Warszawa, 24 maja 2021 r.

KANCELARIA PREZESA RADY MINISTRÓW
PEŁNOMOCNIK RZĄDU DO SPRAW
CYBERBEZPIECZEŃSTWA

Marek Zagórski

DC.WSC.72421.3.7.2021

Stanowisko Pełnomocnika Rządu ds. Cyberbezpieczeństwa w sprawie zdalnej identyfikacji tożsamości subskrybentów usług zaufania

Rosnąca mobilność społeczeństwa i wzrastające w związku z tym zapotrzebowanie na narzędzia zdalnej identyfikacji i zdalnego składania oświadczeń woli generuje wzrost zapotrzebowania na różnego rodzaju usługi zaufania, w tym na usługi związane z wydawaniem kwalifikowanego certyfikatu podpisu elektronicznego i kwalifikowanego certyfikatu pieczęci elektronicznej. Zidentyfikowaną barierą w rozwoju rynku usług zaufania jest konieczność fizycznej obecności klienta (subskrybenta) usługi zaufania w punkcie rejestracyjnym. Bariera ta jest szczególnie wyraźna w sytuacji zagrożenia epidemiologicznego, kiedy w celu ograniczenia epidemii wprowadzane są różnego rodzaju ograniczenia w fizycznych kontaktach międzyludzkich. W związku z tym rodzi się potrzeba wykorzystywania mechanizmów zdalnej weryfikacji tożsamości klientów usług zaufania. Prawidłowa identyfikacja osób fizycznych w procesie wydawania kwalifikowanych certyfikatów ma decydujące znaczenie dla bezpieczeństwa procesów e-administracji i innych cyfrowych procesów biznesowych. Krytycznym aspektem ustalania tożsamości jest niezawodne zapobieganie i wykrywanie oszustw, polegających na kradzieży tożsamości lub posługiwaniu się tożsamością nieistniejącą. Szczególne znaczenie ma to w przypadku wydawania certyfikatów kwalifikowanego podpisu elektronicznego, który ma skutki prawne zrównane z podpisem odręcznym osoby go składającej i w związku z tym może powodować znaczne straty w obrocie gospodarczym i w obrocie majątkiem osobistym, w przypadku gdy certyfikat podpisu zostanie wydany niewłaściwej osobie.

Należy zauważyć, że z podobnym problemem, związanym ze zdalnym potwierdzeniem tożsamości, spotkał się Urząd Komisji Nadzoru Finansowego we wdrażaniu dyrektywy (UE) 2018/843 w sprawie zapobiegania wykorzystywaniu systemu finansowego do celów prania pieniędzy lub finansowania terroryzmu (AMLD5), co skutkowało wydaniem przez ten urząd w dniu 5 czerwca 2019 r. komunikatu ze stanowiskiem dotyczącym identyfikacji klienta i weryfikacji jego tożsamości w bankach oraz oddziałach instytucji kredytowych w oparciu o metodę wideoweryfikacji.

Podstawą prawną, regulującą funkcjonowanie rynku usług zaufania jest *rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 910/2014 z dnia 23 lipca 2014 r. w sprawie identyfikacji elektronicznej i usług zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznym oraz uchylające dyrektywę 1999/93/WE* (eIDAS).

Ustalenie tożsamości klienta usług zaufania regulują przepisy art. 24 ust. 1 eIDAS, niemniej zgodnie z motywem 13 eIDAS państwa członkowskie powinny zachować swobodę w stosowaniu lub wprowadzaniu środków dostępu do usług online do celów identyfikacji elektronicznej. W związku z tym, jako organ ustanowiony przepisem art. 2 *ustawy z dnia 5 września 2016 r. usługach zaufania oraz identyfikacji elektronicznej* (Ustawa) do zapewnia funkcjonowania krajowej infrastruktury zaufania wyrażam następujące stanowisko w kwestii interpretacji przepisów art. 24 ust. 1 eIDAS na potrzeby świadczenia usług zaufania przez przedsiębiorców zarejestrowanych na obszarze Rzeczypospolitej Polskiej.

Zgodnie z przepisami art. 24 ust. 1 eIDAS kwalifikowany dostawca usług (QTSP) zaufania weryfikuje, za pomocą odpowiednich środków i zgodnie z prawem krajowym, tożsamość i, w stosownym przypadku, wszelkie specjalne atrybuty osoby fizycznej lub prawnej, której wydaje kwalifikowany certyfikat:

a) Przez fizyczną obecność osoby fizycznej lub upoważnionego przedstawiciela osoby prawnej w punkcie rejestracji. Tożsamość osoby fizycznej weryfikowana jest na podstawie, uznanego przez przepisy odrębne, dokumentu tożsamości i porównaniu wizerunku osoby zamieszczonego w tym dokumencie z wizerunkiem osoby stawającej. Pracownik (operator) QTSP musi posiadać udokumentowane przeszkolenie w zakresie rozpoznawania dokumentów tożsamości, ich podstawowych zabezpieczeń w zakresie autentyczności oraz wykrywania typowych fałszerstw dokumentów tożsamości. Ważność dokumentu tożsamości, o ile to jest możliwe, powinna być potwierdzona poprzez zapytanie do rejestru referencyjnego. W przypadku dokumentów z warstwą elektroniczną wskazane jest porównanie zapisów warstwy graficznej z zapisami warstwy elektronicznej.
b) Zdalnie, przy użyciu środka identyfikacji elektronicznej, w przypadku którego przed wydaniem kwalifikowanego certyfikatu zapewniono fizyczną obecność osoby fizycznej lub upoważnionego przedstawiciela osoby prawnej i który spełnia wymogi określone w art. 8 eIDAS w odniesieniu do średniego lub wysokiego poziomu bezpieczeństwa. W tym przypadku zastosowanie mogą mieć środki identyfikacji elektronicznej określone w przepisie dotyczącym środka identyfikacji elektronicznej wydanego w systemie identyfikacji elektronicznej przyłączonym do węzła krajowego identyfikacji elektronicznej, o którym mowa w art. 21a ust. 1 pkt 2 lit. a Ustawy. Rozliczalność użycia środka identyfikacji zapewniona jest poprzez funkcjonalność węzła krajowego.
c) Za pomocą certyfikatu kwalifikowanego podpisu elektronicznego lub kwalifikowanej pieczęci elektronicznej wydanych zgodnie z lit. a) lub b).
d) Przy użyciu innych metod identyfikacji uznanych na szczeblu krajowym, które zapewniają pewność równoważną, pod względem wiarygodności, fizycznej obecności. Równoważna pewność musi być potwierdzona przez jednostkę oceniającą zgodność.

W zakresie „innych metod", o których mowa w przepisie art. 24. ust. 1 lit. d eIDAS znajduje się metoda wideoweryfikacji. Przy rozpatrywaniu tej metody należy wziąć pod uwagę opracowany przez ENISA w lutym 2021 r. dokument pt. *Remote ID proofing - Analysis of Methods to carry out identity proofing remotely* (Zdalne dowodzenie ID – Analiza metod prowadzenia zdalnej identyfikacji).

W dokumencie zauważono, że cyt.: „Nie wszystkie rozwiązania w zakresie zdalnej identyfikacji są odpowiednie dla wszystkich okoliczności. Czasami bardziej istotne jest posiadanie większej

pewności co do tożsamości danej osoby, nawet jeśli sprawdzenie zajmuje dużo czasu lub kosztuje więcej. W innych sytuacjach akceptowalna jest mniejsza pewność co do tożsamości, która pozwala na zastosowanie szybszych, tańszych lub łatwiejszych procesów potwierdzania tożsamości. To, co jest dopuszczalne, zależy np. od finansowych konsekwencji fałszywej tożsamości.".

W przypadku wideoweryfikacji jest to metoda **podobna** do metody "na miejscu z operatorem" (ale nie tożsama), gdzie obecność osoby fizycznej (subskrybenta usługi) jest realizowana za pomocą zdalnego połączenia internetowego lub innego rodzaju teletransmisji. Operator bierze udział w procesie identyfikacji na żywo, prowadząc z wnioskodawcą dialog w oparciu o udokumentowane instrukcje. Proces ten jest wspierany przez system teleinformatyczny, na który składa się między innymi kamera cyfrowa i mikrofon, które służą do zbierania i rejestrowania materiału dowodowego. Można stosować dodatkowe zabezpieczenia i gromadzić dodatkowe atrybuty z odpowiednich zaufanych źródeł. Do wspomagania lub usprawniania gromadzenia informacji może być wykorzystywane oprogramowanie, w tym sztuczna inteligencja, ale to człowiek, który jest operatorem prowadzącym proces, podejmującym ostateczną decyzję.

Z uwagi na ogólny charakter przepisu art. 24. ust. 1 lit. d eIDAS niezbędne jest wskazanie dodatkowych wyjaśnień, czemu służy niniejsze Stanowisko.

Dostawca kwalifikowanych usług zaufania (QTSP) opracowuje, dokumentuje i wprowadza procedury dotyczące procesu wideoweryfikacji uwzględniając:

- proces szacowania ryzyka związany z zagrożeniami występującymi podczas wideoweryfikacji;
- określenie ograniczeń wynikający z postępowania z ryzykiem w odniesieniu do możliwości nawiązania relacji z klientem przy pomocy wideoweryfikacji, np. ograniczenie się wyłącznie do obywateli polskich, rezydentów w Polsce, rezydentów w UE, do wybranych usług;
- określenie wymogów sprzętowych po stronie klienta (określenie minimalnych wymogów jakościowych sprzętu, np. rozdzielczości kamery, np.) oraz wymagań w stosunku do oprogramowania np. rodzaj komunikatora; subskrybent musi złożyć deklarację spełnienia wymogów, a operator QTSP musi, w miarę możliwości, zweryfikować deklarację;
- określenie rozwiązań, które zmniejszają ryzyko subskrypcji usługi w drodze wideoweryfikacji na osobę trzecią, bądź osobę nieświadomą celu wykonywanych czynności. Można to zrobić, poprzez ustalenie wymogów zewnętrznych dotyczących miejsca i czasu (np. wykluczenie możliwości przeprowadzenia wideoweryfikacji w miejscach publicznych, w których panuje duży hałas i w zasięgu kamery jest ciągła obecność osób trzecich, nieakceptowanie wstrzymywania/zawieszania procesu – wyjścia osoby poza strefę widzenia obiektywu kamery, wprowadzenie ograniczeń czasowych na wykonanie poszczególnych działań):
  - wymóg dokonania przeglądu i ewentualnie modyfikacji procedury (z odpowiednią częstotliwością), w tym pod kątem skuteczności przyjętych kryteriów oceny ryzyka i stosowanych środków bezpieczeństwa,
  - wymóg archiwizowania zapisów wideo (zarówno dźwięku jak i obrazu) z rozmowy z klientami; w procedurach QTSP powinny być odpowiednie przepisy dotyczące

nagrywania i przechowywania zapisów wideo. Okres przechowywania danych powinien spełniać wymogi Ustawy;

- dokonywanie analizy przypadków odmowy nawiązania relacji z klientem przy pomocy wideoweryfikacji;
- prowadzenie i dokumentowanie szkoleń pracowników operacyjnych usługodawcy, w szczególności w zakresie identyfikacji i weryfikacji tożsamości subskrybenta oraz szkoleń z weryfikacji dokumentów tożsamości;
- objęcie rozwiązań w zakresie wideoweryfikacji systemem kontroli wewnętrznej oraz systemem informacji zarządczej, w tym systemem zarządzania bezpieczeństwem informacji;
- jako wzmocnione środki bezpieczeństwa w przypadku wideoweryfikacji, należy uznać (o ile są dostępne):
  - sprawdzenie klienta i informacji zawartych w jego dokumencie tożsamości – w bazach danych, jak np. w:
    - Rejestrze Dowodów Osobistych,
    - Rejestrze Paszportów,
    - Rejestrze PESEL,
    - Wewnętrznej bazie danych usługodawcy (np. poprzez prowadzenie bazy danych o nieudanych próbach zdalnego potwierdzenia danej tożsamości);
  - upewnienie się o nieprzebywaniu osób trzecich w towarzystwie subskrybenta podczas dokonywania wideoweryfikacji oraz o braku jakiejkolwiek ingerencji osób trzecich (np. podpowiedzi kierowane do subskrybenta przez takie osoby). Niedopuszczalne jest także opuszczenie pomieszczenia przez subskrybenta, czy inny rodzaj przerwy w toku wideoweryfikacji, co może sugerować konsultacje subskrybenta z osobami trzecimi,
  - przeprowadzanie wideoweryfikacji z udziałem pracownika usługodawcy; w sytuacji gdy usługodawca dopuszcza automatyczną wideoweryfikację, niezbędne jest ścisłe określenie warunków/kryteriów takiego procesu oraz w jakim zakresie i w jakich przypadkach weryfikacja musi zostać potwierdzona bądź uzupełniona przez pracownika usługodawcy,
  - okazanie dokumentu tożsamości do kamery pod wieloma kątami z wielu stron oraz okazanie krawędzi dokumentu w dużym powiększeniu w celu weryfikacji jego autentyczności,
  - zweryfikowanie autentyczności dokumentu tożsamości oraz integralności danych,
  - porównanie zdjęć z dowodu tożsamości bezpośrednio z wizerunkiem klienta oraz ze zdjęciem twarzy (wskazane bez okularów), przy zagwarantowaniu odpowiednio wysokiego poziomu jakości wykonywanych fotografii,
  - przesłanie przez pracownika usługodawcy w trakcie wideoweryfikacji kodu SMS na numer telefonu komórkowego klienta, który musi być podany konsultantowi podczas wideorozmowy,
  - pozostawienie w archiwach usługodawcy (jako materiału dowodowego) zapisu całej wideorozmowy przez okres określony w art. 17 ust. 2 Ustawy i zapewnienie zapisowi konserwacji zapewniającej integralność i dostępność przez okres przechowywania.

Przy opracowaniu procedur wideoweryfikacji muszą zostać przez QTSP uwzględnione następujące elementy:

1) Kryteria:
    - art. 24 ust. 1 lit. d rozporządzenia eIDAS.
2) Wymagania:
    a) Metoda identyfikacji musi dawać poziom pewności tożsamy, pod względem niezawodności, z prowadzoną identyfikacją w trakcie spotkania fizycznego z subskrybentem usługi.
    b) Tożsamy (analogiczny do weryfikacji w trakcie spotkania fizycznego) poziom pewności w kwestii identyfikacji klienta musi zostać poświadczony przez jednostkę oceniającą zgodność (CAB), akredytowaną zgodnie z art. 3 ust. 18 rozporządzenia eIDAS:
        - CAB musi posiadać uznane doświadczenie w dziedzinie metod zdalnej identyfikacji tożsamości osób;
        - CAB musi zweryfikować zgodność QTSP z ogólnym rozporządzeniem o ochronie danych osobowych (RODO).
3) Wymagania dotyczące raportu certyfikacyjnego:
    - jednoznaczne potwierdzenie równoważności metody zdalnej weryfikacji tożsamości z obecnością fizyczną.

Marek Zagórski
Pełnomocnik Rządu
ds. Cyberbezpieczeństwa
/podpisano kwalifikowanym
podpisem elektronicznym/