Załącznik nr 12
do Regulaminu świadczenia usług certyfikacyjnych
przez Centrum Certyfikacji Województwa Podlaskiego

Polityka Certyfikacji Niekwalifikowanej
Centrum Certyfikacji Województwa Podlaskiego

SŁOWNIK POJĘĆ

Ilekroć w Polityce Certyfikacji Niekwalifikowanej Centrum Certyfikacji Województwa Podlaskiego jest mowa o:

1. **Algorytmie RSA,** należy przez to rozumieć - algorytm szyfrowania asymetrycznego wykorzystującego parę kluczy prywatny – publiczny;
2. **Bezpiecznym środowisku,** należy przez to rozumieć – infrastrukturę kryptograficzną w której generowane są w sposób bezpieczny para kluczy (prywatny i publiczny) wraz z certyfikatem;
3. **Centrum Certyfikacji**, należy przez to rozumieć – część Centrum Certyfikacji Województwa Podlaskiego wystawiającą certyfikaty. Do Centrum Certyfikacji należy wpisywanie certyfikatów na listę wystawionych certyfikatów przez CCWP, ich dystrybucja i unieważnianie certyfikatów, w przypadkach przewidzianych w Regulaminie;
4. **Centrum Certyfikacji Województwa Podlaskiego (CCWP),** należy przez to rozumieć – jednostkę organizacyjną Urzędu Marszałkowskiego Województwa Podlaskiego powołaną do wydawania certyfikatów niekwalifikowanych pracownikom jednostek samorządu terytorialnego oraz społeczności województwa podlaskiego;
5. **Certyfikacie klucza publicznego,** należy przez to rozumieć - certyfikat CCWP, w którym zawarty jest klucz publiczny subskrybenta;
6. **Certyfikacie niekwalifikowanym**, należy przez to rozumieć – certyfikat wydany przez Województwo zgodnie z Polityką Certyfikacji;
7. **Certyfikatach pośrednich**, należy przez to rozumieć - certyfikaty wystawione przez RootCA dla EsigCA, EmailCA, NetCA;
8. **CRL**, należy przez to rozumieć - listę certyfikatów unieważnionych;
9. **EmailCA**, należy przez to rozumieć - certyfikaty dla subskrybentów korzystających z poczty elektronicznej. Umożliwia uwierzytelnianie nadawców poczty elektronicznej, szyfrowanie wiadomości i autoryzację użytkowników względem serwerów sieciowych;
10. **EsigCA**, należy przez to rozumieć - certyfikaty wydawane dla subskrybentów korzystających z niekwalifikowanego podpisu elektronicznego;
11. **Karcie mikroprocesorowej**, należy przez to rozumieć – komponent techniczny bezpiecznego urządzenia do składania podpisów elektronicznych w rozumieniu ustawy z dnia 18 września 2001 r. o podpisie elektronicznym (Dz.U. 2001 r. Nr 130, poz.1450 ze zm.) dotyczący certyfikatu niekwalifikowanego, spełniający wymagania określone w tej ustawie;
12. **Kluczu prywatnym pośrednim,** należy przez to rozumieć - certyfikaty wystawione dla esigCA, emailCA, netCA;

13. **Kluczu prywatnym**, należy przez to rozumieć – dane służące do składania podpisu elektronicznego w rozumieniu ustawy o podpisie elektronicznym; służy do podpisywania wiadomości;

14. **Kluczu publicznym**, należy przez to rozumieć - dane służące do weryfikacji podpisu elektronicznego w rozumieniu ustawy o podpisie elektronicznym; klucz publiczny zawarty jest w certyfikacie wystawionym przez CCWP; klucz publiczny służy do szyfrowania;

15. **Łańcuchu certyfikacji**, należy przez to rozumieć:

    a. proces, w którym subskrybent zobowiązany jest do pobrania z repozytorium umieszczonego na stronie internetowej pod adresem http://ccwp.wrotpodlasia.pl certyfikatów: obowiązkowo RootCA, aby mógł używać swojego podpisu niekwalifikowanego; oraz w zależności od otrzymanego certyfikatu, NetCA, EmailCA, EsigCA;

    b. proces, w którym strona ufająca, aby zweryfikować certyfikat subskrybenta, musi pobrać z repozytorium obowiązkowo certyfikat RootCA oraz certyfikat analogiczny do tego którym posłużył się subskrybent (NetCA, EmailCA, EsigCA)

16. **NetCA**, należy przez to rozumieć - certyfikaty dla urządzeń i serwerów sieciowych;

17. **Unikalny Identyfikator (OID), numer identyfikacyjny,** należy przez to rozumieć identyfikator wydany przez CCWP wskazujący na politykę certyfikacji;

18. **Parze kluczy**, należy przez to rozumieć - klucz prywatny wraz z kluczem publicznym przypisanym Subskrybentowi;

19. **PKCS#10,** należy przez to rozumieć – proces w którym subskrybent generuje na swoim urządzeniu sieciowym w środowisku aplikacyjnym właściwym dla swojego urządzenia, polecenie uzyskania certyfikatu podpisane przez CCWP;

20. **Podpisie niekwalifikowanym**, należy przez to rozumieć – podpis składany za pomocą karty mikroprocesorowej wydanej przez CCWP;

21. **Polityce Certyfikacji CCWP**, należy przez to rozumieć - zbiór szczegółowych rozwiązań, w tym technicznych i organizacyjnych, wskazujący sposób, zakres oraz warunki tworzenia i stosowania certyfikatów niekwalifikowanych wydanych przez CCWP;

22. **Punkcie rejestracji**, należy przez to rozumieć - wydzieloną część CCWP zajmującą się przyjmowaniem wniosków o wydanie certyfikatów i wydające certyfikaty subskrybentom;

23. **Regulaminie świadczenia usług certyfikacyjnych przez Centrum Certyfikacji Województwa Podlaskiego,** zwanego dalej **Regulaminem** należy przez to rozumieć - opis procedur dotyczących ubiegania się o certyfikat, wydawania certyfikatu, zawieszania i unieważniania certyfikatu, zmian danych subskrybenta, zlecenia odnowienia certyfikatu i świadczenia usług gwarancyjnych;

24. **Repozytorium**, należy przez to rozumieć - miejsce, w którym składowane są certyfikaty oraz CRL CCWP, mieszczące się pod adresem internetowym: http://www.ccwp.wrotapodlasia.pl/repozytorium.php;

25. **RootCA,** należy przez to rozumieć – poświadczenie certyfikatu dla EsigCA, EmailCA, NetCA. RootCA nie wydaje certyfikatów dla subskrybentów;

26. **Skrócie klucza publicznego**, należy przez to rozumieć – skrót danych służących do weryfikacji poświadczenia elektronicznego CCWP.

27. **Sprzętowym module kryptograficznym HSM,** należy przez to rozumieć - sprzętowy moduł kryptograficzny pracujący w strukturze PKI, zapewniający wysoki poziom bezpieczeństwa dla kluczy kryptograficznych;

28. **Stronie ufającej,** należy przez to rozmieć – odbiorcę korespondencji, który za pomocą klucza publicznego – dostępnego w repozytorium- potwierdza ważność certyfikatu CCWP, którym posługuje się subskrybent;

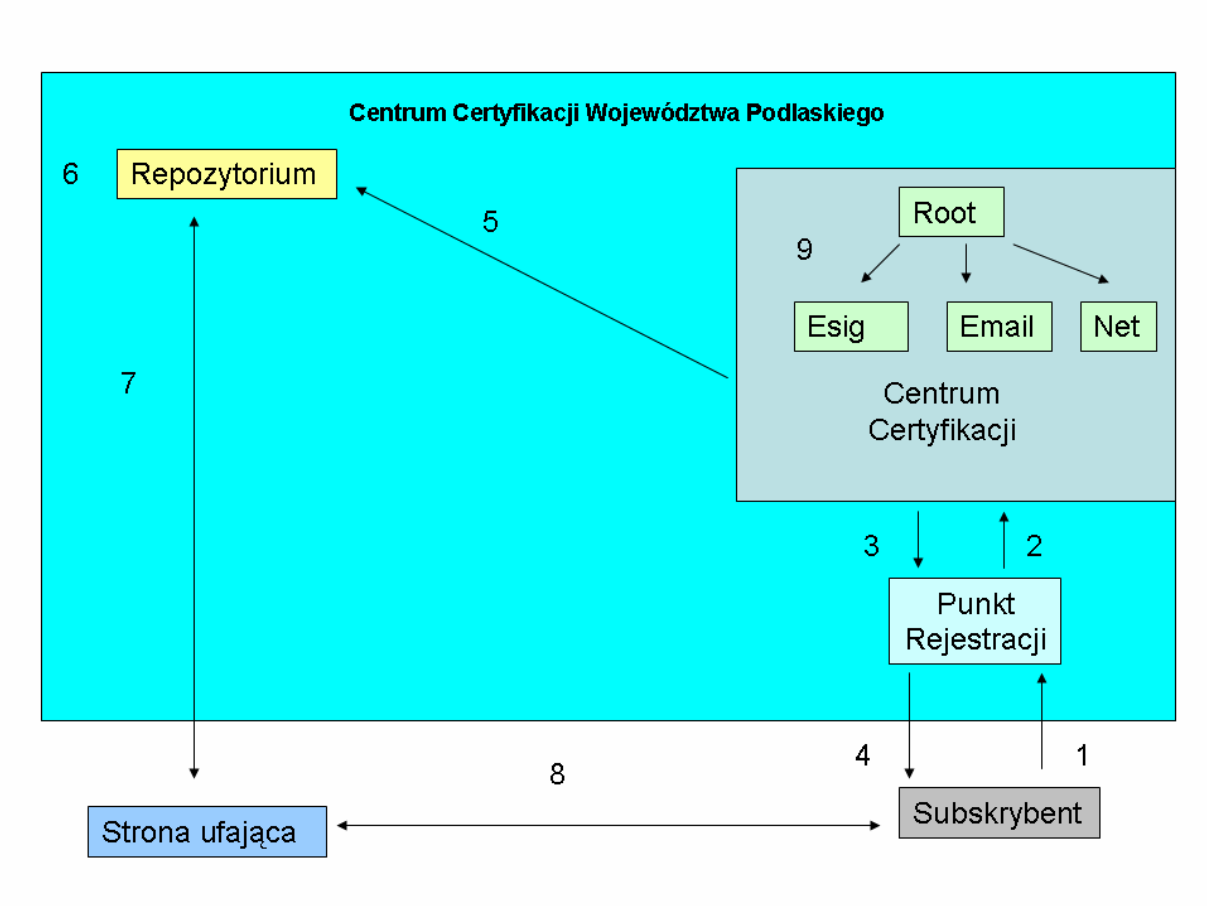
29. **Subskrybencie**, należy przez to rozumieć – osobę fizyczną uprawnioną do otrzymania certyfikatu;

30. **Ścieżce certyfikacji,** należy przez to rozumieć - łańcuch certyfikatów, w którym pierwszym ogniwem jest RootCA, następnie w zależności od ubieganego się certyfikatu - esigCA, emailCA, netCA. Na samym końcu znajduje się certyfikat subskrybenta;

31. **Użytkowniku końcowym,** należy przez to rozumieć - osobę, która uzyskała certyfikat CCWP;

32. **Weryfikacji ważności certyfikatu,** należy przez to rozumieć - proces w którym strona ufająca sprawdza czy certyfikat użyty przez subskrybenta nie stracił terminu ważności;

Schemat procedury certyfikacji



1. Subskrybent składa wniosek o przyznanie lub unieważnienie certyfikatu w Punkcie Rejestracji. Sprawdzana jest tożsamość subskrybenta składającego wniosek.
2. Wniosek trafia do Centrum Certyfikacji, gdzie generowana jest para kluczy - prywatny i publiczny - przypisanych konkretnej osobie wraz z certyfikatem CCWP. Certyfikaty wraz z parą kluczy generowane są na karcie mikroprocesorowej.
3. Centrum Certyfikacji przekazuje karty mikroprocesorowe do Punktu Rejestracji.
4. Punkt Rejestracji wydaje karty osobom, które składały wniosek – w momencie otrzymania zestawu do podpisu niekwalifikowanego osoba taka staje się subskrybentem.
5. Centrum Certyfikacji przekazuje do Repozytorium certyfikaty CCWP (RootCA, EsigCA, EmailCA oraz listę CRL).
6. W Repozytorium przechowywane są certyfikaty CCWP wraz z aktualną listą CRL (lista certyfikatów unieważnionych).
7. Aby strona ufająca mogła poprawnie zweryfikować tożsamość nadawcy musi mieć jego klucz publiczny oraz certyfikaty CCWP i aktualną listę CRL. Strona ufająca musi pobrać certyfikaty CCWP oraz aktualną listę CRL w celu sprawdzenia, czy subskrybent korzystający z certyfikatu wystawionego przez CCWP ma do tego prawo i jego certyfikat nie został unieważniony.
8. Wysłanie podpisanej wiadomości do strony ufającej. Strona ufająca ma możliwość zweryfikowania nadawcy po wykonaniu kroku 7.
9. Root – wystawia certyfikat dla certyfikatów pośrednich Email, Esig, Net.