



Tradiss Piotrowski-Iwaniuk spółka jawna  
40-403 Katowice, ul. Oswobodzenia 1  
telefon: 032 757 25 71, faks: 032 757 28 32  
e-mail: epodpis@tradiss.pl  
internet: www.tradiss.pl

Oprogramowanie - Komputery - Integracja systemowa

## Bezpieczny podpis elektroniczny dla płatników ZUS

Po 21 lipca 2008 roku przedsiębiorstwa prowadzące elektroniczne rozliczenia z ZUS, i zatrudniające więcej niż 5 pracowników, nie otrzymują od ZUS niekwalifikowanego certyfikatu do podpisywania dokumentów. Od tego dnia są zobowiązane nabyć tzw. certyfikat kwalifikowany (czyli taki bezpieczny podpis elektroniczny, który prawo zrównuje z podpisem odręcznym).

Zgodnie z ustawą z 13 czerwca 2008 r. o zmianie ustawy o informatyzacji działalności podmiotów realizujących zadania publiczne (Dz. U. nr 127, poz. 817) niekwalifikowane certyfikaty wydane płatnikom przez ZUS przed dniem 21 lipca 2008 roku będą ważne jeszcze przez 12 miesięcy. Po upływie terminu ważności certyfikatu niekwalifikowanego przedsiębiorcy muszą korzystać tylko z certyfikatów kwalifikowanych (bezpiecznych e-podpisów).

Na potrzeby obsługi programu Płatnik, i co najważniejsze, podpisywania deklaracji do ZUS certyfikatem kwalifikowanym, oferujemy zestaw, w skład którego wchodzi:

- certyfikat kwalifikowany ważny 1 rok lub 2 lata;
- karta kryptograficzna;
- czytnik kart kryptograficznych.

### **Cena zestawu z certyfikatem jednorocznym - 245 zł netto\*, z dwuletnim - 298 zł netto\***

Dodatkowo otrzymają Państwo najlepszą obecnie pod względem funkcjonalności aplikację do składania i weryfikacji podpisów elektronicznych SZAFIR.

Moc prawna bezpiecznego podpisu elektronicznego pozwala stosować go również w innych, niż Zakład Ubezpieczeń Społecznych, obszarach. Możliwości zastosowania tej technologii do dokumentów elektronicznych są w praktyce nieograniczone. Wiele aktów prawnych, obok tradycyjnej formy podpisu, pozwala praktycznie wykorzystywać bezpieczny podpis elektroniczny weryfikowany przy pomocy kwalifikowanych certyfikatów. Istnieje wiele dziedzin zastosowania bezpiecznych podpisów elektronicznych i kwalifikowanych certyfikatów: ochrona zdrowia, gospodarka (e-faktura), przetargi i aukcje, KRS, urzędy administracji publicznej, Generalny Inspektor Ochrony Danych Osobowych, Generalny Inspektor Informacji Finansowej czy Urząd Skarbowy.

Rozporządzenie z dnia 19 grudnia 2007 r. stanowi, że z dniem 1 stycznia 2008 r. składać można do fiskusa 32 rodzaje deklaracji, m.in. VAT-7, VAT-UE, CIT-8. Z dniem 1 kwietnia 2008 r. zakres ten został rozszerzony o kolejne 12 deklaracji, m.in.: PIT-37, PIT-36, PIT-38, PIT-36L, PIT/O, PIT/D. Następnym etapem to 1 lipca 2008 r., kiedy można składać dodatkowe 17 deklaracji, m.in. PIT-11 oraz 1 stycznia 2009 r. - kolejne 20 deklaracji, m.in. PIT-40, PIT-28.

\* Do cen należy doliczyć podatek VAT.  
Ceny nie zawierają ewentualnych kosztów instalacji, szkolenia oraz dojazdu.

#### **Kontakt:**

**Tradiss**, 40-403 Katowice, ul. Oswobodzenia 1,  
telefon: (032) 757 25 71, faks: (032) 757 28 32,  
e-mail: epodpis@tradiss.pl

Więcej informacji... zapraszamy na [www.tradiss.pl](http://www.tradiss.pl)



Tradiss Piotrowski-Iwaniuk spółka jawna  
40-403 Katowice, ul. Oswobodzenia 1  
telefon: 032 757 25 71, faks: 032 757 28 32  
e-mail: epodpis@tradiss.pl  
internet: www.tradiss.pl

Oprogramowanie - Komputery - Integracja systemowa

## Podpis elektroniczny – Informacja ogólna

**e-podpis** czyli **podpis elektroniczny** to techniczny sposób potwierdzania autentyczności dokumentu i tożsamości nadawcy na dokumencie przesyłanym drogą elektroniczną. Istnieją dwa rodzaje podpisów elektronicznych: zwykły i bezpieczny. **Bezpieczny podpis elektroniczny** weryfikowany za pomocą ważnego kwalifikowanego certyfikatu ma, zgodnie z ustawą, moc prawną taką samą, jak podpis odręczny. **Zwykły podpis elektroniczny** jest wiążący prawnie jedynie na podstawie umów cywilnych pomiędzy podmiotami je stosującymi i jest używany wówczas, jeżeli prawo nie wymaga dla danej czynności formy pisemnej. Tak więc, nie powinno się odmawiać zwyktemu podpisowi skuteczności prawnej czyli traktowania go jako dowodu..

### Podstawowe właściwości podpisu elektronicznego:

- Unikalność - każdy elektroniczny dokument posiada unikalny podpis cyfrowy ściśle z nim związany.
- Integralność - jakakolwiek zmiana dokumentu podpisanego cyfrowo zostanie natychmiast wykryta w momencie weryfikacji podpisu.
- Niezaprzeczalność - tylko osoba posiadająca klucz prywatny korespondujący z kluczem publicznym wykorzystanym do weryfikacji podpisu mogła wygenerować podpis pod dokumentem.

**Certyfikat kwalifikowany** jest wystawiony przez urząd certyfikacyjny, który znajduje się na liście Ministra Gospodarki. Certyfikat kwalifikowany to certyfikat klucza publicznego zgodny z wymaganiami określonymi w Ustawie o podpisie elektronicznym z 18 września 2001 roku. Certyfikat jest to plik, podpisany cyfrowo przez podmiot świadczący usługi certyfikacyjne, który zawiera dane o właścicielu certyfikatu, jego klucz publiczny oraz informacje, kto wystawił ten certyfikat, a tym samym poświadcza prawdziwość zawartych w nim danych.

**Konstrukcja podpisu elektronicznego** wykorzystuje technikę szyfrowania z kluczem publicznym. Podstawą działania szyfrów z kluczem publicznym są dwa klucze: klucz prywatny oraz klucz publiczny. Tak, jak wskazują nazwy kluczy, klucz publiczny jest udostępniany wszystkim osobom, z którymi kontaktuje się dana osoba, zaś klucz prywatny, dla zachowania bezpieczeństwa systemu, musi pozostać pod wyłączną kontrolą jego właściciela. Istotną własnością wymienionych kluczy jest to, iż praktycznie niemożliwe jest odgadnięcie klucza prywatnego na podstawie znajomości klucza publicznego. Własność ta gwarantuje, iż podpisany dokument, który został poprawnie zweryfikowany kluczem publicznym mógł być stworzony tylko przez posiadacza klucza prywatnego.

**Bezpieczny podpis elektroniczny** w rozumieniu ustawy to podpis elektroniczny, który:

- jest przyporządkowany wyłącznie do osoby składającej ten podpis,
- jest sporządzony za pomocą podlegających wyłącznej kontroli osoby składającej podpis elektroniczny bezpiecznych urządzeń służących do składania podpisu elektronicznego i danych służących do składania podpisu elektronicznego (klucza prywatnego),
- jest powiązany z danymi, do których został dołączony w taki sposób, że jakakolwiek późniejsza zmiana tych danych jest rozpoznawalna.

**SZAFIR** to system zarządzania certyfikatami kluczy publicznych stworzony przez **Krajową Izbę Rozliczeniową S.A.** W ramach tego systemu KIR S.A. świadczy różnego rodzaju usługi związane z [podpisem elektronicznym](#). Krajowa Izba Rozliczeniowa S.A. jest jedynym w Polsce centrum certyfikacji o tak znaczącym doświadczeniu w dziedzinie infrastruktury klucza publicznego. Od wielu lat certyfikaty wydawane przez KIR S.A. są wykorzystywane do uwierzytelniania transakcji przesyłanych w systemie rozliczeń międzybankowych ELIXIR. Wiedza zdobyta między innymi w tej dziedzinie jest teraz z powodzeniem wykorzystywana przy świadczeniu usługi certyfikacji kluczy w ramach systemu SZAFIR.

Więcej informacji... zapraszamy na [www.tradiss.pl](http://www.tradiss.pl)



TECHNIKA KOMPUTEROWA

Tradiss Piotrowski-Iwaniuk spółka jawna  
40-403 Katowice, ul. Oswobodzenia 1  
telefon: 032 757 25 71, faks: 032 757 28 32  
e-mail: epodpis@tradiss.pl  
internet: www.tradiss.pl

Oprogramowanie - Komputery - Integracja systemowa

## Cennik zestawów, urządzeń i usług certyfikacyjnych

Zestawy z certyfikatem kwalifikowanym (z czytnikiem)	Ważność	Cena netto
Certyfikat kwalifikowany, certyfikat niekwalifikowany (na życzenie klienta), karta kryptograficzna CryptoCard multiSIGN z oprogramowaniem do obsługi karty, czytnik kart kryptograficznych SCR 3310, licencja na aplikację SZAFIR®.	1 rok	245 zł
	2 lata	298 zł

Zestawy z certyfikatem kwalifikowanym (bez czytnika)	Ważność	Cena netto
Certyfikat kwalifikowany, certyfikat niekwalifikowany (na życzenie klienta), karta kryptograficzna CryptoCard multiSIGN z oprogramowaniem do obsługi karty, licencja na aplikację SZAFIR®.	1 rok	199 zł
	2 lata	252 zł

Certyfikaty kwalifikowane i niekwalifikowane	Ważność	Cena netto
Kwalifikowany certyfikat	1 rok	190 zł
	2 lata	260 zł
Odnowienie kwalifikowanego certyfikatu dla danego subskrybenta	1 rok	95 zł
	2 lata	130 zł
Niekwalifikowany certyfikat zapisany na karcie	1 rok	120 zł
Niekwalifikowany certyfikat zapisany w pliku	1 rok	90 zł
Odnowienie niekwalifikowanego certyfikatu dla danego subskrybenta	1 rok	60 zł
Niekwalifikowany certyfikat dla serwerów i urządzeń sieciowych	1 rok	370 zł
	2 lata	490 zł
Odnowienie niekwalifikowanego certyfikatu dla danego serwera lub urządzenia sieciowego	1 rok	330 zł
	2 lata	410 zł

Urządzenia kryptograficzne i oprogramowanie	Cena netto
Karta CryptoCard multiSIGN z oprogramowaniem CryptoCard Suite (12 miesięczna gwarancja, nadruk na karcie danych właściciela: imię, nazwisko, nazwa firmy)	99 zł
Czytnik kart elektronicznych SCR 3310 (podłączany do portu USB)	89 zł
Token USB (karta CryptoCard multiSign + czytnik Omnikey Cardman 6121)	189 zł
Licencja na aplikację SZAFIR służącą do składania i weryfikowania bezpiecznych podpisów elektronicznych (także strumieniowo)	99 zł
Karta do logowania/zabezpieczenia komputera CryptoCard LOGON	73 zł

Inne usługi	Cena netto
Unieważnienie, zawieszenie certyfikatu	0 zł
Zmiana statusu certyfikatu po zawieszeniu	0 zł
Wsparcie techniczne dla aplikacji SZAFIR® na kolejne 12 miesięcy	20 zł

Do podanych cen należy doliczyć podatek VAT. Cenniki obowiązują od 30.04.2009.  
Wymiana wadliwych kart, czytników i nośników na poprawnie funkcjonujące jest bezpłatna.  
W przypadku, gdy wada dotyczy karty, nowa karta oraz nowy certyfikat wydawane są bezpłatnie.  
Ceny nie zawierają ewentualnych kosztów instalacji, szkolenia oraz dojazdu.  
Powyższe cenniki nie stanowią oferty handlowej w rozumieniu prawa handlowego.