Województwo Śląskie

UMWS Certificate Authority
Polityka certyfikacji UMWS CA

Historia zmian dokumentu:

Wersja	Data publikacji	Data obowiązywania	Opis
v1.0	2020-08-31	2020-09-01	Uruchomienie centrum certyfikacji. Pierwsza zatwierdzona wersja dokumentu.

Spis treści

1. Wstęp

Polityka certyfikacji UMWS CA, zwana dalej *Polityką*, określa ogólne zasady świadczenia usług zaufania, w tym techniczne i organizacyjne rozwiązania, wskazujące sposób, zakres oraz warunki tworzenia i stosowania certyfikatów. Polityka określa proces świadczenia usług zaufania oraz jego uczestników. Szczegółowy opis zawiera: **Kodeks postępowania certyfikacyjnego UMWS CA**, zwany dalej *Kodeksem*. Definicje pojęć użytych w Polityce są określone w Kodeksie.

Usługi zaufania w zakresie wydawania zaufanych certyfikatów niekwalifikowanych dla Partnerów SEKAP, zwanych dalej *Certyfikatami*, realizuje *Urząd Marszałkowski Województwa Śląskiego*, zwany dalej *UMWS*, w ramach *Centrum Certyfikacji UMWS CA*, zwanym dalej *UMWS CA*.

1.1. Nazwa dokumentu i jego identyfikacja

Polityka ma przyznaną następującą klasę identyfikatorów OID: 1.3.6.1.4.1.56210.1.1.2

> iso(1) identified-organization(3) dod(6) internet(1) private(4) enterprise(1) umws(56210) umws-ca(1) doc(1) umws-ca-cp(2)

Aktualna oraz poprzednie wersje Polityki są publikowane na stronie internetowej UMWS CA, dostępnej pod adresem *http://cc.slaskie.pl*.

2. Zakres zastosowania polityki certyfikacji

Polityka jest stosowana do wydawania i zarządzania certyfikatami wydawanymi przez UMWS CA. Przez certyfikat należy rozumieć elektroniczny plik poświadczony elektronicznie przez UMWS, w którym klucz publiczny jest przyporządkowany do subskrybenta i umożliwia jego identyfikację.

Certyfikaty, wydawane zgodnie z Kodeksem, nie są certyfikatami kwalifikowanymi. Podpis elektroniczny weryfikowany przy pomocy tych certyfikatów nie wywołuje skutków prawnych równorzędnych podpisowi własnoręcznemu.

Certyfikaty opisane w Polityce są generowane przez urząd certyfikacji UMWS CA prowadzony przez UMWS.

Certyfikaty mogą zawierać dane i służyć do identyfikacji Partnerów SEKAP.

Odpowiedzialność UMWS, w tym finansowa, odpowiedzialność subskrybenta, odbiorcy usług zaufania oraz strony ufającej jest określona w Kodeksie.

Identyfikatory polityk dla certyfikatów UMWS CA mają OID rozpoczynający się od: 1.3.6.1.4.1.56210.1.2.

> iso(1) identified-organization(3) dod(6) internet(1) private(4) enterprise(1) umws(56210) umws-ca(1) policy(2)

2.1. Certyfikat OCSP

Używany wewnętrznie w UMWS CA przez usługę odpowiadającą w trybie online do podpisywania odpowiedzi na żądania informacji o stanie certyfikatów.

Identyfikator polityki certyfikacji: 1.3.6.1.4.1.56210.1.2.1 – OCSP certificate / Certyfikat OCSP.

Okres ważności: 40 dni.

Minimalna długość klucza: 2048.

Zasady aplikacji: OCSP Signing – 1.3.6.1.5.5.7.3.9.

Użycie klucza: Digital Signature.

2.2. Certyfikat pieczęci elektronicznej

Używany do zapewnienia integralności i autentyczności pochodzenia informacji przesyłanych drogą elektroniczną. Pozwala na podpisywanie danych w postaci elektronicznej oraz uwierzytelnianie subskrybentów.

Identyfikator polityki certyfikacji: 1.3.6.1.4.1.56210.1.2.2 – Electronic seal certificate / Certyfikat pieczęci elektronicznej.

Okres ważności: od 1 roku do 3 lat.

Minimalna długość klucza: 2048.

Identyfikacja subskrybenta: identyfikator organizacji.

Użycie klucza: Non Repudiation.

3. Świadczenie usług zaufania

Usługi udostępniane przez UMWS CA wspierają działalność UMWS, jego personelu, partnerów oraz klientów.

Podstawą wydania pierwszego oraz kolejnego certyfikatu, w tym odnowienia certyfikatu jest złożenie wniosku oraz weryfikacja tożsamości subskrybenta i prawa do uzyskania certyfikatu. Sposób weryfikacji tożsamości oraz prawa do uzyskania certyfikatu zależy od rodzaju certyfikatu oraz od tego, czy jest to pierwszy, czy też kolejny certyfikat dla danego subskrybenta. Szczegóły dotyczące wydania certyfikatu określa Kodeks.

Unieważnienie, zawieszenie lub odwieszenie certyfikatu może nastąpić tylko w odniesieniu do certyfikatu, którego okres ważności nie upłynął i może być zrealizowane na wniosek subskrybenta, podmiotu, którego dane są zawarte w certyfikacie, odbiorcy usług zaufania, innej upoważnionej osoby lub samodzielnie przez UMWS. Szczegóły dotyczące zmiany statusu certyfikatu określa Kodeks.

4. Subskrybent

Subskrybent jest zobowiązany przede wszystkim do ochrony posiadanego klucza prywatnego związanego z kluczem publicznym zawartym w wydanym mu przez UMWS CA certyfikacie. W przypadku stwierdzenia lub podejrzenia naruszenia bezpieczeństwa klucza prywatnego subskrybent i odbiorca usług certyfikacyjnych zobowiązani są zgłosić do UMWS CA wniosek o zawieszenie lub unieważnienie certyfikatu.

5. Strona ufająca

Strona ufająca jest zobowiązana do wykorzystywania certyfikatów zgodnie z ich przeznaczeniem oraz do weryfikowania podpisu elektronicznego, podpisu cyfrowego i poświadczenia elektronicznego w chwili dokonywania weryfikacji lub innym wiarygodnym momencie z wykorzystaniem listy zawieszonych i unieważnionych certyfikatów dla certyfikatów i zaświadczeń certyfikacyjnych wchodzących w skład właściwej ścieżki certyfikacji. Przed podjęciem jakichkolwiek czynności w zaufaniu do certyfikatu strona ufająca powinna zapoznać się z postanowieniami Kodeksu.

6. Zmiany polityk, publikacje

UMWS ma prawo do okresowych aktualizacji Polityki. Po zatwierdzeniu przez UMWS zmian zaktualizowana Polityka będzie publikowana na stronie internetowej UMWS CA. Informacje dotyczące usług certyfikacyjnych świadczonych przez UMWS są dostępne na stronie internetowej oraz przez *Operatorów UMWS CA* określonych w Kodeksie.

Listy zawieszonych i unieważnionych certyfikatów są generowane przez UMWS CA nie rzadziej niż co 24 godziny lub po zawieszeniu albo unieważnieniu certyfikatu. Aktualizacja list odbywa się nie później niż w ciągu 1 godziny od zawieszenia lub unieważnienia certyfikatu. Dopuszczalny okres opóźnienia zawieszenia lub unieważnienia certyfikatu może wynieść 24 godziny.