**Eksperci PIIT o identyfikacji elektronicznej**

2017-10-31

Identyfikacja elektroniczna umożliwia użytkownikom systemów teleinformatycznych potwierdzenie swoich danych np. imienia, nazwiska i PESEL w oparciu o wybraną przez siebie usługę dostawcy tożsamości. Dostawcą tożsamości może być ktoś, kto posiada nasze dane osobowe, w sposób bezpieczny nimi zarządza i umożliwia bezpieczne zalogowanie się. Systemy bankowości elektronicznej, posiadające wszystkie powyżej wymienione cechy są pierwszymi dostawcami tożsamości elektronicznej.

Korzystanie z systemu identyfikacji elektronicznej jest realizowane zawsze pod kontrolą użytkownika, który po zalogowaniu do systemu identyfikacji elektronicznej każdorazowo wydaje zgodę jakie jego dane zostaną przekazane. Systemy identyfikacji elektronicznej nie przekazują samodzielnie danych osobowych i nie umożliwiają ściąganie tych danych poza kontrolą użytkownika.

Każdy system identyfikacji elektronicznej jest oznaczony poziomem jego bezpieczeństwa (wiarygodności) – niskim, średnim lub wysokim. Aby udostępniać usługę identyfikacji na odpowiednim poziomie dostawca eID musi spełnić szereg warunków technicznych i organizacyjnych określonych w rozporządzeniu Komisji Europejskiej.

Systemy udostępniające usługi publiczne lub prywatne w oparciu o eID określają poziom akceptowalnej wiarygodności środków identyfikacji elektronicznej, w wyniku czego uwierzytelnienie do tych usług jest możliwe tylko w przypadku posługiwania się środkami o odpowiednim poziomie wiarygodności. Innymi słowy to udostępniający usługę decyduje jaki poziom bezpieczeństwa jest adekwatny do udostępnianej przez niego usługi i w przypadku usług o wyższym ryzyku akceptuje środki o poziomie wiarygodności wysokim.

Krajowy schemat identyfikacji elektronicznej w znaczącym stopniu jest oparty o systemy identyfikacji elektronicznej o średnim poziomie wiarygodności dostarczane przez podmioty komercyjne, które spełnią rygorystyczne kryteria jakościowe. Natomiast dostarczenie środków o poziomie wiarygodności wysokim może pozostać ostatecznie w gestii państwa polskiego w nowym dowodzie osobistym z warstwą elektroniczną.

Przepisy Unii Europejskiej są jednoznaczne - 29 września 2018 polska administracja będzie zobowiązana w usługach publicznych akceptować identyfikację elektroniczną z innych krajów Unii Europejskiej. Obowiązek ten będzie niezależny od tego, czy polski obywatel będzie miał w kraju własne narzędzie do identyfikacji elektronicznej czy też nie.

Wdrożenie czysto administracyjnych rozwiązań takich jak elektroniczny dowód osobisty czy nowy Profil Zaufany wymaga przygotowania infrastruktury oraz zbudowania potencjału użytkowników. Przyjmując optymistyczny scenariusz uruchomienia nowego dowodu na początku 2019 roku, potencjał odpowiadający dzisiejszemu rynkowi użytkowników bankowości elektronicznej i mobilnej – około dwudziestu milionów użytkowników będzie można osiągnąć dopiero za 7-8 lat.

W krajowym systemie identyfikacji elektronicznej nie jest realizowane przekazywanie danych osobowych do dostawców identyfikacji elektronicznej, system ten bazuje na danych, które są w posiadaniu banków lub innych dostawców identyfikacji elektronicznej i będą przekazywane do administracji publicznej w procesie identyfikacji. Wobec powyższego powstanie schematu nie narusza bezpieczeństwa danych osobowych.

Stosowanie komercyjnych środków identyfikacji elektronicznej nie stanowi zagrożenia dla bezpieczeństwa państwa, ponieważ usługi o większym „apetycie” na bezpieczeństwo powinny być chronione środkami identyfikacji o poziomie

wiarygodności wysokim, natomiast usługi najczęściej wykorzystywane przez obywateli powinny być oparte o rozwiązania bardziej dostępne. W tym zakresie bardzo duże znaczenie mają dwa fakty:

1. Pozytywne doświadczenie użytkownika, w którym rozwiązania dostosowane są do potrzeb, łatwe w użytkowaniu oraz użyteczne.
2. Zakres usług dla środka identyfikacji jest szeroki, tj. dotyczy zarówno spraw administracji publicznej jak i używania w codziennych sprawach.

Wydawanie środków identyfikacji elektronicznej na poziomie wysokim, używanych przez obywateli zarówno w usługach publicznych jak i komercyjnych powinno być jednym z działań administracji publicznej nastawionych na przyszłość. Równolegle konieczne jest funkcjonowanie środków identyfikacji elektronicznej na poziomie średnim, który umożliwi każdemu obywatelowi używanie usług publicznych i komercyjnych. W zakresie tych drugich środek taki powinien gwarantować korzystającym z niego usługodawcom odpowiedni poziomi wiarygodności i gwarancje. Rozwiązaniem najbardziej efektywnym dla środków na poziomie średnim i niskim jest proponowany krajowy schemat identyfikacji elektronicznej.

Brak wdrożenia krajowego schematu identyfikacji elektronicznej w Polsce może w niedługim czasie skutkować rozwojem na polskim rynku notyfikowanych schematów zagranicznych, z których polscy obywatele będą mogli skorzystać, natomiast administracja już za rok będzie musiała je uznawać.

Eksperci ds. Identyfikacji, uwierzytelnienia i podpisu elektronicznego Polskiej Izby Informatyki i Telekomunikacji

Fakty i mity o elektronicznej identyfikacji

1. **Krajowy System Identyfikacji Elektronicznej będzie gromadził dane o obywatelach co stanowi o ich zagrożeniu.**

**FAŁSZ!** W ramach krajowego systemu identyfikacji elektronicznej odużytkowników nie są pozyskiwane dodatkowe dane. W ramach tego systemu dane będące już wcześniej w posiadaniu banków, a także np. zgromadzone w Profilu Zaufanym, są wykorzystywane do uwierzytelnienia w usługach publicznych. W ramach funkcjonowania krajowego systemu identyfikacji elektronicznej dostawcy tożsamości nie uzyskują danych z systemów administracji publicznej, tylko administracja publiczna korzysta z danych będących w posiadaniu dostawców tożsamości.

1. **Krajowy System Identyfikacji Elektronicznej będzie w sposób niekontrolowany udostępniał dane osobowe.**

**FAŁSZ!** Wykorzystanie usługi identyfikacji elektronicznej odbywa siępokażdorazowym uwierzytelnieniu się użytkownika, który wyraża zgodę komu i jakie dane z systemu zarządzania tożsamością zostaną przekazane. Innymi słowy system umożliwia użytkownikowi po zalogowaniu się pobranie potwierdzenia tożsamości dla usługi, z której chce korzystać i użytkownik osobiście decyduje o tym, czy te dane zostaną jednorazowo przekazane. W ramach Krajowego Systemu Identyfikacji Elektronicznych nie jest możliwe pobieranie danych osobowych z systemów tożsamości bez każdorazowej wyłącznej kontroli osoby, której dane dotyczą.

1. **Funkcjonowanie krajowego schematu identyfikacji elektronicznej wymaga ochrony danych osobowych**

**PRAWDA!** Zgodnie z rozporządzeniem obowiązującym w UniiEuropejskiej dotyczącym ochrony danych osobowych RODO wszystkie podmioty przetwarzające dane osobowe zobowiązane są do realizacji szczególnych wymagań związanych z ich ochroną. Wymaganie to dotyczy zarówno dostawców tożsamości, węzłów identyfikacji elektronicznej oraz podmiotów z tych danych korzystających, w tym administracji publicznej. Wejście w życie RODO zwiększy bezpieczeństwo danych osobowych niezależnie od tego, czy są przetwarzane przez podmioty administracji publicznej, czy przez podmioty komercyjne.

1. **Dopuszczenie do węzła podmiotów komercyjnych jest działaniem ryzykownym ze względu na ochronę danych osobowych.**

**FAŁSZ!** Dane osobowe sąi będąprzetwarzane we wszystkichinstytucjach, które zgodnie planowaną ustawą wprowadzającą krajowy schemat identyfikacji elektronicznej staną się dostawcami identyfikacji elektronicznej. Zarówno banki, telekomy jak i np. spółki energetyczne przetwarzają dane osobowe. W ramach wejścia w życie przepisów o identyfikacji elektronicznej podmioty te nie będą otrzymywały więcej danych osobowych. To podmioty publiczne będą mogły korzystać z tych danych komercyjnych.

1. **Krajowy Węzeł Identyfikacji Elektronicznej będzie krytycznym elementem infrastruktury państwa.**

**PRAWDA!** Krajowy WęzełIdentyfikacji Elektronicznej jako miejsce,przez które przekazywane są dane osobowe od dostawców identyfikacji elektronicznej celem korzystania z usług administracji publicznej stanowi krytyczny element, ponieważ brak jego działania będzie ograniczał możliwość skorzystania z usług elektronicznych przez obywateli. Każdy system zarządzania identyfikacją elektroniczna na poziomie krajowym będzie miał podobną krytyczność w zakresie dostępności dla usług e-administracji. Co więcej brak działania krajowego węzła identyfikacji elektronicznej będzie utrudniał wywiązanie się z obowiązków nakładanych na dostawców e-usług administracji publicznej związanych z akceptowaniem zagranicznych środków identyfikacji elektronicznej. W związku z tym Krajowy Węzeł Identyfikacji Elektronicznej będzie w gestii Ministra Cyfryzacji i pod całkowitą kontrolą administracji publicznej.

1. **Dostęp do elektronicznych usług publicznych powinien zapewniać jedynie Profil Zaufany.**

**FAŁSZ!** Profil Zaufany ze swojej natury jest systemem administracjipublicznej o ograniczonych gwarancjach i zastosowaniu. Na dzień dzisiejszy Profil Zaufany zapewnia w zakresie uwierzytelnienia poziom wiarygodności niski, a w zakresie podpisu średni, co stanowi problem jego użytkowania. Administracja publiczna nie umożliwia korzystania z Profilu Zaufanego przez podmioty komercyjne i nie daje żadnych gwarancji dotyczących jego wiarygodności w zakresie usług komercyjnych. Użytkownicy naturalnie nie będą korzystali z rozwiązań, które dają im ograniczony zakres stosowania – np. które będą tylko do rzadko stosowanych usług publicznych.

Zgodnie z rozporządzeniem eIDAS wszystkie systemy administracji publicznej będą zobowiązane rozpoznawać identyfikację elektroniczną pochodzącą z notyfikowanych systemów zagranicznych, więc z obowiązku prawa Profil Zaufany nie będzie jedynym środkiem identyfikacji w Polsce.

1. **Profil Zaufany rozwija się dzięki logowaniu się do niego poprzez banki.**

**PRAWDA!** Aktualnie Profili Zaufany jest dostępny z poziomu kilku

banków umożliwiających wykorzystanie konta bankowości elektronicznej

do założenia i wykorzystywania Profilu Zaufanego. Działanie to

spowodowało znaczny wzrost popularności Profilu Zaufanego, było jednak

działaniem nastawionym na przetestowanie na ile wiarygodnie można

wykorzystać tożsamość pochodzącą z podmiotów komercyjnych na

potrzeby administracji publicznej. Dostawcy komercyjni, którzy

udostępniają dane identyfikacyjne z natury rzeczy będą rozszerzać zakres

swoich usług na inne obszary zastosowań jakimi są usługi prywatne.

Popularyzacja identyfikacji elektronicznej umożliwia łatwiejszy rozwój

równolegle usług administracji publicznej i komercyjnych.

1. **Za korzystanie z komercyjnych systemów identyfikacji elektronicznej obywatel będzie musiał płacić.**

**FAŁSZ!** Wszystkie podmiotyświadczące usługęidentyfikacji będąjąudostępniały na rzecz administracji publicznej bezpłatnie i nie będą pobierały opłaty za korzystanie z identyfikacji przez obywateli w usługach publicznych. Opłaty za usługi komercyjnej identyfikacji będą ponosiły podmioty komercyjne ją wykorzystujące w swoich usługach.

1. **Minister nie dysponuje odpowiednimi środkami do oceny poziomu bezpieczeństwa informatycznego systemów identyfikacji elektronicznej.**

**PRAWDA!** Minister nie dysponuje zespołami i narzędziamipozwalaj ą cymi kompleksowo i profesjonalnie oceni ć poziom bezpieczeństwa dostawców identyfikacji elektronicznej, niezależnie od tego czy są to podmioty publiczne, czy komercyjne. Natomiast od podmiotów komercyjnych może żądać zaświadczeń niezależnych audytorów, którzy w sposób pełny i wiarygodny dokonają analizy bezpieczeństwa dostawcy i wystawią odpowiedni certyfikat. W przypadku dostawców komercyjnych koszty takiej certyfikacji ponoszą same podmioty, natomiast minister na podstawie dokumentacji audytowej może podjąć decyzję o dopuszczeniu podmiotu do świadczenia usług identyfikacji na rzecz administracji publicznej.

**10.Węzeł będzie umożliwiał dostęp do danych wrażliwych przez dostawców tożsamości.**

**FAŁSZ!** Dostawca tożsamości nie ma dostępu do innych danych niżte,które już posiada. Rozwiązanie krajowego schematu identyfikacji elektronicznej umożliwia przekazywanie danych osobowych klientów dostawców tożsamości do administracji publicznej i innych dostawców usług elektronicznych, a nie w drugą stronę. Administracja publiczna nie będzie udostępniała swoich danych do dostawców tożsamości.

**11.Rozwój Profilu Zaufanego i nowy dowód osobisty są skuteczną alternatywą dla Krajowego Systemu Identyfikacji Elektronicznej.**

**FAŁSZ!** Nowy dowód osobisty nie zostałjeszcze wdrożony, wstępnie jegowdrożenie ma nastąpić na początku 2019 roku. Nowy dowód będą dostawali obywatele w trybie tzw. zwyczajnej wymiany dowodów, której całkowity cykl wynosi 10 lat, co oznacza, że masa krytyczna kilkunastu milionów elektronicznych dowodów osobistych zostanie osiągnięta w ciągu 5-6 lat od wdrożenia. Istniejący dziś Profil Zaufany rozwija się dzięki komercyjnym dostawcom identyfikacji elektronicznej, którzy przeprowadzają proces potwierdzenia Profilu Zaufanego – w szczególności są to banki. Profil Zaufany zgodnie z dotychczasowymi założeniami nie będzie dawał gwarancji wiarygodności dla podmiotów komercyjnych, co

ogranicza jego zastosowanie tylko do administracji publicznej. Ograniczenie zastosowania Profilu Zaufanego tylko do administracji publicznej powoduje go mało użytecznym dla przeciętnego użytkownika.

**12.Rozwój krajowego schematu identyfikacji elektronicznej może skutkować spadkiem popularności Profilu Zaufanego.**

**PRAWDA!** Wprowadzenie krajowego schematu identyfikacjielektronicznej b będzie skutkować spadkiem popularności Profilu Zaufanego w obecnej postaci, jednakże pozostaną obszary, w których użytkownicy będą chcieli całkowicie pozostać w obszarze administracji publicznej, w szczególności może dotyczyć to urzędników administracji publicznej. Jeżeli Profil Zaufany będzie się rozwijał i stanie się notyfikowanym środkiem identyfikacji elektronicznej o zasięgu europejskim to jego udział może dotyczyć wszystkich tych usług, w których obywatel polski korzystać będzie z usług publicznych w innych krajach. Jednakże jednym z podstawowych warunków funkcjonowania mechanizmu identyfikacji jest jego możliwość szerokiego i łatwego wykorzystania w różnych usługach nie tylko administracji publicznej, a także łatwość uzyskania dostępu do takiego mechanizmu.

**13.Wszystkie usługi dotyczące identyfikacji i tożsamości elektronicznej powinny zostać w gestii polskich instytucji państwowych.**

**FAŁSZ!** Po pierwsze jest niemożliwe, aby identyfikacja została w gestiipolskich instytucji państwowych, ponieważ eIDAS wymusza akceptację notyfikowanej zagranicznej identyfikacji elektronicznej, która może być udostępniana przez instytucje komercyjne. Po drugie dotychczasowe doświadczenia budowy wyłącznie rządowych systemów identyfikacji elektronicznej nie przyniosły wymiernych skutków. Rzeczywisty rozwój Profilu Zaufanego był dopiero możliwy w oparciu o komercyjne – bankowe systemy tożsamości – co w efekcie jest realizacją krajowego schematu identyfikacji elektronicznej w ograniczonym zakresie.

**14.Brak nowelizacji ustawy o usługach zaufania oraz identyfikacji elektronicznej nie wpłynie negatywnie na rozwój usług publicznych w Polsce**

**FAŁSZ!** Projekt ustawy umożliwiałrzeczywiste wykorzystanie potencjałurozporządzenia eIDAS do udostępnienia obywatelowi polskiemu narzędzia pochodzącego od dostawców będących pod kontrolą Ministra Cyfryzacji. Brak takich rozwiązań będzie skutkował ograniczonym rozwojem polskich usług i ograniczoną możliwością konkurowania z rozwiązaniami zagranicznym, które niezależnie do wspomnianej ustawy będą musiałby być akceptowane przez polską administrację publiczną..

Stanowisko opracowali Eksperci PIIT:

***Artur Miękina, Andrzej Ruciński i Michał Tabor***