Jeden login do systemów administracji publicznej

Rozwój technologii pozwala na identyfikowanie się w różnych systemach i usługach na podstawie smartfona, natomiast zmiany prawne pozwalają na wykorzystanie tej samej identyfikacji elektronicznej zarówno w usługach administracji publicznej, jak i komercyjnych.

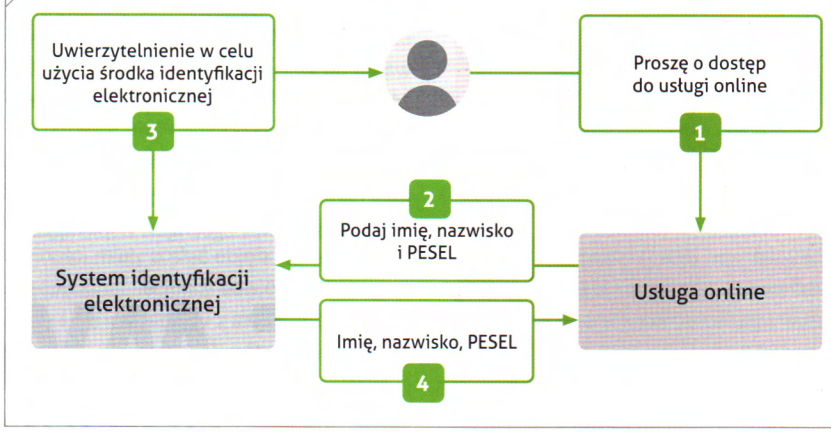
Michał Tabor

Wykorzystanie usług elektronicznych w realizacji zobowiązań podmiotów publicznych wymaga umożliwienia bezpiecznego i pewnego kontaktu, który nawiązuje klient tych usług. Zapewnienie bezpieczeństwa obejmuje potwierdzenie tożsamości klienta usług online oraz zabezpieczenie tworzonych dokumentów i składanych oświadczeń, w szczególności dokumentów i pism. Do zagwarantowania bezpieczeństwa dokumentów służą podpisy i pieczęcie elektroniczne, a także inne usługi zaufania, które nie będą omawiane w niniejszym artykule. Z kolei potwierdzenie tożsamości użytkownika i przekazanie do usługi jego danych osobowych jest wynikiem działania identyfikacji elektronicznej.

Raz a dobrze

Problem autoryzowanego dostępu osób uprawnionych do usług online nie jest nowy i praktycznie występuje we wszystkich systemach teleinformatycznych zarówno komercyjnych, jak i podmiotów publicznych. Założeniem bezpieczeństwa usług udostępnianych przez internet jest udostępnienie zasobów informacyjnych i usług oferowanych przez dany system tylko dla osób uprawnionych, w sposób zapewniający poufność komunikacji. Przez wiele lat każdy system teleinformatyczny rozwijał swoje mechanizmy uwierzytelniania, najczęściej bazujące na loginach i hasłach. Jednakże zarządzanie loginami i hasłami do wielu systemów nie jest zadaniem trywialnym dla użytkownika, co w efekcie kończy się albo posługiwaniem się jednym hasłem do wielu systemów teleinformatycznych, albo zapisywaniem haseł przez użytkowników na karteczkach przylepianych do komputera. Dodatkowo opieranie bezpieczeństwa danych w systemach teleinformatycznych tylko na hasłach rodzi niebezpieczeństwo utraty tych haseł – jeśli zostaną wykradzione, dostęp do systemu zostanie przejęty przez nieuprawnione

Jak działa identyfikacja elektroniczna



Uwierzytelnianie w usługach cyfrowych

osoby. Z problemem bezpiecznego dostępu do usług publicznych mierzono się już ponad 10 lat temu poprzez utworzenie profilu zaufanego (dalej: pz). Jego celem było udostępnienie pojedynczego mechanizmu identyfikacji elektronicznej, z którego mogą korzystać wszystkie systemy administracji publicznej.

Profil zaufany ze względu na dużą różnorodność systemów administracji publicznej był wykorzystywany głównie do składania podpisu elektronicznego potwierdzonego pz, który miał za zadanie zapewnić połączenie tożsamości z dokumentem i dzięki temu w jednolity sposób dostarczać potwierdzenia w usługach publicznych. Rozwój pz jako systemu tworzonego i wykorzystywanego wyłącznie przez samą administrację nie pozwalał na znaczny wzrost użytkowników rozwiązania, ponieważ dołączenie do systemu użytkownika wymagało, aby udał się on do punktu potwierdzającego pz. Takie podejście przy ograniczonym zakresie użycia pz tylko do spraw administracji publicznej czyniło rozwiązanie użytecznym tylko dla osób często korzystających z tego typu usług. Zmianę przyniosło dopiero włączenie możliwości potwierdzania pz dla użytkowników bankowości elektronicznej, które stanowiło podstawę wypracowania krajowego schematu identyfikacji elektronicznej.

Schemat (nie tylko) krajowy

Krajowy schemat identyfikacji elektronicznej został wprowadzony ustawą z dnia 5 września 2016 r. o usługach zaufania oraz identyfikacji elektronicznej (tekst jedn. DzU z 2020 r., poz. 1173), a jego celem jest umożliwienie wykorzystania różnego rodzaju rozwiązań zdalnego potwierdzania tożsamości w systemach administracji publicznej. Krajowy schemat zakłada, że dostawcami tożsamości mogą być zarówno podmioty publiczne, jak i prywatne, przy czym te drugie muszą spełnić szereg wymagań, aby móc świadczyć taką funkcjonalność. Dzięki temu jeżeli mamy konto w banku, który sprawdził naszą tożsamość w momencie otwierania konta, możemy ten fakt wykorzystać do późniejszego uwierzytelnienia w usługach online – i tych publicznych, i prywatnych.

Podstawą prawną dla stosowania usług identyfikacji elektronicznej w usługach online jest rozporządzenie eIDAS (DzUrz UE L 257 z 28.08.2014), które zdefiniowało, czym jest identyfikacja elektroniczna, uwierzytelnianie oraz środki identyfikacji elektronicznej. Definicje te obowiązują jednolicie w całej Unii Europejskiej. Rozporządzenie dodatkowo ustaliło poziomy wiarygodności dla usług identyfikacji elektronicznej oraz wskazało, w jaki sposób z tej wiarygodności można korzystać pomiędzy krajami UE. Dodatkowo regulacja dała podstawy do ustanowienia usług identyfikacji elektronicznej, które są stosowane zarówno przez podmioty publiczne, jak i usługi komercyjne, przy czym model dostarczania tych usług został powierzony państwom członkowskim, które mają dowolność w zbudowaniu tylko państwowych usług lub kooperacji w tym zakresie z rynkiem prywatnym – co właśnie miało miejsce w Polsce.

Środek dla tożsamości

Rozporządzenie eIDAS definiuje identyfikację elektroniczną jako proces, który używa unikalnych danych osobowych identyfikowanych w celu jego uwierzytelnienia w usługach online. W tym procesie mają zastosowanie środki identyfikacji elektronicznej zawierające unikalne dane osobowe identyfikowanego, a ich aktywacja odbywa się w taki sposób, że z dużą dozą pewności tylko osoba identyfikowana →

Z e-tożsamością po UE

Notyfikacja środków identyfikacji elektronicznej ma umożliwić korzystanie z własnych środków identyfikacji w kontaktach w całej Unii Europejskiej. Każde państwo członkowskie UE może notyfikować wybrane przez siebie środki identyfikacji na poziomie paneuropejskim, dzięki czemu użytkownicy notyfikowanych systemów logują się w oparciu o własne mechanizmy w usługach publicznych w innych krajach UE. Podmioty publiczne są zobowiązane do uznawania notyfikowanych przez inne kraje środków identyfikacji elektronicznej, co w Polsce ma być gwarantowane przez integrację węzła krajowego z węzłem transgranicznym. Kraj członkowski, realizując notyfikację, określa poziom wiarygodności środka, który będzie notyfikował. Wiele krajów już notyfikowało swoje środki identyfikacji elektronicznej, natomiast Polska nie rozpoczęła jeszcze tego procesu ani dla profilu zaufanego, ani dla profilu osobistego.

posługuje się danym środkiem identyfikacji elektronicznej. Wspólną cechą danych identyfikujących osobę zawartych w środku identyfikacji elektronicznej jest możliwość ustalenia tożsamości identyfikowanej osoby – czyli na końcu jednoznacznego wskazania, kto to jest. Warto w tym miejscu podkreślić, że zgodnie z rozporządzeniem eIDAS identyfikowaną osobą może być zarówno osoba fizyczna, jak i osoba prawna. Wspomniana identyfikacja osób prawnych będzie miała szczególne znaczenie przy rozwoju usług, w których to systemy informatyczne będą się identyfikowały w usługach w imieniu firm, np. w celu odbioru korespondencji w ramach rejestrowanego elektronicznego doręczenia.

Środki identyfikacji elektronicznej mogą mieć różną postać, w szczególności mogą to być materialne lub niematerialne rozwiązania zawierające dane identyfikujące osobę oraz umożliwiające uwierzytelnienie się online. Przykładem materialnego środka identyfikacji elektronicznej jest nowy elektroniczny dowód osobisty zawierający dane służące do identyfikacji elektronicznej określane jako profil osobisty. Użycie dowodu osobistego w celu identyfikacji elektronicznej wymaga jego umieszczenia na czytniku bezstykowym i podania kodu dostępowego wydrukowanego na samym blankiecie – tzw. kodu CAN. Gdy karta dowodu połączy się z systemem komputerowym, system zażąda podania PIN-u, w wyniku czego karta uwolni dla konkretnego żądania identyfikacji jednorazowe dane uwierzytelniające. Dane te są tworzone za pomocą technik kryptograficznych i umieszczonego w procesorze dowodu osobistego klucza prywatnego. Prawidłowe potwierdzenie danych będzie mogło zostać zweryfikowane na podstawie certyfikatu identyfikacji i uwierzytelniania, który zawiera imię, nazwisko oraz PESEL. Ważność tego certyfikatu może zostać zweryfikowana tak samo jak ważność certyfikatu podpisu elektronicznego. Rolę czytnika może też pełnić telefon komórkowy wraz z aplikacją do identyfikacji elektronicznej. Udostępniona przez Polską Wytwórnię Papierów Wartościowych aplikacja eDO App umożliwia w bardzo łatwy sposób posłużenie się profilem osobistym w usługach online.

Innym środkiem identyfikacji elektronicznej jest pz – przechowywany jako dane w systemie ministra ds. informatyzacji, czyli w systemie profilu zaufanego. Uwolnienie danych pz w celu uwierzytelnienia online w systemach publicznych wymaga najpierw zalogowania się identyfikowanej osoby do samego systemu pz za pomocą loginu, hasła, SMS-a lub zewnętrznego systemu oferującego uwierzytelnienie (systemy bankowe). Uwolnione dane identyfikujące, czyli imię, nazwisko, PESEL, są przekazywane do usługi online.

Procesy identyfikacji elektronicznej

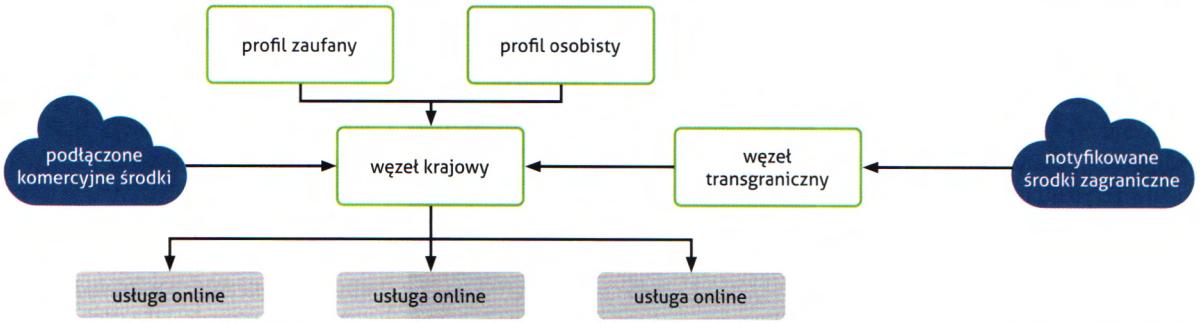
Aby umożliwić funkcjonowanie wielu systemów identyfikacji elektronicznej na potrzeby pojedynczej usługi online, utworzono instytucję węzła identyfikacji, który umożliwia wybór systemu i środka identyfikacji elektronicznej, w posiadaniu którego jest użytkownik. Węzły identyfikacji elektronicznej są budowane zarówno dla usług komercyjnych, jak i publicznych, a także na potrzeby usług transgranicznych. Systemy identyfikacji elektronicznej budowane zgodnie z rozporządzeniem eIDAS oparte są na trzech podstawowych procesach: 1) procesie rejestracji w celu utworzenia środka identyfikacji elektronicznej; 2) procesie zarządzania środkiem identyfikacji elektronicznej oraz 3) procesie użycia środka identyfikacji elektronicznej w celu uwierzytelnienia w usługach online. Sposób realizacji każdego z tych procesów może być inny w zależności od systemu identyfikacji elektronicznej oraz środka identyfikacji elektronicznej. Rozporządzenie wykonawcze Komisji (UE) 2015/1502 z dnia 8 września 2015 r. (DzUrz UE L 235 z 9.09.2015) w sprawie poziomów zaufania środków identyfikacji zdefiniowało dokładne wymagania wymienionych wyżej procesów dla określenia poziomu wiarygodności środka

Komercyjne środki identyfikacji

Podobnie jak profil zaufany jest utrzymywany w ramach systemu identyfikacji elektronicznej, w ten sam sposób usługi komercyjne mogą tworzyć własne systemy i środki identyfikacji elektronicznej. W szczególności dane o naszej tożsamości przechowywane w systemach bankowych są środkami identyfikacji elektronicznej, a ich użycie może pozwalać na uwierzytelnianie w innych systemach. Przyjęty w Polsce model funkcjonowania identyfikacji elektronicznej zakłada równoległe funkcjonowanie państwowych i komercyjnych środków identyfikacji elektronicznej, przy czym administracja publiczna może korzystać z komercyjnych środków identyfikacji nieodpłatnie. Profil osobisty umieszczony w dowodzie osobistym może być używany w systemach administracji publicznej, natomiast profil zaufany może być wykorzystywany tylko przez podmioty publiczne na potrzeby świadczonych przez siebie usług.

Równolegle do wykorzystania profilu zaufanego oraz profilu osobistego realizowany jest rozwój komercyjnych środków identyfikacji, które mogą być wykorzystywane nie tylko na potrzeby publiczne, ale także w usługach konsumenckich, bankowych, a także usługach zaufania. Swoje środki identyfikacji pierwsze udostępniły banki. W ramach rozwoju tego typu usług została zbudowana usługa węzła identyfikacji elektronicznej „Moje ID" oferowana przez Krajową Izbę Rachunkową. Oferuje ona środki identyfikacji głównie na potrzeby usług finansowych oraz medycznych. Niezależnie od tej usługi powstają nowe rozwiązania identyfikacji elektronicznej, np. oferowane przez Blue Media lub Autenti, które oparte są nie tylko na tożsamości pochodzącej z banków, ale także na innych usługach identyfikacji elektronicznej. Dodatkowo na rynku komercyjnym dostępnych jest kilka rozwiązań identyfikacji elektronicznej bazujących na weryfikacji dowodu osobistego realizowanej automatycznie na podstawie tzw. selfie. W przypadku tych usług procesy rejestracji, utworzenia środka identyfikacji i uwierzytelniania odbywają się jednocześnie.

Krajowy schemat identyfikacji elektronicznej



Ustawa o usługach zaufania oraz identyfikacji elektronicznej wprowadziła krajowy schemat identyfikacji elektronicznej, który obejmuje wszystkie systemy identyfikacji elektronicznej obsługiwane przez węzeł krajowy identyfikacji elektronicznej, węzeł transgraniczny oraz systemy publiczne korzystające z identyfikacji elektronicznej. W ramach krajowego schematu wszystkie podmioty publiczne mają mieć możliwość podłączenia do wielu systemów identyfikacji elektronicznej – zarówno krajowych, jak i notyfikowanych systemów zagranicznych. Dzięki takiemu podejściu użytkownik usług online administracji publicznej ma możliwość wybrania tych środków, które użytkuje i pozwalają mu na łatwą i bezpieczną identyfikację w usługach. Do krajowego schematu jako systemy identyfikacji podłączone są aktualnie (w momencie pisania niniejszego artykułu) profil zaufany, profil osobisty oraz jeden bank. W ramach krajowego schematu środki identyfikacji udostępniane są bezpłatnie na potrzeby usług publicznych. Krajowy schemat nie umożliwia udostępnienia usługi na potrzeby podmiotów niepublicznych, natomiast podłączone komercyjne środki identyfikacji elektronicznej mogą być używane w usługach publicznych, jak w ramach krajowego schematu, i w usługach niepublicznych. Wizytówką krajowego schematu identyfikacji elektronicznej jest strona **login.gov.pl**.

identyfikacji elektronicznej. Poziom wiarygodności wskazuje, czy środek może być używany w danym typie usługi online, czy też gwarancje związane z użyciem tego rozwiązania są niewystarczające dla zapewnienia bezpieczeństwa.

Rejestracja w systemie identyfikacji elektronicznej umożliwia utworzenie środka identyfikacji elektronicznej. Jej zadaniem jest potwierdzenie na wstępie tożsamości identyfikowanej osoby, tak aby utworzyć wiarygodną cyfrową reprezentację jej tożsamości. Rejestracja może odbywać się bezpośrednio, np. w punkcie rejestracji na podstawie weryfikacji fizycznego dokumentu tożsamości, na podstawie wideosesji lub poprzez weryfikację informacji o tożsamości pochodzących z wielu źródeł. O jakości procesu rejestracji decyduje to, czy podczas jego przebiegu tożsamość jest weryfikowana w systemach źródłowych, sprawdzane są bazy zastrzeżeń dokumentów oraz czy personel realizujący ten proces jest regularnie szkolony w zakresie wykrywania fałszerstw. Przyjmuje się, że proces wydania dokumentu tożsamości jest referencyjnym modelem bezpieczeństwa procesu rejestracji. Ma to szczególne znaczenie, gdy większość procesów rejestracji jest właśnie oparta na wiarygodnym dokumencie tożsamości. Udany proces rejestracji kończy się utworzeniem środka identyfikacji (np. wydaniem karty, utworzeniem konta użytkownika) oraz wydaniem środka uwierzytelniającego.

Zarządzanie środkiem identyfikacji elektronicznej to w szczególności procesy organizacyjne podmiotu odpowiedzialnego za system identyfikacji elektronicznej. Składają się na nie wdrożony system bezpieczeństwa informacji, np. zgodny z normą ISO 27001, bezpieczna realizacja usług zarządzających ważnością środka identyfikacji, w tym zgłoszenie jego utraty, oraz usługa zmiany PIN-u do karty. Proces ten pozwala na to, aby wszystkie działania związane z bezpieczeństwem środka identyfikacji elektronicznej zostały zrealizowane z należytą starannością oraz gwarantowały poufność danych osobowych i oczekiwaną dostępność systemu teleinformatycznego obsługującego środek identyfikacji elektronicznej. Jakość zarządzania systemem identyfikacji elektronicznej wpływa na jakość pozostałych procesów, tj. rejestracji i uwierzytelniania, a głównie na wiarygodność instytucjonalną operatora systemu identyfikacji.

Poziomy wiarygodności

Uwierzytelnianie jest procesem polegającym na użyciu środka identyfikacji elektronicznej na potrzeby dostępu do usług online. Może być realizowane z wykorzystaniem jednej cechy bezpieczeństwa, np. loginu/hasła – mówimy wtedy o słabym mechanizmie uwierzytelniania. Z kolei kiedy proces uwierzytelniania jest oparty na wielu czynnikach – w tym na hasłach jednorazowych lub tokenach uwierzytelniających – wówczas mówimy o silnym mechanizmie uwierzytelniania. Najwyższy poziom uwierzytelnienia zapewniają mechanizmy kryptograficzne, np. te zawarte w nowym dowodzie osobistym. Mechanizm uwierzytelniania jest przypisany indywidualnie do środka identyfikacji elektronicznej, a odpowiednie urządzenia, hasła i identyfikatory pozwalające na uwierzytelnienie są zazwyczaj przypisywane w momencie rejestracji użytkownika. Nowoczesne systemy uwierzytelnienia i identyfikacji elektronicznej coraz częściej są wspierane przez silne mechanizmy biometryczne, np. biometrię twarzy lub odcisku palca. Dane biometryczne stosowane do uwierzytelnienia muszą być przechowywane w sposób zabezpieczony. Z tego powodu zazwyczaj →

nie są przechowywana centralnie, a jedynie na urządzeniu uwierzytelniającym, np. telefonie, który na podstawie naszego odcisku palca lub porównania twarzy realizuje proces uwierzytelniania. Zgodnie z normami urządzenie, które przed uwierzytelnieniem weryfikuje biometrię lub wymaga podania hasła, zastępuje dwa czynniki uwierzytelniania, dostarczając silnego mechanizmu uwierzytelniającego.

Od tego, jak jest realizowany pod względem bezpieczeństwa każdy z trzech powyżej opisanych procesów, zależy poziom wiarygodności środka identyfikacji elektronicznej. W niniejszym artykule używamy sformułowania: poziom wiarygodności (ang. level of assurance), który w oficjalnym tłumaczeniu rozporządzenia eIDAS na język polski został nazwany poziomem bezpieczeństwa. Rozporządzenie eIDAS określa trzy poziomy wiarygodności: niski (low), znaczący-średni[1] (substantial) i wysoki (high). Poziom wiarygodności jest taki, jak najniższy z poziomów każdego z trzech wymienionych procesów, tj. jeżeli rejestracja jest na poziomie średnim, a uwierzytelnienie i zarządzanie są na poziomie wysokim, to poziom wiarygodności środka identyfikacji jest średni.

Pewny, ale z ryzykiem

Analizując środki identyfikacji udostępniane przez podmioty publiczne, można dojść do wniosku, że dowód osobisty z warstwą elektroniczną spełnia wymagania poziomu wysokiego wiarygodności, natomiast profil zaufany może aspirować do poziomu średniego, o ile zarządzanie pz jest realizowane zgodnie ze standardami bezpieczeństwa, a rejestracja w punktach potwierdzających jest audytowana i podlega kontroli. Ze względu na ścisłe wymagania przepisów bankowych i kontrole realizowane przez Komisję Nadzoru Finansowego bankowe środki identyfikacji elektronicznej spełniają wymagania poziomu średniego.

Dla usług publicznych poziom średni wiarygodności środka identyfikacji elektronicznej jest zazwyczaj wystarczający do zapewnienia bezpieczeństwa usługi online. Zapewnia on dostęp do danych osobowych i obsługi konta użytkownika. Środek identyfikacji elektronicznej na poziomie średnim pozwala też wydać kwalifikowany certyfikat podpisu elektronicznego, o ile proces rejestracji przed wydaniem środka identyfikacji został zrealizowany bezpośrednio przez operatora na podstawie fizycznego dokumentu tożsamości. O tym, jaki powinien być poziom wiarygodności środka na potrzeby danej usługi online, powinna zadecydować analiza ryzyka.

Aplikacja mobilna – eDO App

Jedną z najciekawszych nowości ostatnich miesięcy w dziedzinie elektronizacji administracji publicznej jest aplikacja eDO App. Aplikacja jest dostępna do pobrania w sklepie Google Play od czerwca 2020 r. i umożliwia zalogowanie się do niektórych aplikacji oraz założenie i potwierdzenie profilu zaufanego za pomocą telefonu. Warunkiem koniecznym jej uruchomienia jest posiadanie e-dowodu, czyli dokumentu tożsamości z wbudowaną warstwą elektroniczną (na chwilę obecną są to wszystkie dowody osobiste wydane na podstawie wniosku złożonego po 4 marca 2019 r.). Jednakże korzystanie z funkcjonalności e-dowodu zostało uzależnione od aktywowania usługi osobiście w urzędzie, w trakcie której generowane są dwa kody PIN, służące do weryfikacji osoby korzystającej z dostępu do e-administracji. Innowacyjność eDO App polega na zastąpieniu dotychczas stosowanego czytnika, służącego do weryfikacji tożsamości, smartfonem.

Co nie jest podpisem

Identyfikacja elektroniczna i usługi zaufania to dwa oddzielne rozdziały rozporządzenia eIDAS. Podpis elektroniczny nie jest identyfikacją elektroniczną, a identyfikacja elektroniczna nie jest usługą zaufania. Natomiast identyfikacja elektroniczna z powodzeniem może potwierdzać tożsamość osoby ubiegającej się o kwalifikowany certyfikat podpisu elektronicznego, pozwalając na jego pozyskanie bez konieczności osobistego stawiennictwa. Takie podejście umożliwia wygenerowanie kwalifikowanego certyfikatu na potrzeby pojedynczej transakcji, co jest bardzo przydatne wtedy, gdy użytkownik tylko sporadycznie korzysta z kwalifikowanych podpisów elektronicznych. Sama usługa identyfikacji elektronicznej nie zastępuje podpisów elektronicznych, ponieważ nie pozwala na powiązanie tożsamości z konkretnym dokumentem lub oświadczeniem woli.

W najbliższych miesiącach spodziewany jest rozwój systemów identyfikacji elektronicznej, powstawanie nowych usług, w ramach których dostarczane będą środki identyfikacji elektronicznej. Jednocześnie rozwijają się mechanizmy uwierzytelniania pozwalające na efektywne wykorzystanie telefonu komórkowego do bezpiecznego procesu. Systemy publiczne podłączone do węzła krajowego będą miały możliwość korzystania ze środków identyfikacji elektronicznej – nowych i dołączających się do krajowego schematu identyfikacji – bez konieczności wprowadzania zmian w swoich systemach, ponieważ niezależnie od tego, jaki środek identyfikacji elektronicznej zostanie użyty, uwolnione dane identyfikujące osobę będą przekazane do usługi online w ten sam sposób. Ważnym aspektem nadchodzących miesięcy będzie pełne uruchomienie transgranicznie dostępnych notyfikowanych środków identyfikacji elektronicznej, które także będą dostępne za pomocą węzła krajowego. Niestety, na notyfikację naszych krajowych środków identyfikacji elektronicznej przyjdzie nam jeszcze poczekać. IT

Autor jest ekspertem ds. identyfikacji, uwierzytelniania i podpisu elektronicznego PIIT, rzeczoznawcą PTI, ekspertem Komitetu Technicznego ESI ETSI oraz partnerem Obserwatorium.biz i kierownikiem rozwoju Autenti. Pomysłodawca składania deklaracji PIT zabezpieczonych kwotą z deklaracji zeszłorocznej, projektant Profilu Zaufanego ePUAP i inicjator Forum eIDAS_PL zajmującego się wdrożeniem eIDAS w Polsce.

Przypisy:

1 Błąd polskiego tłumaczenia eIDAS w zakresie terminu określającego średni poziom wiarygodności (ang. substantial). Powinien on być określany mianem: „znaczący".