EPODPIS.PL

PODPIS ELEKTRONICZNY

Jaka jest idea podpisu elektronicznego?

Droga elektroniczna jest znacznym ułatwieniem wymiany informacji pomiędzy ludźmi.
Internet stał się powszechnym narzędziem wykorzystywanym w urzędach oraz przedsiębiorstwach i coraz większa ich liczba posługuje się nim do przesyłania wniosków, podań i umów. Jednak ze względu na dość dużą anonimowość użytkowników Internetu, narzędzie to stwarza pewne zagrożenia. Nie da się ze 100% pewnością stwierdzić kto jest autorem lub nadawcą elektronicznego dokumentu nawet na podstawie źródłowej jego wersji. Dodatkowo istnieje możliwość przechwycenia „podróżującego" przez Internet dokumentu, edycja jego treści i dalej dostarczenie do adresata w zmodyfikowanej postaci. Niewinna z pozoru zmiana treści umowy może spowodować wymierne straty finansowe dla zawierających ją kontrahentów oraz mieć ogromny wpływ na ich dalszą współpracę.

Czym jest podpis elektroniczny?

Podpis elektroniczny – definicja ustawowa (Art. 3 ustawy z dnia 18 września 2001r. o podpisie elektronicznym, Dz. U. Nr 130, Poz. 1450, z dnia 15.11.2001r.):

1. 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.
2. bezpieczny podpis elektroniczny – 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.

Upraszczając - podpis elektroniczny to ogólna nazwa różnych technik potwierdzania autentyczności dokumentu elektronicznego i tożsamości jego autora.
Podpis elektroniczny musi spełnić te same warunki co podpis zwykły, tzn. powinien być trudny lub niemożliwy do podrobienia, stwarzać możliwość weryfikacji i trwale łączyć się z dokumentem. Chodzi o to, aby odbiorca dokumentu miał pewność, że dokument wysłany drogą elektroniczną i podpisany "e-podpisem" pochodzi od konkretnego nadawcy oraz, że treść wiadomości nie uległa zmianie bez jego wiedzy.

Podpis elektroniczny i certyfikat. Czym jest certyfikat?

Pojęcia podpisu elektronicznego i certyfikatu są ze sobą nierozerwalnie związane. Dokumenty elektroniczne podpisuje się elektronicznym podpisem, a certyfikat służy do weryfikacji tego podpisu.

Czym różni się certyfikat kwalifikowany od niekwalifikowanego? Rodzaje podpisu elektronicznego.

Są dwa rodzaje certyfikatów i dwa rodzaje podpisów, których nazwa pochodzi od weryfikujących je certyfikatów. Różnią się one przede wszystkim mocą prawną, a w konsekwencji tego – użytecznością:

I. Podpis elektroniczny kwalifikowany (bezpieczny) – weryfikowany certyfikatem kwalifikowanym.
II. Podpis elektroniczny niekwalifikowany (zwykły) – weryfikowany certyfikatem niekwalifikowanym.

Odpowiednikiem podpisu odręcznego w komunikacji elektronicznej jest elektroniczny podpis kwalifikowany weryfikowany przy użyciu kwalifikowanego certyfikatu. Gwarantuje on, że podpisany nim dokument dotrze do adresata w niezmienionej formie, a każda, nawet przypadkowa zmiana w treści dokumentu będzie zasygnalizowana odbiorcy.
Dzięki umocowaniu prawnemu bezpieczny podpis elektroniczny można wykorzystać np. do rozliczeń z urzędem skarbowym czy podpisywania faktur elektronicznych. Certyfikat kwalifikowany może być używany jedynie do składania/weryfikacji podpisu elektronicznego. Ustawa zabrania używania go do innych celów takich jak logowanie lub szyfrowanie.

Podpis zwykły, weryfikowany przy użyciu certyfikatu niekwalifikowanego, również umożliwia podpisywanie dokumentów elektronicznych. Ma on jednak inne umocowanie prawne - wysłanie jakiegokolwiek dokumentu podpisanego przy użyciu tego certyfikatu niesie ze sobą skutki prawne tylko wtedy, gdy obie strony się na to zgodzą.
Podobnie jak podpis bezpieczny, pozwala on na jednoznaczną identyfikację osoby wysyłającej dokument, jednak z mocy prawa nie jest on równoważny z podpisem własnoręcznym.
W przypadku podpisywania umowy pomiędzy stronami posługującymi się certyfikatami niekwalifikowanymi, umowa musi zawierać zapis o wzajemnym uznaniu takich podpisów oraz identyfikatory ich certyfikatów np. "nr seryjne".
Na mocy ustawy o podpisie elektronicznym, podpis niekwalifikowany nie może być stosowany do kontaktów z urzędami i administracją publiczną. Z tego względu certyfikaty niekwalifikowane są najczęściej wykorzystywane przy podpisywaniu i zabezpieczaniu (szyfrowaniu) poczty elektronicznej. W przeciwieństwie do certyfikatów kwalifikowanych, certyfikaty niekwalifikowane nie posiadają ograniczeń pod względem ich użyteczności.

Zalety wykorzystywania certyfikatów kwalifikowanych:

- możliwość załatwiania spraw urzędowych, biznesowych, cywilno-prawnych za pośrednictwem Internetu oraz skrócenie czasu ich realizacji,
- dostępność urzędów elektronicznych on-line przez 24h/dobę, 7 dni w tygodniu.
- zastąpienie dotychczasowej „dyskietki” w kontaktach z ZUS przez urządzenia, które można podłączyć do standardowych portów dostępnych w każdym komputerze klasy PC (np. USB),
- zabezpieczenie podpisanych dokumentów elektronicznych przed zmianami przez osoby nieupoważnione,

Jak uzyskać certyfikat kwalifikowany?

Certyfikat kwalifikowany może być wydany jedynie osobie fizycznej.

Do wydania certyfikatu kwalifikowanego niezbędne jest potwierdzenie tożsamości osoby ubiegającej się o bezpieczny podpis elektroniczny i wymaga to osobistego stawienia się w punkcie rejestracji lub notarialnego potwierdzenia tożsamości.
W przypadku gdy osoba ubiegająca się o wydanie lub przedłużenie czasu ważności certyfikatu kwalifikowanego posiada już ważny podpis kwalifikowany to może się nim posłużyć w zgłoszeniu certyfikacyjnym.

Certyfikaty kwalifikowane wydawane są wyłącznie przez podmioty świadczące usługi certyfikacyjne (tzw. Centra Certyfikacji - na chwilę obecną trzy w Polsce), wpisane na mocy decyzji ministra gospodarki do rejestru kwalifikowanych podmiotów świadczących usługi certyfikacyjne.

Urząd certyfikacji (centrum certyfikacji). Co to jest?

Urząd certyfikacji (centrum certyfikacji) nazywany też zaufaną stroną trzecią to podmiot świadczący usługi certyfikacyjne, który podejmuje się realizacji zadań związanych z weryfikacją tożsamości subskrybentów. Subskrybent to osoba do której przypisany jest certyfikat kwalifikowany czyli ogólnie mówiąc – osoba posługująca się swoim podpisem elektronicznym. Wszystkie zasady, według których urząd certyfikacji prowadzi swoją działalność zwane są polityką certyfikacji i są opisane w publicznie udostępnionym przez urząd dokumencie.

Jak wspomniano wcześniej, w Polsce certyfikaty kwalifikowane mogą być wydawane jedynie przez podmioty sprawdzone i wpisane do rejestru kwalifikowanych podmiotów prowadzonego przez ministra gospodarki. Podmiot taki uzyskuje miano kwalifikowanego podmiotu świadczącego usługi certyfikacyjne i otrzymuje od głównego narodowego urzędu certyfikacji odpowiednie zaświadczenie certyfikacyjne.

Dzięki hierarchii w strukturze drogi certyfikacji i dzięki zaufaniu bezpośrednio do głównego narodowego urzędu certyfikacji możliwa jest wzajemna weryfikacja certyfikatów kwalifikowanych, które znajdują się w posiadaniu subskrybentów, a które zostały wydane przez różne urzędy certyfikacji.

Znakowanie czasem. Co to jest?

Przy przesyłaniu dokumentów opatrzonych bezpiecznym podpisem elektronicznym istotny jest również czas ich wysłania. Z pomocą przychodzi usługa znakowania czasem. Polega ona na powiązaniu dokumentu z określoną datą (pochodzącą z wiarygodnego źródła) przy użyciu metod kryptograficznych. Pozwala to na precyzyjne określenie czasu złożenia podpisu elektronicznego oraz zaświadcza o istnieniu dokumentu w momencie wskazanym w znaczniku czasu. Uniemożliwia to manipulowanie czasem w obrocie dokumentów i wyklucza wielokrotne wprowadzanie do obiegu tego samego dokumentu elektronicznego. Użycie kwalifikowanego znacznika czasu ma takie same skutki prawne jak data pewna w rozumieniu prawa cywilnego.

Elementy niezbędne do złożenia bezpiecznego podpisu elektronicznego.

Złożenie podpisu elektronicznego wymaga posługiwania się dokumentem w postaci cyfrowej.

Do złożenia bezpiecznego podpisu elektronicznego niezbędne są następujące elementy:

- certyfikat kwalifikowany (zapisany wraz z odpowiednimi kluczami kodującymi na karcie kryptograficznej)
- czytnik kart kryptograficznych
- oprogramowanie podpisujące

Czytnik Kart

Warto tutaj przypomnieć, że podpis elektroniczny to wyłącznie sposób kodowania danych, umożliwiający identyfikację osoby, która go złożyła oraz gwarantujący integralność dokumentu. Sam podpis elektroniczny nie służy do szyfrowania danych.

Oprogramowanie do składnia podpisu kwalifikowanego współpracuje wyłącznie z systemem operacyjnym Microsoft Windows 2000/XP (lub nowszym). Na razie nie jest dostępne oprogramowanie pod systemy Linux lub Mac OS.

Złożenie podpisu elektronicznego i jego późniejsza weryfikacja.

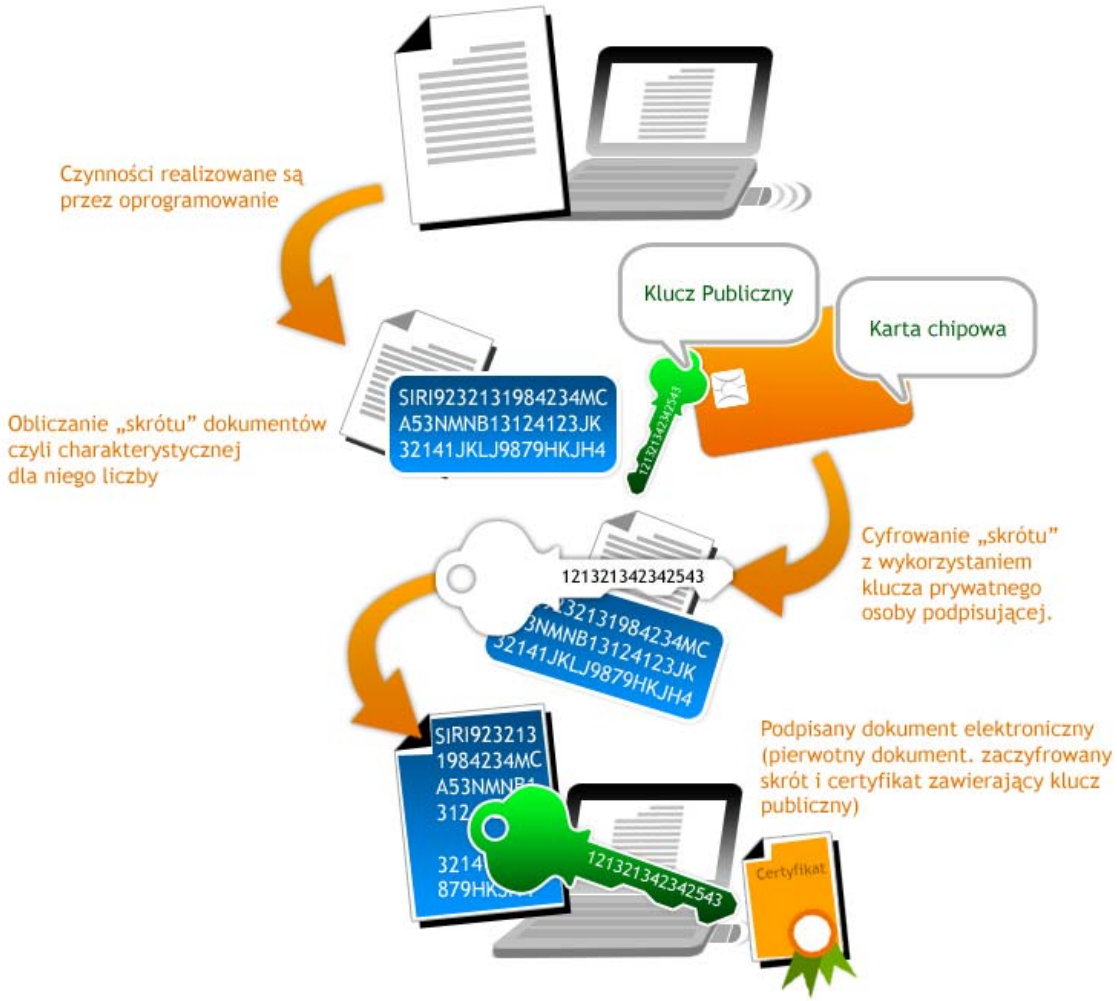
Podpis elektroniczny to właściwie dwa, powiązane ze sobą klucze – publiczny, przekazywany każdemu zainteresowanemu i klucz prywatny, który użytkownik powinien chronić przed ujawnieniem i pozostawić wyłącznie do własnej dyspozycji.

Czynności nazywane złożeniem podpisu oraz weryfikacją podpisu realizowane są przez oprogramowanie.

Podpisanie:

Dokument w postaci cyfrowej, widziany przez nas w zrozumiałej postaci na ekranie komputera jest w jego pamięci zapisany jako ciąg zer i jedynek. Oprogramowanie podpisujące wylicza tzw. skrót dokumentu, czyli charakterystyczną dla danego dokumentu liczbę o określonej długości.

Następnie skrót ten jest szyfrowany przy wykorzystaniu klucza prywatnego osoby podpisującej. W trakcie wykorzystywania klucza prywatnego użytkownik proszony jest o udzielenie zgody na jego użycie przez podanie kodu PIN karty kryptograficznej. Po zaszyfrowaniu skrótu dokument elektroniczny jest już podpisany.
Dokument pierwotny wraz z dołączonym do niego zaszyfrowanym skrótem jest podpisanym dokumentem elektronicznym.



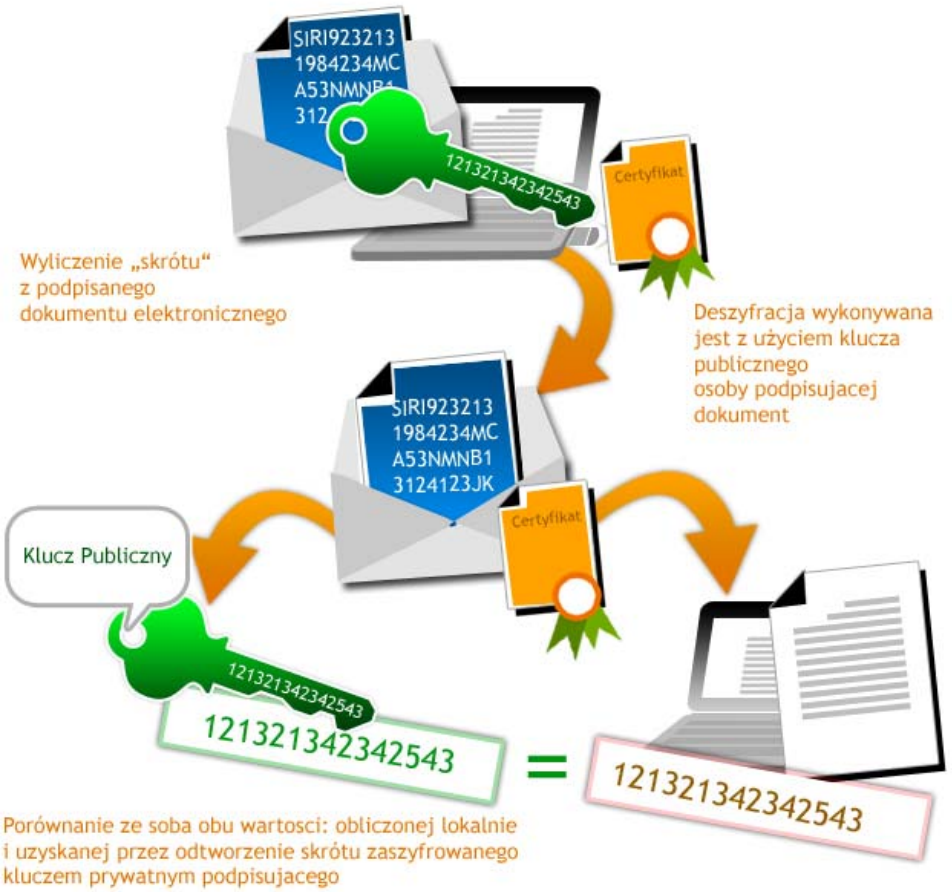
Weryfikacja:

Program odbiorcy podpisanego dokumentu elektronicznego wykonuje następujące czynności:

1. Wylicza skrót z podpisanego dokumentu elektronicznego.
2. Deszyfruje zaszyfrowany skrót będący częścią podpisanego dokumentu elektronicznego (deszyfrowanie wykonywane jest z użyciem klucza publicznego osoby podpisującej dokument)
3. Porównuje ze sobą obie wartości

Jeżeli wartości są jednakowe oznacza to, że dokument jest autentyczny i dotarł do odbiorcy w niezmienionej formie.

Sprawdzenie autentyczności podpisu od strony technologicznej może być realizowane w trybie off-line jednak sprawdzenie ważności certyfikatu weryfikującego podpis wymaga już kontaktu z urzędem certyfikacji.



Weryfikacja ważności certyfikatu realizowana jest następująco:
- w przypadku braku możliwości kontaktu z serwerem wydawcy certyfikatu program użytkownika korzysta z ostatnich posiadanych list certyfikatów unieważnionych i/lub informuje, że nie jest w stanie sprawdzić czy certyfikat używany do podpisu nie został unieważniony
- w przypadku gdy odbiorca jest w stanie połączyć się z serwerem urzędu certyfikacji, program aktualizuje listę certyfikatów unieważnionych lub przesyła do serwera zapytanie o aktualny status certyfikatu.

Ważność certyfikatu.

W myśl art. 21 ustawy z dnia 18 września 2001 r. o podpisie elektronicznym, certyfikat kwalifikowany jest ważny przez okres w nim wskazanym – maksymalnie dwa lata.

Są jednak sytuacje, w których urząd certyfikacji ma prawo
unieważnić certyfikat kwalifikowany przed upływem okresu jego ważności.
Ma to miejsce w następujących przypadkach:

- certyfikat został wydany na podstawie nieprawdziwych lub nieaktualnych danych
- osoba składająca podpis elektroniczny weryfikowany na podstawie tego certyfikatu nie dopełniła obowiązków, o których mowa w art. 15 wspomnianej ustawy - "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"
- zażąda tego osoba składająca podpis elektroniczny lub osoba trzecia wskazana w certyfikacie
- zażąda tego minister właściwy do spraw gospodarki
- osoba składająca podpis elektroniczny utraciła pełną zdolność do czynności prawnych
- podmiot świadczący usługi certyfikacyjne nie dopełnił obowiązków określonych w ustawie
- podmiot świadczący usługi certyfikacyjne zaprzestaje świadczenia usług certyfikacyjnych, a jego praw i obowiązków nie przejmie inny kwalifikowany podmiot

Możliwość unieważnienia certyfikatu kwalifikowanego istnieje w każdym przypadku uzasadnionego podejrzenia, że istnieją przesłanki do tego unieważnienia.
W takiej sytuacji urząd certyfikacji jest zobowiązany niezwłocznie zawiesić certyfikat i nie dłużej niż w przeciągu 7 dni wyjaśnić powstałe wątpliwości. Po upływie tego okresu oraz w przypadku braku możliwości wyjaśnienia powstałych wątpliwości, urząd certyfikacji zobowiązany jest do niezwłocznego unieważnienia certyfikatu kwalifikowanego.
W przypadku braku potwierdzenia przesłanek do unieważnienia certyfikatu, zwieszenie może zostać uchylone.

Certyfikat, który został unieważniony, nie może być ponownie uznany za ważny.

Zgodnie z obowiązującymi przepisami zawieszenie lub unieważnienie certyfikatu nie może nastąpić z mocą wsteczną.

Urząd certyfikacji ma obowiązek niezwłocznego powiadomienia osoby składającej podpis elektroniczny weryfikowany na podstawie certyfikatu kwalifikowanego o jego unieważnieniu lub zawieszeniu.

Każdy podmiot świadczący usługi certyfikacyjne publikuje listę zawieszonych i unieważnionych certyfikatów (lista CRL). Informacje o zawieszeniu lub unieważnieniu certyfikatu są umieszczane na liście nie później niż w ciągu 1 godziny od zawieszenia lub unieważnienia certyfikatu.

Bezpieczeństwo.

Konstrukcja podpisu elektronicznego jest obecnie najbezpieczniejszym sposobem zabezpieczania danych.
Jeśli chodzi o integralność podpisanej wiadomości, w praktyce wygląda to tak, że gdybyśmy chcieli zmienić chociaż jedno słowo lub znak (np. dopisali spację), jest to od razu możliwe do wykrycia. Na dokumencie papierowym zmiana dokonana już po jego podpisaniu jest w praktyce trudna do wykrycia.
Kolejną wadą dokumentów papierowych jest to, że podpis złożony pod dokumentem mało mówi o jego posiadaczu. Jest to ciąg znaków, z którego czasem trudno odczytać imię i nazwisko. W przypadku podpisu elektronicznego, certyfikat zawiera niezbędne dane pozwalające na jednoznaczną identyfikację właściciela podpisu. Liczba informacji zawartych w certyfikacie zależy od jego rodzaju i zastosowania, jednak łatwo zidentyfikować imię i nazwisko oraz NIP lub PESEL posiadacza podpisu.
Ważną rolę odgrywa również procedura weryfikacji danych. Certyfikat kwalifikowany można otrzymać, jedynie po przedstawieniu dokumentów potwierdzających tożsamość osoby ubiegającej się o bezpieczny podpis elektroniczny. Przez to jest on często nazywany elektronicznym odpowiednikiem dowodu osobistego.

W kwestii bezpieczeństwa istnieje istotna różnica pomiędzy obydwoma rodzajami certyfikatów:

Nośnikiem (czyli miejscem przechowywania) certyfikatu kwalifikowanego jest urządzenie kryptograficzne (karta mikroprocesorowa, etoken itp.). Urządzenie takie musi posiadać odpowiedni certyfikat bezpieczeństwa. Certyfikaty kwalifikowane mogą być używane tylko z "bezpiecznymi aplikacjami" czyli takim oprogramowaniem które posiada oświadczenie producenta o zgodności z wymogami ustawy o podpisie elektronicznym i towarzyszących jej rozporządzeń.

Certyfikat niekwalifikowany może być przechowywany na komputerze użytkownika lub na urządzeniu kryptograficznym (karta mikroprocesorowa, etoken itp.). Użytkownik ma pełną dowolność w wyborze nośnika certyfikatu.

Jak wcześniej wspomniano, czynności nazywane złożeniem przez użytkownika podpisu elektronicznego realizowane są przez oprogramowanie. Aplikacja podpisująca, z mocy ustawy, uniemożliwia sfałszowanie podpisu lub zmianę danych przygotowanych do podpisu przez podpisującego na inne przy użyciu wrogiego oprogramowanie takiego jak wirusy, konie trojańskie, robaki sieciowe itp.

Skutki prawne.

Bezpieczny podpis elektroniczny weryfikowany przy pomocy certyfikatu kwalifikowanego jest równoważny pod względem skutków prawnych z podpisem własnoręcznym. Dodatkowo jest on niezaprzeczalny, co oznacza, że nie ma możliwości zaprzeczenia faktu jego złożenia.

Osoba ubiegająca się o bezpieczny podpis elektroniczny jest zobowiązana do podania prawdziwych danych we wniosku o certyfikat kwalifikowany przekazywanym do punktu rejestracji. Musi mieć świadomość odpowiedzialności za szkody będące konsekwencją sfałszowania danych. Z mocy ustawy ma obowiązek nie udostępniania swojego klucza prywatnego (karty kryptograficznej) oraz związanego z nim kodu PIN osobom trzecim. W przypadku naruszenia ochrony klucza prywatnego ma obowiązek powiadomić o tym niezwłocznie wydawcę certyfikatu (urząd certyfikacji).

Dokumenty wymagane do uzyskania podpisu elektronicznego.

Certyfikat kwalifikowany zawsze wydawany jest na osobę fizyczną, a podpis elektroniczny weryfikowany za pomocą tego certyfikatu jest zawsze traktowany jak podpis własnoręczny tej osoby. Każdy certyfikat kwalifikowany obowiązkowo zawiera dane jednoznacznie identyfikujące osobę fizyczną, która jest jego właścicielem-użytkownikiem (tzw. subskrybentem). Dlatego też certyfikat zawsze zawiera obowiązkowo imię, nazwisko oraz PESEL lub NIP.

Certyfikat kwalifikowany zawierający jedynie dane osobowe jest certyfikatem uniwersalnym i może być stosowany we wszystkich kontaktach z administracją publiczną, wszelkimi instytucjami (w tym z ZUS) oraz w relacjach biznesowych.
Osoba posiadająca taki certyfikat i składająca podpis elektroniczny może działać zarówno we własnym imieniu, jak i w imieniu reprezentowanego podmiotu bez konieczności wpisania informacji o tym podmiocie do certyfikatu.

Istnieje także możliwość umieszczenia w certyfikacie kwalifikowanym dodatkowych informacji, takich jak dane reprezentowanego podmiotu. Jest to uzasadnione gdy zakres uprawnień danej osoby fizycznej wynika np. z przepisów prawa (prezydent miasta, burmistrz, wójt). Nie ma natomiast uzasadnienia wpisywania danych o reprezentowanym podmiocie oraz pełnionej roli, gdy szczegółowy zakres uprawnień i pełnomocnictw właściciela certyfikatu nie wynika z tych danych. Zapisana w certyfikacie nazwa podmiotu, w imieniu którego osoba posługująca się nim działa nie daje bowiem informacji o zakresie posiadanych uprawnień.

Wnioskodawca musi w tym przypadku dodatkowo dostarczyć dokumenty potwierdzające dane reprezentowanego podmiotu oraz określające zasady reprezentacji (takie jak np. potwierdzenie nadania NIP, potwierdzenie nadania numeru REGON oraz odpis z KRS/EDG lub odpowiedni Akt Powołania). W związku z koniecznością dokładniejszej weryfikacji tego typu danych, proces wydania jest dłuższy niż w przypadku certyfikatów kwalifikowanych, zawierających jedynie dane osoby fizycznej.

WYKAZ DOKUMENTÓW WYMAGANYCH PRZY ZAKUPIE ZESTAWU Z CERTYFIKATEM KWALIFIKOWANYM UNIWERSALNYM

zawierającym jedynie dane osobowe, zalecanym dla płatników ZUS, do kontaktów z administracją publiczną oraz w relacjach biznesowych

Dane zawarte w certyfikacie	Dane osobowe identyfikujące użytkownika certyfikatu (imię, nazwisko, PESEL lub NIP)
Kto płaci za zestaw?	Sam użytkownik certyfikatu lub podmiot w imieniu którego użytkownik certyfikatu będzie działał (do wyboru w formularzu)
Niezbędne dokumenty do uzyskania certyfikatu	Dowód osobisty lub paszport użytkownika certyfikatu (do wyboru w formularzu)
Dokumenty otrzymane po wypełnieniu formularza	• Umowa z Subskrybentem • Załącznik nr 1 do ww. Umowy • Faktura proforma • Instrukcja dalszego postępowania

WYKAZ DOKUMENTÓW WYMAGANYCH PRZY ZAKUPIE ZESTAWU Z CERTYFIKATEM KWALIFIKOWANYM ZAWIERAJĄCYM DODATKOWE DANE zalecanym dla osoby fizycznej pełniącej funkcje publiczne lub dla pełnomocników firmy

Dane zawarte w certyfikacie	Dane osobowe użytkownika certyfikatu oraz dane reprezentowanego podmiotu.	
Kto płaci za zestaw?	Sam użytkownik certyfikatu lub podmiot w imieniu którego użytkownik certyfikatu będzie działał (do wyboru w formularzu)	
Niezbędne dokumenty do uzyskania certyfikatu	Firmy: • Odpis z KRS* nie starszy niż 6 miesięcy od daty jego wydania lub w przypadku osób prowadzących indywidualną działalność gospodarczą odpis z EDG**, • Potwierdzenie nadania numeru NIP, • Zaświadczenie o numerze identyfikacyjnym REGON, • Pełnomocnictwo (jeżeli osoba występująca o certyfikat nie jest organem danego podmiotu – tzn. nie jest osobą upoważnioną do samodzielnego reprezentowania danej instytucji).	Instytucje publiczne: • Dokument potwierdzający pełnienie funkcji upoważnionej do reprezentowania danego podmiotu (akt powołania / mianowania / wyboru), dokument musi dotyczyć osoby która podpisuje w imieniu danej instytucji pełnomocnictwo dla danego Subskrybenta, • Potwierdzenie nadania numeru NIP, • Zaświadczenie o numerze identyfikacyjnym REGON • Pełnomocnictwo (jeżeli osoba występująca o certyfikat nie jest organem danego podmiotu – tzn. nie jest osobą upoważnioną do samodzielnego reprezentowania danej instytucji).
Dokumenty otrzymane po wypełnieniu formularza	• Umowa z Subskrybentem • Załącznik nr 1 do ww. Umowy • Faktura proforma • Pełnomocnictwo (wymagane od osób występujących w imieniu innych podmiotów lub innych osób fizycznych). • Instrukcja dalszego postępowania	

* KRS - Krajowy Rejestr Sądowy ** EDG - Ewidencja Działalności Gospodarczej

Ważne: Dostarczone dokumenty powinny być oryginałami lub kopiami poświadczonymi za zgodność z oryginałem przez Notariusza lub Radcę Prawnego lub osobę w danym podmiocie upoważnioną do tego typu czynności (zgodnie z dokumentami określającymi zasady reprezentacji).

Do czego w praktyce można wykorzystać podpis elektroniczny?

Teoretycznie wszystkie sprawy urzędowe można już załatwić wykorzystując bezpieczny podpis elektroniczny, ponieważ z mocy ustawy od dnia 1 maja 2008 r. urzędy administracji publicznej muszą umożliwić obywatelom wnoszenie podań i innych dokumentów w postaci elektronicznej. Niestety, w praktyce jeszcze nie wszystkie urzędy administracji publicznej przygotowane są do takiej obsługi interesantów.

Jak wspomniano wcześniej, na mocy ustawy do kontaktów z administracją publiczną może być wykorzystywany wyłącznie podpis elektroniczny weryfikowany przy użyciu certyfikatu kwalifikowanego. Może on służyć między innymi do:

- kontaktów drogą elektroniczną z Zakładem Ubezpieczeń Społecznych (ZUS), np.: podpisania wniosku o wydanie zaświadczenia o niezaleganiu ze składkami na ubezpieczenie społeczne, podpisania deklaracji,
- nadawania mocy prawnej dokumentom w kontaktach prawnych przez Internet (np. upoważnienia elektroniczne w ZUS),
- pozyskiwania wypisów elektronicznych dotyczących wszystkich podmiotów gospodarczych wpisanych do Krajowego Rejestru Sądowego (KRS) (pdi.cors.gov.pl),
- podpisywania urzędowej korespondencji z podmiotami administracji publicznej za pośrednictwem elektronicznej skrzynki podawczej,
- składania e-deklaracji podatkowych (www.e-deklaracje.gov.pl),
- zawierania umów cywilno-prawnych w formie elektronicznej,
- wystawiania faktur w formie elektronicznej,
- uczestniczenia w aukcjach i przetargach elektronicznych (np. www.e-przetarg.pl),
- podpisywania raportów do Generalnego Inspektora Informacji Finansowej (GIIF),
- zgłaszania drogą elektroniczną zbiorów danych osobowych do Generalnego Inspektora Ochrony Danych Osobowych (GIODO),
- składania e-deklaracji do Ubezpieczeniowego Funduszu Gwarancyjnego (UFG).

Pytania i odpowiedzi:

Czy można mieć dwa certyfikaty kwalifikowane?
Oczywiście. Liczba posiadanych certyfikatów nie jest ograniczona przez przepisy, ani przez centrum certyfikacji.

Czy na certyfikacie musi widnieć numer PESEL?
Zgodnie z Ustawą o podpisie elektronicznym obowiązkowym atrybutem zawartym w certyfikacie kwalifikowanym jest numer NIP lub PESEL – do wyboru przez wnioskodawcę.

Co zapewnia certyfikat kwalifikowany?
Certyfikat kwalifikowany zapewnia:

- weryfikację kwalifikowanego (bezpiecznego) podpisu elektronicznego, który jest równoważny z podpisem odręcznym
- ochronę przed zmianą treści dokumentów przez osoby nieuprawnione
- identyfikację osoby składającej podpis elektroniczny pod dokumentem

Czy do bezpiecznego podpisu potrzebna jest karta?
Tak, do złożenia podpisu kwalifikowanego niezbędna jest mikroprocesorowa karta kryptograficzna na której znajdują się: klucz prywatny, klucz publiczny oraz certyfikat kwalifikowany.

Co to jest lista certyfikatów unieważnionych?
Lista certyfikatów unieważnionych CRL jest elektronicznym dokumentem zawierającym numery seryjne zawieszonych lub unieważnionych certyfikatów wraz z podanymi datami i przyczynami ich zawieszenia lub unieważnienia.

Czy podpis elektroniczny będzie obowiązkowy?
Na mocy ustawy z 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (Dz.U. nr 64, poz. 565 z późn. zm.) od 21 lipca 2008 r. wszystkie dokumenty elektroniczne przekazywane do ZUS przez firmy zatrudniające więcej niż pięć osób powinny być opatrzone bezpiecznym e-podpisem.

Czy w kontaktach z ZUS nadal będą ważne deklaracje papierowe?
Od 21 lipca 2008 r. nadal w kontaktach z ZUS będą funkcjonowały deklaracje w wersji papierowej, jednak możliwość posługiwania się nimi będą miały tylko firmy zatrudniające do pięciu osób. Przedsiębiorstwa zatrudniające więcej osób są zobligowane do wysyłania deklaracji do ZUS wyłącznie w formie elektronicznej opatrując je bezpiecznym podpisem elektronicznym.

Czy biuro rachunkowe może posiadać jeden podpis elektroniczny i wykorzystywać go do rozliczania wszystkich klientów, czy też konieczny jest zakup osobnych podpisów dla każdego klienta?
Wystarczy aby biuro rachunkowe zaopatrzyło się wyłącznie w jeden certyfikat kwalifikowany dla jednego ze swoich pracowników. Osoba ta będzie swoim certyfikatem podpisywała dokumenty w imieniu wszystkich rozliczanych firm.