

Informacje dla osób odbierających certyfikat kwalifikowany na karcie do kwalifikowanego podpisu elektronicznego:

1. Usługa zaufania polegająca na wystawieniu kwalifikowanego certyfikatu jest świadczona przez Enigma Systemy Ochrony Informacji Sp. z o.o., (zwana dalej „Enigma”), pod marką CenCert. Usługa jest świadczona na podstawie *Rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 910/2014 (eIDAS) oraz ustawy z dnia 5 września 2016 r. o usługach zaufania oraz identyfikacji elektronicznej.*
2. Kwalifikowany certyfikat wystawiany przez Enigma służy do składania i weryfikacji kwalifikowanych podpisów elektronicznych.
3. Zasady posługiwania się kwalifikowanym certyfikatem, w tym prawa i obowiązki Enigma oraz Subskrybenta, określone są w *Polityce dla kwalifikowanych usług zaufania*, dostępnej na stronie CenCert (www.cencert.pl). W szczególności rozdział 4.5.2 polityki opisuje obowiązki Subskrybenta związane z zabezpieczeniem klucza prywatnego i procesu składania podpisu, a rozdział 9.8 określa ograniczenia odpowiedzialności CenCert.
4. Kwalifikowany podpis elektroniczny ma skutek prawny równoważny podpisowi własnoręcznemu (art. 25.2 eIDAS). Kwalifikowany podpis elektroniczny oparty na kwalifikowanym certyfikacie wydanym w jednym państwie członkowskim jest uznawany za kwalifikowany podpis elektroniczny we wszystkich pozostałych państwach członkowskich (art. 25.3 eIDAS).
5. Kartą elektroniczną z kwalifikowanym certyfikatem może się posługiwać wyłącznie Subskrybent (osoba fizyczna), dla którego certyfikat został wydany. Posługiwanie się cudzą kartą w celu składania podpisów elektronicznych jest czynem karalnym (art. 40 ust. 1 ustawy o usługach zaufania).
6. Subskrybent może w każdej chwili złożyć wniosek o unieważnienie certyfikatu. W przypadku, gdy do certyfikatu są wpisane także dane firmy/instytucji, certyfikat może być unieważniony także przez tę firmę/instytucję. Szczegóły dotyczące procedury unieważnienia certyfikatu są dostępne na stronie CenCert (www.cencert.pl). Zgodnie z rozporządzeniem eIDAS, CenCert ma obowiązek unieważnić certyfikat nie później niż w ciągu 24 godzin od otrzymania prawidłowego wniosku.
7. Subskrybent powinien unieważnić swój certyfikat w każdym przypadku, gdy zagrożone jest bezpieczeństwo certyfikatu lub związanych z nim kluczy zapisanych na karcie procesorowej (np. gdy utracił kartę lub gdy dostęp do karty ma osoba nieupoważniona).
8. Karta elektroniczna z certyfikatem jest zabezpieczona kodem PIN i PUK nadanym samodzielnie przez Subskrybenta. **ZAŁECAMY ZAPISANIE NADANYCH KODÓW PIN/PUK W BEZPIECZNYM MIEJSCU. Po trzykrotnym podaniu błędnego kodu PIN, kod zostaje zablokowany.** Zablokowany PIN można odblokować i zmienić przy pomocy kodu PUK. W przypadku wprowadzania błędnego kodu PUK, ten kod również zostanie zablokowany. Liczba dozwolonych prób dla kodu PUK zależy od typu karty i jest określona w mailu z kodem aktywacyjnym do karty. **Ze względów bezpieczeństwa, CenCert nie posiada kodów PIN i PUK Subskrybenta, zabezpieczających klucz do podpisu. Po zablokowaniu kodów PIN i PUK karta jest bezużyteczna, a wada taka nie podlega gwarancji.**
9. Subskrybent jest zobowiązany do sprawdzenia danych w certyfikacie przed jego pierwszym użyciem. W przypadku błędnych danych – jest zobowiązany do niezwłocznego kontaktu z CenCert w celu unieważnienia certyfikatu i otrzymania nowego, z poprawnymi danymi. Składanie podpisów przy użyciu certyfikatu zawierającego nieprawdziwe dane jest czynem karalnym.

Uwaga! Po podłączeniu nowej karty (tokenu) do komputera, oprogramowanie obecne na Twoim komputerze może wyświetlić okno z komunikatem: **Z przyczyn bezpieczeństwa należy zmienić token Hasło lub For security reasons you must change the Token Password.**

Jest to sytuacja normalna, ale nie wolno tego robić.

Do aktywacji karty użyj wyłącznie naszego programu *PEM-HEART Aktywacja kart* z pakietu *PEM-HEART Signature*.

Jeśli będziesz próbował "zmienić PIN" do karty, która nie została jeszcze aktywowana, po 3 próbach nastąpi nieodwracalne uszkodzenie (blokada) karty.