SOŁTYSIŃSKI KAWECKI SZLĘZAK

XIII Kongres Prawa Bankowego
Warszawa, 10 czerwca 2026 r.

Silne uwierzytelnianie klienta z wykorzystaniem EUDI na gruncie PSR

dr Michał Mostowik

Silne uwierzytelnianie klienta (SCA) w PSR

'**authentication**' means a procedure which allows the payment service provider to **verify the identity of a payment service user** or the validity of the use of a specific payment instrument, including the use of the user's personalised security credentials

'**strong customer authentication**' means an **authentication** which is based on the use of **two or more elements** categorised as **knowledge** (something only the user knows), **possession** (something only the user possesses) and **inherence** (something the user is) that are independent, in that the breach of one does not compromise the reliability of the others, and is designed in such a way as to protect the confidentiality of the authentication data

The two or more elements [...], on which strong customer authentication shall be based need to belong to **different categories**, except for the category inherence [...]

1. **Obowiązek SCA** w przypadku gdy płatnik:
   - uzyskuje dostęp do swojego rachunku w trybie on-line
   - składa zlecenie płatnicze na transakcję elektroniczną
   - przeprowadza za pomocą kanału zdalnego inną czynność, która może wiązać się z ryzykiem oszustwa związanego z wykonywanymi usługami płatniczymi lub innych nadużyć
2. Utrzymany wymóg **dynamic linking** (w tym dla przypadku inicjowania elektronicznej transakcji płatniczej za pomocą kanału zdalnego)
3. **Zwolnienia z obowiązku stosowania SCA w ramach RTS** powinny opierać się na:
   - poziomie ryzyka oszustwa związanego ze świadczoną usługą,
   - kwocie transakcji, częstotliwości lub obu czynnikach,
   - kanale wykorzystywanym do wykonania transakcji,
   - ocenie czy płatnik jest konsumentem, czy nie.

Rozporządzenie eIDAS 2.0

- **Nowelizacja rozporządzenia eIDAS z 2014 r.**
  - ✓ Rozpowszechnienie i standaryzacja usług cyfrowej tożsamości w UE
  - ✓ Przynajmniej jeden EUDI Wallet (Europejski Portfel Tożsamości Cyfrowej) w każdym państwie UE
  - ✓ Nacisk na ochronę danych, funkcjonalności i dostępność portfela
  - ✓ **Rejestracja strony ufającej w państwie siedziby**

- W Polsce – nowa aplikacja **mObywatel Europa** jako przedłużenie prac legislacyjnych i informatycznych w zakresie aplikacji mObywatel

- **Ważne daty:**
  - ✓ Udostępnienie EUDI Wallet – **24 grudnia 2026 r.**
  - ✓ Obowiązek akceptacji dla banków – **24 grudnia 2027 r.**

Obowiązek akceptacji EUDI na potrzeby SCA

Art. 5f.2 eIDAS

W przypadku gdy prywatne strony ufające, które świadczą usługi - z wyjątkiem mikroprzedsiębiorstw i małych przedsiębiorstw zdefiniowanych w art. 2 załącznika do zalecenia Komisji 2003/361/WE – **zobowiązane są na podstawie prawa Unii lub prawa krajowego do stosowania silnego uwierzytelnienia użytkownika do celów identyfikacji elektronicznej** lub w przypadku gdy silne uwierzytelnienie użytkownika do celów identyfikacji elektronicznej wymagane jest na podstawie zobowiązania umownego, w tym w obszarach transportu, energii, bankowości, usług finansowych, zabezpieczenia społecznego, zdrowia, wody pitnej, usług pocztowych, infrastruktury cyfrowej, edukacji lub telekomunikacji, te prywatne strony ufające, nie później niż 36 miesięcy od dnia wejścia w życie aktów wykonawczych, o których mowa w art. 5a ust. 23 i art. 5c ust. 6, oraz wyłącznie na dobrowolny wniosek użytkownika, również **akceptują europejskie portfele tożsamości cyfrowej**, które są zapewniane zgodnie z niniejszym rozporządzeniem.

Art. 3.51 eIDAS

"**silne uwierzytelnienie użytkownika**" oznacza uwierzytelnienie w oparciu o zastosowanie co najmniej dwóch składników uwierzytelniania należących do różnych kategorii: **wiedza**, czyli coś, co wie wyłącznie użytkownik, **posiadanie**, czyli coś, co posiada wyłącznie użytkownik, albo **cecha** użytkownika, czyli coś, czym jest użytkownik, **niezależnych** w tym znaczeniu, że naruszenie jednego z nich nie osłabia wiarygodności pozostałych, które to uwierzytelnienie jest zaprojektowane, tak aby zapewniać **ochronę poufności danych uwierzytelniających**

Procesy do obsłużenia z wykorzystaniem EUDI (przykłady)

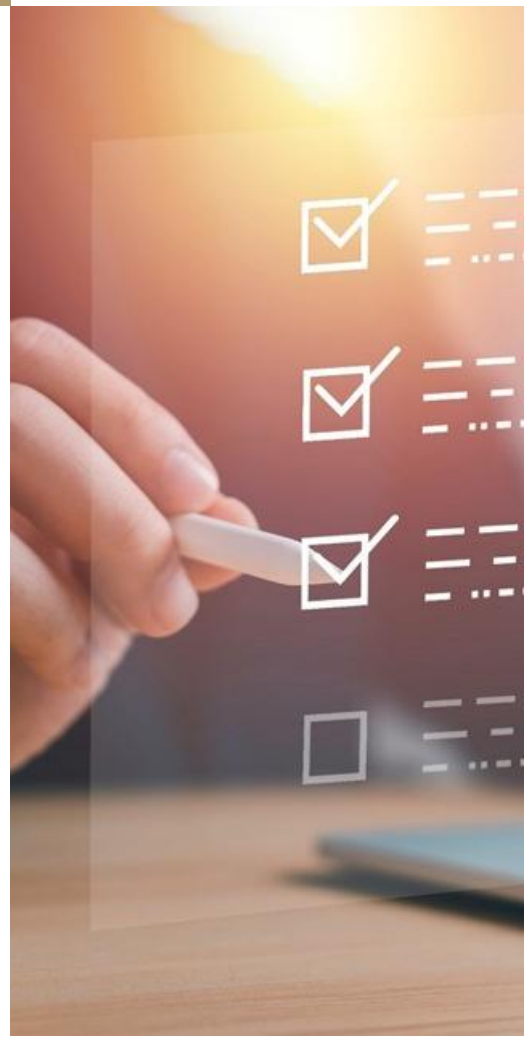
Dostęp do rachunku w trybie online	Zlecenie elektronicznej transakcji	Czynność z ryzykiem oszustwa
• Logowanie do bankowości internetowej • Logowanie do aplikacji mobilnej banku • Dostęp do rachunku przez dostawcę usług informacji o rachunku (AISP) • Dostęp do rachunku przez korporacyjny portal bankowości elektronicznej • Sprawdzenie salda w bankomacie (ATM)	• Zlecenie płatnicze przez bankowość internetową • Zlecenie płatnicze przez aplikację mobilną banku • Transakcja kartą płatniczą w fizycznym punkcie sprzedaży (POS) • Transakcja zbliżeniowa kartą lub telefonem (NFC) przy POS • Transakcja kartą w środowisku e-commerce (CNP – Card Not Present) • Płatność z użyciem kodu BLIK • Zainicjowanie transakcji przez PISP (poprzez API) • Transakcja w bankomacie (ATM) • Płatność subskrypcyjna (MIT – Merchant Initiated Transaction)	• *Tokenizacja instrumentu płatniczego (dodanie karty do walleta AP/GP)* • *Podwyższenie limitów transakcyjnych* • *Zmiana hasła lub kodu PIN do bankowości internetowej/aplikacji* • Zmiana danych kontaktowych (np. numer telefonu do OTP/SMS, adres do wysyłki karty) • Dodanie nowego urządzenia zaufanego (trusted device) • Aktywacja aplikacji mobilnej na nowym urządzeniu • Dodanie nowego odbiorcy zaufanego • Zmiana metody uwierzytelnienia • Odblokowanie zablokowanej karty płatniczej przez kanał zdalny • Zastrzeżenie i zamówienie nowej karty płatniczej online

Brak integracji z wydawcą portfela?

- Efektywna integracja z wydawcą – warunek *de facto* akceptacji EUDI
- Rola wydawcy EUDI – weryfikacja sprawdzenia tożsamości
- Obowiązek rejestracji zgodnie z eIDAS – „efektywny kosztowo i proporcjonalny względem zagrożeń”

Art. 87.1 PSR: The payment service provider of the payer shall enter into an outsourcing agreement with the technical service provider in case that technical service provider is providing and verifying the elements of strong customer authentication

Art. 58 PSR: Technical service providers and operators of payment schemes that either provide services to the payee, or to the payment service provider of the payee or of the payer, shall be liable for direct financial damage caused to the payee, to the payment service provider of the payee or of the payer for, and proportionate to, their failure, within the remit of their contractual relationship, and not exceeding the amount of the transaction in question to provide the services that are necessary to enable the application of strong customer authentication.



SCA poprzez usługę poświadczania atrybutów?

- "**atrybut**" oznacza cechę charakterystyczną, właściwość, prawo lub zezwolenie osoby fizycznej lub prawnej lub przedmiotu;
- "**elektroniczne poświadczenie atrybutów**" oznacza poświadczenie w postaci elektronicznej, które umożliwia uwierzytelnienie atrybutów;
- **bezpieczne żądanie, otrzymywanie, wybieranie, łączenie, przechowywanie, usuwanie, udostępnianie i prezentację - pod wyłączną kontrolą użytkownika - danych identyfikujących osobę** oraz, w stosownych przypadkach, **w połączeniu z elektronicznymi poświadczeniami atrybutów, uwierzytelnianie wobec stron ufających** w trybie online oraz, w stosownych przypadkach, w trybie offline, w celu uzyskania dostępu do usług publicznych i prywatnych, przy jednoczesnym zapewnieniu możliwości selektywnego ujawniania danych

Art. 2.2 eIDAS: Niniejsze rozporządzenie nie ma zastosowania do świadczenia usług zaufania wykorzystywanych wyłącznie w obrębie zamkniętych systemów wynikających z prawa krajowego lub z porozumień zawartych przez określoną grupę uczestników.

SCA a transakcje nieautoryzowane: odpowiedzialność

PSD2	UUP	PSR
Art. 74. 2	**Art. 46.4a**	**Art. 60.2**
Where the payer's payment service provider does not require strong customer authentication, **the payer shall not bear any financial losses unless the payer has acted fraudulently**. Where the payee or the payment service provider of the payee fails to accept strong customer authentication, it shall refund the financial damage caused to the payer's payment service provider.	W przypadku gdy dostawca płatnika nie wymaga silnego uwierzytelniania użytkownika, **płatnik nie ponosi odpowiedzialności za nieautoryzowane transakcje płatnicze, chyba że działał umyślnie**. W przypadku gdy odbiorca lub dostawca odbiorcy nie akceptują silnego uwierzytelniania użytkownika, odpowiadają oni za szkody poniesione przez dostawcę płatnika.	Where the payer's payment service provider fails to fulfil the obligation to require strong customer authentication set out in Article 85, **the payer shall not bear any financial losses unless the payer has acted fraudulently. The payer shall not bear any financial losses also where either the payment service provider of the payer or of the payee applies an exemption from the application of strong customer authentication**.

SCA a transakcje nieautoryzowane: ciężar dowodu

PSD2	UUP	PSR
Art. 72 1. […] it is for the payment service provider to prove that the payment transaction was **authenticated**, accurately recorded, entered in the accounts and not affected by a technical breakdown or some other deficiency of the service provided by the payment service provider. 2. […] the use of a payment instrument recorded by the payment service provider, including the payment initiation service provider as appropriate, shall in itself **not necessarily be** sufficient to prove either that the payment transaction was authorised by the payer or that the payer acted fraudulently or failed with intent or gross negligence to fulfil one or more of the obligations under Article 69.	**Art. 45** 1. […] Na dostawcy użytkownika spoczywa ciężar udowodnienia, że transakcja płatnicza została **autoryzowana** i prawidłowo zapisana w systemie służącym do obsługi transakcji płatniczych dostawcy oraz że nie miała na nią wpływu awaria techniczna ani innego rodzaju usterka związana z usługą płatniczą świadczoną przez tego dostawcę […]. 2. […] Wykazanie przez dostawcę zarejestrowanego użycia instrumentu płatniczego **nie jest wystarczające** do udowodnienia, że transakcja płatnicza została przez użytkownika autoryzowana albo że płatnik umyślnie albo wskutek rażącego niedbalstwa doprowadził do nieautoryzowanej transakcji płatniczej albo umyślnie albo wskutek rażącego niedbalstwa dopuścił się naruszenia co najmniej jednego z obowiązków, o których mowa w art. 42.	**Art. 55** 1. […] the burden shall be on the payment service provider to prove that the payment transaction was **authorised**, accurately recorded, entered in the accounts and not affected by a technical breakdown or some other deficiency of the service provided by the payment service provider. […] the fact that the payment transaction was authenticated, including where applicable, via strong customer authentication, accurately recorded, entered in the accounts and not affected by a technical breakdown or some other deficiency of the service provided, shall in itself **not necessarily be sufficient** to prove either that the payment transaction was authorised by the payer or that the payer acted fraudulently or failed with intent or gross negligence to fulfil one or more of the obligations under Article 52.

EUDI Wallet – całe SCA czy jeden element?

PSR	eIDAS
Art. 3.35 PSR '**strong customer authentication**' means an authentication which is based on the use of two or more elements categorised as **knowledge** (something only the user knows), **possession** (something only the user possesses) and **inherence** (something the user is) that are independent, in that the breach of one does not compromise the reliability of the others, and is designed in such a way as to protect the confidentiality of the authentication data	**Art. 5a.4.a** Europejskie portfele tożsamości cyfrowej muszą umożliwiać użytkownikowi, w sposób przyjazny, przejrzysty i identyfikowalny dla użytkownika [...], w stosownych przypadkach, w połączeniu z elektronicznymi poświadczeniami atrybutów, uwierzytelnianie wobec stron ufających w trybie online oraz, w stosownych przypadkach, w trybie offline, w celu uzyskania dostępu do usług publicznych i prywatnych, przy jednoczesnym zapewnieniu możliwości selektywnego ujawniania danych; **Art. 5a.5.d** Europejskie portfele tożsamości cyfrowej [...] muszą spełniać wymogi określone w art. 8 w odniesieniu do wysokiego poziomu bezpieczeństwa, w szczególności w zakresie wymogów dotyczących potwierdzania i weryfikacji tożsamości, zarządzania środkami identyfikacji elektronicznej oraz uwierzytelniania; **Art. 5a.11** Europejskie portfele tożsamości cyfrowej zapewnia się w ramach systemu identyfikacji elektronicznej, na wysokim poziomie bezpieczeństwa.

Od średniego wzwyż – **wymóg 2FA**

Czy RTS-y to WD-40 regulacji sektora finansowego?

Art. 89.1 PSR

The EBA shall develop **draft regulatory technical standards** which shall specify:

(a) the requirements of strong customer authentication as referred to in Article 85;

(b) the exemptions from the application of Article 85(1), (8) and (9), based on the criteria laid down in Article 85(11);

[...]

Art. 89.3 PSR

In accordance with Article 10 of Regulation (EU) No 1093/2010, the EBA shall review and, if appropriate, update the regulatory technical standards on a regular basis in order, inter alia, to take account of innovation and technological developments, and the provisions of Chapter II of Regulation (EU) 2022/2554, and the **European Digital Identity Wallets** implemented under Regulation (EU) No 910/2014.

Dziękuję za uwagę!

dr Michał Mostowik

Senior Counsel

+48 22 608 72 69
+48 698 173 297
michal.mostowik@skslegal.pl