Informacje dla osób odbierających certyfikat kwalifikowany DO 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. Podpis kwalifikowany może składać wyłącznie Subskrybent, dla którego wystawiono certyfikat. Posługiwanie się danymi do składania podpisu należącymi do innej osoby 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. Aplikacja rSign na telefonie komórkowym jest zabezpieczona nadanym samodzielnie przez Subskrybenta **kodem PIN**. SUGERUJEMY ZAPISANIE NADANEGO KODU PIN W BEZPIECZNYM MIEJSCU. **CenCert nie posiada kodu PIN Subskrybenta. Bez znajomości kodu PIN nie da się odblokować aplikacji mobilnej, a wada taka nie podlega gwarancji.** Niezbędny jest wtedy zakup nowego certyfikatu.
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.
10. Wymagania na urządzenie mobilne (np. telefon komórkowy) służące do aktywacji podpisu:
    a. Urządzenie mobilne powinno być zarządzanie zgodnie z wymaganiami producenta, w szczególności urządzenie nie może być „rootowane" (Android rooting, iOS jailbreaking).
    b. Urządzenie powinno być tak skonfigurowane, aby po upływie określonego czasu ekran się blokował. Odblokowanie ekranu powinno być możliwe jedynie po uwierzytelnieniu użytkownika (np. odcisk palca, hasło itp.)

.....
Podpis osoby ubiegającej się o certyfikat