługi, na podstawie wyżej przedstawionej tabeli można określić dozwolone rodzaje tokenów. Przykładem usługi wymagającego poziomu 4 jest usługa udostępnienia danych medycznych, gdzie mamy do czynienia z informacjami wrażliwymi. Jak łatwo zauważyć, dla tego typu usług należy stosować wyłącznie tokeny sprzętowe (np. mikroprocesorowe karty kryptograficzne)²³. Z drugiej strony protokół SAML 2.0 wprowadza własne poziomy wiarygodności dla różnych metod uwierzytelnienia, tzw. „context classes”. Są one jednak zdefiniowane w odmienny sposób niż w powyższej tabeli, w związku z tym nie da się utworzyć bezpośredniej analogii pomiędzy nimi. Jednak co najistotniejsze, obie specyfikacje poziomów wiarygodności odnoszą się tylko do metod uwierzytelnienia. Dlatego w pracy [1] zwrócono uwagę, że faktyczny pan-europejski system uwierzytelnienia powinien polegać na poziomach wiarygodności obejmujących także inne elementy

²³ por. z wymaganiami z poziomem 4 (LoA 4) wg ISO 29115, rozdz. 0

Identyfikacja i uwierzytelnianie w usługach elektronicznych

występujące w procesie uwierzytelnienia (np. procesy rejestracji, czy zarządzania danymi uwierzytelniającymi).

Tabela 2

Rodzaje dozwolonych tokenów	Poziomy wiarygodności			
	1	2	3	4
Token sprzętowy	X	X	X	X
Token programowy lub urządzenie do generowania haseł jednorazowych	X	X	X	
Hasło losowe, kod PIN lub lista haseł (hasła i kody PIN niegenerowane przez użytkownika)	X	X		
Hasło lub kod PIN generowane przez użytkownika	X			

Podsumowując, model przedstawiony w specyfikacji IDABC spełnia następujące cele:

- jest **sfederowany** – polega na strukturze stanowiącej federację wielu PEPS oraz IDP jako podległym mechanizmom uwierzytelnienia, pozostawiając dowolność decyzji krajom członkowskim o sposobie realizacji,
- jest **wielopoziomowy** – system polega na wspólnej definicji poziomów uwierzytelnienia,
- opiera się na **wiarygodnych źródłach** – implementacja w oparciu o narodowych dostawców tożsamości (IDP),
- pozwala na tzw. **kontekstowe/sektorowe podejście** – możliwe jest użycie pseudonimów dla zwiększenia ochrony prywatności,
- umożliwia **udział sektora prywatnego** – prywatni dostawcy usług mogą wykorzystywać mechanizmy uwierzytelnienia dostarczane przez ten model, a także mogą być stworzone systemy translacyjne do uzyskania interoperacyjności z innymi (prywatnymi) modelami; ponadto system jest dostępny dla prywatnych dostawców usług bez obligatoryjnego wymogu wcześniejszej rejestracji, gdyż system może rozróżnić pomiędzy zarejestrowanymi i niezarejestrowanymi usługodawcami i ostrzec użytkownika, gdy usługa nie jest zarejestrowana (nie jest usługą zaufaną).

4.4 STORK

Projekt STORK (ang. *Secure Identity Across Borders Linked*) jest praktyczną realizacją koncepcji zawartej w programie IDABC. Celem projektu STORK jest ustanowienie europejskiej platformy interoperacyjności elektronicznych identyfikatorów (eID), która pozwoli na ustanowienie nowych, transgranicznych „elektronicznych relacji” z wykorzystaniem narodowych eID. W ramach projektu testowane jest transgraniczne uwierzytelnienie elektroniczne do istniejących (rzeczywistych) publicznych usług elektronicznych w krajach członkowskich Unii Europejskiej²⁴.

W ramach tego projektu zrealizowano 6 projektów pilotażowych:

- Transgraniczne uwierzytelnienie (“Cross-border Authentication Platform for Electronic Services”) – umożliwia bezpieczny dostęp do publicznych e-usług kraju członkowskiego przez obywatela innego kraju członkowskiego z użyciem jego narodowego eID;
- “SAFERCHAT” – demonstruje realizację transgranicznych „rozmów” przez Internet w bezpieczniejszy sposób;
- “Student Mobility” – umożliwia zagranicznym studentom dostęp „on-line” do usług oferowanych przez europejskie uczelnie wyższe;
- Przekaz elektroniczny (“Electronic Delivery”) – demonstruje interoperacyjność infrastruktury usług elektronicznego przekazu, który umożliwia przesyłanie dokumentów od urzędu do obywatela poprzez granice, z wykorzystaniem narodowych portali elektronicznego przekazu;
- Zmiana adresu (“Address change”) – interoperacyjna usługa pozwalająca obywatelowi zagranicznego kraju poinformowanie wszystkie istotne jednostki o zmianie adresu, bez zmiany wewnętrznych procedur w danym kraju;
- “ECAS Integration” – integracja infrastruktury uwierzytelnienia STORK z serwisem uwierzytelnienia Komisji Europejskiej (ECAS, European Commission Authentication Service).

Oprócz przeprowadzenia w/w pilotaży oraz opracowania specyfikacji technicznych, jednym z głównych produktów projektu jest opracowanie zestawu poziomów wiarygodności uwierzytelnienia QAA (ang. *Quality Authentication Assurance Levels*) [2]. Projekt STORK ma na celu stworzenie możliwości dostępu do usług oferowanych przez dowolnego europejskiego dostawcy z użyciem tokenów uwierzytelnienia dostarczanych przez rząd dowolnego kraju europejskiego (lub w jego imieniu). Akceptacja w danym kraju elektronicznych danych uwierzytelniających, wydanych za granicą, wymaga ponadto znajomości poziomu wiarygodności systemu uwierzytelnienia związanego z tymi danymi. Dlatego potrzebne było „zmierzenie” jakości różnych procedur uwierzytelnienia i określenie poziomów wiarygodności wg jednolitej skali. Stąd w ramach STORK stworzono własną skalę oceny poziomów wiarygodności – STORK Quality Authentication Assurance Levels (dalej zwane „poziomy QAA”). Punktem wyjścia było studium przeprowadzone w ramach IDABC (zob. 4.3). Każdy poziom wiarygodności określa stopień, w którym strona ufająca w transakcji elektronicznej może być pewna, że zaprezentowane informacje o tożsamości rzeczywiście reprezentują osobę, do której te informacje należą.

QAA są zdefiniowane w dwóch wymiarach: organizacyjnym i technicznym, które charakteryzują proces uwierzytelnienia. W wymiarze organizacyjnym pod uwagę brane są czynniki związane z procesem

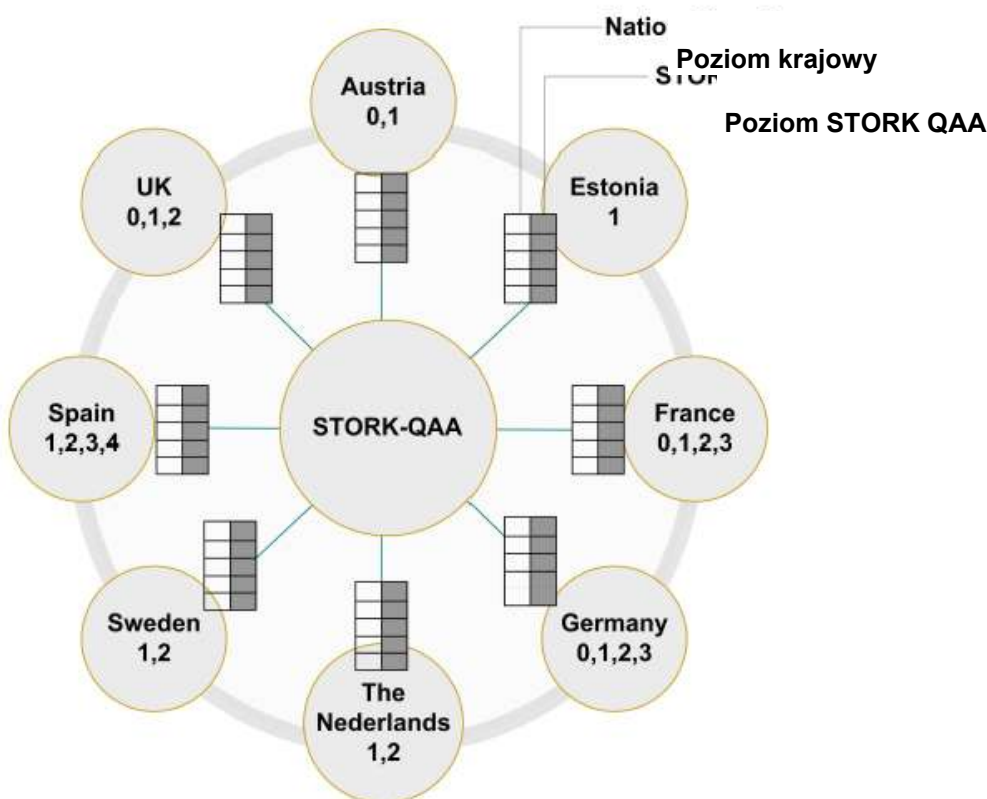
²⁴ na podst. [4]

Identyfikacja i uwierzytelnianie w usługach elektronicznych

rejestracji, takie jak jakość procesów identyfikacji, wydawania danych uwierzytelniających oraz ocena samej jednostki je wydającej. Wymiar techniczny dotyczy jakości samego procesu uwierzytelnienia elektronicznego, w tym rodzaju i „odporności” danych uwierzytelniających i ich nośnika oraz mechanizmów bezpieczeństwa procesu zdalnego uwierzytelnienia. Jednocześnie dostawcy usług muszą zarządzać ryzykiem dostarczenia usługi do niewłaściwego użytkownika, dlatego wymagane jest przeprowadzenie analizy ryzyka i określenie poziomu QAA.

W modelu STORK QAA określono cztery poziomy wiarygodności. Generalnie poziomy są sklasyfikowane wg środków, które są użyte do uwierzytelnienia oraz wg procesów związanych z ich wydaniem i zarządzaniem. Przykładowo karty elektroniczne z PKI są uznawane za bardziej wiarygodne rozwiązanie, certyfikaty programowe (software'owe) jako umiarkowane, a nazwa użytkownika i hasło jako dość słabe. Z kolei z punktu widzenia procesowego, na przykład certyfikat programowy wydany przez Internet bez fizycznej obecności właściciela, może mieć mniejszą wiarygodność niż nazwa użytkownika i hasło uzyskane po fizycznej weryfikacji osoby przez urząd administracji publicznej.

Należy wspomnieć, iż w momencie rozpoczynania projektu STORK, wiele krajów posiadało już swoje systemy uwierzytelnienia, a co za tym idzie własne, wzajemnie niezgodne, skale dla oceny poziomu wiarygodności. Dlatego w ramach projektu STORK została najpierw wykonana dogłębna analiza systemów uwierzytelnienia w poszczególnych krajach (uczestniczących w projekcie), które następnie zostały „zmapowane” na skalę STORK QAA.



Rysunek 6. Mapowanie poziomów STORK QAA na poziomy krajowe (na podst. [2]).

STORK QAA określa 4 poziomy:

- 1) brak lub minimalna wiarygodność,
- 2) niska wiarygodność,
- 3) znacząca wiarygodność,
- 4) wysoka wiarygodność.

Poziomy QAA odpowiadają dotkliwości konsekwencji szkód, które mogą powstać w wyniku błędnej identyfikacji i uwierzytelnienia tożsamości – im bardziej dotkliwe i bardziej prawdopodobne konsekwencje, tym wyższy poziom pewności co do stwierdzanej tożsamości jest wymagany przed zaangażowaniem się dostawcy usługi w daną transakcję.

Poziom 1 określa najniższy poziom wiarygodności co do stwierdzanej tożsamości lub brak pewności w ogóle. Dane uwierzytelniające są akceptowane bez jakiegokolwiek weryfikacji. Jeśli subskrybent dostarcza adres e-mail, jedyną weryfikacją jest sprawdzenie poprawności adresu. Poziom ten jest właściwy w sytuacji, gdy negatywne konsekwencje błędnego uwierzytelnienia są bardzo małe lub nieistotne. Poziom ten odpowiada usługom elektronicznym nieposiadającym lub posiadającym minimalny zestaw mechanizmów ochronnych.

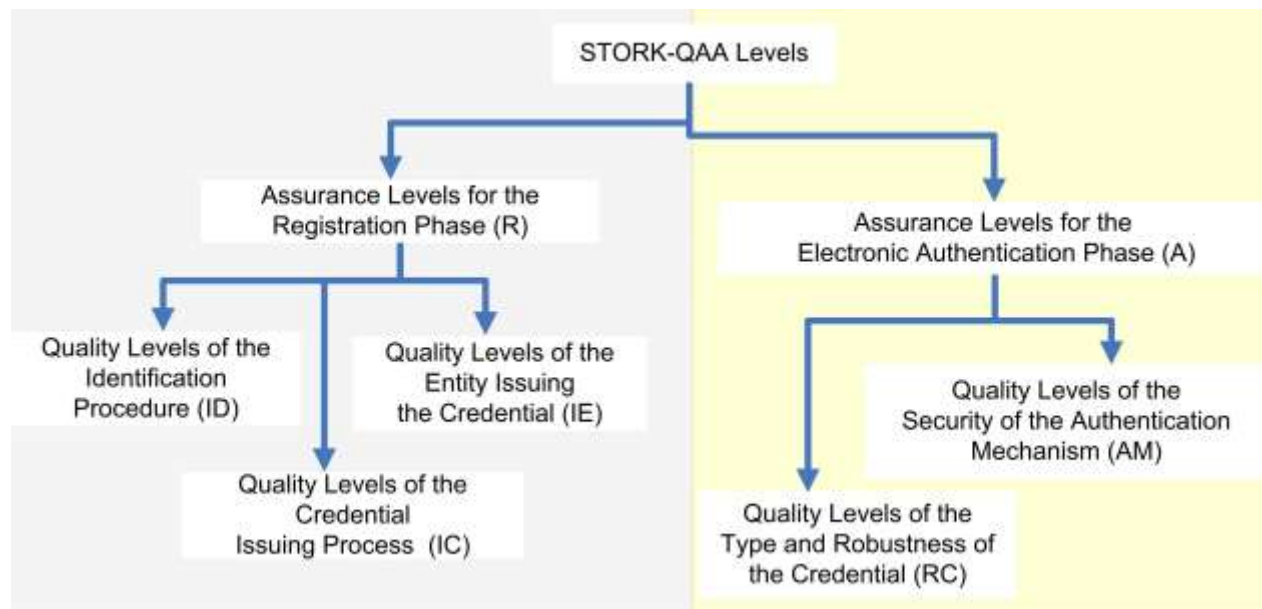
Poziom 2 określa te usługi, dla których szkody wynikające z błędnego uwierzytelnienia tożsamości mają niski wpływ. Nawet jeśli nie jest wymagana obecność osobista pretendenta (ang. *claimant*) przy rejestracji, to jednak odpowiadająca mu tożsamość rzeczywista musi być zweryfikowana, a nośnik poświadczeń tożsamości musi być wydany przez organ zaakceptowany na poziomie rządowym. Nośnik musi być dostarczony z zachowaniem należytej staranności, a w procesie uwierzytelnienia muszą być używane odpowiednio silne protokoły.

Poziom 3 odpowiada usługom, które mogą w przypadku błędnego uwierzytelnienia spowodować znaczące szkody. Rejestracja tożsamości musi być przeprowadzona metodami pozwalającymi jednoznacznie i z wysokim poziomem pewności zidentyfikować osobę uwierzytelniającą się. Dostawcy tożsamości w tym przypadku powinni podlegać rządowemu nadzorowi lub posiadać akredytację rządu. Dane uwierzytelniające powinny być przynajmniej w postaci certyfikatów programowych (ang. *soft certificates*) lub umieszczonymi na tokenie sprzętowym (ang. *hard certificates*). Mechanizmy uwierzytelnienia w procesie zdalnego uwierzytelnienia powinny być odpowiednio silne.

Poziom 4 jest najwyższym poziomem wiarygodności i odpowiada usługom, dla których błędne uwierzytelnienie może wywołać poważne szkody. Proces rejestracji wymaga przynajmniej jednokrotnej obecności osoby (np. przy pierwszym wydaniu danych uwierzytelniających; przy odnowieniu już niekoniecznie) lub też fizycznego spotkania przy dostarczaniu danych uwierzytelniających (np. żądanie wystawienia certyfikatu jest przesyłane on-line, dostarczone do domu i wręczone osobie po weryfikacji jej tożsamości). Alternatywnie, w przypadku rejestracji on-line, tożsamość osoby jest sprawdzana poprzez weryfikację zaufanego (kwalifikowanego) podpisu elektronicznego. Aneks II Dyrektywy 1999/93/EC o podpisie elektronicznym pozostawia szczegóły realizacji procesu weryfikacji tożsamości do decyzji krajów członkowskich. Dlatego poziom 4 jest osiągnięty, jeśli proces spełnia wymagania prawa lokalnego w zakresie wydawania certyfikatów kwalifikowanych. Ponadto, dostawca tożsamości musi być podmiotem kwalifikowanym zgodnie z Aneksiem II w/w dyrektywy, a dane uwierzytelniające są w postaci certyfikatu elektronicznego wydanego na tokenie sprzętowym (*hard certificate*) zgodnie z Aneksiem I (czyli

spełniającym wymagania dla SSCD). Na tym poziomie w procesie uwierzytelnienia mogą być używane wyłącznie najsilniejsze mechanizmy.

Każdy z poziomów QAA jest zdefiniowany jako zestaw wymagań dla określonych czynników uwierzytelnienia. Wymagania dla poszczególnych czynników są zorganizowane hierarchicznie, oddzielnie dla fazy rejestracji (on-line lub off-line) i fazy uwierzytelnienia (on-line), co przedstawia poniższy rysunek.



Rysunek 7. Czynniki wpływające na poziomy QAA [2].

W dalszej części dokument [2] opisuje konkretne wymagania. Nie przytaczamy wszystkich wymagań i ich interpretacji (zainteresowanych odsyłamy do dokumentu [2]), natomiast przedstawimy przykład dla zobrazowania idei.

W zakresie procedury identyfikacji ID (zob. rys. Rysunek 7), określone są następujące czynniki i wymagania dla każdego z nich:

- i. fizyczna obecność osoby
 - a. identyfikacja nie wymaga fizycznej obecności,
 - b. identyfikacja wymaga przynajmniej jednokrotnej fizycznej obecności,
 - c. identyfikacja wymaga obecności przy wydaniu danych uwierzytelniających (przynajmniej jeden raz, przy pierwszym wydaniu),
- ii. jakość deklaracji atrybutów tożsamości (ang. *assertion*)
 - a. deklaracja pojedynczej danej związanej z osobą deklarującą, która niekoniecznie jest znana tylko przez tą osobę (np. imię i nazwisko czy data urodzenia), niezapewniającej jednoznacznej identyfikacji,
 - b. deklaracja wielu danych związanych z osobą deklarującą, które niekoniecznie znane są tylko przez tą osobę (np. imię i nazwisko wraz z adresem), zapewniających jednak jednoznaczną identyfikację,

Identyfikacja i uwierzytelnianie w usługach elektronicznych

- c. deklaracja przynajmniej jednej unikalnej danej, którą przyjmuje się, że znana jest wyłącznie osobie deklarującej (np. numer paszportu) i która może być zweryfikowana z użyciem oficjalnych rejestrów; deklaracja ta musi oznaczać jednoznaczną identyfikację.
- iii. weryfikacja deklaracji atrybutów tożsamości
 - a. weryfikacja jest ograniczona do sprawdzenia adresu e-mail, jeśli adres został dostarczony; w przeciwnym razie nie ma żadnej weryfikacji,
 - b. weryfikacja jest przeprowadzana poprzez sprawdzenie deklarowanych danych w oficjalnym źródle lub bazie tożsamości z neutralnego lub godnego zaufania źródła, takiego jak bank, instytucja ubezpieczeniowa lub urząd państwowy,
 - c. weryfikacja wymaga, aby deklarowana dana była podpisana niekwalifikowanym podpisem elektronicznym,
 - d. weryfikacja wymaga przedstawienia fizycznego, oficjalnego (wydanego przez państwo) dokumentu tożsamości zawierającego (przynajmniej) zdjęcie lub podpis, takiego jak dowód osobisty, czy paszport,
 - e. weryfikacja wymaga, aby deklarowana dana była podpisana podpisem elektronicznym, zweryfikowanym z pomocą wystawcy certyfikatu przed wydaniem tokenu/danych uwierzytelniających.

Poniższa tabela wskazuje minimalne wymagania dla każdego z poziomów QAA dla procedury identyfikacji (ID).

Tabela 3.

Wymagania	Poziom QAA dla procedury identyfikacji			
	ID1	ID2	ID3	ID4
Fizyczna obecność: niewymagana, np. typu (i.a), rejestracja on-line Jakość deklaracji atrybutów tożsamości (ang. <i>assertion</i>): co najmniej typu (ii.a) Weryfikacja deklaracji: co najmniej typu (iii.a)	●			
Fizyczna obecność: nie wymagana, np. typu (i.a) Jakość asercji: co najmniej typu (ii.b) Weryfikacja deklaracji: typu (iii.b)	●	●		
Fizyczna obecność: wymagana, typu (i.b) Jakość asercji: co najmniej typu (ii.b) Weryfikacja deklaracji: co najmniej typu (iii.c)	●	●	●	
Fizyczna obecność: niewymagana, typu (i.b), rejestracja on-line Jakość asercji: typu (ii.c) Weryfikacja deklaracji: co najmniej typu (iii.d)	●	●	●	
Fizyczna obecność: wymagana, co najmniej typu (i.b) Jakość asercji: typu (ii.c) Weryfikacja deklaracji: co najmniej typu (iii.d)	●	●	●	●

Identyfikacja i uwierzytelnianie w usługach elektronicznych

Z powyższej tabeli można odczytać, jakie wymagania należy spełnić, aby osiągnąć określony poziom wiarygodności dla procesu identyfikacji (ID). Podobnie postępuje się z pozostałymi elementami i procesami przedstawionymi na rysunku Rysunek 7 (tj. IE, IC, RC, AM, a następnie R i A), przy czym, aby całkowity poziom wiarygodności posiadał założony poziom, wszystkie elementy podrzędne muszą posiadać poziom nie niższy od założonego. Innymi słowy, całkowity poziom STORK QAA jest **równy zawsze najniższemu poziomowi spośród elementów podrzędnych** (zob. Tabela 4). Ta zasada jest uniwersalna dla wszystkich tego typu metodyk (por. 0).

Tabela 4. Poziomy STORK QAA (na podst. [2]).

		Assurance Levels for Electronic Authentication phase			
		EA1	EA2	EA3	EA4
Assurance Levels for Registration phase	RP1	STORK QAA Level 1	STORK QAA Level 1	STORK QAA Level 1	STORK QAA Level 1
	RP2	STORK QAA Level 1	STORK QAA Level 2	STORK QAA Level 2	STORK QAA Level 2
	RP3	STORK QAA Level 1	STORK QAA Level 2	STORK QAA Level 3	STORK QAA Level 3
	RP4	STORK QAA Level 1	STORK QAA Level 2	STORK QAA Level 3	STORK QAA Level 4

Na koniec słowo komentarza na temat relacji pomiędzy identyfikatorami obecnie wydawanymi i planowanymi w Polsce, a oceną jakości za pomocą poziomów wiarygodności QAA. Wg STORK najwyższy poziom (4) mogą uzyskać jedynie certyfikaty kwalifikowane (na tokenie sprzętowym) wydawane przez kwalifikowane podmioty świadczące usługi certyfikacyjne²⁵. Oznacza to, że polski dowód osobisty z warstwą elektroniczną (pl.ID) zawierającą jedynie niekwalifikowany certyfikat (tzw. podpis osobisty, który miał być wydawany przez MSW) nigdy nie osiągnie poziomu 4, a co najwyżej poziom 3. Jak wspomniano wcześniej, wymagany poziom bezpieczeństwa (a tym samym poziom QAA) dla danej usługi elektronicznej określa się na podstawie właściwej oceny ryzyka. Ale nawet bez przeprowadzenia oceny ryzyka można przyjąć, że istnieją rodzaje usług publicznych, dla których wymagany jest najwyższy poziom wiarygodności procesu uwierzytelnienia, np. usługa dostępu do danych medycznych (danych wrażliwych). Zatem planowany polski dowód nie umożliwi dostępu do wielu usług publicznych bez wykupienia dodatkowego certyfikatu (kwalifikowanego), co przeczy idei powstania

²⁵ zob. tabela 7 w [2]

certyfikatu podpisu osobistego²⁶. Z drugiej strony poziom 3 może być osiągnięty przez podmioty niekwalifikowane, ale podlegające państwowemu nadzorowi czy akredytacji, jak banki i instytucje ubezpieczeniowe. Oznacza to, że na równi z pl.ID i podpisem osobistym mogą w Polsce funkcjonować tokeny wydane przez komercyjne instytucje.

Druga konkluzja jest taka, że biorąc pod uwagę kryterium rodzaju i odporności danych uwierzytelniających (RC), Profil Zaufany bez jednorazowych kodów potwierdzających przesyłanych SMS'em nie osiągnie poziomu wyższego niż 2²⁷. Z kolei platforma ePUAP, jako system dostarczający mechanizmów uwierzytelnienia, nie będzie umożliwiał dostępu do usług na poziomie najwyższym (np. do usług związanych z dostępem do danych medycznych), jeśli nie będzie prezentował poziomu bezpieczeństwa co najmniej porównywalnego z Common Criteria EAL4+²⁸.

4.5 Rozporządzenie „eIDAS”

Niniejszy rozdział dotyczy identyfikacji i uwierzytelnienia w projekcie *Rozporządzenia Parlamentu Europejskiego i Rady w sprawie identyfikacji elektronicznej i usług zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznym* (potocznie zwanej „eIDAS”), które ma docelowo zastąpić dyrektywę UE 93/99/EC. Projekt został opracowany w wyniku dogłębnych analiz i konsultacji, w których stwierdzono, że „*transnarodowy charakter identyfikacji elektronicznej, uwierzytelniania elektronicznego i podpisu elektronicznego sprawia, że konieczne jest podjęcie działań na poziomie UE, gdyż cele jakie stawiane były przez obecny układ legislacyjny nie zostały obecnie osiągnięte poprzez dobrowolną koordynację między państwami członkowskimi i nie wydaje się, aby miało to nastąpić w najbliższej przyszłości*”.

Problemy zidentyfikowane w obszarze identyfikacji i uwierzytelnienia w UE przedstawiono na rys. Rysunek 8, na którym określono również powody ich zaistnienia i środki zaradcze jakie należałoby podjąć, aby dostosować rozwiązania do aktualnych potrzeb rynkowych. Brak wspólnej podstawy prawnej, nakładającej na każde państwo członkowskie obowiązek uznawania i akceptowania środków identyfikacji elektronicznej wydanych w innych państwach członkowskich w celu zapewnienia dostępu do usług online, wraz z nieodpowiednią transgraniczną interoperacyjnością krajowych systemów identyfikacji elektronicznej, tworzą bariery, które nie pozwalają obywatelom i przedsiębiorstwom korzystać w pełni z jednolitego rynku cyfrowego. Proponowane ramy prawne, mają umożliwić bezpieczne i płynne interakcje drogą elektroniczną między przedsiębiorstwami, obywatelami i organami administracji publicznej, zwiększając przez to skuteczność publicznych i prywatnych usług online, biznesu i handlu elektronicznego w UE. Zapewnienie wzajemnego uznawania i akceptowania identyfikacji elektronicznej i uwierzytelniania elektronicznego jest niezbędne, aby transgraniczna opieka zdrowotna dla obywateli Europy stała się rzeczywistością. Celem działania jest wzmocnienie i rozszerzenie istniejących przepisów w taki sposób, aby obejmowały wzajemne uznawanie i akceptowanie na szczeblu UE krajowych

²⁶ O ile koncepcja określona w Ustawie o dowodach osobistych z dn. 6.08.2010 zostanie utrzymana w przyszłości; w czasie tworzenia tego raportu trwały prace nad zmianą ustawy podlegające m.in. na wykreśleniu warstwy elektronicznej

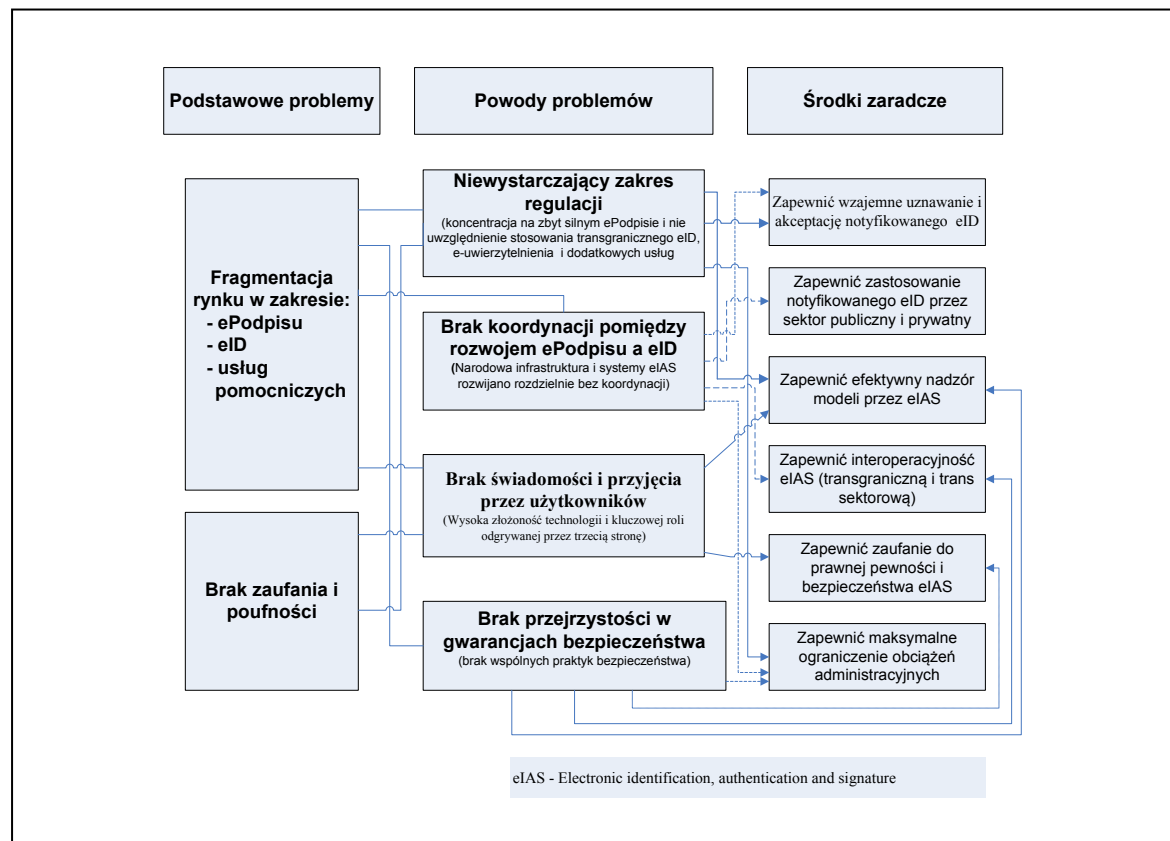
²⁷ zob. tabela 9 na str. 26 w [2]

²⁸ zob. tabela 10 na str. 28 w [2]

Identyfikacja i uwierzytelnianie w usługach elektronicznych

systemów identyfikacji elektronicznej i innych podstawowych elektronicznych usług zaufania, które są z nimi powiązane.

Rozporządzenie określa warunki uznawania i akceptowania przez państwa członkowskie środków identyfikacji elektronicznej osób fizycznych i prawnych, objętych zgłoszonym systemem identyfikacji elektronicznej innego państwa członkowskiego. Państwa członkowskie mogą zgłaszać systemy identyfikacji elektronicznej, które akceptują zgodnie ze swoją jurysdykcją w przypadkach, w których identyfikacja elektroniczna jest wymagana na potrzeby usług publicznych. Zgodnie z dodatkowym wymaganie odpowiednie środki identyfikacji elektronicznej muszą być wydawane przez państwo członkowskie zgłaszające system, w jego imieniu lub co najmniej na jego odpowiedzialność.



Rysunek 8. Uwarunkowania i cele wdrożenia regulacji eIDAS.

Systemy identyfikacji elektronicznej kwalifikują się do zgłoszenia zgodnie z art. 7, jeżeli spełnione są następujące warunki:

- środki identyfikacji elektronicznej zostały wydane przez zgłaszające państwo członkowskie, w jego imieniu lub na jego odpowiedzialność;
- środki identyfikacji elektronicznej mogą być używane w celu zapewnienia dostępu przynajmniej do usług publicznych wymagających identyfikacji elektronicznej w zgłaszającym państwie członkowskim;
- zgłaszające państwo członkowskie gwarantuje, że dane osobowe związane z identyfikacją są jednoznacznie przypisywane do osoby fizycznej lub prawnej;

Identyfikacja i uwierzytelnianie w usługach elektronicznych

- d) zgłaszające państwo członkowskie gwarantuje dostępność mechanizmów uwierzytelniania online w dowolnym czasie i nieodpłatnie, tak aby wszystkie strony ufające mogły dokonać weryfikacji danych identyfikujących osobę otrzymanych w formie elektronicznej. Państwa członkowskie nie nakładają żadnych specjalnych wymagań technicznych na strony ufające posiadające siedzibę poza ich terytorium, które zamierzają dokonać takiego uwierzytelnienia. Jeżeli nastąpi naruszenie lub częściowe uszkodzenie zgłoszonego systemu identyfikacji lub mechanizmu uwierzytelniania, państwo członkowskie bezzwłocznie zawiesza lub wycofuje zgłoszony system identyfikacji lub mechanizm uwierzytelniania, lub jego uszkodzone części, i powiadamia o tym pozostałe państwa członkowskie i Komisję zgodnie z art. 7;
- e) zgłaszające państwo członkowskie bierze odpowiedzialność za:
 - (i) jednoznaczne przypisanie danych identyfikujących osobę, o których mowa w lit. c), oraz
 - (ii) mechanizm uwierzytelniania wymieniony w lit. d).

Państwa członkowskie, które zgłaszają systemy identyfikacji elektronicznej, bezzwłocznie przekazują Komisji następujące informacje i ewentualne późniejsze zmiany:

- a) opis zgłaszanego systemu identyfikacji elektronicznej;
- b) organy odpowiedzialne za zgłaszany system identyfikacji elektronicznej;
- c) informację o tym, kto zarządza rejestracją jednoznacznych identyfikatorów osób;
- d) opis mechanizmu uwierzytelniającego;
- e) ustalenia dotyczące zawieszania lub wycofywania zgłoszonego systemu identyfikacji lub mechanizmu uwierzytelniającego, lub ich uszkodzonych części.

Transgraniczne stosowanie środków identyfikacji elektronicznej objętych zgłoszonym systemem nakłada na państwa członkowskie obowiązek współpracy w zakresie zapewnienia interoperacyjności technicznej. Wyklucza to wszelkie krajowe szczegółowe przepisy techniczne nakładające na strony z innych krajów np. obowiązek instalowania specjalnego sprzętu lub oprogramowania w celu sprawdzenia i zatwierdzenia zgłoszonej identyfikacji elektronicznej. Państwa członkowskie muszą zapewnić jednoznaczne powiązanie między danymi związanymi z identyfikacją elektroniczną a osobą, której identyfikacja ta dotyczy. Ten obowiązek nie oznacza, że jedna osoba nie może korzystać z kilku środków identyfikacji elektronicznej, lecz wszystkie takie środki muszą być powiązane z tą samą osobą. Wiarygodność identyfikacji elektronicznej zależy od dostępności środków uwierzytelniania (tzn. możliwości sprawdzenia ważności danych powiązanych z identyfikacją elektroniczną) i rozporządzenie nakłada na zgłaszające państwa członkowskie obowiązek nieodpłatnego zapewnienia stronom trzecim dostępu do danych o ważności środków identyfikacji elektronicznej. Mechanizm weryfikacji ważności musi być dostępny bez przerwy. Rozporządzenie nie nakłada na państwa członkowskie obowiązku wprowadzania lub zgłaszania systemów identyfikacji elektronicznej, lecz **nakazuje uznawać i akceptować zgłoszone środki identyfikacji elektronicznej dla tych usług, w przypadku których identyfikacja elektroniczna jest wymagana, aby można było uzyskać dostęp na szczeblu krajowym**. Państwa członkowskie muszą przyjąć odpowiedzialność za jednoznaczność powiązania (tj. za to, aby dane identyfikacyjne przypisane jednej osobie nie zostały przypisane żadnej innej osobie) i za mechanizm uwierzytelniający (tj. za możliwość sprawdzenia ważności danych związanych z identyfikacją elektroniczną).

Istotne wnioski dla niniejszego raportu wynikające z treści projektu rozporządzenia są następujące:

- “państwowe” (notyfikowane) środki identyfikacji elektronicznej nie muszą być wydawane przez państwo – mogą to być środki wydane w imieniu państwa lub uznawane przez państwo (a więc także przez sektor prywatny),

Identyfikacja i uwierzytelnianie w usługach elektronicznych

- rozporządzenie umożliwia (wręcz zachęca) do wykorzystania środków identyfikacji elektronicznej „państwowych” w sektorze prywatnym,
- rozporządzenie umożliwia wykorzystanie przez państwo i sektor publiczny środków identyfikacji elektronicznej wydanych przez sektor prywatny,
- jedna osoba może posiadać kilka elektronicznych tożsamości (środków identyfikacji elektronicznej), co *implicite* daje możliwość federacji tożsamości,
- mechanizmy uwierzytelnienia (potwierdzania ważności środków identyfikacji) mają być dostarczane nieodpłatnie dla notyfikowanych środków identyfikacji elektronicznej.

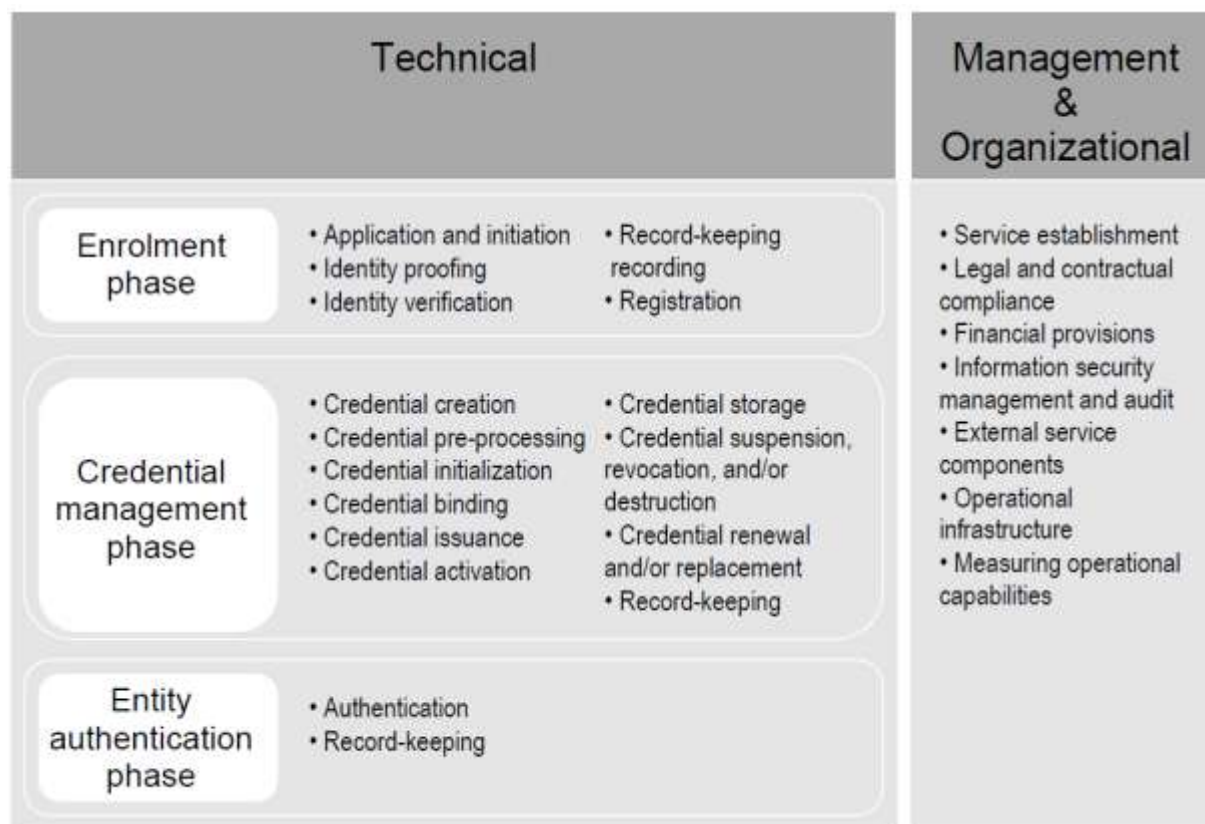
Zatem, przynajmniej w intencji, rozporządzenie ma zunifikować sektor prywatny i publiczny, stworzyć jednolity rynek usług elektronicznych oparty na wspólnych ramach dla identyfikacji i uwierzytelnienia, wymusić niejako przejście z modelu silosowego do modelu bardziej zunifikowanego i (potencjalnie) sfederowanego.

Z kolei w toku dalszych prac nad rozporządzeniem pojawiły się propozycje zmian lub nowych zapisów, m.in. dotyczących określania poziomów wiarygodności środków identyfikacji i uwierzytelnienia oraz ich interoperacyjności. Nowością jest także nałożenie odpowiedzialności prawnej na kraj członkowski za notyfikowane środki identyfikacji elektronicznej, która daje szansę zniesienia bariery wykorzystania przez sektor prywatny w usługach o wyższym poziomie ryzyka (np. bankowość elektroniczna). Jednak ostateczny kształt zapisów rozporządzenia na dzień tworzenia niniejszej pracy nie został ustanowiony, zatem w toku dalszych prac może ulec zmianie.

4.6 Norma ISO 29115

4.6.1 Struktura i poziomy wiarygodności uwierzytelnienia

Niedawno opracowana została nowa 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 urzędów**. 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 9.



Rysunek 9. Diagram poglądowy struktury wiarygodności uwierzytelnienia wg ISO 29115 [3].

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 5 przedstawia potencjalny wpływ błędnego uwierzytelnienia, przy czym siła każdego z czynników jest określona w ogólnej skali wartości: niski, umiarkowany, znaczący, wysoki²⁹. 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.

²⁹ na podstawie [3]

Tabela 5.

Potencjalny wpływ błędnego uwierzytelnienia	Poziom wiarygodności (<i>Level of Assurance</i>)			
	1	2	3	4
Niewygoda, dolegliwość lub uszczerbek na reputacji lub pozycji	niski	umiarkowany	znaczący	wysoki
Strata finansowa lub odpowiedzialność podmiotu ³⁰	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

Należy dodać, iż norma dopuszcza zdefiniowanie przez organizację używającą standardu dodatkowych czynników (niewymienionych w tabeli Tabela 5) 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);

³⁰ w oryginale „agency liability”

Identyfikacja i uwierzytelnianie w usługach elektronicznych

- 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 tę operację stronie trzeciej.

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

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.

4.6.2 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

Identyfikacja i uwierzytelnianie w usługach elektronicznych

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 6 – 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

Identyfikacja i uwierzytelnianie w usługach elektronicznych

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 wytworzenia. 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 środkami 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.

Identyfikacja i uwierzytelnianie w usługach elektronicznych

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 fizycznie (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 uwierzytelniających (jeśli stosuje się).

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.

4.6.3 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.

4.6.4 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 poziom 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 wchodzi 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).

4.7 Standard NIST SP 800-53

Omawiając problematykę identyfikacji i uwierzytelnienia z punktu widzenia regulacji unijnych (dyrektywa 99/93/EC, projekt rozporządzenia eIDAS, standardy CWA i ETSI) i normy międzynarodowej ISO 29115, nie sposób nie wspomnieć również o standardzie amerykańskim NIST SP 800-53. *Special Publication* Narodowego Instytutu Standaryzacji i Technologii (NIST). „SP 800-53” opisuje praktycznie wszystkie możliwe zabezpieczenia spotykane w systemach teleinformatycznych. Generalnie podzielono je na trzy klasy: „techniczne” (ang. *technical*), „operacyjne” (ang. *operational*) i „zarządcze” (ang. *management*). Ponadto wyróżniono kilkanaście rodzin (ang. *family*), wśród których znajduje się „Identyfikacja i uwierzytelnienie” (ang. *Identification and Authentication* - IA), zaliczona do klasy „technicznej”.

W zakresie IA NIST wymaga na wstępie, aby jednostka organizacyjna opracowała i udokumentowała, jak również zakomunikowała zainteresowanym stronom, a następnie – w miarę potrzeby – aktualizowała politykę i procedury związane z identyfikacją i uwierzytelnieniem. Polityka i procedury muszą być przeglądane nie rzadziej niż raz do roku, ewentualnie aktualizowane i publikowane zgodnie z odpowiednią procedurą.

W polityce identyfikacji i uwierzytelnienia określa się:

- a) cel i zakres działań dot. identyfikacji i uwierzytelnienia,
- b) role i odpowiedzialność pracowników zajmujących się identyfikacją i uwierzytelnieniem,
- c) zasady zaangażowania kierownictwa,
- d) zasady koordynacji działań związanych z identyfikacją i uwierzytelnieniem w ramach jednostki organizacyjnej oraz
- e) zasady zapewnienia zgodności.

Z kolei odpowiednie procedury postępowania stanowią implementację zapisów polityki, a działania wykonywane zgodnie z procedurami mają zapewnić skuteczne wdrożenie mechanizmów identyfikacji i uwierzytelnienia.

Warto odnotować, że standard NIST SP 800-53 zawiera szczególnie dużo (na tle innych dokumentów normatywnych i standaryzacyjnych) wskazówek praktycznych związanych z administrowaniem (wdrożeniem), poszczególnych grup zabezpieczeń, w tym również IA. Poznanie tych szczegółowych

Identyfikacja i uwierzytelnianie w usługach elektronicznych

wymagań i rekomendacji może być pomocne przy podejmowaniu decyzji związanych z mechanizmami identyfikacji i uwierzytelnienia. W rozdziale 11 (załączniku) przedstawiono najważniejsze aspekty poprawnie wdrożonej polityki bezpieczeństwa w zakresie identyfikacji i uwierzytelnienia wg dokumentu NIST SP 800-53.

5 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.

5.1 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 szczególnie użyteczny dla podpisu elektronicznego – oświadczenie woli jest szyfrowane przy pomocy klucza A („prywatnego”), natomiast weryfikacja podpisu odbywa się przy pomocy klucza komplementarnego B („publicznego”). Najbardziej popularnym przykładem takiego algorytmu jest RSA.³¹

5.1.1 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 najprostszej 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 (zwykle na nośniku tradycyjnym - papierowym). 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;

³¹ nazwa pochodzi o nazwisk autorów: Ron Rivest, Adi Shamir i Leonard Adleman

Identyfikacja i uwierzytelnianie w usługach elektronicznych

- 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.

Norma PN ISO/IEC 18031 odnosi się generalnie do dwóch rodzajów generatorów: niedeterministycznych (losowych, wykorzystujących zjawisko fizyczne) i deterministycznych (tzw. pseudolosowych, opartych o przekształcenia kryptograficzne)³². Zwraca się uwagę, że w przypadku generatorów deterministycznych musi być wykorzystywane ziarno losowe o entropii nie mniejszej niż 128 bitów. Ten aspekt jest często pomijany i zastosowane ziarno ma zdecydowanie niższą entropię, co nie powinno mieć miejsca. Np. wykorzystuje się parametr daty i czasu kodowanej formalnie na 12 znakach (po dwa na: rok-miesiąc-dzień-godzina-minuta-sekunda). Jednak taki argument nie posiada entropii porównywalnej z długością bitową parametru, a zdecydowanie dużo mniejszą, gdyż atakujący z góry odrzuci ciągi niemożliwe, np. miesiąc „13”, czy godzinę „27”, nie mówiąc o tym, że pole „rok” nie daje żadnej entropii, albo co najwyżej 1-bitową (jest praktycznie jednoznacznie zdeterminowane).

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

³² lub „hybrydowych”, będących połączeniem obu rodzajów

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:

$$H_i = \text{SHA}(\text{KEY} \parallel \text{NR_KONTA} \parallel i), \text{ gdzie } \parallel \text{ oznacza konkatencję bitów.}$$

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 nieznanym 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

Identyfikacja i uwierzytelnianie w usługach elektronicznych

pamięci przechowuje klucz poufny (KEY_{NR_TOKEN}). Każdy token ma klucz indywidualny, który jest obliczany z klucza losowego serwera (KEY) wg następującego wzoru:

$$KEY_{NR_TOKEN} = \text{SHA}(\text{KEY} \parallel \text{NR_TOKEN}) \quad (\&).$$

Natomiast hasło jednorazowe H_i jest generowane przez token w oparciu o aktualną datę i czas (DATA_TIME) z dokładnością do 1 minuty³³ oraz klucz indywidualny tokena:

$$H_i = \text{SHA}(KEY_{NR_TOKEN} \parallel \text{DATA_TIME}) \quad (\&\&).$$

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 pkt. 0.

5.1.1.1 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 którym 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

³³ „jednorazowość” hasła klienta polega na tym, że zmienia się w każdej minucie

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.

5.1.2 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. tę 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.

5.1.2.1 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 zwykle 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 nierozzerwalnie 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.

5.1.2.2 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 GUI³⁴, 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 elektronicznych” 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.

³⁴ ang. *Graphical User Interface* – interfejs graficzny użytkownika

5.1.3 Podpis serwerowy

W niniejszym pkt. opracowania zostaną omówione kwestie *podpisów serwerowych*, które są modyfikacjami standardowych rozwiązań PKI z tokenami programowymi lub sprzętowymi, a mianowicie „profil zaufany” i „mediator”. W obu przypadkach twórcy koncepcji nie brali pod uwagę konieczności ścisłej zgodności z normami i standardami, stąd *mediator* nie wyszedł poza stadium koncepcji, natomiast *profil zaufany* został wdrożony przez polską administrację rządową, jednak co najmniej dyskusyjna jest w jego przypadku kwestia bezpieczeństwa rozwiązania, jak również zgodność ze standardami w zakresie stosowanych formatów danych.

Zanim jednak zaprezentowane zostaną te „krajowe” rozwiązania, należy poruszyć kwestię dobrych praktyk implementacji podpisów elektronicznych weryfikowanych w ramach infrastruktury PKI i dokonania rozróżnienia, czy mamy do czynienia z uwierzytelnieniem w ramach składania różnego rodzaju oświadczeń woli, czy też uwierzytelnień wykonywanych w ramach protokołów logowania się on-line do usług/aplikacji serwerowych.

5.1.3.1 Podpis elektroniczny vs podpis cyfrowy

Profesjonalne podejście do implementacji mechanizmów PKI i związanych z nimi metod realizacji podpisów elektronicznych do „identyfikacji” bądź składania oświadczenia (np. woli – patrz pkt 4.1.2), czy to przy pomocy dowodu osobistego, „profilu zaufanego”, karty zdrowia itp., wymaga rozróżnienia „rodzaju podpisu” jaki składa obywatel w danej sytuacji. Przede wszystkim rozróżnia się, czy „podpis” jest składany w ramach protokołów logowania się do danego serwera („on-line”, czyli identyfikacja), czy też jest to podpis związany z oświadczeniem woli typu podpisanie umowy kupna sprzedaży (zwykle wykonywany „off-line”). Otóż w tym pierwszym przypadku (logowania do serwera) składający podpis jest proszony o podpisanie losowych danych, tzw. wyzwania (ang. *challenge*) w ramach protokołu challenge-response. Gdy przedstawia się on pewnym certyfikatem (klucza publicznego), serwer weryfikuje, czy certyfikat jest ważny (podpis urzędu CA na certyfikacie i sprawdzenie, czy certyfikat przypadkiem nie jest unieważniony), a następnie serwer żąda potwierdzenia, czy dana osoba jest w posiadaniu klucza prywatnego, komplementarnego z publicznym zawartym w sprawdzonym i zaakceptowanym certyfikacie. W tym celu serwer wysyła losowe dane, które podpisuje host przy pomocy swojego klucza prywatnego. Dzięki czemu jest w stanie wykazać posiadanie klucza prywatnego bez jego ujawniania. W standardach zwraca się uwagę na aspekt składania podpisu pod losowymi danymi, co rodzi ryzyko ataków na implementacje, w ramach których można byłoby „wyludzić” podpisy – składający podpis w dobrej wierze podpisuje dane w ramach logowania się do serwera, a atakujący ingeruje w ich losowość i podstawia dane specjalnie przez niego spreparowane. Jest to istotne o tyle, że nigdy nie podpisuje się bezpośrednio wiadomości, a jedynie skrót wykonany kryptograficzną funkcją skrótu, np. SHA. Atakujący może wobec tego podmienić skrót i przedstawić taki, który pochodzi z wiadomości przygotowanej przez napastnika.

Stąd do podpisów w ramach logowania do serwera należy stosować jedną parę kluczy, a przy „oświadczeniach” drugą. To rozróżnienie odbywa się technicznie w ramach certyfikatu X.509 w rozszerzeniu „keyUsage”. Przy logowaniu do serwera ustawia się bit „digital signature” (czyli jest to tzw. podpis cyfrowy), a przy różnego rodzaju oświadczeniach ustawia się z kolei bit „nonRepudiation”. W ten sposób aplikacje weryfikujące wiedzą, który z certyfikatów wybrać i tym samym redukują ryzyko skutecznych ataków.

Należy jednocześnie zaznaczyć, iż najnowsze prace standaryzacyjne dotyczące profilu certyfikatów X.509 (RFC 5280) zmieniły nazwę bitu *nonRepudiation* na *contentCommitment*, czyli „zobowiązanie odnośnie treści”. Z kolei rozróżnienie o jaki rodzaj zobowiązania chodzi w przypadku danego podpisu (oświadczenie woli, potwierdzenie dostarczenia, potwierdzenie wysłania itp.) dokonuje się nie w certyfikacie, a w tzw. podpisanym atrybucie zawartym w treści wiadomości. Nie ma to jednak znaczenia dla „podpisów cyfrowych” (logowanie do serwera i podpisywanie losowych wyzwań), a jedynie dla „podpisów elektronicznych” (różnego rodzaju oświadczenia), gdzie podpisuje się skróty z konkretnych plików.

5.1.3.2 Profil zaufany

W „normalnej” implementacji PKI 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*).

„Profil zaufany” nie należy do kategorii *standardowej* implementacji PKI. Otóż w jego przypadku podpisującym jest zawsze serwer, który posiada jedną parę kluczy (przechowywaną w sprzętowym tokenie). W celu złożenia podpisu pod pewną wiadomością dokonuje się standardowych przekształceń matematycznych z wykorzystaniem klucza prywatnego. Jednak ten sam klucz prywatny (serwera) jest wykorzystywany do składania podpisów elektronicznych przez dowolną osobę, stąd trzeba dodatkowo dokonać rozróżnienia, w czym imieniu dany podpis jest składany. W „normalnej” PKI służy do tego wspomniany wcześniej certyfikat X.509 klucza publicznego podpisującego, a podpisujący jest identyfikowany w polu „właściciel” (ang. *Subject*). Natomiast w ramach informacji zamieszczonej w tzw. formacie podpisanej wiadomości znajduje się jednoznaczne wskazanie, jakim certyfikatem należy weryfikować podpis pod daną wiadomością. Normy i standardy są tak pomyślane, że podpisujący może mieć kilka certyfikatów, nawet dla jednego klucza publicznego, stąd wymusza się jednoznaczne wskazanie konkretnego certyfikatu dla danego podpisu. W przypadku profilu zaufanego mamy odwrócenie zasady na bazie której stworzono standardy, iż identyfikacja podpisującego odbywa się poprzez jego certyfikat. W przypadku profilu zaufanego certyfikat jest jeden (klucza publicznego serwera), a rozróżnienie o czyj podpis chodzi w konkretnym pliku dokonuje się w ramach pola *SignerRole*. Dokumenty standaryzacyjne przewidują, iż pole „rola podpisującego” („*SignerRole*”) może zawierać doprecyzowanie w jakiej roli występuje podpisujący w kontekście tego konkretnego podpisu elektronicznego, np. podpisujący Jan Kowalski złożył dany podpis elektroniczny jako kierownik działu sprzedaży³⁵, a w innym przypadku ten sam Jan Kowalski (ten sam certyfikat i oczywiście ten sam klucz prywatny) składa podpis jako osoba fizyczna. W przypadku profilu zaufanego nie ma możliwości doprecyzowania „roli podpisującego”, gdyż to pole zostało wykorzystane do wskazania prawdziwego podpisującego, a nie jego roli. Innymi słowy w przypadku profilu zaufanego dokonano zamiany znaczenia pewnych pól w formacie podpisanej wiadomości (podpisującym nie jest „właściciel” certyfikatu – pole *Subject*), a poprzez usunięcie możliwości doprecyzowania w podpisie roli podpisującego, dokonano

³⁵ ang. *Sales Director* (przykład wzięty bezpośrednio ze standardu ETSI TS 101 903 - XAdES, pkt 7.2.8)

ograniczenia zakresu wykorzystania podpisów elektronicznych w stosunku do aplikacji wykorzystujących zdefiniowane w standardach pola (SignerRole może wystąpić tylko raz).

Formaty podpisanych wiadomości pełnią istotną funkcję przy implementacji rozwiązań w zakresie elektronicznej identyfikacji i elektronicznego uwierzytelnienia. Zgodność z odpowiednimi standardami gwarantuje odporność na pewne rodzaje ataków, a przede wszystkim pozwala na zapewnienia *interoperacyjności*. O ile w sektorze bankowym interoperacyjność rozwiązań nie jest kluczowym atrybutem, a często wręcz uznaje się ją za wadę produktu, w administracji publicznej zagadnienie to jest uregulowane prawnie. Dość przypomnieć, że obowiązuje rozporządzenie Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych, w którym *do elektronicznego podpisywania, weryfikacji podpisu (...) stosuje się następujące formaty XMLsig, XAdES, PAdES i CAdES*, a które to formaty pole *SignerRole* definiują jak wyżej, czyli odmiennie niż w „profilu zaufanym”. Oczywisty konflikt norm prawnych rodzi uzasadnione obawy co do statusu profilu zaufanego oraz wątpliwości, czy w przyszłości rząd będzie dalej wspierał rozwiązanie nie tylko niestandardowe, lecz także wadliwe od strony prawnej.

Podjmując decyzję o wykorzystaniu profilu zaufanego należy wziąć pod uwagę aspekt zgodności aktualnie funkcjonującego rozwiązania z przepisami dot. ochrony danych osobowych, jak również to, iż technologia „profilu zaufanego” nie pozwala na wykorzystanie go do uwierzytelnień (identyfikacji) *on-line*, a jedynie do *off-line*. Chodzi o to, że po zalogowaniu się do serwera przy pomocy login'u i hasła podpisujący rozpoczyna procedurę składania podpisu elektronicznego, jednak do jej pomyślnego zakończenia musi dodatkowo podać serwerowi kod autoryzujący, który otrzymuje na swoją skrzynkę mail'ową lub za pośrednictwem komunikatu SMS. O ile sesja łączności podpisujący-serwer odbywa się w ramach protokołu https (zabezpieczonego kryptograficznie), to już połączenie serwer-skrzynka mail'owa jest *zwykłe*, czyli bez ochrony kryptograficznej. Natomiast przepisy rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych wyraźnie nakazują, *aby administrator danych stosował środki kryptograficznej ochrony wobec danych wykorzystywanych do uwierzytelnienia, które są przesyłane w sieci publicznej*. Stąd – poza aspektem niezgodności formatów danych ze standardami (i tym samym braku interoperacyjności) – dodatkowo dochodzi problem naruszenia przepisów ustawy o ochronie danych osobowych w przypadku podpisu elektronicznego realizowanego w technologii „profilu zaufanego”.

5.1.3.3 Mediator

Podstawą mechanizmów rozproszonego podpisywania jest możliwość złożenia podpisu elektronicznego przez więcej niż jednego uczestnika procesu (z wykorzystaniem wielu kluczy prywatnych), natomiast podpis taki jest weryfikowany pojedynczym kluczem publicznym. Mechanizmy rozproszonego podpisywania zostały stworzone celem umożliwienia budowania różnych schematów zapewnienia kontroli nad procesem podpisywania przy jednoczesnym zapewnieniu interoperacyjności w procesie ich weryfikacji.

Mechanizm rozproszonego podpisywania został zaproponowany do realizacji podpisu osoby fizycznej w środowisku dodatkowo kontrolowanym przez dostawcę usługi podpisywania – podpis z „mediatorem”. W przypadku tej technologii do złożenia i weryfikacji podpisu wykorzystuje się parę kluczy

Identyfikacja i uwierzytelnianie w usługach elektronicznych

asymetrycznego algorytmu kryptograficznego. Klucz prywatny podpisującego w procesie generacji kluczy jest modyfikowany o przypisaną mu indywidualną wartość klucza „finalizującego”, który jest wyliczany po stronie serwera zabezpieczającego proces podpisywania zwanego potocznie *mediatorem*. W celu wygenerowania podpisu elektronicznego użytkownik dokonuje przekształceń matematycznych z wykorzystaniem posiadanego klucza prywatnego, produkt tego przekształcenia nazywany jest „prepodpisem”. Następnie ten „prepodpis” jest wysyłany do serwera, który również dokonuje przekształceń matematycznych z wykorzystaniem odpowiedniego klucza finalizującego. Podpis będący produktem „finalizacji” jest weryfikowany certyfikatem X.509 wydanym dla pojedynczego klucza publicznego.

Rozwiązanie opisane algorytmem podpisu z mediatorem - „podzielenia klucza” prywatnego służącego do składania podpisów elektronicznych nie jest nowe, natomiast nie ma w tym momencie komercyjnych wdrożeń rozwiązania i nie jest wspierany przez dostawców technologii, w tym przez producentów sprzętowych tokenów SSCD. Chodzi o to, że „karty SSCD” w ich obecnej implementacji są certyfikowane pod kątem odporności na różne kategorie ataków, w tym ataków obliczonych na uzyskanie dostępu do klucza prywatnego w oparciu o obserwację czasu realizacji podpisów i/lub poboru prądu podczas wykonywania obliczeń z wykorzystaniem klucza prywatnego (atakujący obserwuje zachowania karty przy realizacji różnych podpisów), jak również ataków typu „fault injection”, inaczej zwanymi atakami typu „Bellcore”. W ostatnim przypadku przeciwnik usiłuje zmusić kartę do wykonania nieprawidłowego podpisu poprzez wymuszenie błędu przy realizacji obliczeń. Karty bez certyfikowanej odporności na „Bellcore attack” można umieścić we wrogim środowisku (np. w kuchence mikrofalowej), które powoduje błędną realizację obliczeń przy wykonywaniu podpisu. Pokazano, że dysponując podpisywanymi danymi, kluczem publicznym, podpisem błędnym i podpisem właściwym można stosunkowo prosto wyznaczyć klucz prywatny. W związku z tym karty elektroniczne SSCD nie przekazują na zewnątrz wyniku podpisu, jeśli nie można go zweryfikować wewnątrz karty kluczem publicznym – uważają wtedy, że podczas podpisywania nastąpił błąd i taki błędny podpis nie jest przekazywany na zewnątrz. Natomiast filozofia mediatora wymaga, aby token wykonał „prepodpis”, czyli wydał na zewnątrz „półprodukt”, który nie weryfikuje się kluczem publicznym i wymaga finalizacji. Akceptacja koncepcji mediatora wymagałaby certyfikacji kart pod kątem nowego algorytmu, przy niewystarczającej świadomości nowych, dotyczących go zagrożeń. Zabezpieczenie adresujące wyżej wymienione ataki, polegające na dwukrotnym wykonaniu operacji kryptograficznych i porównaniu wyników przed udostępnieniem jest rzadziej stosowane w kartach elektronicznych. Powodem zapewne jest istotne wydłużenie czasu składania podpisów (operacji matematycznych) w procesorze karty elektronicznej.

Podpis z mediatorem umożliwia zapewnienie serwerowej kontroli środowiska złożenia podpisu. Mediator w procesie podpisywania może zweryfikować dodatkowe atrybuty i poprzez finalizację dokonać autoryzacji podpisu. Podstawowymi atrybutami, których weryfikacja jest możliwa w procesie podpisywania są: czas złożenia podpisu, ważność certyfikatów służących do weryfikacji podpisu, aktualność danych zawartych w certyfikacie. Ważną cechą podpisu z mediatorem jest możliwość uzależnienia autoryzacji podpisu przez serwer finalizujący od przeprowadzenia dodatkowego uwierzytelnienia (np. sms) lub weryfikacji (np. uprawnienie w systemie wewnętrznym). Serwer mediatora może zbierać informacje o złożonych podpisach, stanowiąc dodatkowy punkt zapewnienia niezaprzeczalności procesu podpisywania.

Podpis z mediatorem i jego wykorzystanie w procesie generowania podpisu osoby fizycznej z wykorzystaniem karty kryptograficznej jest jednym z potencjalnych zastosowań rozwiązania podpisu rozproszonego. Podpisy rozproszone mogą być realizowane w oparciu o inne algorytmy (np. algorytm

Schnorra), istnieje też duże portfolio przykładowych rozwiązań, w szczególności tam, gdzie zmniejszenie wymaganych zabezpieczeń po stronie podpisującego jest kompensowane zabezpieczeniami po stronie serwerowej, a także w procesie składania podpisów za pomocą urządzeń mobilnych, podpisach grupowych, podpisach identyfikujących skopiowanie kluczy prywatnych (tzw. *forgery evident signatures*).

5.1.4 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 obszernie 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. Poświadczenie 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. pieczęć „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,
- rodzaj świadczonej usługi niezaprzeczalności,
- identyfikatora wyróżniającego podmiotu poświadczania,
- identyfikatora wyróżniającego wystawcy poświadczania w przypadku, gdy nie jest on podmiotem poświadczania,
- identyfikatora wyróżniającego podmiotu, współpracującego z podmiotem poświadczania (np. nadawcy wiadomości, albo odbiorcy, dla którego przeznaczono wiadomość albo organu dostarczającego),
- identyfikatora wyróżniającego żądającego poświadczanie w przypadku, gdy nie jest on podmiotem poświadczania,
- identyfikatorów wyróżniających pozostałych podmiotów, zaangażowanych w działanie (np. odbiorców, dla których przeznaczono wiadomość),
- daty oraz czasu wystawienia poświadczania,
- 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.

5.2 Uwierzytelnienie biometryczne

5.2.1 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) wyznaczone 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.

5.2.2 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:
 - karta elektroniczna, certyfikat cyfrowy, dowód osobisty, paszport, legitymacja, rekomendacje/listy polecające,
- czym naprawdę jesteśmy, czyli 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.

Biometryczna weryfikacja tożsamości 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. System biometryczny weryfikuje i potwierdza tożsamość i najczęściej (głównie ze względów bezpieczeństwa) prezentuje swoją decyzję w formie binarnej (tak/nie).

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)

Stosowane w biometrii cechy biologiczne to:

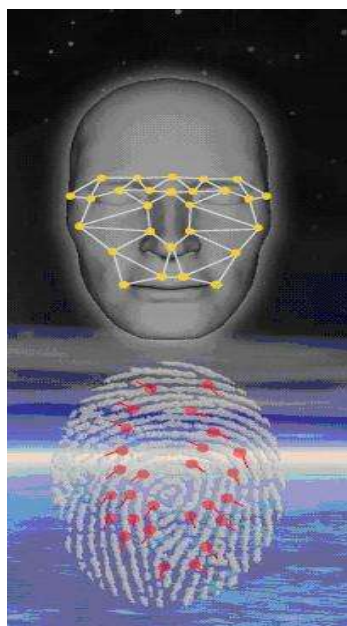
- linie papilarne - odciski palców, (prawdopodobieństwo błędnej akceptacji lub odrzucenia 10^{-3}),
- geometria dłoni, twarzy (10^{-4}),
- DNA (trudno odróżnić bliźniaków),
- obraz siatkówki, tęczówki (10^{-6}),
- naczynia krwionośne palca (ang. *Finger Vein*) i dłoni (ang. *Palm Vein*).

Stosowane w biometrii cechy behawioralne to:

- podpisy - kształt i dynamika,

Identyfikacja i uwierzytelnianie w usługach elektronicznych

- głos,
- dynamika pisania na klawiaturze (ang. *keystroke pattern*),
- chód - sposób chodzenia (ang. *gait*),
- etc.



Rysunek 10. Ilustracja idei tworzenia cech biometrycznych – twarzy i odcisku linii papilarnych.

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

Rejestracja/akwizycja danych (zapisywanie obrazu i/lub tworzenie bazy danych):

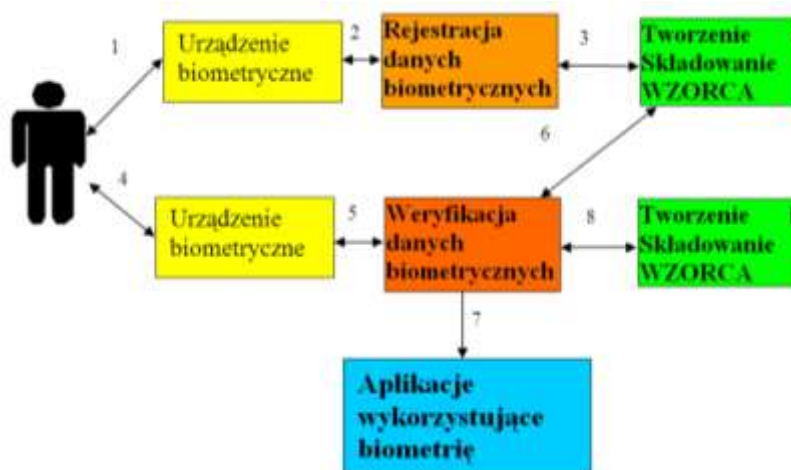
- pozyskanie wybranej cechy biometrycznej - czytnik biometryczny skanuje określoną cechę biometryczną osoby ubiegającej się o dostęp do systemu,
- przetwarzane do postaci cyfrowej, filtrowanie i tworzenie wzorca,
- zapisywanie wzorca w lokalnym lub centralnym repozytorium, lub przenośnym tokenie takim jak karta elektroniczna.

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,

Identyfikacja i uwierzytelnianie w usługach elektronicznych

- dostarczenie wyniku porównania do aplikacji biznesowej, która rozstrzyga o dopuszczeniu lub odrzuceniu potencjalnego użytkownika,
- zapisanie danych do audytu, zgodnie z wymaganiami.



Rysunek 11. Schemat wykorzystania biometrii do uwierzytelnienia.

Rysunek 11 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.

Poniższa tabela przedstawia zestawienie najpopularniejszych metod biometrycznych na rynku.

Tabela 7.³⁶

Metoda	Opis metody	Wybrani producenci

³⁶ Źródło RAPORT BIOMETRYCZNY 2.0 „Bankowość biometryczna” Grupa ds. Biometrii FTB

Identyfikacja i uwierzytelnianie w usługach elektronicznych

biometryczna		urządzeń/rozwiązań
Odcisku palca	Bazuje na układzie punktów charakterystycznych (minucji) linii papilarnych	NEC, Morpho, Precise, Crossmatch, Gemalto
Tęczówki oka	Bazuje na cechach charakterystycznych tęczówki oka	Panasonic, 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, NEC
Geometria dłoni	Bazuje na cechach charakterystycznych dłoni	HandPunch
Głosowa	Bazuje na analizie charakterystyki głosu	Nuance, EasyVoiceBiometrics, Salmat
Podpis odręczny	Bazuje na charakterystyce wizualnej podpisu (dwuwymiarowy obraz), ale także na sposobie, w jaki podpis został złożony, tj. dynamice ruchu pióra	Xyzmo, Wacom

W chwili obecnej niezawodność poszczególnych metod jest jeszcze niezadowalająca. Poniższa tabela przedstawia wskaźniki niezawodności biometrycznej weryfikacji.

Tabela 8³⁷

	Twarz	Odcisk palca	Tęczówka
Wskaźnik błędnego odrzucenia (ang. <i>False Rejection Rate – FRR</i>) np. uprawniony, lecz niez zaakceptowany (ang. <i>Authorized but rejected</i>)	3.3-70%	0.2-30%	1.9-6%
Wskaźnik błędnej akceptacji (ang. <i>False Acceptance Rate – FAR</i>) np. nieuprawniony, lecz zaakceptowany (ang. <i>Unauthorized but accepted</i>)	0.3-5%	0-8%	<1%
Wskaźnik niemożności rejestracji (ang. <i>Failure to Enroll Rate</i>)	0%	2-5%	0.5%

Przedstawione wskaźniki będą ulegać polepszeniu z poprawą technologii i poprzez użycie dwu lub więcej identyfikatorów biometrycznych – obecnie przy użyciu wizerunku twarzy i 2 odcisków palców uzyskuje się poprawność rzędu 96%.

5.2.3 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

³⁷ Źródło (Source: U.S General Accounting Office report, "Using Biometrics for Border Security", Nov 2002)

Identyfikacja i uwierzytelnianie w usługach elektronicznych

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 uwierzytelniania 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.

5.2.4 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.

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

Identyfikacja i uwierzytelnianie w usługach elektronicznych

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 wypłatach 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,
- uwierzytelnianie transakcji w terminalach POS - Pay by Finger,
- kontrola dostępu do skrzytek depozytowych w bankach i na poczcie.

Poniżej z kolei przedstawione są przykłady wykorzystania uwierzytelnienia biometrycznego po stronie wewnętrznej organizacji/przedsiębiorcy.

- 1) kontrola dostępu do pomieszczeń - biometria stanowi idealne rozwiązanie do ochrony krytycznych stref w budynkach,
- 2) rejestracja czasu pracy - biometria pozwala na rzetelną kontrolę czasu pracy pracowników,
- 3) biometria podnosi poziom bezpieczeństwa logowania do zasobów sieciowych i systemów biznesowych,
- 4) biometria uwierzytelnia operacje na komputerach PC (drukowanie, modyfikacje plików itd.),
- 5) 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.

5.3 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 nieruchomości, 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.

5.4 Uwierzytelnienie oparte na wiedzy

Uwierzytelnienie oparte na wiedzy (ang. *knowledge-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.

5.5 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).

5.6 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, przynależności zawodowej (zob. także rozdział 5.7).

5.7 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.

Identyfikacja i uwierzytelnianie w usługach elektronicznych

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. Jedną 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 jakiegokolwiek informacji związanej z podpisywaną wiadomością lub podpisaną wiadomością,
- 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 Assessment (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

Identyfikacja i uwierzytelnianie w usługach elektronicznych

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 techniczne³⁸:

- 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 implementacje 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) przekazany 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;

³⁸ z wykorzystaniem kart elektronicznych

Identyfikacja i uwierzytelnianie w usługach elektronicznych

- 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.

6 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. Mikroprocesor³⁹ 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 bardziej poprawnie IAS (*Identification, Authentication, Signature* co oznacza w języku polskim identyfikację, uwierzytelnienie i podpis).

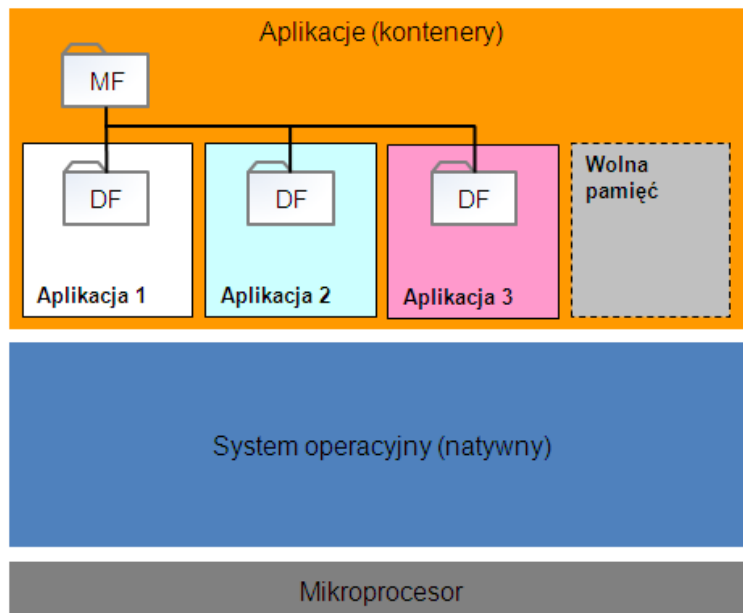
Wyróżnia się dwa podstawowe rodzaje kart elektronicznych (ze względu na technologię systemu operacyjnego):

- 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

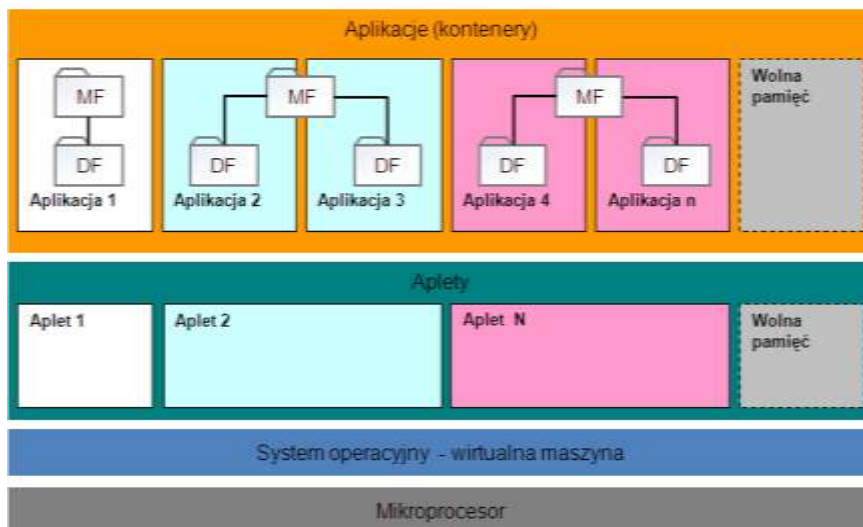
³⁹ przyjęła się potoczna nazwa „mikroprocesor”, chociaż prawidłowo powinno mówić się „mikrokontroler”. Mikroprocesor jest jedynie elementem mikrokontrolera, obok pamięci, szyny adresowej i danych.

„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 12. 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 13. Uproszczony model warstwowy karty z maszyną wirtualną.

6.1.2 Karty do kwalifikowanego podpisu elektronicznego - SSCD

Urządzenia stosowane w szeroko rozumianym PKI są dwójakiego rodzaju: HSM⁴⁰,y używane przez root-a i podmioty świadczące usługi certyfikacyjne (CA) oraz „bezpieczne urządzenia do składania podpisów elektronicznych⁴¹” (ang. *Secure Signature Creation Devices* - SSCD) wykorzystywane przez użytkowników końcowych. Wymagania unijne⁴² dla tych dwóch rodzajów urządzeń są istotnie różne.

Otóż HSM musi mieć jeden z trzech rodzajów certyfikatów:

- FIPS 140 poziom 3 (lub poziom 4);
- Common Criteria (CC) EAL 4 (lub wyżej) albo
- ITSEC E3 „high” (lub wyżej).

Natomiast SSCD muszą mieć certyfikat Common Criteria (CC) EAL4+, ale:

- a) wydany przez *designated body* zgodnie z dyrektywą 1999/93/WE oraz
- b) procesor (tzw. „krzem”) i system operacyjny karty (ewentualnie z apletem w przypadku kart typu Java) łącznie muszą mieć potwierdzoną zgodność z profilem SSCD.

⁴⁰ ang. *Hardware Security Module*

⁴¹ polskie przepisy dot. podpisu elektronicznego używają nazwy „komponent techniczny”

⁴² Decyzja Komisji nr 709 z dnia 6 listopada 2000 roku w sprawie minimalnych kryteriów, które muszą być wzięte pod uwagę przy ustanawianiu jednostek certyfikujących (*designated body*), potwierdzających zgodność bezpiecznych urządzeń do składania podpisów elektronicznych z wymaganiami unijnymi oraz Decyzji Komisji nr 511 z dnia 14 lipca 2003 roku, która wprowadza obligatoryjność pewnych dokumentów Europejskiego Komitetu Normalizacyjnego (CEN)

Identyfikacja i uwierzytelnianie w usługach elektronicznych

Często dostawcy kart starają się wykorzystać brak wiedzy odbiorcy i prezentują nieuprawnione stanowisko, że posiadają stosowne certyfikaty na SSCD, bo np. potwierdzili, że spełniają amerykański standard FIPS 140 na poziomie 3, albo mają certyfikat CC EAL5 na procesor karty (brak zgodności z profilem SSCD), albo mają CC EAL 4+ wydany przez podmiot, który nie ma statusu „wyznaczonego” zgodnie z dyrektywą.

Warto odnotować, że w obszarze oceny zgodności w UE mamy do czynienia z dwoma zagadnieniami: „certyfikatami” i „deklaracjami zgodności”. Certyfikaty są zawsze wydawane przez *strony trzecie* (niezależna ocena), natomiast deklarację zgodności może również wydawać *strona pierwsza* (producent) lub *strona druga* (dystrybutor), a nie tylko *trzecia*. Zarówno certyfikaty, jak i deklaracje zgodności, wydaje się na podstawie testów i badań. W związku z tym „deklaracja zgodności” jest często niepoprawnie określana mianem „samocertyfikacji”. Pojęcie certyfikatu w UE jest bowiem zarezerwowane dla niezależnych od producentów lub sprzedawców badań i ocen danego produktu. W dalszym pkt. dokumentu zostaną przedstawione zagadnienia certyfikacji „bezpiecznych urządzeń do składania podpisów elektronicznych” (SSCD) w odniesieniu do *stron trzecich*, uprawnionych do wydawania certyfikatów („ciała wyznaczone”) oraz szczegółowych wymagań stawianych takim urządzeniom (profil SSCD).

Ciała wyznaczone (ang. designated body)

Sprawdzenie, czy pewien certyfikat jest wydany przez *ciało wyznaczone* jest proste. Mówi o tym dyrektywa 1999/93/WE, a mianowicie art. 3.4:

„Zgodność bezpiecznych urządzeń służących do składania podpisu z wymogami ustanowionymi w załączniku III, stwierdza właściwy organ publiczny lub prywatny, wskazany przez Państwo Członkowskie. Komisja, zgodnie z procedurą ustanowioną w art. 9, formułuje kryteria obowiązujące Państwa Członkowskie w celu ustalenia, jak taki organ powinien być powołany. Stwierdzenia zgodności z wymogami ustanowionymi w załączniku III wydawane przez organy określone w akapicie pierwszym, uznawane są przez wszystkie Państwa Członkowskie”.

Ponadto art. 11 dyrektywy nakazuje państwom członkowskim poinformowanie Komisji oraz pozostałych krajów członkowskich:

- kto jest nadzorcą nad podmiotami wydającymi kwalifikowane certyfikaty (w Polsce jest to Minister Gospodarki),
- nazwy i adresy kwalifikowanych podmiotów świadczących usługi certyfikacyjne oraz
- nazwy i adresy ciał wyznaczonych (*designated body*), czyli jednostek certyfikujących, które wydają certyfikaty na komponenty techniczne związane z podpisem elektronicznym.

Czyli *designated body* to podmiot, o którym mowa w art. 3.4 dyrektywy i Unia publikuje listę takich „wyznaczonych ciał” na stronie <http://www.fesa.eu/countries.html>

Certyfikat wydany przez taki podmiot musi być honorowany na obszarze całej Unii. W przypadku wątpliwości można zwrócić się do organu nadzorującego z ramienia danego rządu, ale nie wolno kwestionować „jakości” certyfikatu. W przypadku uzasadnionych wątpliwości Jednostka Certyfikująca wdraża stosowne środki w ramach nadzoru nad wydanym certyfikatem, w tym w ostateczności unieważnia certyfikat.

Identyfikacja i uwierzytelnianie w usługach elektronicznych

Jak wspomniano wyżej certyfikat musi być wydany na urządzenie SSCD jako całość, czyli na procesor i system operacyjny (ewentualnie także odpowiedni aplet) łącznie. Decyzja Komisji nr 511 z 2003 r. narzuciła wymaganie, aby SSCD były zgodne z profilem zabezpieczeń opisanym w dokumencie CWA 14169 „Secure signature-creation devices - EAL 4+”. Regulacje UE mówią, że jest możliwe etapowe uzyskiwanie takiego certyfikatu i zwykle tak się dzieje. To znaczy, że w pierwszym etapie producent uzyskuje certyfikat CC na procesor, natomiast dopiero na drugim etapie jest uzyskiwany certyfikat na system operacyjny (i aplet) osadzony na wcześniej certyfikowanej masce krzemowej.

Używając daną kartę elektroniczną jako SSCD trzeba wziąć pod uwagę tzw. raport z certyfikacji, w którym *wyznaczone ciało* może zawrzeć pewne zastrzeżenia dotyczące ważności certyfikatu. Parę lat temu zastrzeżenia te istotnie ograniczały funkcjonalność możliwą do wykorzystania, natomiast produkty ostatnio certyfikowane jako SSCD mają tych zastrzeżeń mniej. Np. w przeszłości nie można było dodać do certyfikowanej karty jakiegokolwiek niescertyfikowanego apletu, w przeciwnym razie traciło się certyfikat na SSCD. Dzisiaj zwykle można dodawać inne aplety, przynajmniej tak jest w ofercie wiodących producentów kart. W każdym przypadku należy sprawdzić w Certification Report, czy mechanizmy separujące w systemie operacyjnym karty są wystarczające.

Można spotkać interpretację rozszerzającą Decyzji 2000/709/EC polegającą na tym, że skoro *designated body* z listy Komisji są członkami porozumień o wzajemnym uznawaniu certyfikatów wydanych przez jakikolwiek podmiot będący sygnatariuszem porozumienia (np. SOGIS MRA) to certyfikaty o podobnym poziomie zabezpieczeń wydane przez dowolny podmiot z tego porozumienia powinny być również akceptowalne. Taka interpretacja stoi jednak w sprzeczności z kolejnym dokumentem Europejskiego Komitetu Normalizacyjnego, a mianowicie uzgodnieniem roboczym CWA 14172-5. Znajduje się tam następujący zapis:

(...)

G.5.8 Wyznaczone ciała uczestniczące w porozumieniach o wzajemnym uznawaniu certyfikatów powinny dokonać rozróżnienia między wydawaniem certyfikatów zgodności dla bezpiecznych urządzeń do składania podpisów elektronicznych (dobrowolna certyfikacja produktów) i aprobat dla takich urządzeń (oficjalnych dokumentów potwierdzających w ramach UE spełnienie przez urządzenie wymagań zawartych w aneksie III Dyrektywy 199/93/EC). To powoduje, że certyfikaty wydawane przez podmiot będący członkiem np. porozumienia SOGIS MRA lub CCRA, nie są automatycznie aprobatą zgodną z prawem Unii na takie urządzenie. Wyznaczone ciało powinno żądać w takiej sytuacji od wnioskującego o aprobatę dostarczenia raportu z badań i oceny, i dopiero na tej podstawie zdecydować niezależnie o wydaniu aprobaty bez wykonywania ponownych badań urządzenia.

Reasumując: karta elektroniczna SSCD to taka karta kryptograficzna, która posiada stosowny certyfikat na zgodność z „profilem SSCD” wydany przez wyznaczoną jednostkę certyfikującą (*designated body*).

Karty elektroniczne z „certyfikatem SSCD” cechują się potwierdzoną odpornością na całe spektrum ataków, w tym w szczególności ataków obliczonych na uzyskanie dostępu do klucza prywatnego w oparciu o obserwację czasu realizacji podpisów i/lub poboru prądu podczas wykonywania obliczeń z wykorzystaniem klucza prywatnego (atakujący obserwuje zachowania karty przy realizacji różnych podpisów), jak również ataków typu *fault injection*, inaczej zwanymi atakami typu „Bellcore”.

Na rynku znajduje się wiele kart elektronicznych z funkcjonalnościami „SSCD”, jednak bez stosownego certyfikatu. Karty te są tańsze, ale ich użycie niesie z sobą ryzyko przełamania zabezpieczeń i np. sklonowania karty. **Należy zaznaczyć, że bardzo prawdopodobne jest, iż karta elektroniczna z funkcjonalnościami SSCD nie posiada „certyfikatu SSCD”, gdyż podczas procesu oceny wykazano jakieś słabości danego rozwiązania**, stąd należy wziąć taką ewentualność pod uwagę przy decyzji o wyborze konkretnej oferty dostawy kart elektronicznych.

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 - nośników podpisu kwalifikowanego (SSCD), a więc zgodnie z wymaganiami dla najwyższego poziomu wiarygodności uwierzytelnienia⁴³.

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 tę 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.

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:

⁴³ tak stanowi dokument PKN-CEN/TS 15480 „Identification card systems – European Citizen Card”

Identyfikacja i uwierzytelnianie w usługach elektronicznych

- przesyłane pocztą karty zdrapki lub karty haseł jednorazowych,
- jednorazowe hasła przesyłane przez SMS.

W przypadku generowania haseł po stronie uwierzytelniającego najczęściej stosowane są:

- tokeny kryptograficzne, zawierające czynnik losowy (ang. *salt*),
- aplikacje na telefony komórkowe.

Do niedawna najpopularniejszą i zarazem najprostszą metodą dostarczania haseł jednorazowych do użytkownika była dystrybucja pregenerowanych 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.

6.4 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 14. 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),

Identyfikacja i uwierzytelnianie w usługach elektronicznych

- 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, w tym trybie 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 Uwierzytelnienie a czytniki kart elektronicznych

6.5.1 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 OSI⁴⁴). Obecnie najbardziej rozpowszechnionym standardem protokołu komunikacyjnego czytników z komputerem jest PC/SC. Rozszerzeniem funkcji czytnika było dodanie klawiatury do wprowadzania kodów PIN (ang. PinPad).

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

⁴⁴ ang. *Open System Interconnections*

Identyfikacja i uwierzytelnianie w usługach elektronicznych

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), podlegająca 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.



Rysunek 15. 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 założenia 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.

Identyfikacja i uwierzytelnianie w usługach elektronicznych

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 CVC⁴⁵) 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. udowodnia 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.

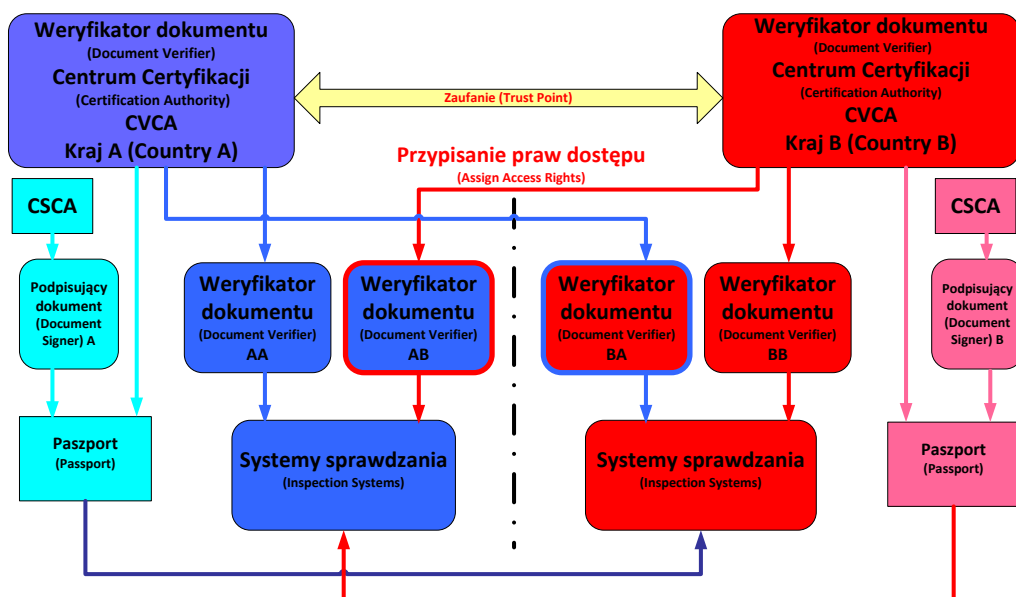
6.5.2 Uwierzytelnienie terminala

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.

⁴⁵ ang. Card Verifiable Certificate – certyfikat weryfikowalny przez kartę; jest to „lekka” wersja certyfikatu klucza publicznego, który, w odróżnieniu od certyfikatu X.509, może być interpretowany przez mikroprocesor karty

Identyfikacja i uwierzytelnianie w usługach elektronicznych



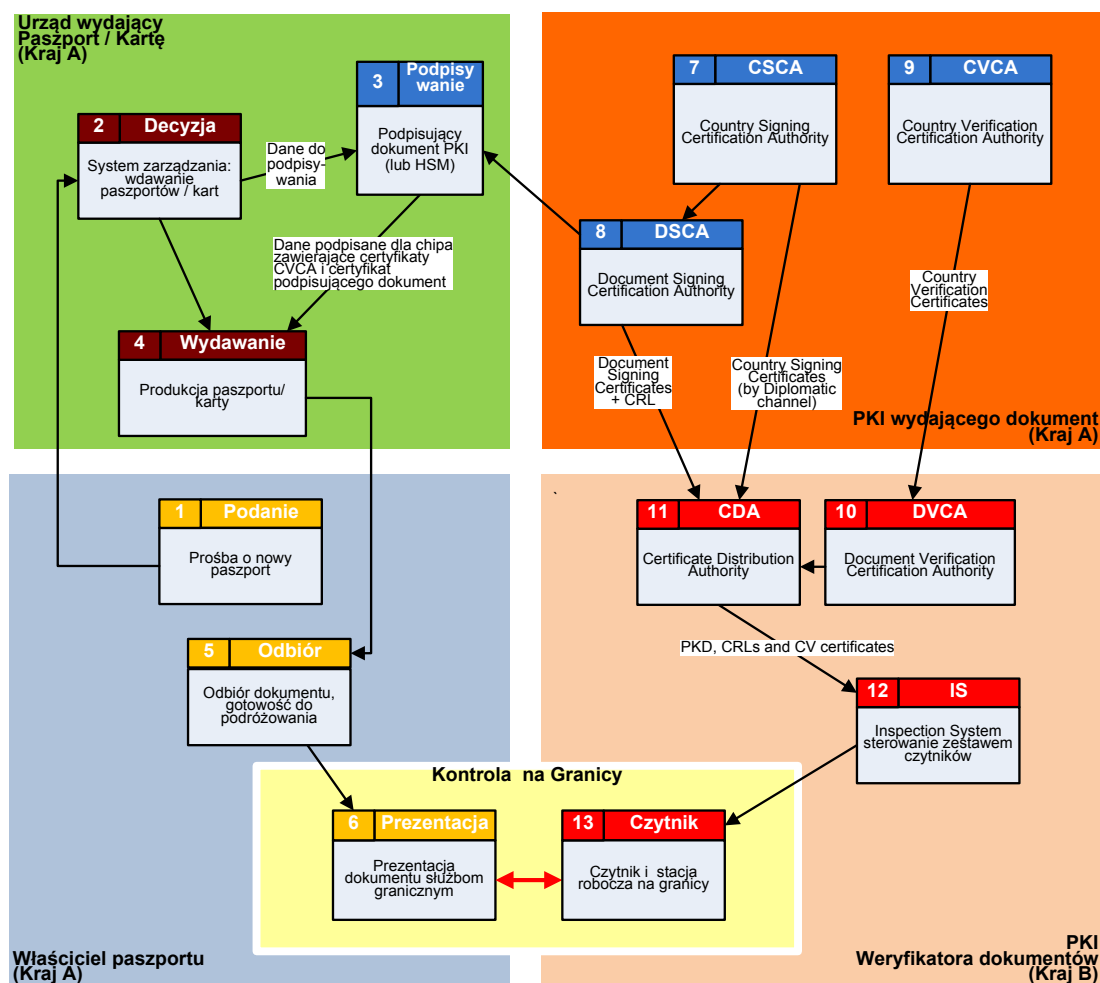
Materiały: Franciszek Wołowski

Rysunek 16. 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.

Identyfikacja i uwierzytelnianie w usługach elektronicznych

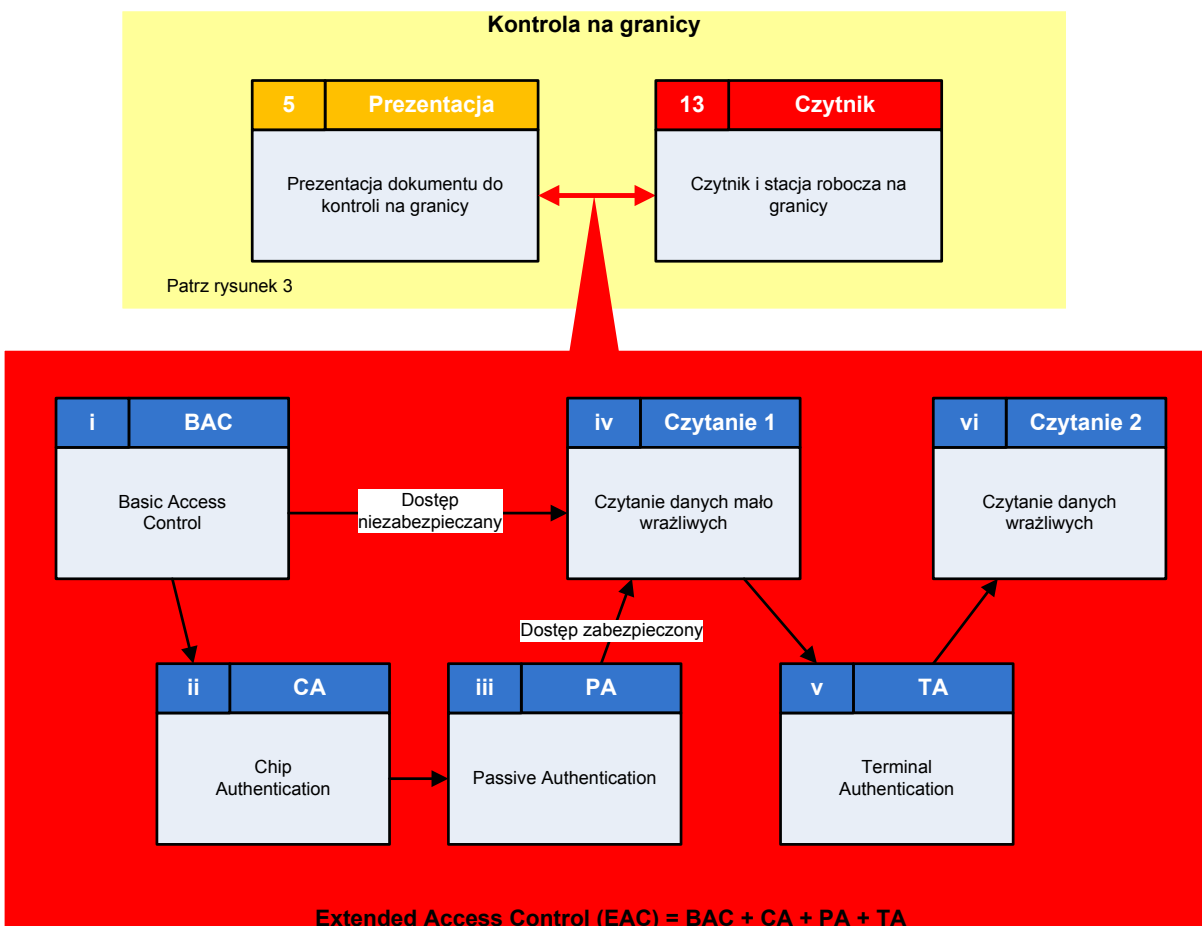


Rysunek 17. Proces związany z cyklem życia paszportów biometrycznych.

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 realizowana 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 paszportu⁴⁶), czy również rozszerzona kontrola dostępu, tj. dodatkowo odciski palców.

⁴⁶ ang. *Active Authentication* lub *Chip Authentication*, czyli potwierdzenie, iż paszport nie został sklonowany

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



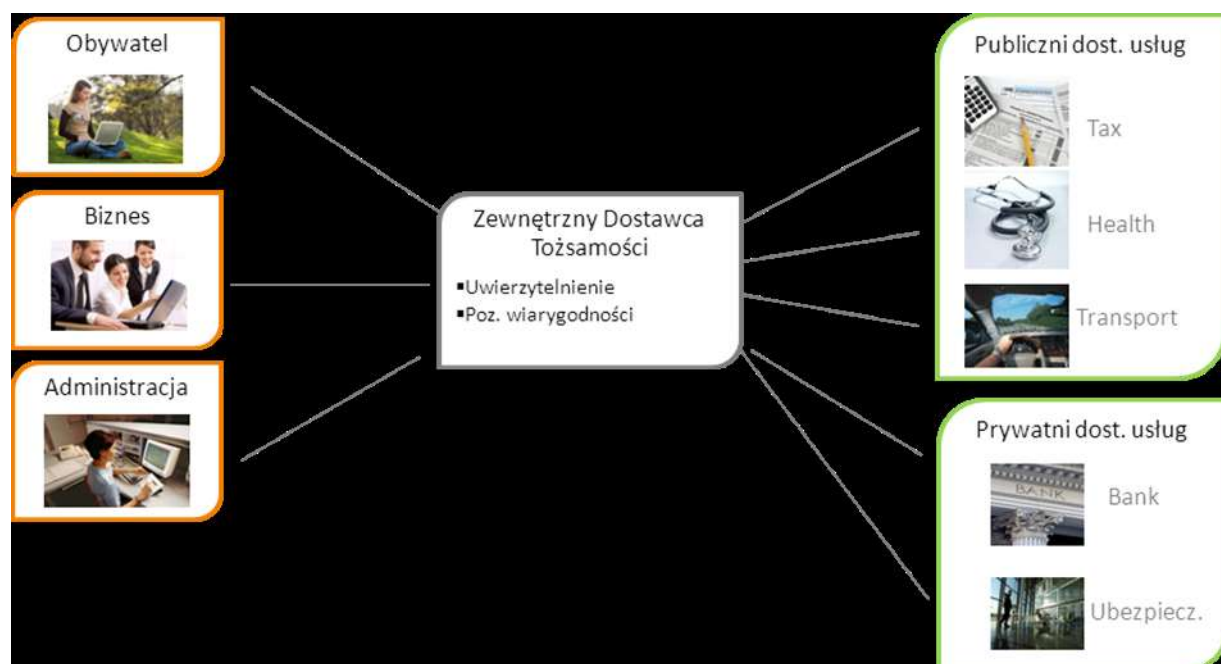
Rysunek 18. Schemat weryfikacji paszportu na granicy.

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, profili ochrony, specyfikacji testów itp.) oraz wdrożeniu do eksploatacji we wszystkich krajach członkowskich paszportów elektronicznych z dwoma cechami biometrycznymi została rozwiązana w roku 2011. Dokument ten jest jednak nadal uzupełniany i aktualizowany przez kolejne grupy robocze specjalistów z poszczególnych krajów, powoływane doraźnie w tym celu.

6.6 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 w sposób bezpieczny i wiarygodny wynik 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.

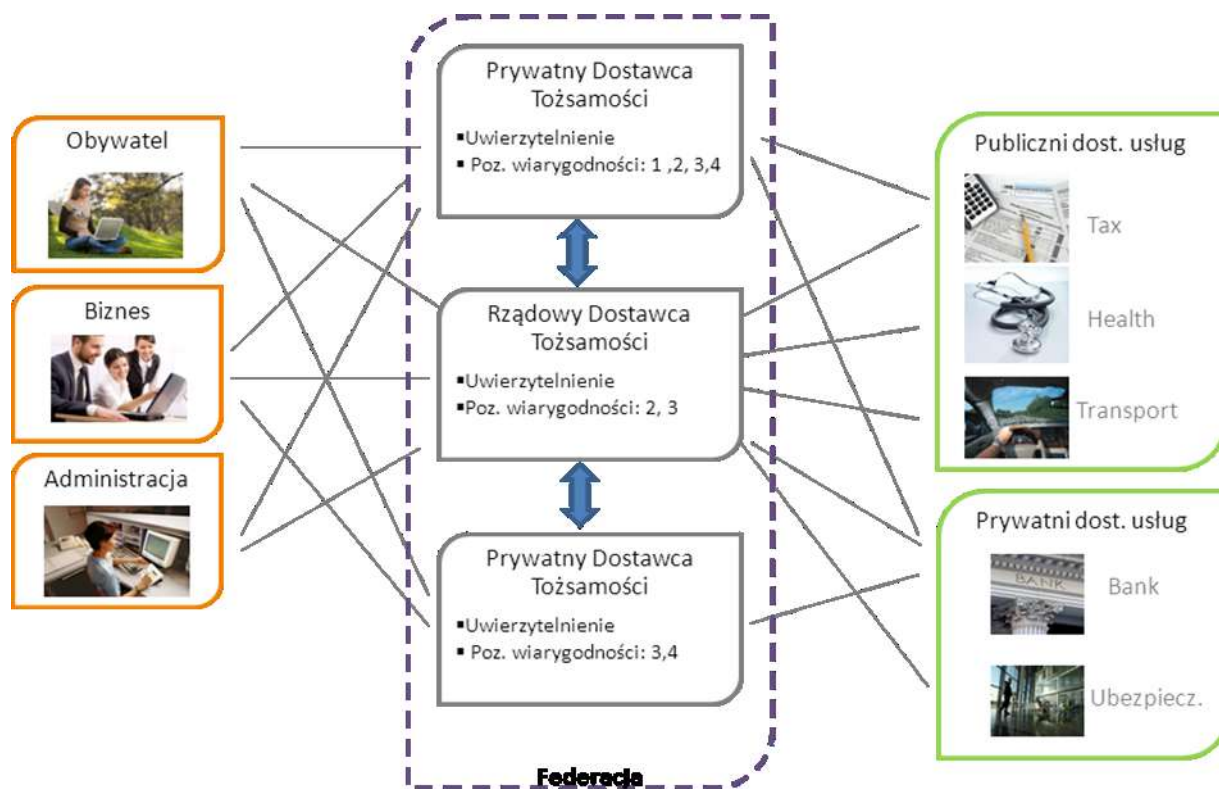


Rysunek 19. Schemat przedstawiający ideę zewnętrznego dostawcy tożsamości.

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

Identyfikacja i uwierzytelnianie w usługach elektronicznych

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 poziomowi wiarygodności uwierzytelnienia jest zgodny z wymaganiem tej drugiej usługi. Idea ta przedstawiona jest na poniższym rysunku.



Rysunek 20. 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.

7 Aspekty prawne

Każda osoba fizyczna lub prawna posiada jedną tożsamość, jeden zbiór cech, który ją jednoznacznie określa, przy czym pojedyncza cecha tożsamości nie musi być ani unikalna, ani stała w czasie. W polskim prawie, wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej określa się terminem danych osobowych⁴⁷. Dla osoby prawnej nie definiuje się danych osobowych, gdyż albo należy do możliwej do zidentyfikowania jednej lub kilku osób fizycznych, albo jest reprezentowana przez taką osobę⁴⁸.

Znaczenie danych osobowych rośnie wraz z rozwojem społeczeństwa informacyjnego zdolnego do masowego przechowywania, przesyłania oraz przetwarzania informacji stanowiącej szczególnie rodzaj dobra niematerialnego, równoważnego lub nawet cenniejszego niż dobra materialne. Towarzyszący temu rozwój zdalnych usług sprawia, że informację o tożsamości osoby coraz łatwiej można przekształcić w operacje majątkowe.

7.1 Przestępstwa przeciwko tożsamości

Z prawnego punktu widzenia nie ma rozróżnienia na to jakimi metodami zostanie wykonane przestępstwo przeciwko prawu - czy przestępstwo zostanie wykonane w świecie rzeczywistym, czy elektronicznym. W prawie wyróżnia się kilka grup przestępstw przeciwko lub z wykorzystaniem tożsamości.

W pierwszej kolejności należy wyróżnić przestępstwa związane z podszywaniem się lub fałszowaniem tożsamości. W świecie elektronicznym i dziesiątków systemów społecznościowych warto pamiętać, że karze pozbawienia wolności do lat 3 podlega, kto podszywając się pod inną osobę wykorzystuje jej wizerunek lub inne jej dane osobowe w celu wyrządzenia jej szkody majątkowej lub osobistej⁴⁹. Z kolei, kto bez uprawnienia uzyskuje informacje dla niego nieprzeznaczone, bez względu na postać tej informacji, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat 2⁵⁰.

Użyczenie tożsamości również może stać się przestępstwem, gdy zostanie ona użyta jako narzędzie przestępstwa. Użyczający odpowiada wówczas za pomocnictwo, czyli ułatwianie innej osobie popełnienia czynu zabronionego⁵¹ nawet jeżeli samemu nie ma się świadomości o współuczestniczeniu w nim. Dwa najbardziej podstawowe przypadki to firmanctwo i paserstwo.

Firmanctwo to działanie pod szyldem i firmą innej osoby. W Polsce jest to karalne, gdy naraża na uszczuplenie⁵² wpływy podatkowe. Od wysokości uszczuplenia zależy, czy jest ono traktowane jako

⁴⁷ Art. 6 ustawy o ochronie danych osobowych (Dz.U.1997.133.883)

⁴⁸ Art. 9.1.2 ustawy o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu (Dz.U.2003.153.1505)

⁴⁹ Art. 190a.2 kodeksu karnego (Dz.U.1997.88.553)

⁵⁰ Art. 267 kodeksu karnego

⁵¹ Art. 18.3 kodeksu karnego

⁵² Art. 55.1 kodeksu karnego skarbowego (Dz.U.2007.111.765)

wykroczenie skarbowe, czy przestępstwo skarbowe i tylko w tym drugim przypadku firmant, czyli użyczający swojej tożsamości, może odpowiadać za pomocnictwo. Warto przy tym pamiętać, że firmując działania innych osób nigdy nie ma się pewności, że nie uczestniczy się, albo nie będzie się uczestniczyć w naruszeniu prawa w przyszłości, co jest szczególnie niebezpieczne, zważywszy na fakt, że firmant ponosi solidarną odpowiedzialność całym swoim majątkiem za zaległości podatkowe z podatnikiem, którego działania firmuje⁵³ [1].

Paserstwo to działanie polegające na nabyciu rzeczy uzyskanej za pomocą czynu zabronionego lub udzieleniu pomocy w jej zbyciu lub jej ukryciu, bez względu na to, czy jest to działanie umyślne czy nieumyślne⁵⁴. Ofiarą paserstwa można się stać podejmując pracę jako tzw. „asystent finansowy” lub „pracownik obsługi transferów” w odpowiedzi na ogłoszenia o pracę pojawiające się cyklicznie w Internecie. W rzeczywistości, takie ogłoszenie może okazać się werbunkiem do grupy przestępczej do odpłatnego uczestniczenia w roli tzw. słupa finansowego w dystrybucji środków pochodzących z kradzieży. W takim wypadku zostaje odpłatnie użyczona tożsamość grupie przestępczej, za co użyczający będzie ponosił pełną odpowiedzialność.

Wraz z rozwojem społeczeństwa informacyjnego ilość przestępstw, wykroczeń oraz naruszeń tożsamości rośnie. Amerykańska Federalna Komisja Handlu prowadząca długofalowy program⁵⁵ poświęcony odzyskiwaniu skradzionej tożsamości opublikowała w 2003 roku raport z wynikami badań ankietowych, które mówią, że prawie 5% populacji USA, tj. 10 milionów obywateli USA, mogło się wówczas spotkać z różną formą kradzieży tożsamości [2]. Podobne badania przeprowadzone w 2012 roku podnoszą ten odsetek do ponad 80% [4]. Ta sama komisja podaje, że w 2012 roku otrzymała już ponad ćwierć miliona skarg dotyczących kradzieży tożsamości od ludzi, którzy zauważyli, że stali się jej ofiarą [3].

Jak wynika z powyższych przykładów, przestępstwo przeciwko tożsamości jest dwuetapowe. W pierwszej kolejności przestępca musi wejść w posiadanie danych osobowych, a w drugim etapie musi te dane wykorzystać do popełnienia czynu zabronionego. W uproszczeniu można powiedzieć, że ochrona prawna tożsamości również jest dwuetapowa. W pierwszej kolejności regulacjom prawnym podlega gromadzenie, przetwarzanie oraz ochrona danych osobowych. W drugim etapie wszelkie instytucje korzystające z danych osobowych do świadczenia usług, w szczególności elektronicznych usług zdalnych, zobligowane są do przestrzegania szeregu regulacji prawnych zmierzających do zagwarantowania, że usługi świadczone będą właściwej osobie.

7.2 Ochrona danych osobowych

Prawna ochrona danych osobowych spoczywa na kilku fundamentach. Po pierwsze, każdy obywatel Polski ma konstytucyjne prawo do ochrony własnych danych osobowych zagwarantowane w artykule 51 Konstytucji Rzeczypospolitej Polskiej⁵⁶. Na mocy tego artykułu nikt nie może być obowiązany do ujawniania informacji o sobie inaczej niż na podstawie ustawy, a ponadto każdy ma

⁵³ Art. 113 ordynacji podatkowej (Dz.U.1997.137.926)

⁵⁴ Art. 291, 292, 293 i 294 kodeksu karnego (Dz.U.1997.88.553) oraz art. 122 kodeksu wykroczeń (Dz.U.2010.46.275)

⁵⁵ <http://www.consumer.ftc.gov/features/feature-0014-identity-theft>

⁵⁶ Art. 51 Konstytucji Rzeczypospolitej Polskiej (Dz.U.1997.78.483)

prawo dostępu do zgromadzonych na swój temat danych urzędowych, oraz ich modyfikacji lub sprostowania.

Po drugie, ochrona danych osobowych jest wpisana w fundamenty prawne Unii Europejskiej i chociaż kolejny traktat rewizyjny⁵⁷ zmienia konstrukcję podstawowych aktów normatywnych tzw. prawa pierwotnego (umów międzynarodowych zawieranych przez Państwa członkowskie) Wspólnoty Europejskiej, to prawo każdej osoby do ochrony własnych danych osobowych nie ulega zmianie⁵⁸ i jest zapisane w prawie pierwotnym Unii Europejskiej.

Podstawowym prawem wtórnym (utworzonym już przez odpowiednie instytucje Unii Europejskiej na podstawie prawa pierwotnego), w zakresie ochrony danych osobowych jest Dyrektywa 95/46/WE Parlamentu Europejskiego i Rady z dnia 24 października 1995 roku w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych i swobodnego przepływu tych danych⁵⁹ między państwami członkowskimi.

Wreszcie zasady gromadzenia, przetwarzania oraz udostępniania danych osobowych w prawie polskim określa ustawa o ochronie danych osobowych⁶⁰, która jednocześnie ustanawia instytucję Generalnego Inspektora Ochrony Danych Osobowych⁶¹ odpowiedzialnego za kontrolę zgodności przetwarzania danych z przepisami tejże ustawy⁶².

Każdej osobie przysługuje prawo do kontroli przetwarzania własnych danych, a zwłaszcza prawo do uzyskania informacji, czy taki zbiór istnieje, kto i w jakim celu go prowadzi, a także prawo do żądania uzupełnienia, uaktualnienia, sprostowania tych danych, czasowego lub stałego wstrzymania ich przetwarzania lub ich usunięcia, jeżeli są one niekompletne, nieaktualne, nieprawdziwe lub zostały zebrane z naruszeniem prawa, lub są już zbędne do realizacji celu, dla którego zostały zebrane⁶³.

Najważniejszą zasadą dopuszczalności przetwarzania danych osobowych jest uzyskanie zgody do ich przetwarzania od osoby, której te dane dotyczą⁶⁴. Z drugiej strony, ustawy o ochronie danych osobowych nie stosuje się do podmiotów mających siedzibę poza terytorium Polski, które na terenie Polski zajmują się tylko przekazywaniem danych poza obszar kraju ani też w przypadku prasowej działalności dziennikarskiej⁶⁵ w rozumieniu prawa prasowego⁶⁶.

⁵⁷ Traktat z Lizbony z 13 grudnia 2007 roku, zmieniający Traktat o Unii Europejskiej i Traktat ustanawiający Wspólnotę Europejską, opublikowany w Dzienniku Urzędowym Unii Europejskiej Seria C Nr 306 oraz w polskim Dzienniku Ustaw (Dz.U.2009.203.1569). Wraz z wejściem w życie Traktatu z Lizbony w dniu 30 listopada 2009 roku, Wspólnota Europejska przestała istnieć, a jej spadkobiercą prawnym została Unia Europejska.

⁵⁸ Art. 16 Traktatu o Funkcjonowaniu Unii Europejskiej – poprzednio art. 286 Traktatu ustanawiającego Wspólnotę Europejską.

⁵⁹ Dziennik Urzędowy Seria L 281 z 23.11.1995 roku.

⁶⁰ Ustawa o ochronie danych osobowych (Dz.U.1997.133.883)

⁶¹ www.giodo.gov.pl

⁶² Art. 12 ustawy o ochronie danych osobowych (Dz.U.1997.133.883).

⁶³ Art. 32 tamże.

⁶⁴ Art. 23 tamże.

⁶⁵ Art. 3a tamże.

⁶⁶ Prawo prasowe (Dz.U.1984.5.24)

Regulacje w zakresie ochrony danych osobowych stale ewoluują. Do najważniejszych ostatnich zmian należy zaliczyć wejście w życie 1 stycznia 2013 roku amerykańskiej ustawy o ujawnianiu informacji finansowych o rachunkach zagranicznych obywateli amerykańskich na cele podatkowe (FATCA⁶⁷). Na jej mocy wszystkie instytucje finansowe zostały zobligowane do przekazywania danych obywateli amerykańskich, w tym imiona, nazwiska, adresy zamieszkania, numery identyfikacji podatkowej, dochody, wydatki oraz płatności, do urzędu podatkowego Stanów Zjednoczonych [5][6].

Drugą istotną zmianą jest projekt rozporządzenia Unii Europejskiej w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych i swobodnego przepływu tych danych⁶⁸, które ma szansę wejść w życie w 2014. W projekcie tym wprowadza się wrażliwe przetwarzanie w miejsce ochrony danych wrażliwych, wprowadza się obowiązkowego administratora bezpieczeństwa informacji, wprowadza się też kontrowersyjny pomysł „profilu” charakteryzujących kategorię przynależności społecznej danej osoby, który może zostać wykorzystany do automatyzowania analiz i predykcji zachowań osoby fizycznej [7].

Można założyć, że oprócz zmian już zachodzących, prawna ochrona danych osobowych w niedalekiej przyszłości będzie musiała stawić czoła nowym wyzwaniom. Po pierwsze ocenia się, że rosnące znaczenie chmur obliczeniowych wpłynie na przyspieszenie rozwiązań prawnych związanych z chmurami, poczynając od precedensowych sporów sądowych, a kończąc na inicjatywach legislacyjnych w kwestiach technologicznych i biznesowych oraz w zakresie ochrony użytkowników tych usług. Według wice przewodniczącej Komisji Europejskiej i Komisarz ds. Agendy Cyfrowej Neelie Kroes, największym ryzykiem przetwarzania w chmurze jest utrata kontroli nad przetwarzaniem danych osobowych [8]. Tymczasem GIODO przypomina, że administrator danych, który decyduje się na korzystanie z przetwarzania w chmurze, nie przestaje być odpowiedzialny za ich właściwe przetwarzanie, w tym ich zabezpieczenie, co według niego oznacza, że administrator ten powinien mieć możliwość kontrolowania firmy, która na jego rzecz przetwarza dane [9]. Ważne jest jednak to, że GIODO nie widzi przeciwwskazań prawnych do przetwarzania w chmurze zauważając jednocześnie, że większość zagadnień prawnych może zostać rozwiązana w umowach na przetwarzanie w chmurze zawartych po poprawnie toczonych negocjacjach [8]. Pogłębioną analizę aspektów prawnych związanych z przetwarzaniem w chmurze w sektorze finansowym zawiera Raport Forum Technologii Bankowych przy Związku Banków Polskich dostępny bezpłatnie z serwera ZBP [10].

Kolejnym wyzwaniem jest ochrona danych biometrycznych rozumianych zarówno jako surowe próbki pomiarowe, jak i przetworzone wzorce biometryczne. Z jednej strony wysoki stopień zabezpieczeń stosowanych w biometrii sprawia, że określenie tożsamości osoby na podstawie skradzionych danych biometrycznych wymaga nadmiernych kosztów, czasu i działań, a więc zgodnie z ustawą o ochronie danych osobowych same dane biometryczne nie muszą być uważane za dane osobowe⁶⁹. Z drugiej strony ilość dostępnych technologii, zróżnicowanie właściwości poszczególnych technik i technologii biometrycznych oraz zastosowanych metod zabezpieczeń danych nie pozwala na takie uproszczenie i w odpowiedzi na pytanie „czy dane biometryczne są danymi osobowymi” konieczne jest indywidualne zbadanie skutku możliwości identyfikacji tożsamości na podstawie konkretnych danych. Pogłębioną analizę prawną tego zagadnienia zawiera raport Forum Technologii Bankowych przy Związku Banków Polskich [11].

⁶⁷ Foreign Account Tax Compliance Act

⁶⁸ COM(2012) 11 z 25 stycznia 2012 roku.

⁶⁹ Art. 6.3 ustawy o ochronie danych osobowych (Dz.U.1997.133.883)

7.3 Identyfikacja i uwierzytelnianie

Drugim etapem ochrony tożsamości po ochronie danych osobowych jest zagwarantowanie, że zdalne usługi elektroniczne świadczone będą właściwej osobie. Kluczowe z punktu widzenia bezpieczeństwa jest w tym przypadku prawidłowe przeprowadzenie procesu identyfikacji, uwierzytelniania oraz autoryzacji, wykonane każdorazowo przed udostępnieniem zasobów systemów informatycznych użytkownikowi.

Identyfikacja jest pierwszą fazą procesu identyfikacji i uwierzytelniania, i sprowadza się do deklarowania tożsamości. Służy do tego identyfikator, który jest ustaloną formą prezentacji unikalnej w danej populacji wartości cechy, lub grupy wartości cech tożsamości. Jedna tożsamość może posiadać wiele identyfikatorów, tak jak do wielu różnych grup społecznych może należeć. Siła identyfikatora jest tym większa im większą część populacji obejmuje i w Polsce najsilniejszym obecnie identyfikatorem jest dowód osobisty, którego posiadanie - w przeciwieństwie do karty bankowej, prawa jazdy, czy paszportu - jest obowiązkowe⁷⁰. Drugą fazą procesu identyfikacji i uwierzytelniania jest uwierzytelnianie, czyli potwierdzanie autentyczności zadeklarowanego wcześniej identyfikatora (ang. *proof-of-possession*), a następnie tożsamości. Bezpieczna gospodarka elektroniczna wymaga, by uwierzytelnianie pozwalało na jednoznaczne rozstrzygnięcie autentyczności deklarowanej tożsamości. Tylko pozytywny wynik uwierzytelniania pozwala na wykonanie trzeciej fazy procesu identyfikacji i uwierzytelniania, czyli autoryzacji, która polega na określeniu, czy uwierzytelniona tożsamość jest uprawniona do korzystania z żądanego zasobu i w jakim zakresie. W kularach konferencji poświęconych bezpieczeństwu informatycznemu usłyszeć też można o czwartej fazie procesu identyfikacji i uwierzytelniania, jaką jest według niektórych reakcja na zauważone uchybienia natury zewnętrznej, jak i wewnętrznej. Innymi słowy odpowiedź na pytanie, jak zareagować na próby wprowadzenia systemu w błąd, albo na stwierdzone posługiwanie się fałszywą tożsamością lub wreszcie na stwierdzone wewnętrznie słabości systemowe procesu identyfikacji i uwierzytelniania. Zakłada się, że procedury reakcji powinny być zapisane w polityce bezpieczeństwa instytucji udostępniającej swoje zasoby, czyli odpowiedzialnej za prawidłowość przeprowadzenia procesu identyfikacji i uwierzytelniania.

Warto zauważyć, że proces identyfikacji i uwierzytelniania dotyczy wszystkich operacji gospodarczych, administracyjnych oraz prawnych, w których nadanie uprawnienia do korzystania z danego zasobu lub wykonanie czynności proceduralnych wymaga jednoznacznego i niepodważalnego ustalenia tożsamości stron. Nie ma w gospodarce narodowej drugiego tak powszechnie występującego procesu. Pomimo tego, w polskim zbiorze aktów prawnych nie ma przepisów, które jednoznacznie i w sposób spójny definiowałyby sam proces, prawa i obowiązki stron w trakcie tego procesu, ani tym bardziej żadnych wytycznych dotyczących polityki bezpieczeństwa, czy jakichkolwiek procedur reakcji na naruszenie bezpieczeństwa.

Zamiast tego jest zauważalna tendencja do narzędziowego definiowania procesu w zależności od kontekstu, przy czym prawodawca myli pojęcia zapisując na przykład, że przez uwierzytelnianie rozumiana jest identyfikacja użytkownika⁷¹. Wydaje się, że nawet poprawne zdefiniowanie

⁷⁰ Art. 34 ustawy o ewidencji ludności i dowodach osobistych (Dz.U.2006.139.993)

⁷¹ Art. 2.8 rozporządzenia Ministra Sprawiedliwości w sprawie trybu zakładania konta oraz sposobu posługiwania się podpisem elektronicznym w elektronicznym postępowaniu upominawczym (Dz.U.2009.226.1830)

uwierzytelniania jako weryfikacji deklarowanej tożsamości użytkownika⁷² jest mniej znacząca niż sam fakt wielokrotnego definiowania tego procesu.

W gospodarce elektronicznej procesy identyfikacji i uwierzytelnienia są procesami krytycznymi z punktu widzenia zarządzania ryzykiem operacyjnym rozumianym jako „ryzyko straty wynikającej z niedostosowania lub zawodności wewnętrznych procesów, ludzi i systemów technicznych lub ze zdarzeń zewnętrznych”. W zakres ryzyka operacyjnego wchodzi ryzyko prawne, natomiast wyłącza się z niego ryzyko reputacji i ryzyko strategiczne” [12].

Ryzyko prawne związane jest tu bezpośrednio z możliwością zanegowania, czy też kwestionowania wykonania danej operacji, a w szczególności zanegowania ważności transakcji finansowych. Jest to punkt, w którym materializują się wszelkie ryzyka związane z tożsamością i z tego powodu jest to moment szczególnie chroniony w prawie bankowym. Bank dokonujący wypłat z rachunku bankowego jest obowiązany sprawdzić autentyczność i prawidłowość formalną dokumentu stanowiącego podstawę do wypłaty oraz tożsamość osoby dającej zlecenie⁷³. Innymi słowy ryzyko prawne związane jest z uwierzytelnianiem aż trzech elementów: dokumentu będącego podstawą transakcji, tożsamości osoby składającej zlecenie oraz samego identyfikatora.

7.3.1 Uwierzytelnianie dokumentu

Z tych trzech elementów, prawnie uregulowane najlepiej jest uwierzytelnianie dokumentu osadzone na trzech podstawach prawnych. Po pierwsze zdefiniowany jest zarówno dokument⁷⁴, jak i dokument elektroniczny⁷⁵, jako stanowiący odrębną całość znaczeniową zbiór danych uporządkowanych w określonej strukturze wewnętrznej i zapisany na informatycznym nośniku danych. Po drugie jest zdefiniowana wola osoby dokonującej czynności prawnej⁷⁶, następnie składanie oświadczenia woli w formie pisemnej⁷⁷ i wreszcie zrównanie oświadczenia woli, które złożone jest w postaci elektronicznej i opatrzone bezpiecznym podpisem elektronicznym weryfikowanym przy pomocy ważnego kwalifikowanego certyfikatu z oświadczeniem woli złożonym w formie pisemnej⁷⁸. Jakkolwiek zrównanie skutku prawnego nie jest tożsame z całkowitym zastąpieniem podpisu własnoręcznego podpisem elektronicznym. Nadal w prawie pozostają czynności wymagające podpisu własnoręcznego jak chociażby notarialne poświadczenie podpisu, czy też własnoręczny testament⁷⁹. Wreszcie, trzecią podstawą prawną uwierzytelniania dokumentu jest akt prawny poświęcony tylko podpisowi elektronicznemu⁸⁰, który

⁷² Art. 2.1. rozporządzenia Ministra Spraw Wewnętrznych i Administracji w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych. (Dz.U.2004.100.1024)

⁷³ Art. 65 prawa bankowego (Dz.U.2002.72.665)

⁷⁴ Art. 115.14 kodeksu karnego (Dz.U.1997.88.553)

⁷⁵ Art. 3.2. ustawy o informatyzacji działalności podmiotów realizujących zadania publiczne (Dz.U.2005.64.656)

⁷⁶ Art. 60 kodeksu cywilnego (Dz.U.1964.16.93)

⁷⁷ Art. 78.1 tamże

⁷⁸ Art. 78.2 tamże

⁷⁹ Art. 949.1 tamże

⁸⁰ Ustawa o podpisie elektronicznym (Dz.U.2001.130.1450)

dokładnie definiuje warunki, w jakich podpis elektroniczny uważa się za bezpieczny, ponadto określa obowiązki stron oraz reguluje skutki prawne zastosowania bezpiecznego podpisu elektronicznego.

Zgodnie z ustawą bezpieczny podpis elektroniczny to podpis elektroniczny, który spełnia 3 warunki. Po pierwsze jest przyporządkowany wyłącznie do osoby składającej ten podpis. Po drugie jest sporządzany za pomocą podlegających wyłącznej kontroli osoby składającej podpis elektroniczny bezpiecznych urządzeń służących do składania podpisu elektronicznego i danych służących do składania podpisu elektronicznego. Po trzecie, jest powiązany z danymi, do których został dołączony, w taki sposób, że jakakolwiek późniejsza zmiana tych danych jest rozpoznawalna⁸¹.

Tak jak w Polsce funkcje identyfikacyjną, dowodową oraz kontraktową w obrocie prawnym i gospodarczym pełni bezpieczny podpis elektroniczny weryfikowany za pomocą kwalifikowanego certyfikatu, tak prawo wspólnotowe⁸² rozróżnia podpis elektroniczny, podpis zaawansowany, oraz podpis kwalifikowany. Podpis elektroniczny to dane w postaci elektronicznej, które służą tylko do identyfikacji osoby składającej podpis. Zaawansowany podpis elektroniczny jest podpisem elektronicznym, który kryptograficznie, jednoznacznie oraz w sposób trudny do sfalszowania jest związany z dokumentem oraz autorem podpisu. Wreszcie kwalifikowany podpis elektroniczny jest podpisem zaawansowanym złożonym przy pomocy certyfikatu kwalifikowanego oraz bezpiecznego urządzenia do składania podpisów elektronicznych.

W pewnym uproszczeniu można założyć, że odpowiednikiem wspólnotowego podpisu zaawansowanego w polskim prawie może być podpis osobisty, który ma znaleźć się w warstwie elektronicznej nowego dowodu osobistego⁸³. Z jednej strony wykorzystuje on mechanizmy kryptograficzne, ale z drugiej, skutek prawny złożenia tego podpisu jest ograniczony lub umowny. Ścisłej rzecz biorąc, dla podmiotu publicznego skutek prawny równoznaczny jest ze złożeniem własnoręcznego podpisu pod dokumentem w postaci papierowej⁸⁴. Natomiast dla podmiotów innych niż publiczne może mieć taki sam skutek, tylko jeżeli obie strony wyrażą na to zgodę⁸⁵, co z systemowego punktu widzenia wprowadza zagrożenie niepotrzebnego zamieszania i w efekcie jest mocno kontrowersyjne.

Jakkolwiek można odnieść wrażenie, że ustawa o podpisie elektronicznym jest utołma i skupia się tylko na bezpiecznym podpisie elektronicznym pomijając zwykły podpis elektroniczny, podpis zaawansowany czy osobisty, szczególnie w sferze regulacji wywoływanych skutków prawnych, to i tak regulacje prawne wyprzedzają rzeczywistość biznesową. Są centra wydające certyfikaty kwalifikowane, jest infrastruktura systemowa, brakuje powszechności.

7.3.2 Uwierzytelnianie osoby

Całkowicie odmienna sytuacja panuje w obszarze uwierzytelniania osoby, szczególnie w świecie usług zdalnych. Jest powszechna praktyka. Są dziesiątki narzędzi: od różnych modeli loginu i hasła, przez zdrapki, piny, puki, tokeny, karty, smsy, aż po wielorakie narzędzia biometryczne. Brakuje regulacji

⁸¹ Art. 3.2 ustawy o podpisie elektronicznym (Dz.U.2001.130.1450).

⁸² Dyrektywa o Wspólnotowej Infrastrukturze Podpisów Elektronicznych (1999/93/EC).

⁸³ Art. 13.1 ustawy o dowodach osobistych (Dz.U.2010.167.1131).

⁸⁴ Art. 16.1 tamże.

⁸⁵ Art. 16.2 tamże.

i standaryzacji, wymienności i federacyjności. Jest chaos lokalnych rozwiązań, dziesiątki rejestrów danych, w których gubią się klienci i które osłabiają się wzajemnie. Ogólne zalecenia dotyczące uwierzytelniania można znaleźć w raportach dotyczących zarządzania ryzykiem operacyjnym pochodzących zarówno od Komitetu Bazylejskiego, jak i Komisji Nadzoru Finansowego oraz w Rekomendacji M powstałej jeszcze za czasów działalności Komisji Nadzoru Bankowego. Raport Komitetu Bazylejskiego zaleca, by w ramach zasad zarządzania ryzykiem w bankowości elektronicznej, banki między innymi posiadały politykę i procedury określające metodologię zapewniającą właściwe uwierzytelnianie osoby, stosowały metody potwierdzania transakcji uniemożliwiające ich negowanie, wprowadzały odpowiedzialność za transakcje elektroniczne oraz posiadały właściwe mechanizmy kontroli autoryzacji i dostępu do systemów [13]. W Rekomendacji M uwierzytelnianie, rozumiane jako odpowiednia weryfikacja identyfikacji osoby, znajduje się w części opisowej ryzyka operacyjnego poświęconej bezpieczeństwu informacyjnemu banku. Pomimo faktu, że sama Rekomendacja M oparta jest na prawie bankowym⁸⁶ trudno postrzegać jej zapisy dotyczące uwierzytelniania jako twarde regulacje, tym bardziej, że w części rekomendującej działania dla rady nadzorczej banku, zarządu czy komórek kontroli wewnętrznej o uwierzytelnianiu w sensie ścisłym już się nie wspomina.

7.3.3 Identyfikacja

Wreszcie w sferze procesu identyfikacji określone są wymagania prawne, a brakuje narzędzia, które umożliwiłoby efektywne im sprostanie w warunkach gospodarki elektronicznej. Problem widoczny jest szczególnie w sytuacji zdalnego zawiązywania umowy na usługi z nowym klientem, który jeszcze nie posiada identyfikatora zgodnego z przyszłą umową. Zgodnie z ustawą o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu, zwanej potocznie AML (od j. ang. *Anti Money Loundering*)⁸⁷, przy zawieraniu umowy z klientem należy zastosować środki bezpieczeństwa finansowego⁸⁸, które polegają na identyfikacji klienta i weryfikacji jego tożsamości na podstawie dokumentów lub informacji publicznie dostępnych⁸⁹. Zgodnie z ustawą identyfikacja osób fizycznych polega między innymi na ustaleniu i zapisaniu cech dokumentu tożsamości osoby⁹⁰, a weryfikacja na sprawdzeniu i potwierdzeniu tych danych przed zawarciem umowy⁹¹. Dodatkowo, w przypadku zdalnego zawierania umowy, gdy klient nie jest obecny, dla celów identyfikacji należy zastosować co najmniej jeden z trzech środków dodatkowych⁹². Pierwszym jest ustalenie tożsamości klienta na podstawie dodatkowych dokumentów lub informacji. Drugim jest dodatkowa weryfikacja autentyczności przedstawionych dokumentów lub poświadczenie ich zgodności z oryginałem przez notariusza, organ administracji rządowej lub samorządowej lub podmiot usług finansowych. Trzecią możliwością jest ustalenie, że pierwsza transakcja została przeprowadzona za pośrednictwem istniejącego już rachunku klienta. Praktyka biznesowa korzysta najczęściej z opcji pierwszej lub trzeciej, przy czym w pierwszej opcji informacji dodatkowych udziela kurier dowożący umowę do klienta, którego obarcza się dodatkowo zadaniem potwierdzenia zgodności wizerunku klienta ze zdjęciem w jego dokumencie tożsamości. Tak czy inaczej wszystkie stosowane rozwiązania w praktyce posiadają swoje ułomności, a prawdziwym rozwiązaniem problemu

⁸⁶ Art. 137.5 prawa bankowego (Dz.U.2002.72.665).

⁸⁷ Ustawa o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu (Dz.U.2000.116.1216).

⁸⁸ Art. 8b.4 tamże.

⁸⁹ Art. 8b.3.1 tamże.

⁹⁰ Art. 9.1.1 tamże.

⁹¹ Art. 9a.1 tamże.

⁹² Art. 9e.2 tamże.

Identyfikacja i uwierzytelnianie w usługach elektronicznych

byłoby dostarczenie klientom nowego elektronicznego dowodu osobistego w roli narodowego identyfikatora, który posiadałby w warstwie elektronicznej mechanizm potwierdzający, iż dokument został wydany przez uprawniony podmiot i nie jest sklonowany. Mogłoby to zostać zrealizowane w oparciu o standardy ICAO dotyczące dokumentów podróży (Active i Passive authentication – patrz pkt. 6.5.2) lub poprzez certyfikat dowodu osobistego, czyli elektroniczne zaświadczenie przyporządkowujące dane do weryfikacji informacji uwierzytelniającej do dowodu osobistego⁹³. Rozwiązanie z „certyfikatem dowodu osobistego” zapewnia tylko „nieklonowalność”, natomiast zgodne ze standardami ICAO pozwala na realizację innych funkcji, np. selektywnego udostępniania podpisanych danych.

⁹³ Art. 2.1.1. ustawy o dowodach osobistych (Dz.U.2010.167.1131 z późniejszymi zmianami)

8 Identyfikacja i uwierzytelnienie – stan obecny w Polsce

8.1 Praktyka sektora finansowego

Banki od ponad dziesięciu lat aktywnie promują bankowość elektroniczną. Z jednej strony jest to zgodne z potrzebami klientów, którzy oczekują możliwości zdalnej i wygodnej obsługi bankowej, niezależnej od trybu pracy i godzin otwarcia oddziałów bankowych, a jednocześnie stanowi to wsparcie dla realizacji celów biznesowych banków, związanych zarówno z redukcją kosztów operacyjnych, jak i generowaniem nowych przychodów dzięki tzw. „cross-sell’owi” usług i produktów przez kanały zdalne. Przez to dziesięciolecie wyklarował się obraz bankowości elektronicznej, który można opisać z dwóch punktów widzenia: kanałów dostępu oraz segmentacji klientów, a co za tym idzie dostępnych platform/produktów bankowości elektronicznej. Co do kanałów dostępu to za dominujący można uznać kanał internetowy oparty na dostępie przez przeglądarkę z aktywnym dostępem do produktów bankowych, tj. umożliwiającym aktywne wykonywanie transakcji. Równolegle do kanału internetowego funkcjonuje kanał telefoniczny, bazujący na systemach automatycznych lub obsłudze przez konsultanta – ten kanał wydaje się aktualnie nie zyskiwać na popularności. Z kolei coraz większą wagę zyskuje kanał bankowości mobilnej dostępnej przez telefony komórkowe, w tym tzw. smartfony, funkcjonujący w obrębie wariantów dostępnych przez wersję przeglądarkową oraz aplikacyjną. Co do segmentów i platform, to najczęściej dla klientów detalicznych oraz małych i średnich przedsiębiorstw, proponowany jest jeden typ platformy / produktu bankowości elektronicznej, natomiast dla dużych przedsiębiorstw i korporacji inny. W tym drugim przypadku, w części banków funkcjonują jeszcze rozwiązania off-linowe, instalowane na komputerach użytkowników, które są stopniowo wypierane przez rozwiązania w pełni internetowe z dostępem przez przeglądarkę.

Najbardziej powszechną metodą identyfikacji i uwierzytelnienia użytkowników bankowości elektronicznej jest weryfikacja wydanego klientowi identyfikatora oraz statycznego hasła o określonej złożoności, które dodatkowo może być potwierdzane stosowanym w danym banku narzędziem autoryzacji (np. hasła jednorazowe). Identyfikatorem najczęściej jest unikalny (na poziomie danej instytucji) dla klienta ciąg znaków, najczęściej liczb i najczęściej 8-mio znakowy. Za standard można uznać „one-login view” czyli możliwość podglądu oraz zarządzania przez klienta danej instytucji wszystkimi posiadanymi produktami posługując się jednym identyfikatorem i hasłem. Wyjątek stanowią serwisy bankowości elektronicznej banku i innych podmiotów funkcjonujących w ramach jednej grupy kapitałowej np. domu maklerskiego – w tym przypadku część banków posiada rozwiązania zintegrowane („single sign on”), oparte na jednym identyfikatorze wydanym dla jednego użytkownika, a część podmiotów takiej integracji nie posiada. W przypadku rozwiązań dla firm identyfikator jest przypisany do danego użytkownika, a zakres dostępnych czynności oraz np. limity transakcji powiązane są z analogicznymi uprawnieniami, które są przypisane do danej osoby w KRS danego podmiotu.

Polityka autoryzacyjna banków generalnie polega na przypisaniu określonego zakresu czynności użytkownika do jedno- lub dwu-czynnikowego uwierzytelnienia, gdzie do jednoczynnikowego zalicza się najczęściej udane logowanie poprzez podanie poprawnej pary identyfikatora i hasła, a dwuczynnikowe jest wzbogacone o jednorazowe użycie stosowanej przez bank tzw. dodatkowej metody uwierzytelnienia. Do pierwszej puli czynności najczęściej zalicza się czynności, które nie skutkują zawarciem umowy z bankiem lub realizacją transakcji polegającej na przesłaniu środków pieniężnych poza rachunki klienta (np. spłata karty kredytowej, przelewy na rachunki własne). Wyjątkiem jest często realizacja przelewu na rachunek oznaczony jako zaufany przez samego użytkownika. Pozostałe czynności, w tym przede

wszystkim przelewami na rachunki obce, umowy produktowe czy czynności związane z zarządzaniem rachunkiem, jak np. zmiany limitów, najczęściej objęte są dodatkowo koniecznością użycia drugiej metody uwierzytelnienia, gwarantującej zdecydowanie ograniczenie ryzyka operacyjnego, wynikające z możliwością przejęcia przez niepowołany podmiot identyfikatora i hasła uprawnionego użytkownika. W przeważającej części są to narzędzia informatyczne znajdujące się w posiadaniu klienta, a wcześniej wydane mu przez dany bank, generujące unikalne kody, które - po wprowadzeniu przez użytkownika - umożliwiają uwierzytelnienie transakcji jak tokeny sprzętowe. Najczęściej stosowanymi narzędziami są tokeny sprzętowe, tokeny mobilne oraz tzw. kody SMS. W platformach bankowości korporacyjnej stosuje się również karty procesorowe oraz podpis elektroniczny. W niektórych bankach stosuje się karty kodów jednorazowych, ale stopniową są one wypierane przez rozwiązania wspomniane wyżej

Z powyższej analizy wynika, że banki stosują dość spójne metody autoryzacji i uwierzytelnienia, korzystają z podobnych rozwiązań biznesowych i technicznych, natomiast są to podejścia silosowe, wzajemnie niezintegrowane. Oznacza to, że użytkownik stając się klientem danego banku każdorazowo musi na nowo rejestrować się i otrzymuje unikalne dla danego banku (choć często funkcjonalnie podobne do rynkowego standardu) dane uwierzytelniające, narzędzia dostępu do bankowości elektronicznej i uwierzytelnienia zleczanych transakcji. Klient nie ma więc, co do zasady, możliwości identyfikacji tym samym, uniwersalnym narzędziem w kilku instytucjach, w zakresie aktywnego korzystania z kanałów bankowości elektronicznej. Ten silosowy model wynika zarówno z braku takiego jednego spójnego i interoperacyjnego identyfikatora wydawanego np. przez instytucję centralną (organ administracji rządowej), jak i wysoki poziom konkurencyjności między poszczególnymi bankami, które nie widzą celu biznesowego w ułatwieniu dostępu do korzystania z produktów kilku banków.

8.2 Dostępne powszechne narzędzia identyfikacji i uwierzytelnienia

8.2.1 Certyfikaty elektroniczne

Podstawową powszechną metodą identyfikacji i uwierzytelnienia jest wykorzystanie certyfikatów elektronicznych wydawanych przez kwalifikowane podmioty świadczące usługi certyfikacyjne. Temat ten jest obszernie przedstawiony w rozdziałach wcześniejszych (zob. m.in. 4.1). Natomiast certyfikaty kwalifikowane, dostępne na gruncie prawa polskiego, nie nadają się do wykorzystania do uwierzytelnienia on-line (podpis cyfrowy), gdyż posiadają atrybut niezaprzeczalności („non-repudiation” lub „content commitment”), który wyklucza inne zastosowania niż składanie oświadczeń woli⁹⁴ (zob. 5.1.3.1). Pozostaje wykorzystanie certyfikatów niekwalifikowanych. Niemniej liczba użytkowników certyfikatów jest stosunkowo niewielka.

8.2.2 ePUAP

System ePUAP (Elektroniczna Platforma Usług Administracji Publicznej) jest systemem zbudowanym przez MSWiA (aktualnie podlegającym pod MAiC) jako wspólna platforma umożliwiająca podmiotom publicznym udostępnianie swoich usług. Platforma ta posiada podsystem uwierzytelniania użytkowników i autoryzacji do usług administracji publicznej. Ze względu na to, że użytkownikami

⁹⁴ chociaż znane są przypadki wykorzystywania certyfikatów kwalifikowanych do uwierzytelniania

platformy są obywatele, którzy sprawy w administracji publicznej załatwiają w imieniu własnym, ale także w imieniu podmiotów, w których są zatrudnieni lub z którymi są powiązani, przyjęto następujący model utrzymywania tożsamości w ePUAP.

Każdy użytkownik – osoba fizyczna może mieć tylko jedno konto w ePUAP (warunek z regulaminu), do którego przypisany jest mechanizm uwierzytelnienia – login/hasło lub podpis/certyfikat. Do każdej tożsamości może być przypisanych wiele organizacji (podmiotów), w ramach których użytkownik może występować, uzyskiwać uprawnienia i się identyfikować jako osoba uprawniona w ramach danej organizacji. W procesie uwierzytelniania użytkownik wybiera na czas sesji korzystania z ePUAP w jakim kontekście będzie występował – tj. czy będzie działał jako osoba fizyczna, czy uczestnik pewnej organizacji, do której jest przypisany. Podczas sesji nie można płynnie zmieniać kontekstów – aby uniemożliwić mieszanie spraw prywatnych i służbowych. Szczególnym kontekstem użytkownika jest działanie w ramach przypisanego podmiotu publicznego. Użytkownik działając w takim kontekście może uzyskać uprawnienia do zarezerwowanych funkcji systemu ePUAP. Platforma działa jako zewnętrzny dostawca tożsamości i wykorzystuje protokół SAML2.0. Jednak obecny stan prawny wyklucza korzystanie z ePUAP przez podmioty prywatne. Także jego implementacja nie uwzględnia potrzeb sektora prywatnego, w szczególności nie zadbano o realizację i organizację działania systemu, która wzbudzałaby zaufanie tego sektora⁹⁵. Nie jest także określony poziom wiarygodności uwierzytelnienia.

8.2.3 Profil Zaufany⁹⁶

Profil zaufany jest to mechanizm oparty o platformę ePUAP, gdzie użytkownik posiadający konto na ePUAP może w wyniku czynności administracyjnej uzyskać potwierdzenie, że dane osobowe zapisane na koncie są zgodne z rzeczywistością, a osoba tam ujawniona jest tą, która posiada kontrolę nad kontem. Podstawowym mechanizmem profilu zaufanego jest podpis potwierdzony profilem zaufanym. Działanie podpisu potwierdzonego profilem zaufanym polega na tym, że do podpisywanego dokumentu dołączane są dane zawarte w profilu zaufanym, a całość jest podpisywana podpisem systemu ePUAP (pieczęcią elektroniczną). Celem wprowadzenia podpisu potwierdzonego profilem zaufanym w formie podpisu (pieczęci), zamiast federacji mechanizmów uwierzytelniania, było zapewnienie interoperacyjności w dokumentowych procesach administracji publicznej, gdzie uczestnictwo obywatela w procesach administracyjnych wymaga zobowiązań wyrażonych podpisem. Struktura podpisu potwierdzonego profilem zaufanym umożliwia jego weryfikację standardowymi narzędziami służącymi do weryfikacji podpisu zaawansowanego; jest realizowana w formacie XAdES, a dane profilu zaufanego stanowią atrybut podpisu – istnieją wątpliwości, czy zgodny ze standardem – patrz pkt 5.1.3.2. W obecnej koncepcji i na obecnym etapie funkcjonowania Profil Zaufany nie jest narzędziem dedykowanym do uwierzytelnienia do e-usług (a raczej do podpisu), nie przewidziano także jego zastosowania w usługach komercyjnych (brak podstawy prawnej oraz implementacja nieuwzględniająca potrzeb rynku komercyjnego). Ponadto jego poziom wiarygodności nie jest znany, więc trudno sektorowi prywatnemu określić do jakich e-usług można by go wykorzystać. Natomiast stosując kryteria STORK czy ISO29115 nigdy nie osiągnie najwyższego poziomu LoA, a więc do

⁹⁵ zob. m.in. www.computerworld.pl/artykuly/382785/Nie.uzywam.profilu.zaufanego.na.ePUAP.html

⁹⁶ bardziej szczegółowy opis techniczny profilu zaufanego znajduje się w rozdz. 5.1.3.2

niektórych zastosowań (e-usług) i tak będzie wymagane inne narzędzie (oparte o PKI i certyfikowany token sprzętowy).

8.3 Kwestia narodowego identyfikatora

Rozwiązaniem problemu modelu silosowego (przedstawionym m.in. w rozdziale 8.1), może być wprowadzenie powszechnego, „narodowego” identyfikatora elektronicznego (tożsamości elektronicznej) wraz z dostępnym dla strony komercyjnej systemem uwierzytelnienia. Poprzez powszechny, „narodowy” identyfikator rozumie się tutaj identyfikator, który jest:

- dostępny dla szerokich mas obywateli, potencjalnie dla wszystkich dorosłych,
- posiadany masowo,
- wydawany przez państwo lub uznawany przez państwo (w przypadku wydawców komercyjnych),
- dostępny dla e-usług zarówno publicznych, jak i komercyjnych,
- wiarygodny (“bezpieczny”),
- interoperacyjny.

Istnienie takiego powszechnego identyfikatora, otworzyłoby szansę bankom (i innym firmom komercyjnym) na oszczędności wynikające z bezpłatnego outsourcingu usług związanych z identyfikacją i uwierzytelnieniem. Dziś każdy bank tworzy i utrzymuje własne systemy, co generuje określone koszty. W efekcie wiele instytucji mogłoby korzystać z tego samego identyfikatora, także z korzyścią dla klientów, którzy wolą mniej elektronicznych tożsamości (które trzeba chronić), czy mniej haseł do zapamiętania (zob. także 3.8 i 6.6).

Obecnie w Polsce mamy dwóch „kandydatów” pretendujących w zamyśle twórców do miana powszechnych identyfikatorów – są to: kwalifikowany podpis elektroniczny i Profil Zaufany. Jednak żaden z nich nie spełnia wszystkich w/w kryteriów: podpis kwalifikowany pozostaje narzędziem marginalnym po 10 latach od wprowadzenia, a Profil Zaufany nie jest dostępny dla sektora komercyjnego, oferuje niski poziom wiarygodności i jest to rozwiązanie specyficznie, potencjalnie nieinteroperacyjne. Co prawda poziom wiarygodności nie został określony przez dostawcę (MSW), ale stosując kryteria wg projektu normy ISO 29115 (zob.4.6) lub STORK (zob. 4.4) można domniemywać, że jest to poziom 2 lub co najwyżej 3 (o ile wszystkie szczegółowe kryteria są spełnione, co nie jest pewne).

Z kwalifikowanym podpisem elektronicznym jest jeszcze jeden problem: nie powinien być stosowany do uwierzytelnienia on-line do usług elektronicznych w ogóle, gdyż jest to narzędzie do składania wyłącznie oświadczeń woli (pole „key usage” określone jako „non repudiation”/”content commitment” – niezaprzeczalność). Ze względu na swoją moc prawną (równoważną podpisowi odręcznemu) oraz wymagania z aktów prawnych (obowiązek prezentacji podpisanych danych podpisującemu), nie powinno się go stosować do uwierzytelnienia, gdzie następuje podpisanie nieznanego dla podpisującego ciągu danych. Kwestię tą zmieni dopiero nowelizacja rozporządzenia 1094 w sprawie warunków technicznych i organizacyjnych dla podmiotów kwalifikowanych, którą ma zamiar wprowadzić Ministerstwo Gospodarki jeszcze przed wejściem w życie rozporządzenia eIDAS.

Zapewne powszechnym identyfikatorem miał szansę zostać tzw. podpis osobisty przewidziany do umieszczania w elektronicznych dowodach tożsamości (projekt pl.ID). Certyfikaty podpisu osobistego

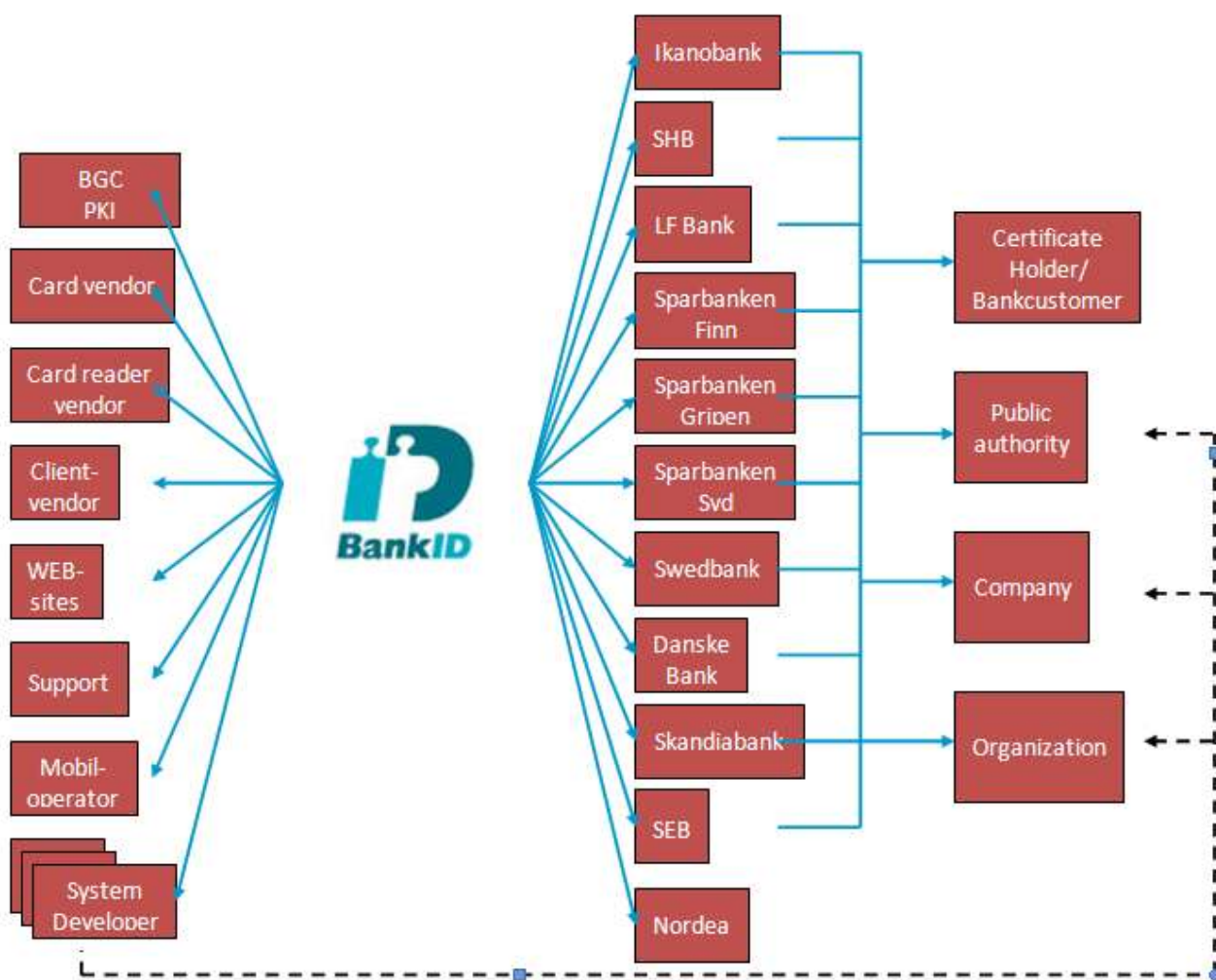
Identyfikacja i uwierzytelnianie w usługach elektronicznych

miały być wydawane nieodpłatnie, wszystkim obywatelom (którym to prawo przysługiwało), miał funkcjonować w analogiczny sposób jak podpis kwalifikowany, spełniać te same wymagania (np. nośnik sprzętowy z certyfikacją „SSCD”), a więc reprezentowałby ten sam lub zbliżony poziom wiarygodności (czyli szansa na najwyższy, 4 poziom) oraz miał szanse być interoperacyjny. Mankamentem natomiast było określenie jego zastosowania analogicznego do podpisu kwalifikowanego (tylko do oświadczeń woli), natomiast wydaje się, że to niedopatrzenie dałoby się naprawić na poziomie implementacji np. poprzez wprowadzenie drugiego certyfikatu, z innym zastosowaniem określonym w rozszerzeniu „key usage” certyfikatu. Jednak po rezygnacji z tego rozwiązania, na lata pogrzebana została szansa wprowadzenia powszechnego identyfikatora i trudno zatem spodziewać się przełomu w rozwoju powszechnych usług elektronicznych, a jedyną nadzieją pozostaje obecnie Elektroniczna Karta Ubezpieczenia Zdrowotnego – eKUZ (planowane rozpoczęcie wydawania w 2015 roku).

9 Studium przypadków

9.1 Bank ID (Szwecja)

BankID to wiodąca identyfikacja elektroniczna w Szwecji, w oparciu o standard techniczny PKI (Public Key Infrastructure). BankID został opracowany przez kilka dużych banków, do stosowania przez społeczeństwo, sferę publiczną i przedsiębiorstwa. Pierwsza implementacja BankID została wdrożona w 2003 roku. BankID to sieć, obejmująca Danske Bank, Ikanobank, Länsförsäkringar Bank, SEB, Skandiabanken, Sparbanken Øresund, Sparbanken Syd, Svenska Handelsbanken, Swedbank i Nordea. 3 miliony osób wykorzystują BankID mając do dyspozycji ponad 1000 usług prywatnych i publicznych.



Rysunek 21. Struktura projektu BankID.

Firma Finansiell ID-Teknik świadczy usługi w zakresie tożsamości elektronicznej dla banków w Szwecji. W chwili obecnej dziewięć banków działa jak emitenci BankID (Certification Authorities) dla swoich klientów. Razem stanowią one około 5,6 milionów użytkowników bankowych online (Szwecja ma około 7,3 mln obywateli w wieku powyżej 18 lat). BankID jest więc wiodącym systemem cyfrowej identyfikacji w Szwecji, z udziałem w rynku wynoszącym 75%.

System posiada ponad 3 miliony aktywnych użytkowników. W wielu usługach BankID obywatele mogą korzystać z cyfrowej identyfikacji, jak również z podpisu elektronicznego. Usługi rozciągają się od bankowości internetowej, e-handlu do składania deklaracji podatkowej i są dostarczane przez rząd, gminę, banki oraz firmy. BankID jest wykorzystywany zarówno do identyfikacji, jak również podpisania. Według szwedzkiego prawa i w ramach prawa Unii Europejskiej, BankID to zaawansowany podpis i złożony podpis z BankID jest prawnie wiążącym.

Identyfikacja klienta jest gwarantowana przez bank wydający BankID. Urzędy, firmy i inne organizacje powinny sprawdzić ważność potwierdzenia tożsamości klienta i podpis, używając oprogramowania opracowanego przez specjalistyczne certyfikowane firmy. BankID jest dostępny na karcie elektronicznej, jako „miękki” certyfikat⁹⁷ jak i w telefonie komórkowym, iPad'zie i innych komputerach typu tablet

9.2 NemID (Dania)

W Danii od dłuższego czasu funkcjonowały dwa klasyczne rozwiązania podpisu elektronicznego – Net-ID oraz OCES. Ich ograniczona popularność oraz wysokie koszty operacyjne utrzymania infrastruktury skłoniły duński bank centralny do zainicjowania prac nad nowym rozwiązaniem w zakresie uwierzytelnienia. Ich owocem, zaakceptowanym następnie w skali duńskiego sektora bankowego oraz w administracji publicznej i w niektórych internetowych serwisach sektora prywatnego, jest system NemID (w tłumaczeniu na angielski – EasyID). System został opracowany przez firmę DanID, należącą do banku centralnego Danii i został zainaugurowany 1 czerwca 2010 roku. Od tej pory każdy obywatel lub rezydent Danii w wieku powyżej 15 lat, legitymujący się indywidualnym numerem CPR (odpowiednik polskiego Pesela) może zwrócić się do jednego z licznych centrów obsługi NemID z wnioskiem o założenie konta w systemie. Wnioski przyjmowane są w bankach, centrach usług administracji publicznej, urzędach podatkowych (SKAT). Z punktu widzenia posiadacza konta w systemie jego elementami są:

- identyfikator posiadacza (którym może być numer CPR lub dowolnie wybrany łańcuch znaków),
- poufne, statyczne hasło stałe posiadacza,
- karta będąca nośnikiem dla 148 haseł jednorazowych, wygenerowanych w oparciu o klucz prywatny posiadacza.

Alternatywą dla wykorzystania karty z hasłami jednorazowymi jest zakup tokena spersonalizowanego danymi użytkownika. W takim przypadku czas życia nośnika haseł jednorazowych jest ograniczony jedynie czynnikami administracyjnymi (przykład karty i tokena na ilustracjach poniżej).

⁹⁷ certyfikat software'owy; certyfikaty takie są składowane w komputerze użytkownika, klucze prywatne są często przechowywane w standardowym rejestrze lub lokalnym systemie plików. Generowanie par kluczy PKI może odbywać się na komputerze użytkownika albo serwerze urzędu certyfikacji.

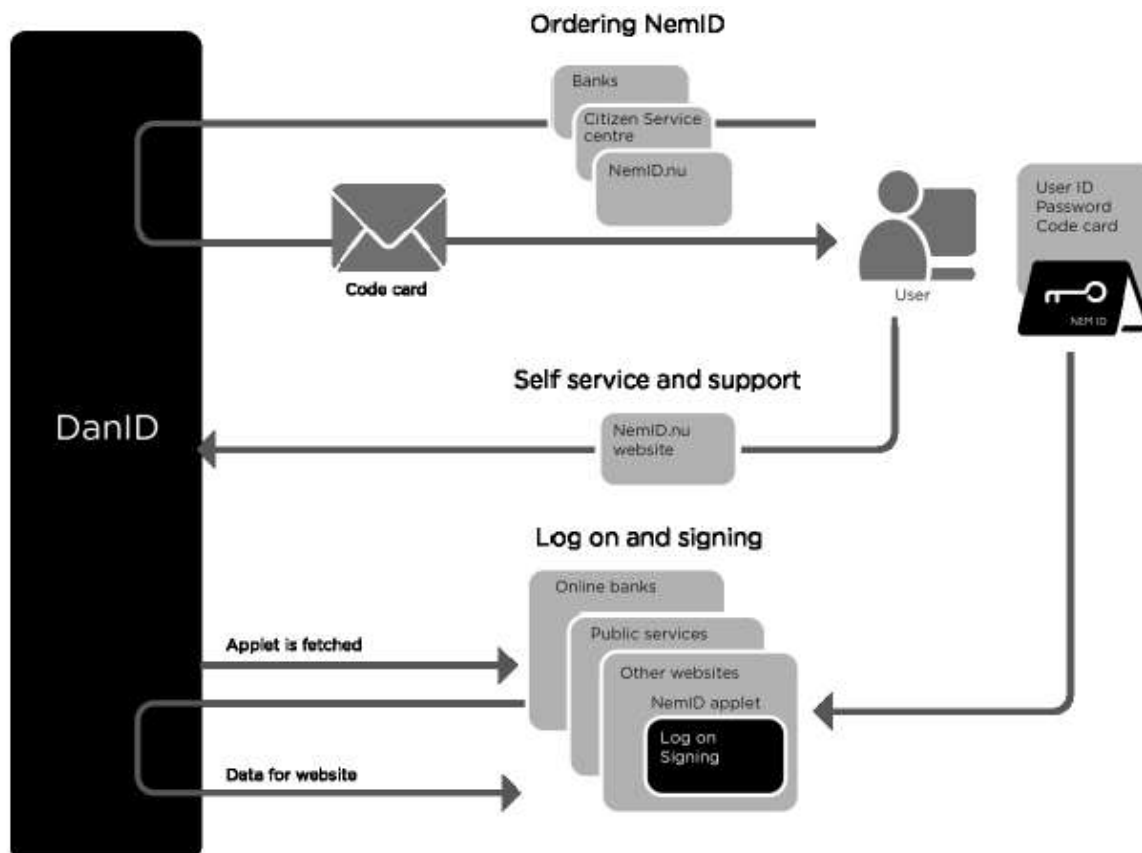


Rysunek 22. Przykłady karty z hasłami jednorazowymi i tokena OTP w programie NemID.

Dwuczynnikowa procedura uwierzytelnienia z wykorzystaniem NemID zakłada użycie informacji znanej wyłącznie użytkownikowi (identyfikator i hasło statyczne - coś, co użytkownik wie) oraz wykorzystanie haseł jednorazowych z posiadanej karty (coś, co użytkownika ma). Procedura użycia systemu jest następująca:

- 1) użytkownik loguje się w systemie używając swego identyfikatora i hasła statycznego;
- 2) system wyświetla pierwsze cztery z dziesięciu cyfr jednego z do tej pory niewykorzystanych haseł jednorazowych z karty,
- 3) użytkownik odnajduje na karcie hasło, którego pierwsze cyfry zostały wyświetlone przez system i wprowadza pozostałe sześć cyfr.

Procedura zakładania konta i wykorzystania NemID została zaprezentowana w skrócie na ilustracji poniżej.



Rysunek 23. Diagram procesów rejestracji i wykorzystania NemID.

Administrator systemu dba o przesłanie nowej karty z hasłami jednorazowymi, gdy liczba niewykorzystanych haseł na obecnie posiadanej karcie spada poniżej określonego poziomu. Założenie konta i wykorzystanie go do uwierzytelniania są nieodpłatne dla użytkownika, opłatę ponoszą natomiast właściciele serwisów, w których posiadacz konta uwierzytelnia się.

Począwszy od kwietnia 2011 roku poszerzono zasięg wykorzystania systemu NemID, oferując na jego bazie technicznej także identyfikator pracownika. Zasadnicza różnica pomiędzy NemID dla osób fizycznych i prawnych sprowadza się do tego, że drugi rodzaj identyfikatora nie jest powiązany z indywidualnym numerem CPR, lecz numerem identyfikacji korporacyjnej CVR. Dla jednego numeru CVR można otrzymać wiele identyfikatorów NemID, odpowiadających indywidualnym pracownikom i identyfikującym ich jednoznacznie. Dla jednej korporacji pierwsze trzy identyfikatory NemID wydawane są bezpłatnie, kolejne wiążą się z odpłatnością. W 2011 roku identyfikatory NemID posiadało około trzech milionów mieszkańców Danii. Rozwiązanie jest uważane za przykład harmonijnej współpracy sektora publicznego i prywatnego. Specjaliści bezpieczeństwa teleinformatycznego krytykują jednak samą zasadę konstrukcji systemu, zakładającą przechowanie unikalnego klucza prywatnego użytkownika w ramach infrastruktury administratora NemID.

9.3 Niemiecki eID (nPA)

Elektroniczny dokument tożsamości („neuer Personalausweis”, nPA) wszedł w Niemczech do użytku 1 listopada 2010 roku. Jego premiera była ukoronowaniem około 10-letniego procesu planowania i projektowania. Formalnie pierwsza zapowiedź wprowadzenia dokumentu znalazła się w planie przyjętym przez rząd federalny 13 października 2006 roku i zatytułowanym „Zorientowane na przeszłość zarządzanie przez innowację” (*Zukunftsorientierte Verwaltung durch Innovationen*). Jednym z jego dokumentów szczegółowych była strategia rozwoju usług elektronicznej administracji „eGovernment 2.0”, w ramach której przewidziano 4 pola działania; jednym z nich było udostępnienie obywatelom uniwersalnej metody elektronicznej identyfikacji i uwierzytelnienia w formie elektronicznego dokumentu tożsamości. Jednakże przesłanki dla wdrożenia w skali całego kraju uniwersalnej metody elektronicznego uwierzytelnienia pojawiły się już we wcześniejszych programach rozwoju usług elektronicznych, np. w przyjętym w 2003 roku programie „Deutschland-Online”, zakładającym m.in. integrację usług elektronicznych świadczonych przez rząd federalny i rządy krajów związkowych, oraz przyjętym w 2000 roku programie „BundOnline2005”, przewidującym udostępnienie w sieci wszystkich nadających się do informatyzacji usług administracji federalnej do roku 2005.

W marcu 2005 roku rząd federalny zaprezentował „Strategię eCard” – dokument określający wspólne podstawy techniczne i organizacyjne dla (początkowo) dwóch usług elektronicznych, które planowano udostępnić obywatelom: karty ubezpieczenia zdrowotnego oraz elektronicznego dokumentu tożsamości. W momencie swej premiery „Strategia eCard” zakładała, że obie funkcje zostaną połączone we wspólnym dokumencie. W listopadzie 2005 roku Niemcy rozpoczęły dystrybucję paszportów nowego wzoru, zgodnych z rozporządzeniem EU. Pozwoliło to podjąć prace nad projektem wspólnych standardów technicznych i organizacyjnych w odniesieniu do szeregu elektronicznych poświadczeń tożsamości emitowanych na poziomie federalnym. Ich wypracowanie zlecono Federalnemu Urzędowi Bezpieczeństwa Teleinformatycznego (*Bundesamt für Sicherheit in der Informationstechnik*, BSI). Efektem pracy specjalistów urzędu był zestaw wytyczny dokumentów tzw. *Technical Report*, określających m.in. architekturę elektronicznego dokumentu tożsamości, protokoły kryptograficzne, testy zgodności, czy wymogi dotyczące infrastruktury.

W czerwcu 2008 roku Bundestag rozpoczął procedurę legislacyjną prawa o elektronicznym dokumencie tożsamości. Dodatkową komplikacją w tym procesie była konieczność zmiany konstytucji; dotychczasowa ustawa zasadnicza przypisywała niektóre funkcje związane z emisją dokumentów tożsamości krajom związkowym. Nieco wcześniej, bo w kwietniu tego samego roku rząd federalny przyjął rozporządzenie inicjujące proces opracowania i wydawania funkcjonariuszom publicznym i personelowi wojskowemu elektronicznego poświadczenia tożsamości, określającego uprawnienia do użytkowania systemów informatycznych sektora publicznego oraz armii. W ten sposób elektroniczny identyfikator funkcjonariusza publicznego wyprzedził emisję powszechnego dokumentu tożsamości, stając się dlań swego rodzaju poligonem doświadczalnym. Ustawa o dowodzie osobistym i elektronicznym poświadczeniu tożsamości (*Gesetz über Personalausweise und den elektronischen Identitätsnachweis*) została uchwalona 18 czerwca 2009 roku. Zmiany w konstytucji niezbędne dla implementacji projektu nPA zostały przyjęte przez Bundestag 1 sierpnia 2009 roku, w ramach pakietu reform struktury federalnej niemieckiego państwa. Niezbędne dla implementacji tej reformy porozumienie pomiędzy rządem federalnym i krajami związkowymi weszło w życie 1 kwietnia 2010 r. Nieco wcześniej, bo w styczniu 2010 roku, opublikowano specyfikację techniczną dokumentu tożsamości oraz zainicjowano podprojekt projektu nPA, którego celem było wdrożenie przez wybranych partnerów usług elektronicznych bazujących na

Identyfikacja i uwierzytelnianie w usługach elektronicznych

- wzrost (w cm),
- kolor oczu,
- adres zamieszkania,
- obywatelstwo,
- oznaczenie serii i numer serii dokumentu,
- przydomek wyznaniowy lub pseudonim artystyczny (opcjonalnie),
- termin wydania i termin ważności dokumentu,
- numer CAN (*Card Access Number*, patrz opis protokołu PACE poniżej).

Warstwa elektroniczna dokumentu zawiera kopię danych zawartych w warstwie graficznej za wyjątkiem danych dotyczących wzrostu, koloru oczu oraz podpisu posiadacza. Przewidziano możliwość umieszczenia w warstwie elektronicznej dokumentu biometrycznych charakterystyk linii papilarnych dwóch palców, są one jednak umieszczane w dokumencie wyłącznie na wniosek jego posiadacza.

Trzem funkcjonalnościom nPA odpowiadają trzy odrębne aplikacje zapisane w pamięci mikroprocesora karty. Pierwsza z nich, określana mianem *ePass*, realizuje funkcję bezpiecznego dokumentu tożsamości i dokumentu podróży. Posiada ona dostęp wyłącznie do tych danych posiadacza, które zostały zapisane w strefie MRZ (*Machine Readable Zone*) dokumentu oraz danych biometrycznych (wizerunku twarzy oraz, opcjonalnie, odcisków palców). Jest ona wywoływana wyłącznie po wzajemnym uwierzytelnieniu dokumentu oraz terminala (którego mechanizmy zostaną opisane dalej) oraz identyfikacji terminala jako należącego do służb uprawnionych do kontroli tożsamości posiadacza (policja, straż graniczna, służby celne itp.).

Druga aplikacja, określana mianem *eID*, pozwala posiadaczowi dokumentu uwierzytelić się w systemach informatycznych, zarówno lokalnych, jak zdalnych. Interesującą cechą uwierzytelnienia z wykorzystaniem aplikacji *eID* jest możliwość wykorzystania mechanizmu selektywnej identyfikacji. W ramach tego mechanizmu identyfikacji dla każdego serwisu korzystającego z funkcjonalności *eID* zdefiniowano uprawnienia do żądania określonych elementów spośród zestawu danych zapisanych w nPA. W trakcie procedury identyfikacji posiadacz dokumentu jest informowany o uprawnieniach serwisu, w którym usiłuje się uwierzytelić, po czym może podjąć decyzję o udostępnieniu lub odmowie udostępnienia serwisowi dowolnego elementu lub podzbioru danych z tego zestawu. Aplikacja *eID* nie ma jednak dostępu do zapisanych w nPA danych biometrycznych, zastrzeżonych dla aplikacji *ePass*. Drugą specyficzną funkcjonalnością aplikacji *eID* jest możliwość posługiwania się przez posiadacza nPA nieograniczoną liczbą pseudonimów cyfrowych, specyficznych dla obszarów jej/jego aktywności w Internecie. Cyfrowy pseudonim użytkownika jest wyznaczany m.in. na podstawie unikalnego identyfikatora sektora oraz również unikalnego sekretu, przechowywanego w nPA, dzięki czemu pseudonim tej samej osoby w różnych sektorach przyjmuje różną wartość. Cyfrowy pseudonim pozwala na jednoznaczną identyfikację użytkownika i jego uwierzytelnienie wobec serwisu internetowego, dla którego pseudonim został zdefiniowany, bez ujawniania danych osobowych posiadacza. Użycie różnych pseudonimów w relacjach z różnymi serwisami zapewnia ścisłą wzajemną separację pseudonimowej tożsamości; nawet w wypadku współdziałania dwóch lub więcej serwisów nie są one w stanie określić związku pomiędzy przypadkami użycia pseudonimów powiązanych z rzeczywistą tożsamością użytkownika.

Protokół identyfikacji i uwierzytelnienia z wykorzystaniem funkcji *eID* jest protokołem trójstronnym. Obok posiadacza nPA oraz dostawcy usługi, wobec której posiadacz usiłuje się uwierzytelić, uczestniczy w nim administrator tożsamości, określany jako serwer *eID*. Serwer *eID* dysponuje trzema interfejsami programowymi. Od strony dostawcy usługi jest to interfejs *eID*, zapewniający komunikację pomiędzy

Identyfikacja i uwierzytelnianie w usługach elektronicznych

oprogramowaniem serwera usług oraz funkcją eID. Od strony posiadacza nPA widoczny jest interfejs eCard-API, zapewniający komunikację serwera z kartą nPA i middleware. Trzeci interfejs pozwala na komunikację z dostawcami usług certyfikacyjnych w ramach infrastruktury nPA (zarządzanie certyfikatami CSCA i DVCA oraz listami certyfikatów unieważnionych). Typowy scenariusz komunikacji pomiędzy posiadaczem nPA, dostawcą usługi oraz serwerem eID przedstawiono na rysunku poniżej.



Rysunek 25. Schemat komunikacji między elementami systemu niemieckiego eID (nPA).

Zanim usługodawca będzie mógł zacząć świadczyć usługi wykorzystujące funkcjonalność nPA, musi uzyskać odpowiedni certyfikat, potwierdzający tożsamość usługodawcy i zakres danych w nPA, do których może żądać dostępu. W tym celu zwraca się do właściwej placówki administracji federalnej (*Vergabestelle für Berechtigungszertifikate* w *Bundesverwaltungsamt*), która potwierdza tożsamość usługodawcy i określa zakres adekwatnego do charakteru świadczonych przezeń usług dostępu do danych w nPA. Na podstawie uzyskanego poświadczenia usługodawca zwraca się następnie do urzędu certyfikacji BerCA (*Berechtigung CA*) z wnioskiem o wystawienie odpowiedniego certyfikatu. Jednym z atrybutów tego certyfikatu jest określenie pól danych w nPA, do których posiadacz certyfikatu może żądać dostępu. W chwili obecnej rolę BerCA pełni 3 podmioty.

Od strony biznesowej funkcja serwera eID może zostać zrealizowana na dwa sposoby. Przy znaczącej skali operacji uwierzytelnienia administrator danego sektora może zdecydować w wdrożeniu własnego serwera eID, posługując się jednym z dostępnych rozwiązań komercyjnych. Do chwili obecnej (listopad 2012) BSI certyfikował na zgodność z zaleceniem TR-03130 systemy serwera eID oferowane przez czterech producentów. Alternatywą dla budowy własnego serwera eID jest skorzystanie z analogicznej usługi, realizowanej przez dostawcę komercyjnego. W chwili obecnej usługi serwera eID świadczone są przez 10 podmiotów.

Trzecią aplikację nPA stanowi standardowa aplikacja obsługująca funkcjonalność podpisu elektronicznego potwierdzonego kwalifikowanym certyfikatem. Wykorzystanie tej funkcjonalności przez

Identyfikacja i uwierzytelnianie w usługach elektronicznych

posiadacza nPA jest opcjonalne. Świadczenie usług certyfikacyjnych o komercyjnym charakterze stanowiłoby nieuprawnioną pomoc publiczną w rozumieniu dyrektyw UE, toteż nPA stanowi jedynie nośnik dla klucza i certyfikatu kwalifikowanego, wydawanego i instalowanego w nPA przez jednego z dostawców komercyjnych.

Poza określonymi powyżej mechanizmami wykorzystującymi funkcjonalności nPA, na użytek projektu wypracowano szereg rozwiązań technicznych, które albo zostały zatwierdzone w formie odpowiednich standardów, albo znajdują się w stadium zatwierdzania. W pierwszym rzędzie należy zauważyć, że mechanizmy kryptograficzne wykorzystane w nPA opierają się na kryptografii krzywych eliptycznych (ECC, w zgodności z zaleceniem TR-03111). Można założyć, że decyzja ta była konsekwencją wyczerpywania się potencjału rozwoju dominującej dotąd kryptografii RSA; oczekiwanego wzrostu bezpiecznej długości klucza poza granice praktycznego użytku. Oparcie się na ECC pozwala skrócić czas generacji kluczy oraz znacząco zredukować ich bezpieczną długość.

Drugą nowością w nPA jest uzupełnienie klasycznego protokołu BAC (*Basic Access Control*), wymaganego na podstawie przepisów ICAO w dokumentach podróży przez zaprojektowany z myślą o nPA protokół PACE (*Password Authenticated Connection Establishment*). Konieczność użycia obu protokołów wiąże się z wykorzystaniem w dokumentach podróży kart z interfejsem bezstykowym i wynikającym zeń zagrożeniem odczytem danych przechowywanych na karcie bez zgody, a nawet bez świadomości posiadacza dokumentu. Protokół BAC jest standardem powszechnie obowiązującym, jednak krytykowanym ze względu na niski poziom entropii danych wejściowych. Krytyka kierowana pod adresem BAC, jak również konieczność używania skanerów optycznych w czytnikach realizujących protokół BAC (istotny koszt), doprowadziły do opracowania na użytek nPA nowego protokołu – PACE. W przypadku wykorzystania funkcji *eID* przez posiadacza dokumentu wartością wejściową protokołu PACE jest jego sekretny PIN. W przypadku kontroli tożsamości przez przedstawiciela uprawnionych do tego władz wartością wejściową protokołu PACE jest numer CAN. Warto dodać, że obecnie istnieje już międzynarodowa specyfikacja protokołu PACE przyjęta przez organizację ICAO w dokumencie ICAO Technical Report - Supplemental Access Control (SAC). Od grudnia 2014 roku wszystkie nowo wydawane dokumenty podróży będą musiały go stosować obok BAC (rezygnacja z BAC jest przewidywana od 2018 r.). Opracowanie jednolitej, uznawanej międzynarodowo specyfikacji jest krokiem w kierunku uzyskania interoperacyjności między własnymi rozwiązaniami niemieckimi, a rozwiązaniami międzynarodowymi, w szczególności europejskimi.

Kolejnym poziomem zabezpieczenia danych i operacji w nPA jest rodzina protokołów określanych wspólnie mianem *Extended Access Control* (EAC). Potrzeba ich opracowania wyniknęła z decyzji Komisji Europejskiej numer 2909 z 28 czerwca 2006, w której opisano zasadnicze wymagania dotyczące zabezpieczeń danych biometrycznych zawartych w elektronicznych paszportach. Na ich podstawie niemiecki BSI opracował specyfikację TR-03110 v.1.11, która została następnie przyjęta jako standard obowiązujący w odniesieniu do dokumentów podróży wydawanych przez kraje UE. Jakkolwiek przyczyną podjęcia prac nad specyfikacją EAC było zabezpieczenie danych w dokumentach podróży, specyfikacja TR-03110 stanowi część wspólnej platformy bezpieczeństwa opracowanej przez BSI na potrzeby rodziny silnie zabezpieczonych dokumentów i w tym charakterze zasługuje na krótkie przedstawienie w kontekście nPA.

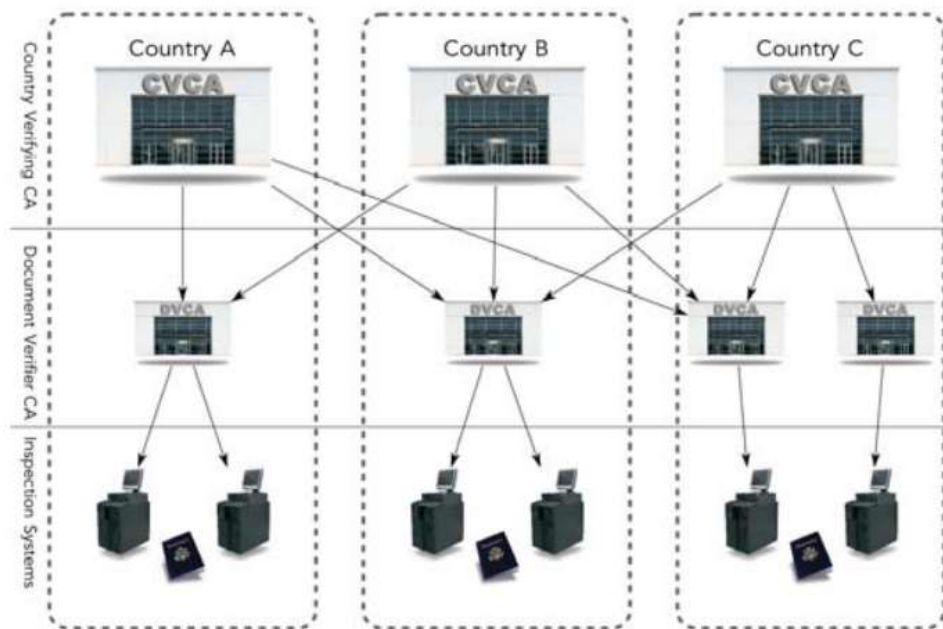
Celem użycia protokołów EAC jest zapewnienie wzajemnego, silnego uwierzytelnienia dokumentu (*Chip Authentication* - CA) i terminala (*Terminal Authentication* - TA) oraz ustanowienie bezpiecznej sesji wymiany informacji pomiędzy nimi.

Identyfikacja i uwierzytelnianie w usługach elektronicznych

Faza TA jest bardziej złożona i wymaga określenia (przynajmniej pobieżnie) infrastruktury PKI funkcjonującej w ramach ekosystemu nPA (ePass). Jak wynika z informacji przedstawionych wcześniej, w różnych scenariuszach użycia nPA wykorzystuje się różne zawarte w dokumencie dane. Użycie nPA w roli dokumentu podróży implikuje konieczność dostępu do zawartych w nim danych biometrycznych. Użycie nPA w roli eID implikuje dostęp do wybranych danych osobowych, ale nie biometrycznych. Konieczne jest rozróżnienie i potwierdzenie uprawnień terminali wykorzystywanych przez różne władze dokonujące inspekcji dokumentu do dostępu do określonych, zawartych w nim informacji. W tym celu w każdym kraju wykorzystującym (aktywnie lub pasywnie) protokół EAC konieczne jest zbudowanie elementów infrastruktury klucza publicznego EAC-PKI. Jeżeli kraj emituje dokumenty wykorzystujące funkcjonalność EAC, jej lokalnym centrum jest urząd certyfikacji CVCA (*Country Verifying Certification Authority*). Zadaniem CVCA jest generowanie i dystrybucja certyfikatów na rzecz krajowych i zagranicznych urzędów certyfikacji DVCA (*Document Verifier Certification Authority*). Jeżeli dany kraj nie emituje dokumentów wykorzystujących protokół EAC, lecz prowadzi ich inspekcję, jego DVCA otrzymuje niezbędne certyfikaty bezpośrednio od CVCA krajów – emitentów dokumentów. CVCA przekazują odpowiednie certyfikaty do DVCA wszystkich krajów uprawnionych do inspekcji dokumentów emitowanych przez dany kraj (przykładową strukturę i zależności pomiędzy CVCA i DVCA przedstawiono na ilustracji poniżej). W typowym scenariuszu urzędy certyfikacji DVCA są organizowane przez władzę nadzorującą służbę uprawnioną do kontroli dokumentów (np. policję, służbę graniczną itp.). Certyfikaty te uprawniają DVCA do generacji certyfikatów CVC (*Card Verifiable Certificates*), które są instalowane bezpośrednio w terminalach i zawierają określenie uprawnień danego terminala dostępu do danych zawartych w dokumencie.

Ze względu na dynamiczną strukturę organizacyjną służb uprawnionych do inspekcji dokumentów oraz możliwość zagubienia/kradzieży/utrąty uprawnień ze strony systemu inspekcji certyfikaty CVC mają bardzo ograniczony czas ważności, rzędu 30 dni. Certyfikaty te są weryfikowane przez oprogramowanie wbudowane do procesora karty elektronicznej (paszportu), gdzie są bardzo ograniczone zasoby. Stąd nie są one zgodne ze znanym i powszechnie wykorzystywanym w systemach PKI formacie X.509, lecz jako certyfikaty krótkoterminowe w formacie „CV” opisanym w normie ISO/IEC 7816.

Ostatnim wartym wzmianki elementem ekosystemu nPA jest czytnik kart. Niemieckie władze zalecają wykorzystanie z nPA jednego z trzech typów czytników, które zostały certyfikowane przez BSI; podstawowy, standardowy i komfortowy. Wersje standardowa i komfortowa dysponują klawiaturą umożliwiającą wprowadzenie hasła protokołu PACE. Wersja podstawowa i standardowa są wystarczające dla realizacji funkcji eID, podczas gdy wykorzystanie kwalifikowanego podpisu elektronicznego wymaga użycia czytnika w wersji komfortowej (wyposażonego w wyświetlacz i autonomiczny moduł kryptograficzny).



Rysunek 26. Model architektury PKI dla realizacji Terminal Authentication (TA) w protokole Extended Access Control (EAC).

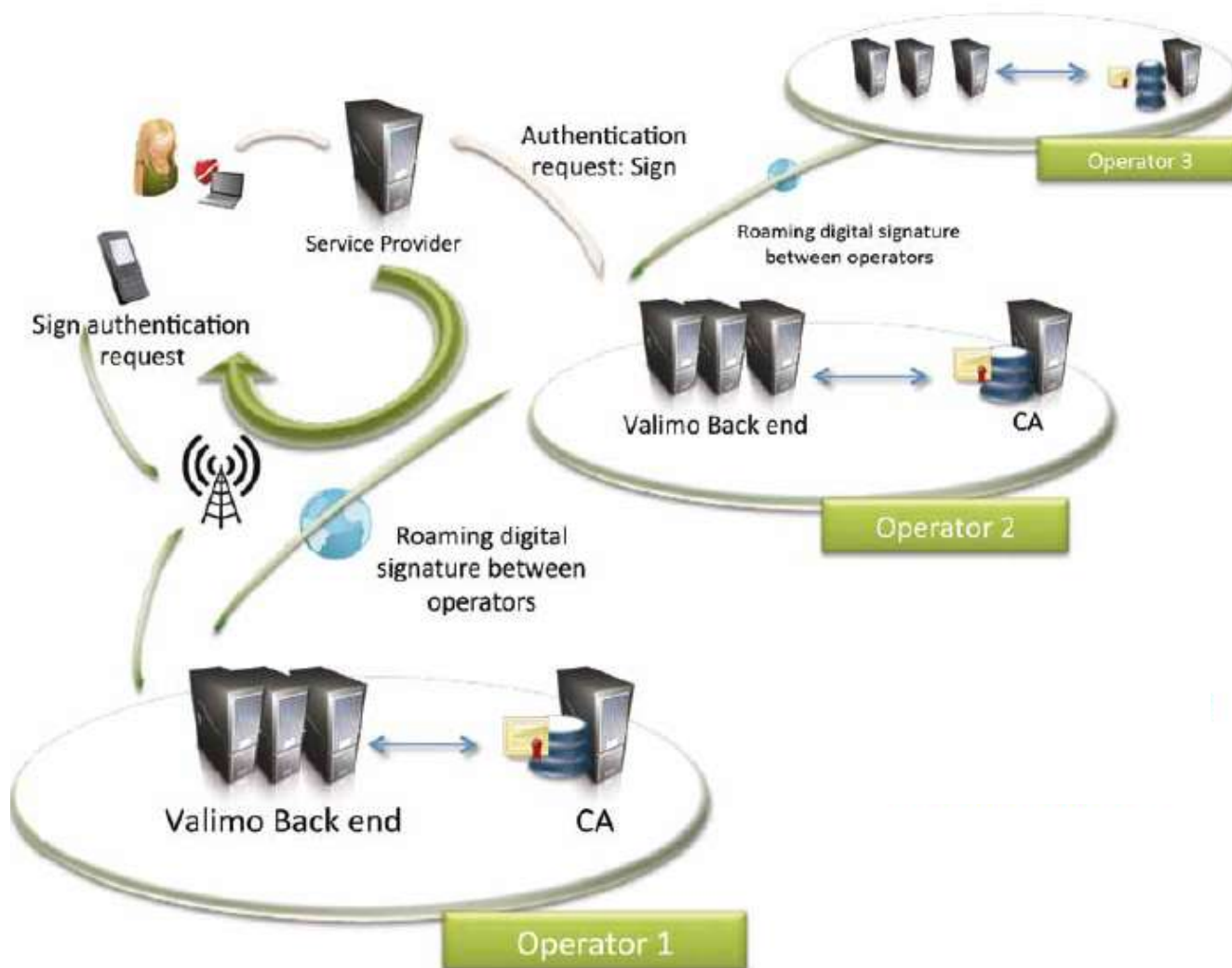
9.4 MobileID (Finlandia)

MobileID to termin określający systemy do identyfikacji i uwierzytelnienia (elektronicznego) z użyciem urządzeń mobilnych takich jak telefon komórkowy czy tablet. Rozwiązania takie wykorzystują typowe metody uwierzytelnienia (np. PKI, czy OTP). Wyróżnikiem tych rozwiązań jest ich specyficzny sposób realizacji – wykorzystanie karty SIM jako bezpiecznego elementu przenoszącego sekrety, aplikacji urządzeń mobilnych oraz infrastruktury operatorów telekomunikacyjnych i komunikatów SMS do przekazywania danych między elementami systemu. Rozwiązania mobilne wykorzystujące PKI, często nazywane są „MobilePKI”.

Główną metodą uwierzytelnienia do usług bankowych w Finlandii są hasła jednorazowe (OTP). Wg lokalnego prawa, ta metoda jest zaliczana do silnego uwierzytelnienia, co jest ewenementem w skali Europy. Jednym z celów wdrożenia „mobile PKI” było zastąpienie OTP przez mechanizm faktycznie silnego uwierzytelnienia, przy jednoczesnym zapewnieniu masowości i łatwości użycia, jak w przypadku OTP.

Operatorzy telefonii komórkowej (m.in. DNA Finland, Elisa, i TeliaSonera) zdecydowali się na stworzenie krajowego standardu podpisu mobilnego bazującego na standardach ETSI Mobile Signature Services (najważniejsze to: ETSI TS 102 204, ETSI TS 102 207, ETSI TR 102 203). Następnie każdy operator wdrożył swój system, zapewniając jego interoperacyjność z pozostałymi rozwiązaniami, a mobilne uwierzytelnienie może przebiegać przez infrastrukturę dowolnego operatora włączonego w system

MobileID (wykorzystywany jest tzw. roaming podpisu elektronicznego). Idea ta jest zobrazowana na rys. Rysunek 27.



Rysunek 27. Zasada działania mobilnego podpisu w Finlandii.

Infrastruktura rozwiązania składa się z następujących komponentów⁹⁸:

- Serwer Podpisu – zgodny z ETSI MSS dostawca podpisu serwerowego (Mobile Signature Service Provider – MSSP), oferujący podstawowe mechanizmy MobileID – składanie i weryfikację podpisów elektronicznych oraz uwierzytelnienie PKI – a także zarządza komunikacją z urządzeniami mobilnymi i całością transakcji podpisu;

⁹⁸ Dostawcą komponentów jest firma Valimo, z wyłączeniem Urzędu Certyfikacji.

Identyfikacja i uwierzytelnianie w usługach elektronicznych

- Serwer (Urząd) Rejestracji – realizuje różne procesy rejestracji użytkowników i dostarczania danych uwierzytelniających MobileID;
- Serwer Wiadomości (ang. Messaging Server) – zapewnia komunikację pomiędzy aplikacją na urządzeniu mobilnym a pozostałymi serwerami systemu, wykorzystując systemy SMS poszczególnych operatorów;
- MSS SDK – zestaw narzędzi programistycznych do integracji z elementami systemu Mobile ID;
- VMAC – aplikacja podpisująca umieszczona na kartach SIM;
- Urząd Certyfikacji – system do wydawania certyfikatów elektronicznych X.509.

Proces rejestracji odbywa się w punktach obsługi klienta operatorów lub zdalnie - on-line (pod warunkiem uwierzytelnienia za pomocą mechanizmu OTP wydanego przez bank oraz posiadania aplikacji VMAC na karcie SIM). Ponadto w zdalnym procesie wydawania certyfikatu, tożsamość osoby aplikującej jest weryfikowana względem rejestru państwowego (VRK). W modelu fińskim każdy operator posiada własne (kwalifikowane) centrum certyfikacji, a certyfikaty spełniają wymagania dyrektywy UE o podpisie elektronicznym i są ważne 5 lat.

9.5 OpenID

OpenID pozwala na wykorzystanie istniejącego konta do logowania się na wielu stronach internetowych, bez konieczności tworzenia nowych haseł. OpenID został opracowany w lecie 2005 roku przez społeczność open source próbującą rozwiązać problem, którego nie było łatwo rozwiązać za pomocą innych istniejących technologii tożsamości. Jako takie, OpenID jest zdecentralizowany, i nie jest własnością kogokolwiek, ani też nie powinno być. Dziś każdy może zdecydować się na stosowanie OpenID lub stać się dostawcą OpenID za darmo, bez konieczności rejestracji lub zatwierdzenia przez jakąkolwiek organizację

OpenID to system uwierzytelniania, w którym wystarczy jedno konto OpenID by móc "logować" się na wszystkich serwisach wspierających OpenID. Logowanie dokonuje się tylko na stronie konta openID a nie na np. 50 różnych stronach, dla których trzeba zapamiętać loginy i hasła. By utworzyć konto openID wystarczy zarejestrować się na którejś ze stron, która obsługuje konta OpenID np. openid.pl. Po takiej rejestracji można logować się na wszystkie strony wspierające openID - wystarczy podanie swojego loginu openID.

OpenID został opracowany w lecie 2005 roku przez społeczność open source próbującą rozwiązać problem, którego nie było łatwo rozwiązać za pomocą innych istniejących technologii tożsamości. Jako takie, OpenID jest zdecentralizowana, i nie jest własnością kogokolwiek, ani też nie powinno być. Dziś każdy może zdecydować się na stosowanie OpenID lub stać dostawcą OpenID za darmo, bez konieczności rejestracji lub zatwierdzenia przez jakąkolwiek organizację. Powstała Fundacja OpenID w celu wspierania modelu open source, zapewniając prawną obsługę dla społeczności poprzez zapewnienie niezbędnej infrastruktury i pomagającą promować i wspierać rozszerzone adaptacje OpenID.

OpenID szybko zyskuje akceptację w Internecie, obecnie jest ponad miliard kont użytkowników OpenID i ponad 50.000 stron internetowych akceptujących logowanie OpenID. Kilka dużych organizacji wydaje

Identyfikacja i uwierzytelnianie w usługach elektronicznych

lub akceptuje OpenIDs, w tym Google, Facebook, Yahoo, Microsoft, AOL, MySpace, Sears, Universal Music Group, France Telecom, Novell, Sun, Telecom Italia, i wiele innych.

Zalety OpenID:

- łatwość korzystania -- bo użytkownik w każdym serwisie posługuje się jednym identyfikatorem, zamiast w każdym z nich zakładać oddzielne konto, wypełniać dane i ustawiać hasło
- decentralizacja -- możliwa dlatego że identyfikator jest równocześnie adresem serwera; architektura nie wymusza korzystania z jednej, centralnej bazy haseł bo każdy może postawić swój serwer i używać jego adresu jako identyfikatora
- kontrola prywatności -- to użytkownik wskazuje, jakie informacje może pobrać serwis (np. email - tak, telefon - nie) i ma później wgląd w historię pobieranych informacji
- łatwość aktualizacji -- ponieważ dane są przechowywane w jednej lokalizacji, a w razie zmian wszystkie serwisy zaktualizują je sobie automatycznie

Zagrożenia OpenID

- kradzież tożsamości - kradzież danych dostępowych do serwera OpenID (najczęściej login i hasło) umożliwia włamywaczowi posługiwanie się tożsamością ofiary bez ograniczeń we wszystkich serwisach z których ona korzystała - a także w nowych. Ze względu na to, że logowanie odbywa się na stronie innej, niż docelowa, phishing jest znacznie ułatwiony.
- koncentracja danych - gromadzenie wszystkich danych o użytkowniku na jednym serwerze naraża w przypadku włamania na serwer OpenID, na kradzież ważnych danych takich jak numery kart kredytowych.

10 Literatura

- [1] IDABC eID Interoperability for PEGS, Common specifications for eID interoperability in the eGovernment context
- [2] STORK - D2.3 - Quality authenticator scheme
- [3] ISO/IEC 29115, 01.04.2013, Information technology – Security techniques – Entity authentication assurance framework
- [4] www.eid-stork.eu
- [5] PN-I-02000:2002 Technika informatyczna - Zabezpieczenia w systemach informatycznych – Terminologia; marzec 2002 z poprawką z kwietnia 2010
- [6] „Interchange of Data between Administrations (IDA) - Authentication Policy” (<http://ec.europa.eu/idabc/en/document/3532/5585>); lipiec 2004
- [7] NIST Special Publication 800-53 “Security and Privacy Controls for Federal Information Systems and Organizations” (<http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf>)
- [8] NIST Special Publication 800-162 DRAFT – FINAL “Guide to Attribute Based Access Control (ABAC) Definition and Considerations” (http://csrc.nist.gov/publications/drafts/800-162/sp800_162_draft.pdf)
- [9] PN-ISO/IEC 13888 “Technika informatyczna – Techniki zabezpieczeń – Niezaprzeczalność”
- [10] CWA 14365-1 “Guide on the Use of Electronic Signatures - Part 1: Legal and Technical Aspects”
- [11] CWA 14167-1 “Security Requirements for Trustworthy Systems Managing Certificates for Electronic Signatures - Part 1: System Security Requirements”
- [12] CWA 14167-2 “Cryptographic module for CSP signing operations with backup - Protection profile - CMCSOB PP”
- [13] CWA 14169 “Secure signature-creation devices “EAL 4+””
- [14] CWA 14172-5 “EESSI Conformity Assessment Guidance - Part 5: Secure signature-creation devices”
- [15] ETSI TS 101 733 “Electronic Signatures and Infrastructures (ESI); CMS Advanced Electronic Signatures (CAdES)”
- [16] ETSI TS 101 862 “Qualified Certificate profile”
- [17] ETSI TS 101 903 “Electronic Signatures and Infrastructures (ESI); XML Advanced Electronic Signatures (XAdES)”

Identyfikacja i uwierzytelnianie w usługach elektronicznych

[18] ETSI TS 102 176-1 "Electronic Signatures and Infrastructures (ESI); Algorithms and Parameters for Secure Electronic Signatures; Part 1: Hash functions and asymmetric algorithms"

[19] ETSI TR 102 203 "Mobile Commerce (M-COMM); Mobile Signatures; Business and Functional Requirements"

[20] ETSI TS 102 204 "Mobile Commerce (M-COMM); Mobile Signature Service; Web Service Interface"

[21] ETSI TR 102 206 "Mobile Commerce (M-COMM); Mobile Signature Service; Security Framework"

[22] ETSI TS 102 207 "Mobile Commerce (M-COMM); Mobile Signature Service; Specifications for Roaming in Mobile Signature Services"

[23] ETSI TS 102 778 "Electronic Signatures and Infrastructures (ESI); PDF Advanced Electronic Signature Profiles"

[24] COMMISSION DECISION of 6 November 2000 on the minimum criteria to be taken into account by Member States when designating bodies in accordance with Article 3(4) of Directive 1999/93/EC of the European Parliament and of the Council on a Community framework for electronic signatures – 2000/709/EC (Dz. Urz. UE L 289/42)

[25] COMMISSION DECISION of 14 July 2003 on the publication of reference numbers of generally recognised standards for electronic signature products in accordance with Directive 1999/93/EC of the European Parliament and of the Council – 2003/511/EC (Dz. Urz. UE L 175/45)

[26] DYREKTYWA PARLAMENTU EUROPEJSKIEGO I RADY 1999/93/WE z dnia 13 grudnia 1999 r. w sprawie wspólnotowych ram w zakresie podpisów elektronicznych (Dz. Urz. UE L 13/12)

[27] ROZPORZĄDZENIE PARLAMENTU EUROPEJSKIEGO I RADY w sprawie identyfikacji elektronicznej i usług zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznym – COM(2012) 238 final (projekt)

11 Załącznik - polityka bezpieczeństwa wg NIST SP 800-53

Poniżej przedstawiono najważniejsze aspekty poprawnie wdrożonej polityki bezpieczeństwa w zakresie identyfikacji i uwierzytelnienia wg dokumentu NIST SP 800-53.

Uwaga 1: treść pkt. *Zabezpieczenie* (razem z *Dodatkowymi wskazówkami i wymaganiami*) ma status obligatoryjności, natomiast *Zabezpieczenia rozszerzające* są rekomendowane, ale nie obligatoryjne w każdym przypadku (do decyzji kierownika jednostki organizacyjnej), aczkolwiek często zabezpieczenie rozszerzające – fakultatywne wg NIST – jest wymagane przepisami polskiego lub unijnego prawa.

Uwaga 2: standard dopuszcza pewną elastyczność poprzez użycie określeń [przypisanie:], których treść musi być zmodyfikowana przez organizację w zależności od (i) wymagań bezpieczeństwa organizacji mających na celu wspieranie konkretnej misji, funkcji biznesowej lub działalności operacyjnej; (ii) wymagań mających swoje źródło w lokalnym prawie, dyrektywach, politykach, regulacjach, standardach itp.

IA-2 Identyfikacja i uwierzytelnianie użytkowników jednostki organizacyjnej

Zabezpieczenie: system teleinformatyczny identyfikuje wszystkich użytkowników jednostki organizacyjnej z osobna (jak również procesy działające na żądanie tych użytkowników).

Dodatkowe wskazówki i wymagania:

- użytkownicy jednostki organizacyjnej to pracownicy oraz osoby posiadające porównywalny status, co pracownicy (np. osoby zatrudnione na podstawie umowy cywilno-prawnej, podwykonawcy). Użytkownicy są identyfikowani w sposób unikalny i uwierzytelniani przy wszystkich próbach dostępu. Należy rozważyć konieczność unikalnej identyfikacji osób korzystających z konta grupowego na potrzeby rozliczalności działań, przy czym taka rozliczalność jest wymagana w przypadku konta grupowego dla zdarzeń podlegających zapisom w logach audytowych.
- dostęp do systemów teleinformatycznych organizacji może mieć charakter lokalny lub sieciowy. *Dostęp lokalny* to taki dostęp użytkownika (lub działającego na jego żądanie procesu) do systemów teleinformatycznych jednostki organizacyjnej, który nie wymaga pośrednictwa sieci teleinformatycznej, a z kolei *dostęp sieciowy* wymaga pośrednictwa sieci teleinformatycznej. Ponadto wyróżnia się *dostęp zdalny*, który jest rodzajem dostępu sieciowego, wymagającym połączeń poprzez sieci zewnętrzne (np. przez sieć publiczną). Sieci wewnętrzne obejmują LAN, WAN (z techniką VPN), które są w całości kontrolowane przez jednostkę organizacyjną. Sieci VPN są uznawane, jako wewnętrzne, jeśli jednostka organizacyjna ustanawia połączenia VPN pomiędzy punktami będącymi pod jej kontrolą i w sposób, który nie uzależnia jednostki organizacyjnej (poza aspektem dostępności) od zewnętrznej sieci, oraz w której VPN przesyła swoje dane i zabezpiecza poufność i integralność przesyłanych informacji.

W przypadku dostępu sieciowego, do identyfikacji i uwierzytelnienia użytkowników na poziomie systemu (przy logowaniu), powinny być stosowane ponadto mechanizmy identyfikacji i uwierzytelnienia na poziomie aplikacji, a administrator definiuje listę zdarzeń, które wymagają od użytkownika ponownego (dodatkowego) uwierzytelnienia w systemie.

Identyfikacja i uwierzytelnianie w usługach elektronicznych

- System teleinformatyczny wykorzystuje silne uwierzytelnienie⁹⁹ (np. wieloczynnikowe) w przypadku dostępu sieciowego do kont uprzywilejowanych.

Zabezpieczenia rozszerzające:

- 1 System teleinformatyczny wykorzystuje silne uwierzytelnienie w przypadku dostępu sieciowego do kont nieuprzywilejowanych.
- 2 System teleinformatyczny wykorzystuje silne uwierzytelnienie (wieloczynnikowe) w przypadku dostępu lokalnego do kont uprzywilejowanych.
- 3 System teleinformatyczny wykorzystuje silne uwierzytelnienie (wieloczynnikowe) w przypadku dostępu lokalnego do kont nieuprzywilejowanych.
- 4 Jednostka organizacyjna:
 - a) umożliwia wykorzystanie uwierzytelnienia grupowego wyłącznie w połączeniu z indywidualnym/unikalnym uwierzytelnieniem; oraz
 - b) wymaga, aby osoby były uwierzytelnione indywidualnie przed korzystaniem z konta grupowego.
- 5 System teleinformatyczny wykorzystuje silne uwierzytelnienie w przypadku dostępu sieciowego do kont uprzywilejowanych, gdzie jeden z czynników wykorzystuje urządzenie odseparowane od systemu, do którego realizowany jest dostęp.

Dodatkowe wskazówki dla zabezpieczenia rozszerzającego: przykładem urządzenia odseparowanego od systemu, do którego realizowany jest dostęp, wykorzystywanego do uwierzytelnienia jest kryptograficzna karta elektroniczna i techniki stosujące tzw. wyzwania (ang. *challenge*) lub technologia SecurID firmy RSA hasel jednorazowych opartych o element bieżącej daty i czasu.

- 6 System teleinformatyczny wykorzystuje silne uwierzytelnienie w przypadku dostępu sieciowego do kont nieuprzywilejowanych, gdzie jeden z czynników wykorzystuje urządzenie odseparowane od systemu, do którego realizowany jest dostęp.
- 7 System teleinformatyczny wykorzystuje mechanizm uwierzytelnienia odporny na ataki powtórzeniowe w przypadku dostępu sieciowego do kont uprzywilejowanych.

Dodatkowe wskazówki dla zabezpieczenia rozszerzającego: mechanizm uwierzytelnienia jest odporny na ataki powtórzeniowe, jeśli atak polegający na nagraniu i powtórzeniu poprzedniej próby logowania jest niepraktyczny. Techniki, do których odnosi się to rozszerzenie to techniki stosujące tzw. wyzwania (ang. *challenge*) lub mechanizmy zależne od czasu.

- 8 System teleinformatyczny wykorzystuje mechanizm uwierzytelnienia odporny na ataki powtórzeniowe w przypadku dostępu sieciowego do kont nieuprzywilejowanych.

IA-3 Identyfikacja i uwierzytelnianie urządzeń

Zabezpieczenie: system teleinformatyczny identyfikuje i uwierzytelnia każde urządzenie z osobna [przypisanie: zdefiniowana przez jednostkę organizacyjną lista urządzeń lub rodzajów urządzeń¹⁰⁰] przed nawiązaniem połączenia.

⁹⁹ patrz pkt 3.1 raportu

Dodatkowe wskazówki i wymagania:

- Urządzenia wymagające identyfikacji i uwierzytelnienia mogą być zdefiniowane przez rodzaj lub poprzez specyficzne cechy urządzenia (lub przez połączenie rodzaju i specyficznych cech urządzenia) w zależności od uznania jednostki organizacyjnej. System teleinformatyczny typowo wykorzystuje adres MAC (ang. *Media Access Control*), adres IP lub rozwiązania zaawansowane (np. IEEE 802.1x i EAP (ang. *Extensible Authentication Protocol*), serwer Radius z uwierzytelnieniem EAP-TLS, Kerberos) w celu identyfikacji i uwierzytelnienia urządzeń w sieciach LAN i WAN.

Zabezpieczenia rozszerzające:

- 1 System teleinformatyczny uwierzytelnia urządzenia przed nawiązaniem zdalnych i bezprzewodowych połączeń sieciowych stosując dwustronne uwierzytelnienie oparte na mechanizmach kryptograficznych.

Dodatkowe wskazówki dla zabezpieczenia rozszerzającego: zdalne połączenie sieciowe to połączenie z urządzeniem komunikującym się przez sieć zewnętrzną, np. sieć publiczną.

- 2 System teleinformatyczny uwierzytelnia urządzenia przed nawiązaniem połączeń sieciowych stosując dwustronne uwierzytelnienie oparte na mechanizmach kryptograficznych.
- 3 Jednostka organizacyjna, w oparciu o dynamiczne przydzielanie adresów (DHCP), normalizuje informacje dotyczące długości czasu alokacji (ang. *lease*) i czas przydzielony urządzeniom oraz informacje audytowe dotyczące długości czasu alokacji, gdy są one przypisane do urządzenia.

Dodatkowe wskazówki dla zabezpieczenia rozszerzającego: w odniesieniu do dynamicznej alokacji adresów urządzeń, klienci DHCP zwykle otrzymują długości czasu alokacji od serwerów DHCP.

IA-4 Zarządzanie identyfikatorami

Zabezpieczenie: jednostka organizacyjna zarządza identyfikatorami użytkowników i urządzeń w systemie teleinformatycznym. Identyfikatory są nadawane zgodnie z ustaloną przez jednostkę organizacyjną procedurą.

Dodatkowe wskazówki i wymagania:

Typowe identyfikatory urządzeń to adresy MAC, adresy IP, lub unikalne identyfikatory tokenowe. Zwykle identyfikatorem użytkownika jest nazwa konta związanego z użytkownikiem. W takim przypadku zarządzanie identyfikatorami jest ściśle związane z zarządzaniem kontami. IA-4 dotyczy również identyfikatorów użytkowników niekoniecznie związanych z kontem w systemie teleinformatycznym (np. identyfikatorów związanych z fizycznym dostępem do pomieszczeń bazy danych, czy innej aplikacji).

Zabezpieczenia rozszerzające:

- 1 Jednostka organizacyjna zabrania wykorzystywania identyfikatorów kont w systemie teleinformatycznym, jako identyfikatory publiczne konta poczty elektronicznej użytkownika (fragmentu adresu email).

¹⁰⁰ NIST dopuszcza, aby ta lista pozostała pusta w przypadku systemu teleinformatycznego o niskiej kategorii bezpieczeństwa, co NIE powinno mieć miejsca w przypadku sektora bankowego

Identyfikacja i uwierzytelnianie w usługach elektronicznych

Dodatkowe wskazówki dla zabezpieczenia rozszerzającego: jednostka organizacyjna wdraża to zabezpieczenie rozszerzające w takim stopniu, w jakim jest to możliwe i praktyczne w systemie teleinformatycznym.

- 2 Jednostka organizacyjna wymaga, aby rejestracja początkowa w celu otrzymania identyfikatora użytkownika i hasła, wymagała autoryzacji przełożonego i osobistej wizyty w Punkcie Rejestracji.
- 3 Jednostka organizacyjna dokonuje dokładnej weryfikacji tożsamości, wymagając przedstawienia w Punkcie Rejestracji: dokumentów tożsamości lub połączenia dokumentów i cech biometrycznych.
- 4 Jednostka organizacyjna zarządza identyfikatorami użytkownika poprzez unikalne identyfikowanie użytkownika, jako [przypisanie: zdefiniowana przez jednostkę organizacyjną charakterystyka określająca status użytkownika].

Dodatkowe wskazówki dla zabezpieczenia rozszerzającego: charakterystyka określająca status użytkownika może dotyczyć np. podwykonawstwa lub statusu obcokrajowca.

- 5 System teleinformatyczny dynamicznie zarządza identyfikatorami, atrybutami i powiązаныmi autoryzacjami dostępu.

Dodatkowe wskazówki dla zabezpieczenia rozszerzającego: w przeciwieństwie do tradycyjnej identyfikacji i uwierzytelnienia, które wykorzystują statyczne konta w systemach teleinformatycznych przypisane zarejestrowanym użytkownikom, wiele architektur zorientowanych na usługi opiera się na dynamicznym ustanawianiu tożsamości i przyporządkowywaniu atrybutów i uprawnień tym tożsamościom. Ważne jest w takim przypadku wstępne ustanowienie relacji i mechanizmów zaufania z podmiotami weryfikującymi tożsamości i uprawnienia.

IA-5 Zarządzanie danymi uwierzytelniającymi

Zabezpieczenie: jednostka organizacyjna zarządza danymi uwierzytelniającymi użytkowników i urządzeń poprzez:

- a) weryfikację tożsamości osoby lub urzędnika, podczas początkowej dystrybucji danych uwierzytelniających,
- b) ustanowienie początkowej zawartości danych uwierzytelniających,
- c) zapewnienie, że siła danych uwierzytelniających jest odpowiednia do ochrony zabezpieczanych informacji,
- d) ustanowienie i implementację procedury dystrybucji początkowych danych uwierzytelniających, dystrybucji po utracie/kompromitacji/zniszczeniu danych uwierzytelniających i unieważnieniu danych uwierzytelniających,
- e) zmianę początkowych (np. domyślnych) danych uwierzytelniających po instalacji systemu teleinformatycznego,
- f) ustanowienie minimalnego i maksymalnego czasu wymiany i warunków ponownego użycia danych uwierzytelniających (o ile ma to zastosowanie),
- g) zmianę/odświeżenie danych uwierzytelniających [przypisanie: co ustalony przez jednostkę organizacyjną okres zależny od rodzaju danych uwierzytelniających],

- h) zabezpieczenie zawartości danych uwierzytelniających przed nieautoryzowaną zmianą lub ujawnieniem, oraz
- i) wymaganie od użytkowników, aby pobrali i posiadali urządzenia implementujące lub specyficzne środki do ochrony danych uwierzytelniających.

Dodatkowe wskazówki i wymagania:

- Dane uwierzytelniające to np. hasła, tokeny, dane biometryczne, certyfikaty PKI, karty (nośniki) kluczy. Początkowa zawartość danych uwierzytelniających to zawartość stosowana przy pierwszym uwierzytelnieniu, np. hasło początkowe. Wiele komponentów systemów teleinformatycznych jest przesyłanych z domyślnymi danymi uwierzytelniającymi w celu umożliwienia początkowej instalacji i konfiguracji. Ustawienia domyślne są zwykle powszechnie dostępne i stanowią ryzyko dla bezpieczeństwa, więc są zmieniane podczas instalacji. Wymaganie zabezpieczenia danych uwierzytelniających użytkowników może być zaimplementowane poprzez zabezpieczenie PL-4¹⁰¹ lub PS-6 dla danych uwierzytelniających będących w posiadaniu użytkowników lub przez AC-3, AC-6 albo SC-28 dla danych uwierzytelniających w systemach teleinformatycznych (np. hasła przechowywane w postaci skrótu lub w postaci szyfrogramu, albo pliki zawierające skróty lub szyfrogramy haseł dostępne są jedynie dla użytkowników uprzywilejowanych). Systemy teleinformatyczne wspierają zarządzanie danymi uwierzytelniającymi użytkowników poprzez zdefiniowane przez jednostkę organizacyjną (administratora) ustawienia i ograniczenia dla różnych danych uwierzytelniających, łącznie np. z wymuszeniem minimalnej długości haseł, złożoności haseł, długości okna czasu walidacji dla tokenów jednorazowych synchronizowanych w czasie, procent dopuszczalnych błędów podczas weryfikacji w uwierzytelnieniu wykorzystującym metody biometryczne. Środki służące do zabezpieczenia danych uwierzytelniających obejmują np.: wymuszenie posiadania indywidualnych danych uwierzytelniających, nie pożyczanie i nie dzielenie danych uwierzytelniających z innymi osobami, natychmiastowe zgłaszanie utraty lub kompromitacji danych uwierzytelniających. Zarządzanie danymi uwierzytelniającymi obejmuje wystawianie, unieważnianie, gdy nie są dłużej potrzebne, tworzenie danych uwierzytelniających dla dostępu tymczasowego, takie jak np. do zdalnego utrzymania urządzeń. Dane uwierzytelniające urządzeń obejmują np. certyfikaty i hasła.
- System teleinformatyczny, dla uwierzytelnienia wykorzystującego hasła:
 - a) wymusza minimalną złożoność hasła [przypisanie: wymagania zdefiniowane przez jednostkę organizacyjną dla rozpoznawania wielkości liter, liczby znaków, zawartości małych liter, dużych liter, liczb, znaków specjalnych itp.],
 - b) szyfruje przechowywane i przesyłane hasła,
 - c) wymusza minimalny i maksymalny czas życia hasła [przypisanie: zdefiniowany przez jednostkę organizacyjną; „minimalny” - nie krótszy niż 2 tygodnie i „maksymalny” - nie dłuższy niż 180 dni],
 - d) zabrania ponownego użycia hasła przez [przypisanie: ustaloną przez jednostkę organizacyjną liczbę generacji kolejnych haseł].

To zabezpieczenie jest wymagane do stosowania w środowiskach, w których hasła są wykorzystywane jako pojedynczy czynnik uwierzytelnienia użytkowników lub – w podobny sposób – łącznie z jednym lub kilkoma dodatkowymi danymi uwierzytelniającymi. Wymaganie nie ma zastosowania do przypadku, w którym hasło jest wykorzystywane do odblokowania sprzętowych

¹⁰¹ zabezpieczenia z innych rodzin, do których jest odwołanie w treści IA umieszczono na końcu rozdziału w ppkt. 4.7.8

Identyfikacja i uwierzytelnianie w usługach elektronicznych

danych uwierzytelniających (tzw. PIN). Implementacja takich mechanizmów haseł (odblokowywanie sprzętowych tokenów) może nie spełniać wszystkich wymagań tego zabezpieczenia.

„Minimalny” dwutygodniowy czas życia hasła podyktowany jest zagrożeniem, iż w przypadku braku takiego parametru użytkownik będzie mógł obejść zabezpieczenie, o którym mowa w ppkt. d) poprzez kilkukrotną „pod rząd” zmianę haseł i ustawienie na koniec „starego”.

Zabezpieczenia rozszerzające:

1 System teleinformatyczny dla uwierzytelnienia wykorzystującego PKI:

- a) waliduje certyfikaty poprzez weryfikację ścieżki certyfikacji;
- b) wymusza autoryzację dostępu do klucza prywatnego, oraz
- c) odwzorowuje uwierzytelnianą tożsamość użytkownika na nazwę konta użytkownika.

Dodatkowe wskazówki dla zabezpieczenia rozszerzającego: walidacja statusu ścieżki certyfikacji wymaga weryfikacji listy unieważnionych certyfikatów lub bieżącego sprawdzenia statusu certyfikatu mechanizmem OCSP.

2 Jednostka organizacyjna wymaga, aby proces otrzymania [przypisanie: zdefiniowanych przez jednostkę organizacyjną rodzajów danych uwierzytelniających] był przeprowadzany osobiście w Punkcie Rejestracji i wymagał autoryzacji wskazanej osoby, np. przełożonego.

3 Jednostka organizacyjna wykorzystuje automatyczne narzędzia do określenia, czy dane uwierzytelniające są wystarczająco silne, by wytrzymać atak mający na celu ich kompromitację.

4 Jednostka organizacyjna wymaga od sprzedawców lub producentów komponentów systemów teleinformatycznych zmiany domyślnych ustawień danych uwierzytelniających na unikalne dane przed dostawą komponentu.

Dodatkowe wskazówki dla zabezpieczenia rozszerzającego: niniejsze zabezpieczenie rozszerzające zwiększa wymaganie zmiany przez jednostkę organizacyjną ustawień domyślnych danych uwierzytelniających przy instalacji systemu, na wymaganie, aby sprzedawca/producent komponentu systemu teleinformatycznego dostarczył unikalnych danych uwierzytelniających lub zmienił ustawienia domyślne dla komponentów przed dostarczeniem ich jednostce organizacyjnej. Unikalne dane uwierzytelniające są przypisywane przez sprzedawcę/producenta do specyficznych komponentów systemów teleinformatycznych (dostarczanych produktów) o różnych numerach seryjnych. To wymaganie jest zawierane w dokumentacji zakupu (np. w dokumentacji przetargowej) przygotowywanych przez jednostkę organizacyjną do celów zakupu systemu lub komponentów systemu.

5 Jednostka organizacyjna zabezpiecza dane uwierzytelniające proporcjonalnie do klasy i wrażliwości informacji, do których dostęp jest przez niezabezpieczony.

6 Jednostka organizacyjna zapewnia, że niezaszyfrowane statyczne dane uwierzytelniające nie są zaszyte w aplikacjach lub skryptach dostępu, lub dostępne pod klawiszami funkcyjnymi.

Dodatkowe wskazówki dla zabezpieczenia rozszerzającego: jednostka organizacyjna określa, czy zaszyte lub przechowywane dane uwierzytelniające są w postaci zaszyfrowanej, czy niezaszyfrowanej. Jeśli postać przechowywana jest taka sama jak postać wykorzystywana w procesie uwierzytelnienia, mamy do czynienia z danymi przechowywanymi w postaci niezaszyfrowanej. W takim przypadku nie ma znaczenia, czy przechowywane dane są zaszyfrowaną wersją czegoś innego, np. hasła.

Identyfikacja i uwierzytelnianie w usługach elektronicznych

- 7 Jednostka organizacyjna podejmuje [przypisanie: zdefiniowane przez jednostkę organizacyjną działania] mające na celu zarządzanie ryzykiem kompromitacji danych uwierzytelniających z powodu korzystania przez użytkowników z tych samych danych uwierzytelniających w wielu systemach teleinformatycznych.

Dodatkowe wskazówki dla zabezpieczenia rozszerzającego: gdy użytkownicy mają konta w wielu systemach teleinformatycznych, istnieje ryzyko, że użytkownik używa tego samego identyfikatora i danych uwierzytelniających do wielu kont i po kompromitacji jednego konta, pozostałe konta są również skompromitowane. Możliwe alternatywy to: (i) te same identyfikatory, a inne dane uwierzytelniające w różnych systemach, (ii) różne identyfikatory i dane uwierzytelniające w różnych systemach, (iii) zastosowanie mechanizmu SSO (single-sign-on) lub (iv) wykorzystywanie haseł jednorazowych we wszystkich systemach.

- 8 Jednostka organizacyjna ustala maksymalny czas wymiany danych uwierzytelniających użytkowników uprzywilejowanych krótszy niż dla danych uwierzytelniających użytkowników „zwykłych”.
- 9 Hasła do kont uprzywilejowanych muszą być przechowywane w depozycie w postaci zabezpieczonej (np. w zaklejonej kopercie). Procedura deponowania i pobierania z depozytu musi być udokumentowana.
- 10 Tokeny zawierające dane uwierzytelniające, podczas gdy nie są używane, muszą być przechowywane osobno od urządzenia, w którym są wykorzystywane.
- 11 BIOS (Basic Input/Output System) zabezpiecza się hasłem w celu ochrony dostępu do haseł systemowych.
- 12 Hasła (z wyjątkiem haseł jednorazowych) muszą być przechowywane w systemie w postaci skrótu (tj. przekształconej za pomocą kryptograficznej funkcji jednokierunkowej). Mechanizm przekształcenia powinien być zatwierdzony, najpóźniej na etapie wydawania aprobaty dla systemu.

IA-6 Maskowanie danych uwierzytelniających

Zabezpieczenie: system teleinformatyczny maskuje informacje uwierzytelniające w trakcie procesu uwierzytelniania, aby zapobiec wykorzystaniu ich przez nieautoryzowane osoby.

Dodatkowe wskazówki i wymagania:

System teleinformatyczny nie może dostarczać informacji, które umożliwiłyby kompromitację mechanizmu uwierzytelniającego przez osobę nieupoważnioną. Wyświetlanie gwiazdek przy wprowadzaniu hasła jest przykładem mechanizmu maskującego.

Zabezpieczenia rozszerzające:

- 1 W procesie uwierzytelniania system TI powinien przekazywać użytkownikowi jedynie niezbędne informacje.

Dodatkowe wskazówki dla zabezpieczenia rozszerzającego: system TI powinien zapobiegać uzyskiwaniu przez użytkownika dodatkowych informacji w procesie uwierzytelniania. System nie powinien wyświetlać podpowiedzi, ani ujawniać nazw kont dostępnych w systemie.

IA-7 Uwierzytelnienie modułów kryptograficznych

Zabezpieczenie: system teleinformatyczny stosuje mechanizmy uwierzytelnienia do modułów kryptograficznych, spełniające wymagania prawne, normy i zalecenia dot. uwierzytelnienia.

Dodatkowe wskazówki i wymagania:

Sprzętowe urządzenia szyfrowe wymagają – jako minimum – specjalnego uwierzytelnienia w przypadku realizacji funkcji administracyjnych i/lub audytowych (tzw. *inspektor bezpieczeństwa*). Uwierzytelnienie użytkownika może być niezbędne, ale jego ewentualne stosowanie wynika ze specyfiki danego szyfratora. Np. karty kryptograficzne realizujące kwalifikowane podpisy elektroniczne muszą zostać odblokowane przy pomocy PIN-u w celu wykonania podpisu, przy czym należy zaznaczyć, że to odblokowanie może być tylko na jeden podpis lub na wiele podpisów, ale w takim przypadku aplikacja wyraźnie sygnalizuje użytkownikowi, iż odblokowanie będzie na określoną ilość podpisów i/lub na określony czas (np. do godz. 15:30 danego dnia).

IA-8 Identyfikacja i uwierzytelnienie użytkowników spoza jednostki organizacyjnej

Zabezpieczenie: system teleinformatyczny identyfikuje i uwierzytelnia wszystkich użytkowników spoza jednostki organizacyjnej z osobna (lub procesy działające na żądanie użytkowników spoza jednostki organizacyjnej).

Dodatkowe wskazówki i wymagania:

Użytkownicy spoza jednostki organizacyjnej to wszyscy użytkownicy z wyjątkiem jawnie wymienionych w IA-2. Użytkownicy ci są jednoznacznie identyfikowani i uwierzytelniani przy dostępie w systemie innym niż wymieniony w AC 14. Do określenia potrzeb jednostki organizacyjnej w zakresie uwierzytelnienia w systemie TI wykorzystywana jest analiza ryzyka. Przy wyborze rozwiązań brane są pod uwagę elastyczność, praktyczność i bezpieczeństwo, tak, aby osiągnąć kompromis między łatwością użytkowania systemów, a potrzebą zabezpieczenia systemu. Identyfikację i uwierzytelnienie w systemach teleinformatycznych dla pracowników jednostki organizacyjnej opisano w IA-2.

Wymagania innych rodzin

Wymagania, do których odwołuje się IA, a opisane w innych rodzinach dokumentu NIST SP 800-53:

- AC – Kontrola dostępu (ang. *Access Control*)
- PL – Planowanie (ang. *Planning*)
- PS – Bezpieczeństwo osobowe (ang. *Personnel Security*)
- SC - Ochrona systemu i łączności (ang. *System and Communications Protection*)

AC-3 Wymuszenie kontroli dostępu do zasobów

Zabezpieczenie: w systemie TI, poza mechanizmem uwierzytelnienia do konta, stosuje się dodatkowe mechanizmy kontroli dostępu do pewnych zasobów, np. listy kontroli dostępu w urządzeniach sieciowych, kontrola dostępu do zarządzania urządzeniami szyfrowymi. Dostęp do zasobów wymaga uprzedniego uwierzytelnienia się w ramach dostępu do odpowiednich kont użytkowników, w szczególności:

- a) określa się rodzaje dopuszczalnych kont (np. indywidualne, grupowe, systemowe, aplikacyjne, tymczasowe),
- b) dla poszczególnych rodzajów kont ustanawia się warunki, których spełnienie pozwala na umożliwienie dostępu użytkownika do danego konta,
- c) prowadzi się rejestr uprawnionych użytkowników z informacjami o posiadanych uprawnieniach,

Identyfikacja i uwierzytelnianie w usługach elektronicznych

- d) odpowiedni administrator tworzy konto, ustanawia dostęp do konta, modyfikuje uprawnienia lub usuwa konto, dopiero po uzyskaniu stosownej decyzji uprawnionej osoby,
- e) dokonuje się przeglądu kont tymczasowych nie rzadziej niż raz na 2 tygodnie, a pozostałych kont nie rzadziej niż raz na kwartał,
- f) upoważnione osoby wydają niezwłocznie stosowne polecenia aktywacji/dezaktywacji kont i uprawnień zgodnie z zasadą wiedzy uzasadnionej (ang. *need to know*) oraz zasadą współdzielenia wiedzy (ang. *need to share*).

Dodatkowe wskazówki i wymagania:

Dodatkowe uwierzytelnienie na poziomie aplikacji jest przykładem tego zabezpieczenia, jednakże należy zauważyć, że nie jest ono bezwzględnie wymagane dla każdej aplikacji.

Zabezpieczenia rozszerzające:

- 1 W systemie TI wymaga się podwójnej zgody na przyznanie uprawnień (np. Dyrektora pionu IT i Dyrektora komórki realizującej audyt wewnętrzny).
- 2 W systemie TI stosuje się obligatoryjny system kontroli dostępu (ang. *Mandatory Access Control – MAC*), który polega na tym, że każdy zasób informacyjny systemu (plik, rekord, itp.) zawiera w metadanych informację o rodzaju i klauzuli dostępu (np. ogólnodostępne, tylko dla zarządu, tylko dla bankowości korporacyjnej) i istnieje automatyczny mechanizm udzielania (lub blokowania) dostępu do zasobu dla osób, które posiadają (lub nie posiadają) formalnego upoważnienia.
- 3 W systemie TI blokowany jest dostęp do zasobów lub pewnych funkcji do momentu wprowadzenia tego systemu lub jego części (np. urzędzenia szyfrowego) do bezpiecznego stanu, zwykle związanego z wyłączeniem z normalnej eksploatacji.
- 4 W jednostce organizacyjnej przechowuje się w bezpiecznej lokalizacji (off-line) chronione informacje na oddzielnych nośnikach i w postaci zaszyfrowanej, co redukuje ryzyko nieuprawnionego dostępu do danych i ryzyko nieuprawnionej modyfikacji. Uwaga: tryb szyfrowania musi wspierać integralność, np. CBC (ang. *Cipher Block Chaining – CBC*), w szczególności nie może to być tryb ECB (ang. *Electronic Code Book – ECB*).

AC-6 Minimum uprawnień

Zabezpieczenie: w systemie TI nadaje się uprawnienia zgodnie z zasadą „niezbędności”, czyli tylko w takim zakresie, jaki jest wymagany dla danego użytkownika (w tym administratora/inspektora) w ramach jego zadań służbowych.

Dodatkowe wskazówki i wymagania:

- Należy pamiętać, że poza zasadą „wiedzy uzasadnionej” (ang. *need-to-know*) występuje nie mniej ważna zasada „współdzielenia wiedzy” (ang. *need-to-share*).
- W systemie TI dostęp do niektórych funkcji zarządzających i informacji związanych z zabezpieczeniami jest ograniczony do specjalnie autoryzowanego kręgu osób. Odnosi się to w szczególności do takich zadań jak: ustanawianie kont, przydzielanie uprawnień do konta, ustawianie listy zdarzeń podlegających audytowi, konfigurowanie sond IDS/IPS.

Zabezpieczenia rozszerzające:

- 1 W systemie TI uprawnieni administratorzy/inspektorzy mający dostęp do niektórych funkcji zarządzających/kontrolnych i informacji związanych z zabezpieczeniami, używają swoich uprzywilejowanych kont tylko dla zadań związanych z zarządzaniem/kontrolowaniem. W przypadku innych zadań stosują oddzielne konta, „nieuprzywilejowane” (niepozwalające na zarządzanie/kontrolowanie).
- 2 W systemie TI monitoruje się przypadki używania kont „uprzywilejowanych”, o których mowa w rozszerzeniu 1, do realizacji innych funkcji, niezwiązanych z zarządzaniem/kontrolowaniem.
- 3 W systemie TI dostęp do sieci wymaga uwierzytelnienia urządzenia. Przykładem tego rozwiązania jest system typu NAC (ang. *Network Access Control*), w którym udzielenie dostępu do sieci jest poprzedzone uwierzytelnieniem i weryfikacją m.in. aktualności tzw. poprawek (ang. *patches*). Rozwiązanie z serwerem DHCP (ang. *Dynamic Host Configuration Protocol*), który automatycznie przyznaje adres IP dowolnemu urządzeniu włączanemu do sieci jest przykładem implementacji, która NIE spełnia tego rozszerzenia.

AC-14 Dozwolone działania bez identyfikacji i autoryzacji

Zabezpieczenie: w pewnych sytuacjach może być dopuszczalne wykonywanie ściśle określonych działań bez uprzedniego uwierzytelnienia i autoryzacji, aczkolwiek zgoda na takie działania wcale nie musi być w ogóle wydana. Zwykle taka funkcjonalność (działanie bez identyfikacji i autoryzacji) jest związane z publiczną stroną www, przy pomocy której można np. wysłać anonimowo wiadomość do danej jednostki organizacyjnej.

Dodatkowe wskazówki i wymagania:

Nie istnieje obowiązek podłączania publicznej strony www (oczywiście za pośrednictwem dodatkowych mechanizmów separujących, programowych i sprzętowych) do systemu IT. Dla uzyskiwania informacji od anonimowych osób poprzez publiczną stronę www (lub udostępniania informacji publicznej poprzez taką stronę) rekomenduje się rozwiązanie polegające na wdrożeniu innego systemu teleinformatycznego, niepodłączonego w żaden sposób do systemu przetwarzającego informacje wrażliwe (separacja fizyczna).

PL-4 Zasady pracy w systemie

Zabezpieczenie: jednostka organizacyjna:

- a) ustanawia i komunikuje wszystkim użytkownikom systemu zasady pracy w systemie, które opisują odpowiedzialność użytkowników za informacje i sposób postępowania z informacjami w systemie teleinformatycznym,
- b) wymaga podpisania oświadczenia o zapoznaniu się, zrozumieniu i zobowiązaniu do stosowania zasad pracy w systemie TI. Użytkownicy składają oświadczenia przed dopuszczeniem do użytkowania informacji i systemu teleinformatycznego.

Dodatkowe wskazówki i wymagania:

Jednostka organizacyjna stosuje różne zasady pracy w sieci, w zależności od roli użytkownika w systemie teleinformatycznym (np. różne procedury dla administratorów, użytkowników zaawansowanych i zwykłych użytkowników systemu).

Zabezpieczenia rozszerzające:

- 1 Jednostka organizacyjna określa kary dyscyplinarne za nieprzestrzeganie zasad pracy w systemie. Jednostka organizacyjna informuje użytkowników systemu o karach.

PS-6 Umowy o dostępie

Zabezpieczenie: jednostka organizacyjna:

- a) zapewnia, że osoby spoza jednostki wymagające dostępu do informacji i systemów TI organizacji podpisują stosowne umowy/porozumienia w sprawie dostępu, zanim taki dostęp zostanie im zapewniony,
- b) przegląda i uaktualnia porozumienia w sprawie dostępu [przypisanie: z częstością definiowaną przez organizację; nie rzadziej niż raz do roku].

Dodatkowe wskazówki i wymagania:

Umowy/porozumienia w sprawie dostępu zawierają przykładowo uzgodnienia w sprawie nieujawniania informacji, zakresu ich wykorzystania oraz zasady postępowania w przypadku konfliktu interesów. Podpisanie umowy/porozumienia w sprawie dostępu oznacza potwierdzenie, że osoby, których ono dotyczy przeczytały, zrozumiały oraz wyraziły zgodę na postępowanie zgodne z uregulowaniami obowiązującymi w systemie TI, do którego otrzymały uprawnienia dostępu. W tym względzie akceptowalny jest podpis elektroniczny chyba, że jest wykluczony przez politykę bezpieczeństwa obowiązującą w instytucji.

SC-28 Zabezpieczenie przechowywanych informacji

Zabezpieczenie: system teleinformatyczny chroni poufność i integralność przechowywanych informacji.

Dodatkowe wskazówki i wymagania:

Celem tego zabezpieczenia jest uwzględnienie poufności i integralności informacji przechowywanych w stacjonarnych urządzeniach i obejmuje informacje użytkowników oraz informacje systemowe. Informacje „w stanie spoczynku” to informacje w urządzeniu w pamięci masowej (napęd dyskowy, napęd taśmowy) wchodzącego w skład systemu TI jednostki organizacyjnej. Zwraca się uwagę, że konfiguracje i zbiory reguł zapór sieciowych, bram, systemów wykrywania/zapobiegania włamaniom oraz routerów filtrujących i dane służące do

uwierzytelnienia, to również przykłady informacji systemowych wymagających ochrony, zwykle ograniczonej do zachowania integralności (w niektórych przypadkach również poufności). Jednostki organizacyjne mogą zdecydować o wykorzystaniu różnych mechanizmów dla uzyskania poufności i integralności, według swoich potrzeb.

Zabezpieczenia rozszerzające:

- 1 Jednostka organizacyjna wykorzystuje mechanizmy kryptograficzne do zapobiegania nieautoryzowanemu ujawnieniu i modyfikacji przechowywanych informacji, o ile nie są one chronione przez zabezpieczenia fizyczne.

RECENZJE

Tematyka identyfikacji uwierzytelnienia i autoryzacji jest jednym z kluczowych obszarów bezpieczeństwa transakcji elektronicznych. Niestety, wiedza dotycząca wymienionych tematów jest zazwyczaj opisywana w pojedynczych publikacjach, które ze względu na techniczny charakter mogą być trudne do przyswojenia dla osób niezaznajomionych z tematyką. Raport "Identyfikacja i uwierzytelnianie w usługach elektronicznych" jest publikacją, która umożliwia czytelnikowi na stopniowe zagłębienie się w przedmiotową tematykę. Ze względu na ten fakt, Raport może być traktowany zarówno jako źródło podstawowej wiedzy o uwierzytelnieniu i identyfikacji, jak również jako baza do bardziej wnikliwych studiów. Podział publikacji na fragmenty, mogące zainteresować osoby o różnym charakterze zawodowym (prawnicy, osoby techniczne). Takie podejście pozwala na studiowanie specyficznych aspektów identyfikacji i uwierzytelnienia, bez zbędnego zagłębiania się w detale nieistotne z punktu widzenia danej grupy zawodowej. Mimo wszystko warto jednak przeczytać całość, tak aby uzyskać bardziej ogólny obraz tematu, w którym prawo spotyka technologię.

Osoby, które szukają informacji na temat projektów UE związanych z identyfikacją i uwierzytelnieniem, znajdą w Raporcie źródło zsyntetyzowanej wiedzy wraz z odnośnikami, umożliwiającymi pogłębienie tematu.

Można mieć tylko nadzieję na to, że w kontekście dynamicznych zmian zachodzących w ostatnich latach pojawią się kolejne wersje raportu.

Daniel Wachnik
Specjalista ds. Podpisu Elektronicznego w Laboratorium Podpisu Elektronicznego IMM

Identyfikacja i uwierzytelnianie w usługach elektronicznych

Przewodnik „Identyfikacja i uwierzytelnianie w usługach elektronicznych” to całościowe i wielopłaszczyznowe opracowanie obejmujące tematykę zarządzania elektroniczną tożsamością w zastosowaniu do usług świadczonych elektronicznie. W monografii tej można znaleźć szczegółowo udokumentowany przegląd definicji, standardów oraz norm wraz z omówieniem ich historycznej genezy. Wartością dodatkową jest to, że są one w wielu przypadkach omówione w odniesieniu do projektów na bazie których były inicjowane i są dalej rozwijane. Przekrój analizy obejmuje zarówno perspektywę rozwiązań krajowych, europejskich i międzynarodowych.

Z równą kompetencją przedstawione są rozwiązania techniczne wraz z pełną dokumentacją i referencjami do materiałów źródłowych oraz strona procesowa i prawna identyfikacji i uwierzytelniania. W opracowaniu omówiona jest szeroko rozumiana tematyka ochrony danych osobowych wraz z analizą wymagań, ryzyk i zagrożeń. Przegląd obowiązujących wymagań prawnych przedstawiony jest wraz ze wskazaniem obszarów w których prawna ochrona danych osobowych będzie miała coraz większe znaczenie. Szczególnie zagrożenia utraty społecznego zaufania do systemów uwierzytelniania i przetwarzania danych osobowych dostrzegane jest w kontekście rosnącego znaczenia chmur obliczeniowych, przetwarzania danych biometrycznych i zagrożeń wynikających z przestępstw przeciw tożsamości.

Wartością opracowania jest przedstawienie konkretnych studium przypadków wdrożonych interoperacyjnych systemów uwierzytelniania w wybranych krajach europejskich. Ważne są również przykłady projektów, które nie przyniosły oczekiwanych wyników oraz przedstawione okoliczności przyczyn niepowodzeń.

Kompendium zabrane w przewodniku będzie bardzo cennym źródłem wiedzy dla specjalistów zaangażowanych w poszczególnych dziedzinach rozwoju usług elektronicznej gospodarki i administracji, także dla studentów i kadr akademickich. Powinno być również dobrym punktem odniesienia do otwartej dyskusji wszystkich uczestników rynku w tej skomplikowanej i wielowątkowej materii.

Pewien niedosyt, który może być łatwo uzupełniony, powstaje z tytułu braku podsumowania stanu bieżącego odnośnie funkcjonujących systemów uwierzytelniania w Polsce. Niewątpliwie ważne byłoby uświadomienie tego w jakim punkcie rozwoju systemów identyfikacji i uwierzytelniania teraz jesteśmy, i jakie najważniejszy krytyczne kroki są przed nami, zarówno w perspektywie krajowej, jak i europejskiej.

Antoni Hanusik
Członek Prezydium Rady Bankowości Elektronicznej ZBP