



eIDAS – uwierzytelnienie a podpisy elektroniczne

126873

Plan wykładu

- ▶ Uwierzytelnianie
- ▶ Rodzaje uwierzytelniania
- ▶ Podpis elektroniczny
- ▶ Zastosowania podpisu elektronicznego
- ▶ eIDAS

Uwierzytelnianie – co to jest?

- ▶ Proces polegający na potwierdzeniu zadeklarowanej tożsamości podmiotu biorącego udział w procesie komunikacji.
- ▶ Celem uwierzytelniania jest uzyskanie określonego poziomu pewności, że dany podmiot jest w rzeczywistości tym, za który się podaje

Źródło: <http://ii.uwb.edu.pl/rudnicki/wp-content/uploads/2016/02/21.pdf>

Uwierzytelnianie – klasyfikacja

- ▶ Jedną z funkcjonalnych klasyfikacji uwierzytelniania jest podział na metody wykorzystujące:
 - ▶ coś co wiesz
 - ▶ coś co masz
 - ▶ coś czym jesteś

Uwierzytelnianie – poziomy wiarygodności

- ▶ Poziom wiarygodności określa stopień zaufania dopuszczalny i akceptowalny biorąc pod uwagę straty, jakie mogą być poniesione w przypadku błędnego uwierzytelnienia.
- ▶ Poziomy:
 - ▶ LoA 1 – minimalna wiarygodność lub jej brak - serwisy internetowe;
 - ▶ LoA 2 – ograniczona wiarygodność deklarowanej tożsamości - serwis instytucji ubezpieczeniowej;
 - ▶ LoA 3 – wysoka wiarygodność deklarowanej tożsamości - dostęp do rachunku inwestycyjnego;
 - ▶ LoA 4 – bardzo wysoka wiarygodność deklarowanej tożsamości - serwis umożliwiający aptekarzowi wydanie leków.

Rodzaje uwierzytelniania

- ▶ Podział ze względu na stronę uwierzytelniania:
 - ▶ jednokierunkowe;
 - ▶ dwukierunkowe;
 - ▶ z udziałem zaufanej trzeciej strony.
- ▶ Podział ze względu na ilość etapów:
 - ▶ jednoskładnikowe;
 - ▶ dwuskładnikowe.

Rodzaje uwierzytelniania – jednokierunkowe

- ▶ Polega na uwierzytelnieniu jednego podmiotu (uwierzytelnianego), np. klienta aplikacji, wobec drugiego (uwierzytelniającego) – serwera.
- ▶ Jest to prosta weryfikacja przekazanych danych uwierzytelniających np. hasło.



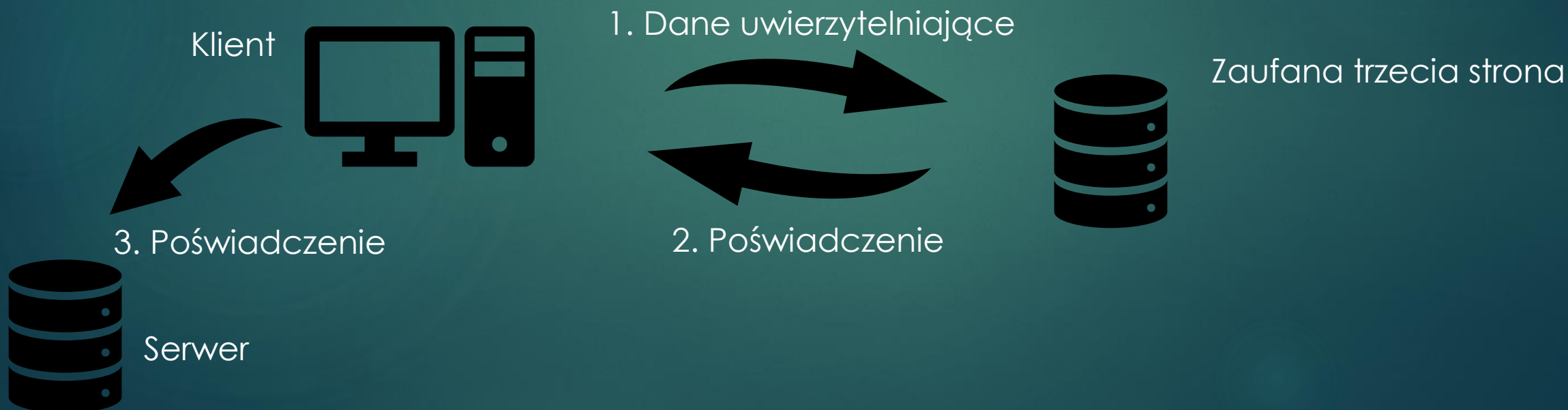
Rodzaje uwierzytelniania – dwukierunkowe

- ▶ Polega na kolejnym lub jednoczesnym uwierzytelnieniu obu podmiotów (które są wzajemnie i naprzemiennie uwierzytelnianym oraz uwierzytelniającym).
- ▶ Jeżeli wzajemne uwierzytelnianie następuje sekwencyjnie mówimy o uwierzytelnianiu dwuetapowym, natomiast jednoczesne uwierzytelnienie obu stron nazywamy jednoetapowym.



Rodzaje uwierzytelniania – z udziałem zaufanej trzeciej strony

- ▶ Włącza w proces uwierzytelniania trzecią zaufaną stronę, która bierze na siebie ciężar weryfikacji danych uwierzytelniających podmiotu uwierzytelnianego. Po pomyślnej weryfikacji podmiot uwierzytelniany otrzymuje poświadczenie, które następnie przedstawia zarządcy zasobów, do którego dostępu żąda



Rodzaje uwierzytelniania – jednoskładnikowe

- ▶ Polega na uwierzytelnianiu użytkownika za pomocą tylko jednego mechanizmu np. hasła.
- ▶ Nie ma dodatkowych zabezpieczeń.

Rodzaje uwierzytelniania – dwuskładnikowe

- ▶ Dwuskładnikowe uwierzytelnianie polega na wprowadzeniu przez właściciela usługi dodatkowego, opcjonalnego etapu podczas procesu uzyskiwania dostępu do konta.
- ▶ Po jego włączeniu, logując się do serwisu, oprócz hasła będziemy musieli wpisywać także kod wygenerowany przez token - może nim być nasz smartfon albo zdalny serwer, który przyśle nam kod za pomocą SMS-a.

Metody uwierzytelniania

W zależności od kanału komunikacyjnego stosuje się różne metody i protokoły uwierzytelniania.

- ▶ w stosunku do dokumentów papierowych:
 - ▶ podpisy,
 - ▶ pieczęcie,
 - ▶ parafowanie,
 - ▶ znak wodny (metody),
 - ▶ poświadczenie notarialne (protokół);

Metody uwierzytelniania

- ▶ w stosunku do osób i innych istot żywych:
 - ▶ zabezpieczenie biometryczne,
 - ▶ dokument tożsamości,
 - ▶ hasło,
 - ▶ karta elektroniczna (smart card),
 - ▶ biochip,
 - ▶ token (generator kodów);

Metody uwierzytelniania

- ▶ w stosunku do wiadomości i dokumentów elektronicznych:
 - ▶ podpis cyfrowy,
 - ▶ kod uwierzytelniania wiadomości (ang. message authentication code);
- ▶ w stosunku do podmiotów w komunikacji elektronicznej:
 - ▶ metody oparte na dowodzie posiadania hasła lub klucza prywatnego,
 - ▶ dowód z wiedzą zerową,
 - ▶ hasło jednorazowe;

Podpis elektroniczny – co to jest?

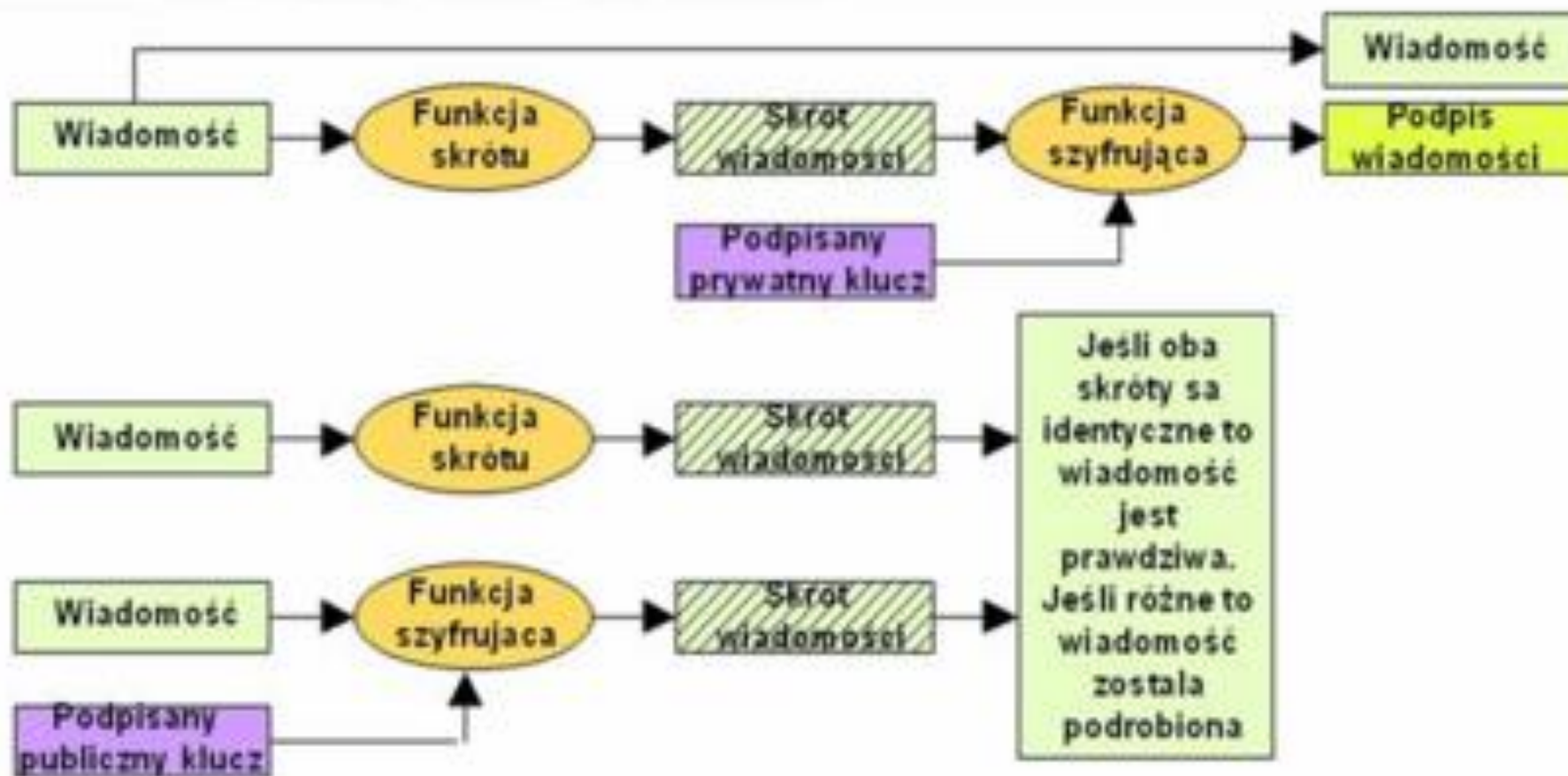
- ▶ Są to dane w postaci elektronicznej, które są dołączone lub logicznie powiązane z innymi danymi w postaci elektronicznej, i które użyte są przez podpisującego jako podpis.
- ▶ Jest odpowiednikiem podpisu odręcznego w procesie elektronicznej wymiany danych.
- ▶ Dane które użyte są przez podpisującego jako podpis, ale jednocześnie są dołączone lub logicznie powiązane z innymi danymi w postaci elektronicznej.

([Dz.U.U.E.910/2014](#), [Dz.U.2019.162](#))

Podpis elektroniczny – procedura składania podpisu

- ▶ Użycie podpisu następuje poprzez wydanie komputerowi polecenia złożenia podpisu elektronicznego, co prowadzi do obliczania skrótu podpisywanego dokumentu. Jest on określany indywidualnie dla danego dokumentu.
- ▶ Następnie przy użyciu otrzymanego oprogramowania następuje szyfrowanie kluczem prywatnym.
- ▶ Dokument z bezpiecznym podpisem elektronicznym przesyłany jest do adresata.

Podpis elektroniczny – procedura składania podpisu



Podpis elektroniczny – funkcje podpisu

- ▶ Identyfikacja:
 - ▶ podpisy i certyfikaty służą w tym przypadku tylko do uwierzytelnienia w systemie i identyfikacji osoby starającej się o dostęp, np. do serwera, bazy danych;
- ▶ Uwierzytelnienie:
 - ▶ podpisy są składane całkowicie automatycznie bez świadomości i ingerencji osoby składającej i nie służą do składania oświadczeń woli;
- ▶ Oświadczenie wiedzy:
 - ▶ nie służą do składania oświadczeń woli;
- ▶ Oświadczenie woli:
 - ▶ stanowią dowód złożenia oświadczenia woli;

Zastosowania podpisu elektronicznego – B2A

- ▶ Relacje z administracją i urzędami:
 - ▶ Zakład Ubezpieczeń Społecznych – e-korespondencja z ZUS jest możliwa wyłącznie z użyciem podpisu elektronicznego, który jest potrzebny do przekazania dokumentów w formie elektronicznej w ramach aplikacji Płatnik.
 - ▶ e-PUAP – szybsze uzyskanie dostępu do systemu e-PUAP dzięki zastosowaniu podpisu elektronicznego do potwierdzenia danych użytkownika
 - ▶ Krajowy Rejestr Sądowy – przesyłanie wniosków rejestrowych i aktualizacja informacji możliwa jest drogą elektroniczną wyłącznie przy użyciu podpisu elektronicznego, który jest wymagany do rejestracji w platformie e-KRS.

Zastosowania podpisu elektronicznego – B2B

- ▶ Relacje biznesowe:

- ▶ Zdalne zawieranie umów cywilno-prawnych. Podpis elektroniczny jest równoważny odręcznej sygnaturze dlatego umożliwia podpisywanie wszelkiego rodzaju umów między przedsiębiorstwami.
- ▶ Udział w zabezpieczonych aukcjach i przetargach elektronicznych organizowanych za pośrednictwem odpowiednich platform internetowych. W przypadku zamówień publicznych istnieje obowiązek złożenia zgłoszenia opatrzonego bezpiecznym podpisem elektronicznym.

Zastosowania podpisu elektronicznego – B2C

- ▶ Kontakty biznesu z klientami:
 - ▶ E-faktury – wygodne przesyłanie faktur elektronicznych drogą online. Obowiązujące prawo wymaga odpowiedniego zapewnienia wiarygodności e-faktur, które można zapewnić poprzez potwierdzenie dokumentu podpisem elektronicznym.
 - ▶ Wiarygodna korespondencja elektroniczna z klientami dzięki podpisywaniu dokumentów i korespondencji elektronicznej.

eIDAS – co to jest?

- ▶ Przepisy Electronic Identification and Trust Services Regulation (eIDAS, 910/2014/EC) to zunifikowane, standardowe reguły mające zastosowanie we wszystkich państwach członkowskich Unii Europejskiej, które zapewniają spójną strukturę prawną przyjmowania tożsamości i podpisów elektronicznych. Wprowadzono w nich również pieczętki cyfrowe dla firm.
- ▶ W projekcie eIDAS oddzielono funkcję „identyfikacji” do osobnej kategorii, a pozostałe rodzaje podpisów elektronicznych podzielono na „podpis elektroniczny”, który jest zawsze składany przez osobę fizyczną i „pieczęć elektroniczną”, która jest składana przez osobę prawną („automatycznie” przez sprzęt i/lub oprogramowanie)

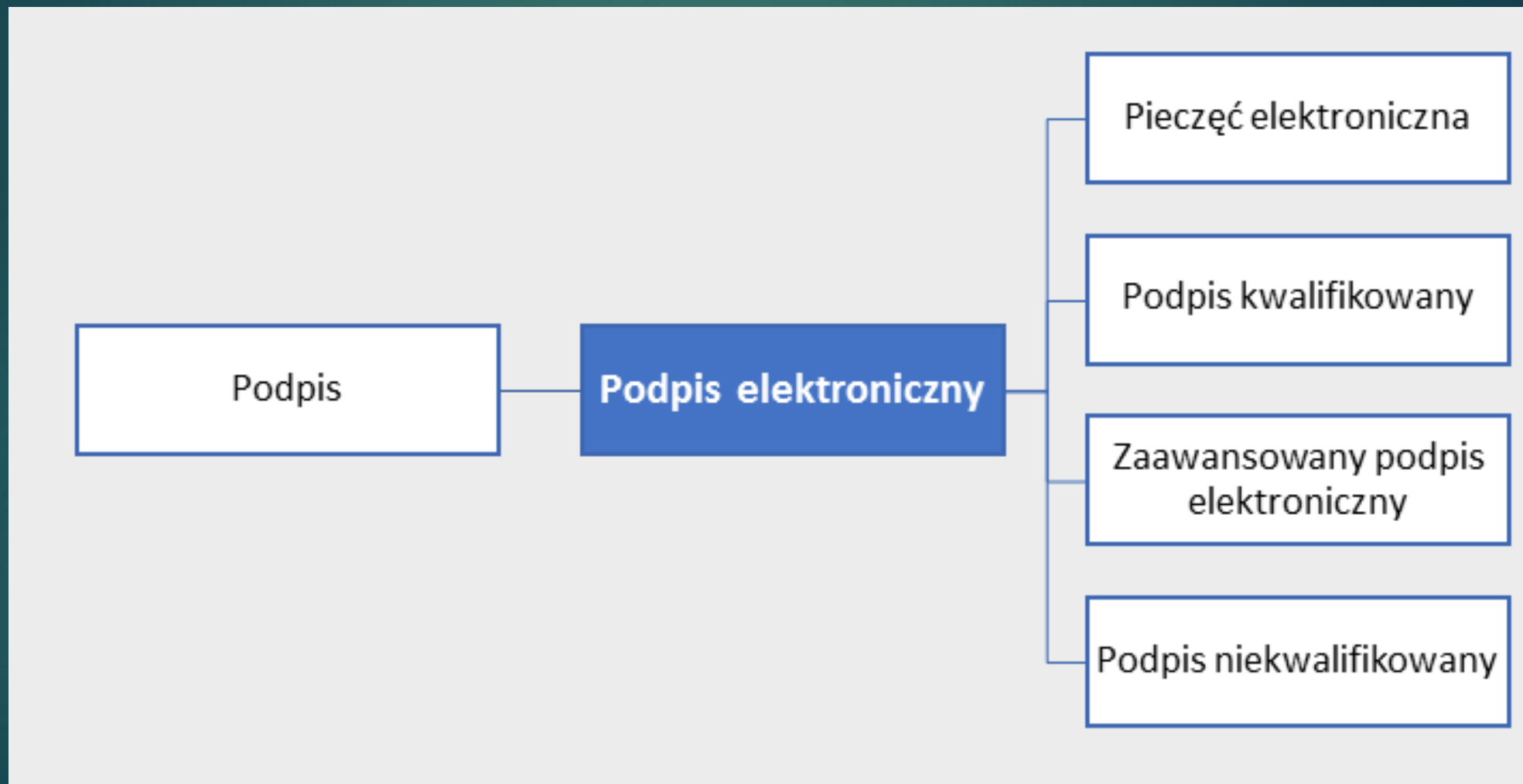
Definicje wg eIDAS

- ▶ **identyfikacja elektroniczna** – oznacza proces używania danych identyfikujących osobę w formie elektronicznej, w sposób jednoznaczny reprezentujący osobę fizyczną lub prawną;
- ▶ **uwierzytelnianie** – oznacza proces elektroniczny, który umożliwia weryfikację identyfikacji elektronicznej osoby fizycznej lub prawnej lub pochodzenia i integralności danych elektronicznych;
- ▶ **podpis elektroniczny** – oznacza dane w formie elektronicznej dodane do innych danych elektronicznych lub logicznie z nimi powiązane i służące podpisującemu do składania podpisu;

eIDAS – środki identyfikacji elektronicznej

- ▶ **środek identyfikacji elektronicznej** to materialna lub niematerialna jednostka zawierająca dane identyfikujące osobę i używana do celów uwierzytelniania dla usługi online.
- ▶ musi zostać wydany w ramach systemu identyfikacji elektronicznej wymienionego w wykazie opublikowanym przez Komisję Europejską
- ▶ musi odpowiadać poziomowi bezpieczeństwa równemu lub wyższemu od poziomu bezpieczeństwa wymaganego przez odpowiedni podmiot sektora publicznego na potrzeby dostępu do tej usługi online

eIDAS – rodzaje podpisów

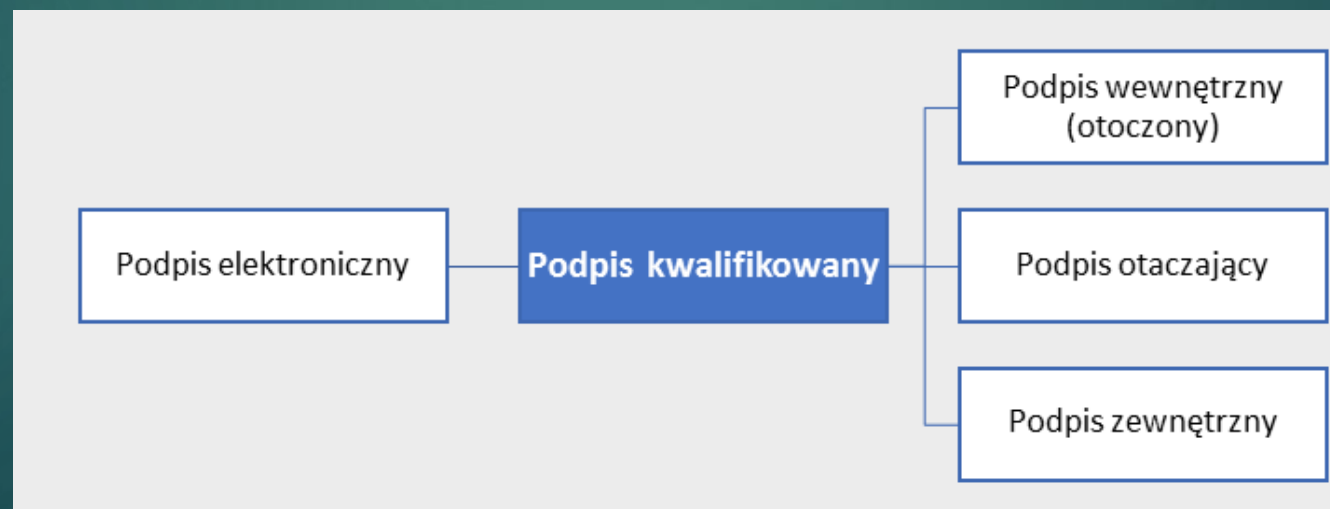


eIDAS – Pieczęć elektroniczna

- ▶ W sensie technicznym niczym nie różni się w działaniu i sposobie generacji od podpisu elektronicznego poza tym, że nie stawia jej człowiek, lecz system informatyczny, w wyniku jakiegoś wcześniej zdefiniowanego zdarzenia.

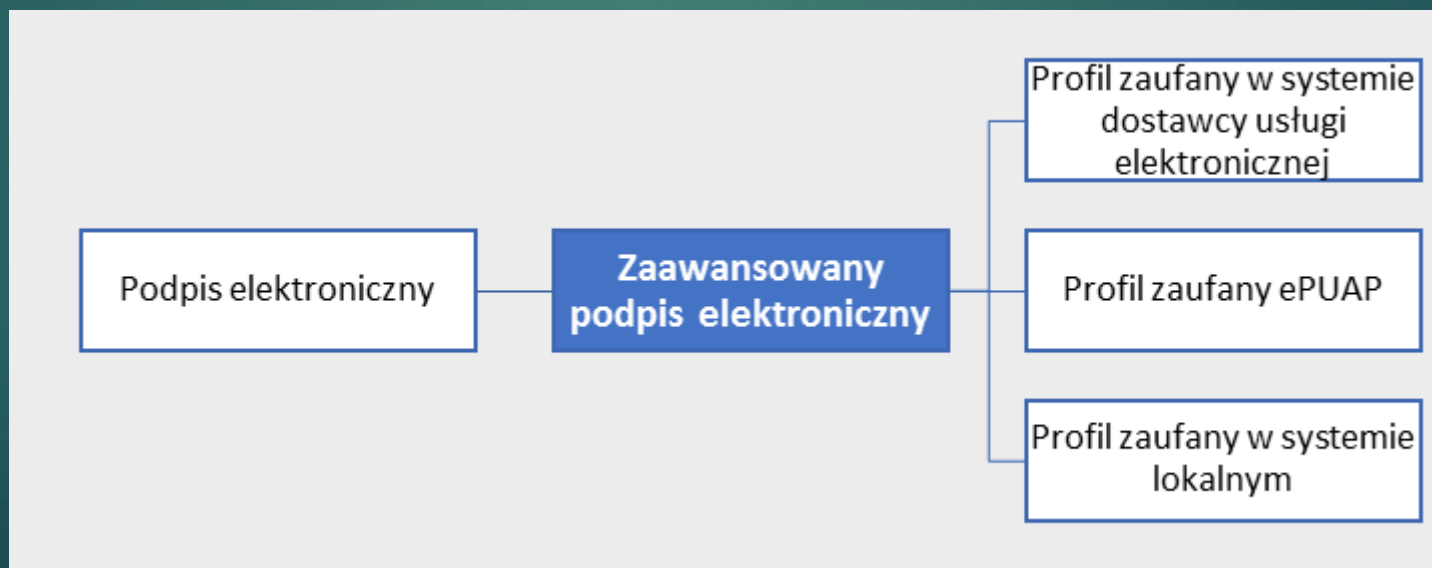
eIDAS – Podpis kwalifikowany

- ▶ Jest to podpis, który w dawniejszych regulacjach prawnych nazywany był bezpiecznym podpisem elektronicznym weryfikowanym za pomocą ważnego kwalifikowanego certyfikatu.
- ▶ Teraz jest to zaawansowany podpis elektroniczny, który jest składany za pomocą kwalifikowanego urządzenia do składania podpisu elektronicznego i który opiera się na kwalifikowanym certyfikacie podpisu elektronicznego.



eIDAS – Zaawansowany podpis elektroniczny

- ▶ Jest składany przy użyciu danych służących do składania podpisu elektronicznego, których podpisujący może, z dużą dozą pewności, użyć pod wyłączną swoją kontrolą.
- ▶ Jest powiązany z danymi podpisanymi w taki sposób, że każda późniejsza zmiana danych jest rozpoznawalna.



eIDAS – Podpis niekwalifikowany

- ▶ Handlowa nazwa podpisu elektronicznego służącego do sygnowania różnych dokumentów mniejszego znaczenia niż podpis kwalifikowany.
- ▶ Potoczna nazwa każdego podpisu elektronicznego innego niż kwalifikowany.