

## FAQ – aspekty prawne, teoria

### 1. Co to jest podpis elektroniczny?

Zgodnie z art.3 Ustawy z dnia 18 września 2001 r. o podpisie elektronicznym:

*Podpis elektroniczny to 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.*

Podpis elektroniczny porównywany jest do podpisu własnoręcznego. Ustawa o podpisie elektronicznym wprowadza pojęcie bezpiecznego podpisu elektronicznego jako równoważnego do podpisu własnoręcznego.

Zgodnie z art.3 Ustawy o podpisie elektronicznym:

*Bezpieczny podpis elektroniczny to podpis który:*

- *jest przyporządkowany wyłącznie do osoby składającej ten podpis*
- *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*
- *jest powiązany z danymi, do których został dołączony, w taki sposób, że jakakolwiek późniejsza zmiana tych danych jest rozpoznawalna.*

### 2. Co to jest certyfikat?

Zgodnie z art.3 Ustawy z dnia 18 września 2001 r. o podpisie elektronicznym

*Certyfikat 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.*

Certyfikat cyfrowy jest wirtualnym odzwierciedleniem dowodu osobistego w rzeczywistości. Wiąże on tożsamość osoby widniejącej w certyfikacie z kluczami (publicznym i prywatnym) tejże osoby. Tożsamość weryfikowana jest przez Centrum Certyfikacji, które tworzy klucze oraz wystawia certyfikat.

Certyfikat cyfrowy wykorzystywany jest w celu weryfikacji podpisu elektronicznego. Bezpieczny podpis elektroniczny weryfikowany jest przy pomocy certyfikatu kwalifikowanego. Zgodnie z art. 3 Ustawy o podpisie elektronicznym

*Kwalifikowany certyfikat to certyfikat spełniający warunki określone w ustawie, wydany przez kwalifikowany podmiot świadczący usługi certyfikacyjne, spełniający wymogi określone w ustawie.*

### 3. Co to jest bezpieczne urządzenie do składania podpisu elektronicznego?

*Bezpieczne urządzenie jest to urządzenie służące do składania podpisu elektronicznego spełniające wymagania określone w ustawie.*

Bezpieczne urządzenie służące do składania podpisu elektronicznego powinno co najmniej:

- 1) uniemożliwiać pozyskiwanie danych służących do składania podpisu lub poświadczenia elektronicznego,

- 2) nie zmieniać danych, które mają zostać podpisane lub poświadczane elektronicznie, oraz umożliwić przedstawienie tych danych osobie składającej podpis elektroniczny przed chwilą jego złożenia,
- 3) gwarantować, że złożenie podpisu będzie poprzedzone wyraźnym ostrzeżeniem, że kontynuacja operacji będzie równoznaczna ze złożeniem podpisu elektronicznego,
- 4) zapewniać łatwe rozpoznawanie istotnych dla bezpieczeństwa zmian w urządzeniu do składania podpisu lub poświadczenia elektronicznego.

#### **4. Co to jest podmiot świadczący usługi certyfikacyjne (Centrum Certyfikacji)?**

Jest to podmiot zajmujący się świadczeniem usług certyfikacyjnych m.in. wydawaniem certyfikatów i świadczeniem usługi znakowania czasem. Przykładem takiego podmiotu jest Sigillum Polskie Centrum Certyfikacji Elektronicznej.

#### **5. Co to jest usługa znakowania czasem?**

Zgodnie z art. 3 Ustawy o podpisie elektronicznym:

*Znakowanie czasem to usługa polegająca na dołączaniu do danych w postaci elektronicznej logicznie powiązanych z danymi opatrzonymi podpisem lub poświadczeniem elektronicznym, oznaczenia czasu w chwili wykonania tej usługi oraz poświadczenia elektronicznego tak powstałych danych przez podmiot świadczący tę usługę.*

Usługa ta pozwala oznaczyć dokument elektroniczny wiarygodnym czasem, który według Ustawy o podpisie elektronicznym stanowi „datę pewną” w rozumieniu przepisów Kodeksu Cywilnego. W przypadku tradycyjnych dokumentów czas złożenia podpisu ma znaczenie w większości umów cywilno-prawnych, dokumentach rozliczeniowych i w różnorodnych transakcjach. Analogiczną rolę odgrywa znacznik czasu, w przypadku gdy mamy do czynienia z elektronicznym obiegiem dokumentów.

#### **Usługi certyfikacyjne a bezpieczeństwo**

#### **6. Jakie funkcje można realizować przy użyciu certyfikatu kwalifikowanego?**

Certyfikat kwalifikowany służy **tylko i wyłącznie** do złożenia bezpiecznego podpisu elektronicznego pod określonym dokumentem elektronicznym. W przypadku użycia certyfikatów kwalifikowanych niezbędne jest wykorzystanie dedykowanego oprogramowania umożliwiającego składanie podpisów elektronicznych zgodnie z Ustawą o podpisie elektronicznym i odpowiednim do niej Rozporządzeniem.

**Niemożliwe** jest wykorzystanie certyfikatów kwalifikowanych w powszechnie używanym oprogramowaniu biurowym i uzyskanie oczekiwanej funkcjonalności. Wynika to jednoznacznie z ograniczeń technicznych i prawnych jakie zostały zamieszczone w przepisach wykonawczych.

#### **7. Jakie funkcje można realizować przy użyciu certyfikatu komercyjnego?**

Certyfikat komercyjny ma szersze zastosowanie niż certyfikat kwalifikowany. Nie można jednak przy jego użyciu zrealizować bezpiecznego podpisu elektronicznego. Można natomiast:

- szyfrować i podpisywać pocztę elektroniczną,
- logować się do systemów informatycznych,
- podpisywać dokumenty wykorzystując funkcje popularnego oprogramowania biurowego,

- i wiele innych.

## **Aspekty prawne**

### **8. Jakie skutki prawne wiążą się ze złożeniem bezpiecznego podpisu elektronicznego?**

Bezpieczny podpis elektroniczny weryfikowany przy pomocy kwalifikowanego certyfikatu wywołuje skutki prawne określone ustawą, jeżeli został złożony w okresie ważności tego certyfikatu. Zgodnie z art. 5 ust. 2 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. Bezpieczny podpis elektroniczny weryfikowany przy pomocy ważnego kwalifikowanego certyfikatu stanowi dowód tego, że został on złożony przez osobę określoną w tym certyfikacie jako składająca podpis elektroniczny. Dodatkowo zgodnie z art. 78. § 2 Kodeksu Cywilnego oświadczenie woli złożone w postaci elektronicznej opatrzone bezpiecznym podpisem elektronicznym weryfikowanym przy pomocy ważnego kwalifikowanego certyfikatu jest równoważne formie pisemnej.

### **9. Jakie są skutki stosowania usługi znakowania czasem?**

Zgodnie z art. 7 ust. 2 znakowanie czasem przez kwalifikowany podmiot świadczący usługi certyfikacyjne wywołuje w szczególności skutki prawne daty pewnej w rozumieniu przepisów Kodeksu Cywilnego.

### **10. Gdzie można się dowiedzieć więcej o certyfikatach cyfrowych?**

Podstawowym dokumentem, z którym warto się zapoznać jest Ustawa z dnia 18 września 2001 r. o podpisie elektronicznym. Ponadto wiele użytecznych informacji umieszczonych jest na stronie internetowej Sigillum PCCE [www.sigillum.pl](http://www.sigillum.pl).

## **Sigillum PCCE**

### **11. Co to jest Sigillum PCCE**

Sigillum PCCE jest podmiotem świadczącym usługi certyfikacyjne w ramach Polskiej Wytwórni Papierów Wartościowych S.A.

Zadaniem Sigillum PCCE jest pełnienie roli zaufanej trzeciej strony we wszelkiego rodzaju transakcjach elektronicznych, realizowane poprzez wydawanie certyfikatów cyfrowych i świadczenie usług związanych z infrastrukturą klucza publicznego.

Działalność Sigillum PCCE umocowana jest na Ustawie o podpisie elektronicznym oraz standardach polskich i międzynarodowych, co zostało sprawdzone przez audyt Ministerstwa Gospodarki i potwierdzone wpisem do Rejestru Kwalifikowanych Podmiotów Świadczących Usługi Certyfikacyjne pod pozycjami 3 i 5 ([www.centrastr.pl](http://www.centrastr.pl)).

## **Usługi Sigillum PCCE**

### **12. Jakie usługi oferuje Sigillum PCCE?**

Sigillum PCCE oferuje dla swoich klientów certyfikaty kwalifikowane zgodnie z Ustawą o podpisie elektronicznym oraz certyfikaty komercyjne dostosowane do poszczególnych grup klientów oraz operacji wykonywanych przy ich zastosowaniu. Ponadto Sigillum PCCE świadczy usługę znakowania czasem.

### 13. Co otrzymuje Subskrybent w zestawie do podpisu elektronicznego?

**Zestaw M** do podpisu elektronicznego Sigillum PCCE składa się z:

- certyfikat kwalifikowany Sigillum TOP (do kwalifikowanego podpisu),
- karta kryptograficzna (z kluczem prywatnym),
- czytnik do kart oraz oprogramowanie CryptoCard Suite do czytnika i karty,
- oprogramowanie do składania bezpiecznego podpisu.

Komponent techniczny (w postaci karty kryptograficznej), oprogramowanie CryptoCard Suite oraz aplikacja do składania bezpiecznego podpisu stanowią bezpieczne urządzenie do składania podpisu elektronicznego. Bezpieczne urządzenia spełnia szereg kryteriów bezpieczeństwa i funkcjonalności określonych w Ustawie o podpisie elektronicznym oraz związanych z nią rozporządzeniach.

**Karta kryptograficzna** (mikroprocesorowa) jest nośnikiem certyfikatu Subskrybenta wraz z przywiązanymi do niego kluczami (prywatnym i publicznym). Karta kryptograficzna zabezpieczona jest kodem PIN, który zna tylko Subskrybent. Mechanizmy zabezpieczające karty kryptograficznej uniemożliwiają niepowołany dostęp do klucza prywatnego.

**Czytnik kart kryptograficznych** jest urządzeniem dołączanym do komputera np. przez port USB lub RS 232, które wraz z zainstalowanym oprogramowaniem umożliwia odczyt danych zawartych na karcie kryptograficznej.

**Oprogramowanie do składania bezpiecznego podpisu** pomaga użytkownikowi złożyć podpis elektroniczny oraz dokonać weryfikacji podpisu.

### 14. Co to jest Repozytorium Sigillum PCCE?

Sigillum PCCE udostępnia bezpłatnie Repozytorium (czyli dostępną on-line bazę danych) na stronie internetowej pod adresem [www.sigillum.pl](http://www.sigillum.pl). Można tam znaleźć obowiązujące wersje Polityk i Regulaminów certyfikacji, aktualne listy unieważnionych certyfikatów (tzw. CRL), certyfikaty osób, które wyraziły zgodę na ich publikację w Repozytorium, podstawową wiedzę o podpisie elektronicznym oraz wiele innych informacji.

### ***Używanie certyfikatów Sigillum PCCE***

#### 15. Czy adres poczty elektronicznej można zmienić w okresie ważności certyfikatu?

Nie, po wygenerowaniu certyfikatu nie można wprowadzać już żadnych zmian w treści certyfikatu. W celu zmiany danych w treści certyfikatu należy wystąpić z wnioskiem o wystawienie kolejnego certyfikatu

#### 16. Kiedy należy nadać/zmienić kod osobisty w certyfikacie, tzw. kod PIN ?

Kody PIN należy nadać/zmienić przed pierwszym użyciem klucza prywatnego związanego z certyfikatem. Kodu nie należy ujawniać osobom trzecim

#### 17. Na czym polega proces unieważnienia, zawieszenia i uchylecia zawieszenia certyfikatu?

Certyfikat ważny jest przez okres wskazany w jego treści. Cykl życia certyfikatu może zostać skrócony przez unieważnienie certyfikatu. Odbywa się ono zgodnie z zapisami w odpowiedniej Polityce certyfikacji. Najczęściej powodem jest zgubienie bądź kradzież karty

lub zmiana danych zawartych w certyfikacie. Unieważnienie certyfikatu jest procesem nieodwracalnym.

Proces czasowym związanym z certyfikatem jest jego zawieszenie. Maksymalny okres na jaki może zostać zawieszony certyfikat to 7 dni. W tym czasie można uchylić zawieszenia certyfikatu. W przeciwnym przypadku certyfikat zostanie unieważniony.

### **18. Czy po okresie ważności certyfikatu istnieje możliwość odnowienia certyfikatu?**

Tak, jest możliwe odnowienie certyfikatu. Odnowienie wiąże się z podpisaniem kolejnej umowy o świadczenie usług certyfikacyjnych oraz wygenerowaniem nowego certyfikatu.

### **19. Jakie dane zawiera certyfikat?**

Do najważniejszych danych zgromadzonych w certyfikacie należą:

- Imię i nazwisko właściciela certyfikatu – np. Jan Kowalski;
- Nazwa firmy – jeśli certyfikat ma być używany w ramach działalności firmy;
- Adres firmy;
- Wystawca certyfikatu – np. Sigillum PCCE;
- Termin ważności certyfikatu – np. ważny od 12.12.2006 do 12.12.2007;
- Numer PESEL lub NIP;
- Adres e-mail;
- Klucz publiczny;
- Przeznaczenie certyfikatu – np. niezaprzeczalność, szyfrowanie poczty, podpisywanie poczty, logowanie;
- Inne – np.: numer seryjny, algorytm odcisku palca (np. SHA1), identyfikator polityki certyfikacji;

### **20. Co to jest lista CRL?**

Lista CRL gromadzi dane o certyfikatach, które uległy odwołaniu. Odwołanie certyfikatu następuje z różnych przyczyn – zwykle na wniosek właściciela certyfikatu, choć w niektórych przypadkach odwołanie certyfikatu może nastąpić na wniosek Urzędu Certyfikacji.

### **21. Czy podpis elektroniczny może być wydrukowany?**

Logika podpisu elektronicznego nakierowana jest na potwierdzanie integralności dokumentów w formie elektronicznej i w związku z tym nie funkcjonuje ona dla dokumentów drukowanych. Dlatego podpisu elektronicznego się nie drukuje, ani nie przedstawia w postaci graficznej.

### **22. Jak w skrócie przebiega podpisywanie elektroniczne dokumentów?**

W najprostszym przypadku podpisanie elektroniczne dokumentu sprowadza się do:

- wskazania dokumentu i wywołanie programu podpisującego
- wybranie certyfikatu używanego do podpisu
- wprowadzenie kodu PIN do odpowiedniej struktury karty kryptograficznej.

Całość, w zależności od używanego oprogramowania, uzupełniają komunikaty o statusie wykonywanych operacji i jej powodzeniu/niepowodzeniu, ew. dodanie dodatkowych opcji – np. znakowania czasem, czy szyfrowania.

### **23. Co to jest wielopodpis?**

Termin „wielopodpis” lub „podpis wielokrotny” używany jest w dwóch kontekstach:

- jako synonim kontrasygnaty, czyli umieszczania wielu różnych podpisów (podpisów elektronicznych różnych osób) pod jednym dokumentem
- jako możliwość podpisywania na raz wielu dokumentów – czyli podpisywanie tych dokumentów za pomocą pojedynczego wprowadzenia kodu PIN (standardową opcją jest wprowadzanie PIN-u dla każdego podpisywanego dokumentu osobno) – w przypadku korzystania z oprogramowania Sigillum, wielopodpis w tym sensie jest możliwy jedynie przy użyciu programu Sigillum Sign Pro (wersja darmowa oprogramowania – Sigillum Sign – wymaga wpisywania kodu PIN osobno podczas podpisywania każdego dokumentu).

Wybór właściwego znaczenia terminu wynika zwykle z kontekstu wypowiedzi.

**Więcej informacji możecie Państwo uzyskać pod numerem infolinii: +48 22 464 79 79**