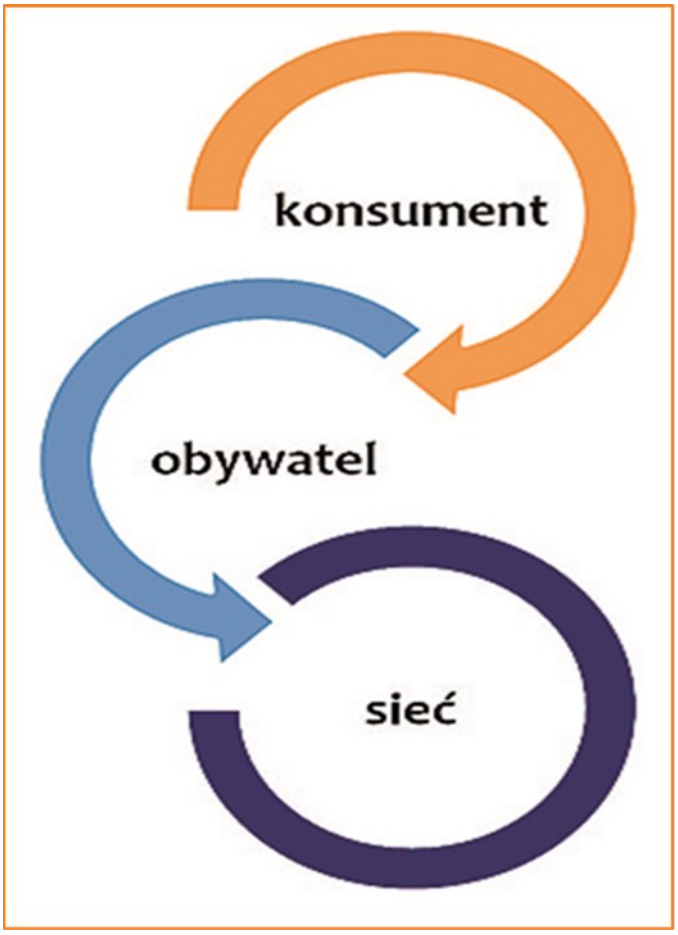
Prawa obywatela w Internecie

W TYM NUMERZE:

Newsletter nr 10 **styczeń 2014**

KOLPING Bochnia



Projekt realizowany przy wsparciu Szwajcarii w ramach szwajcarskiego programu współpracy z nowymi krajami członkowskimi Unii Europejskiej.

SWISS CONTRIBUTION

ECORYS

Euroregion Bałtyk

Rodzaje podpisów elektronicznych

Niekiedy przepisy wymagają, aby dokument miał zachowana formę pisemną, tj. aby był zaopatrzony własnoręcznym podpisem. Jeśli posługujemy się Internetem w kontaktach z organami administracji, również musimy stosować się do wymogów prawa proceduralnego, które reguluje m. in. formę składanych podań. Brak podpisu może spowodować, że podanie nie będzie mogło spełniać wymogów przewidzianych prawem i nie wywoła zamierzonych skutków. Z natury rzeczy trudno byłoby mówić o własnoręcznym podpisie jeśli posługujemy się dokumentem elektronicznym. Zwykle do składania podań nie wystarczy więc forma mailowa – niezbędne będzie złożenie podpisanego podania. Stąd potrzeba istnienia podpisu elektronicznego spełniającego określone standardy, a który będzie wywoływał takie same skutki, jak gdybyśmy złożyli własnoręczny podpis, np. na kartce papieru. Podpis elektroniczny (zwany również e-podpisem i pomimo pewnych zastrzeżeń powszechnie traktowany jako synonim podpisu cyfrowego) jest rozwiązaniem funkcjonującym od niedawna. Podstawowym aktem prawnym odnoszącym się do podpisu elektronicznego jest ustawa z 18 września 2001 r. o podpisie elektronicznym (t. j. Dz. U. z 2013 r., poz. 262). Polskiemu prawu znane są następujące rodzaje podpisów elektronicznych:

Podpis elektroniczny

Bezpieczny podpis elektroniczny

Bezpieczny podpis elektroniczny weryfikowany przy pomocy kwalifikowanego certyfikatu

Ustawa definiuje podpis elektroniczny jako:

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.

Skróty:

BPKE C - bezpieczny podpis elektroniczny weryfikowany przy pomocy kwalifikowanego certyfikatu

KC – Kodeks Cywilny

Kpa – Kodeks postepowania administracyjnego

ZAPAMIĘTAJ!

Nie każdy podpis elektroniczny jest bezpiecznym podpisem elektronicznym weryfikowanym przy pomocy kwalifikowanego certyfikatu.

Bezpieczny podpis elektroniczny

jest to podpis elektroniczny, który:

a) jest przyporządkowany wyłącznie do osoby składającej ten podpis,

b) jest sporządzany za pomocą podlegających wyłącznej kontroli osoby składającej podpis elektroniczny bezpiecznych urządzeń służących do składania podpisu elektronicznego i danych służących do składania podpisu elektronicznego,

c) jest powiązany z danymi, do których został dołączony, w taki sposób, że jakakolwiek późniejsza zmiana tych danych jest rozpoznawalna.

Skutki prawne bezpiecznego podpisu elektronicznego weryfikowanego przy pomocy kwalifikowanego certyfikatu.

Największą rolę zdaje się spełniać bezpieczny podpis elektroniczny weryfikowany przy pomocy kwalifikowanego certyfikatu (dalej: BPEKC). Certyfikat jest to elektroniczne zaświadczenie, za pomocą którego dane służące do weryfikacji podpisu elektronicznego są przyporządkowane do osoby składającej podpis elektroniczny i które umożliwiają identyfikację tej osoby. Jeśli spełnia warunki określone w ustawie i jest wydany przez kwalifikowany podmiot świadczący usługi certyfikacyjne, spełniający wymogi określone w ustawie – jest wówczas kwalifikowanym certyfikatem.

Ustawa stanowi, że:

Dane w postaci elektronicznej opatrzone bezpiecznym podpisem elektronicznym weryfikowanym przy pomocy ważnego kwalifikowanego certyfikatu są równoważne pod względem skutków prawnych dokumentom opatrzonym podpisami własnoręcznymi, chyba że przepisy odrębne stanowią inaczej.

Kodeks cywilny traktuje BPEKC jako równoznaczny z podpisem własnoręcznym.

Wg art. 78 § 2 KC:

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. Z kolei w myśl przepisów Kodeksu postepowania administracyjnego podanie złożone w formie elektronicznej zaopatrzone takim podpisem jest podaniem wniesionym równie skutecznie co przy pomocy tradycyjnego pisma.

BPEKC odgrywa coraz większą rolę, w szczególności daje możliwość zarejestrowania działalności gospodarczej, składania deklaracji płatników składek do ubezpieczenia społecznego, czy np. wystawiania e-faktur. Od kilku lat istnieje też możliwość zastosowania BPEKC w celu złożenia podania do organów administracji publicznej. Wg danych będących w posiadaniu Ministerstwa Gospodarki, w grudniu 2013 r. było w Polsce 279 000 aktywnych certyfikatów kwalifikowanych.

Kodeks postepowania administracyjnego przewiduje obok pisemnej formy m.in. możliwość składania podań także elektronicznie. Nie daje jednak możliwości złożenia podania zwykłym mailem.

Z art. 63 Kpa wynika, że podanie (żądanie, wyjaśnienie, odwołanie, zażalenie) złożone do organu administracji może być wniesione m. in. elektronicznie

za pomocą innych środków komunikacji elektronicznej przez elektroniczną skrzynkę podawczą organu administracji publicznej utworzoną na podstawie ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne.

Podanie wniesione w formie dokumentu elektronicznego powinno być uwierzytelnione przy użyciu mechanizmów określonych w art. 20a ust. 1 albo ust. 2 ustawy o informatyzacji działalności podmiotów realizujących zadania publiczne oraz zawierać dane w ustalonym formacie, zawartym we wzorze podania określonym w odrębnych przepisach - jeżeli te przepisy nakazują wnoszenie podań według określonego wzoru.

Powołane przepisy ustawy o informatyzacji (…) stanowią:

1. Identyfikacja użytkownika systemów teleinformatycznych udostępnianych przez podmioty określone w art. 2 następuje przez zastosowanie kwalifikowanego certyfikatu przy zachowaniu zasad przewidzianych w ustawie z dnia 18 września 2001 r. o podpisie elektronicznym (Dz. U. Nr 130, poz. 1450, z późn. zm.), lub profilu zaufanego ePUAP.

2. Podmiot publiczny, który używa do realizacji zadań publicznych systemów teleinformatycznych, może umożliwiać użytkownikom identyfikację w tym systemie przez zastosowanie innych technologii, chyba że przepisy odrębne przewidują obowiązek dokonania czynności w siedzibie podmiotu publicznego.

Krótko mówiąc, podanie, jakie wpłynęło w postaci elektronicznej na elektroniczną skrzynkę podawczą organu, zaopatrzone w BPEKC jest podaniem równie skutecznie wniesionym co podanie w formie pisemnej (tj. zaopatrzonej własnoręcznym podpisem).

ZAPAMIĘTAJ!

Podanie (żądanie, wyjaśnienie, odwołanie, zażalenie) do organu administracji może być wniesione również elektronicznie na elektroniczną skrzynkę podawczą organu, przy zastosowaniu bezpiecznego podpisu elektronicznego weryfikowanego przy pomocy kwalifikowanego certyfikatu.

Przypomnijmy w tym miejscu, że wniosek o udostępnienie informacji publicznej jest wyjątkiem od powyższej reguły, gdyż nie wszczyna postepowania administracyjnego, a co za tym idzie – nie odnoszą się do niego wymogi przewidziane w cytowanym art. 63 kpa. Dlatego wniosek o udostepnienie informacji publicznej nie wymaga BPEKC i może zostać złożony nawet zwykłym mailem – jest to jednak wyjątek od zasady.

Ustawa o podpisie elektronicznym stanowi, że bezpieczny podpis elektroniczny weryfikowany przy pomocy kwalifikowanego certyfikatu wywołuje skutki prawne określone ustawą, jeżeli został złożony w okresie ważności tego certyfikatu. Jeżeli jednak został złożony w okresie zawieszenia kwalifikowanego certyfikatu wykorzystywanego do jego weryfikacji wywołuje skutki prawne z chwilą uchylenia tego zawieszenia.

Bezpieczny podpis elektroniczny weryfikowany przy pomocy kwalifikowanego certyfikatu zapewnia integralność danych opatrzonych tym podpisem i jednoznaczne wskazanie kwalifikowanego certyfikatu, w ten sposób, że rozpoznawalne są wszelkie zmiany tych danych oraz zmiany wskazania kwalifikowanego certyfikatu wykorzystywanego do weryfikacji tego podpisu, dokonane po złożeniu podpisu.

BPEKC stanowi dowód tego, że został on złożony przez osobę określoną w tym certyfikacie jako składającą podpis elektroniczny; nie odnosi się to do certyfikatu po upływie terminu jego ważności lub od dnia jego unieważnienia oraz w okresie jego zawieszenia, chyba że zostanie udowodnione, że podpis został złożony przed upływem terminu ważności certyfikatu lub przed jego unieważnieniem albo zawieszeniem. Nie można powoływać się, że BPKCE nie został złożony za pomocą bezpiecznych urządzeń i danych, podlegających wyłącznej kontroli osoby składającej podpis elektroniczny. Jeśli zaś chodzi o podpisy elektroniczne nie spełniające wymogów BPKCE, to nie można odmówić ważności i skuteczności podpisowi elektronicznemu tylko na tej podstawie, że istnieje w postaci elektronicznej lub dane służące do weryfikacji podpisu nie mają kwalifikowanego certyfikatu, lub nie został złożony za pomocą bezpiecznego urządzenia służącego do składania podpisu elektronicznego.

Umowa z podmiotem świadczącym usługi certyfikacyjne

Podstawowym krokiem w kierunku uzyskania BPEKC jest zawarcie umowy pomiędzy podmiotem świadczącym usługi certyfikacyjne a odbiorcą usług certyfikacyjnych.

Niezbędne jest wyjaśnienie pojęć.

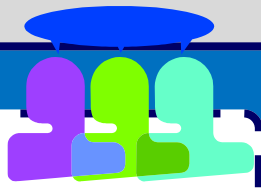
Podmiot świadczący usługi certyfikacyjne – jest to przedsiębiorca w rozumieniu przepisów ustawy z dnia 2 lipca 2004 r. o swobodzie działalności gospodarczej, Narodowy Bank Polski albo organ władzy publicznej, świadczący co najmniej jedną z usług certyfikacyjnych. NBP i organy władzy może świadczyć takie usługi wyłącznie na użytek własny lub innych organów władzy publicznej, z zastrzeżeniem, ze organy władzy publicznej mogą także świadczyć te usługi na zasadach niezarobkowych dla członków wspólnoty samorządowej. W obecnej chwili certyfikaty kwalifikowane wydają jedynie przedsiębiorcy wpisani do rejestru prowadzonego przez ministra gospodarki.

Usługi certyfikacyjne - wydawanie certyfikatów, znakowanie czasem lub inne usługi związane z podpisem elektronicznym.

Odbiorca usług certyfikacyjnych – osoba fizyczna, osoba prawna lub jednostka organizacyjna nieposiadającą osobowości prawnej, która:

a) zawarła z podmiotem świadczącym usługi certyfikacyjne umowę o świadczenie usług certyfikacyjnych lub

b) w granicach określonych w polityce certyfikacji może działać w oparciu o certyfikat lub inne dane elektronicznie poświadczone przez podmiot świadczący usługi certyfikacyjne.



Umowa o świadczenie usług certyfikacyjnych powinna być sporządzona w formie pisemnej pod rygorem nieważności.

Odbiorca usług certyfikacyjnych jest obowiązany przechowywać dane służące do składania podpisu elektronicznego w sposób zapewniający ich ochronę przed nieuprawnionym wykorzystaniem w okresie ważności certyfikatu służącego do weryfikacji tych podpisów (art. 15).

Certyfikat

Już z cytowanych wyżej przepisów wynika, że certyfikat nie jest przyznawany bezterminowo.

Termin jego ważności jest jednym ze składników certyfikatu. W praktyce jego ważność ogranicza się do okresu jednego roku lub dwóch lat. Może jednak wystąpić sytuacja, że podmiot świadczący usługi unieważni certyfikat wcześniej.

Sytuacja taka ma miejsce jeśli:

1) certyfikat ten został wydany na podstawie nieprawdziwych lub nieaktualnych danych, o których mowa w art. 20 ust. 1 pkt 4 i ust. 2 ustawy (np. imię i nazwisko);
2) podmiot świadczący usługi certyfikacyjne nie dopełnił obowiązków określonych w ustawie;
3) osoba składająca podpis elektroniczny weryfikowany na podstawie tego certyfikatu nie dopełniła obowiązków w zakresie przechowywania danych służących do składania podpisu elektronicznego w sposób zapewniający ich ochronę przed nieuprawnionym wykorzystaniem w okresie ważności certyfikatu;
4) podmiot świadczący usługi certyfikacyjne zaprzestaje świadczenia usług certyfikacyjnych, a jego praw i obowiązków nie przejmie inny kwalifikowany podmiot;
5) zażąda tego osoba składająca podpis elektroniczny lub osoba trzecia wskazana w certyfikacie;
6) zażąda tego minister właściwy do spraw gospodarki;
7) osoba składająca podpis elektroniczny utraciła pełną zdolność do czynności prawnych.

ZAPAMIĘTAJ!

Należy przechowywać dane służące do składania podpisu elektronicznego w sposób zapewniający ich ochronę przed nieuprawnionym wykorzystaniem w okresie ważności certyfikatu.

Zawieszenie certyfikatu

Zawieszenie certyfikatu jest dopuszczalne w przypadku istnienia uzasadnionego podejrzenia, że istnieją przesłanki do unieważnienia kwalifikowanego certyfikatu. Podmiot świadczący usługi certyfikacyjne jest wówczas obowiązany niezwłocznie zawiesić certyfikat i podjąć działania niezbędne do wyjaśnienia tych wątpliwości. Zawieszenie kwalifikowanego certyfikatu nie może trwać dłużej niż 7 dni.

Po upływie tego okresu, w przypadku niemożności wyjaśnienia wątpliwości, podmiot świadczący usługi certyfikacyjne niezwłocznie unieważnia kwalifikowany certyfikat. Certyfikat, który został zawieszony, może zostać następnie unieważniony lub jego zawieszenie może zostać uchylone. Certyfikat, który został unieważniony, nie może być następnie uznany za ważny. O unieważnieniu lub zawieszeniu certyfikatu podmiot świadczący usługi certyfikacyjne zawiadamia niezwłocznie osobę składającą podpis elektroniczny weryfikowany na jego podstawie. Zawieszenie lub unieważnienie certyfikatu nie może następować z mocą wsteczną.

Kwalifikowany certyfikat zawiera co najmniej następujące dane:

1) numer certyfikatu;
2) wskazanie, że certyfikat został wydany jako certyfikat kwalifikowany do stosowania zgodnie z określoną polityką certyfikacji;
3) określenie podmiotu świadczącego usługi certyfikacyjne wydającego certyfikat i państwa, w którym ma on siedzibę, oraz numer pozycji w rejestrze kwalifikowanych podmiotów świadczących usługi certyfikacyjne;
4) imię i nazwisko lub pseudonim osoby składającej podpis elektroniczny; użycie pseudonimu musi być wyraźnie zaznaczone;
5) dane służące do weryfikacji podpisu elektronicznego;
6) oznaczenie początku i końca okresu ważności certyfikatu;
7) poświadczenie elektroniczne podmiotu świadczącego usługi certyfikacyjne, wydającego dany certyfikat;
8) ograniczenia zakresu ważności certyfikatu, jeżeli przewiduje to określona polityka certyfikacji;
9) ograniczenie najwyższej wartości granicznej transakcji, w której certyfikat może być wykorzystywany, jeżeli przewiduje to polityka certyfikacji lub umowa, o której mowa w art. 14 ust. 1.

Podmiot świadczący usługi certyfikacyjne, wydając kwalifikowany certyfikat, jest obowiązany zawrzeć w tym certyfikacie inne dane niż wymienione wyżej na wniosek osoby składającej podpis elektroniczny, a w szczególności wskazanie, czy osoba ta działa:

1) we własnym imieniu albo

2) jako przedstawiciel innej osoby fizycznej, osoby prawnej albo jednostki organizacyjnej nieposiadającej osobowości prawnej, albo

3) w charakterze członka organu albo organu osoby prawnej, albo jednostki organizacyjnej nieposiadającej osobowości prawnej, albo

4) jako organ władzy publicznej.

Podmiot świadczący usługi certyfikacyjne, wydając kwalifikowany certyfikat, potwierdza prawdziwość tych danych. Przy podpisaniu umowy niezbędna jest weryfikacja tożsamości, która jest dokonywana na podstawie dokumentów – jest to niezbędne, ażeby podpis elektroniczny przyporządkowany danej osobie fizycznej nie otrzymała osoba do tego nieuprawniona. W wyniku zawarcia umowy odbiorca usług certyfikacyjnych otrzymuje oprogramowanie oraz sprzęt pozwalające na składanie podpisu elektronicznego.

Wymagania sprzętowe

Możliwość skorzystania z podpisu elektronicznego wiąże się z koniecznością korzystania z odpowiedniego oprogramowania.

Posługując się kluczem prywatnym może generować podpis elektroniczny. Z reguły posługiwanie się kluczem wymaga posłużenia się kartą kryptograficzną, której można używać za pomocą czytnika. Klucz prywatny, który jest znany tylko właścicielowi, związany z kartą kryptograficzną i niemożliwy do skopiowania należy odróżnić od klucza publicznego. Klucz publiczny pozwala na weryfikację podpisu elektronicznego i może zostać rozpowszechniony. Karta kryptograficzna nie zawsze jest niezbędna: klucz może być generowany również za pomocą tokena USB.

Tak więc oprócz podpisanej umowy niezbędne jest wyposażenie w odpowiednie oprogramowanie oraz sprzęt, który służy do generowania klucza prywatnego (z reguły jest to karta kryptograficzna oraz czytnik kart).

Na stronie podmiotowej BIP Starostwa Powiatowego w Bochni znajduje się informacja:
Wymagania dla dokumentów elektronicznych dostarczanych do Starostwa:

1. Dokumenty elektroniczne muszą być podpisane ważnym, kwalifikowany podpisem cyfrowym w formacie Xades-Bes;

2. Akceptowane formaty załączników to:
   a. DOC, RTF, ODT **b.** XLS **c.** TXT **d.** GIF, TIF, BMP, JPG **e.** PDF **f.** ZIP
3. Wielkość wszystkich załączników dołączonych do jednego formularza (dokumentu elektronicznego) nie może przekroczyć 3MB.
4. Dokumenty lub nośniki zawierające oprogramowanie złośliwe będą automatycznie odrzucane i nie zostaną rozpatrzone.
5. Osobiście można dostarczać dokumenty podpisane elektronicznie na n/w zapisywalnych nośnikach:
   a. Dyskietka 1,44 MB
   b. Pamięć masowa USB 1.1 lub 2.0
   c. Płyta CD-RW
   d. Inne - po wcześniejszym uzgodnieniu.

Dostarczony nośnik musi posiadać możliwość zapisania na nim Urzędowego Poświadczenia Odbioru.

Podsumujmy zatem:

Niewątpliwą zaletą podpisu elektronicznego jest to, że jakakolwiek zmiana dokonana po podpisaniu dokumentu jest rozpoznawalna (integralność podpisu) oraz że jest on przypisany do konkretnej, jednej osoby fizycznej. Dlatego uważa się, że jest bezpieczniejszy aniżeli podpis własnoręczny – przy podpisie własnoręcznym istnieje bowiem ryzyko przerobienia dokumentu (naniesienia zmian po jego podpisaniu) oraz jego podrobienia.

Słabą stroną podpisu elektronicznego jest przede wszystkim to, że posługiwanie się nim wymaga nakładów finansowych. Koszt zakupu zestawu do korzystania z BPEKC wynosi kilkaset zł, również przedłużenie certyfikatu następuje odpłatnie. Niedogodności te spowodowały konieczność wprowadzenia bezpłatnej możliwości składania podań do organów administracji – funkcję tę spełnia profil zaufany, któremu poświęcimy następny numer newslettera dotyczącego praw obywatela w Internecie.

Projekt realizowany przy wsparciu Szwajcarii w ramach szwajcarskiego programu współpracy z nowymi krajami członkowskimi Unii Europejskiej.

Biuro projektu:
„Konsument-Obywatel–Sieć”

ul. Wyspiańskiego 25,
Bochnia 32-700
el./fax: 14/635 11 17
bochnia@kolping.pl

Organizator:

Partnerzy: