KIR

Europejski portfel tożsamości cyfrowej w eIDAS 2.0 a SCA

Robert Podpłoński
Radca prawny

Europejski Portfel Tożsamości Cyfrowej – EPTC

Środek identyfikacji elektronicznej, który umożliwia użytkownikowi przechowywanie i pobieranie danych dotyczących tożsamości, elektronicznych poświadczeń atrybutów związanych z jego tożsamością, dostarczanie ich stronom ufającym na żądanie i wykorzystywanie ich do uwierzytelniania, online i, w stosownych przypadkach, offline, w ramach usługi zgodnie z art. 6a; oraz składanie podpisu za pomocą kwalifikowanych podpisów elektronicznych i pieczęci za pomocą kwalifikowanych pieczęci elektronicznych.

Cechy

- środek identyfikacji elektronicznej **osoby fizycznej, prawnej lub osoby reprezentującej:**
  - pozwala bezpiecznie żądać, wybierać, łączyć, przechowywać, usuwać elektroniczne **poświadczenie atrybutów i dane identyfikujące osobę** stronom ufającym, w tym do uwierzytelniania online i offline
  - w celu korzystania z **publicznych i prywatnych** usług,
  - przy jednoczesnym zapewnieniu możliwości **selektywnego ujawniania danych,**
- pozwala podpisywać za pomocą kwalifikowanych podpisów elektronicznych i za pomocą kwalifikowanych pieczęci elektronicznych.

Uznawanie EPTC przez organy sektora publicznego

art. 6db ust. 1

Jeżeli państwa członkowskie wymagają identyfikacji elektronicznej przy użyciu środka identyfikacji elektronicznej oraz uwierzytelnienia w celu uzyskania dostępu do usługi internetowej świadczonej przez organ sektora publicznego, akceptują one również portfele europejskiej tożsamości cyfrowej zgodnie z niniejszym rozporządzeniem w celu uwierzytelnienia użytkownika.

Uznawanie EPTC przez sektor prywatny (finansowy)

art. 6db ust. 2

W przypadku gdy prywatne strony ufające świadczące usługi są zobowiązane **na mocy prawa krajowego lub unijnego** do stosowania silnego uwierzytelniania użytkownika na potrzeby **identyfikacji online** lub gdy silne uwierzytelnianie użytkownika jest wymagane **na mocy zobowiązania umownego**, w tym w obszarach bankowości, finansowych, płatniczych i związanych z pieniądzem elektronicznym, infrastruktury cyfrowej, (…), **wyłącznie na dobrowolny wniosek użytkownika**, akceptują również korzystanie z EPTC w odniesieniu do **minimalnych danych niezbędnych** do świadczenia **konkretnej usługi** online, dla której **wymagane jest uwierzytelnienie** użytkownika.

pkt 31 Preambuły

Bezpieczna identyfikacja elektroniczna i dostarczanie poświadczeń atrybutów powinny zapewniać sektorowi usług finansowych dodatkową elastyczność oraz rozwiązania umożliwiające (…) spełnienie wymogów silnego uwierzytelniania klienta w odniesieniu do logowania do rachunku i inicjowania transakcji w dziedzinie usług płatniczych.

Praktycznie brak SCA w innych sektorach niż finansowy

Warunki uznawania SUA jako SCA

- SCA wymagane na mocy:
  - prawa krajowego lub unijnego,
  - zobowiązania umownego,

- dobrowolny wniosek użytkownika,

- w odniesieniu do:
  - **minimalnych** danych **niezbędnych,**
  - świadczenia **konkretnej usługi** online,
    dla której **wymagane jest uwierzytelnienie** użytkownika.

Silne uwierzytelnienie w eIDAS 2.0 a PSD II

Silne uwierzytelnienie użytkownika – SUA

oznacza uwierzytelnianie oparte na wykorzystaniu co najmniej dwóch czynników uwierzytelniających z różnych kategorii, takich jak wiedza (coś, co tylko użytkownik wie), posiadanie (coś, co posiada tylko użytkownik) lub dziedziczenie (coś, czym użytkownik jest), które są **niezależne, w taki sposób, że naruszenie jednego nie zagraża wiarygodności pozostałych** i jest zaprojektowany w taki sposób, aby chronić poufność danych uwierzytelniających.

Silne uwierzytelnienie klienta – SCA

oznacza uwierzytelnianie w oparciu o zastosowanie co najmniej dwóch elementów należących do kategorii: wiedza (coś, co wie wyłącznie użytkownik), posiadanie (coś, co posiada wyłącznie użytkownik) i cechy klienta (coś, czym jest użytkownik), **niezależnych w tym sensie, że naruszenie jednego z nich nie osłabia wiarygodności pozostałych**, które to uwierzytelnianie jest zaprojektowane w sposób zapewniający ochronę poufności danych uwierzytelniających.

Uwierzytelnienie w eIDAS a PSD II

Uwierzytelnienie wg eIDAS

proces elektroniczny, który umożliwia identyfikację elektroniczną osoby (…), lub potwierdzenie pochodzenia oraz integralności weryfikowanych danych w postaci elektronicznej

identyfikacja elektroniczna oznacza proces stosowania danych identyfikujących osobę (…) jednoznacznie reprezentujących osobę (…)

dane identyfikujące osobę oznaczają zbiór danych, **wydany zgodnie z prawem unijnym lub krajowym**, umożliwiający ustalenie tożsamości osoby (…).

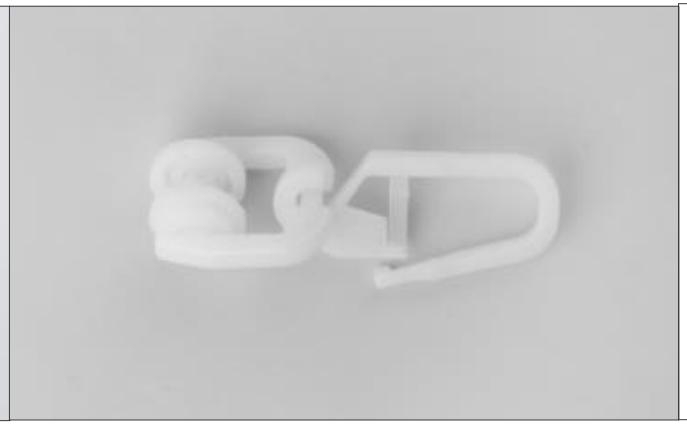
Uwierzytelnienie wg PSD II

oznacza procedurę umożliwiającą dostawcy usług płatniczych weryfikację tożsamości użytkownika usług płatniczych lub ważności stosowania konkretnego instrumentu płatniczego, **łącznie ze stosowaniem indywidualnych danych uwierzytelniających** tego użytkownika

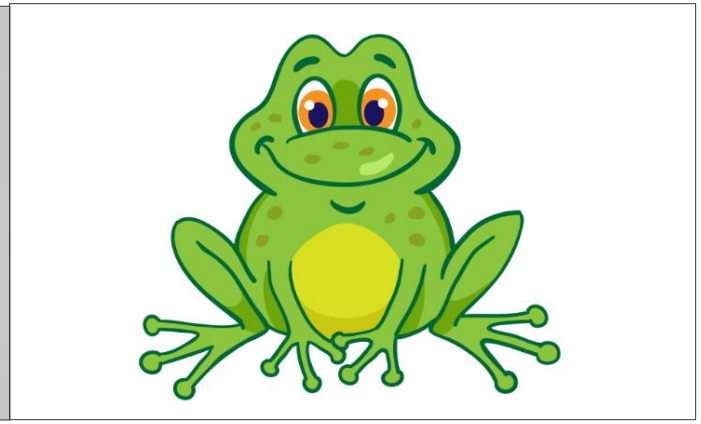
indywidualne dane uwierzytelniające oznaczają indywidualne cechy **zapewniane przez dostawcę usług płatniczych** użytkownikowi usług płatniczych do celów uwierzytelnienia.

Czy te pojęcia są tożsame?

ŻABKA



ŻABKA



ŻABKA

SILNA ŻABKA

SILNA ŻABKA

SILNA ŻABKA

Czy EPTC zapewnia silne uwierzytelnienie użytkownika – SUA?

- **Żaden przepis** eIDAS 2.0 nie stanowi, że EPTC zapewnia lub jest stosowany w sposób zapewniający silne uwierzytelnienie użytkownika.
- Spełnienie przez EPTC poziomu bezpieczeństwa high nie oznacza spełnienia wymogów SUA lub SCA.
- Definicje silnego uwierzytelnienia w eIDAS i PSD II różnią się niuansami, ale pojęcia te de facto różnią się bardzo. Odwołują się bowiem do **„uwierzytelnienia", które jest w nich bardzo odmiennie rozumiane**.
- Brak standardów, norm i aktów wykonawczych do eIDAS 2.0.
- Czy EPTC to nowy rodzaj indywidualnych danych uwierzytelniających?

2FA ≠ ≤ SUA2FA ≠ ≤ SCA SUA ≠ SCA

SUA a wymagania SCA

- Jak spełnić wymóg dynamicznego łączenia transakcji?
- Jak zapewnić wartość dowodową przy założeniu, że wydawca EPTC nie gromadzi informacji na temat korzystania z EPTC?
- Czy ASPSP ma umożliwić TPP świadczenie usług w oparciu o uwierzytelnianie stosowane w relacji między użytkownikiem a dostawcą prowadzącym rachunek?
- Czy PSP jest zobowiązany do przyjmowania zgłoszeń „utraty” EPTC?
- Czy EPTC musi być stosowany wraz z indywidualnymi danymi uwierzytelniającymi?
- Czy niedochowanie staranności przy ochronie EPTC rozszerza odpowiedzialność płatnika?
- Jak – dla EPTC – PSP zapewnią poufność i integralność indywidualnych danych uwierzytelniających użytkowników usług płatniczych(…) na wszystkich etapach uwierzytelniania?
- Czy o akceptacji EPTC za SCA decyduje niepowtarzalny i trwały identyfikator?

Powiązanie EPTC z indywidualnymi danymi uwierzytelniającymi

ROZPORZĄDZENIE 2018/389

1. Dostawcy usług płatniczych zapewniają, aby wyłącznie użytkownik usług płatniczych był w bezpieczny sposób powiązany z indywidualnymi danymi uwierzytelniającymi, urządzeniami uwierzytelniającymi i oprogramowaniem uwierzytelniającym.
2. Do powiązania tożsamości użytkownika usług płatniczych z indywidualnymi danymi uwierzytelniającymi, urządzeniami i oprogramowaniem uwierzytelniającym (…) dochodzi w bezpiecznym środowisku, za które odpowiedzialność ponosi dostawca usług płatniczych (…).
3. Powiązanie tożsamości użytkownika usług płatniczych z indywidualnymi danymi uwierzytelniającymi, urządzeniami uwierzytelniającymi lub oprogramowaniem uwierzytelniającym za pomocą kanału zdalnego przeprowadza się z zastosowaniem SCA.
4. PSP zapewnia, aby w przypadku gdy indywidualne dane uwierzytelniające, urządzenia uwierzytelniające lub oprogramowanie uwierzytelniające wymagają aktywacji przed ich pierwszym użyciem, aktywacja miała miejsce w bezpiecznym środowisku i odbywała się zgodnie z procedurami powiązania (zastosowanie SCA).

Co do zasady klient posługuje się jednym mechanizmem SCA

Ryzyka związane z uznawaniem SUA jak SCA

- Jak coś jest do wszystkiego, to jest do niczego.
- Brak SLA i brak odpowiedzialności wydawcy EPTC.
- Brak kontroli nad mechanizmem uwierzytelnienia.
- Brak wpływu na urządzenie wielofunkcyjne.
- Ograniczenie mechanizmów minimalizujących ryzyko.
- Zewnętrzne standardy komunikacyjne i luki bezpieczeństwa.
- Ograniczone bezpieczeństwo dowodowe.
- Rezygnacja z SCA i obniżenie bezpieczeństwa klientów.

Ryzyka użytkownika EPTC

- Brak świadomości zastosowania EPTC i ryzyk z tym związanych.
- Wiele portfeli na te same dane. Brak ochrony.
- Brak możliwości wyłączenia się z EPTC.
- Utrata EPTC wymaga wydania nowego EPTC i powtórzenia procesu powiązania u PSP – wizyta w dwóch okienkach.
- Ułatwienie podszycia się pod cudzą tożsamość i nowy typ oszustw.
- Obniżenie bezpieczeństwa.
- Zwiększone ryzyko w przypadku współdzielenia urządzeń.

Robert Podpłoński
robert.podplonski@kir.pl