# E-PODRĘCZNIK

## Vademecum


Streszczenie

Vademecum ma stanowić pomoc w rozwiązywaniu merytorycznych i technicznych problemów związanych z komunikacją elektroniczną, przesyłaniem i uwierzytelnianiem dokumentów w postaci elektronicznej i papierowej, a także z wykorzystywaniem elektronicznych usług administracji publicznej.



Kajetan Wojsyk

# Spis treści:

Motto:

„Jeśli nie znasz celu, zajdziesz gdzieś indziej…"

# Od autora

Budowa **e-administracji** trwa już dziesiątki lat. Trudno się oprzeć wrażeniu, że usiłujemy osiągnąć cel, którego nie potrafimy dokładnie zdefiniować, a tym samym osiągnąć. To, że nie potrafimy osiągnąć znaczniejszej poprawy jakości naszego życia dzięki wykorzystywaniu informatyki, mając wszelkie po temu możliwości, wydaje się niezrozumiałe. Stosunkowo nieliczne sukcesy pojedynczych podmiotów, które wdrożyły i skutecznie wykorzystują **systemy teleinformatyczne** są dowodem, że takie systemy daje się budować. Jednak - mimo iż potrafiliśmy zbudować odrębne, silosowe rozwiązania, nie potrafiliśmy ich połączyć w większą całość. Aktualnie obowiązujące prawo - rozporządzenie Rady Ministrów z dnia 12 kwietnia 2012 r w sprawie **Krajowych Ram Interoperacyjności**, **minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej** oraz **minimalnych wymagań dla systemów teleinformatycznych** (dalej zwane RozpKRI) umożliwia **interoperacyjność** systemów Problemy pojawiają się na styku prawa, mającego głębokie, historyczne zakorzenienie w posługiwaniu się **dokumentami papierowymi**, oraz współczesnych technologii cyfrowych, umożliwiających posługiwanie się **dokumentami elektronicznymi**. Zderzenie tych dwóch technicznie różnych „światów" stwarza sytuacje, w których administratywiści (ale nie tylko oni) stają często w obliczu podjęcia decyzji bez poczucia **bezpieczeństwa prawnego**, bez przekonania, że przyjmowany **dokument** jest wiarygodny, **autentyczny**, że może być silnym i **niezaprzeczalnym dowodem** w sprawie.

Niniejszy e-podręcznik zdecydowanie nie stanowi odpowiedzi na wątpliwości natury prawnej – gdyż będą one istniały tak długo, jak długo będziemy mieli do czynienia z **prawem** pełnym luk i nieprecyzyjnych sformułowań wynikających z różnych przyczyn. Prawo – z uwagi na długotrwałe procesy jego stanowienia – nigdy nie nadąży za postępem technicznym, a więc w sposób naturalny zawsze będzie hamowało proces usprawniania funkcjonowania administracji; z drugiej jednak strony funkcjonowanie administracji bez podstaw prawnych co do zasady jest niedopuszczalne.

Zawarte w niniejszym e-podręczniku odpowiedzi na pytania natury technicznej powinny pozwolić na uporanie się ze zdecydowaną większością problemów dotyczących dokumentów w **postaci elektronicznej**, problemów związanych z **konwersją** ***formy*** i ***postaci*** oraz rozpoznawaniem obecności **podpisów elektronicznych** i ich rodzajów

# Wstęp

W celu ułatwienia pracownikom e-administracji rozstrzyganie pojedynczych, szczególnych przypadków dokumentów elektronicznych (lub tylko plików, co do których jeszcze nie wiadomo, czy można je zakwalifikować do grupy dokumentów) proponuje się stosowanie pewnej procedury, w wyniku której rozstrzygnięcie takie powinno być łatwiejsze. Procedura polega przejściu przez ścieżkę decyzyjną mającą strukturę drzewa, którego korzeniem jest e-usługa, a głównymi gałęziami „dokument" i „podpis" Elementy „dokumentu" oraz „podpisu" są opisane w poszczególnych punktach. Jeśli otrzymany plik będzie spełniał kryteria dokumentu, będzie mógł być jako taki traktowany Jeśli nie – będzie musiał być uzupełniony o elementy brakujące lub/i będzie musiał być uwierzytelniony

W każdej sytuacji potrzebny będzie pewien ciąg działań, którego celem będzie stwierdzenie, czy przesłany plik:

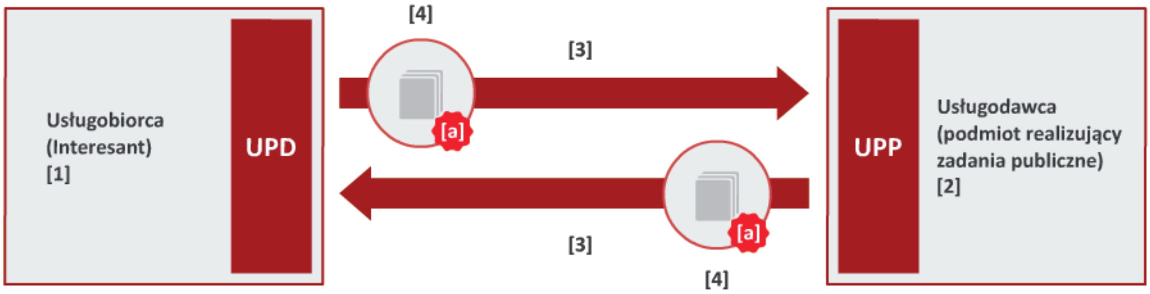
a) Jest sporządzony w formacie pozwalającym na jego odczyt,
b) Jest sporządzony w sposób jednoznaczny i czytelny (tzn. wiadomo, czego dotyczy),
c) Jest zabezpieczony przed niekontrolowaną modyfikacją,
d) Został sporządzony przez dającego się jednoznacznie i niezaprzeczalnie zidentyfikować wystawcę/twórcę dokumentu,
e) Został stworzony w konkretnym, znanym celu,
f) Został sporządzony w określonym czasie i miejscu.

Szczegóły wyjaśnione są w punktach dotyczących poszczególnych elementów e-usługi.

# 1. e-Usługi publiczne

| |
|---|
| e-usługi - usługi świadczone drogą elektroniczną (za pośrednictwem środków komunikacji elektronicznej); (Dz.U 2013.1422 j.t.) |

**E-administracja** to administracja nowoczesna, realizująca funkcje administracji tradycyjnej, polegające na wykonywaniu wewnętrznych zadań i świadczenia usług zewnętrznych z wykorzystaniem środków komunikacji elektronicznej, czyli e-usług. Jakkolwiek by nie rozpatrywać procesów komunikacji między uczestnikami – obojętnie – z wykorzystaniem **dokumentów elektronicznych** czy papierowych, muszą istnieć co najmniej dwie strony procesu komunikacji; nawet gdy jest ich więcej, też można rzecz zawsze sprowadzić do zbioru komunikujących się par nadawca – odbiorca, czy jak w rozważanej przez nas e-administracji – usługobiorca (interesant) i usługodawca (organ, urząd obsługujący organ). Można to zobrazować następującym rysunkiem:



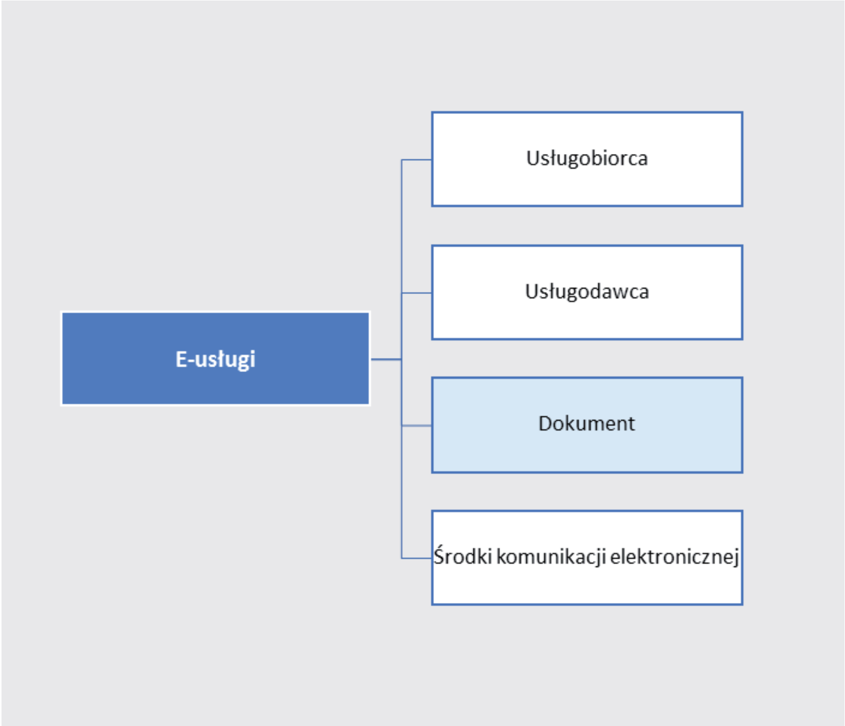

*Podstawowe elementy procesu komunikacji w ramach świadczenia e-usługi*

Elementy główne, wskazane kolejnymi numerami na rys. 1, to:

- **(1) usługobiorca (interesant, strona postępowania),**
- **(2) usługodawca** (podmiot realizujący zadania publiczne),
- **(3) środki komunikacji elektronicznej**, w tym mechanizmy potwierdzenia przedłożenia/doręczenia dokumentów (**UPP**, **UPD**),
- **(4) dokument**, którego elementem (jeśli występuje) jest [a] **podpis**.

Jest to najbardziej ogólne przedstawienie dwustronnej relacji, powstającej w czasie inicjowania procesu załatwiania sprawy – bez względu na to, która ze stron proces ten rozpoczyna, oraz z jakich środków komunikacji korzysta. Ważne jest, że wyżej wymienione elementy główne zawsze dają się wyraźnie wskazać – i w jakiś sposób opisać pewnymi cechami, które pozwalają kontrolować proces realizacji e-usługi.

Poniżej przedstawiono elementy składowe **e-usługi** – jako pojęcia stojącego najwyżej w hierarchii strukturalnej omawianych zagadnień.



*E-usługa i jej elementy.*

Realizacja e-usługi (niezależnie od tego, czego dotyczy) zawsze wymaga **czterech** elementów składowych, które muszą być odrębnie wzięte pod uwagę. Są to **usługobiorca, usługodawca**, pośredniczący między nimi **środek komunikacji elektronicznej**, oraz **dokument**. Pozornie wydawać by się mogło, że e-usługi świadczone są niekiedy bez tworzenia **dokumentów**, gdyż wymagają jedynie podania pewnych danych, potrzebnych **usługodawcy** do ich realizacji. Jednak, poza usługami czysto informacyjnymi (BIP), dokumenty tworzone są zawsze, lecz nie zawsze jest to wyraźnie widoczne, gdyż nie zawsze żądane są one od **usługobiorcy**. Na tym bowiem polega specyfika e-usług, że wiele **dowodów** (świadczących o fakcie realizacji e-usługi, terminie realizacji, statusie, osobie usługobiorcy) wykonują programy zaimplementowane w systemach teleinformatycznych dedykowanych do realizacji określonej usługi.

Na rysunku pokazano podstawowe elementy e-usługi. Jeden z nich – **dokument** – został wyróżniony z uwagi na fakt, że jest elementem najtrudniejszym do zdefiniowania i zbadania w codziennej praktyce; w każdym przypadku to z niego będą wynikały wszystkie informacje dotyczące pozostałych elementów e-usługi. Zamiast jednego dokumentu występować może cały ich zbiór (paczka), jednak dla rozumienia istoty rzeczy nie ma to żadnego znaczenia - analizie podlegał będzie zawsze **każdy** dokument.

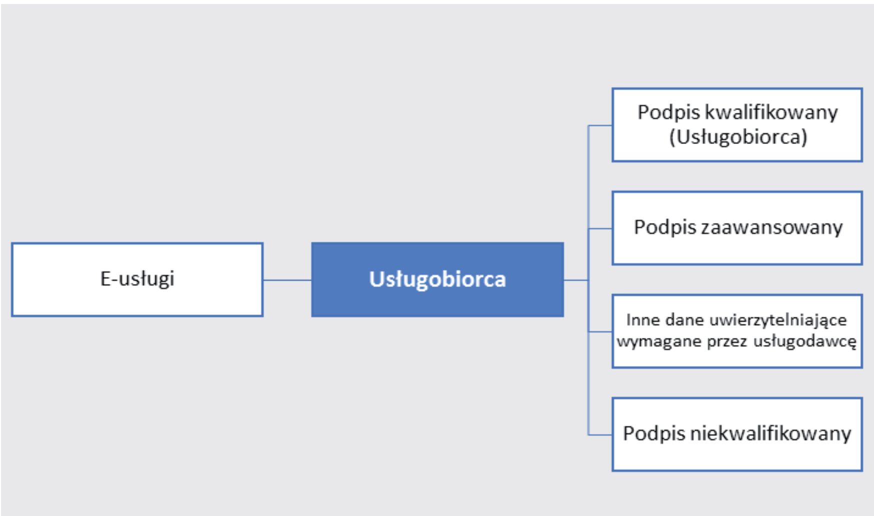
# 2. Usługobiorca

| |
|---|
| **Usługobiorca** - osoba fizyczna, osoba prawna albo jednostka organizacyjna nieposiadająca osobowości prawnej, która korzysta z usługi świadczonej drogą elektroniczną; (Dz.U.2013.1422 j.t.) |

**Identyfikacja i uwierzytelnianie**

**Jednoznacznym identyfikatorem** usługobiorcy będącego osobą fizyczną jest **numer PESEL**, identyfikatorem usługobiorcy będącego podmiotem jest **numer REGON (Dz.U.2012.526)**.

Usługobiorca, korzystając z e-usługi, musi się uwierzytelnić przed usługodawcą. Do tego celu służy podpis elektroniczny lub inne dane, które usługodawca uzna za wystarczające do upewnienia się co do tożsamości usługobiorcy




*Usługobiorca i środki identyfikacji wykorzystywane w komunikacji z usługodawcą*

Cechą podstawową **usługobiorcy** jest to, że to od niego właśnie zaczyna się proces realizacji e-usługi (wszczynanie). Jest oczywiste, że aby można było z e-usługi skorzystać, musi być ona wcześniej opracowana, przygotowana przez **usługodawcę** i udostępniona – wystawiona w miejscu, w którym można będzie z niej skorzystać (np. strona internetowa, dedykowany portal). Usługobiorca korzystający z e-usługi udostępnionej na stronie internetowej – jeśli nie jest ona wyłącznie usługą informacyjną, musi się usługodawcy w wiarygodny sposób „przedstawić" Istnieją różne sposoby **identyfikacji**, jednak– by działania przy realizacji e-usługi mogły **skutkować prawnie** – identyfikacja musi cechować się **niezaprzeczalnością**– a więc musi dawać usługodawcy **pewność**, że usługobiorca (interesant) zamierzający skorzystać z e-usługi jest tym, za kogo się podaje i nie będzie mógł się tego wyprzeć.

W bezpośrednich kontaktach, mających miejsce przy załatwianiu spraw w urzędach, osoba fizyczna w celu udowodnienia swojej tożsamości powinna okazać osobie przyjmującej dokumenty **dowód tożsamości** (dowód osobisty lub paszport); ten powinien być przez pracownika przyjmującego dokumenty zweryfikowany, wizerunek na dowodzie tożsamości porównany z twarzą okaziciela. To jest właśnie moment, w którym następuje **uwierzytelnienie**.

Istotą **e-usług** jest ich realizacja bez potrzeby równoczesnej obecności usługodawcy i usługobiorcy w tym samym miejscu i w tym samym czasie, a więc usługodawca nie ma możliwości bezpośredniego sprawdzenia **tożsamości usługobiorcy** – i jej weryfikacja musi odbyć się inaczej.

**Identyfikacja i uwierzytelnianie z punktu widzenia usługodawcy**

Z punktu widzenia usługodawcy - dowód tożsamości usługobiorcy realizowany środkami komunikacji elektronicznej powinien być dobrany racjonalnie i adekwatnie do sytuacji, a także celowo – tak, by zapewniał uzyskanie pewności przez usługodawcę, że przesłany **dokument jest integralny**, a tożsamość osoby z nim związanej (podpisującej) nie budzi wątpliwości. Żądanie przez usługobiorcę stosowania środków nieadekwatnych do poziomu zagrożenia jest pozbawione sensu – i jest jedynie wyrazem lęku przed naruszeniem prawa wynikającym z braku rozumienia narzędzi informatycznych, oraz procedur postępowania, jakimi można zapewnić wiarygodność dokumentów Usługobiorca może do zapewnienia wiarygodności dokumentu elektronicznego (zapewnienia jego integralności) oraz udowodnienia swojej tożsamości zastosować wszelkie środki adekwatne do poziomu zagrożenia, jakie usługodawca akceptuje, lub sam wskaże, jako możliwe do wykorzystania w konkretnej sytuacji.


Np. jeśli organ administracji samorządowej województwa (marszałek) wprowadzi możliwość stosowania **elektronicznych podpisów zaawansowanych** w relacjach mieszkańców województwa, przedsiębiorców i innych podmiotów z urzędami, a certyfikaty będą wydawane przez centrum certyfikacji zarządzane przez marszałka czy też pracowników organów gmin, pełniących funkcje inspektorów ds. certyfikacji (np. SEKAP lub Platforma e-Usług Miasta Opole), to certyfikaty takie będą jak najbardziej wiarygodne i nie ma żadnych powodów, by nie mogły być stosowane zamiast certyfikatów kwalifikowanych. Podobnie, jeśli usługodawca w swoim systemie teleinformatycznym zapewni **rozliczalność** – czyli umożliwi korzystanie z niego jedynie osobom, których **tożsamość** jest potwierdzona **certyfikatem kwalifikowanym**, **profilem zaufanym ePUAP, profilem zaufanym utworzonym przez usługodawcę** lub stawiennictwem osobistym, w czasie którego nastąpi wydanie certyfikatu albo loginu i hasła, to będzie to działanie zgodne z zasadami bezpieczeństwa obrotu prawnego – z każdego z tych zdarzeń można wywodzić skutki prawne. Mogą też być stosowane inne dane autoryzujące – przykład stanowią **e-deklaracje**, gdzie danymi autoryzującymi są nr PESEL, imię, nazwisko, data urodzenia, kwota z ubiegłorocznej deklaracji podatkowej. Kontakt usługodawcy z usługobiorcą realizowany jest wyłącznie za pośrednictwem **środków komunikacji elektronicznej** i z wykorzystaniem **dokumentów elektronicznych.**

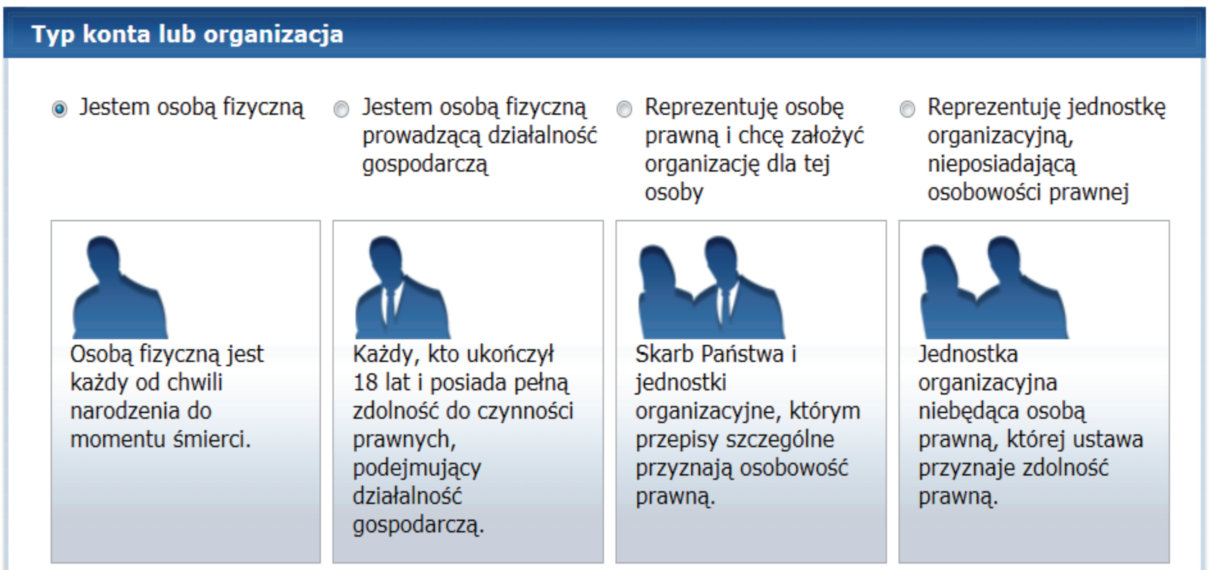
**Systemy dedykowane – grupy użytkowników**

Usługodawcy, tworząc systemy dedykowane, konstruują je w celu realizacji ściśle określonych, sparametryzowanych usług, przeznaczonych dla usługobiorców będących albo osobami fizycznymi, albo przedsiębiorcami prowadzącymi działalność gospodarczą, albo osobami prawnymi mającymi lub niemającymi osobowości prawnej. Takie rozróżnienia grup użytkowników stosowane są powszechnie.

Np. na stronie **SEKAP** uwidocznione są trzy różne grupy użytkowników (usługobiorców) obsługiwanych przez administrację samorządową Województwa Śląskiego:


*Grupy usługobiorców i usługodawców w SEKAP*

Podobnie, przy zakładaniu profilu na platformie **ePUAP** należy określić typ konta lub rodzaj organizacji, dla której zakładane jest konto:




*Grupy usługobiorców i usługodawców na ePUAP*

Wstępne określenie grupy usługobiorców skutkuje koniecznością podania danych identyfikacyjnych (które zostaną później potwierdzone przez „zaufaną stronę trzecią" – uprawnionego pracownika centrum certyfikacji, urzędu gminy lub innego podmiotu będącego **punktem potwierdzającym**.

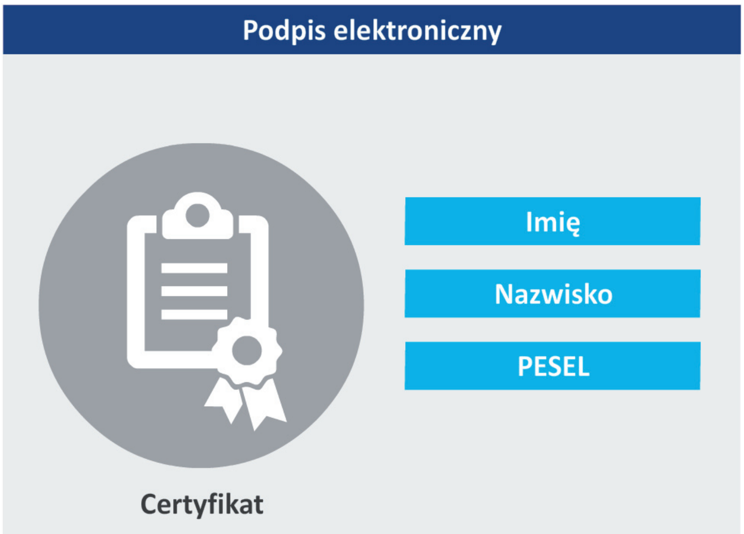
## 2.1 Podpis kwalifikowany (Usługobiorca)

**Definicje**

> **Podpis kwalifikowany** - zaawansowany podpis elektroniczny, który jest składany za pomocą kwalifikowanego urządzenia do składania podpisu elektronicznego i który opiera się na kwalifikowanym certyfikacie podpisu elektronicznego; (Dz.U.UE.910/2014)

„Podpis kwalifikowany" to powszechnie – jako skrót – używana nazwa bezpiecznego **podpisu elektronicznego** weryfikowanego za pomocą ważnego **kwalifikowanego certyfikatu**.

Z uwagi na bezpieczeństwo obrotu prawnego dokumenty przedkładane usługodawcy przez usługobiorcę za pośrednictwem **środków komunikacji elektronicznej** muszą być zabezpieczone przed niekontrolowaną modyfikacją, a więc muszą być elektronicznie podpisane. Stosuje się w tym celu **podpisy elektroniczne**.




> **Podpis elektroniczny** - dane w postaci elektronicznej, które wraz z innymi danymi, do których zostały dołączone lub z którymi są logicznie powiązane, służą do identyfikacji osoby składającej podpis elektroniczny; (Dz.U.2013.262)

**Wieloznaczność pojęcia podpis**

Należy w tym miejscu wyraźnie podkreślić, że samo pojęcie „podpis" jest pojęciem wieloznacznym, dlatego zawsze trzeba sprecyzować, o jakim podpisie jest mowa i w jakim celu ma być użyty Podpis elektroniczny służy bowiem nie tylko do identyfikacji składającej go osoby, ale także (bezwarunkowo) do zabezpieczenia podpisywanej treści przed niekontrolowaną modyfikacją.

Jest to oczywiste – gdyby bowiem można było po elektronicznym podpisaniu dokumentu zmienić w nim choćby jeden znak, wtedy stosowanie takiego podpisu nie miałoby żadnego sensu. Intencją ustawodawcy było zapewnienie **niezaprzeczalnego** związku osoby podpisującej dokument z tym dokumentem w związku z faktem, że podpisywanie odbywa się „zaocznie", tzn. o dowolnej porze i w dowolnym miejscu dogodnym dla podpisującego a nie tak, jak ma to miejsce w przypadku składania podpisu własnoręcznego – w obecności odbierającego dokument urzędnika, któremu wcześniej należy okazać dowód tożsamości. Właśnie **podpis elektroniczny**, dzięki **certyfikatowi** służącemu do jego złożenia, zapewnia ów związek konkretnej osoby z podpisywanym dokumentem. Certyfikat jest widoczny w czasie czynności weryfikacji podpisu – i zawiera dane jednoznacznie wskazujące na konkretną osobę fizyczną, która podpis złożyła. Jednoznaczne wskazanie to co najmniej imię, nazwisko i nr PESEL (lub NIP – w przypadku przedsiębiorcy).


**Podpis własnoręczny a bezpieczny podpis elektroniczny weryfikowany za pomocą ważnego kwalifikowanego certyfikatu**

Podpis złożony własnoręcznie (podpis własnoręczny) składany jest w zupełnie inny sposób, niż **bezpieczny podpis elektroniczny weryfikowany za pomocą ważnego kwalifikowanego certyfikatu**, w skrócie nazywanym **podpisem kwalifikowanym**.

Jednak – mimo zasadniczej różnicy w sposobie składania ww podpisów skutki prawne złożenia dokumentu w postaci elektronicznej opatrzonego bezpiecznym podpisem elektronicznym weryfikowanym za pomocą ważnego kwalifikowanego certyfikatu są równoważne skutkom prawnym złożeniu dokumentu papierowego opatrzonego podpisem własnoręcznym. Wymaga to komentarza w świetle brzmienia art. 78. § 2. Kodeksu cywilnego, zgodnie z którym „oświadczenie woli złożone w postaci elektronicznej opatrzone bezpiecznym podpisem elektronicznym weryfikowanym przy pomocy ważnego kwalifikowanego certyfikatu jest równoważne z oświadczeniem woli złożonym w formie pisemnej". Należy zwrócić uwagę na następujące fakty:

a) mowa jest o **oświadczeniu woli** – a nie każdy dokument jest oświadczeniem woli (dokument może być np. zdjęciem, rysunkiem, rozmową w trakcie wywiadu);

b) jest to prawo cywilne (prywatne), a administracja publiczna funkcjonuje w oparciu o kodeks postępowania administracyjnego (przedkładane dokumenty powinny być kompletne, czytelne, jednoznacznie związane z miejscem, czasem, osobą tworzącą);

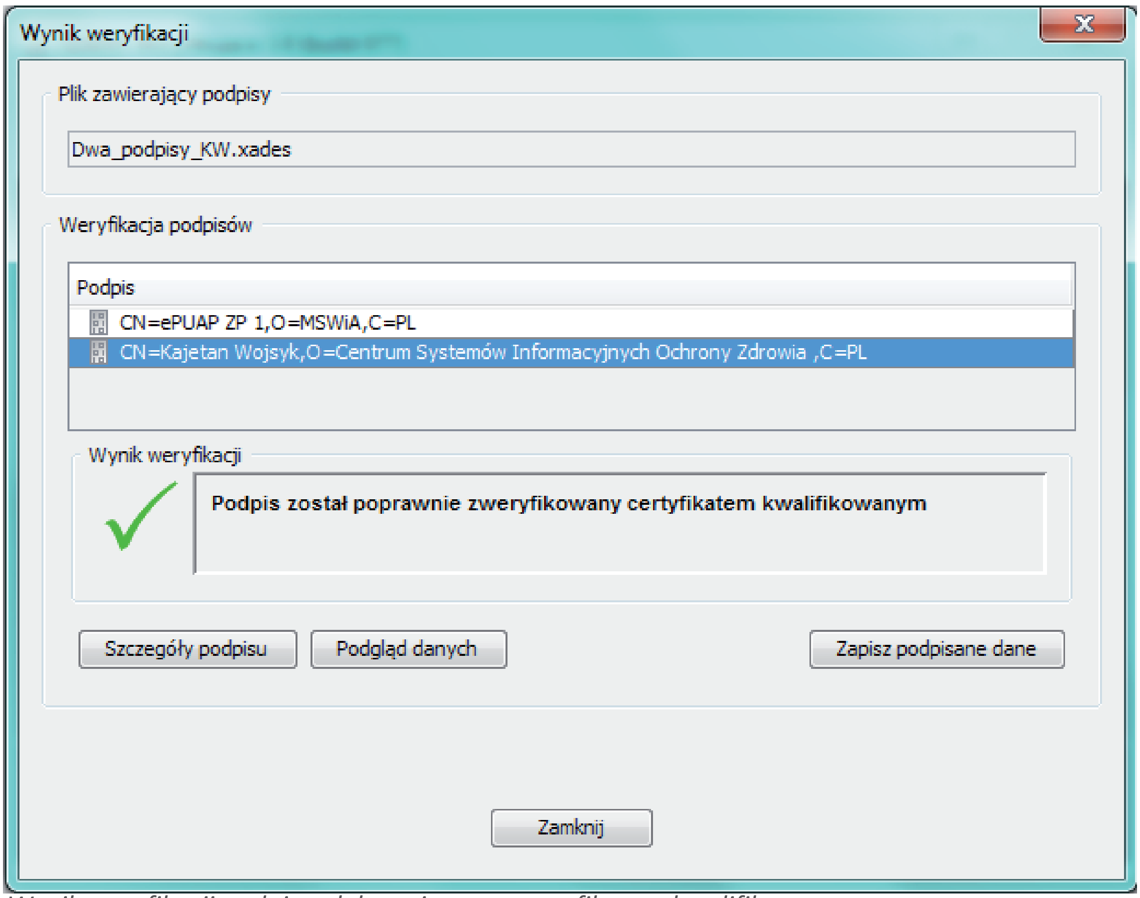
c) zamierzeniem ustawodawcy było zapewnienie niezaprzeczalnego powiązania osoby podpisującej dokument z tym dokumentem - niezależnie od tego, czy dokument ma **postać elektroniczną** czy **papierową**. To **postać** zastosowanego dokumentu determinuje rodzaj podpisu, jakiego należy użyć: dokument papierowy opatruje się **podpisem własnoręcznym**, dokument elektroniczny – **podpisem elektronicznym**.


W tym miejscu należy wskazać, że niezależnie od rodzaju podpisu elektronicznego – jeśli tylko zapewnione są warunki jego weryfikacji pozwalające na stwierdzenie:

- kto podpisał dokument (imię, nazwisko, PESEL),
- że podpisany dokument jest integralny, tzn. nie został zmieniony po złożeniu podpisu, a także ,
- że podpis został złożony w czasie ważności certyfikatu,

nie ma racjonalnych podstaw do formalnego kwestionowania dokumentu elektronicznego, ani samego podpisu – tylko dlatego, że jest w postaci elektronicznej (Dz.U 2013.262). Co więcej, tożsamość osoby, która widnieje jako sygnatariusz (podpisujący) jest nieporównywalnie łatwiejsza do zweryfikowania (**może zrobić to każdy**, w dowolnym momencie, za pomocą powszechnie dostępnego weryfikatora podpisu), niż tożsamość osoby, która złożyła podpis własnoręczny, lecz nieczytelny – może zrobić to tylko pracownik usługodawcy, **w obecności którego został złożony podpis,** po okazaniu dowodu tożsamości przez osobę podpisującą dokument. W późniejszym czasie weryfikacja „własnoręczności podpisu" będzie zdecydowanie trudniejsza. Z tego powodu należy jak najszerzej korzystać z możliwości przyjmowania **dokumentów** elektronicznie podpisanych; podmioty realizujące zadania publiczne mają taki obowiązek już od 1 maja 2008 r (Dz.U 2013.262)

**Weryfikacja podpisu elektronicznego**



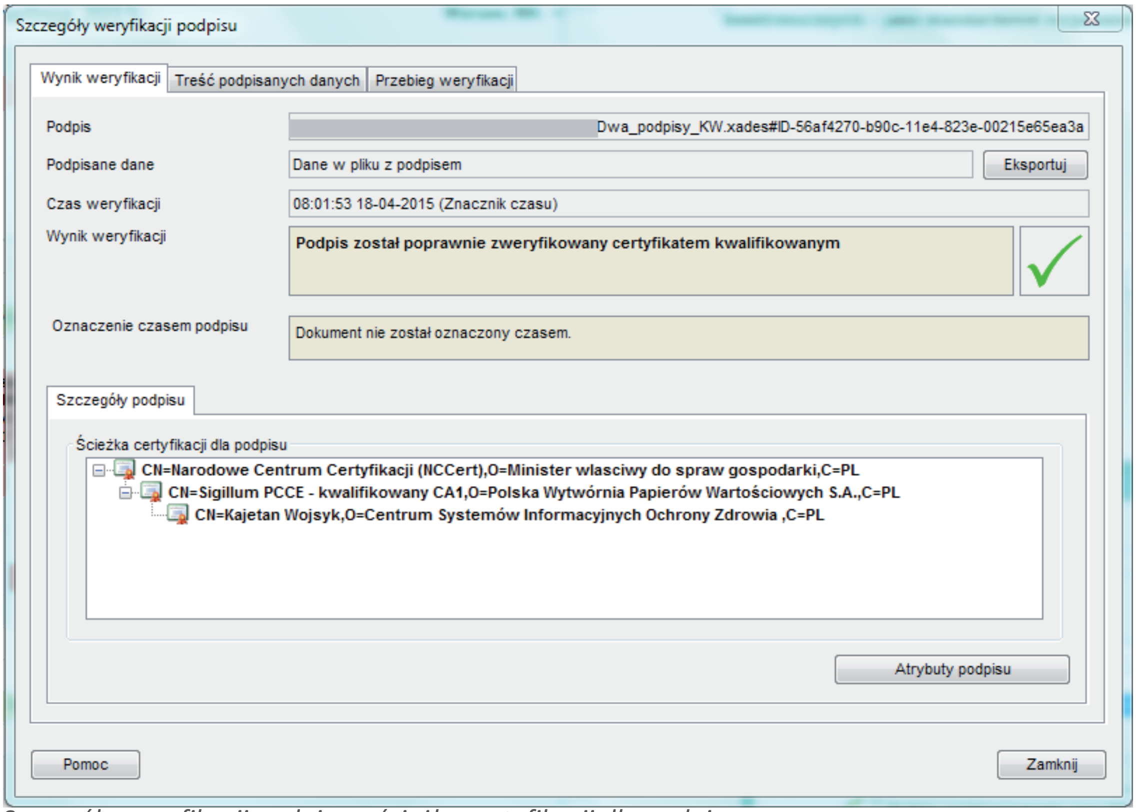
*Wynik weryfikacji podpisu elektronicznego certyfikatem kwalifikowanym*

Na rysunku *Fragment przebiegu weryfikacji kwalifikowanym certyfikatem podpisu* pokazano początkowy i końcowy fragment przebiegu weryfikacji certyfikatem kwalifikowanym podpisu elektronicznego – proces składał się z 52 kroków – po lewej stronie opisu każdego kroku widoczny jest dokładny czas dokonywania weryfikacji.

(1) 2015-04-18 08:02:08: Weryfikuję certyfikat => CN=Kajetan Wojsyk,O=Centrum Systemów Informacyjnych Ochrony Zdrowia ,C=PL
(2) 2015-04-18 08:02:08: Pobieram certyfikat CA z pliku z podpisem => serialNumber=Nr wpisu: 3, C=PL, O=Polska Wytwórnia Papierów Wartościowych S.A., CN=Sigillum PCCE - kwalifikowany CA1
(3) 2015-04-18 08:02:08: Certyfikat pobrany z pliku z podpisem poprawnie => serialNumber=Nr wpisu: 3, C=PL, O=Polska Wytwórnia Papierów Wartościowych S.A., CN=Sigillum PCCE - kwalifikowany CA1
(4) 2015-04-18 08:02:08: Weryfikuję czas ważności certyfikatu
(5) 2015-04-18 08:02:08: Certyfikat ważny w weryfikowanym czasie
(6) 2015-04-18 08:02:08: Weryfikuję atrybut określający użycie klucza
(7) 2015-04-18 08:02:08: Atrybuty określające użycie klucza zweryfikowane pomyślnie
(8) 2015-04-18 08:02:08: Weryfikuję podpis RSA
(9) 2015-04-18 08:02:08: Weryfikacja podpisu RSA zakończona pomyślnie
(10) 2015-04-18 08:02:08: Pobieram listę CRL => CA: CN=Sigillum PCCE - kwalifikowany CA1,O=Polska Wytwórnia Papierów Wartościowych S.A.,C=PL URL: http://193.178.164.4/repozytorium/ca1_newroot.crl
(11) 2015-04-18 08:02:08: Pobieram listę CRL => CA: CN=Sigillum PCCE - kwalifikowany CA1,O=Polska Wytwórnia Papierów Wartościowych S.A.,C=PL URL: http://193.178.164.4/repozytorium/ca1_newroot.crl
(12) 2015-04-18 08:02:08: Dekoduję listę CRL
(13) 2015-04-18 08:02:08: Lista CRL zdekodowana poprawnie
(14) 2015-04-18 08:02:08: Weryfikuję listy CRL
(15) 2015-04-18 08:02:08: Lista CRL zweryfikowana prawidłowo
-------
(46) 2015-04-18 08:02:08: Pobieram listę CRL => CA: CN=Narodowe Centrum Certyfikacji (NCCert),O=Minister wlasciwy do spraw gospodarki,C=PL URL: http://www.nccert.pl/arl/nccert-n.crl
(47) 2015-04-18 08:02:08: Pobieram listę CRL => CA: CN=Narodowe Centrum Certyfikacji (NCCert),O=Minister wlasciwy do spraw gospodarki,C=PL URL: http://www.nccert.pl/arl/nccert-n.crl
(48) 2015-04-18 08:02:08: Weryfikuję listy CRL
(49) 2015-04-18 08:02:08: Lista CRL zweryfikowana prawidłowo
(50) 2015-04-18 08:02:08: Sprawdzam certyfikat na liście CRL => CN=Narodowe Centrum Certyfikacji (NCCert),O=Minister wlasciwy do spraw gospodarki,C=PL
(51) 2015-04-18 08:02:08: Certyfikat nie znajduje się na liście CRL => CN=Narodowe Centrum Certyfikacji (NCCert),O=Minister wlasciwy do spraw gospodarki,C=PL
(52) 2015-04-18 08:02:08: Weryfikacja certyfikatu zakończona pomyślnie => CN=Narodowe Centrum Certyfikacji (NCCert),O=Minister wlasciwy do spraw gospodarki,C=PL

*Fragment przebiegu weryfikacji kwalifikowanym certyfikatem podpisu*

**Każdy pracownik e-administracji powinien mieć zainstalowany weryfikator podpisów elektronicznych – jako standardowe wyposażenie stanowiska pracy e-urzędnika.**




*Szczegóły weryfikacji podpisu – ścieżka certyfikacji dla podpisu.*

Istotą wiarygodności podpisu kwalifikowanego jest procedura uzyskiwania **certyfikatu** służącego do jego weryfikacji oraz zastosowane mechanizmy, w uproszczony sposób pokazane na rysunkach. Jak wynika ze „szczegółów podpisu" na rys. *Szczegóły weryfikacji podpisu*, głównym Centrum Certyfikacji w Polsce jest Narodowe Centrum Certyfikacji, wykonujące tę funkcję w imieniu Ministra właściwego do Spraw Gospodarki. Centrum to wydaje certyfikaty innym podmiotom świadczącym usługi certyfikacyjne, a te z kolei wydają **certyfikaty** fizycznym **osobom podpisującym** dokumenty (subskrybentom). Są to **certyfikaty kwalifikowane** służące właśnie do podpisywania dokumentów zawierających przede wszystkim wyrażenie woli, ale także wszelkich innych, a także certyfikaty niekwalifikowane, służące np. do uwierzytelniania się wobec systemów teleinformatycznych (logowanie za pomocą certyfikatu) lub do szyfrowania przesyłek.

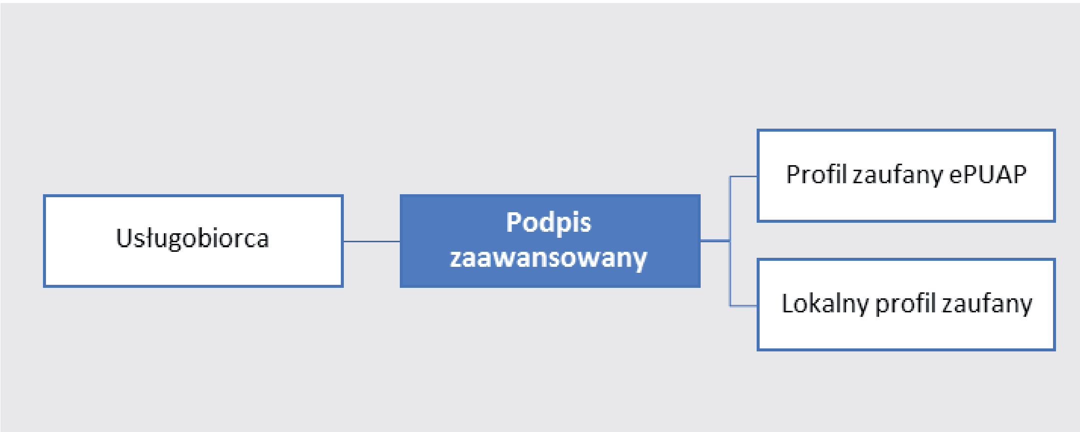
### Korzystanie z certyfikatu kwalifikowanego

Korzystanie z certyfikatu kwalifikowanego wiąże się z używaniem kart kryptograficznych, na których przechowywane są klucze do składania podpisu. W czasie składania podpisu system żąda podania PINu, a także sprawdza obecność karty kryptograficznej w czytniku. Aby więc skutecznie złożyć podpis, trzeba nie tylko znać PIN, ale także umieścić kartę z kluczami (publicznym i prywatnym) w czytniku oraz skorzystać ze stosownego oprogramowania Trzykrotne błędne podanie PINu blokuje kartę.

## 2.2 Podpis zaawansowany

**Podpis zaawansowany -** podpis elektroniczny, który spełnia następujące wymagania:

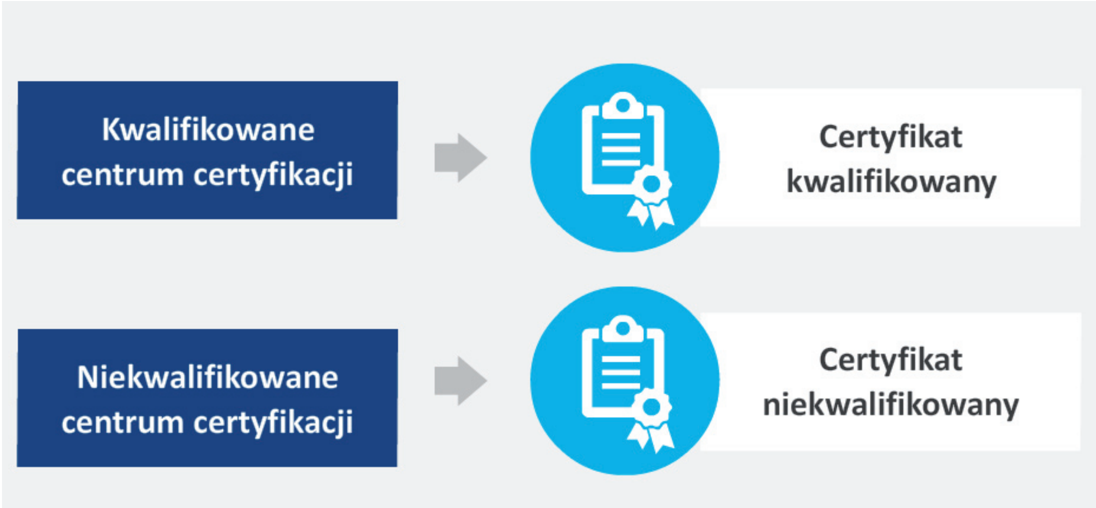
1. jest jednoznacznie powiązany z osobą składającą podpis elektroniczny,
2. pozwala na identyfikację osoby składającej podpis elektroniczny,
3. jest tworzony z wykorzystaniem zasobów, które osoba składająca podpis elektroniczny może utrzymywać pod swoją wyłączną kontrolą,
4. jest powiązany z danymi, do których się odnosi w taki sposób, że każda jakakolwiek późniejsza zmiana tych danych jest rozpoznawalna.




*Podpis zaawansowany*

Rozpoznawalność owej zmiany polega na tym, że nie jest wiadome, co i gdzie w dokumencie uległo zmianie, pewne jest jedynie, że zmiana nastąpiła, a więc nie mamy już do czynienia z dokumentem oryginalnym – i to wystarczy

Zaawansowany podpis elektroniczny jest **równoważny bezpiecznemu podpisowi elektronicznemu,** w przypadku gdy został on złożony za pomocą bezpiecznego urządzenia do składania podpisu elektronicznego (Dz.U 2013.262).




Zaawansowany podpis elektroniczny może być weryfikowany za pomocą **certyfikatu niekwalifikowanego** lub **certyfikatu kwalifikowanego**. W tym ostatnim przypadku zaawansowany podpis elektroniczny nazywany jest często kwalifikowanym podpisem elektronicznym. A więc o **kwalifikowalności decyduje procedura uzyskiwania certyfikatu i rodzaj centrum certyfikacji wystawiającego certyfikat.**

Uwaga – w każdym przypadku wystawiania certyfikatu – by był on wystarczający do wiarygodnego powiązania używającej go osoby z podpisywanym dokumentem konieczne jest potwierdzenie tożsamości tej osoby przez inspektora ds. certyfikacji w czasie procedury zamawiania i generowania certyfikatów – w oparciu o okazany dowód tożsamości. Inspektor ds. certyfikacji swoim podpisem elektronicznym a także własnoręcznym podpisem stosownego dokumentu papierowego potwierdza fakt istnienia subskrybenta i prawdziwość jego danych osobowych. Subskrybent otrzymuje drugi egzemplarz tego dokumentu.

### 2.2.1 Profil zaufany ePUAP

| |
|---|
| **Profil zaufany ePUAP** - zestaw informacji identyfikujących i opisujących podmiot lub osobę będącą użytkownikiem konta na ePUAP, który został w wiarygodny sposób potwierdzony przez organ podmiotu określonego w art. 2 ustawy o informatyzacji działalności podmiotów realizujących zadania publiczne; (Dz.U.2014.1114 j.t.) |


Profil zaufany ePUAP jest alternatywą certyfikatu kwalifikowanego w relacjach osób fizycznych (usługobiorców), a także przedsiębiorców z administracją publiczną. Także pracownicy administracji we wzajemnych relacjach mogą stosować profil zaufany ePUAP do wiarygodnego podpisywania przekazywanych dokumentów (Dz.U.2014.1114 j.t.). Konstrukcja ta wynika bezpośrednio z kilku uwarunkowań:

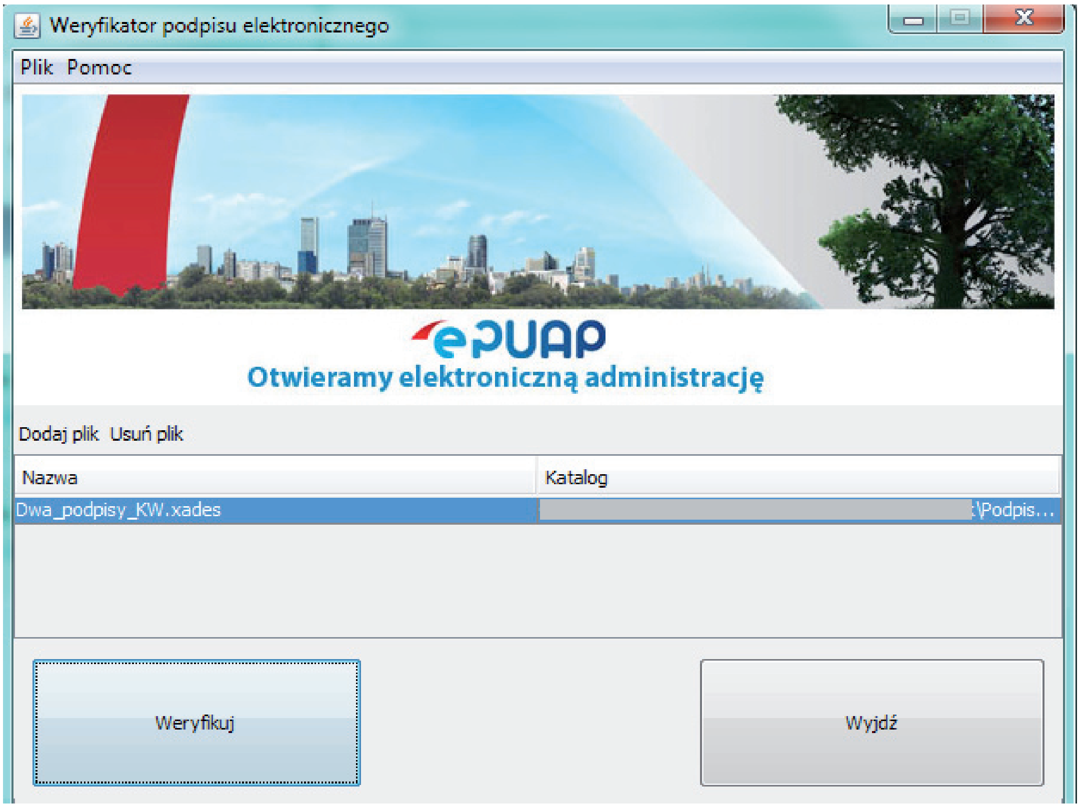
a) Potwierdzenie tożsamości osoby uzyskującej potwierdzenie danych w swoim profilu odbywa się w **punkcie potwierdzającym** (PP) , którego uprawniony pracownik spełnia w istocie funkcję inspektora ds. certyfikacji. Pracownik PP w oparciu o okazany i zweryfikowany dowód tożsamości (sprawdza autentyczność dowodu i porównuje zdjęcie w dowodzie z twarzą osoby okazującej dowód osobisty lub paszport) – za pomocą mechanizmów udostępnionych PP dokonuje potwierdzenia tożsamości – zgodności danych we wniosku z danymi w dowodzie osobistym (imię, nazwisko, PESEL).

b) Weryfikowane (potwierdzane) dane pracownik PP podpisuje własnym profilem zaufanym lub bezpiecznym podpisem elektronicznym weryfikowanym ważnym kwalifikowanym – co do skutków technicznych i prawnych jest to działanie identyczne.

c) Wszelkie działania (założenie profilu, złożenie wniosku, potwierdzenie tego profilu) odbywają się w ramach systemu ePUAP – a więc w bezpiecznym środowisku administrowanym przez ministra właściwego ds. informatyzacji.

d) Mechanizmy podpisywania elektronicznego działają dokładnie tak samo jak w przypadku podpisywania podpisem kwalifikowanym – i z tego powodu skutki złożenia dokumentu podpisanego podpisem potwierdzonym profilem zaufanym są zrównane w skutkach prawnych ze skutkami złożenia dokumentu papierowego podpisanego własnoręcznie (Dz.U 2014.1114 j.t.).

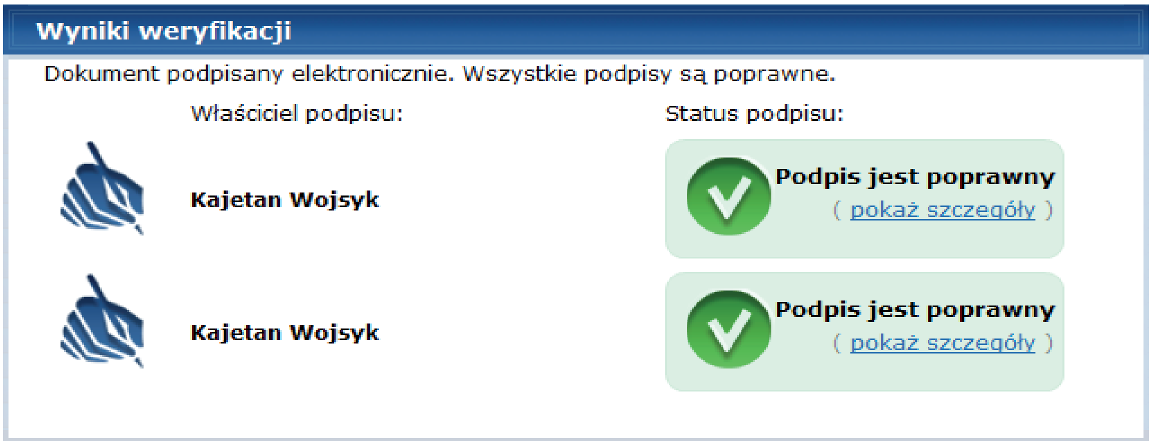
Na rysunku *Weryfikator podpisu elektronicznego...* pokazano przykład weryfikatora podpisów zaimplementowanego na platformie ePUAP




*Weryfikator podpisu elektronicznego z wczytanym plikiem podpisanym dwoma podpisami – kwalifikowanym i profilem zaufanym ePUAP – przed weryfikacją*

Weryfikator ten w pewnych sytuacjach może być użyty także poza ePUAP do weryfikacji elektronicznie podpisanych plików wyeksportowanych (pobranych na dysk) z ePUAP

Rysunek *Wynik weryfikacji pliku Dwa_podpisy_KW.xades* przedstawia wynik weryfikacji podpisów pliku wczytanego do weryfikatora zaimplementowanego na platformie ePUAP




*Wynik weryfikacji pliku Dwa_podpisy_KW.xades z rys. 6.*

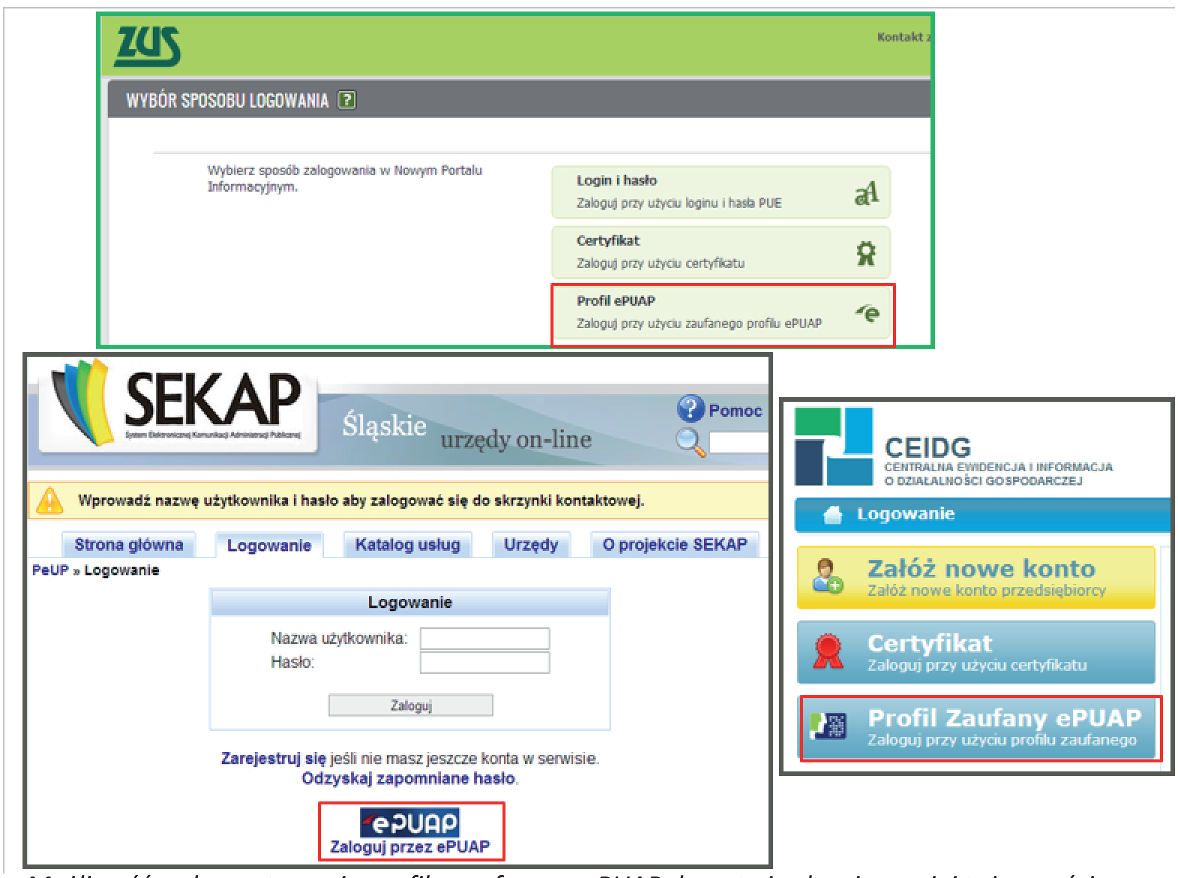
Usługobiorca (wnioskodawca) może więc przedkładać **dokumenty elektroniczne** podpisane podpisem potwierdzonym profilem zaufanym ePUAP usługodawcy (podmiotowi publicznemu) i muszą być one traktowane identycznie, jak **dokumenty papierowe podpisane własnoręcznie** (przedłożone w formie pisemnej).

Wyniki weryfikacji obu podpisów wskazują, że są potwierdzone certyfikatami wystawionymi przez kwalifikowane centrum certyfikacji i oprócz danych identyfikacyjnych samego podpisu (numer seryjny), uwidaczniają imię, nazwisko, PESEL osoby podpisującej oraz czas złożenia podpisu) Dokumenty podpisane podpisem potwierdzonym profilem zaufanym ePUAP mogą być składane do wszystkich podmiotów realizujących zadania publiczne, o których mowa w ustawie o informatyzacji

Aktualnie, po powszechnym udostępnieniu możliwości korzystania z profilu zaufanego ePUAP administracja publiczna nie może żądać od usługobiorców będących osobami fizycznymi podpisywania dokumentów podpisem kwalifikowanym w przypadku przedkładania dokumentów elektronicznych, gdyż byłoby to nie tylko naruszeniem równości praw obywateli (odebraniem możliwości korzystania z e-usług wszystkim obywatelom na równych prawach, wygoda i oszczędność czasu tylko dla tych, którzy zakupią usługę certyfikacyjną w podmiocie świadczącym te usługi), ale zaprzeczeniem idei e-administracji Administracja publiczna utrzymywana jest z pieniędzy wszystkich podatników, a więc także tych, którzy rzadko korzystają bezpośrednio z jej usług; kupowanie przez nich certyfikatów kwalifikowanych byłoby nieracjonalne Każdy ma prawo skorzystać z możliwości, jakie daje ePUAP i możliwość korzystania z profilu zaufanego na tej platformie – a dokumenty złożone za jej pośrednictwem są nie mniej wiarygodne, niż dokumenty podpisane podpisem kwalifikowanym Samo złożenie podpisu wymaga nie tylko zalogowania się do systemu, ale także użycia jednorazowego kodu, przesłanego na adres poczty elektronicznej (rozwiązanie mniej bezpieczne, które powinno być wycofane z użycia) lub kodem przesyłanym SMS-em – i ten sposób jest bezpieczny, ponieważ osoba składająca podpis w tym samym, krótkim, kilkusekundowym czasie ma przed sobą podpisywany dokument oraz okienko do wpisania kodu, a własny telefon przy sobie Jest to więc podpis bezpieczny

### 2.2.2 Lokalny profil zaufany

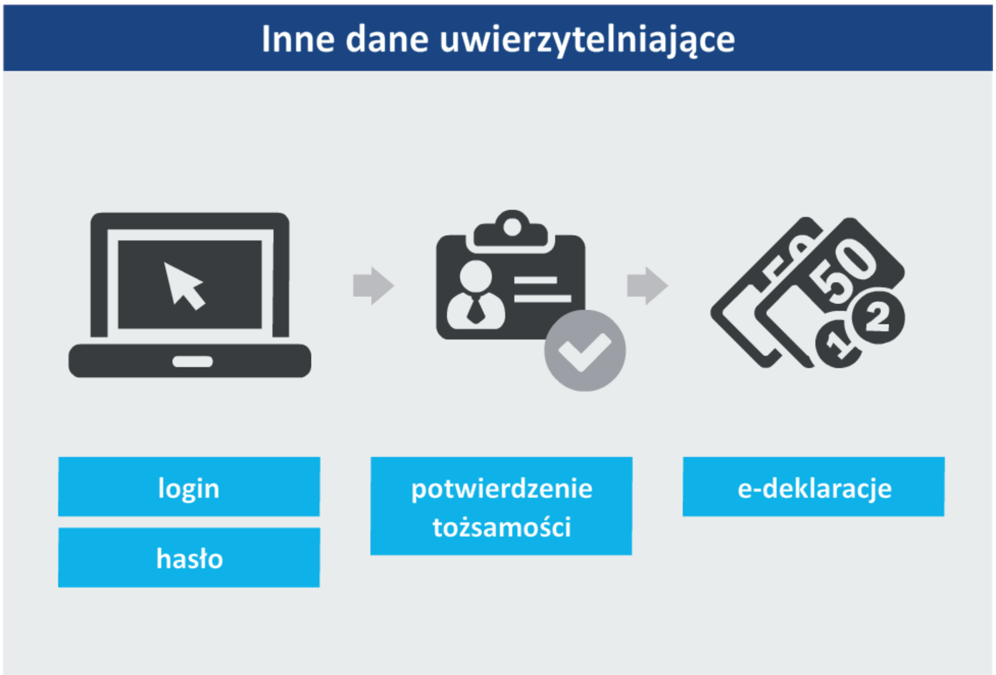
Lokalnym profilem zaufanym możemy określić profil usługobiorcy utworzony w lokalnym systemie teleinformatycznym – należącym do konkretnego podmiotu – bez względu na jego zasięg terytorialny Zaufanie opiera się na bezwzględnie konsekwentnie realizowanej procedurze potwierdzenia tożsamości usługobiorcy w tym systemie – dokładnie tak samo jak dzieje się to w przypadku potwierdzania tożsamości osoby fizycznej przy wystawianiu certyfikatu kwalifikowanego lub potwierdzaniu profilu zaufanego ePUAP Lokalnym profilem zaufanym może być profil założony użytkownikowi w zakładowym systemie elektronicznego zarządzania dokumentami, czy jakimkolwiek innym systemie, wymagającym podania danych identyfikacyjnych, które potwierdza administrator danych lub osoba przez niego upoważniona. Możliwe jest samopotwierdzenie danych w przypadku posiadania wcześniejszego – i ważnego innego certyfikatu, uzyskanego zgodnie z procedurą wymagającą osobistego stawienia się przed inspektorem ds. certyfikacji. Np. osoba fizyczna posiadająca certyfikat kwalifikowany lub profil zaufany ePUAP może za jego pomocą udowodnić swoją tożsamość w innych systemach, jeżeli taka możliwość została w nich przewidziana.




*Możliwość wykorzystywania profilu zaufanego ePUAP do potwierdzania swojej tożsamości w innych systemach dedykowanych – bez potrzeby odwiedzania punktów potwierdzeń właściwych dla tych systemów*

## 2.3 Inne dane uwierzytelniające wymagane przez usługodawcę

Usługodawcy mogą stosować różne sposoby **identyfikacji** i **uwierzytelniania** użytkowników w swoich systemach (identyfikacja usługobiorców), które powinny być dobrane adekwatnie do poziomu zagrożenia.




Każdy system zabezpieczenia (w tym przypadku zabezpieczenia przed korzystaniem z e-usługi przez osobę niezidentyfikowaną, jeśli prawo niezaprzeczalnej identyfikacji (uwierzytelnienia) wymaga. Takim sposobem może być login i hasło, ale zawsze ów login (identyfikator w systemie) powiązany być musi z uwierzytelnionymi danymi w ramach procedury, w której mieści się stawienie się w punkcie obsługi wskazanym przez usługodawcę i podpisanie umowy dotyczącej warunków korzystania z usługi. Usługobiorca chociaż jeden raz musi stawić się z dowodem tożsamości – chyba, że usługodawca posiada inne mechanizmy uwierzytelnienia. Bardzo dobrym przykładem – zastosowania przez usługodawcę powiązania danych dotyczących osoby fizycznej (usługobiorcy) ze składanym dokumentem - jest e-usługa polegająca na odbiorze e-deklaracji, udostępniona przez Ministra Finansów Nie wymaga ona podpisu, a jedynie podania danych uwierzytelniających, znanych zarówno Ministrowi Finansów, jak i podatnikowi. Taka konstrukcja – w tej konkretnej usłudze - jest adekwatna do poziomu zagrożenia podaniem nieprawdziwych danych, a bardzo dynamiczny wzrost liczby jej użytkowników jest dowodem dobrze przemyślanej filozofii gromadzenia danych, ich weryfikacji i potwierdzania odbioru. Warto zauważyć, że jest to deklaracja, a więc swego rodzaju oświadczenie niosące określone skutki prawne.

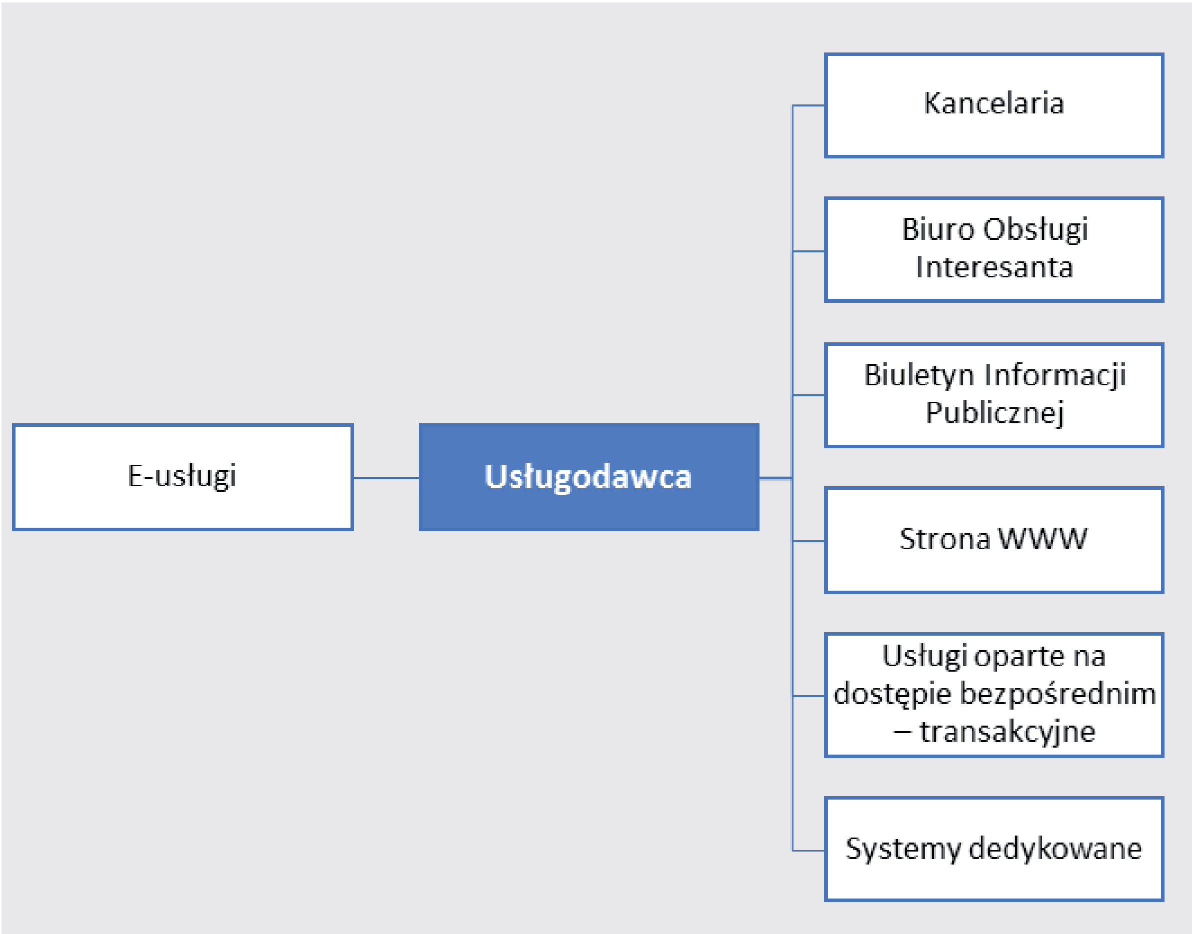
## 2.4 Podpis niekwalifikowany

Podpis niekwalifikowany jest ostatnim ze środków, który może być stosowany do wiarygodnego podpisywania dokumentów czy korzystania z systemów udostępnionych przez usługodawcę. To, jaki certyfikat zostanie wykorzystany w procesie komunikacji zależy jedynie od umowy dwóch stron tej komunikacji. Jeśli zatem np. usługodawca utworzy własne niekwalifikowane centrum certyfikacji, którego certyfikaty będą dla niego wiarygodne (a najbardziej wiarygodne są dla niego własne certyfikaty, gdyż sam je wystawia i samemu sobie najbardziej ufa) i będzie swoim usługobiorcom wystawiał te certyfikaty (nadal z bezwzględnym zachowaniem procedury podpisania stosownej umowy o korzystaniu z certyfikatu i fizycznym sprawdzeniu tożsamości usługobiorcy), to certyfikaty te mogą służyć do podpisywania dokumentów


Przykładem mogą być certyfikaty banków – każdy bank wystawia swoim klientom własne certyfikaty – i tylko takimi można posługiwać się w jego systemach. Podobne certyfikaty mogą być wystawiane przez regionalne centra certyfikacji prowadzone przez marszałków czy szkoły wyższe oraz dowolne inne podmioty, świadczące usługi dla pewnej ograniczonej stosunkowo grupy użytkowników

## 3. Usługodawca

| |
|---|
| **Usługodawca** - osoba fizyczna, osoba prawna albo jednostka organizacyjna nieposiadająca osobowości prawnej, która prowadząc, chociażby ubocznie, działalność zarobkową lub zawodową świadczy usługi drogą elektroniczną; (Dz.U.2013.1422 j.t.) |



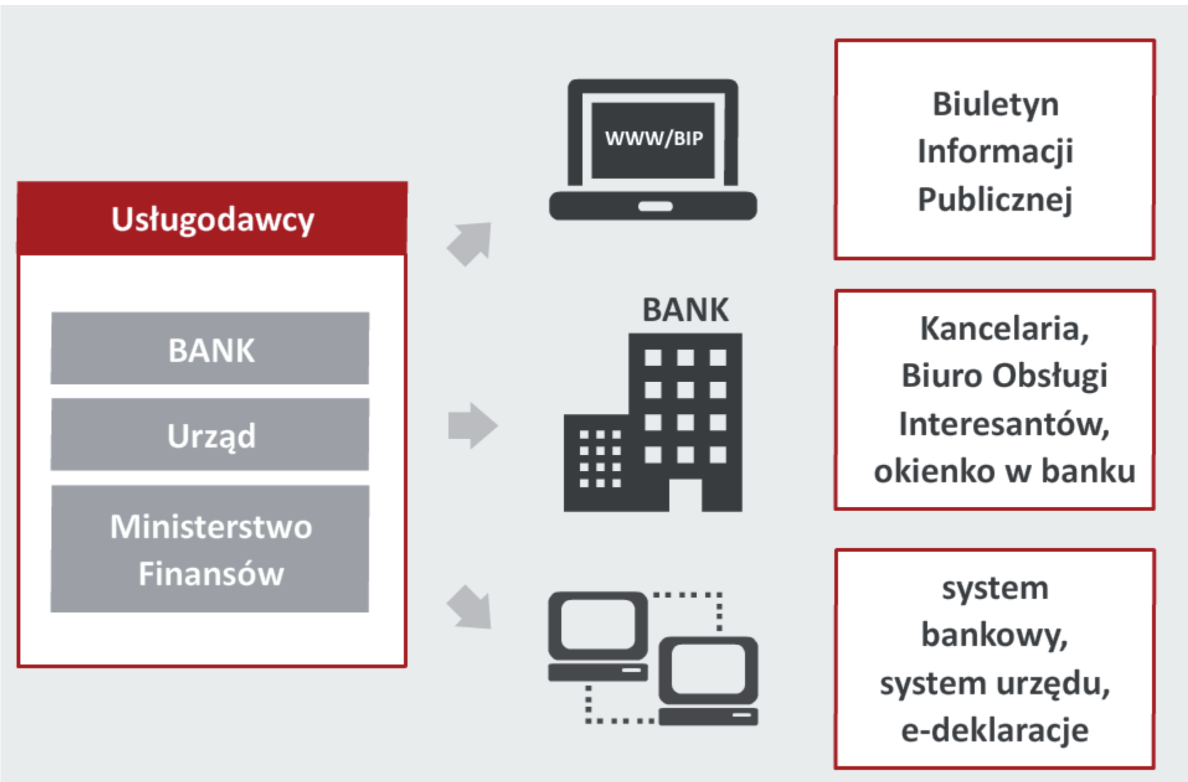

*Usługodawca i „interfejsy" służące do kontaktu z usługobiorcami (interesantami)*

**Obywatel – petent czy klient**

Wyżej podana definicja, pochodząca z ustawy o świadczeniu usług drogą elektroniczną, wskazuje na przedsiębiorców i podmioty prowadzące działalność zarobkową lub zawodową. Trudno w niej dopatrzyć się organów władzy publicznej. Faktem niezaprzeczalnym jednak jest, że obecnie przekształcanie się administracji z „papierowej" w „elektroniczną" zupełnie zmieniło sposoby jej działania i charakter, mimo iż nie zmieniło jej zadań ani kompetencji. W nowoczesnej e-administracji obywatel przestaje być „petentem" – starającym się, ubiegającym o coś, a staje się jej „klientem", podatnikiem, który płaci – i ma prawo wymagać. Te same zadania administracji przy innym pojmowaniu osoby obsługiwanego zmieniają zupełnie relacje. Właśnie zastosowanie technologii informacyjnych staje się kluczowe w przekształcaniu administracji władczej, opresywnej w nowoczesną, służebną w stosunku do obywatela. To nie tylko nowoczesna technologia, której zastosowanie umożliwiło w ogóle zmianę sposobu obsługi interesanta (pojmowanego jako klienta urzędu), technologii umożliwiającej także zmianę „petenta" w „klienta", ale rzeczywisty udział obywateli w procesach zarządzania lokalnego stanowi o przemianie cywilizacyjnej.

**Wpływ technologii na zmianę sposobu wykonywania prawa**

Zmiany dokonują się poprzez poprawę udostępniania informacji (**Biuletyn Informacji Publicznej**, podmiotowe strony WWW), co umożliwia lepszą orientację obywateli w procesach zarządzania, umożliwia realizację budżetu partycypacyjnego itd. Jeszcze większe znaczenie mają systemy dedykowane, tworzone przez usługodawców w celu realizacji drogą elektroniczną konkretnych, pojedynczych usług – już nie tylko informacyjnych, ale transakcyjnych czy wręcz zintegrowanych. Istotą przemiany jest zrozumienie, że technologie informacyjne zostały wprowadzone nie w celu zmiany **techniki pracy biurowej**, lecz w celu zmiany **sposobu wykonywania prawa**. W takim układzie jest zupełnie bez znaczenia kto jest **usługodawcą** – czy będzie to usługodawca rozumiany wąsko, jak w definicji podanej na wstępie (np. bank), czy usługodawca rozumiany szeroko – jako dowolny podmiot świadczący usługi drogą elektroniczną – bez zawężeń. Jeśli wnikliwie przyjrzymy się administracji dobrze zinformatyzowanej, to dostrzeżemy **wpływ technologii na zmianę sposobu wykonywania prawa**.




Dobrym i powszechnie znanym przykładem są **e-deklaracje** – usługi mogące stanowić wzór stosowania zabezpieczeń **integralności** i **niezaprzeczalności** dokumentu adekwatnych do sytuacji i rodzaju usługi. Usługobiorca (podatnik) nie musi posiadać żadnych specjalnych narzędzi, certyfikatów, nie musi stawiać się osobiście w jakimkolwiek urzędzie skarbowym, gdyż wszelkie dane aktualnie wymagane składa bezpośrednio do będącego **usługodawcą** Ministerstwa Finansów posługując się **elektronicznym dokumentem** oraz e-usługą udostępnioną przez wspomniane ministerstwo, a także danymi autoryzującymi, znanymi tylko sobie – i natychmiast otrzymuje **Urzędowe Poświadczenie Odbioru (UPO)** w formie niezaprzeczalnego dokumentu elektronicznego. Dokument ten zawiera wszelkie dane związane zarówno ze złożoną e-deklaracją, jak i samym dokumentem poświadczającym złożenie e-deklaracji, którego złożenie spowodowało wygenerowanie UPO przez system teleinformatyczny Ministerstwa Finansów Usługodawca udostępnił więc kompletną e-usługę – łącznie z wszystkimi dokumentami i zabezpieczeniami integralności niezbędnymi w jej realizacji.

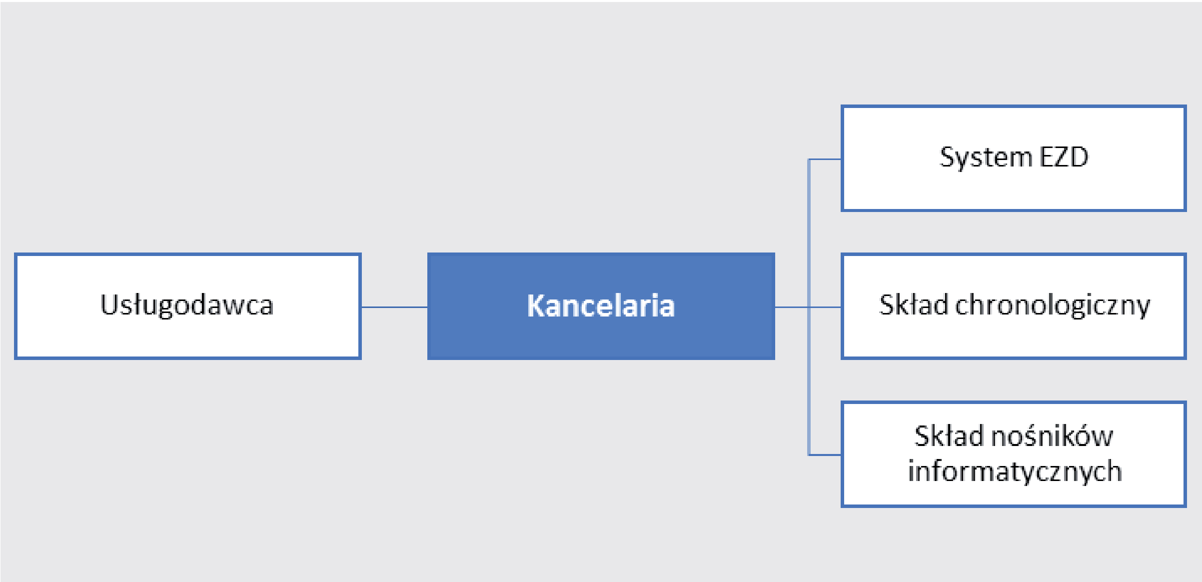
### Systemy dedykowane – ściśle sparametryzowane usługi

Usługodawcy, tworząc systemy dedykowane, konstruują je w celu realizacji ściśle określonych, sparametryzowanych usług, przeznaczonych dla usługobiorców będących albo osobami fizycznymi, albo przedsiębiorcami prowadzącymi działalność gospodarczą, albo osobami prawnymi mającymi lub niemającymi osobowości prawnej. Takie rozróżnienia grup użytkowników stosowane są powszechnie.

Usługodawca – w celu umożliwienia usługobiorcom kontaktów tworzy „interfejsy” – miejsca składania dokumentów w postaci papierowej i elektronicznej, miejsca świadczenia usług drogą elektroniczną, a także miejsca publikacji informacji przeznaczonej dla interesantów

## 3.1. Kancelaria

**Kancelaria** - komórka organizacyjna podmiotu powołana wyłącznie do pełnienia czynności aktotwórczych formalnych - związanych z przyjęciem i rejestracją pism wpływających, przechowywaniem dokumentacji niezbędnej do bieżącego funkcjonowania instytucji, prowadzeniem akt spraw i ekspedycją pism na zewnątrz; również pomieszczenie biurowe przeznaczone dla kancelarii w znaczeniu komórki organizacyjnej, czyli fizyczne miejsce wykonywania czynności kancelaryjnych. (Dz.U.2011.14.67)




*Kancelaria*

Rozważając funkcje kancelarii w e-administracji należy podkreślić, że stanowi ona całościowy, kompleksowy interfejs między podmiotem będącym usługodawcą, a otoczeniem. Oznacza to, że powinna ona przyjmować i wysyłać wszelkie przesyłki wraz dokonywaniem ich **konwersji** z **postaci papierowej** na **elektroniczną** i odwrotnie. Pracownicy merytoryczni – w zależności od organizacji wewnętrznej usługodawcy powinni otrzymywać dokumenty w **formie** i **postaci** właściwej dla danej sprawy i charakteru czynności. . Pracownicy kancelarii nie załatwiają spraw bezpośrednio, a jedynie dbają o to, by do pracowników merytorycznych trafiały dokumenty wpływające opisane właściwymi, niezbędnymi metadanymi. Dokumenty papierowe oraz dostarczane na informatycznych nośnikach danych dokumenty elektroniczne – po wprowadzeniu ich do systemu EZD pozostają w składzie chronologicznym.

Schematycznie miejsce kancelarii w strukturze podmiotu realizującego zadania publiczne przedstawić można na poniższym rysunku:

| Wejście/wyjście | Podmiot realizujący zadania publiczne | | |
|---|---|---|---|
| [1] | [2] | [3] | [4] |
| 1. Informacja publiczna | 1. BIP / podmiotowa strona WWW | 1. Sieć komputerowa, elektroniczny system zarządzania dokumentami | 1. Departamenty, wydziały, ludzie wyposażeni w wiedzę i umiejętności, dokumenty w postaci papierowej, książki, intranet, bazy danych, systemy informatyczne do zarządzania bazami danych, rejestrami - wszelkie zasoby informacyjne w postaci elektronicznej i papierowej |
| 2. Telefon | 2. Call Center | | |
| 3. Faks | 3. Kancelaria (przesyłki papierowe, pisma wnoszone osobiście, przesyłki elektroniczne) | | |
| 4. Poczta elektroniczna | | | |
| 5. Poczta papierowa | | | |
| 6. Wizyta osobista | 4. Biuro Obsługi Interesanta | 2. Dokumenty papierowe | |

*Miejsce kancelarii w strukturze podmiotu realizującego zadania publiczne*

Na rysunku szare pola (kolumna [2]) oznaczają „interfejs" usługodawcy – miejsca wejścia/wyjścia danych i dokumentów W kolumnie [1] pokazane są różne możliwości przekazywania informacji i dokumentów – zarówno jednostronne (np. zamieszczanie informacji publicznej w BIP czy innych informacji (promocja, aktualności, komunikaty) na podmiotowej stronie WWW, jak i dwustronne – przesyłki papierowe, elektroniczne.

Przyjmowane dokumenty w **postaci papierowej** lub **elektronicznej** właściwym kanałem trafiają do pracowników merytorycznych (kolumna [4]), którzy zajmują się załatwianiem spraw Dzięki „interfejsowi" przedstawionemu w kolumnie [2] bezpośredni kontakt z interesantami nie dezorganizuje im pracy

### 3.1.1. System EZD

**System EZD** - uporządkowany zbiór dokumentacji w postaci nieelektronicznej, w układzie wynikającym z kolejności wprowadzenia do systemu EZD, utworzony w podmiocie, w którym wprowadzono system EZD; (Dz.U.2011.14.67)

Elektroniczna administracja posługuje się głównie dokumentami elektronicznymi. Dokumenty tworzone wewnątrz podmiotu (wewnętrzne) mogą być od razu tworzone w postaci elektronicznej jako **naturalne dokumenty elektroniczne,** w takiej postaci rejestrowane, przetwarzane, przechowywane, podpisywane i wysyłane. Jeśli jednak interesant (usługobiorca) zażąda odpowiedzi na papierze, wtedy dokument musi być wydrukowany i podpisany przez upoważnioną do tego osobę. Oczywiście dokumenty zarejestrowane w systemie elektronicznego zarządzania dokumentami pozostają w nim, mimo wysyłki. Należy pamiętać, że system EZD stanowi jednocześnie archiwum zakładowe.


Połączenie **systemu EZD** z **ePUAP** umożliwia bezpośrednie pobieranie dokumentów wpływających do **elektronicznej skrzynki podawczej** podmiotu. System EZD umożliwia wykonanie wszelkich podstawowych czynności w odniesieniu do dokumentu elektronicznego (utworzenie dokumentu, opisanie go metadanymi), ale przekazywanie go dalej zgodnie z procedurą – do kolejnych pracowników Na każdym etapie możliwe jest wygenerowanie **karty obiegu dokumentu** – chronologicznego zapisu wszystkich czynności, jakie w odniesieniu do danego dokumentu zostały wykonane, oraz komentarzy dopisywanych przez pracowników System przechowuje i w prosty sposób udostępnia wszystkie kolejne wersje dokumentu wraz z informacją kto (imię i nazwisko pracownika) i kiedy (czas w formacie rrrr-mm-dd gg:mm:ss) daną wersję utworzył. Zapewnia to dowodowość postępowania.

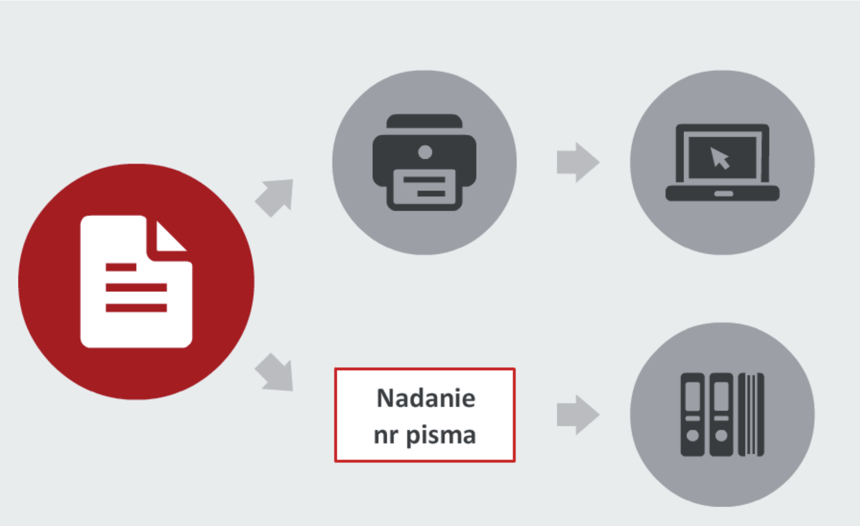
Wszystkie wpisy w karcie obiegu dokumentu tworzone są automatycznie przez system, co jest doskonałą pomocą przy optymalizacji procedury załatwiania sprawy, szczególnie, że rejestr zdarzeń można wyeksportować do pliku w formacie xls czy csv (i innych). Można przeanalizować całą drogę pisma – i „wyprostować" (skrócić drogę) pism tego samego rodzaju w przyszłości.

Ponieważ system EZD umożliwia wykonywanie tych wszystkich czynności w odniesieniu do dokumentów elektronicznych, jakie wykonuje się w odniesieniu do dokumentów papierowych, ale pozwala to zrobić szybciej, lepiej i taniej (wraz z automatycznym dokumentowaniem), co do zasady nie należy prowadzić równolegle systemów zarządzania dokumentami papierowymi i elektronicznymi. Jeśli kierownik podmiotu podjął decyzję o wprowadzeniu systemu EZD, należy nim zastąpić dotychczasowy system zarządzania dokumentami papierowymi (tzw papierowy obieg dokumentów).

### 3.1.2. Skład chronologiczny

> **Skład chronologiczny** - uporządkowany zbiór dokumentacji w postaci nieelektronicznej, w układzie wynikającym z kolejności wprowadzenia do systemu EZD, utworzony w podmiocie, w którym wprowadzono system EZD; (Dz.U.2011.14.67)

Dokumenty papierowe wpływające do podmiotu nie powinny go „zaśmiecać" Pracownicy kancelarii, po wprowadzeniu treści papierowego dokumentu do systemu EZD (poprzez skanowanie i zarejestrowanie skanu w systemie EZD) umieszczają dokumenty papierowe w składzie chronologicznym. Wszelkie dalsze czynności związane np. z tworzeniem odpowiedzi na pismo wpływające wykonywane są już całkowicie w EZD – łącznie z przekazywaniem do podpisu i wysyłką.

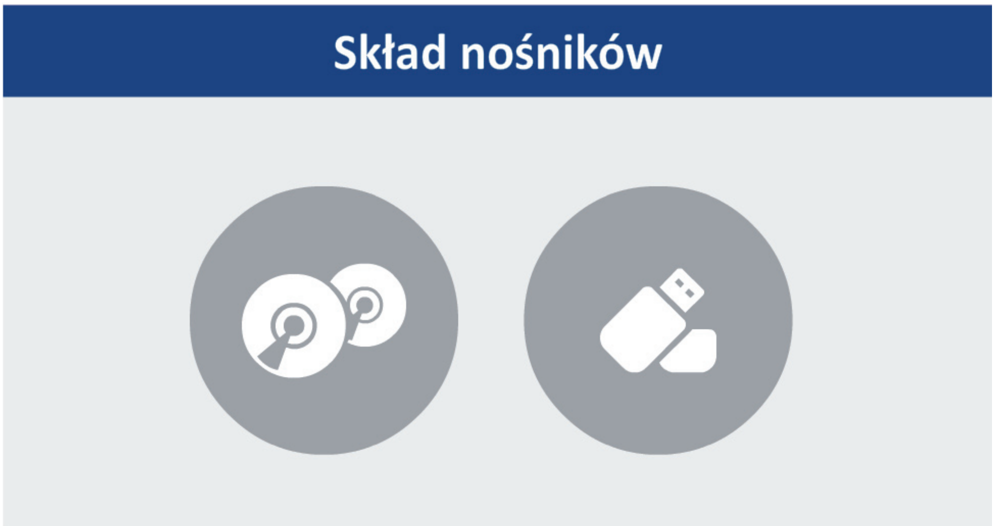



Jeśli pismo ma być wysłane w postaci papierowej, wykonuje się wydruk kompletnego i podpisanego elektronicznie pisma z EZD i po opatrzeniu go własnoręcznym podpisem przez osobę upoważnioną wysyła do adresata. Każdy dokument zarejestrowany w EZD oznakowany jest unikatowym numerem pisma (**UNP**). Numer ten jest jednoznacznym identyfikatorem pisma (a także ewentualnych załączników do niego) w systemie. Należy zaznaczyć, że w sytuacjach, w których jest potrzebne np. wydanie wiarygodnej, źródłowej kopii pisma, numer UNP jest bardzo przydatny, gdyż pozwala natychmiast odnaleźć poszukiwane pismo. Wszystkie kopie oryginalnego dokumentu źródłowego będą identyczne. Dokumenty przechowywane w składzie chronologicznym są oryginałami pism przychodzących - ale dzięki takiemu ich przechowywaniu nie ulegają rozproszeniu i zagubieniu.

### 3.1.3. Skład nośników informatycznych

**Skład informatycznych nośników danych** - uporządkowany zbiór informatycznych nośników danych zawierających dokumentację w postaci elektronicznej; (Dz.U.2011.14.67)

Z uwagi na odmienność postaci dokumentów i fizyczną odmienność informatycznych nośników danych (najczęściej dyski CD, ale także pamięci USB i inne nośniki z zapisanymi na nich plikami i dokumentami w postaci elektronicznej) tworzy się odrębne składy – analogiczne do składów chronologicznych dokumentów papierowych.




Aktualnie (rok 2015) popularne jest przesyłanie na dyskach CD dokumentów w formacie xls, .xlsx oraz dokumentów w formie graficznej, których wydruk mógłby być kłopotliwy ze względu na format (trudność zmieszczenia wydruku na kartce papieru w formacie A4 lub nawet A3, utratę formuł w arkuszach kalkulacyjnych pozwalających na weryfikację poprawności obliczeń itd.). Często zapomina się, że dokumenty te można równie dobrze przesyłać drogą elektroniczną bez potrzeby przesyłania nośników – i również otrzymać urzędowe poświadczenie przedłożenia.

## 3.2. Biuro Obsługi Interesanta

W dobrze zorganizowanym urzędzie interesanci załatwiani są właśnie przez cztery moduły „interfejsu” stanowiącego kolumnę [2] tabeli pokazanej na rysunku.

| Wejście/wyjście | Podmiot realizujący zadania publiczne | | |
|---|---|---|---|
| [1] | [2] | [3] | [4] |
| 1. Informacja publiczna | 1. BIP / podmiotowa strona WWW | 1. Sieć komputerowa, elektroniczny system zarządzania dokumentami | 1. Departamenty, wydziały, ludzie wyposażeni w wiedzę i umiejętności, dokumenty w postaci papierowej, książki, intranet, bazy danych, systemy informatyczne do zarządzania bazami danych, rejestrami - wszelkie zasoby informacyjne w postaci elektronicznej i papierowej |
| 2. Telefon | 2. Call Center | | |
| 3. Faks | 3. Kancelaria (przesyłki papierowe, pisma wnoszone osobiście, przesyłki elektroniczne) | | |
| 4. Poczta elektroniczna | | | |
| 5. Poczta papierowa | | | |
| 6. Wizyta osobista | 4. Biuro Obsługi Interesanta | 2. Dokumenty papierowe | |

Jednym z tych modułów jest Biuro Obsługi Interesanta (BOI). BOI przyjmuje interesantów przychodzących do urzędu, stawiających się osobiście. Pracownicy BOI – w zależności od zakresu spraw realizowanych w poszczególnych „okienkach” – przyjmują papierowe dokumenty bezpośrednio od interesantów lub wydają dokumenty, które interesanci postanowili odebrać osobiście. Pracownicy ci udzielają także informacji dotyczących procedur załatwiania poszczególnych spraw, lub – w niektórych przypadkach - bezpośrednio je załatwiają.

Rolą BOI jest m. innymi zapewnienie, by dokumenty dostarczane przez interesantów (usługobiorców) były kompletne, czytelne i nie powodowały potrzeby późniejszego wzywania interesanta do uzupełnienia braków W bardziej rozwiniętych systemach obsługi interesanta (np. miasto Nowon w Korei Płd.) wprowadzono w praktyce **ustne wnoszenie spraw** w BOI. Nie oznacza to jednak, że sprawy te załatwiane są w **formie ustnej**. Są załatwiane w formie pisemnej, dokumenty są utrwalone – różnica polega jedynie na tym, że to pracownik BOI wypełnia stosowne formularze. Przed rozpoczęciem wypełniania formularza urzędnik weryfikuje tożsamość interesanta na podstawie jego dowodu tożsamości. Pracownik BOI ma znacznie większą wiedzę merytoryczną i wprawę w wyszukiwaniu właściwych formularzy i ich wypełnianiu – jest to jego codzienna, rutynowa praca. Z tego właśnie powodu to on wypełnia stosowne formularze w systemie teleinformatycznym urzędu, okazuje je (po wypełnieniu) na monitorze interesantowi – a ten – po sprawdzeniu poprawności podanych danych składa **podpis własnoręczny** za pomocą tabletu. Całość podpisywana jest elektronicznie przez urzędnika – interesant otrzymuje kopię. Taki sposób wprowadzania danych skrócił 10-cio krotnie czas obsługi interesanta i znacząco podniósł jakość danych, spowodował istotne zmniejszenie formularzy służących do zbierania danych do zakresu rzeczywiście potrzebnego, a także obniżył koszty materialne (całkowita likwidacja papierowych formularzy, tonerów, pieczątek itp.).

## 3.3. Biuletyn Informacji Publicznej

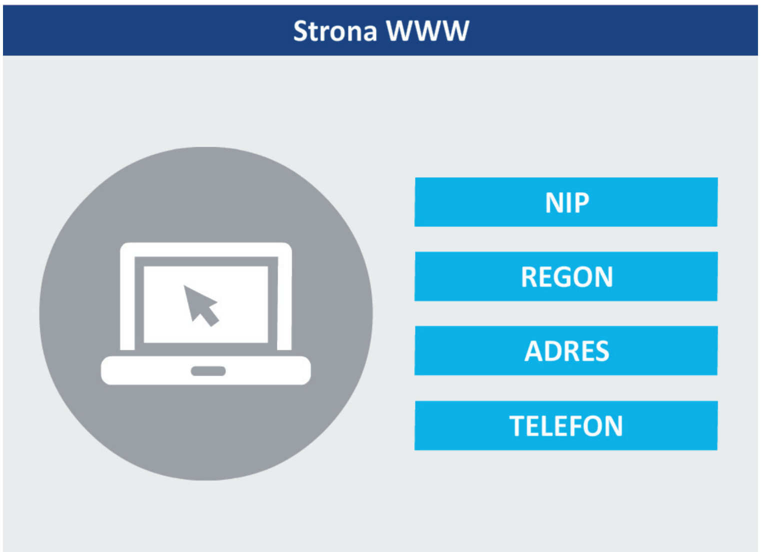
**Biuletyn Informacji Publicznej (BIP)** - urzędowy publikator teleinformatyczny stworzony w postaci ujednoliconego systemu stron w sieci teleinformatycznej, w celu powszechnego udostępniania informacji publicznej; (Dz.U.2014.782 j.t.)

Biuletyn Informacji Publicznej (strona główna BIP: https://www.bip.gov.pl/) stosowany jest przez zobowiązane do tego podmioty do publikowania informacji publicznej – i jest najczęściej wykorzystywany do uzyskiwania przez zainteresowanych podstawowych informacji dotyczących danego podmiotu oraz jego działalności.

Przedmiotem publikacji w BIP dane kontaktowe, dane o kierownictwie i zakresie działalności, majątku, o ofertach pracy i zamówieniach publicznych. Praktyka pokazuje, że podmioty, które w sposób zgodny z prawem aktualizują stronę podmiotową BIP i zamieszczają na niej bieżące i aktualne informacje publiczne same odnoszą z tego tytułu bezpośrednie korzyści – chociażby przez brak potrzeby udzielania odpowiedzi na pytania, na które odpowiedzi znaleźć można w BIP Należy podkreślić, że zgodnie z prawem strona BIP nie może zawierać reklam, a jedynie informacje – i to informacje publiczne, dostępne dla każdego anonimowego odbiorcy bez ograniczeń. Reklama z samej swej natury jest stronnicza, tendencyjna, gdyż pokazuje jedynie aspekty korzystne z punktu widzenia potencjalnego odbiorcy, a więc jest tylko częściowo prawdziwa – i z tego powodu nie może być publikowana w BIP Istnieje możliwość realizacji funkcji strony BIP przez pewien wydzielony obszar podmiotowej strony WWW – jednak wymaga to oznakowania informacji publicznej za pomocą logo BIP Podręcznik redaktora strony podmiotowej BIP dostępny jest pod adresem http://www.bip.gov.pl/files

## 3.4. Strona WWW

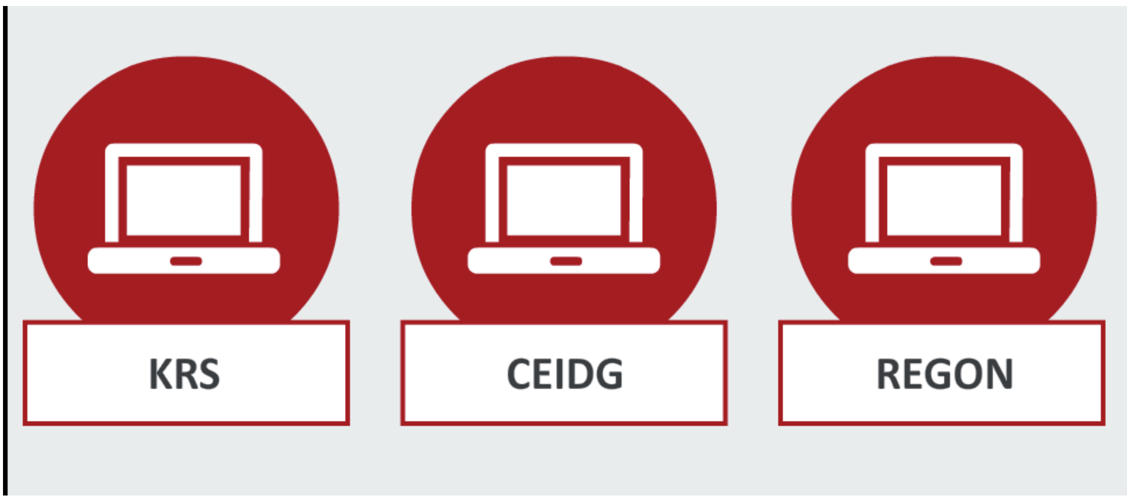
Podmiotowa strona WWW – w przypadku podmiotów realizujących zadania publiczne spełniać może wiele różnych funkcji. Zazwyczaj – z uwagi na aktualny poziom rozwoju technicznego i upowszechnienie się dostępu do Internetu oraz łatwość korzystania ze stron internetowych strony WWW traktowane są przez **usługodawców** jako miejsce reklamy i promocji ich działalności.




Oczywiście informacje (często będące powieleniem tych samych informacji zamieszczonych w BIP, zwłaszcza jeśli chodzi o dane adresowe, numery REGON i NIP, strukturę organizacyjną) również są publikowane na podmiotowych stronach WWW, jednak strona podmiotowa ma w istocie funkcję reklamową, ma zachęcać do jej odwiedzania, gdyż „reklama dźwignią handlu" Wprawdzie podmioty realizujące zadania publiczne mają ściśle określony zakres działalności wynikający z przepisów prawa i statutów tych podmiotów, jednak świadomość owego zakresu działania w społeczeństwie nie jest powszechna. Z tego powodu dobrze skonstruowana strona jest bardzo dobrym miejscem informacji o działalności podmiotu – takiej informacji, dla której ramy BIP są za wąskie. W praktyce podmiotowe strony WWW (na których znajdować się musi odnośnik do podmiotowej strony BIP) odwiedzane są znacznie częściej niż podmiotowe strony BIP Na podmiotowej stronie WWW powinny znajdować się odnośniki do wszelkich zasobów podmiotu, które związane są z realizacją jego zadań. Szczególnie ważna jest publikacja adresu **elektronicznej skrzynki podawczej** (ESP), umożliwiającej usługobiorcy (interesantowi) kontakt z podmiotem w sposób zapewniający uzyskanie **urzędowego poświadczenia przedłożenia** (UPP). Informacje kontaktowe (adresy, telefony, adres poczty elektronicznej oraz elektronicznej skrzynki podawczej, identyfikator REGON powinny być łatwo dostępne - czyli pod klawiszem „kontakt" na stronie głównej podmiotu, a okienko wyszukiwarki powinno znajdować się w polu widzenia bezpośrednio po otwarciu podmiotowej strony WWW

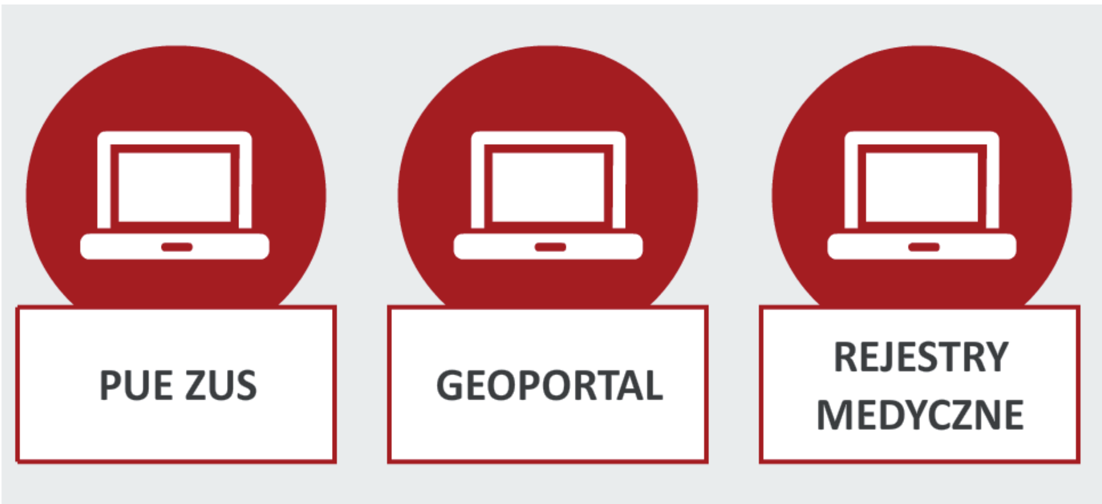
## 3.5. Usługi oparte na dostępie bezpośrednim – transakcyjne

Niektóre usługi podmiotów realizujących zadania publiczne mogą być wykonane bez bezpośredniego udziału pracowników tego podmiotu. Głównie chodzi tu o usługi informacyjne, jednak dotyczące informacji niebędących informacjami publicznymi (tzn. niepodlegającym publikacji w BIP). Przykładami takich usług mogą być np. udostępnianie danych (odpisów) z Krajowego Rejestru Sądowego (https://ems.ms.gov pl/krs/wyszukiwaniepodmiotu), danych dotyczących przedsiębiorców z Centralnej Ewidencji i Informacji o Działalności Gospodarczej (https://prod.ceidg.gov pl/CEIDG/CEIDG.Public.UI/Search.aspx) czy danych z rejestru REGON (https://wyszukiwarkaregon.stat.gov pl/appBIR/index.aspx). Usług tego typu świadczonych przez podmioty realizujące zadania publiczne jest już bardzo wiele. Są to zarówno usługi niewymagające identyfikacji odbiorców informacji, jak i usługi wymagające identyfikacji odbiorców W takich przypadkach stosowany jest podpis potwierdzony profilem zaufanym ePUAP



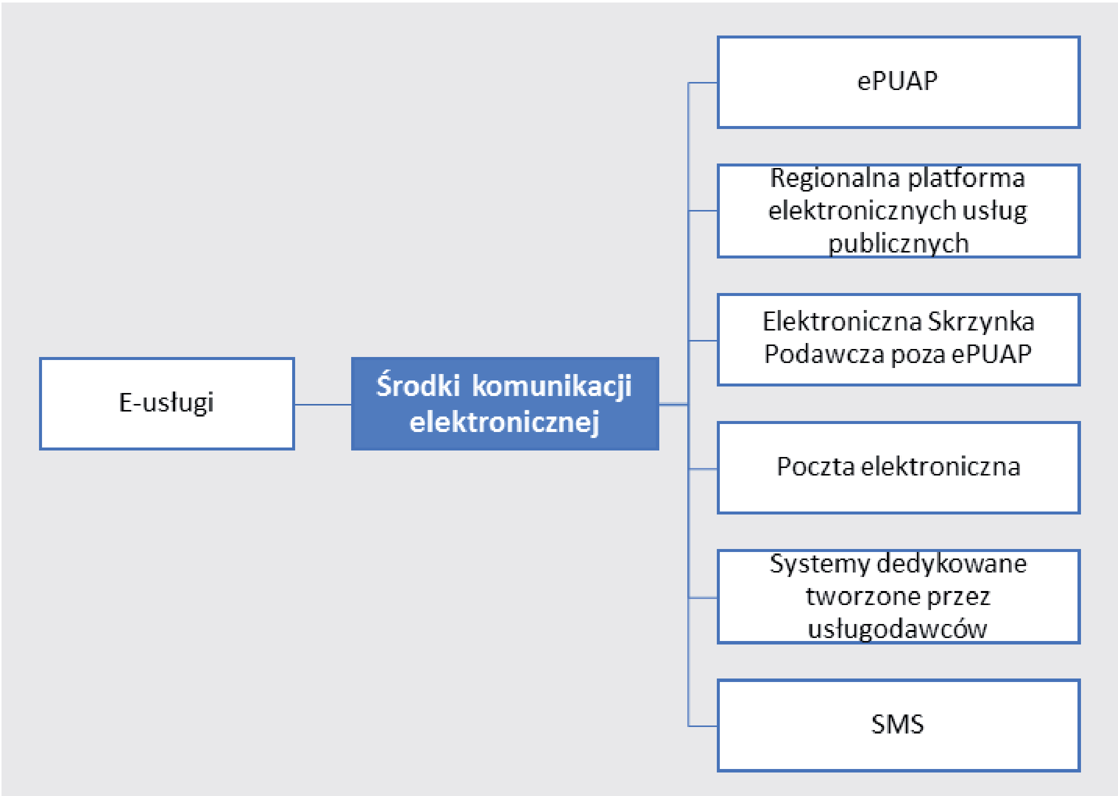
## 3.6. Systemy dedykowane

Niektóre usługi podmiotów realizujących zadania publiczne są bardziej złożone i pozwalają nie tylko na zadawanie pytań i bezpośrednie uzyskiwanie odpowiedzi na nie, ale także pozwalają na wykonywanie pytań złożonych, dokonywanie symulacji albo na kontaktowanie się z pracownikami danego podmiotu w ramach wewnętrznego systemu komunikacyjnego. Generalnie tworzone są jako rozwiązania odrębne, całkowicie osadzone w obszarze merytorycznym danego podmiotu. Przykładami mogą być PUE ZUS (https://pue.zus.pl/), Geoportal (http://geoportal.gov.pl/), Rejestry medyczne (http://www.rejestrymedyczne.csioz.gov.pl/). Co do zasady, są one dostępne dla każdego po spełnieniu pewnych warunków (np. założenie konta, posługiwanie się profilem zaufanym lub podpisem kwalifikowanym, albo tylko loginem i hasłem) – i, co ważne, są nieodpłatne.



# 4. Środki komunikacji elektronicznej

**Środki komunikacji elektronicznej (droga elektroniczna)** - rozwiązania techniczne, w tym urządzenia teleinformatyczne i współpracujące z nimi narzędzia programowe, umożliwiające indywidualne porozumiewanie się na odległość przy wykorzystaniu transmisji danych między systemami teleinformatycznymi, a w szczególności pocztę elektroniczną; (Dz.U.2013.1422 j.t.)




*Środki komunikacji elektronicznej stosowane we wzajemnej komunikacji usługobiorców i usługodawców.*

Powyższa definicja dobrze ilustruje istotę **środków komunikacji elektronicznej** – trzeciego z czterech elementów e-usługi. Urządzenia teleinformatyczne oraz narzędzia programowe łącznie tworzą **kanał komunikacyjny**, bez którego **świadczenie usług drogą elektroniczną** w dowolnym czasie i miejscu (z punktu widzenia usługobiorcy) byłoby niemożliwe, ponieważ nie dochodziłoby do przesyłania danych i dokumentów niezbędnych usługodawcy do realizacji e-usługi wszczętej przez usługobiorcę.

**Poziomy świadczenia e-usług**

Wszczynanie sprawy realizowanej drogą elektroniczną może odbywać się w różny sposób – uzależnione jest to od rodzaju tej usługi, która może być świadczona na jednym z czterech poziomów: informacyjnym, interakcyjnym, transakcyjnym i integracji.

**Poziom informacyjny** – usługodawcy publikują informacje na stronach WWW, w BIP, a usługobiorcy przeglądając opublikowane informacje (np. o zamówieniach publicznych) na swoich komputerach albo w kioskach informacyjnych uzyskują potrzebne informacje;

**Poziom interakcyjny** – usługobiorca może komunikować się drogą elektroniczną z poszczególnymi, pojedynczymi usługodawcami (ściślej – z ich pracownikami), ale usługodawcy nie zawsze komunikują się drogą elektroniczną. W obecnym jednak stanie prawnym, w świetle art. $39^1$ kpa usługodawcy muszą dostosować się do życzeń usługobiorców odnośnie wybranego przez nich środka komunikacji.

**Poziom transakcyjny** – usługobiorca korzysta z odpowiednio przygotowanych aplikacji, udostępnianych przez usługodawców na stronach internetowych, komunikuje się drogą elektroniczną, a odpowiednio przygotowane aplikacje realizują usługę. Taki poziom możliwy jest jednak tylko w szczególnych przypadkach, gdy procedura załatwiania sprawy jest dobrze zalgorytmizowana, tzn. poprawne działanie usługobiorcy oraz usługodawcy zawsze prowadzi do jej zakończenia, ponieważ system uwzględnia wszystkie mogące zaistnieć przypadki oraz stosowne komunikaty, pomagające usługobiorcy przejść przez tę procedurę. Środki komunikacji elektronicznej w takim przypadku muszą być niezawodne, gdyż nie można dopuścić do stosowania środków niedających pewności co do skuteczności transmisji danych czy pewności co do samego faktu przesłania dokumentów

**Poziom integracji** – usługobiorca, korzystając z portalu o określonym, dedykowanym przeznaczeniu używa aplikacji udostępnionej przez usługodawcę, instalowanej na komputerze usługobiorcy, tworzącej środowisko niezbędne do rozpoczęcia korzystania z usługi. System udostępnia wszelkie niezbędne informacje i narzędzia pozwalające na kompletne załatwienie nawet złożonej sprawy, wymagającej pobrania informacji od innych usługodawców (urzędów) – np. w celu weryfikacji danych podawanych przez usługodawcę, zabezpieczenia go przed popełnieniem elementarnych błędów itd. Oprogramowanie takie udostępniane jest przez usługodawcę jako aplikacja wykonywalna. W celu udostępnienia złożonej usługi konieczne jest wcześniejsze przygotowanie systemów teleinformatycznych i baz danych oraz rejestrów współdziałających podmiotów Przy tego rodzaju usłudze usługobiorca proszony jest o wypełnienie **elektronicznego formularza**, gromadzącego niezbędne dane, wśród których znajdują się również **dane identyfikujące**

**osobę** **usługobiorcy**, pozwalające na dokonanie pewnych kontrolnych weryfikacji. Systemy wewnętrzne **usługodawców** współdziałające w realizacji takiej złożonej usługi są zintegrowane na bazie zalgorytmizowanych procesów administracyjnych. Poziom integracji stwarza możliwość dokonania wszystkich czynności niezbędnych do załatwienia danej sprawy urzędowej drogą elektroniczną – od uzyskania informacji, poprzez pobranie odpowiednich formularzy i po ich wypełnieniu odesłanie ich drogą elektroniczną, a także, jeśli są wymagane, wniesienie opłat (przelewem, kartą płatniczą itp.). Również w tym przypadku środki komunikacji elektronicznej muszą być szczególnie niezawodne.


**Środki komunikacji elektronicznej - możliwości**

Opisane wyżej usługi realizowane są w oparciu o bezpośrednią komunikację polegającą na korzystaniu usługobiorcy z systemów teleinformatycznych udostępnianych przez usługodawcę. Jednak w praktyce usługobiorcy najchętniej woleliby korzystać z możliwości przesyłania dokumentów pocztą elektroniczną, a w przypadku najprostszych usług – poprzez korzystanie z portalu udostępnionego przez usługodawcę. Istnieje kilka możliwości przesyłania dokumentów za pośrednictwem środków komunikacji elektronicznej; należą do nich:

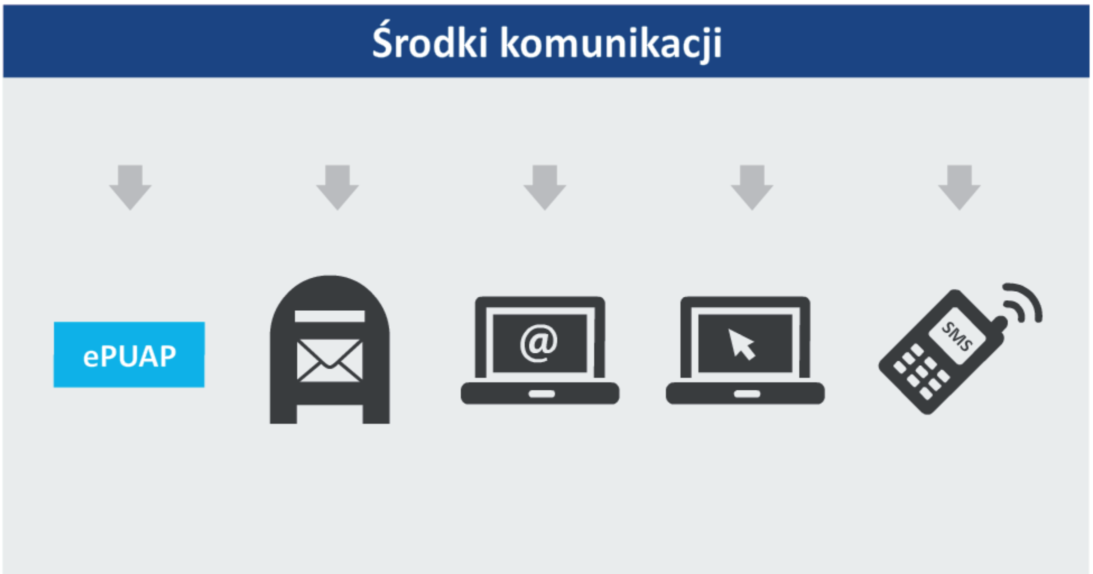
(1) **<u>ePUAP</u>** lub **<u>regionalna platforma elektronicznych usług publicznych</u>**

(2) **<u>Elektroniczna Skrzynka Podawcza</u>** poza ePUAP

(3) Poczta elektroniczna

(4) Dedykowany system, przeznaczony do komunikacji z usługodawcą i przez niego zarządzany

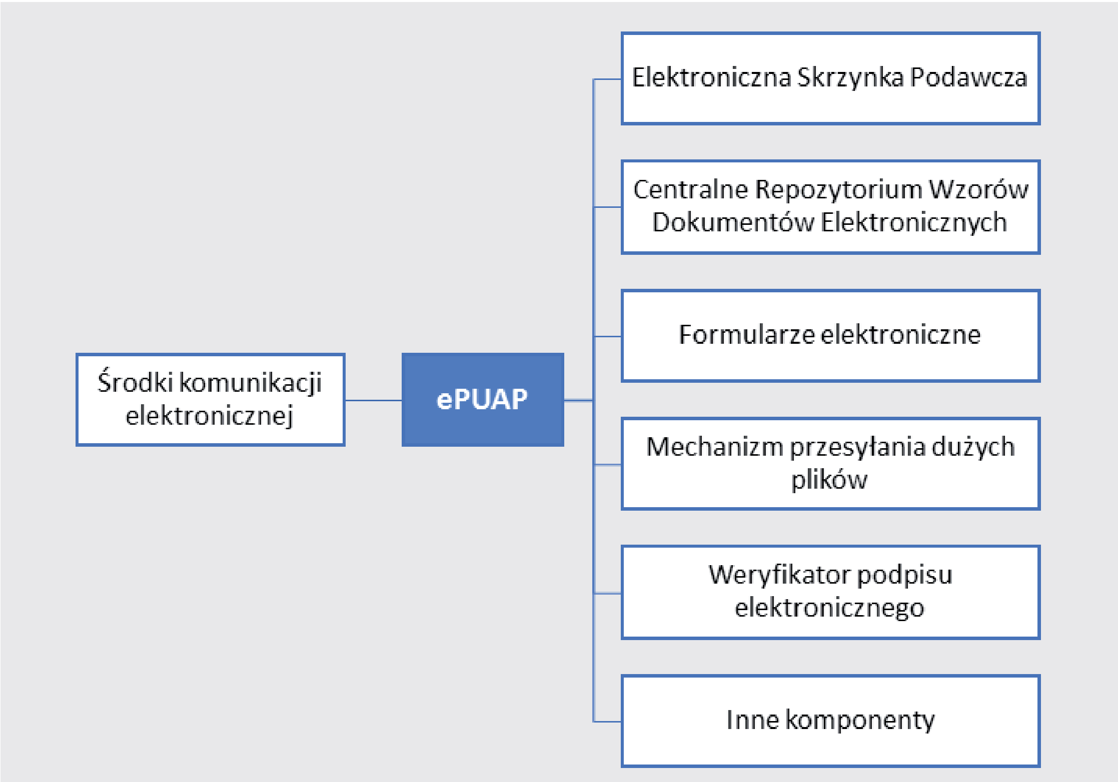
(5) SMS




E-usługi wymagają stosowania **środków komunikacji elektronicznej** we wzajemnych relacjach między usługodawcami a usługobiorcami. W definicji wskazano „w szczególności pocztę elektroniczną", ponieważ w czasach, gdy jej używanie stało się już dość powszechne, wielu administratywistów i prawników miało wątpliwości, czy taki środek komunikacji może być w ogóle uznany Chodziło o zachowanie dowodowości postępowania, o pewność przekazywania przesyłek, o identyfikację stron postępowania, a nawet o archaiczne już dzisiaj rozumienie pojęcia „pisemności", rozumianego jako pisma na papierze podpisanego własnoręcznie przez wnioskodawcę. Rozpatrując jednak środki komunikacji elektronicznej w kontekście jednego z głównych elementów składowych **e-usług** – w których co do zasady nie używa się jako nośnika papierowego, poczta elektroniczna jest z całą pewnością ważnym elementem – tak ważnym, jak listy zwykłe w odniesieniu do korespondencji z wykorzystaniem pism w postaci papierowej. Pisma w postaci papierowej przesłane zwykłą pocztą również mogą nie docierać do adresatów, również mogą zawierać braki formalne czy merytoryczne, również nie dają pewności co do tożsamości osoby, która je podpisała, a jednak nikt takich przesyłek nie kwestionuje. Wobec tego nieufne podejście do poczty elektronicznej wymaga rewizji szczególnie, że obecnie istnieją możliwości wykorzystywania jej jako dodatkowego, pomocniczego środka komunikacji, np. informującego o nadejściu „przesyłki poleconej" w systemie ePUAP

## 4.1. ePUAP

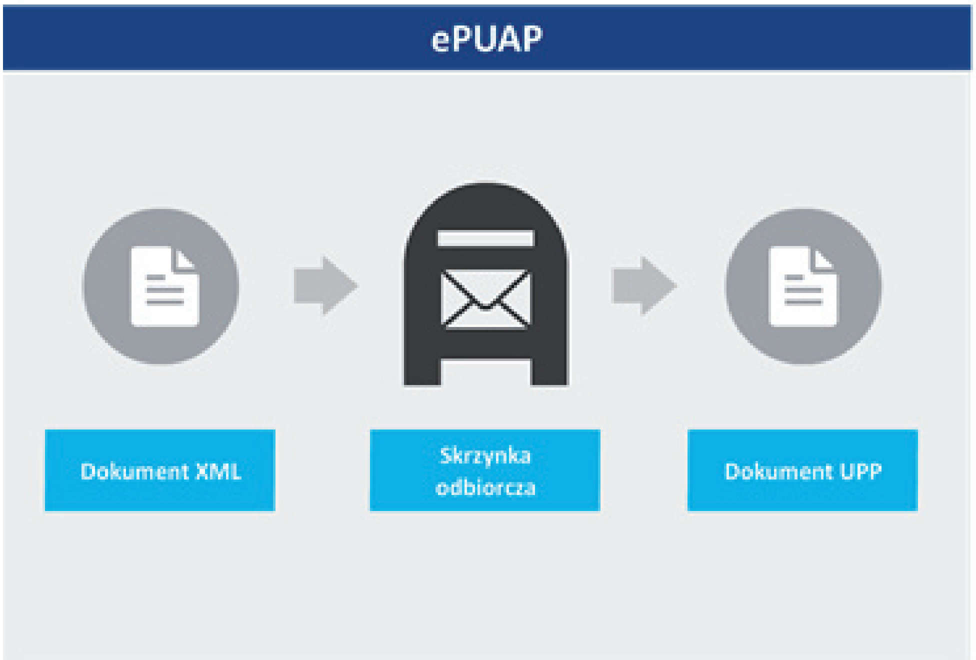
| |
|---|
| **Elektroniczna platforma usług administracji publicznej (ePUAP)** - system teleinformatyczny, w którym instytucje publiczne udostępniają usługi przez pojedynczy punkt dostępowy w sieci Internet; (Dz.U.2014.1114 j.t.) |




*ePUAP*

**Komunikacja - przekazywanie dokumentów xml**

Komunikacja za pośrednictwem ePUAP (platforma krajowa) lub za pośrednictwem regionalnej platformy elektronicznych usług publicznych oparta jest o przekazywanie **dokumentów xml** tworzonych na podstawie opublikowanych w centralnym /regionalnym repozytorium **wzorów dokumentów**. Przekazywanie odbywa się w ramach jednego, tego samego systemu, którego użytkownikami są zarówno usługobiorca, jak i usługodawca, w bezpiecznym środowisku. Dokument tworzony jest w tle, dane w nim zawarte wprowadzane są za pomocą **elektronicznych formularzy** wypełnianych przez usługobiorcę. **Dokumenty xml**, po ich utworzeniu i kompletnym wypełnieniu, przekazywane są na odpowiedni dla danej usługi lub wybrany przez twórcę dokumentu **adres elektroniczny** skrytki, z której są odbierane przez pracowników **kancelarii** czy **punktu kancelaryjnego** usługodawcy lub automatycznie pobierane są przez specjalnie przygotowaną aplikację w **systemie teleinformatycznym usługodawcy**. Przekazanie dokumentu poprzedzone jest jego **walidacją**. System weryfikuje dane stanowiące **podpis elektroniczny** – jakkolwiek byłby on w danym przypadku składany Jeśli proces weryfikacji przebiegnie poprawnie, generowany jest stosowny komunikat oraz wystawiane **Urzędowe Poświadczenie Odbioru (UPO)** - które należy w tej sytuacji definiować i pojmować jako **Urzędowe Poświadczenie Przedłożenia (UPP)**.




Wynika to z faktu, że podmiot przyjmuje dokumenty przesłane drogą elektroniczną w trybie 24/7/365, tzn. przez 24 godziny 7 dni w tygodniu, 365 dni w roku. Odbiór przesyłek wysyłanych do usługobiorcy będącego osobą fizyczną potwierdzany będzie **Urzędowym Poświadczeniem Doręczenia (UPD)**. Przyjęcie przesyłki przesłanej do podmiotu potwierdzane jest automatycznie przez **Elektroniczną Skrzynkę Podawczą** bez udziału człowieka. Jeśli wystąpi jakikolwiek błąd – bez względu na jego źródło – również generowany jest stosowny komunikat, a dokument nie jest przyjmowany  Niektóre systemy umożliwiają także śledzenie statusu przesłanego **dokumentu xml,** jeśli jego walidacja może trwać dłużej. Nie kończy to usługi – jest jedynie jej zainicjowaniem. Po odebraniu dokumentu xml pracownicy usługobiorcy identyfikują nadawcę (usługobiorcę), weryfikują podpis elektroniczny, odczytują pismo przewodnie lub „kopertę" w celu przekazania dokumentu merytorycznie właściwej komórce organizacyjnej czy konkretnemu pracownikowi. W przypadku tego środka komunikacji – z uwagi na zastosowane metody zapewnienia integracji – **podpis kwalifikowany** lub **profil zaufany ePUAP** – podpisane dokumenty weryfikowalne są bardzo łatwo dzięki zaimplementowanym na platformach e-usług aplikacjom służącym do **weryfikacji podpisów elektronicznych**.

**Dokument xml - kontener na dane**

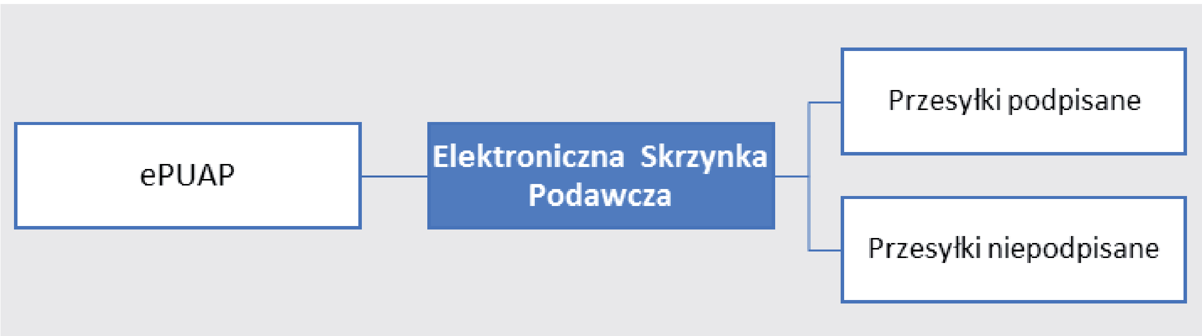
Przekazywanie **dokumentu xml** na platformie ePUAP / platformie regionalnej zasadniczo różni się od przesyłania dokumentów pocztą elektroniczną. Każdy **dokument xml** składa się z **dokładnie jednego dokumentu głównego**, wewnątrz którego mogą być przekazywane inne dokumenty, np. załączniki dołączane z dysku lokalnego usługobiorcy Jednak fakt, że główny dokument jest **dokumentem xml** ma swoje istotne konsekwencje. Podpisanie go elektroniczne **jednym tylko podpisem** zapewnia integralność **wszystkim dokumentom** i kontenerom na dane znajdującym się wewnątrz tego pliku głównego. Temat ten jest szerzej omówiony w rozdziale dotyczącym dokumentu elektronicznego. Stosowanie tego środka komunikacji zapewnia uzyskanie **UPP**, czyli można go traktować jako kanał nadawania przesyłki poleconej z potwierdzeniem odbioru – tyle że szybciej, pewniej i bezpłatnie. Na koniec należy zdecydowanie wskazać, że osobami odpowiedzialnymi i właściwymi do odbierania przesyłek z **elektronicznej skrzynki podawczej (ESP)** są pracownicy Kancelarii, a nie informatycy Informatycy winni zapewnić poprawną konfigurację ESP oraz – w podmiotach posiadających elektroniczny system zarządzania dokumentami (EZD) – integrację z tym systemem. Czynności odbierania oraz ekspedycji przesyłek – bez względu na ich postać – należą do pracowników Kancelarii, którzy powinni opanować nowe umiejętności, związane z **konwersją formy** i **postaci** dokumentów przychodzących i wychodzących.


W zamierzeniu ustawodawcy platforma ePUAP miała spełniać funkcję centralnego rozwiązania, które byłoby „punktem startowym” w poszukiwaniu e-usług świadczonych przez podmioty realizujące zadania publiczne. Innymi słowy, ePUAP miał umożliwiać zarówno odszukanie konkretnej usługi, jak i umożliwić skorzystanie z niej. Korzystanie z usługi może wiązać się zarówno z uzyskiwaniem informacji, jak i składaniem wniosków na udostępnionych formularzach.

To specyfika danej usługi determinuje zakres koniecznych środków – zarówno komunikacji, jak i dokumentowania przebiegu - wiąże się z użyciem środków adekwatnych do sytuacji. Elektroniczna Platforma Usług Administracji Publicznej wyposażona została w różnego rodzaju moduły dedykowane do realizacji zadań związanych z przyjmowaniem, wysyłaniem (importem i eksportem) dokumentów elektronicznych, kopiowaniem, podpisywaniem i weryfikowaniem podpisów, instalacją e-usług na tej platformie.

### 4.1.1. Elektroniczna Skrzynka Podawcza

**Elektroniczna skrzynka podawcza (ESP)** - dostępny publicznie środek komunikacji elektronicznej służący do przekazywania dokumentu elektronicznego do podmiotu publicznego przy wykorzystaniu powszechnie dostępnego systemu teleinformatycznego; (Dz.U.2014.1114 j.t.)




*Elektroniczna Skrzynka Podawcza*

Powyższa definicja jednoznacznie wskazuje, że chodzi o **środek komunikacji elektronicznej** dostępny publicznie, a więc dla każdego (bez opłat) służący do przekazywania **dokumentu elektronicznego** do podmiotu publicznego.

Cechą istotną tego środka komunikacji jest to, że jest on częścią systemu ePUAP, jego modułem, zarządzanym przez ministra właściwego ds. informatyzacji. Elektroniczna Skrzynka Podawcza podmiotu publicznego wystawia **Urzędowe Poświadczenie Przedłożenia** dokumentu przesłanego na jej adres (mający format inny niż poczta elektroniczna): /id_podmiotu/SkrytkaESP Przesłanie przesyłki pomiędzy użytkownikami ePUAP jest w istocie przekazaniem jej w ramach jednego systemu; jest to rozwiązanie dużo bardziej bezpieczne, niż poczta elektroniczna, gdyż przesyłka nie opuszcza bezpiecznego środowiska. Z punktu widzenia nadawcy przesyłki ważna jest funkcja dostarczenia przesyłki w sposób udowadnialny, a także możliwość jej pobrania na swój dysk. Przesyłki tworzone są jako dokumenty elektroniczne w formacie XML, co ma swoje daleko idące konsekwencje.

Elektroniczna skrzynka podawcza może być odpowiednio skonfigurowana przez usługodawcę – i np. nie przyjmować niepodpisanych przesyłek, dla zapewnienia bezpieczeństwa obrotu prawnego i rozliczalności. Jednak nie każda przesyłka musi być podpisana – wniosek o udostępnienie informacji publicznej nieudostępnionej w BIP wymaga wprawdzie podania adresu zwrotnego, natomiast nie wymaga podpisu.

Należy podkreślić, że Elektroniczna Skrzynka Podawcza na ePUAP jest dla instytucji publicznej rozwiązaniem idealnym, gdyż nie pociąga za sobą żadnych dodatkowych kosztów po stronie podmiotu (usługodawcy) ani po stronie usługobiorcy – jest utrzymywana z pieniędzy podatnika. Jednak wydaje się, że rozwiązanie takie stawia interesanta w nierównoważnej pozycji w stosunku do urzędu, gdyż wszelkie dowody – zarówno przesyłane dokumenty jak i dowody ich dostarczenia (UPP) przechowywane są u jednej ze stron – a nie u tzw „zaufanej strony trzeciej” Może to budzić poważne wątpliwości – szczególnie u obywateli, którzy z różnych przyczyn nie mają pełnego zaufania do państwa…

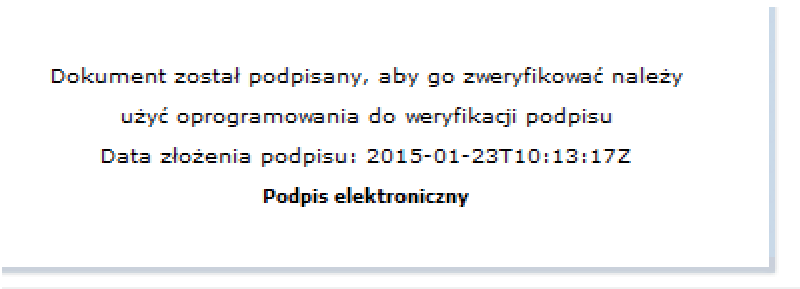
#### 4.1.1.1. Przesyłki podpisane

Przesyłki przekazywane za pośrednictwem Elektronicznej Skrzynka Podawczej należy traktować jako elektroniczną analogię papierowej przesyłki poleconej ze zwrotnym potwierdzeniem odbioru. Aby przesyłka mogła być traktowana jako dokument (stanowiący potencjalny dowód w przyszłości) musi być elektronicznie podpisana.

Istnieją trzy podstawowe możliwości podpisywania dokumentu elektronicznego przesyłanego za pośrednictwem ESP

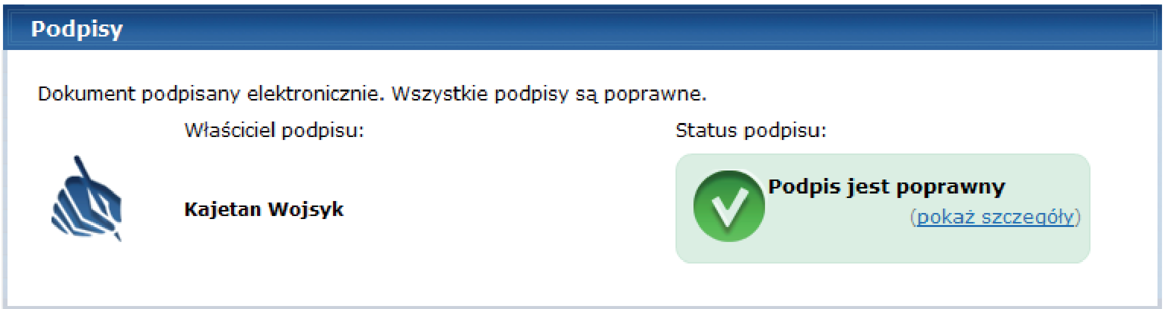
Sposób pierwszy, to podpisanie pisma ogólnego do podmiotu publicznego podpisem kwalifikowanym lub podpisem potwierdzonym profilem zaufanym ePUAP Taki podpis jest zabezpieczeniem zawartości wszystkich kontenerów z danymi i dokumentów, zawartych w pliku XML stanowiącym pismo przewodnie i zarazem dokument główny

Fakt złożenia podpisu widoczny jest u dołu pisma ogólnego (stanowiącego pismo przewodnie i jednocześnie kontener dla kolejnych kontenerów zawierających ewentualne załączniki – każdy w odrębnym kontenerze). Nad słowami „Podpis elektroniczny” widoczna jest informacja, że dokument został podpisany, a także podane są data i czas złożenia podpisu




*Pismo ogólne do podmiotu publicznego podpisane elektronicznie jednym podpisem (zrzut ekranu przedstawiający pismo ogólne do podmiotu publicznego).*

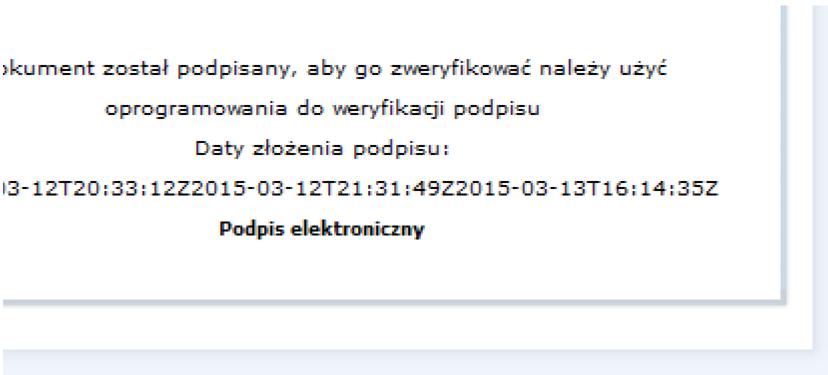
Odbiorca może podpis zweryfikować bezpośrednio dzięki zaimplementowanemu na platformie ePUAP weryfikatorowi podpisów elektronicznych:




*Widok okienka weryfikatora podpisu – informacja o stanie podpisu i odnośnik (pokaż szczegóły) pozwalający na odczytanie szczegółów złożonego podpisu – danych z certyfikatu.*

Jeśli przesyłka zostanie z Elektronicznej Skrzynki Podawczej pobrana do EZD, wtedy podpis będzie można zweryfikować w EZD

Gdyby dokument podpisany był wielokrotnie (są sytuacje wymagające np. dwóch lub więcej podpisów – Głównego Księgowego i kierownika podmiotu oraz radcy prawnego), wtedy w okienku weryfikatora widoczne będą imiona i nazwiska osób podpisujących, a u dołu dokumentu będą widoczne odrębnie, w kolejności składania daty i czas złożenie każdego z podpisów (duża litera T separuje datę od godziny złożenia podpisu, poszczególne czasy złożenia podpisu odseparowane są dużą literą Z wskazującą, że do pokazywanego czasu należy dodać 1 godzinę dla naszej strefy czasowej):




*Dokument elektroniczny podpisany podpisami potwierdzonymi profilem zaufanym ePUAP przez 3 osoby.*

Drugi sposób (zdecydowanie gorszy, bardziej kłopotliwy i niepotrzebnie zwiększający objętość przesyłki) polega na odrębnym podpisywaniu każdego z przesyłanych plików W takim przypadku występują dwa zagrożenia – można – przy dużej liczbie plików przekroczyć objętość dopuszczalną przesyłki w ePUAP (5 MB dla całości, 3,5 MB dla pliku pojedynczego) lub nie dołączyć któregoś z plików stanowiących podpis lub plik podpisywany, jeśli stosowane tzw podpis zewnętrzny Niepodpisanie pisma przewodniego może skutkować odrzuceniem przesyłki przez ESP skonfigurowaną na przyjmowania wyłącznie przesyłek podpisanych (chodzi p podpis kontenera głównego).

Co do zasady, dokument – by mógł w przyszłości stanowić dowód, musi być zabezpieczony przez niekontrolowanymi zmianami, a więc musi być elektronicznie podpisany

#### 4.1.1.2. Przesyłki niepodpisane

Przesyłki niepodpisane stanowią odpowiedniki listów zwykłych, czy wręcz anonimów – brak podpisu elektronicznego (podpis potwierdzony profilem zaufanym lub certyfikatem kwalifikowanym) powoduje, że usługodawca nie ma żadnej pewności co do tożsamości przesyłającego pismo, więc może wezwać nadawcę – jeśli przesłane dane to umożliwią do uzupełnienia braków formalnych; jeśli interesant stawi się w urzędzie, należy wydrukować przesłane pismo i uzupełnić je o datę złożenia i podpis własnoręczny

### 4.1.2. Centralne Repozytorium Wzorów Dokumentów Elektronicznych

**Centralne repozytorium wzorów dokumentów elektronicznych (CRD, CR)** - centralne repozytorium wzorów dokumentów elektronicznych prowadzone przez ministra właściwego do spraw informatyzacji w ramach ePUAP, w którym to repozytorium umieszcza się, przechowuje i udostępnia wzory dokumentów, uwzględniające niezbędne elementy struktury dokumentów elektronicznych określone w przepisach wydanych na podstawie art. 5 ust. 2a ustawy z dnia 14 lipca 1983 r. o narodowym zasobie archiwalnym i archiwach (Dz. U. z 2011 r. Nr 123, poz. 698 i Nr 171, poz. 1016 oraz z 2014 r. poz. 822). (Dz.U.2014.1114 j.t.)


Koncepcja centralnego repozytorium wzorów dokumentów (ale także repozytoriów regionalnych i lokalnych) wzięła się z potrzeby zapewnienie jednolitości tworzonych dokumentów obecnie i w przyszłości. Wzory dokumentów zamieszczane są w CR znajdującym się pod adresem http://

epuap.gov pl/wps/portal/E2_CRD; każdy wzór ma swój unikatowy numer składający się z daty w formacie rrrr/mm/dd, ukośnika i kolejnego numeru wzoru. Wzory dokumentów umieszczone w CRD pozostają tam na zawsze. Jeśli ulegają dezaktualizacji, wtedy w kolumnie „czy aktualny" znajduje się litera N

Rys. 16 przedstawia wzór o numerze 2015/04/08/2156 utworzony przez Zakład Ubezpieczeń Społecznych, dotyczący pisma do komornika sądowego o udostępnieniu danych ze zbioru ZUS:

**Dane wzoru**

| ID wzoru | Nr wzoru | Data publikacji | Czy aktualny |
|---|---|---|---|
| 2156 | 2015/04/08/2156 | 2015-04-08 | T |

| Nazwa instytucji |
|---|
| ZAKŁAD UBEZPIECZEŃ SPOŁECZNYCH |

| Dotyczy |
|---|
| Pismo do komornika sądowego o udostępnieniu danych ze zbioru ZUS |

**Pliki wzoru**

| Pliki wzoru: | |
|---|---|
| XML: | http://crd.gov.pl/wzor/2015/04/08/2156/wyroznik.xml |
| XSD: | http://crd.gov.pl/wzor/2015/04/08/2156/schemat.xsd |
| XSL: | http://crd.gov.pl/wzor/2015/04/08/2156/styl.xsl |

| Załączone materiały: | |
|---|---|
| przyklad.xml | Wizualizuj |

*Wzór o numerze 2015/04/08/2156 zamieszczony w centralnym repozytorium*

Niektóre wzory są wizualizowane (zamieszczanie wizualizacji przez podmiot zgłaszający nowy wzór nie jest obowiązkowe) – poniżej fragment wizualizacji dokumentu przykład.xml.

Zakład Ubezpieczeń Społecznych
Inspektorat w Gdyni
ul. Władysława IV 24, 81-364 Gdynia

Gdynia, dnia 18 2012 r.

100300/0002020/2012
Syg. sprawy: 100300/411/12333/2012
Syg. akt: KM 12300/01

**KS PRZY SĄDZIE REJONOWYM DLA WARSZAWY**
**GRZEGORZ KOWALSKI**
**KOŚCIUSZKI 1/2**
**12-345 WARSZAWA**

W odpowiedzi na wniosek o udostępnienie danych ze zbioru danych osobowych z dnia 13.08.2012 r. Zakład Ubezpieczeń Społecznych Inspektorat w Gdyni informuje, że:

| | |
|---|---|
| nazwisko i imię: | NOWAK WOJCIECH |
| adres zameldowania: | 34-678 SOPOT 12 |
| zgłoszony przez: | BANACH JOLANTA |
| podlega ubezpieczeniu z tytułu: | 0111 - pracownik podlegający ubezpieczeniom społecznym i z mocy przepisów szczególnych niepodlegający ubezpieczeniu zdrowotnemu od 13.08.1967 r. |

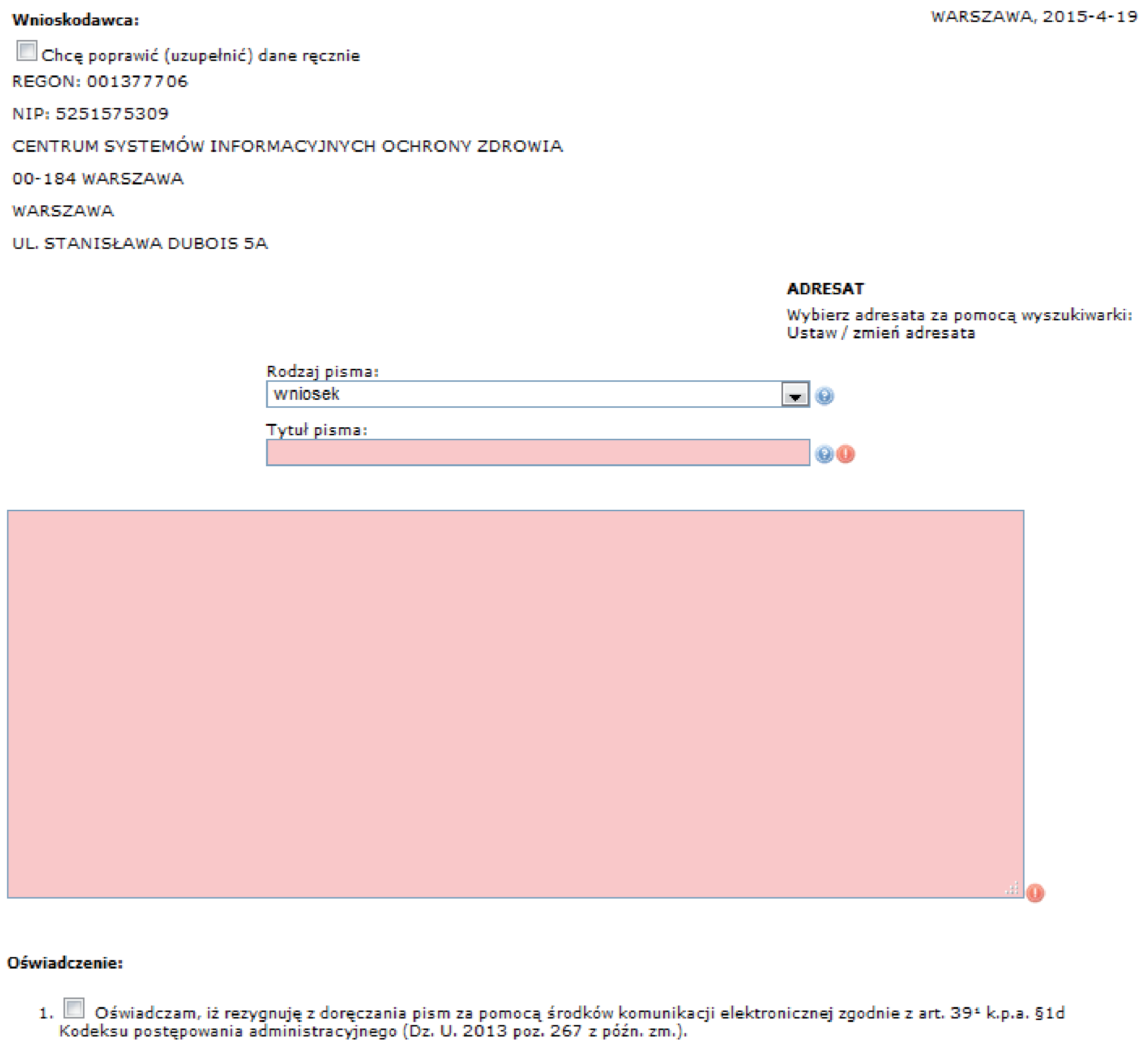
*Wizualizacja dokumentu wygenerowanego na podstawie wzoru nr 2015/04/08/2156*

Bezpośrednio po wejściu do centralnego repozytorium widoczne są ostatnio wprowadzone wzory wyświetlane w porządku antychronologicznym. Dowolny wzór odszukać można podając datę lub dowolny ciąg znaków występujący w jednym z pól opisu wzoru. Zwizualizować wzór można także (tam, gdzie wizualizacji nie udostępniono) otwierając stanowiący element wzoru plik z rozszerzeniem xsl za pomocą przeglądarki internetowej.

### 4.1.3. Formularze elektroniczne

> **Formularz elektroniczny** - graficzny interfejs użytkownika wystawiany przez oprogramowanie służący do przygotowania i wygenerowania dokumentu elektronicznego zgodnego z odpowiadającym mu wzorem dokumentu elektronicznego; (Dz.U.2014.1114 j.t.)

Formularze ekranowe dostępne na ePUAP przy wprowadzaniu danych niezbędnych w piśmie kierowanym do podmiotu różnią się nieco od dokumentu ostatecznie utworzonego. Budowane są w taki sposób, by wypełniający je nie pominął żadnego pola. Formularze posiadają pola, które należy wypełnić danymi zgodnie z pokazującymi się sugestiami czy uwagami. Mogą być wyposażone w kalendarze i listy rozwijane. Przykładem formularza ekranowego jest formularz pisma ogólnego do podmiotu publicznego:



**Wnioskodawca:** WARSZAWA, 2015-4-19

Chcę poprawić (uzupełnić) dane ręcznie

REGON: 001377706

NIP: 5251575309

CENTRUM SYSTEMÓW INFORMACYJNYCH OCHRONY ZDROWIA

00-184 WARSZAWA

WARSZAWA

UL. STANISŁAWA DUBOIS 5A

**ADRESAT**

Wybierz adresata za pomocą wyszukiwarki:
Ustaw / zmień adresata

Rodzaj pisma:
wniosek

Tytuł pisma:

**Oświadczenie:**

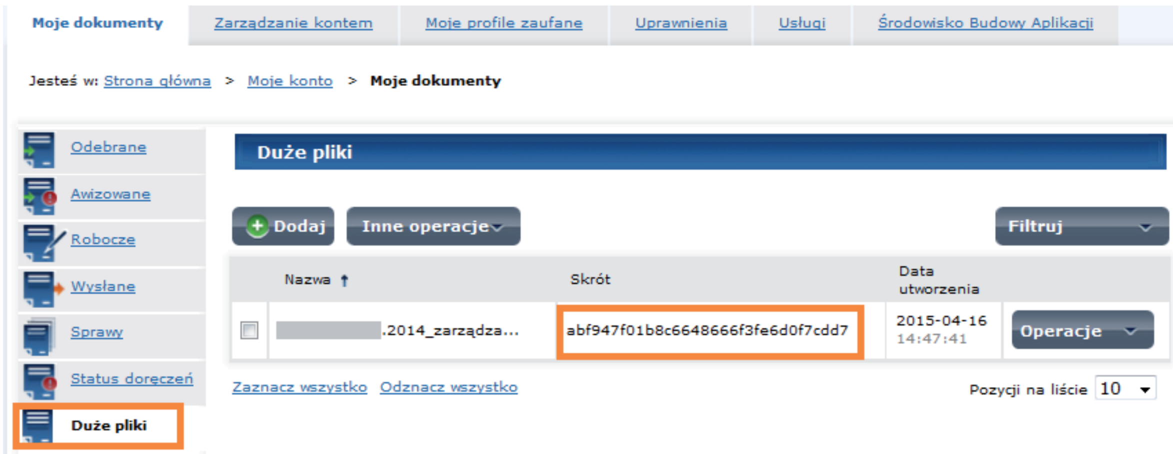
1. Oświadczam, iż rezygnuję z doręczania pism za pomocą środków komunikacji elektronicznej zgodnie z art. 39¹ k.p.a. §1d Kodeksu postępowania administracyjnego (Dz. U. 2013 poz. 267 z późn. zm.).

*Widok formularza ekranowego służącego do sporządzenia pisma ogólnego do podmiotu publicznego*

Po wypełnieniu formularza ekranowego i zapisaniu go dane pojawiają się w dokumencie w jego wersji przeznaczonej do wysyłki. System pozwala zapoznać się z treścią i – w razie dostrzeżenia błędu pozwala wrócić do trybu edycji.

### 4.1.4. Mechanizm przesyłania dużych plików

Mechanizm przesyłania dużych plików jest funkcjonalnością ePUAP, przyznawaną podmiotom publicznym przez ministra właściwego ds. informatyzacji. Z uwagi na ograniczenie wielkości przesyłek na ePUAP (do 5 MB wielkość całej przesyłki, wielkość załącznika do 3,5 MB), istnieje możliwość przesyłania przesyłek o wielkości do 200MB (aktualnie). Tworzenie przesyłki polega na spakowaniu wszystkich przesyłanych dokumentów do jednego archiwum w formacie zip i utworzeniu pisma przewodniego, do którego owo archiwum będzie załącznikiem. System, w czasie przesyłania archiwum do bufora generuje skrót MD5 (niezależnie od wielkości przesyłki skrót ten zawsze składa się z 32 znaków w kodzie heksadecymalnym) dołączając jawnie informację o załączniku i jego skrócie do pisma przewodniego. Pismo przewodnie należy podpisać podpisem potwierdzonym profilem zaufanym lub podpisem kwalifikowanym. Podpisanie skrótu dokumentu jest równoważne z podpisaniem dokumentu.

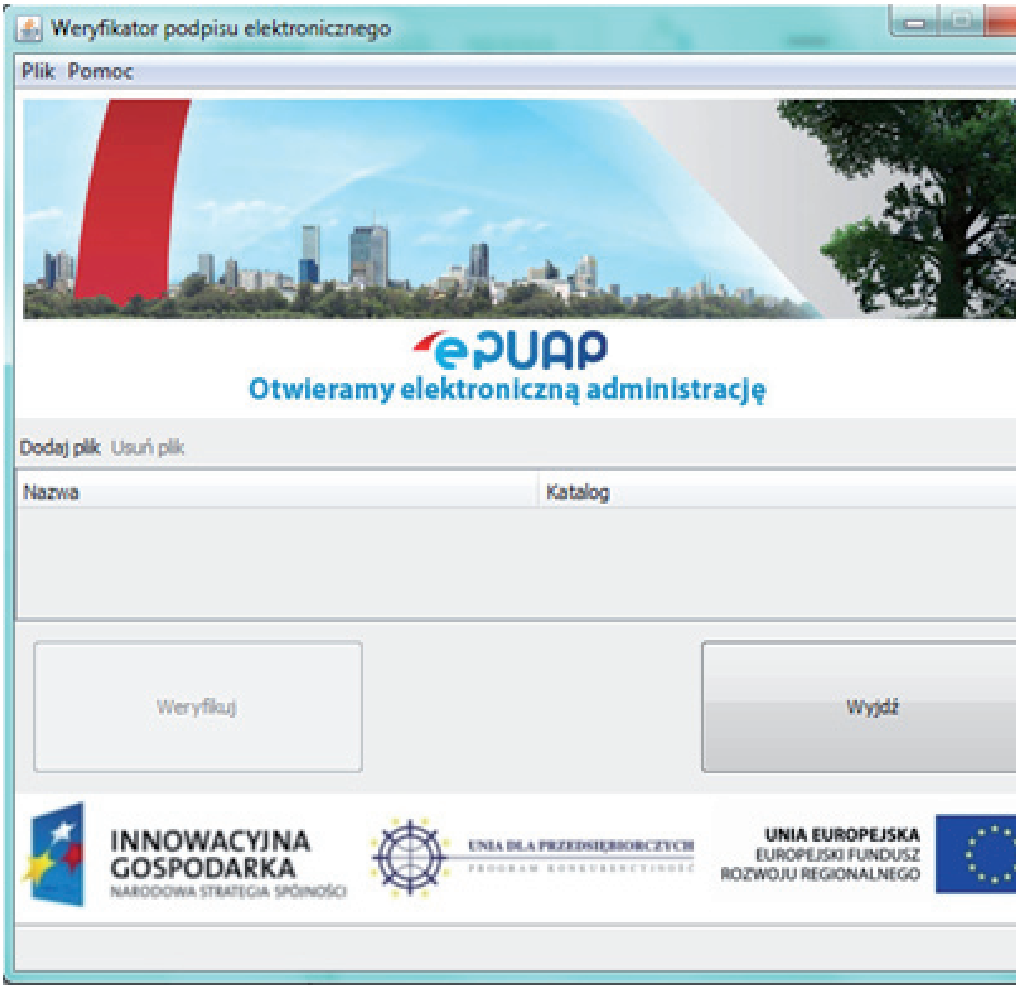


*Przesyłanie dużego pliku (archiwum .zip o objętości kilkudziesięciu megabajtów)*

Należy podkreślić, że podpis elektroniczny – NIEZALEŻNIE od tego, czy jest użyty w odniesieniu do pisma zawierającego wyrażenie woli czy nie (wynikać to musi z rodzaju pisma oraz jawnie wpisanego w jego treści imienia, nazwiska i stanowiska osoby uprawnionej) ZAWSZE zapewnia integralność przesyłki.

### 4.1.5. Weryfikator podpisu elektronicznego

Weryfikator podpisu elektronicznego dostępny jest na platformie ePUAP w części przeznaczonej dla integratorów (Strona główna > Pomoc > Integratorzy > Przykładowe aplikacje). Można go lokalnie zapisać na własnym dysku i używać do weryfikacji podpisów elektronicznych, którymi opatrzone są pliki XML tworzone na ePUAP (po zapisaniu pliku na dysku lokalnym).




*Weryfikator podpisu elektronicznego na ePUAP*

Generalnie wszystkie weryfikatory podpisów elektronicznych umożliwiają weryfikację podpisów, którymi opatrzone są pliki – bez względu na to, czy są to podpisy otoczone, otaczające czy zewnętrzne. Stosuje się też wewnętrzne weryfikatory w elektronicznych systemach zarządzania dokumentami – korzystanie z nich jest znacznie ułatwione; system sygnalizuje, że dany plik jest podpisany elektronicznie – i po kliknięciu klawisza „weryfikuj podpis" lub klawisza o podobnym znaczeniu ukazuje się certyfikat oraz dodatkowe informacje dotyczące podpisu. Z tego typu weryfikatorów korzystają wszyscy użytkownicy EZD – niezależnie od ich roli w systemie. Jednak usługobiorcy przysyłają niekiedy pliki pocztą elektroniczną – i wtedy trzeba móc zweryfikować owe pliki, stanowiące załączniki do poczty

Opisany wyżej weryfikator podpisów udostępniony na ePUAP – po ściągnięciu na dysk lokalny można uruchomić (dwukrotne kliknięcie pliku), a następnie należy wczytać plik do weryfikacji (Dodaj plik) i kliknąć klawisz „Weryfikuj" W wyniku weryfikacji pokaże się stosowny komunikat:

## Wyniki weryfikacji

Dokument podpisany elektronicznie. Wszystkie podpisy są poprawne.

| Właściciel podpisu: | Status podpisu: |
|---|---|
| **Halina** [redacted] | **Podpis jest poprawny** ( pokaż szczegóły |

### Szczegóły

**Certyfikat:**

| | |
|---|---|
| Numer seryjny: | 9214350759863715675 |
| Wystawiony przez: | Sigillum PCCE - kwalifikowany CA1 |
| Właściciel: | Halina [redacted] |
| Właściciel (nazwa powszechna): | Halina [redacted] |
| PESEL właściciela certyfikatu: | [redacted] |
| Status: | Ważny |
| Certyfikat kwalifikowany: | Tak |
| Szczegóły: | |

kwalifikowany, logowanie, Generacja odpowiedzi OCSP na podstawie CRL

**Podpis:**

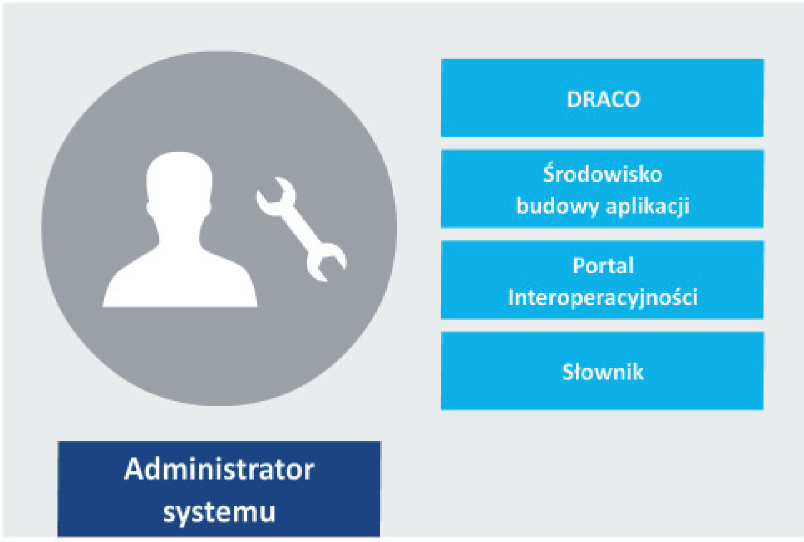
| | |
|---|---|
| Numer seryjny: | EZD_PUW_xCH_ID-d4c9e213-48c9-412d-8188-c0b9d1ce0778 |
| Data podpisania: | Thu Feb 26 11:18:35 CET 2015 |
| Typ zobowiązania: | http://uri.etsi.org/01903/v1.2.2#ProofOfApproval |
| Oznaczenie czasem: | Thu Feb 26 11:23:51 CET 2015 Znacznik prawidłowy |
| Postać archiwalna: | Thu Feb 26 12:24:38 CET 2015 Znacznik prawidłowy |
| Status: | Zgodny z dokumentem |
| Typ podpisu: | XAdES |

Zamknij

*Wynik weryfikacji podpisu.*

### 4.1.6. Inne komponenty

Elektroniczna Platforma Usług Administracji Publicznej zawiera jeszcze inne elementy: służącą celom zarządzania użytkownikami aplikację Draco, Środowisko Budowy Aplikacji, Portal Interoperacyjności, Słownik. Są dedykowane dla węższych grup użytkowników – administratorów systemów.




## 4.2. Regionalna platforma elektronicznych usług publicznych

Regionalne platformy elektronicznych usług publicznych tworzone są dla obszaru regionu (województwa). Przykładami takich platform mogą być Wrota Podlasia, Wrota Małopolski, SEKAP i inne, utrzymywane przez marszałków dla mieszkańców województw Cechą tych rozwiązań są ujednolicone wzory dokumentów w repozytoriach regionalnych oraz niekwalifikowane certyfikaty podpisu elektronicznego, które jednak, z uwagi na stosowne umowy pomiędzy odbiorcami usług certyfikacyjnych a marszałkiem mogą być stosowane

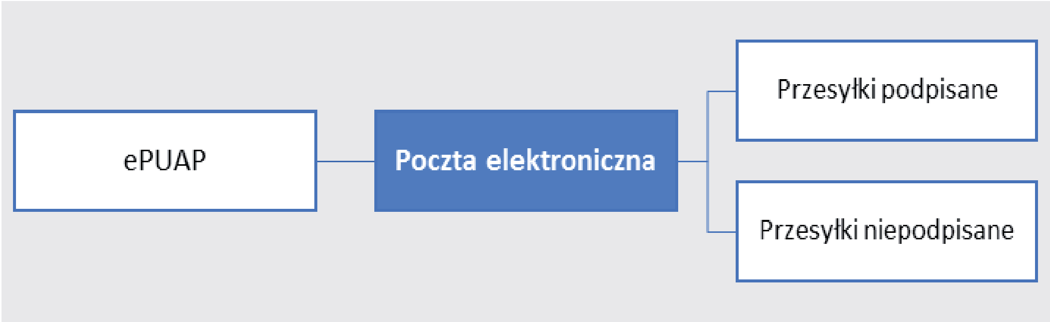
## 4.3. Elektroniczna Skrzynka Podawcza poza ePUAP

Jest to rozwiązanie służące do tego samego celu, co Elektroniczna Skrzynka Podawcza na platformie ePUAP, jednak historycznie zostało wprowadzone wcześniej.


Jedyną funkcjonalną różnicą jest to, że w ESP będących odrębnym rozwiązaniem stosowane były konkretne formularze – i nie było możliwe przesyłanie pism ogólnych, co stanowiło istotną barierę komunikacyjną. Drugim ograniczeniem była konieczność użycia podpisu kwalifikowanego. Należy jednak podkreślić, że samo rozwiązanie, jako takie, może być stosowane przez każdy podmiot (niezależnie od tego, czy jest to podmiot publiczny, czy nie, gdyż celem jego stosowania jest skuteczne i pewne, tj. z uzyskaniem potwierdzenia tego faktu przedłożenie dokumentu). Wykorzystywanie jednej z możliwych do stosowania skrzynek podawczych wynikać powinno z racjonalnych przesłanek (np. pewności działania, niezawodności, kosztów utrzymania itd.)

## 4.4. Poczta elektroniczna

Trzecim powszechnie używanym środkiem komunikacji jest poczta elektroniczna. Jest prosta w użyciu i stanowi analogię zwykłej poczty papierowej, w której nie potwierdza się faktu otrzymania przesyłek.




*Poczta elektroniczna*

Jej wadą jest to, że nie zapewnia dowodu dostarczenia przesyłki, a także nie zapewnia uzyskania **dokumentów strukturalnych** (w **formacie xml**) w sposób naturalny Oczywiście, można w innych aplikacjach dokumenty takie wytworzyć i pocztą elektroniczną przesłać, jednak odbiorca może mieć różnego rodzaju trudności z ich odczytaniem. Nie daje także odbiorcy żadnej pewności co do **tożsamości** nadawcy Z uwagi na konieczność zachowania dowodów co do przebiegu załatwiania sprawy, dotrzymywania terminów, poczty elektronicznej nie można rekomendować mimo iż jest ona jak najbardziej legalnym i użytecznym środkiem komunikacji. Należy też pamiętać, że w przypadku stosowania poczty elektronicznej nie można mieć 100% pewności dotarcia przesyłki do adresata, gdyż przesyłki przechodząc przez różne serwery pocztowe narażone są też na różnego rodzaju zagrożenia. Dokumenty przesyłane jako załączniki pocztą elektroniczną muszą być podpisane podpisem kwalifikowanym, gdyż w innym przypadku nie są dokumentami wiarygodnymi. Jeśli zostaną przyjęte w urzędzie, usługobiorca musi być wezwany do uzupełnienia braków formalnych w postaci własnoręcznego podpisu, chyba że odbiorca uzyska tę pewność w inny sposób.

Jak wspomniano, pracownik urzędu musi mieć pewność co do tożsamości osoby przesyłającej dokument (nie chodzi tu o osobę fizycznie dokonującej wysyłki, ale osoby, która ów dokument podpisała). Ponieważ nazwy kont e-mailowych często nie odzwierciedlają imienia i nazwiska nadawcy, a ten z kolei niekiedy w treści e-maila podpisuje się samym imieniem, lub inicjałami, a nawet wysyła e-mail anonimowo, więc przesyłka taka (załącznik do e-maila) nie spełnia podstawowych warunków uznania jej za dokument. W sytuacjach wcześniej uzgodnionych, gdy usługobiorca np. w wiarygodny sposób poda swój adres elektroniczny, wymiana korespondencji tą drogą jest oczywiście dopuszczalna z zastrzeżeniem, że odbiór przesyłek będzie potwierdzany Należy w końcu pamiętać, że niepodpisany elektronicznie plik mimo iż legalnie, zgodnie z prawem, jest „dokumentem", jest słaby dowodowo – i jest to wystarczający powód, by przyglądać mu się ze szczególną ostrożnością i zadbać o jego uwierzytelnienie w jakikolwiek inny sposób.

### 4.4.1. Przesyłki podpisane

Elektronicznie podpisane dokumenty można przesyłać pocztą elektroniczną – jako załączniki, jednak należy się liczyć z brakiem potwierdzenia odbioru. Niektóre urzędy uprzedzają interesantów, że fakt przesłania przesyłki tą drogą nie będzie potwierdzany Potwierdzanie odbioru poczty wymaga dodatkowych czynności. Zdarza się też przesyłanie przesyłek pod niewłaściwe adresy lub do pracowników przebywających na dłuższym urlopie, którzy to pracownicy nie ustawili autoodpowiedzi informującej o tym fakcie. Nic jednak nie stoi na przeszkodzie (poza wspomnianą niepewnością dostarczenia przesyłki) by w pewnych uzgodnionych wcześniej sytuacjach wykorzystywać pocztę do przesyłania elektronicznie podpisanych dokumentów – i uzyskiwać potwierdzenie otrzymania przesyłki. Należy to jednak wcześniej uzgodnić.

### 4.4.2. Przesyłki niepodpisane

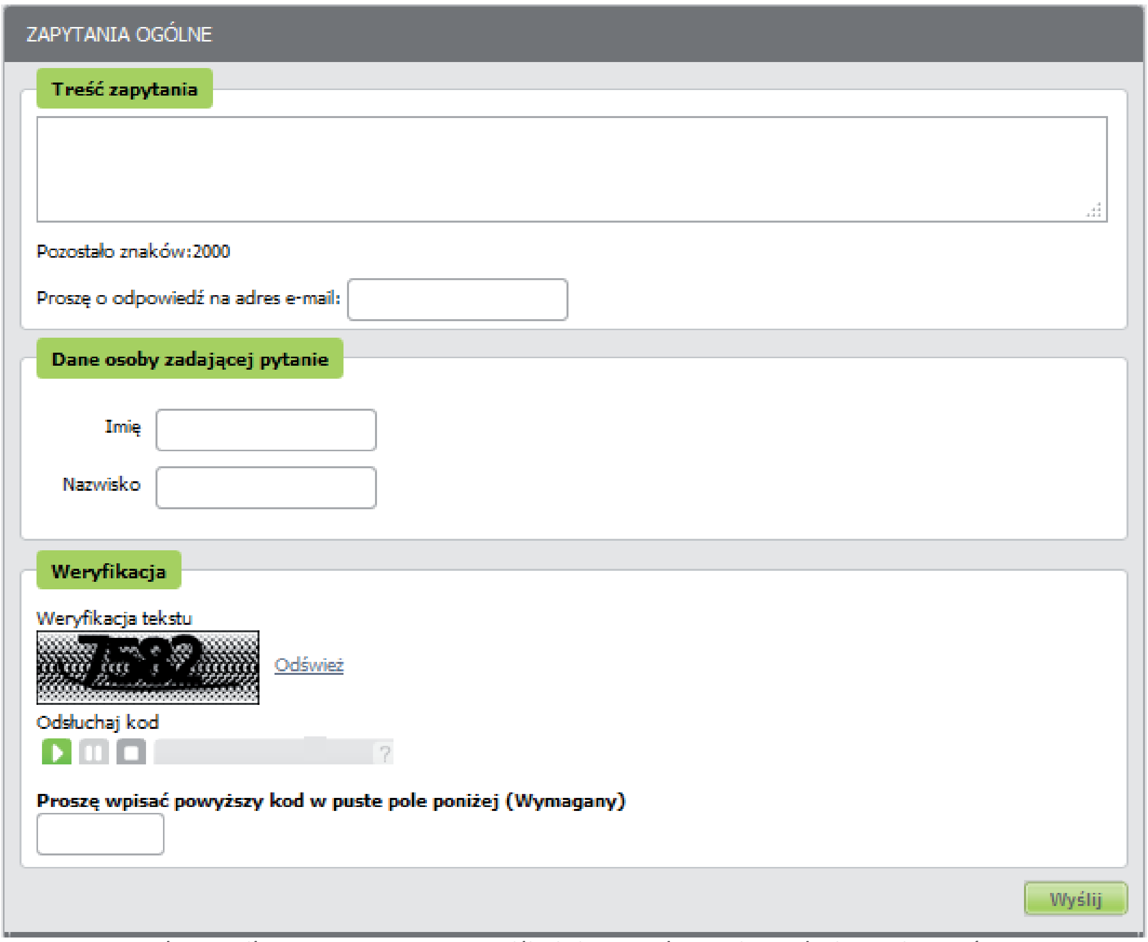
Do przesyłania niepodpisanych elektronicznie plików poczta elektroniczna stosowana jest powszechnie. Jednak należy mieć na uwadze trudność w zapewnieniu bezpieczeństwa przechowywania tego typu przesyłek, a także fakt, że niepodpisane dokumenty elektroniczne są tak samo obciążone brakiem formalnym w postaci braku podpisu jak niepodpisane dokumenty papierowe. Ich moc dowodowa jest b. słaba.

## 4.5. Systemy dedykowane tworzone przez usługodawców

Czwartym środkiem komunikacji elektronicznej jest dedykowany system, tworzony przez usługodawcę, służący do komunikowania się z nim osób fizycznych, interesantów bez wykorzystywania popularnych klientów poczty elektronicznej (MS Outlook, Mozilla Thunderbird, Gmail itp,). System taki zazwyczaj jest bardzo prosty w użyciu, pozwala na zadawanie pytań i sprowadza się również do założenia indywidualnego konta w przedmiotowym systemie. W zależności od sposobu realizacji procedury identyfikacji może być zupełnie wystarczającym środkiem komunikacji. Nie zawsze system taki pozwala dołączać załączniki. Należy podkreślić, że co do zasady powinno się stosować środki komunikacji elektronicznej adekwatne do konkretnej sytuacji, do stopnia zagrożenia zafałszowaniem (zniekształceniem informacji), a jedynie w sytuacjach, gdy konieczne jest tworzenie i zabezpieczanie dokumentów należy stosować mechanizmy bardziej rozbudowane.

**PUE ZUS**

Z reguły dedykowany system komunikacyjny jest częścią większego systemu – przykładem może być system umożliwiający komunikowanie się z usługodawcą w sposób prosty, bez przeprowadzania procesu weryfikacji danych osobowych – jak np. w PUE ZUS w wersji dla osób przedstawiających się jedynie imieniem i nazwiskiem oraz podającym adres e-mail w celu uzyskania odpowiedzi; w systemie tym liczbę potrzebnych danych ograniczono do absolutnie niezbędnego minimum.




*Wewnętrzny komunikator w PUE ZUS umożliwiający zadawanie podmiotowi pytań*

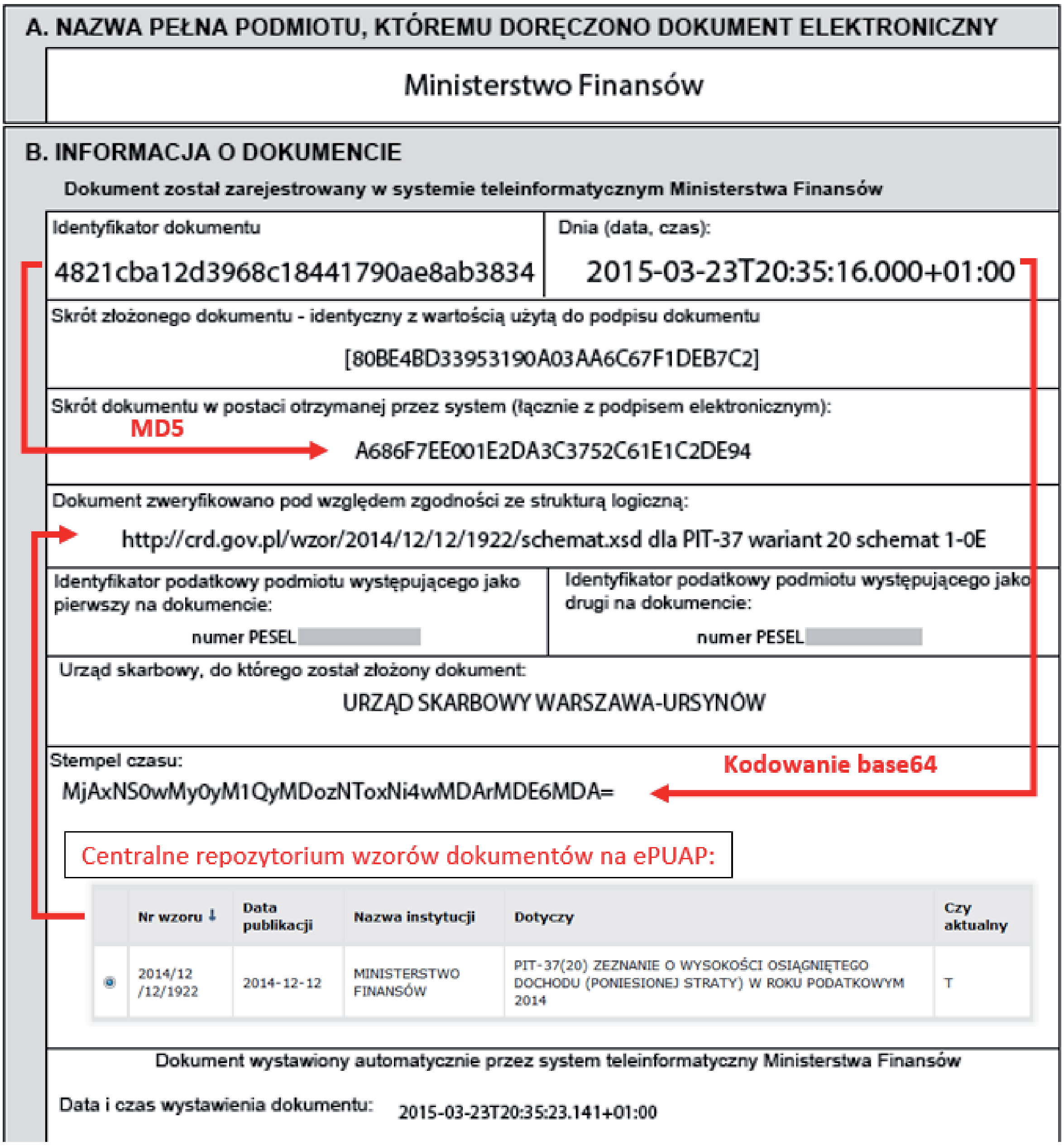
W wersji dla osoby korzystającej już z konta na PUE ZUS, która to osoba po założeniu konta i procesie weryfikacji nie jest już anonimowa i posiada zupełnie inny zakres możliwości pozyskiwania informacji i danych związanych z działalnością ZUS, system komunikacyjny wygląda inaczej:


*Panel komunikatora wewnątrz PUE ZUS – widok dla użytkownika po zalogowaniu się*

Komunikacja wewnątrz systemu dedykowanego jest bezpieczna dla obu komunikujących się ze sobą stron. Jedyną jej wadą jest to, że wymaga ona każdorazowo oswojenia się z danym systemem komunikacyjnym, rozkładem pól informacyjnych, funkcjonowaniem różnych narzędzi wewnętrznych i ich możliwościami. Jest to kłopotliwe dla osób nieposiadających sprawności w opanowywaniu umiejętności posługiwania się interfejsami wielu systemów informatycznych. Wydaje się jednak, że wada to do najistotniejszych nie należy; liczba osób nieumiejących korzystać z dedykowanych systemów komunikacyjnych będzie systematycznie w stosunku do całej populacji malała.

**e-deklaracje**

Systemów dedykowanych do realizacji pewnych zadań jest w chwili obecnej wiele. Ich wspólną cechą jest „resortowość" Każdy z nich tworzony jest w celu realizacji jednego, konkretnego zadania. Przykładem takiego systemu mogą być e-Deklaracje, stanowiące część większego systemu e-Podatki. Aplikacja E-Deklaracje – mimo iż udostępniona jest poza platformą ePUAP, korzysta z wzorów dokumentów opublikowanych w centralnym repozytorium na ePUAP i wystawia UPO – również poza ePUAP Z e-Deklaracji może skorzystać każdy – również osoby nieposiadające profilu zaufanego czy nawet konta na ePUAP Podpis elektroniczny także nie jest potrzebny – zamiast niego wystarczają znane usługobiorcy (podatnikowi) dane autoryzujące, które należy podać podczas wypełniania formularza e-Deklaracji. Poniżej pokazano UPO wygenerowane po przesłaniu e-Deklaracji.



**A. NAZWA PEŁNA PODMIOTU, KTÓREMU DORĘCZONO DOKUMENT ELEKTRONICZNY**

Ministerstwo Finansów

**B. INFORMACJA O DOKUMENCIE**

**Dokument został zarejestrowany w systemie teleinformatycznym Ministerstwa Finansów**

| Identyfikator dokumentu | Dnia (data, czas): |
|---|---|
| 4821cba12d3968c18441790ae8ab3834 | 2015-03-23T20:35:16.000+01:00 |

Skrót złożonego dokumentu - identyczny z wartością użytą do podpisu dokumentu

[80BE4BD33953190A03AA6C67F1DEB7C2]

Skrót dokumentu w postaci otrzymanej przez system (łącznie z podpisem elektronicznym):

MD5

A686F7EE001E2DA3C3752C61E1C2DE94

Dokument zweryfikowano pod względem zgodności ze strukturą logiczną:

http://crd.gov.pl/wzor/2014/12/12/1922/schemat.xsd dla PIT-37 wariant 20 schemat 1-0E

| Identyfikator podatkowy podmiotu występującego jako pierwszy na dokumencie: | Identyfikator podatkowy podmiotu występującego jako drugi na dokumencie: |
|---|---|
| numer PESEL | numer PESEL |

Urząd skarbowy, do którego został złożony dokument:

URZĄD SKARBOWY WARSZAWA-URSYNÓW

Stempel czasu:

MjAxNS0wMy0yM1QyMDozNToxNi4wMDArMDE6MDA=

Kodowanie base64

Centralne repozytorium wzorów dokumentów na ePUAP:

| | Nr wzoru | Data publikacji | Nazwa instytucji | Dotyczy | Czy aktualny |
|---|---|---|---|---|---|
| ◉ | 2014/12 /12/1922 | 2014-12-12 | MINISTERSTWO FINANSÓW | PIT-37(20) ZEZNANIE O WYSOKOŚCI OSIĄGNIĘTEGO DOCHODU (PONIESIONEJ STRATY) W ROKU PODATKOWYM 2014 | T |

Dokument wystawiony automatycznie przez system teleinformatyczny Ministerstwa Finansów

Data i czas wystawienia dokumentu: 2015-03-23T20:35:23.141+01:00

*UPO wystawione przez Ministerstwo Finansów po przesłaniu e-Deklaracji dotyczącej dwóch osób – podatnika i współmałżonka.*

Na powyższym rysunku, przedstawiającym UPO otrzymane po przesłaniu e-deklaracji do Ministerstwa Finansów, widoczne są wygenerowane skróty dokumentów (zastosowano algorytm **MD5** dający zawsze skrót o długości 32 znaków w kodzie szesnastkowym) oraz stempel czasu (będący zakodowanym algorytmem **base64** czasem złożenia e-deklaracji). Opanowanie posługiwania się generatorami i dekoderami MD5, **SHA-1** i base64 jest przydatną umiejętnością zwiększającą pewność posługiwania się dokumentami elektronicznymi, szczególnie przy przekazywaniu plików archiwów, plików w **formacie** .zip o objętościach liczonych w setkach MB.

## 4.6. SMS

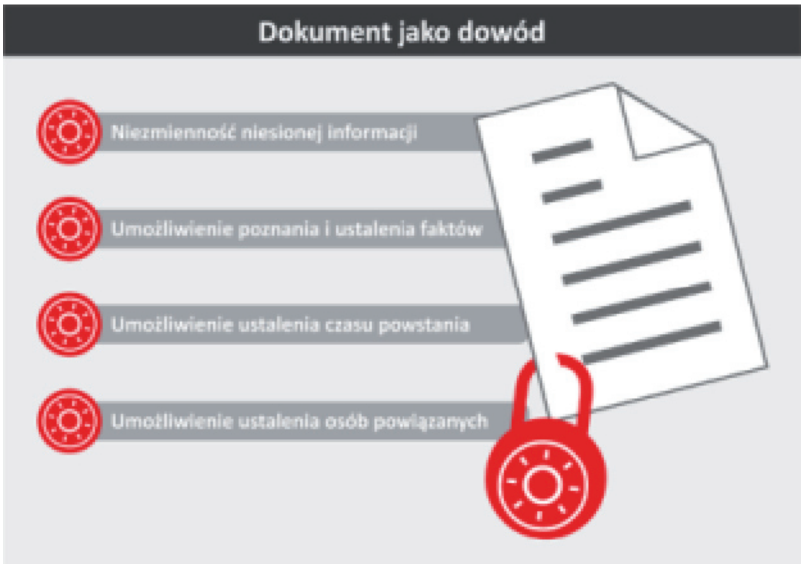
**SMS** (ang. Short Message Service) – usługa przesyłania krótkich wiadomości tekstowych (esemesów) w cyfrowych sieciach telefonii komórkowej.

SMS jest coraz powszechniej wykorzystywany w administracji do przesyłania krótkich wiadomości tekstowych. Stosowany jest po uzgodnieniu z usługobiorcą zarówno do powiadamiania np. o fakcie załatwienia sprawy, jak i do innych czynności, np. wynikających z systemowego rozwiązania realizacji procesu składania podpisu elektronicznego, wysyłania przez niektóre systemy jednorazowych kodów służących do autoryzacji wysyłanego pisma (taki system stosowany jest także w profilu zaufanym ePUAP), albo do weryfikacji poprawności podanego numeru telefonu przy składaniu wniosku o potwierdzenie profilu.

# 5. Dokument

> **Dokument** - zapisana na nośniku informacja, spełniająca pewne minimalne wymagania dotyczące zarówno struktury i wzajemnych relacji między elementami tej struktury, jak i sposobu zapisu, umożliwiającego odtworzenie i przekazanie odczytanej informacji.

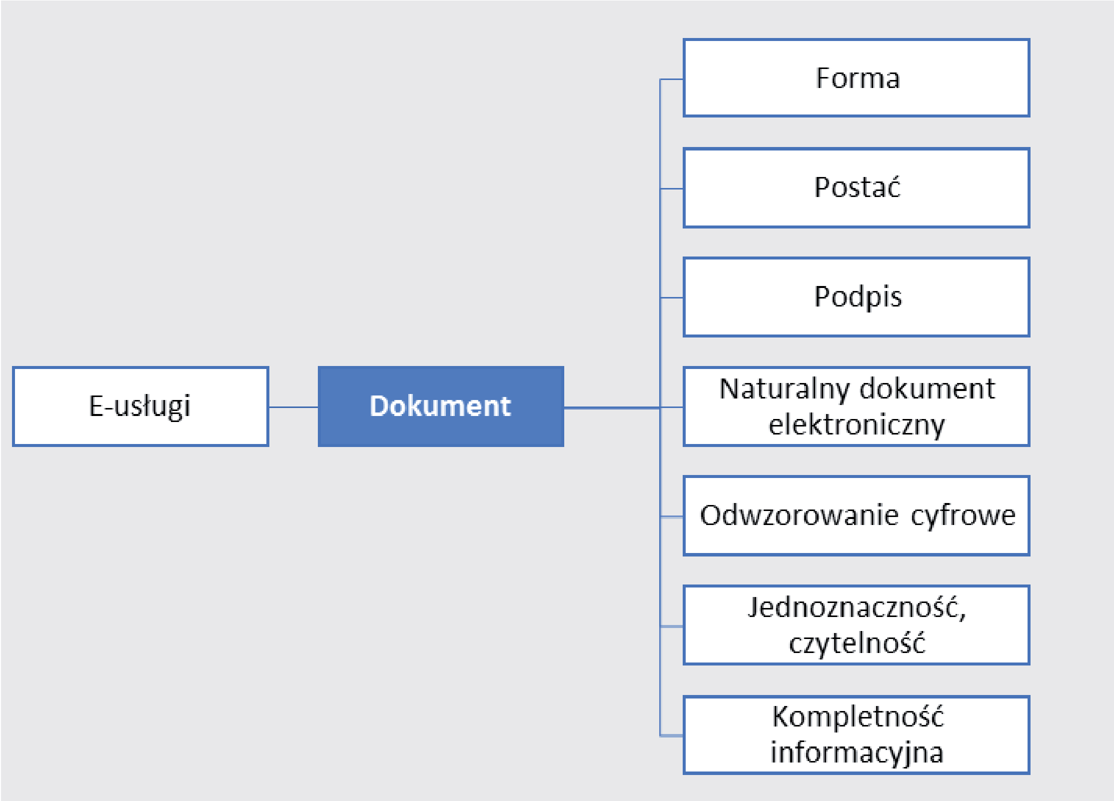
**Dokument** jest ostatnim z czterech elementów e-usługi, najbardziej rozbudowanym znaczeniowo i najtrudniejszym do określenia z uwagi na wielość kontekstów, w jakich może się pojawiać i w jakich może być użyty




Z uwagi na fakt, że z pojęciem **dokumentu** związanych jest najwięcej niejasności i trudności interpretacyjnych, opisany on będzie poprzez pokaz konkretnych przypadków, zarówno rzeczywistych jak i fikcyjnych. Omawiane przypadki dotyczyły będą zarówno samych dokumentów, zarówno papierowych jak i elektronicznych, a także czynności dokonywanych z użyciem dokumentów Punktem wyjścia będzie najogólniejsze określenie dokumentu rozumianego jako pewien byt, z którego można wywodzić skutki prawne.

Dla pewności obrotu prawnego dokument powinien mieć atrybuty **dowodu**, tj. powinien posiadać cechy niezmienności niesionej **informacji** w okresie, w którym powinien istnieć w celu umożliwienia poznania i ustalania faktów z którymi jest związany, a także ustalenia pewnych danych, takich jak **data** i **czas** jego powstania oraz możliwości jednoznacznego ustalenia osób związanych z tym dokumentem, w szczególności osób go **podpisujących**.

W celu lepszego wyeksponowania przypadków pokazywane one będą w odniesieniu do schematycznych rysunków pokazujących omawiany element drzewa cech dokumentu i działań, jakie w odniesieniu do niego mogą być podejmowane.




*Dokument*

Rysunek przedstawia istotne cechy dokumentu, które muszą być w każdym przypadku indywidualnie analizowane. Od wyników tej analizy zależała będzie kwalifikacja dokumentu, jego wartość informacyjna oraz moc dowodowa.

**Dokument i jego cechy**

Pierwszą z cech dokumentu jest jego **forma**.

Forma jest sposobem wyrażenia treści dokumentu, informacji, które on niesie. Dokument może mieć **formę tekstową** (np. decyzja administracyjna), przy czym tekst może być dla lepszego wyrażenia pewnych zależności przedstawiony jako tabela lub tekst zwarty, podzielony na akapity Istotą tej formy jest wyrażenie przekazu informacji za pomocą słów i cyfr – bez względu na nośnik. Zatem dokumentem tekstowym będzie zarówno przywołana wyżej decyzja administracyjna mająca postać elektroniczną (plik w formacie doc, docx, rtf, odt, pdf) jak i wydruk treści tej decyzji na papierze. Zwraca się jednak uwagę, że jest to tylko forma przekazu informacji, utrwalona na nośniku elektronicznym lub papierowym.


Oprócz formy tekstowej, istnieją jeszcze inne sposoby przekazu informacji – zdjęcia, rysunki, wykresy, mapy, które nazywamy **formą graficzną**, **formę mieszaną** – będącą połączeniem wcześniej wspomnianych i w końcu formy dźwiękowej (audialnej) i audiowizualnej, które obecnie utrwalane są w postaci elektronicznej.

Owa postać, to cecha dokumentu, którą określa się rodzaj nośnika, na którym treść w jakiejś formie jest utrwalona. Mówimy wtedy – po utrwaleniu tej treści na jednym z wymienionych nośników, że mamy do czynienia z dokumentem elektronicznym lub papierowym. Nie jest to jeszcze jednak dokument w rozumieniu, jakie podane zostało w definicji – brak bowiem podpisu – ale o tym będzie mowa dalej. Jak widać, forma dokumentu jest pierwotna w stosunku do jego postaci, bowiem najpierw musi powstać zamysł, wyobrażenie treści dokumentu, a dopiero później jej utrwalenie. Jest też oczywiste, że wymienione cechy (forma i postać) muszą współistnieć, by mógł powstać dokument.

Czynnikiem mającym wpływ na powstanie dokumentu jest sposób, w jaki jest on tworzony, czyli **format**. Ma on znaczenie dla czytelności oraz nakładu pracy niezbędnego do utworzenia dokumentu, a także dla wygody późniejszego operowania zawartością dokumentu. Inaczej tworzy się dokument „od zera", a inaczej, jeśli można wykorzystać wzór, który w dodatku pozwala uzyskać dokument częściowo wypełniony danymi, zawartymi w słownikach czy danych konta należącego do twórcy pisma. W systemach elektronicznego zarządzania dokumentami stosowane są również szablony, które umożliwiają zachowanie odpowiedniego układu elementów informacyjnych pisma – ich rozlokowania w stosunku do siebie. W taki sposób tworzone są **naturalne dokumenty elektroniczne**. Naturalny dokument elektroniczny powinien być tworzony **kompletnie** – tak, aby po jego utworzeniu nie były potrzebne żadne czynności, które zazwyczaj wymagały po utworzeniu dokumentu jego wydruku na papierze, w celu uzupełnienia numeru kancelaryjnego, daty, pieczątki imiennej podpisującego oraz jego własnoręcznego podpisu, a także wykaz ewentualnych załączników Wszystkie te dane muszą być już wcześniej umieszczone w treści dokumentu, by można było go elektronicznie podpisać.

Dokumenty w postaci elektronicznej mogą także powstawać jako **odwzorowania cyfrowe** dokumentów utworzonych pierwotnie najczęściej na papierze, a później skanowanych lub fotokopiowanych cyfrowo i zamienianych najczęściej na dokumenty w formacie pdf (nieprzeszukiwalnym, tzn. niepozwalającym na odszukanie konkretnego ciągu znaków po wciśnięciu klawiszy Ctrl+F aktywujących wyszukiwarkę wyrazów w tekście). Odwzorowania cyfrowe tworzy się w podmiotach, w których osoby uprawnione do podpisywania dokumentów wychodzących są „**elektronicznie niepiśmienne**", tzn. z różnych przyczyn (mentalnych, organizacyjnych) nie są w stanie podpisać dokumentu elektronicznie, a podpis mogą złożyć wyłącznie własnoręcznie na pieczątce imiennej, zawierającej w treści imię, nazwisko i stanowisko, uczytelniającej własnoręczny podpis, charakterystyczny dla danej osoby, ale zwykle będący nieczytelnym znakiem graficznym.

**Odwzorowania cyfrowe**, będące kopiami wydruków na papierze są już siłą rzeczy skażone utratą pewnych informacji, wynikającą z jakości skanowania (rozdzielczości skanera), zamiany barw na odcienie szarości lub tylko na kolor czarno-biały, co może prowadzić do całkowitej nieczytelności pewnych fragmentów treści dokumentu. Jeśli na dodatek odwzorowanie cyfrowe wykonywane jest z kopii kserokopii, która już sama jest kopią, efekty mogą być zupełnie niezgodne z celem działania.

Co do zasady – jeśli jakaś informacja nie ma rzeczywistego znaczenia w procesie jej przekazywania – nie powinna być przesyłana, ponieważ stanowi jedynie „szum" Zatem **jednoznaczność odczytu treści dokumentu i jego pełna czytelność** są kolejnymi warunkami poprawności procesu tworzenia dokumentu. Jednoznaczność odczytu każdego znaku gwarantuje albo wysoka jakość odwzorowania cyfrowego, co niesie za sobą z reguły znaczny wzrost wielkości (rozmiaru, objętości) przesyłanego pliku, przy założeniu, że każdy znak jest jednoznaczny (litera, cyfra, znak interpunkcyjny itd…) , albo przesyłanie dokumentu oryginalnego – naturalnego dokumentu cyfrowego.

Plik będący **odwzorowaniem cyfrowym** – by był dokumentem, powinien być podpisany elektronicznie – w rozumieniu funkcji podpisu jako technicznego zabezpieczenia przed niekontrolowaną modyfikacją. Podpis – stanowiący wyrażenie woli/akceptacji treści pisma, umieszczany pod jego treścią (na imiennej pieczątce) - na pliku cyfrowo odwzorowanym znajduje się zawsze (chociaż często jest to nieczytelny podpis na nieczytelnej pieczątce!), natomiast pliki będące naturalnymi dokumentami elektronicznymi bywają podpisywane elektronicznie mimo niepełnej treści (niekompletna data, zawierająca jedynie rok i miesiąc, niekompletny numer kancelaryjny oraz brak imienia i nazwiska oraz stanowiska osoby podpisującej treść dokumentu, kończącego się słowami „z poważaniem"). Jest to błąd, ponieważ treść pisma, po wydrukowaniu, powinna być kompletna. Podpis elektroniczny dotyczy bowiem jedynie dokumentu w postaci elektronicznej – bo tylko w odniesieniu takiego dokumentu można dokonać procesu weryfikacji. To, że jednocześnie może spełniać on drugą funkcję, jako powiązanie konkretnej osoby fizycznej z podpisywanym dokumentem, jest sprawą odrębną.

W tym momencie należy wspomnieć o odnotowanych już praktykach, związanych z tworzeniem i podpisywaniem dokumentów przesyłanych przez podmioty publiczne, które to praktyki z punktu widzenia sensowności działania, bezpieczeństwa obrotu prawnego i wiarygodności dokumentów są niewłaściwe.

(1) Dokument stanowiący **odwzorowanie cyfrowe** podpisanego dokumentu papierowego, podpisany elektronicznie przez inną osobę (pracownika kancelarii) w celu zapewnienia integralności i potwierdzenia źródła – podmiotu z którego pismo zostało wysłane

(2) Dokument stanowiący **naturalny dokument elektroniczny**, z pozostawionymi pustymi miejscami na późniejsze uzupełnienie daty, numeru pisma oraz imienia, nazwiska i stanowiska osoby, która miała podpisać pismo.

Podpis elektroniczny jest ostatnim z elementów, który tworzy dokument w jego rozumieniu jako potencjalnego dowodu **Osoba składająca podpis elektroniczny** nie tylko podpisuje go w znaczeniu tradycyjnym, jako wyrażająca akceptację treści znajdującej się powyżej jawnie wyszczególnionych w piśmie jej imienia, nazwiska i stanowiska, umieszczonych w treści dokumentu w miejscu, w którym zazwyczaj w wersji papierowej przystawia się pieczęć imienną, ale jednocześnie dokonuje zabezpieczenia treści podpisywanego dokumentu przed niekontrolowaną zmianą.

**Definicje dokumentu**

Dokument jest jednym z najtrudniej definiowalnych pojęć. Pojawienie się dokumentów elektronicznych obok dokumentów papierowych pozwoliło jednak wyodrębnić pewne cechy wspólne, które – niezależnie od postaci – są cechami dokumentów, pojmowanych jako potencjalne dowody Jeśli bowiem celem tworzenia dokumentu jest utrwalenie pewnej informacji, to wiadomym jest, że informacja ta musi być później odczytywalna, wiarygodna, zabezpieczona przed niekontrolowaną zmianą, umiejscowiona w czasie i miejscu. Informacja nie musi być jednak trwale związana z tym samym nośnikiem, na którym została pierwotnie zapisana. Właśnie z uwagi na możliwość degradacji nośników możliwość przenoszenia informacji na inne nośniki jest jednym ze sposobów zabezpieczenia jej przed utratą, podobnie jak możliwość zwielokrotnienia zapisanej informacji. Niezależnie od powyższego, dokument musi mieć swojego twórcę, choć niekiedy będzie on wynikiem działania pewnego systemu, który wytworzy dokument w wyniku wcześniej zaprogramowanych procedur Wydaje się, że można byłoby przyjąć także następującą definicję dokumentu:

> **Dokument** – informacja stanowiąca odrębną całość znaczeniową, wyrażona w dowolnej formie, utrwalona w dowolnej postaci, możliwa do jednoznacznego wielokrotnego odczytania, przesłania i zapisania, której powstanie daje się powiązać z czasem, miejscem i okolicznościami jej wytworzenia, i która jest zabezpieczona przed niekontrolowaną modyfikacją.

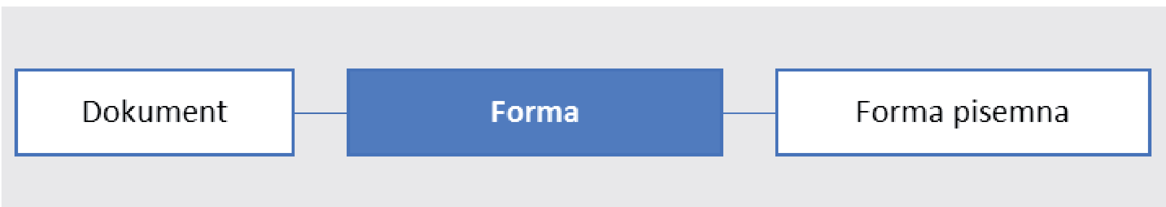
Elementy powyższej definicji również muszą być szczegółowo wyjaśnione. Należy pamiętać, że dokument jest rzeczą, przedmiotem (kartką papieru lub informatycznym nośnikiem danych), a forma czynności prawnej jest działaniem, czynnością mniej lub bardziej rozbudowaną, wykonywaną przez jedną lub więcej osób. Odróżnianie tych subtelności jest niezbędne przy rozpatrywaniu cech, jakie mogą charakteryzować zapis informacji, który w wyniku badania będzie można zakwalifikować jako dokument o słabszej lub silniejszej mocy dowodowej.

W szczególności konieczne jest rozróżnianie formy wyrażenia pewnego przekazu informacji (tekstem, grafiką, dźwiękiem, sekwencją obrazów i wszelką kombinacją wymienionych form), ponieważ w środowisku elektronicznym e-administracji informację zawsze daje się zapisać jako skończony ciąg stanów binarnych, zer i jedynek, które oprogramowanie przekształca do formy czytelnej dla człowieka lub komputera.


*Podstawowe elementy konstytuujące dokument – forma wyrażenia informacji, postać nośnika i zabezpieczenie przed niekontrolowaną modyfikacją*

## 5.1 Forma

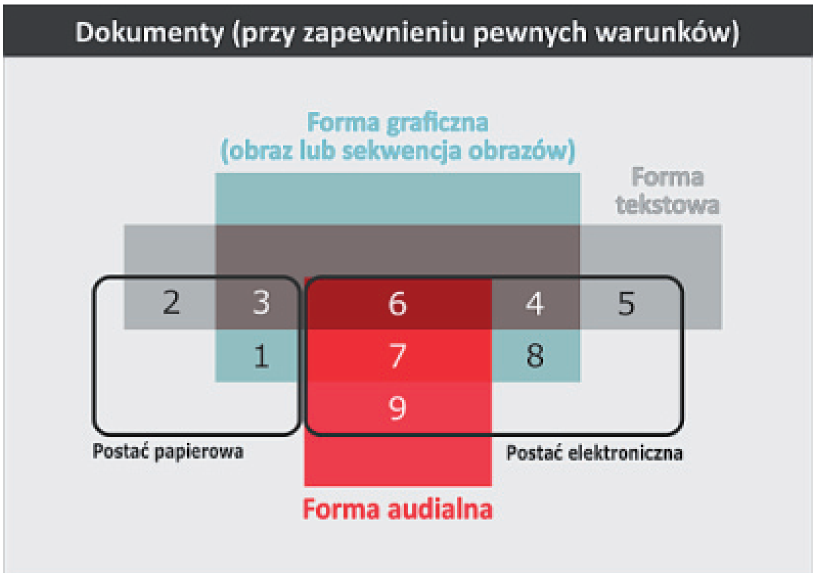
| |
|---|
| **Forma** – tu: sposób wyrażenia i przekazu informacji pismem, obrazem, dźwiękiem lub ich kombinacją. |




*Forma*

„Formę" należy rozumieć jako **sposób wyrażenia informacji** – tekstem, grafiką, dźwiękiem (lub ich kombinacją). Zauważmy, że o ile w świecie „namacalnym", który postrzegamy zmysłami wzroku, dotyku (osoby niewidzące) czy słuchu, **formę pisemną** realizujemy najczęściej poprzez **pisanie tekstu** (słowami, cyframi - a więc zdecydowanie lepiej oddające istotę rzeczy byłoby określenie „**forma tekstowa**"). Podobnie **grafikę** (zdjęcia, rysunki, schematy, diagramy, wykresy, mapy itd.) stosujemy do przekazu takiej informacji, której przekazanie słowami byłoby nieprecyzyjne, nieoddające istoty rzeczy lub wręcz niemożliwe, czyli bezcelowe. Jak bowiem **słowami** precyzyjnie wyrazić podobiznę twarzy umieszczaną np. w dowodzie tożsamości, albo opis części jakiejś maszyny czy plan miasta?

Niestety – i jest to jedna ze słabości nienadążającego za rozwojem techniki prawa, w rozumieniu np. Kodeksu cywilnego **forma pisemna** kojarzona jest bardzo wąsko - z pismem rozumianym jako litery i cyfry - i to na papierze, w połączeniu ze złożeniem własnoręcznego podpisu pod treścią dokumentu, będącego np. oświadczeniem woli, a nie w znaczeniu **utrwalonej informacji,** która, jak już wspomniano, może być zapisana za pomocą **sekwencji zer i jedynek (binarnie)** bez względu na to, czy jest zapisem tekstu, obrazu czy dźwięku. Takie zawężenie pojmowania formy pisemnej prowadzi właśnie do sytuacji, w której aktualne prawo staje się wyraźnie niedostosowane do rzeczywistości technologicznej




*Pojęcia „formy" i „postaci" jako niezależnych cech konstytutywnych dokumentu.*

Ta sama treść oświadczenia woli sporządzona na papierze **w formie pisemnej** (a więc zaopatrzona w podpis własnoręczny) zeskanowana lub wysłana faksem – mimo iż nadal będzie czytelna i wyraźna, a różnica będzie polegała wyłącznie na innym egzemplarzu nośnika, na tym, że skan i faks są kopiami treści oryginału, nie będzie już w rozumieniu prawa formą pisemną. Gołym okiem widoczny fakt, że mamy do czynienia z kopią odbiera pewność, że jest ona treściowo tożsama z treścią oryginału – czyli jest **słabsza dowodowo.** Jeśli jednak twórca pisma ponownie podpisze własnoręcznie ową kopię, znowu będzie to „zachowanie formy pisemnej" Przepisy Art. 78. § 1 Kodeksu cywilnego nie pozostawiają w tej kwestii żadnych wątpliwości. Proponuje się jednak pojmowanie **formy pisemnej** (z uwagi na jej jednoznaczność, co w obrocie prawnym ma fundamentalne znaczenie), jak niżej z zastrzeżeniem, że **zawsze** - niezależnie, czy mowa jest o dokumencie papierowym czy elektronicznym - chodzi o dokument **podpisany** przez właściwą osobę w sposób jednoznaczny i bez żadnych wątpliwości – niezaprzeczalnie, w sposób umożliwiający jednoznaczną i pewną **identyfikację** podpisującego.

Numerowane pola na rysunku stanowiące **część wspólną** prostokątów symbolizujących poszczególne **formy przekazu informacji** i obwiedzionych **czarnymi liniami** pól symbolizujących nośniki, na których informacja została zapisana, oznaczają różnego rodzaju dokumenty, z jakimi w praktyce spotykają się urzędnicy Należy zwrócić uwagę, że o ile formy przekazu informacji mogą w jednym dokumencie występować wspólnie (dlatego prostokąty symbolizujące różne **formy przekazu informacji** mogą się pokrywać), o tyle nośniki są albo elektroniczne, albo nieelektroniczne – i z tego powodu pola wyobrażające **postaci nośników** nie nakładają się (ich krawędzie nie przecinają się). Prostokąty leżące poza obszarami nośników o różnej postaci nie są numerowane, ponieważ **informacja nieutrwalona nie będzie rozumiana jako dokument**. Samo utrwalenie też nie zapewnia jeszcze wszystkich atrybutów dokumentu (niezmienność treści, możliwość ustalenia autora, daty utworzenia).

W poniższej tabeli pokazano w nieco innej formie – tabelarycznej – znaczenie poszczególnych numerowanych pól – znakiem „x" oznaczono pokrywające się obszary, którym odpowiada numer w lewej skrajnej kolumnie:

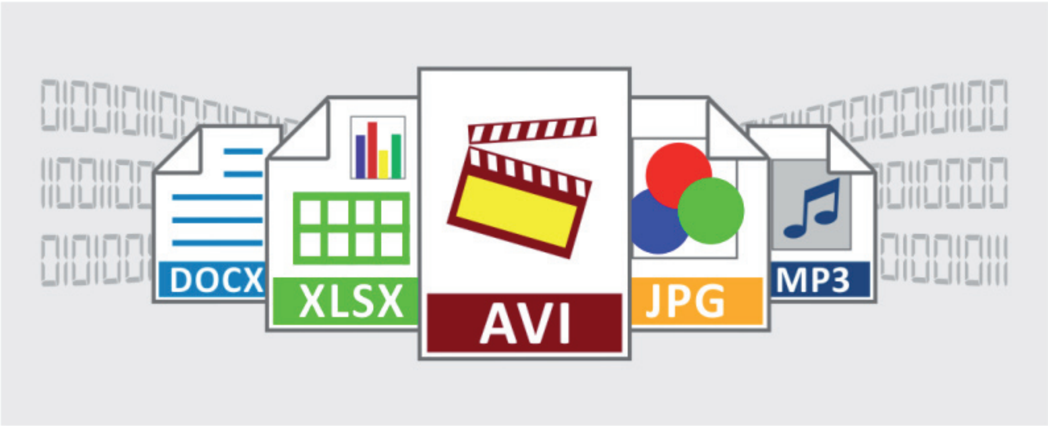
| | Forma | | | Postać | |
|---|---|---|---|---|---|
| | tekstowa | graficzna | audialna | papierowa | elektroniczna |
| 1 | | X | | X | |
| 2 | X | | | X | |
| 3 | X | X | | X | |
| 4 | X | X | | | X |
| 5 | X | | | | X |
| 6 | X | X | X | | X |
| 7 | | X | X | | X |
| 8 | | X | | | X |
| 9 | | | X | | X |

*Zestawienie stosowanych form i postaci dokumentów*

1) Dokument graficzny - zdjęcie, mapa, rysunek na papierze, podpisane własnoręcznie
2) Dokument tekstowy na papierze, podpisany własnoręcznie lub systemowo (identyfikator umożliwiający pobranie treści oryginalnej ze źródła, jak np. wyciąg z KRS czy z REGONu)
3) Dokument tekstowy zawierający rysunki na papierze podpisany własnoręcznie lub systemowo (identyfikator umożliwiający pobranie treści oryginalnej ze źródła)
4) Dokument tekstowy zawierający rysunki - w postaci elektronicznej, podpisany elektronicznie
5) Dokument tekstowy w postaci elektronicznej, podpisany elektronicznie
6) Np. film udźwiękowiony z napisami zrealizowany cyfrowo i podpisany
7) Np. film udźwiękowiony (bez napisów) w postaci elektronicznej, podpisany

8) Obraz lub sekwencje obrazów w postaci elektronicznej, bez dźwięku, elektronicznie podpisane
9) Nagranie dźwiękowe w postaci elektronicznej, elektronicznie podpisane

Jak widać, w **postaci elektronicznej** zapisać można **dwukrotnie więcej** typów dokumentów (co odpowiada dzisiejszym potrzebom i poziomowi technologicznego zaawansowania społeczeństwa informacyjnego), niż w **postaci papierowej**.




Środki przekazu informacji muszą być tak dobrane, by odbiorca tej informacji był w stanie odebrać to, co nadawca przekazać zamierzał – bez zniekształceń, czyli bez utraty istotnej części informacji. Oznacza to, że w pewnych typach dokumentów trzeba będzie użyć zarówno tekstu, jak i obrazu. Jak do tej pory, informację w formie tekstowej i graficznej zapisać można było na papierze. Jeśli jednak chcielibyśmy dodać informację w formie filmu (sekwencja grafik) i dźwięku, musielibyśmy zmienić rodzaj nośnika i zastosować dodatkowe urządzenie umożliwiające odczyt tak zapisanej informacji. I właśnie w tym miejscu z pomocą przychodzi informatyka ze swoimi narzędziami – zapisu informacji w sposób umożliwiający gęste jej upakowanie, szybki i bezbłędny odczyt, przekazywanie na duże odległości w krótkim czasie, powielanie bez utraty jakości. Ten zapis może być zapisem zarówno niewielkiego objętościowo dokumentu, jak i kilkugodzinnego filmu. Niech przykładem będzie stosunkowo niedawno wprowadzona rejestracja rozpraw sądowych, w czasie których nagrywany jest dźwięk oraz obraz.[1] Podobnie, rejestracja audiowizualna sesji rady miasta czy otwarcia ofert przetargowych może odbywać się elektronicznie – i **pliki takie, jeśli zostaną opatrzone podpisami elektronicznymi** – staną się **dokumentami**.

Należy zwrócić uwagę, że wszystkie wymienione wyżej korzyści ze stosowania narzędzi informatyki są **uniwersalne**. Wszędzie bowiem możemy mieć do czynienia z zapisywaniem i przekazywaniem informacji **tekstowej**, **graficznej** czy **audialnej** (dźwiękowej) bez względu na obszar zastosowania; w administracji, wymiarze sprawiedliwości, biznesie, bankowości,

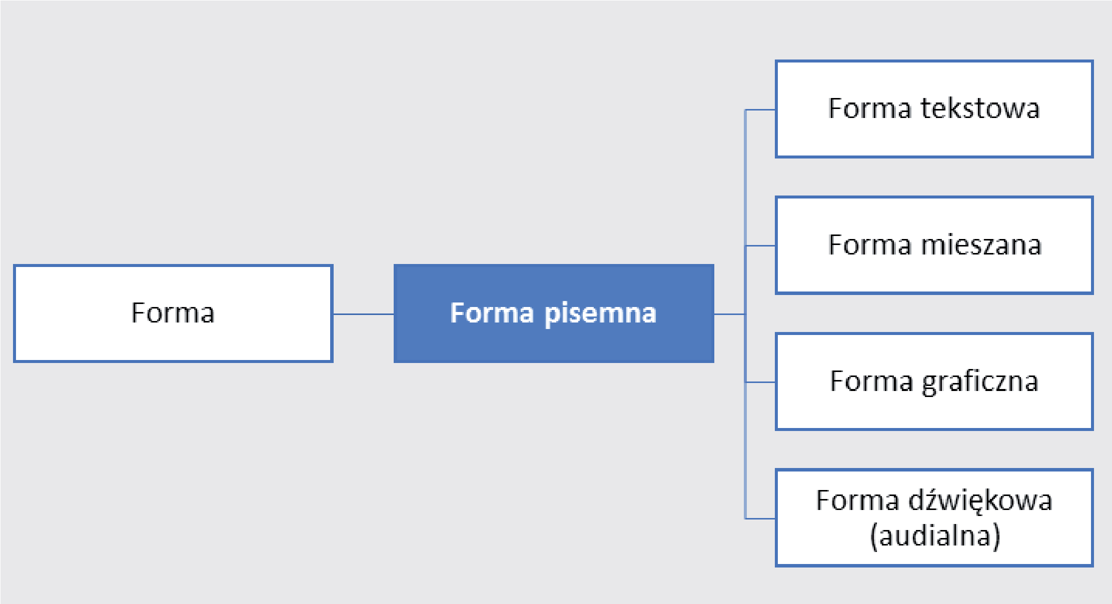
1 Przepis wprowadzający rejestrację rozpraw sądowych.

ochronie zdrowia, sporcie itd. Twierdzenie, że w jakimś sektorze nie można zastosować narzędzi informatycznych i dokumentów w postaci elektronicznej, że musi być stosowany nośnik papierowy nie znajduje obecnie merytorycznego ani technicznego uzasadnienia. Przeszkodą może być wyłącznie organizacyjna niezdolność i trudne do przełamania bariery mentalne.

Dzięki możliwości zapisu **dowolnej informacji** jako ściśle określonej sekwencji stanów binarnych (dwóch, dających się jednoznacznie odróżnić stanów – otwór/brak otworu, czarny/biały, 0/1, namagnesowany/nienamagnesowany, odbija/rozprasza światło itd.), dokonuje się zmiana cywilizacyjna, która umożliwia znaczące obniżenie kosztów **zapisu, przechowywania i przesyłania informacji** przy jednoczesnym **ogromnym wzroście efektywności tego przekazu**, a także zapewnieniu związania treści z ich twórcą. Dzięki oprogramowaniu interpretującemu te sekwencje zero-jedynkowe urealniają się i prezentują zgodnie z zamierzeniami nadawcy - wolne są od zakłóceń wprowadzanych przez pośrednie przetwarzania (drukowanie na papierze, a później skanowanie zadrukowanego papieru).

### 5.1.1. Forma pisemna

**Forma pisemna** – tu: sposób wyrażenia informacji jako utrwalonej, zapisanej, nieulotnej, w przeciwieństwie do formy ustnej, która jest sposobem wyrażenia, przekazania informacji bez jej utrwalenia na jakimkolwiek nośniku trwałym.




*Forma pisemna*

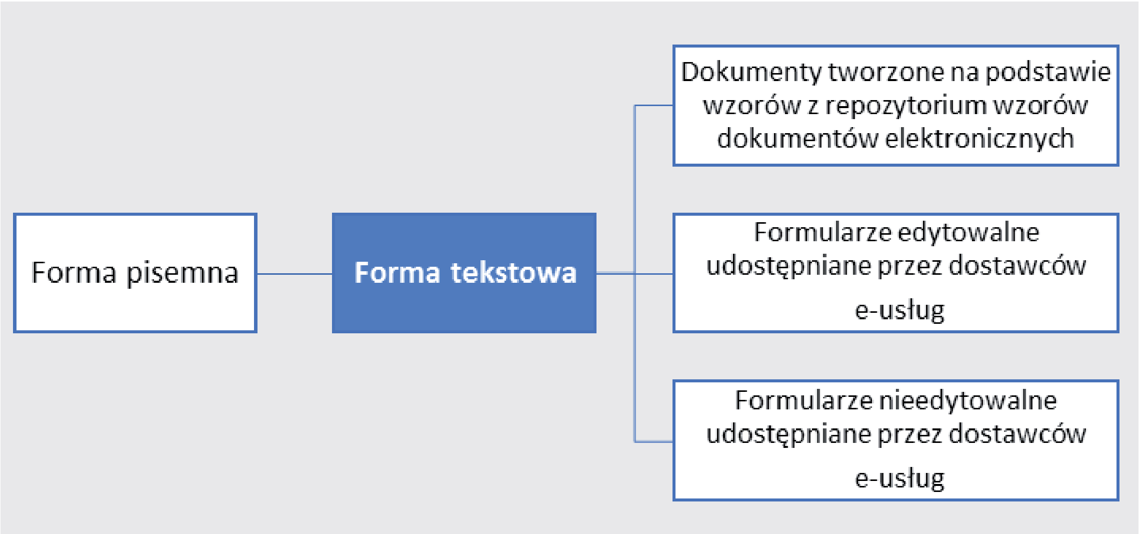
**<u>Uwaga: sposobu wyrażenia informacji nie należy mylić z formą czynności prawnej</u>**. Podobieństwo określeń może być mylące, dlatego postuluje się redefinicję sformułowań zakorzenionych w przeszłości, w której nie istniały jeszcze środki komunikacji elektronicznej ani elektroniczny zapis informacji.


Forma pisemna rozumiana jako **forma czynności prawnej** stosowana jest powszechnie w celu zapewnienia dowodowości postępowania – i w takim znaczeniu występuje w przepisach prawa. Najczęściej mamy do czynienia z formą pisemną zwykłą. Każdy prawnik wie, co pojęcie to oznacza i potrafi dodać jeszcze trzy inne pokrewne: formę pisemną z datą pewną, formę pisemną z podpisami urzędowo lub notarialnie poświadczonymi oraz formę pisemną aktu notarialnego. Formy te różnią się od siebie procedurą ich realizacji (są czynnościami wykonywanymi w odniesieniu do dokumentów w pewnej procedurze), a tym samym różnią się od siebie tzw „mocą dowodową" i skutkami prawnymi, ale mają jedną istotną, kluczową cechę wspólną – są formami wykorzystującymi dokumenty – czyli **treści utrwalone**, nieulotne, co do których prawdziwości istnieje pewność wynikająca z procedury ich wytworzenia.

Dokumenty są utrwalane w różny sposób i ów proces utrwalania – a ściślej procedura realizacji tych form stanowi o tym, czy dane czynności prawne w ogóle będą ważne, i jak mocne będą dowodowo. Wspólną cechą wszystkich form pisemnych jest to, że przekaz informacji (ich treść) zapisany jest za pomocą słów, cyfr, i innych znaków alfanumerycznych **utrwalonych** w sposób umożliwiający **wielokrotne odczytanie** i **powielenie** a także **przekazanie**. Nie jest istotne, czym treść wspomnianych dokumentów jest zapisana (tzn. jakim narzędziem czy urządzeniem do pozostawiania znaków – rylcem, długopisem, tuszem, laserem), na czym jest napisana (tzn. na jakim nośniku – papierze, korze brzozowej, skórze, tkaninie, plastiku, dysku magnetycznym), w jakim języku, jak wielkimi znakami, jaką czcionką, ręcznie czy maszynowo, powoli czy szybko itd. Istotne jest natomiast, że pismo jest utrwalone i wyrażone w sposób umożliwiający jego ponowne jednoznaczne odczytanie w znaczeniu, w jakim zostało zapisane.

#### 5.1.1.1. Forma tekstowa

| |
|---|
| **Forma tekstowa** - sposób wyrażenia informacji tekstem, pismem, słowami i cyframi; |




*Forma tekstowa*

Jest to najczęstszy, przeważający sposób przekazu informacji – teksty dokumentów najczęściej wyrażają się pismem. Zgodnie z definicją dokumentu informacja zapisana tekstem musi być utrwalona, musi dać się odczytać i przesłać, a także musi być zabezpieczona przed niekontrolowaną modyfikacją – i temu celowi służy podpis elektroniczny

Jeśli treść tak utworzonego dokumentu zostanie wydrukowana, niezmienność jej treści – potwierdzenie zgodności treści z treścią elektronicznego oryginału będzie musiała być potwierdzona własnoręcznym podpisem osoby dokonującej konwersji postaci (forma pozostaje ta sama).

Tekst może być organizowany w tabele, w akapity – nie zmienia to istoty kwalifikacji – nadal będzie to forma tekstowa.

##### 5.1.1.1.1. Dokumenty tworzone na podstawie wzorów z repozytorium wzorów dokumentów elektronicznych

Dokumenty tworzone na podstawie wzorów zamieszczonych w repozytoriach lokalnych, regionalnych i centralnym są dokumentami tekstowymi, niekiedy tabelarycznymi.

##### 5.1.1.1.2. Formularze edytowalne udostępniane przez dostawców e-usług

Większość usługodawców zamieszcza na swoich stronach internetowych edytowalne formularze w formatach doc, docx, rtf. Formularze te można wypełniać komputerowo przed wydrukiem, a po wydrukowaniu należy je podpisać i przesłać do usługodawcy lub dostarczyć je osobiście i podpisać na miejscu (po okazaniu dowodu tożsamości) w obecności osoby odbierającej dokumenty – będzie to właśnie forma pisemna zwykła.

##### 5.1.1.1.3. Formularze nieedytowalne udostępniane przez dostawców e-usług

Usługodawcy udostępniają także nieedytowalne formularze w formacie pdf – do wydruku i ręcznego wypełnienia. Formularze takie – podobnie jak edytowalne – należy zanieść do urzędu i podpisać na miejscu (dokument wiarygodny), lub podpisać i przesłać do urzędu (dokument znacznie mniej wiarygodny, gdyż w istocie nie wiadomo, kto dokument ten podpisał).

#### 5.1.1.2. Forma mieszana

| |
|---|
| **Forma mieszana** - sposób wyrażenia informacji w jednym dokumencie za pomocą tekstu, rysunków, zdjęć |

Forma mieszana stosowana jest powszechnie jako kombinacja innych prostszych form przekazu informacji – najczęściej formy tekstowej i graficznej. Warto zauważyć, że z uwagi na fakt, iż każdą informację można zapisać jako skończoną sekwencję stanów binarnych, nie ma przeszkód, by takie formy tworzyć w sposób naturalny – np. jako dokument tekstowy zawierający ilustracje, albo jako sekwencje obrazów z towarzyszącym im dźwiękiem (film).

#### 5.1.1.3. Forma graficzna

**Forma graficzna** – sposób wyrażenia informacji za pomocą grafik, rysunków, schematów, zdjęć

Dokumenty w formie graficznej to wszelkiego rodzaju mapy, schematy, zdjęcia, plany – rysunki wektorowe lub rastrowe. Przekaz informacji grafiką jest powszechnie stosowany w sytuacjach, w których przekazanie informacji słowami byłoby nieprecyzyjne, nieoddające istoty rzeczy lub wręcz niemożliwe.

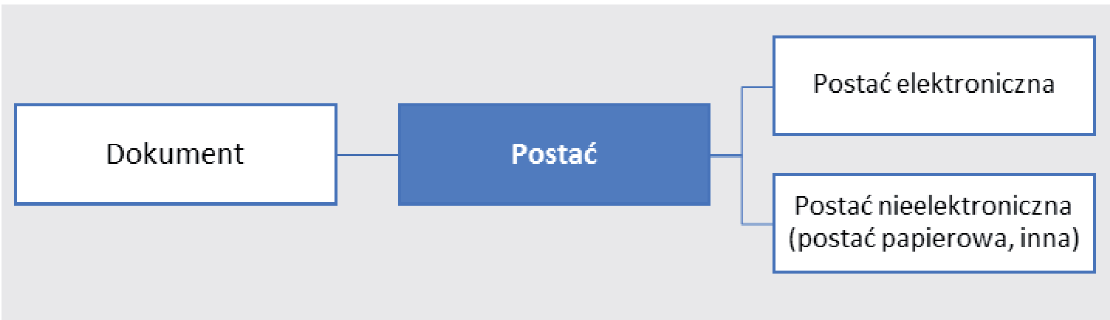
#### 5.1.1.4. Forma dźwiękowa (audialna)

**Forma audialna** – sposób wyrażenia informacji za pomocą dźwięku, nagrania ustnych wypowiedzi

Dokumenty w formie audialnej są już tworzone (protokoły spotkań nagrywane cyfrowo), rozprawy sądowe, reportaże – i należy traktować je na równi z dokumentami papierowymi. W pewnych sytuacjach dokumenty audialne mogą być transkrybowane do formy tekstowej (czyli pisemnej w tradycyjnym rozumieniu) i jako takie udostępniane.

## 5.2 Postać

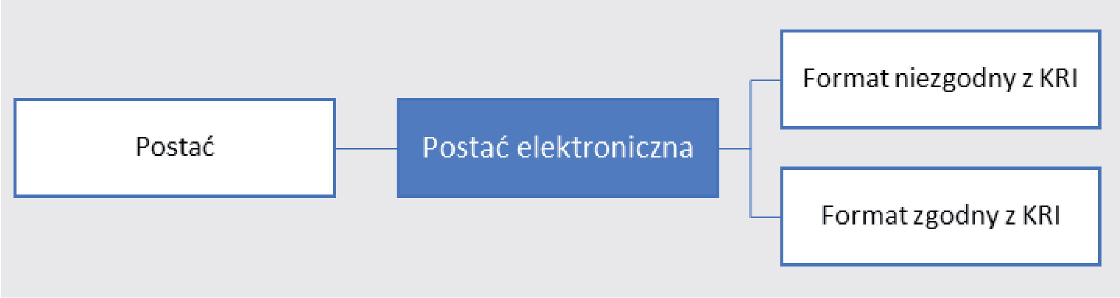
**Postać** - określenie wskazujące na rodzaj nośnika, na którym utrwalona została treść dokumentu - np. postać papierowa, postać elektroniczna;




*Postać*

Informacja może być w różnej postaci zapisana na nośnikach, od których zależy technologia dokonywania tego zapisu.

### 5.2.1. Postać elektroniczna




*Postać elektroniczna*

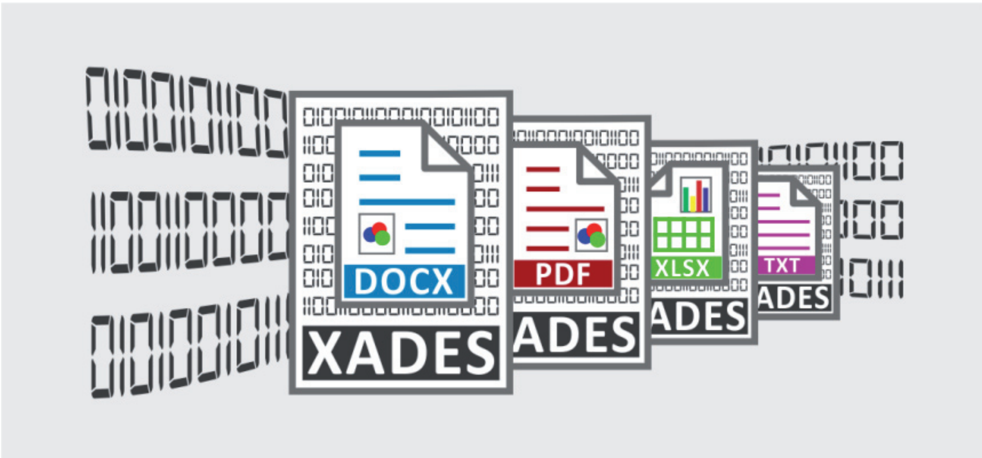
Informacja w postaci elektronicznej może być zapisana na różnych nośnikach, zarówno elektromagnetycznych, jak i plastikowych. O zapisie w postaci elektronicznej mówimy wtedy, gdy do zapisu i odczytu informacji używamy środków technicznych zapisujących informację binarnie, a interpretacji i wyświetlenia (wydrukowania) w formie czytelnej dla człowieka dokonuje się za pomocą odpowiedniego oprogramowania.

#### 5.2.1.1. Format niezgodny z KRI

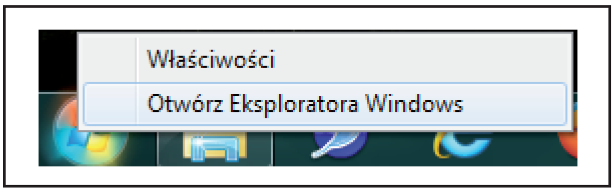

*Format niezgodny z KRI*

W celu umożliwienia pracownikom usługodawcy odczytywania przekazywanych przez usługobiorców dokumentów elektronicznych (lub danych) dokonano wyboru pewnych ogólnoświatowych (de facto) standardów Może się jednak zdarzyć, że dokumenty wpływające do urzędu będą miały format niezgodny z rozporządzeniem w sprawie KRI. Dokumenty tego samego typu (np. tekstowe, arkusze kalkulacyjne, archiwa) – mogą mieć różne **formaty**. Dopuszczalne formaty podane są w kolumnie 2 załącznika nr 2 do **rozporządzenia Rady Ministrów w sprawie KRI**.

Dzisiejszy poziom zaawansowania technologii informatycznych powoduje, że najczęstszą czynnością użytkownika komputera jest klikanie, bez wcześniejszego dociekania, jaka będzie reakcja systemu na to kliknięcie. Coraz łatwiejsze korzystanie z komputerów powoduje, że użytkownicy coraz mniej wiedzą o tym, jak działają systemy informatyczne, jaką budowę mają pliki komputerowe, jaką rolę pełnią tzw rozszerzenia nazw plików Zdarza się, że tzw rozszerzenie pliku (znaki od ostatniej kropki w prawo w nazwie pliku) nie jest systemowi znane. Użytkownicy często wyłączają widoczność rozszerzenia pliku – a tym samym odbierają sobie możliwość szybszego dotarcia do istoty problemów  Rzecz w tym, że dokumenty tworzone w edytorach tekstu mają obecnie najczęściej rozszerzenia  docx,  doc,  rtf, .odt, dość już rzadko  txt. Są jednak również pliki arkuszy kalkulacyjnych (rozszerzenia  xls, .xlsx, .ods) i inne pliki, które mogą wpłynąć do urzędu – i powinny móc być odczytane. Sprawa jednak się komplikuje, kiedy zostaną one podpisane elektronicznymi **podpisami otaczającymi**. Rozszerzenia zmienią się wtedy na .xades lub na  xml. Jeśli osoba otrzymująca taki plik nie posiada programu do weryfikacji podpisu – nie będzie mogła nie tylko zweryfikować podpisu, ale nawet zapoznać się z zawartością pliku.

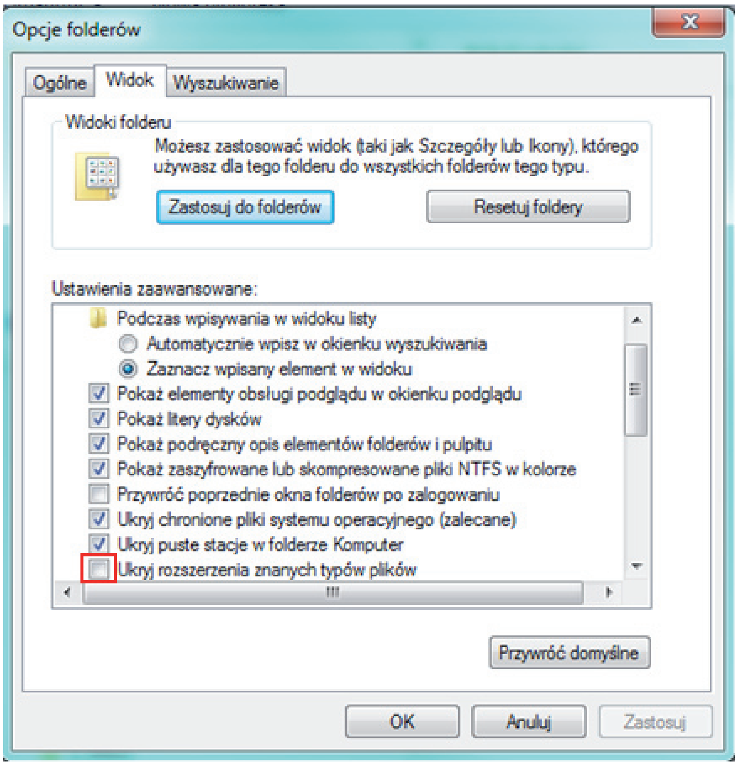



Jak z powyższego wynika, pracownik administracji powinien umieć ustalić (rozpoznać) **rozszerzenie pliku** – by wiedzieć, czy ma do czynienia z plikiem odczytywalnym (o strukturze wskazywanej przez rozszerzenie wymienione w rozp. w sprawie KRI), czy z jakimś „egzotycznym” formatem, nieodczytywalnym bez instalacji szczególnego oprogramowania.




*Otwarcie Eksploratora Windows*

Przede wszystkim należy zatem zadbać o widoczność rozszerzeń wszystkich typów plików  Uzyskać to można klikając w Eksploratorze Windows w menu „Organizuj”, następnie kolejno „Opcje folderów i wyszukiwania”, zakładka „Widok”, następnie w „Ustawieniach zaawansowanych” należy usunąć zaznaczenie z checkboxu obok „Ukryj rozszerzenia znanych plików”, by zawsze widzieć rozszerzenia – i móc stwierdzić bezpośrednio, czy badany plik powinien być otwarty (odczytany), czy nie.




*Ustawienie widoczności rozszerzeń plików.*

Jeśli już zidentyfikujemy rozszerzenie pliku i stwierdzimy, że nie jest nam znane, sprawdzamy w załączniku nr 2 do rozporządzenia Rady Ministrów w sprawie KRI, czy jest to rozszerzenie pliku, który powinniśmy móc odczytać. Jeśli tak, zwracamy się w sposób przyjęty w danym podmiocie o zainstalowanie na używanym przez nas komputerze aplikacji, za pomocą której powinniśmy móc otwierać pliki określonego formatu. Np. zdarza się, że urzędnik otrzyma pocztą elektroniczną spakowany plik archiwum o rozszerzeniu rar W wykazie podanym z załączniku nr 2 do rozporządzenia RM w sprawie KRI nie ma takiego rozszerzenia, ale jest np. 7Z.

Warto wiedzieć, że program 7-Zip, który można pobrać ze strony www 7-zip.org otwiera nie tylko archiwa w formacie 7z, ale także w formatach XZ, ZIP, GZIP, BZIP2, TAR, WIM, LZMA, RAR, CAB, ARJ, Z, CPIO, RPM, DEB, LZH, SPLIT, CHM, ISO, UDF, COMPOUND, DMG, XAR, HFS, NSIS, NTFS, FAT, VHD, MBR, SquashFS, CramFS. Innymi słowy, chociaż pracownik administracji miałby prawo odesłać (nie przyjąć) pliku z rozszerzeniem innym niż wyszczególnione w rozporządzeniu RM w sprawie KRI, może posłużyć się wspomnianym programem do rozpakowania przesłanego pliku archiwum – i dalej postępować zgodnie z procedurą przewidzianą dla danej sprawy Rozpakowanie pliku (wyodrębnienie plików zawartych w archiwum) jest czynnością czysto techniczną, a nie prawną.

Wspomniany program powinien być standardowym wyposażeniem każdej stacji roboczej, gdyż pakowanie wielu plików do jednego archiwum jest przydatne chociażby przy wysyłce pocztą elektroniczną lub przekazywaniu za pośrednictwem ePUAP

#### 5.2.1.1.1. Brak możliwości korekty

Jeśli interesant prześle plik w formacie niedającym się odczytać (np. w formacie wymagającym instalacji specjalnego oprogramowania) – czyli w żadnym z formatów ujętych w załączniku nr 2 do rozpKRI, plik ten może być odrzucony Podmioty publiczne na swoich stronach internetowych oraz w BIP powinny informować o dopuszczalnych formatach przesyłanych plików i sposobach ich dostarczania.

#### 5.2.1.1.2. Możliwość korekty

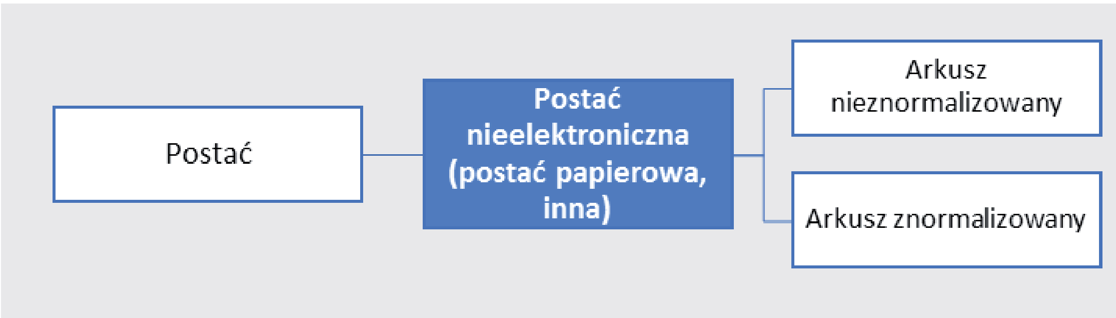
Jeśli możliwe jest odczytanie pliku mimo iż został dostarczony w formacie niewyszczególnionym w załączniku nr 2 do rozporządzenia KRI, można dokonać konwersji do formatu legalnego pod warunkiem zachowania pliku oryginalnego. Powstaje wtedy kopia treści. Sytuacje takie zdarzają się w momentach zmian technologicznych i wskutek stale trwającego postępu technicznego. Np. kiedy pojawił się format .docx wiele urzędów przez pewien okres nie potrafiło odczytać dokumentów przesyłanych w tym formacie, gdyż stosowane edytory pozwalały odczytywać jedynie dokumenty w formacie .doc.

#### 5.2.1.2. Format zgodny z KRI

Pliki w formatach zgodnych z Rozporządzeniem Rady Ministrów z dnia 12 kwietnia 2012 r w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (Dz.U 2012.526) – jako legalne - muszą być przyjmowane przez usługodawców

### 5.2.2. Postać nieelektroniczna (postać papierowa, inna)

Interesanci mogą dostarczać dokumenty w postaci papierowej lub elektronicznej (wybór należy do interesanta) – konwersja dokumentu z postaci papierowej do elektronicznej należy do kancelarii.




*Postać nieelektroniczna*

#### 5.2.2.1. Arkusz nieznormalizowany

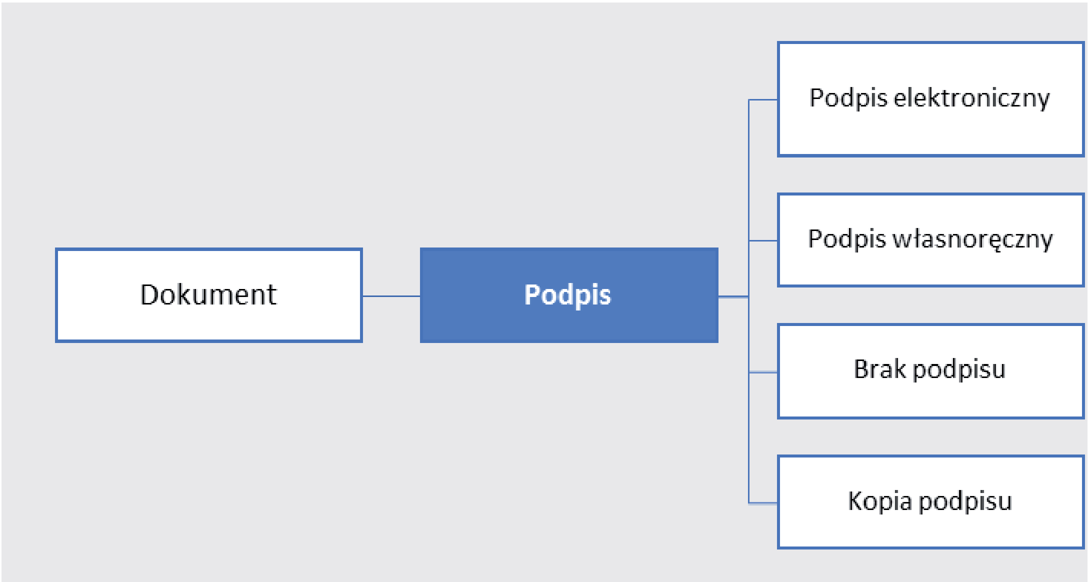
Dokumenty (mapy, rysunki, plany, plakaty) dostarczone w formatach nietypowych, niedających się wprowadzić do EZD, przekazuje się właściwym w sprawie pracownikom, natomiast w kancelarii w EZD wprowadza się jedynie informację o miejscu przekazania dokumentu.

#### 5.2.2.2. Arkusz znormalizowany

Przesyłane dokumenty z reguły tworzone są w formacie A4 (znacznie rzadziej A5 lub A3) i konwersja tych dokumentów do postaci elektronicznej w celu wprowadzenia do EZD nie stwarza trudności. W podmiocie, w którym stosowany jest system EZD, przedłożony dokument papierowy powinien zostać cyfrowo odwzorowany (zeskanowany), a jego treść wprowadzona do EZD, natomiast sam dokument papierowy powinien być umieszczony w składzie chronologicznym.

## 5.3 Podpis

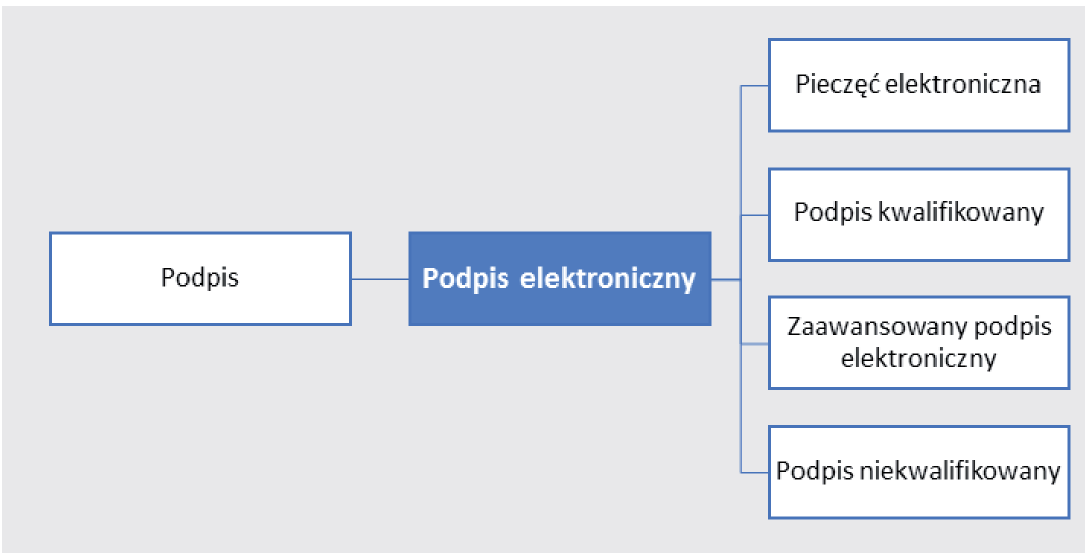
**Podpis** - najogólniej rozumiany znak, ciąg znaków lub zestaw danych, wytworzony przez osobę, do której niezaprzeczalnej identyfikacji służy. W zależności od kontekstu spełniać może rolę potwierdzenia wyrażenia woli, potwierdzenia zapoznania się z treścią, z którą jest związany, lub zapewnienia integralności dokumentu. Fakt istnienia podpisów w różnych formach, postaciach i formatach jest stałym źródłem problemów interpretacyjnych, szczególnie przy stosowaniu kryteriów odnoszących się do podpisu własnoręcznego w stosunku do podpisu elektronicznego - i odwrotnie.




*Podpis*

### 5.3.1. Podpis elektroniczny

**Podpis elektroniczny** - dane w postaci elektronicznej, które wraz z innymi danymi, do których zostały dołączone lub z którymi są logicznie powiązane, służą do identyfikacji osoby składającej podpis elektroniczny; (Dz.U.2013.262)




*Podpis elektroniczny*

Podpis elektroniczny – zgodnie z jego ustawową definicją, służy do **identyfikacji składającej go osoby.** Powszechnym błędem jest kojarzenie owego faktu **identyfikacji** osoby z prawną czynnością wyrażenia woli przez tę osobę.


Podpis elektroniczny może bowiem spełniać kilka funkcji, w tym właśnie potwierdzać wyrażenie woli przez składającą go osobę fizyczną, ale wynikać to musi z kontekstu i charakteru działania , w którym podpis był użyty Funkcją bezwarunkową podpisu elektronicznego jest jednak zapewnienie integralności podpisywanych danych. Z podpisu (ściślej, z wystawionego przez tzw zaufaną stronę trzecią certyfikatu towarzyszącego podpisowi) jednoznacznie wynika, kto złożył podpis. Natomiast z treści podpisywanych danych wynika cel złożenia podpisu. Charakter podpisywanych danych (zdjęcie, obraz, oprogramowanie, zbiór plików w archiwum .zip – wszystko to w postaci elektronicznej jest pewnym zbiorem danych binarnych, skończoną sekwencją zer i jedynek) stanowił będzie o tym czy mamy do czynienia z czynnością techniczną zapewnienia integralności i wskazania osoby lub podmiotu (zamiast podpisu elektronicznego zastosowana będzie pieczęć elektroniczna), która tego zapewnienia integracji dokonała, czy w wyrażeniem woli.

### 5.3.1.1. Pieczęć elektroniczna

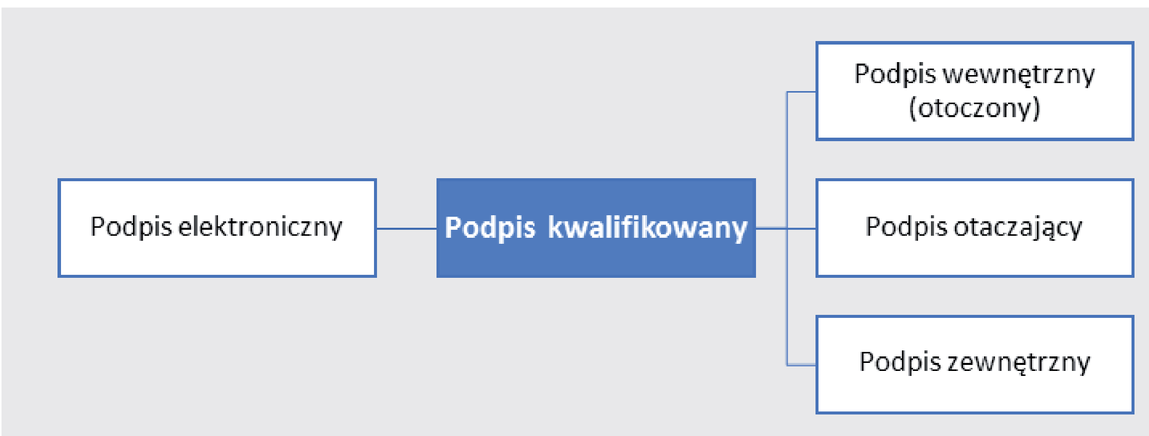
**Pieczęć elektroniczna** - dane w postaci elektronicznej dodane do innych danych w postaci elektronicznej lub logicznie z nimi powiązane, aby zapewnić autentyczność pochodzenia oraz integralność powiązanych danych;

Pieczęć elektroniczna – w sensie technicznym – w 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.


Jeśli np. interesant przekaże podmiotowi publicznemu dokument w trybie przedłożenia, dokument ten wpływając do elektronicznej skrzynki podawczej spowoduje wygenerowanie nowego dokumentu – UPP – który jest podpisany elektronicznie przez system, a nie przez pracownika danego podmiotu.; pieczęć tworzona jest bezwarunkowo, nie wyraża woli. Podobnie jest z profilem zaufanym ePUAP, który wykorzystuje certyfikat systemowy do podpisu danych identyfikujących osobę fizyczną składającą podpis.

#### 5.3.1.2. Podpis kwalifikowany

**Kwalifikowany podpis elektroniczny** - zaawansowany podpis elektroniczny, który jest składany za pomocą kwalifikowanego urządzenia do składania podpisu elektronicznego i który opiera się na kwalifikowanym certyfikacie podpisu elektronicznego;

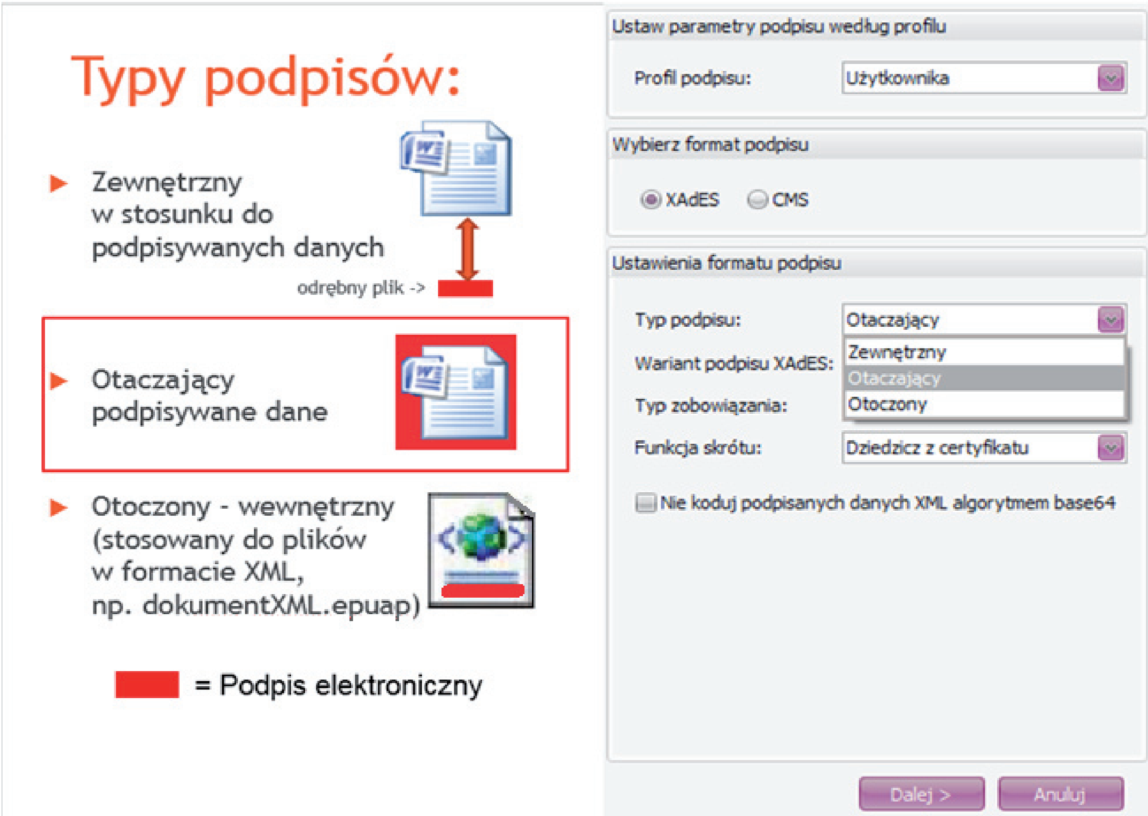



*Podpis kwalifikowany*

„Podpis kwalifikowany" to powszechnie – jako skrót – używana nazwa bezpiecznego **podpisu elektronicznego** weryfikowanego za pomocą ważnego **kwalifikowanego certyfikatu**.

Z uwagi na bezpieczeństwo obrotu prawnego dokumenty przedkładane usługodawcy przez usługobiorcę za pośrednictwem **środków komunikacji elektronicznej** muszą być zabezpieczone przed niekontrolowaną modyfikacją, a więc muszą być elektronicznie podpisane. Stosuje się w tym celu **podpisy elektroniczne**.

Podpis elektroniczny, którym podpisywana jest treść (zawartość informacyjna) dokumentu, może być podpisem wewnętrznym (otoczonym), otaczającym, lub zewnętrznym. Poniżej schematycznie pokazano wspomniane typy podpisów: Ulokowanie danych stanowiących podpis w stosunku do treści dokumentu pokazano schematycznie za pomocą czerwonego koloru.




*Elektroniczny podpis zewnętrzny, podpis otaczający oraz podpis wewnętrzny.*

Używane legalnie formaty danych tworzących dokumenty różnego rodzaju (tekstowe, tekstowo-graficzne i inne) podane są w Załączniku Nr 2 do rozpKRI. Właściwie dobrany format ma znaczenie nie tylko dla mniejszej lub większej wygody tworzenia dokumentu, ale także dla wyboru typu podpisu elektronicznego, jakim wytworzony dokument zostanie opatrzony, nie wszystkie bowiem typy podpisów mogą być użyte w każdej sytuacji.

Np. podpisem **zewnętrznym** podpisać można każdy plik (np. z rozszerzeniem doc, pdf, jpg, avi itd.).

Aplikacje dostarczane przez **podmioty świadczące usługi certyfikacyjne** pozwalają na wybór typu podpisu, jak to pokazano przykładowo na rys. 29 powyżej. W czasie składania elektronicznego podpisu zewnętrznego powstaje odrębny plik o nazwie zgodnej z nazwą pliku podpisywanego, ale o rozszerzeniu wskazującym na rodzaj podpisywanego pliku - np. .xades. Już to rozszerzenie wskazuje, że mamy do czynienia z podpisem elektronicznym. Jeśli np. widzimy plik o nazwie pismo.docx.xades, to wiemy, że plik pismo.docx, wykonany w MS Word, został podpisany podpisem elektronicznym – albo zewnętrznym, albo otaczającym. Na to, którym z nich został podpisany, wskazuje wielkość pliku – kliknięcie prawym przyciskiem myszy na nazwie pliku we „właściwościach" pokazuje jego wielkość (rozmiar) w kilo- czy megabajtach. Jeśli jest to kilka kilobajtów, to mamy do czynienia z podpisem **zewnętrznym** – i musi mu towarzyszyć plik, który został podpisany Podpis **otaczający** daje plik, którego wielkość (rozmiar) jest zawsze siłą rzeczy większy od pliku podpisywanego, ponieważ plik podpisany **zawiera w sobie** podpisywany plik. Podpis **wewnętrzny** (otoczony) można stosować jedynie w odniesieniu do plików, które posiadają budowę strukturalną umożliwiającą osadzanie w nich podpisu. Taką właśnie strukturę posiadają pliki w formacie XML. Nic nie stoi na przeszkodzie, by wewnątrz jednego pliku w formacie XML znajdowały się pliki o innych formatach – pod warunkiem, że będą to formaty opisane w załączniku Nr 2 do rozpKRI. Z tego powodu dokumenty XML doskonale nadają się jako kontenery do osadzania w nich innych plików – i podpisywania **jednym podpisem wewnętrznym w stosunku do kontenera głównego** wszystkich innych plików zawartych w wewnętrznych kontenerach.

##### 5.3.1.2.1. Podpis wewnętrzny (otoczony)

| |
|---|
| **Podpis wewnętrzny** - podpis elektroniczny otoczony przez podpisywane dane; |

Ten typ podpisu stosuje się w plikach mających strukturę (format XML) umożliwiającą osadzenie danych tworzących podpis w kontenerze (bloku) zawierającym dane tworzące dokument. Podpis zabezpiecza jednak owe dane – i gdyby którykolwiek ze znaków w dowolnym kontenerze został zmieniony, podpis będzie zweryfikowany negatywnie. Gdyby usunąć kontener zawierający podpis z kontenera dokumentu głównego, będzie on identyczny jak dokument przed podpisem. Poniżej pokazano przykład prostego pliku w formacie xml, który może być wczytany do MS Worda i zwizualizowany Plik ten został utworzony „ręcznie" w notatniku jako plik xml, a później został podpisany podpisem kwalifikowanym (stąd rozszerzenie xades). Następnie cały kontener (blok) 'Signature' zawierający podpis usunięto, zaznaczając komentarzem miejsce, w którym podpis się znajdował. Widoczne jest, że kontener podpisu utworzony w czasie podpisywania ulokowany był w kontenerze głównym o nazwie 'wordDocument'

```xml
<?xml version="1.0" encoding="utf-8" standalone="no"?><?mso-application progid="Word.Document"?>
<w:wordDocument xmlns:w="http://schemas.microsoft.com/office/word/2003/wordml">
   <w:styles>
    <w:style w:default="on" w:type="paragraph">
      <w:rPr>
        <w:sz w:val="48"/>
      </w:rPr>
    </w:style>
  </w:styles>
    <w:docPr>
      <w:view w:val="print"/>
    </w:docPr>
  <w:body>
    <w:p>
      <w:r>
        <w:t>Tekst napisany czcionką Times New Roman o wysokości 24 punktów.</w:t>
      </w:r>
    </w:p>
  </w:body>
  <!--**** w tym miejscu znajdowały się dane podpisu elektronicznego, zawierające kontener
  'Signature' z danymi podpisu elektronicznego. Z uwagi na wielkość (ok. 5 kB) dane te zostały
  usunięte, gdyż chodziło jedynie o pokazanie lokalizacji bloku z podpisem w stosunku do danych
  dokumentu zawartych w bloku głównym o nazwie wordDocument. ****-->
</w:wordDocument>
```

*Przykład pliku w formacie xml podpisanego podpisem otoczonym*

#### 5.3.1.2.2. Podpis otaczający

**Podpis otaczający** - podpis elektroniczny otaczający podpisywane dane;

```xml
<?xml version="1.0" encoding="utf-8"?>
<!-- **** Tu zaczynają się dane podpisu elektronicznego - z uwagi na wielkość
pokazano tylko znacznik otwierający 'Signature' -->
<ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#" Id=
"Signature-760294158"><ds:Object Id="Dokument-3216410762">
<!-- **** tu rozpoczynają się dane dokumentu niezakodowanego **** -->
<w:wordDocument xmlns:w="http://schemas.microsoft.com/office/word/2003/wordml">
<w:p><w:r><w:t>Tekst napisany czcionką Times New Roman o wysokości 10 punktów.
</w:t></w:r></w:p></w:wordDocument>
<!-- tu kończą się dane dokumentu niezakodowanego **** -->
</ds:Object></ds:Signature>
```

*Przykład pliku w formacie xml podpisanego podpisem otaczającym*

Ten typ podpisu stosuje się w odniesieniu do dowolnych plików – bez względu na ich strukturę i format. Plik osadzony jest wewnątrz danych podpisu (w kontenerze ‘Signature’). Pliki takie przed osadzeniem w kontenerze podpisu kodowane są domyślnie kodem **base64**, chociaż kodowane być nie muszą – jest to opcja, którą można włączać lub wyłączać.

Jak widać na rys. 35 w przypadku **podpisu otaczającego** dokumenty podpisywane osadzane są wewnątrz głównego kontenera o nazwie ‘Signature’ Podpis zabezpiecza dane – i gdyby którykolwiek ze znaków w dowolnym kontenerze został zmieniony, podpis będzie zweryfikowany negatywnie.

#### 5.3.1.2.3. Podpis zewnętrzny

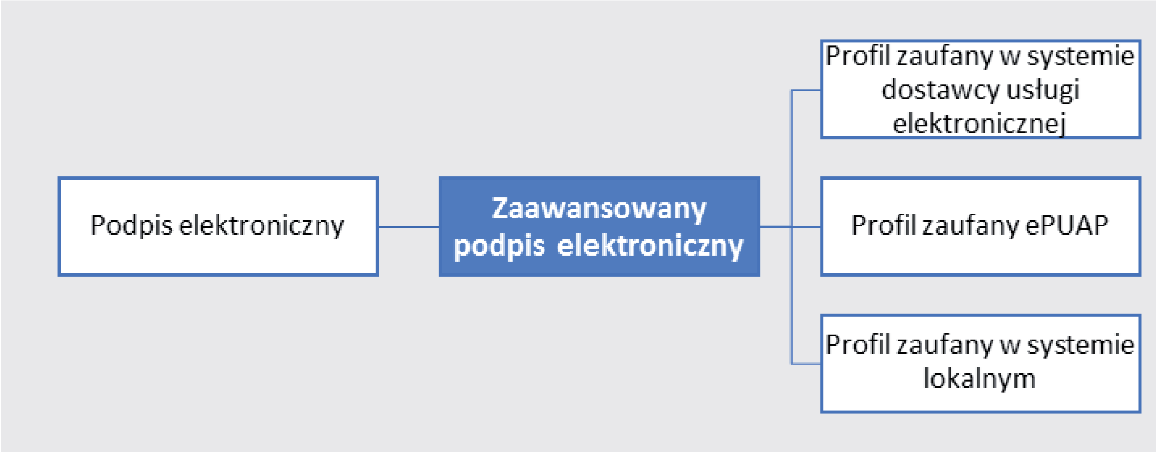
**Podpis zewnętrzny** - podpis elektroniczny stanowiący zewnętrzny w stosunku do podpisywanych danych, odrębny plik;


Podpisem zewnętrznym podpisywać można dowolne pliki (o dowolnym formacie) i wielkości. Plik podpisu generowany jest jako odrębny plik. Przekazuje się go odbiorcy razem z plikiem podpisywanym – i przy pomocy weryfikatora

### 5.3.1.3. Zaawansowany podpis elektroniczny

**Podpis zaawansowany** - podpis elektroniczny, który spełnia następujące wymagania:

1. jest jednoznacznie powiązany z osobą składającą podpis elektroniczny,
2. pozwala na identyfikację osoby składającej podpis elektroniczny,
3. jest tworzony z wykorzystaniem zasobów, które osoba składająca podpis elektroniczny może utrzymywać pod swoją wyłączną kontrolą,
4. jest powiązany z danymi, do których się odnosi w taki sposób, że każda jakakolwiek późniejsza zmiana tych danych jest rozpoznawalna.

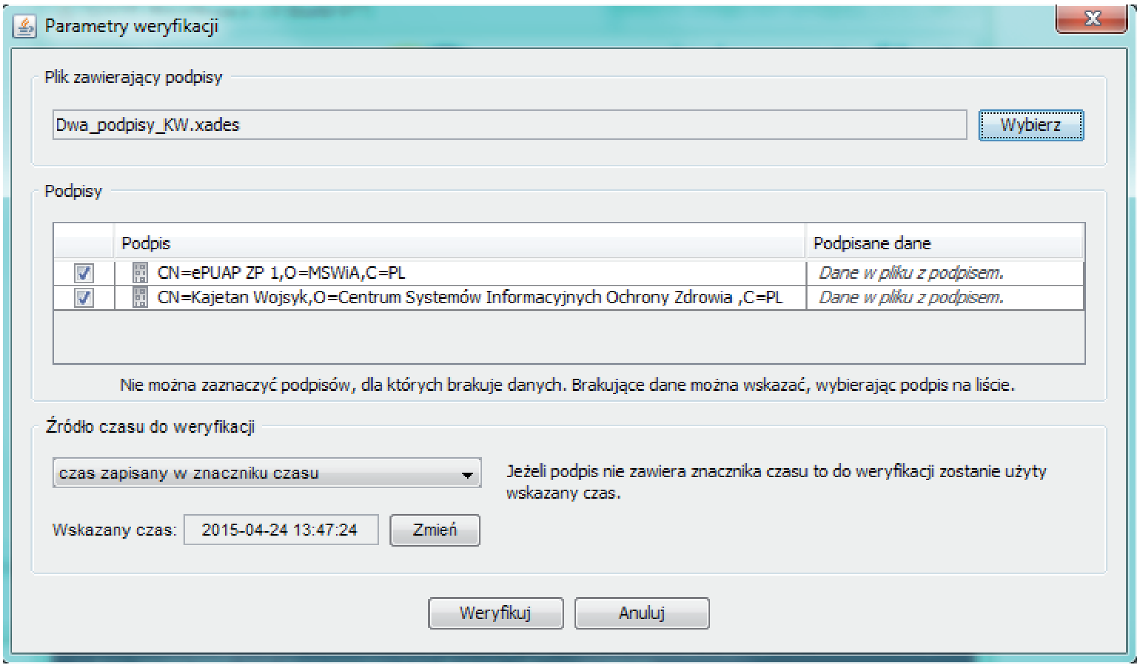



*Zaawansowany podpis elektroniczny*

Zaawansowany podpis elektroniczny jest podpisem o poziomie bezpieczeństwa wystarczającym w relacjach usługobiorca – usługodawca. Wymagania odnoszące się do tego podpisu z jednej strony pozwalają na jednoznaczną identyfikację osoby opatrującej podpisem przesyłany dokument, z drugiej - nie są kłopotliwe w praktycznym stosowaniu ani po stronie podpisującego, ani po stronie weryfikującego. Najczęściej dostawcą usługi certyfikacji jest z zasady usługodawca, czyli podmiot określający (akceptujący) taki poziom bezpieczeństwa jako wystarczający lub zaufana strona trzecia. Przykładami podpisów zaawansowanych mogą być podpisy tworzone z wykorzystaniem certyfikatów wystawianych przez regionalne lub krajowe centra certyfikacji (np. Śląskie Centrum Społeczeństwa Informacyjnego, Centrum Projektów Informatycznych MAiC). Do składania zaawansowanego podpisu elektronicznego może być używany certyfikat przechowywany na kartach kryptograficznych, może być też stosowany system jednorazowych kodów przesyłanych przez system na numer telefonu komórkowego właściciela podpisu. W tym drugim przypadku dane osoby składającej podpis potwierdzane są certyfikatem systemowym. W przypadku ePUAP jest to certyfikat wystawiony przez **kwalifikowane centrum certyfikacji**.

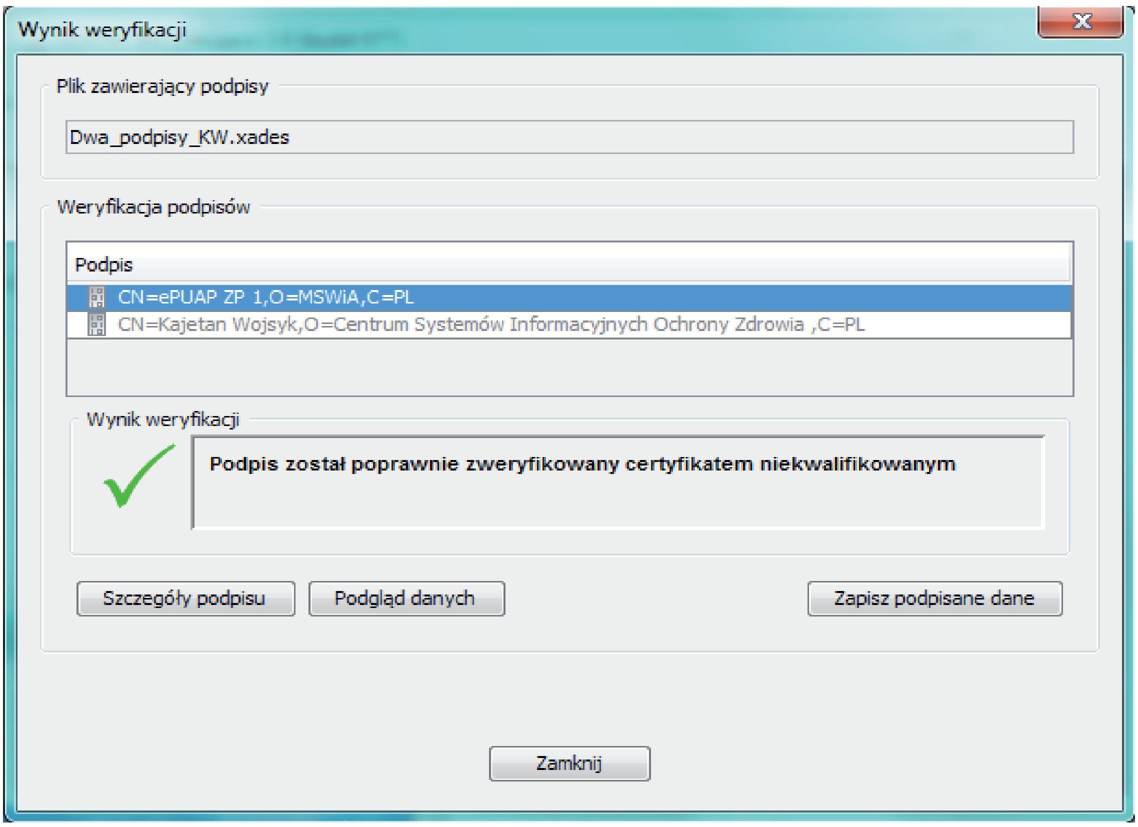
Na rysunku *Przykład weryfikacji dwóch różnych podpisów* pokazano przykład weryfikacji dwóch podpisów, którymi opatrzony został dokument xml Weryfikator pokazuje istnienie dwóch podpisów (widoczne w kolejnych wierszach) Wynik weryfikacji pozwala jednoznacznie ustalić kto (imię, nazwisko, PESEL) i kiedy (data i czas podpisu z dokładnością do jednej sekundy) podpisał dokument. Jeśli plik podpisany jest przez więcej niż jedną osobę, lub kilkukrotnie przez tę samą osobę, każdy z podpisów daje się odrębnie zweryfikować Ponadto w certyfikatach widoczne są daty skrajne (data rozpoczęcia ważności certyfikatu i data upływu jego ważności) oraz rodzaje tych certyfikatów

Innymi słowy, dokumenty elektronicznie podpisane są silne dowodowo, ponieważ pozwalają jednoznacznie, bez jakichkolwiek nakładów ustalić istotne fakty dotyczące czasu podpisania dokumentu oraz osoby, która podpis złożyła, oraz sprawdzić, czy dokument od chwili podpisania nie był modyfikowany

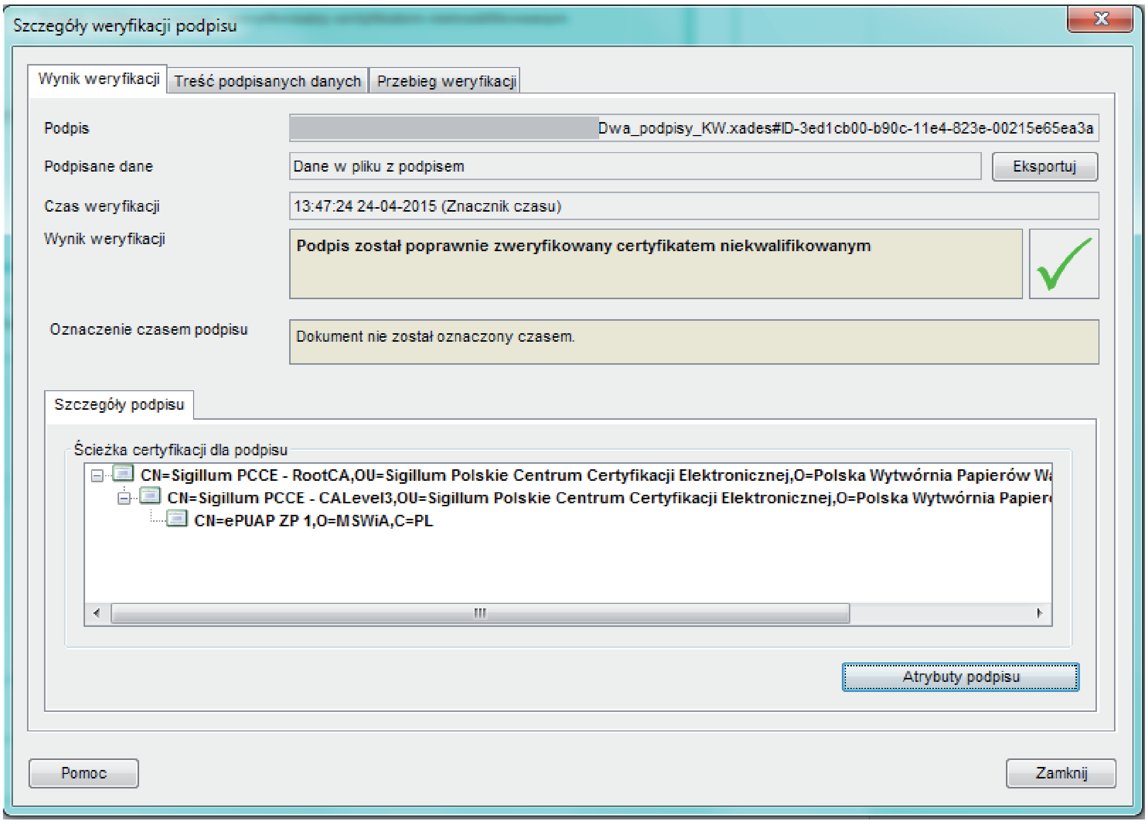



*Przykład weryfikacji dwóch różnych podpisów którym został podpisany dokument xml.*

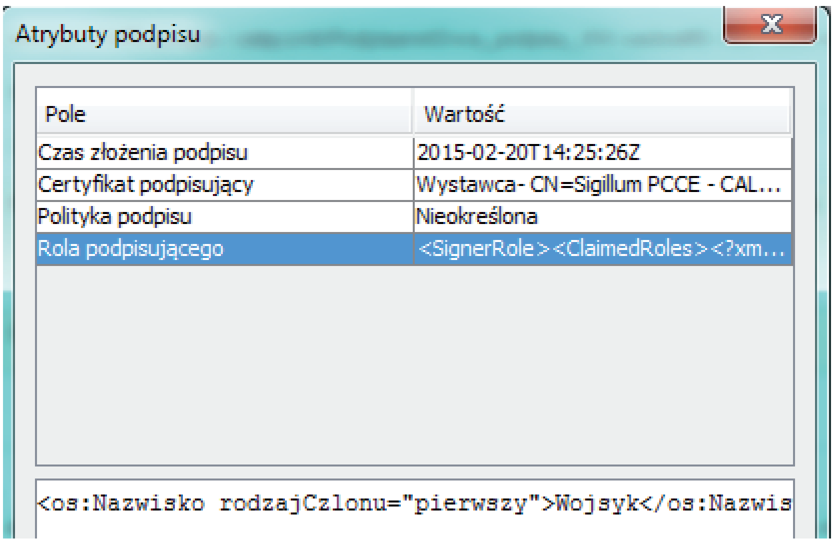
Naciśnięcie klawisza „weryfikuj" umożliwia dokonania weryfikacji wybranego podpisu (w przypadku wybrania kilku podpisów będą one weryfikowane kolejno).




*Przykład weryfikacji podpisu potwierdzonego profilem zaufanym ePUAP.*




*Szczegóły weryfikacji podpisu potwierdzonego profilem zaufanym ePUAP*




*Przykład podpisu potwierdzonego profilem zaufanym ePUAP, weryfikowanego za pomocą weryfikatora Szafir (Krajowa Izba Rozliczeniowa).*

W polu „Rola podpisującego” odczytać można dane osoby składającej podpis – imię, nazwisko oraz PESEL.

W polu „Czas złożenia podpisu” – widoczna jest data i czas złożenia podpisu z dokładnością do jednej sekundy

Podpisywanie dokumentu przez kilka osób w tym samym podmiocie posiadającym konto na ePUAP jest wyjątkowo proste; wystarczy, że każda z nich zaloguje się w kontekście tego podmiotu i podpisze ów dokument. Wszystkie podpisy będą widoczne równocześnie, weryfikować należy je oddzielnie.

#### 5.3.1.3.1. Profil zaufany w systemie dostawcy usługi elektronicznej

Podmiot świadczący usługi elektroniczne może sam wystawiać certyfikaty niekwalifikowane dla odbiorców swoich usług, lub zastosować inne, wiarygodne dla siebie i prawnie wystarczające środki identyfikacji. W szczególności może być to wydawanie loginu i jednorazowego hasła do zmiany hasła osobom zweryfikowanym przez uprawnionego do tego swojego pracownika. Takiej procedurze towarzyszyć winno sporządzenie umowy regulującej prawa i obowiązki stron, w tym szczególnie zasady używania danych autoryzujących i skutki prawne ich użycia.

#### 5.3.1.3.2. Profil zaufany ePUAP

**Profil zaufany ePUAP** - zestaw informacji identyfikujących i opisujących podmiot lub osobę będącą użytkownikiem konta na ePUAP, który został w wiarygodny sposób potwierdzony przez organ podmiotu określonego w art. 2 ustawy o informatyzacji działalności podmiotów realizujących zadania publiczne; (Dz.U.2014.1114 j.t.)


Profil zaufany ePUAP jest alternatywą certyfikatu kwalifikowanego w relacjach osób fizycznych (usługobiorców), a także przedsiębiorców z administracją publiczną. Także pracownicy administracji we wzajemnych relacjach mogą stosować profil zaufany ePUAP do wiarygodnego podpisywania przekazywanych dokumentów (Dz.U 2014.1114 j.t.). Konstrukcja ta wynika bezpośrednio z kilku uwarunkowań:

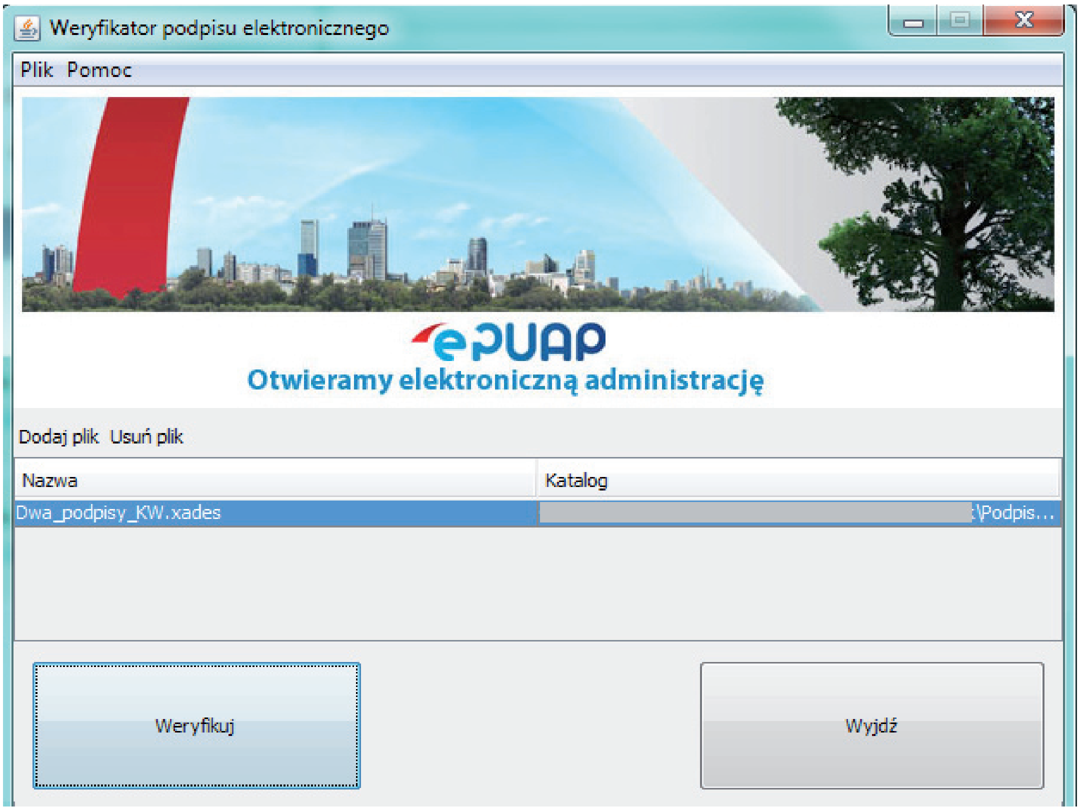
a) Potwierdzenie tożsamości osoby uzyskującej potwierdzenie danych w swoim profilu odbywa się w **punkcie potwierdzającym** (PP) , którego uprawniony pracownik spełnia w istocie funkcję inspektora ds. certyfikacji. Pracownik PP w oparciu o okazany i zweryfikowany dowód tożsamości (sprawdza autentyczność dowodu i porównuje zdjęcie w dowodzie z twarzą osoby okazującej dowód osobisty lub paszport) – za pomocą mechanizmów udostępnionych PP dokonuje potwierdzenia tożsamości – zgodności danych we wniosku z danymi w dowodzie osobistym (imię, nazwisko, PESEL).

b) Weryfikowane (potwierdzane) dane pracownik PP podpisuje własnym profilem zaufanym lub bezpiecznym podpisem elektronicznym weryfikowanym ważnym kwalifikowanym – co do skutków technicznych i prawnych jest to działanie identyczne.

c) Wszelkie działania (założenie profilu, złożenie wniosku, potwierdzenie tego profilu) odbywają się w ramach systemu ePUAP – a więc w bezpiecznym środowisku administrowanym przez ministra właściwego ds. informatyzacji.

d) Mechanizmy podpisywania elektronicznego działają dokładnie tak samo jak w przypadku podpisywania podpisem kwalifikowanym – i z tego powodu skutki złożenia dokumentu podpisanego podpisem potwierdzonym profilem zaufanym są zrównane w skutkach prawnych ze skutkami złożenia dokumentu papierowego podpisanego własnoręcznie (Dz.U 2014.1114 j.t.).

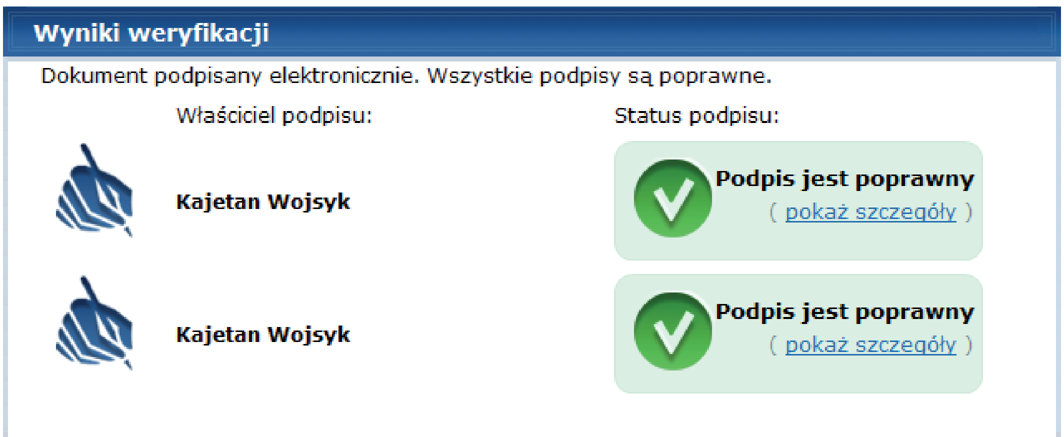
Na rysunku *Weryfikator podpisu elektronicznego…* pokazano przykład weryfikatora podpisów zaimplementowanego na platformie ePUAP




*Weryfikator podpisu elektronicznego z wczytanym plikiem podpisanym dwoma podpisami – kwalifikowanym i profilem zaufanym ePUAP – przed weryfikacją*

Weryfikator ten w pewnych sytuacjach może być użyty także poza ePUAP do weryfikacji elektronicznie podpisanych plików wyeksportowanych (pobranych na dysk) z ePUAP

Rysunek *Wynik weryfikacji pliku Dwa_podpisy_KW.xades* przedstawia wynik weryfikacji podpisów pliku wczytanego do weryfikatora zaimplementowanego na platformie ePUAP




*Wynik weryfikacji pliku Dwa_podpisy_KW.xades*

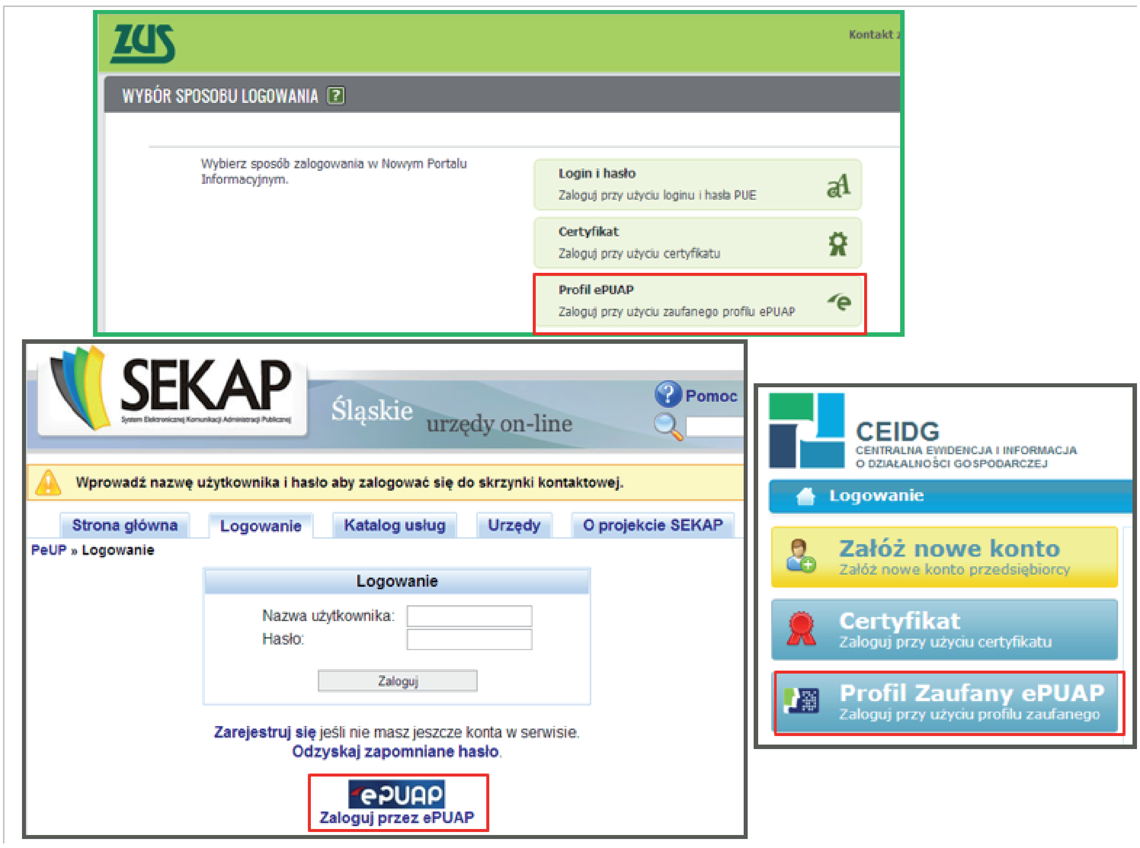
Usługobiorca (wnioskodawca) może więc przedkładać **dokumenty elektroniczne** podpisane podpisem potwierdzonym profilem zaufanym ePUAP usługodawcy (podmiotowi publicznemu) i muszą być one traktowane identycznie, jak **dokumenty papierowe podpisane własnoręcznie** (przedłożone w formie pisemnej).

Wyniki weryfikacji obu podpisów wskazują, że są potwierdzone certyfikatami wystawionymi przez kwalifikowane centrum certyfikacji i oprócz danych identyfikacyjnych samego podpisu (numer seryjny), uwidaczniają imię, nazwisko, PESEL osoby podpisującej oraz czas złożenia podpisu). Dokumenty podpisane podpisem potwierdzonym profilem zaufanym ePUAP mogą być składane do wszystkich podmiotów realizujących zadania publiczne, o których mowa w ustawie o informatyzacji.

Aktualnie, po powszechnym udostępnieniu możliwości korzystania z profilu zaufanego ePUAP administracja publiczna nie może żądać od usługobiorców będących osobami fizycznymi podpisywania dokumentów podpisem kwalifikowanym w przypadku przedkładania dokumentów elektronicznych, gdyż byłoby to nie tylko naruszeniem równości praw obywateli (odebraniem możliwości korzystania z e-usług wszystkim obywatelom na równych prawach, wygoda i oszczędność czasu tylko dla tych, którzy zakupią usługę certyfikacyjną w podmiocie świadczącym te usługi), ale zaprzeczeniem idei e-administracji. Administracja publiczna utrzymywana jest z pieniędzy wszystkich podatników, a więc także tych, którzy rzadko korzystają bezpośrednio z jej usług; kupowanie przez nich certyfikatów kwalifikowanych byłoby nieracjonalne. Każdy ma prawo skorzystać z możliwości, jakie daje ePUAP i możliwość korzystania z profilu zaufanego na tej platformie – a dokumenty złożone za jej pośrednictwem są nie mniej wiarygodne, niż dokumenty podpisane podpisem kwalifikowanym. Samo złożenie podpisu wymaga nie tylko zalogowania się do systemu, ale także użycia jednorazowego kodu, przesłanego na adres poczty elektronicznej (rozwiązanie mniej bezpieczne, które powinno być wycofane z użycia) lub kodem przesyłanym SMS-em – i ten sposób jest bezpieczny, ponieważ osoba składająca podpis w tym samym, krótkim, kilkusekundowym czasie ma przed sobą podpisywany dokument oraz okienko do wpisania kodu, a własny telefon przy sobie. Jest to więc podpis bezpieczny

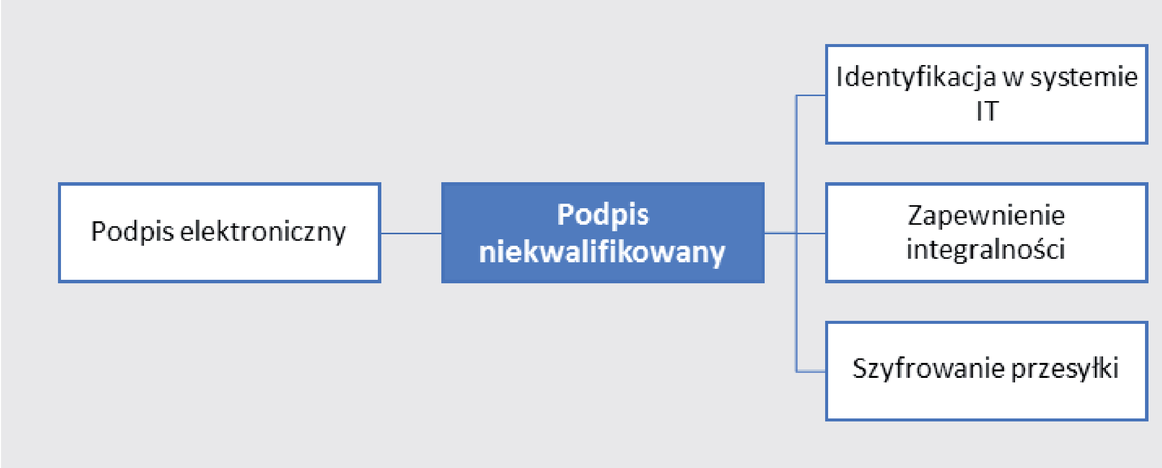
### 5.3.1.3.3. Profil zauf4any w systemie lokalnym

Lokalnym profilem zaufanym możemy określić profil usługobiorcy utworzony w lokalnym systemie teleinformatycznym – należącym do konkretnego podmiotu – bez względu na jego zasięg terytorialny Zaufanie opiera się na bezwzględnie konsekwentnie realizowanej procedurze potwierdzenia tożsamości usługobiorcy w tym systemie – dokładnie tak samo jak dzieje się to w przypadku potwierdzania tożsamości osoby fizycznej przy wystawianiu certyfikatu kwalifikowanego lub potwierdzaniu profilu zaufanego ePUAP Lokalnym profilem zaufanym może być profil założony użytkownikowi w zakładowym systemie elektronicznego zarządzania dokumentami, czy jakimkolwiek innym systemie, wymagającym podania danych identyfikacyjnych, które potwierdza administrator danych lub osoba przez niego upoważniona. Możliwe jest samopotwierdzenie danych w przypadku posiadania wcześniejszego – i ważnego innego certyfikatu, uzyskanego zgodnie z procedurą wymagającą osobistego stawienia się przed inspektorem ds. certyfikacji. Np. osoba fizyczna posiadająca certyfikat kwalifikowany lub profil zaufany ePUAP może za jego pomocą udowodnić swoją tożsamość w innych systemach, jeżeli taka możliwość została w nich przewidziana.




*Możliwość wykorzystywania profilu zaufanego ePUAP do potwierdzania swojej tożsamości w innych systemach dedykowanych*

### 5.3.1.4. Podpis niekwalifikowany




*Podpis niekwalifikowany*

Podpis niekwalifikowany jest ostatnim ze środków, który może być stosowany do wiarygodnego podpisywania dokumentów czy korzystania z systemów udostępnionych przez usługodawcę. To, jaki certyfikat zostanie wykorzystany w procesie komunikacji zależy jedynie od umowy dwóch stron tej komunikacji. Jeśli zatem np. usługodawca utworzy własne niekwalifikowane centrum certyfikacji, którego certyfikaty będą dla niego wiarygodne (a najbardziej wiarygodne są dla niego własne certyfikaty, gdyż sam je wystawia i samemu sobie najbardziej ufa) i będzie swoim usługobiorcom wystawiał te certyfikaty (nadal z bezwzględnym zachowaniem procedury podpisania stosownej umowy o korzystaniu z certyfikatu i fizycznym sprawdzeniu tożsamości usługobiorcy), to certyfikaty te mogą służyć do podpisywania dokumentów


Przykładem mogą być certyfikaty banków – każdy bank wystawia swoim klientom własne certyfikaty – i tylko takimi można posługiwać się w jego systemach. Podobne certyfikaty mogą być wystawiane przez regionalne centra certyfikacji prowadzone przez marszałków czy szkoły wyższe oraz dowolne inne podmioty, świadczące usługi dla pewnej ograniczonej stosunkowo grupy użytkowników

### 5.3.1.4.1. Identyfikacja w systemie IT

Podpis elektroniczny weryfikowany certyfikatem niekwalifikowanym może być autoryzacji urządzeń sieciowych oraz zestawiania bezpiecznych połączeń, np. SSL, VPN, IPSEC. W certyfikacie znajdują się dane identyfikujące osobę właściciela certyfikatu (imię, nazwisko, adres poczty elektronicznej, dane podmiotu wystawiającego certyfikat i data upływu jego ważności a także – opcjonalnie – dane podmiotu reprezentowanego przez właściciela certyfikatu. W certyfikacie znajduje się także klucz publiczny

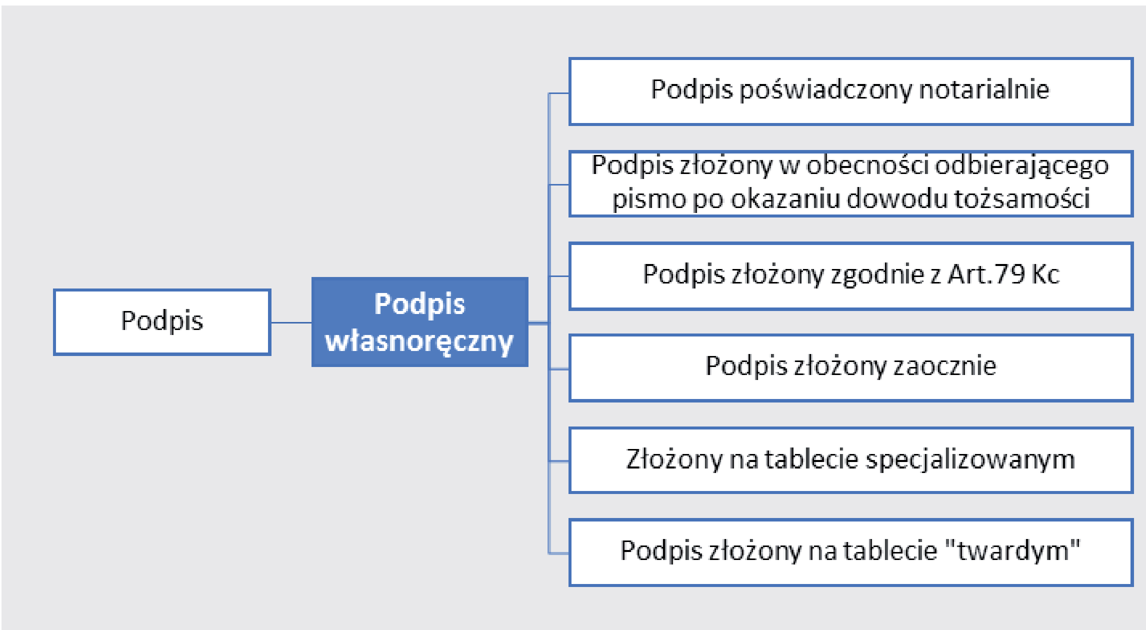

### 5.3.1.4.2. Zapewnienie integralności

Podpis elektroniczny składany z wykorzystaniem certyfikatu kwalifikowanego również stosowany jest do zapewnienia integralności przesyłki, tj. umożliwienia jej odbiorcy stwierdzenia kto jest nadawcą – i czy przesyłka w drodze od nadawcy do odbiorcy nie uległa zmianie.

#### 5.3.1.4.3. Szyfrowanie przesyłki

Certyfikat niekwalifikowany może być stosowany do szyfrowania przesyłanych informacji. Służy do tego klucz publiczny przyporządkowany do klucza prywatnego znajdującego się wyłącznie w posiadaniu użytkownika.


### 5.3.2. Podpis własnoręczny




*Podpis własnoręczny*

Forma pisemna to czynność prawna polegająca na zamieszczeniu przez osobę dokonującą tej czynności własnoręcznego podpisu pod treścią zawierającą oświadczenie woli tejże osoby Co istotne ze względów praktycznych - nie jest konieczne sporządzanie własnoręcznym pismem całego dokumentu; może być on napisany na maszynie do pisania, wydrukowany na drukarce komputerowej – ważny jest tu jedynie fakt złożenia własnoręcznie podpisu – a to oznacza, że mamy najczęściej do czynienia z nośnikiem z papierowym, na którym ma pojawić się własnoręczny podpis… Dochodzimy tutaj do istoty rzeczy, do celowości przepisu: dlaczego podpis własnoręczny, niekiedy nieczytelny , ale jednak własnoręczny? Chodzi o zapewnienie względnie mocnego dowodu, że osoba podpisująca oświadczenie woli rzeczywiście to zrobiła. Składanie podpisu nie jest czynnością techniczną, lecz prawną, a w tym przypadku także jest pozostawieniem swoistych, właściwych tylko podpisującemu cech biometrycznych na dokumencie. Nie chodzi wyłącznie o kształt linii czy zestawu znaków tworzących podpis, ale o inne, mniej uchwytne elementy – dynamikę składania podpisu, jego cechy charakterystyczne, utrwalające się latami. Właśnie te cechy są istotne dla ewentualnego późniejszego postępowania dowodowego. Nie trzeba dodawać, że ów „mocny dowód" dokonania czynności prawnej (własnoręczny podpis pod oświadczeniem woli) zostanie zachowany do celów dowodowych przez stronę przyjmującą owo oświadczenie woli, gdyby oświadczeniodawca chciał się później wycofać – i wypierał się owej czynności. W takiej sytuacji przyjmujący oświadczenie woli może okazać je jako dowód w sądzie.


Biegły pismoznawca poprzez porównywanie okazanego podpisu z próbkami stanowiącymi podpisy osoby zaprzeczającej czynności prawnej dokona specjalistycznej ekspertyzy, którą może kierować się sąd. Dla porządku należy dodać, że istnieje pewien wyjątek, w którym całość pisma – a nie tylko podpis pod jego treścią musi być sporządzony własnoręcznie – testament. W tym przypadku również celowość takiego przepisu jest oczywista: po śmierci trudno byłoby uzyskiwać próbki do porównań, więc w razie wątpliwości taki testament zawierać może dość dużo materiału porównawczego, wiele charakterystycznych cech, które znajdowały się będą w wielu różnych pismach, których autorstwo zmarłego nie budzi wątpliwości.

Zwykła forma pisemna może być ona czynnością jednostronną lub dwu- czy wielostronną. Z taką formą mamy do czynienia np. przy podpisywaniu umów Jeśli strony podpisujące umowę spotykają się przy jednym stole, okazują pełnomocnictwa i dowody tożsamości - wiarygodność dokumentów jest wysoka. Dla zapewnienia, że wszystkie strony podpisują tę samą treść, sygnatariusze składają podpisy na tym samym egzemplarzu. Egzemplarzy powinno być tyle, ilu jest sygnatariuszy, by każdy miał swój oryginalny, podpisany przez pozostałych sygnatariuszy egzemplarz.

Taka technika sporządzania dokumentów jest uciążliwa i kłopotliwa – wymaga spotkania się sygnatariuszy w tym samym czasie i w tym samym miejscu, co już może stanowić – i często stanowi istotną trudność. Stosuje się więc przesyłanie wzajemne dokumentów do chwili, gdy każdy z sygnatariuszy dysponował będzie egzemplarzem z podpisami pozostałych stron. Jednak – w przypadku wielokartkowych, objętościowo dużych dokumentów (kilkanaście- kilkadziesiąt stron) dokonuje się jeszcze parafowania każdej kartki – by zabezpieczyć się przed niekontrolowaną podmianą którejś z kartek. Czynność ta ma zapewnić integralność tekstu, podzielonego na odrębne fragmenty mieszczące się na kolejnych stronach.

Ustawodawca przewidział pewne uproszczenie: do skutecznego zawarcia umowy wystarcza wymiana egzemplarzy podpisanych przez każdą ze stron… Warunkiem jest jednak zapewnienie, że treść wymienianych egzemplarzy będzie kompletna i identyczna. W przypadku dokumentów w postaci elektronicznej stwierdzenie, czy podpisany i zwrócony dokument jest identyczny z wysłanym jest bardzo prosta. Warunkiem jednak jest, by wysyłany dokument był kompletny, tzn. by nie wymagał dopisania lub usunięcia (zmiany) nawet jednego znaku. Treść dokumentu uzgadnia się w trybie roboczym, a następnie jedna strona podpisuje elektronicznie dokument – i drogą elektroniczną przesyła go do podpisu stronie drugiej, która, po podpisaniu dokumentu (i zachowaniu kopii) zwraca go stronie pierwszej.

### 5.3.2.1. Podpis poświadczony notarialnie

Podpis własnoręczny może być poświadczony przez notariusza. Czynność ta dokonywana jest w odniesieniu do podpisów składanych na dokumentach w ważniejszych sprawach, takich jak np. sprzedaż części lub całości przedsiębiorstwa, nieruchomości itp., a także, gdy przepisy prawa przewidują taką formę czynności prawnej dla zachowania jej ważności. Autentyczność podpisu na podpisywanym dokumencie potwierdzana jest przez notariusza jego podpisem, pieczęcią, datą i miejscem sporządzenia, oznaczeniem kancelarii, a także, jeśli klient złoży taki wniosek, godziną i minutą poświadczenia.


Należy wyraźnie podkreślić, że poświadczenie notariusza nie dotyczy treści podpisywanego pisma, lecz wyłącznie samego podpisu, który klient składa w obecności notariusza po okazaniu dowodu tożsamości – dowodu osobistego lub paszportu. Notariusz nie bada prawdziwości treści dokumentu czy jego zgodności z prawem, a jedynie poświadcza fakt, że czynność złożenia własnoręcznego podpisu przez daną osobę pod treścią dokumentu została dokonana w jego obecności.

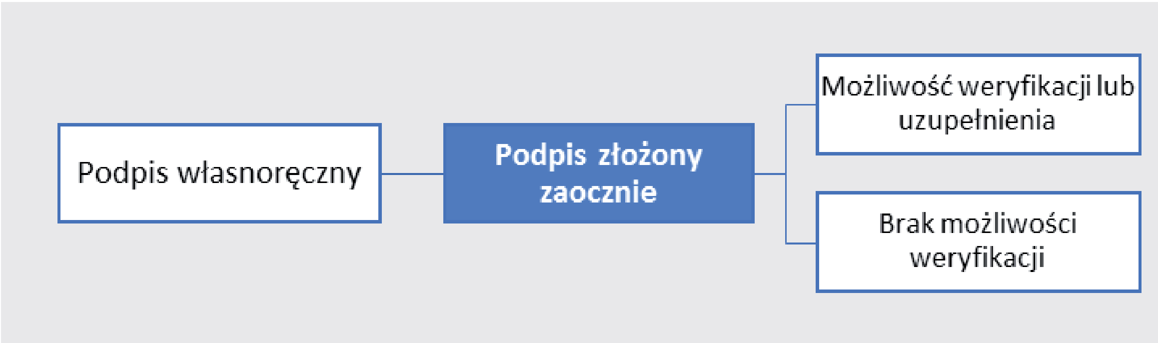
### 5.3.2.2. Podpis złożony w obecności odbierającego pismo po okazaniu dowodu tożsamości

Taki podpis odpowiada formie pisemnej zwykłej – i jest stosowany w administracji w sytuacji osobistego składania przez interesantów dokumentów w urzędach. Pracownik odbierający pismo powinien poprosić o okazanie dowodu tożsamości i złożenie własnoręcznego podpisu w jego obecności – zabezpiecza to przed kłopotliwymi czynnościami badania autentyczności podpisu w przyszłości.

### 5.3.2.3. Podpis złożony zgodnie z Art.79 Kc

Zgodnie z art. 79 ustawy z dnia 23 kwietnia 1964 Kodeks cywilny „Osoba niemogąca pisać, lecz mogąca czytać może złożyć oświadczenie woli w formie pisemnej bądź w ten sposób, że uczyni na dokumencie tuszowy odcisk palca, a obok tego odcisku inna osoba wypisze jej imię i nazwisko umieszczając swój podpis, bądź też w ten sposób, że zamiast składającego oświadczenie podpisze się inna osoba, a jej podpis będzie poświadczony przez notariusza lub wójta (burmistrza, prezydenta miasta), starostę lub marszałka województwa z zaznaczeniem, że został złożony na życzenie niemogącego pisać, lecz mogącego czytać."

### 5.3.2.4. Podpis złożony zaocznie




*Podpis złożony zaocznie.*

Dokumenty podpisane „zaocznie" są wprawdzie dokumentami o mniejszej wiarygodności, jednak pragmatyka i poziom bezpieczeństwa adekwatny do wagi sprawy pozwala przyjmować dokumenty przesłane pocztą. W dokumentach tych znajduje się adres i kontakt do interesanta – więc w przypadku wątpliwości co do autentyczności podpisu można wezwać interesanta do złożenia podpisu w obecności urzędnika.

#### 5.3.2.4.1. Możliwość weryfikacji lub uzupełnienia

W przypadku wątpliwości co do autentyczności podpisu stosowane mogą być inne środki – np. telefon do osoby, której podpis widnieje pod treścią dokumentu z prośbą o potwierdzenie tego faktu.

#### 5.3.2.4.2. Brak możliwości weryfikacji

W przypadku braku możliwości potwierdzenia wiarygodności dokumentu powinien być on traktowany jako obciążony wadą w postaci braku podpisu. Należy jednak ważyć stopień zagrożenia oraz wagę sprawy – kwestionowanie autentyczności każdego podpisu na dokumencie przesłanym pocztą jest zdecydowanie nieuzasadnione, szczególnie, gdy to urząd wysyła pocztą dokumenty do interesanta i uzyskuje je zwrotnie opatrzone podpisem.

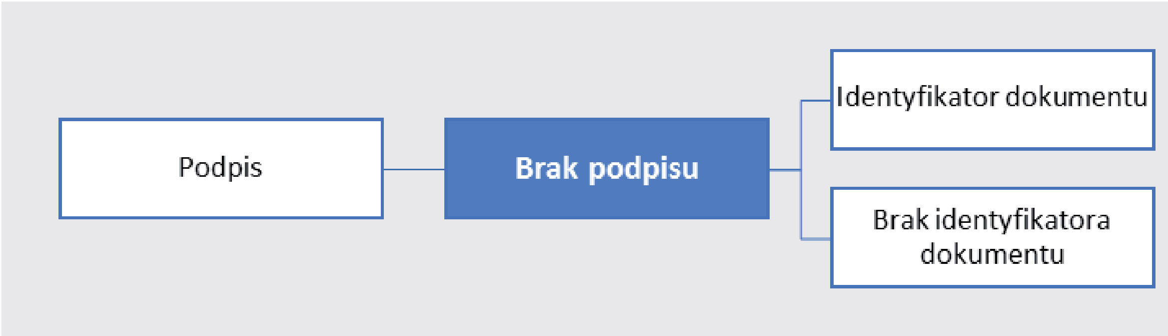
#### 5.3.2.5. Złożony na tablecie specjalizowanym

Podpis pod treścią pisma w postaci elektronicznej składany na tablecie specjalizowanym składa się w obecności osoby odbierającej pismo. Mimo elektronicznych narzędzi jest to podpis własnoręczny, gdyż tego typu tablet zapewnia odwzorowanie dynamiki podpisu, który mógłby być badany przez eksperta – pismoznawcę w razie takiej potrzeby, ale już sama procedura składania zapewnia jego autentyczność.


#### 5.3.2.6. Podpis złożony na tablecie “twardym”

Podpisy własnoręczne tego typu stosowane są w mniej zaawansowanych terminalach wykorzystywanych przez doręczycieli przesyłek pocztowych. Służą one wyłącznie potrzebom udowodnienia faktu doręczenia przesyłki i dla doręczycieli są dowodem wystarczającym.

### 5.3.3. Brak podpisu




*Brak podpisu*

Nie wszystkie dokumenty wymagają podpisu. W szczególności urzędowe pisma tworzone automatycznie w systemach teleinformatycznych w wyniku wcześniej zaprogramowanych procedur, niestanowiące wyrażenia woli, mające charakter informacyjny i oznakowane identyfikatorem pozwalającym na jednoznaczne potwierdzenie autentyczności pisma (np. przez ponowne pobranie). Pisma bez podpisów mogą być także tworzone w pewnych szczególnych przypadkach. Takim przypadkiem jest wezwanie świadka do stawiennictwa osobistego w sądzie. Na podstawie § 19 ust. 4 zarządzenia Ministra Sprawiedliwości z dnia 12 grudnia 2003 r w sprawie organizacji i zakresu działania sekretariatów sądowych oraz innych działów administracji sądowej pismo takie nie wymaga podpisu własnoręcznego jako właściwie zatwierdzone w sądowym systemie teleinformatycznym. Pismami bez podpisu będą także wyciągi z baz poświadczających stan danych w konkretnym dniu (np. wyciąg z REGONu uzyskany na stronie https://wyszukiwarkaregon.stat.gov pl/appBIR/index.aspx).

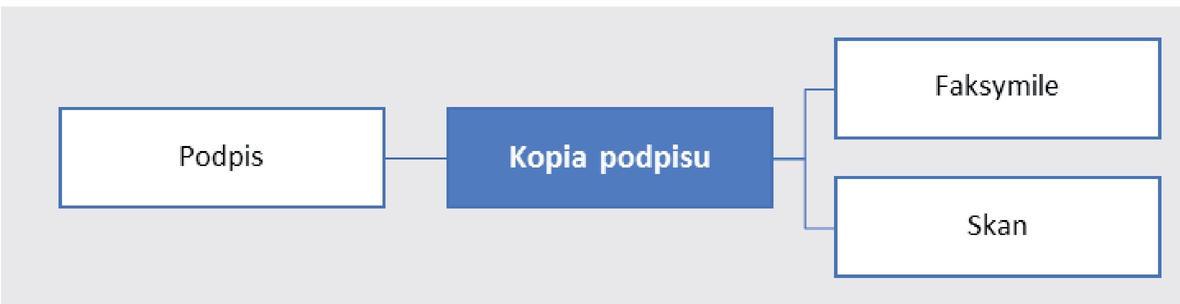
#### 5.3.3.1. Identyfikator dokumentu

Dokument powinien mieć identyfikator, nadawany automatycznie w systemie EZD i będący unikatowym w całym zbiorze przesyłek wpływających. Identyfikator ten określany jest jako numer z rejestru przesyłek wpływających, prowadzonego dla danego roku kalendarzowego (np. UNP 2015-02357, czyli pismo o numerze 2357 w roku 2015). Generalnie każdy dokument powinien mieć identyfikator pozwalający na powołanie się na ten dokument w korespondencji lub na odszukanie go w systemie zarządzania dokumentami – bez względu na ich formę i postać.


### 5.3.3.2. Brak identyfikatora dokumentu

Dokumenty bez identyfikatorów to dokumenty o utrudnionej do ustalenia wiarygodności – identyfikator pozwala ustalić relacje z innymi dokumentami tego samego rodzaju, wydanymi przez tego samego wystawcę, a w razie wątpliwości wskazać na dokument, którego potwierdzona przez wystawcę kopia może posłużyć jako dowód. Idea wszelkich systemów zarządzania dokumentami opiera się właśnie na stworzeniu możliwości takiego znakowania dokumentów, by można było powiązać z czasem i miejscem wytworzenia oraz sytuacją stanowiącą przyczynę ich wystawienia.


## 5.3.4. Kopia podpisu

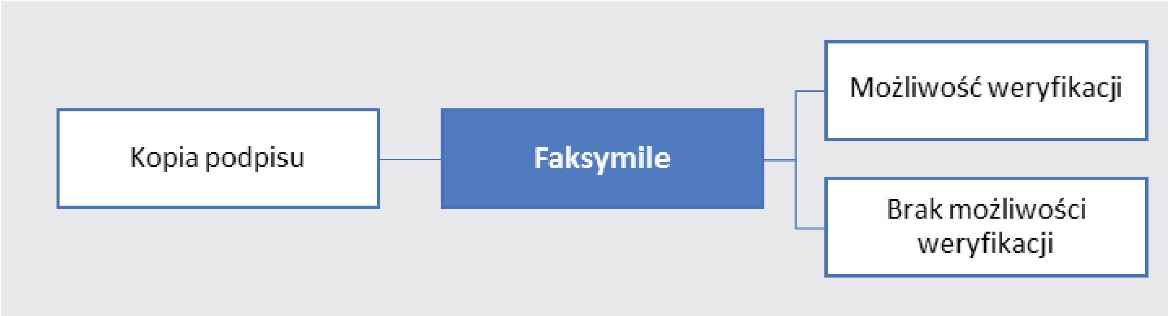



*Kopia podpisu*

Kopia podpisu własnoręcznego w żadnym wypadku nie niesie skutków prawnych podpisu własnoręcznego. Kopia podpisu znajduje się na kopiach – skanach i kserokopiach dokumentów itp. Z uwagi na słabość dowodową kopii dokumentów papierowych, kopia taka może mieć jedynie znaczenie pomocnicze w pewnych, szczególnych sytuacjach. Np. kopia własnoręcznego podpisu osoby uprawnionej do podpisywania dokumentów finansowych stosowana jest powszechnie w bankach jako kopia „karty wzorów podpisów" Pracownik banku ocenia „na oko" czy podpis na okazywanym mu dokumencie jest zgodny z kopią obrazu podpisu widzianą przez niego na monitorze. Podobnie rzecz ma się z obecnie używanymi dokumentami takimi jak dowód osobisty czy prawo jazdy – uwidocznione są na nich **kopie podpisów własnoręcznych** – i to zmienione co do wielkości tak, by zmieściły się w miejscu na to przeznaczonym. Takie wykorzystanie podpisu ma swój sens utylitarny Kopie podpisów własnoręcznych w obrębie pieczęci imiennej stosowane są w niektórych systemach elektronicznego zarządzania dokumentami w celu nadania dokumentom wyglądu jak najbardziej przypominającego pisma tworzone w administracji „papierowej" Podobieństwo wydruku na drukarkach atramentowych tak sporządzonego pisma do dokumentu rzeczywiście podpisanego i opieczętowanego może być łudzące, co oznacza również możliwość tworzenia pism fałszywych (czyli będących od początku pismami, w których kopia podpisu dodana została do tekstu, którego rzekomy sygnatariusz w ogóle nie widział, a tym bardziej nie podpisywał). Z uwagi na powyższe taki sposób tworzenia dokumentów nie jest zalecany

#### 5.3.4.1. Faksymile

| |
|---|
| **Faksymile** - kopia podpisu odbita sposobem mechanicznym na dokumencie. Dopuszczona przez Kodeks cywilny w odniesieniu do dokumentów na okaziciela, a przez Kodeks spółek handlowych – w odniesieniu do akcji; (Wikipedia) |




*Faksymile*

Z uwagi na coraz powszechniejsze używanie silnych dowodowo dokumentów elektronicznych faksymile jest używana w coraz węższym zakresie i w e-administracji praktycznie nie powinna już mieć zastosowania, szczególnie z uwagi na słabość dowodową. Zamiast faksymili powinny być stosowane **naturalne dokumenty elektroniczne** z identyfikatorem pozwalającym na łatwe dotarcie do dokumentu oryginalnego.

#### 5.3.4.1.1. Możliwość weryfikacji

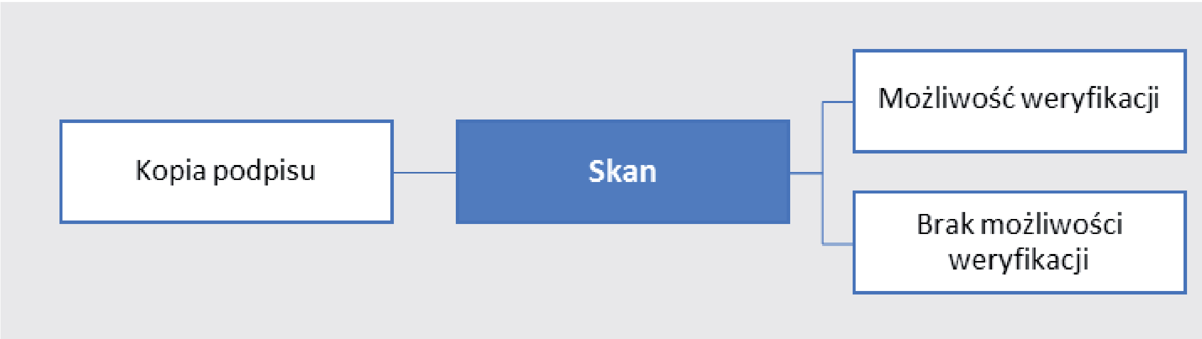
Weryfikacja prawdziwości i integralności dokumentów opatrzonych jakimikolwiek kopiami podpisów, faksymilami itp. powinna opierać się na pozyskaniu przez osobę ustalającą wiarygodność dokumentu kopii ze źródła jego wytworzenia. Przykładem takiego działania może być kontakt z instytucją wystawiającą dokument, powołanie się na identyfikator dokumentu (nr UNP lub znak pisma) oraz prośbę o przesłanie kopii.


Niektóre podmioty udostępniają potwierdzone kopie wystawionych dokumentów automatycznie (zob. mechanizm weryfikacji dokumentów udostępniony przez Ministerstwo Sprawiedliwości pod adresem [https://ems.ms.gov.pl/krs/weryfikujwydruk](https://ems.ms.gov.pl/krs/weryfikujwydruk)). Unikatowy Numer Pisma jest jednoznacznym identyfikatorem dokumentu tworzonym przez system automatycznie, podobnie jak inne identyfikatory, które mogą mieć inną konstrukcję, np. numer seryjny wynikający z daty i czasu wygenerowania oraz dodatkowych znaków System weryfikujący – po podaniu numeru pisma, którego autentyczność budzi wątpliwości, jest ponownie drukowany ze wskazaniem, że jest kopią – i z tego wydruku należy korzystać jako źródłowego.

#### 5.3.4.1.2. Brak możliwości weryfikacji

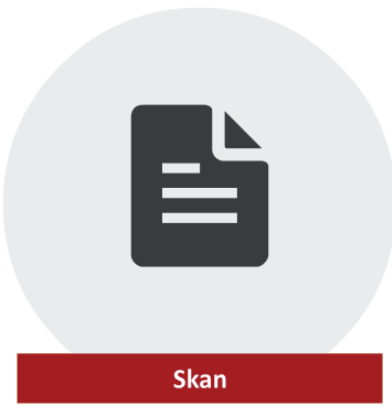
„Dokument", będący tekstem „podpisanym" faksymilą, a niezawierający w swej treści identyfikatora pozwalającego na jednoznaczną weryfikację (uzyskanie kopii danego „dokumentu" ze źródła – lecz nie przez osobę dostarczającą kwestionowany dokument, a przez kwestionującego wiarygodność) nie może być traktowany jako dokument, ponieważ nie posiada cech zapewniających jego autentyczność.

### 5.3.4.2. Skan




*Skan*

Skan (odwzorowanie cyfrowe) dokumentu lub jego kserokopia nie jest wiarygodnym dokumentem, jeśli nie zawiera w swej treści identyfikatora pozwalającego na jednoznaczną weryfikację (uzyskanie kopii danego „dokumentu" ze źródła – lecz nie przez osobę dostarczającą kwestionowany dokument, a przez kwestionującego wiarygodność przedłożonego skanu) i nie może być traktowany jako dokument, ponieważ nie posiada cech zapewniających jego autentyczność. Jeśli jednak skan zostanie wykonany z dokumentu, którego oryginalność nie budzi żadnych wątpliwości i zostanie poświadczony przez osobę, która zachowuje dokument oryginalny jako dowód (np. dla celów ewentualnego postępowania sądowego), wtedy skan poświadczony za zgodność jego treści z treścią oryginału może być wiarygodnym dokumentem wewnątrz podmiotu, posiadającego oryginał. Skany i kserokopie tworzone są w celu powielenia dla celów operacyjnych lub w celu zwiększenia bezpieczeństwa treści (im więcej kopii, tym mniejsza szansa utraty treści oryginalnego dokumentu).



#### 5.3.4.2.1. Możliwość weryfikacji

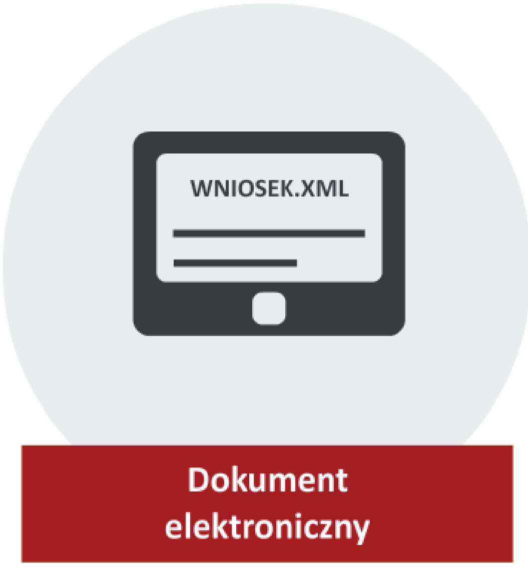
Każda kopia dokumentu – niezależnie od techniki jej utworzenia, może w mniejszym lub większym stopniu osłabiać lub całkowicie usunąć pewność co do autentyczności tej treści. Jest to zależne od tego, kto tę kopię wytwarza i w jakiej procedurze nastąpiło kopiowanie. Osoba tworząca kopię (skan, kserokopię) z dokumentu oryginalnego nie ma żadnych wątpliwości co do autentyczności treści – i tylko ona może wiarygodnie poświadczyć zgodność treści kopii z treścią oryginału. Taki przypadek występuje w kancelarii, w której znajdują się oryginały dokumentów (oznakowane jako przesyłki wchodzące), z których w razie potrzeby pracownicy mogą wykonywać wiarygodne kopie. Podobnie rzecz ma się z uzyskiwaniem kopii materiałów archiwalnych.

#### 5.3.4.2.2. Brak możliwości weryfikacji

Skan dokumentu nieposiadającego identyfikatora umożliwiającego łatwe pozyskanie wiarygodnej kopii oryginału nie powinien być traktowany jako dokument wiarygodny

## 5.4. Naturalny dokument elektroniczny

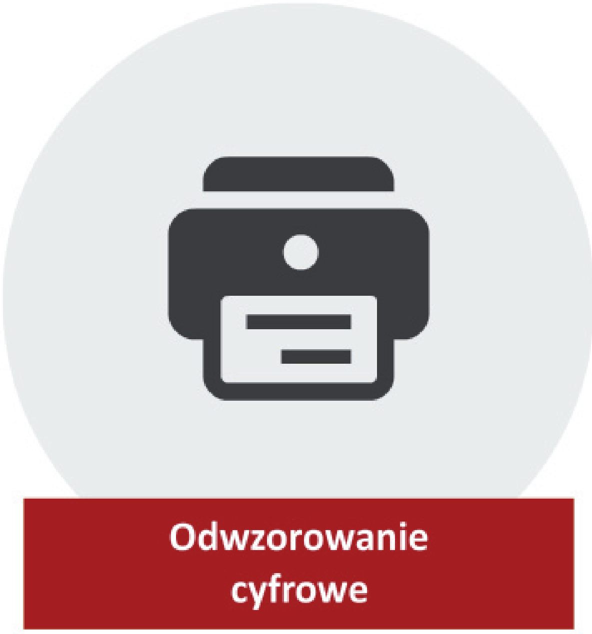
**Naturalny dokument elektroniczny** - dokument będący od początku swojego istnienia zbiorem zapisanym w postaci elektronicznej, możliwym do odczytania wyłącznie za pośrednictwem odpowiednich urządzeń elektronicznych, nieposiadający pierwowzoru w postaci nieelektronicznej; (Dz.U.2011.14.67)




Naturalne dokumenty elektroniczne w e-administracji tworzone są coraz częściej – i proces ten ma tendencję dynamicznie rosnącą. Jest to rezultatem upowszechniania się systemów elektronicznego zarządzania dokumentami (EZD). Dokument tworzony jest za pomocą edytora tekstu lub innego programu (dokument może być także graficzny, dźwiękowy, audiowizualny), a następnie elektronicznie podpisywany Należy podkreślić, że tworzenie naturalnych dokumentów odbywa się bez jakiegokolwiek użycia papieru, drukarek, tonerów, pieczątek, długopisów i innych materiałów biurowych, co automatycznie przekłada się na bezpośrednie korzyści finansowe i organizacyjne. Z uwagi na fakt, że aktualnie administracja publiczna może tworzyć, wysyłać i przyjmować dokumenty elektroniczne, stosowanie dokumentów papierowych należy traktować jako niegospodarność, której wymiarem są wydatki na materiały biurowe związane z tworzeniem, przechowywaniem i wysyłaniem dokumentów papierowych oraz ich kopii.

## 5.5. Odwzorowanie cyfrowe

**Odwzorowanie cyfrowe** - dokument elektroniczny będący kopią elektroniczną dowolnej treści zapisanej w postaci innej niż elektroniczna, umożliwiający zapoznanie się z tą treścią i jej zrozumienie, bez konieczności bezpośredniego dostępu do pierwowzoru; (Dz.U.2011.14.67)



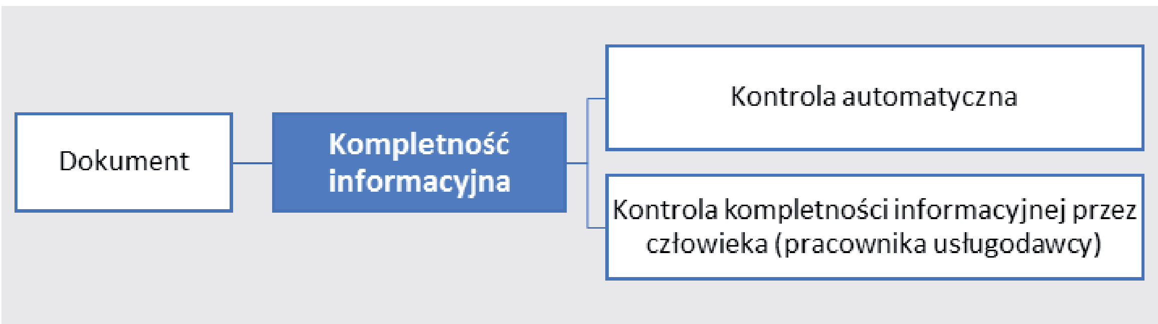

Dokonywanie odwzorowań cyfrowych jest typową, codzienną czynnością pracowników kancelarii; polega ono na skanowaniu z odpowiednią rozdzielczością dokumentów z reguły papierowych i przekazywaniu skanów w systemie EZD do pracowników merytorycznych lub sekretariatów – zależnie od organizacji podmiotu. Skanowany dokument trafia do **składu chronologicznego.**

## 5.6. Jednoznaczność, czytelność

Jedną z wad dokumentów papierowych może być wada nieczytelności i niejednoznaczności znaków wpisanych ręcznie, mających być uzupełnieniem dokumentu wstępnie utworzonego w edytorze i później wydrukowanego. Przyczyną może być zbyt mało miejsca pozostawionego na ręczne dopiski lub charakter pisma osoby dokonującej uzupełnień. Najczęściej brak czytelności i jednoznaczności dotyczy dat oraz znaków pisma (numeru kancelaryjnego) a także podpisów  Jest to z reguły wynik organizacji pracy w otoczeniu „elektronicznie niepiśmiennej" osoby uprawnionej do podpisywania dokumentów – nie wiadomo czy- i kiedy dokument zostanie podpisany, ani jaki numer będzie miało pismo w konkretnej sprawie.

Niejednoznaczność i nieczytelność dotyczy także skanów i kserokopii papierowych dokumentów zawierających treści drukowane na oryginale zbyt drobną czcionką.

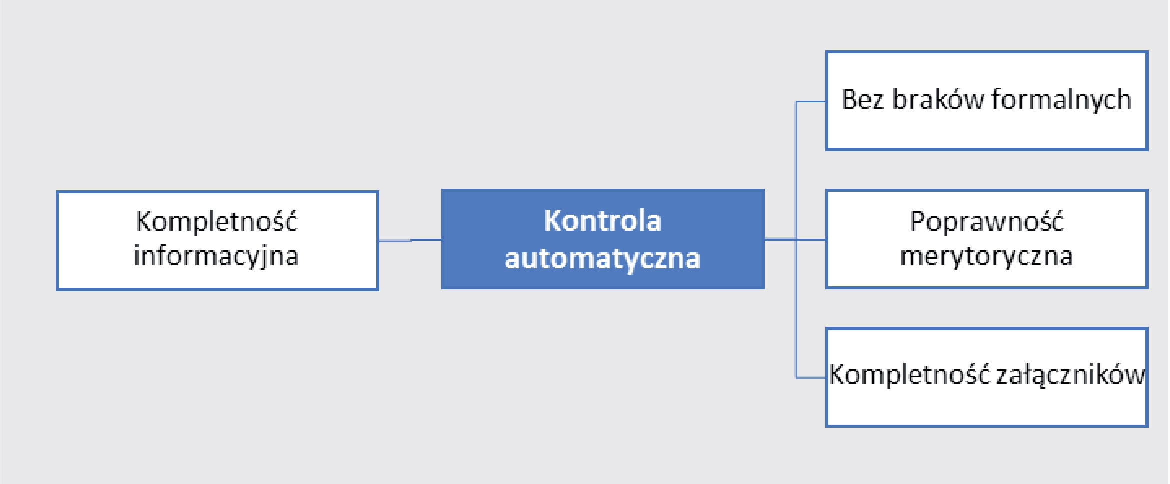
## 5.7. Kompletność informacyjna




*Kompletność informacyjna*

Dokument powinien być informacyjnie kompletny Jeśli np. tworzony jest w oparciu o wzór, pola obligatoryjne powinny być wypełnione. Dokument musi być umiejscowiony w czasie i miejscu, a więc powinien być opatrzony datą i miejscem utworzenia, powinien mieć jednoznacznie określonego adresata i nadawcę (autora, twórcę) oraz treść główną lub – jeśli posiada załączniki – co najmniej informację o ich liczbie. Powinien być także podpisany podpisem, którego funkcją jest zabezpieczenie dokumentu przed niekontrolowaną modyfikacją. Ta funkcja może być realizowana w różny sposób, jednak – ze względów dowodowych - jest istotna.

### 5.7.1. Kontrola automatyczna




*Kontrola automatyczna*

Do tworzenia dokumentów elektronicznych niezbędnych w realizacji konkretnych, ściśle zdefiniowanych spraw (jak np. tworzenie konta na platformie ePUAP, deklaracje podatków i wiele innych) służyć mogą formularze, które już na etapie ich wypełniania mogą sygnalizować błędy, lub mogą zwracać komunikaty wskazujące miejsca błędnie wypełnione lub niewypełnione. Taka kontrola nie wymaga żadnej ingerencji ze strony usługodawcy – usługobiorca na podstawie uzyskanych informacji poprawia dane, aż system je przyjmie, potwierdzając to stosownym komunikatem przyjęcia (UPO).

### 5.7.1.1. Bez braków formalnych

Dokument bez braków formalnych może być przyjęty przez system, jednak nie zawsze można wyeliminować błędy merytoryczne. Zdarzają się one w systemach, w których np. przy podawaniu danych osobowych istnieje możliwość błędnego wpisania imienia i nazwiska (odwrotnie – imię w polu nazwiska, nazwisko w polu imienia) lub błędy podobnego rodzaju, np. nazwa ulicy lub miejscowości w różnych wersjach. Jeśli istnieje możliwość wpisania danych dowolnych, a systemowi przyjmującemu dokument z danymi to „nie przeszkadza", należy podważyć sens ich gromadzenia – szczególnie, jeśli chodzi o gromadzenie danych osobowych.

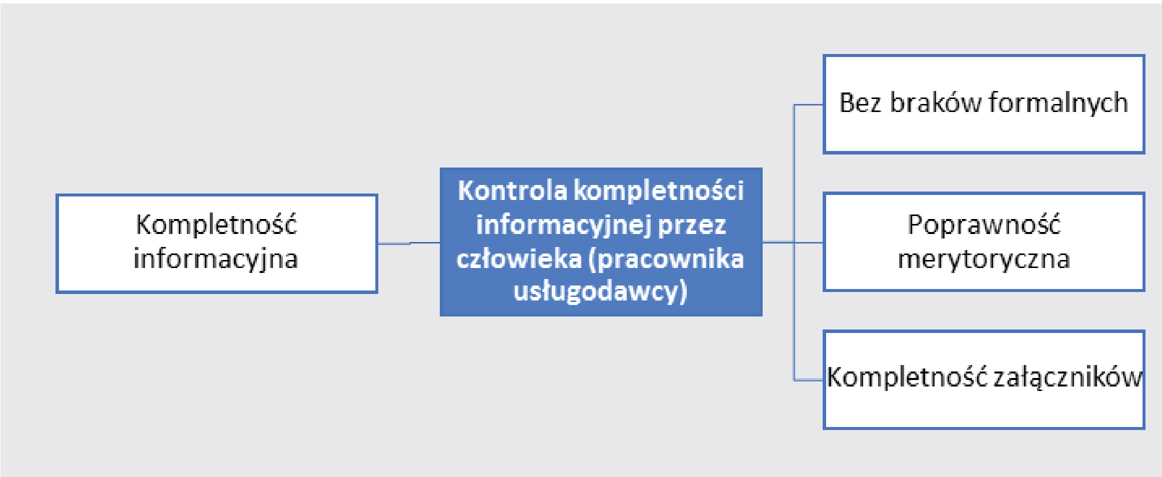

### 5.7.1.2. Poprawność merytoryczna

Kontrola automatyczna merytorycznej poprawności dokumentów (a raczej jest to wspomaganie usługobiorcy) możliwa jest w sytuacji, gdy poszczególne pola danych mogą być wypełniane na podstawie danych w słownikach – i to danych wzajemnie ze sobą powiązanych). Przykładem może być wypełnianie pól miejscowości i ulic w oparciu o słownik TERYT wykorzystywany w ePUAP Jeśli usługobiorca wypełnia formularz poprawnie (czyli w logicznie zaproponowanej kolejności pól – to już poprawne wpisanie miejscowości powoduje automatyczne wypełnienie pól, które mogą być przez system wypełnione). Zasadą jest, że należy oczekiwać na reakcję systemu i pozwolić mu na podpowiadanie wartości właściwych – albo ostatecznych, albo opcjonalnych – do doszczegółowienia z wyświetlonej listy

### 5.7.1.3. Kompletność załączników

Załączniki do pism są także dokumentami. W związku z powyższym dotyczą ich takie same reguły, jakie stosuje się w odniesieniu do dokumentów głównych – z drobną różnicą: załącznik powinien w swojej treści mieć odniesienie do dokumentu, którego dotyczy – lub powinien być odrębnie opisany metadanymi tak, by związek z dokumentem głównym był jednoznaczny Załączniki stanowią uzupełnienie dokumentu głównego, który w szczególności, w dobrze zdefiniowanych sprawach może być jedynie pismem przewodnim, kompletnym informacyjnie (określony nadawca, odbiorca, data i miejsce wytworzenia dokumentu) i zawierającym informację o liczbie i rodzaju przekazywanych załączników Dokument główny powinien być podpisany W przypadku dokumentów składanych za pośrednictwem ePUAP lista załączników tworzona jest automatycznie przez system – i znajdują się one w kontenerze głównym – nie mogą ulec odłączeniu czy zagubieniu. Podpisanie dokumentu głównego jest równoznaczne z podpisaniem wszystkich załączników

## 5.7.2. Kontrola kompletności informacyjnej przez człowieka (pracownika usługodawcy)

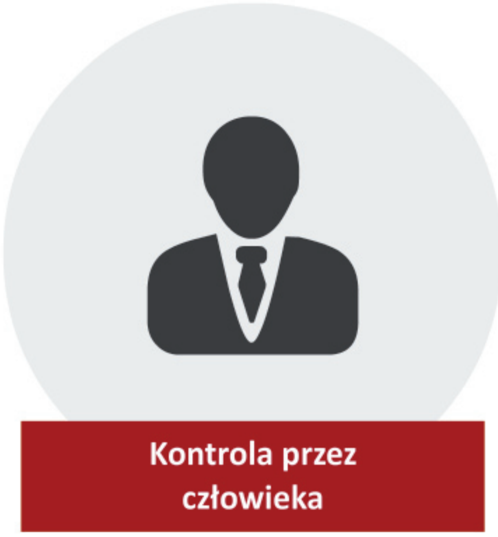



*Kontrola kompletności informacyjnej przez człowieka*

Kontrola kompletności informacyjnej dokumentów przyjmowanych przez człowieka dokonywana jest w kancelarii lub Biurze Obsługi Interesanta. Polega ona na wykonaniu tych samych czynności, które w odniesieni do dokumentów elektronicznych wykonuje stosowne oprogramowanie, czyli stwierdzenie, czy przedkładany dokument jest kompletny, czy w wypełnionych polach znajdują się merytorycznie poprawne dane, czy nie zawiera skreśleń powodujących nieczytelność itd.

### 5.7.2.1. Bez braków formalnych

Dokument bez braków formalnych może być przyjęty przez pracownika kancelarii lub Biura Obsługi interesanta, jeśli ma wszystkie niezbędne elementy takie jak data i miejsce utworzenia, treść główną, podpis, niezbędne załączniki, dowody opłat – jeśli wymagane itd.




### 5.7.2.2. Poprawność merytoryczna

Kontrola merytorycznej poprawności składanych dokumentów dokonywana jest bezpośrednio przez pracowników Biura Obsługi Interesanta lub – jeśli taka jest organizacja instytucji usługodawcy - przez pracowników merytorycznych, którzy będą daną sprawę załatwiać. Mogą oni – mając bezpośredni kontakt z interesantem, wyjaśnić ewentualne braki i pomyłki. Nie jest to jednak metoda rekomendowana – jako uciążliwa dla usługobiorców i pracowników usługodawcy (dezorganizacja czasu pracy, poprawianie ciągle tych samych błędów, wynikających z nieczytelności czy niezrozumienia formularzy przez interesantów).

### 5.7.2.3. Kompletność załączników

Załączniki do pism są także dokumentami W związku z powyższym dotyczą ich takie same reguły, jakie stosuje się w odniesieniu do dokumentów głównych (kompletność, czytelność) – z drobną różnicą: załącznik powinien w swojej treści mieć odniesienie do dokumentu, którego dotyczy – lub powinien być odrębnie opisany metadanymi tak, by związek z dokumentem głównym był jednoznaczny Załączniki stanowią uzupełnienie dokumentu głównego, który w szczególności, w dobrze zdefiniowanych sprawach może być jedynie pismem przewodnim, kompletnym informacyjnie (określony nadawca, odbiorca, data i miejsce wytworzenia dokumentu) i zawierającym informację o liczbie i rodzaju przekazywanych załączników Dokument główny powinien być podpisany, załączniki wymagające podpisu również