

Politechnika Łódzka Centrum Komputerowe
Polityka Certyfikacji

1. Wstęp.

1.1. Cel dokumentu.

Polityka certyfikacji CC-PŁ (Centrum Certyfikacji Politechniki Łódzkiej) reguluje ogólne zasady świadczenia usług certyfikacyjnych przez Centrum Komputerowe Politechniki Łódzkiej.

1.2. Definicje.

CK-PŁ – Centrum Komputerowe Politechniki Łódzkiej.

Certyfikat – certyfikat niekwalifikowany wg ustawy o podpisie elektronicznym.

CC-PŁ – Centrum Certyfikacji Politechniki Łódzkiej, wydzielona usługa zorganizowana w strukturze Centrum Komputerowego, wykonujący zadanie wydawania i zarządzania certyfikatami.

CA-TU – Zamienna nazwa angielska – Certificate Authority of Technical University of Lodz.

Operator – upoważniony przez CK-PŁ lub odbiorcę usług certyfikacyjnych pracownik zajmujący się rejestracją subskrybentów i/ lub przyjmowaniem wniosków o wydanie i unieważnienie certyfikatów. Szczegółowy zakres czynności Operatora określa regulamin świadczenia usług certyfikacyjnych.

Odbiorca (odbiorca usług certyfikacyjnych) – osoba fizyczna, prawna lub jednostka organizacyjna nie posiadająca osobowości prawnej, która zawarła z CK-PŁ umowę na świadczenie usług certyfikacyjnych lub otrzymuje takie świadczenie na podstawie rozporządzenia Rektora Politechniki Łódzkiej.

Subskrybent – osoba fizyczna, wskazana w wykazie osób upoważnionych do uzyskania certyfikatu przez odbiorcę usług certyfikacyjnych, jako osoba uprawniona do otrzymania certyfikatu.

Użytkownik (certyfikatu) – subskrybent lub serwis lub urządzenie.

Regulamin – Regulamin Świadczenia Usług Certyfikacyjnych zwany również zamiennie Kodeksem Postępowania Certyfikacyjnego (KPC) – stanowi zbiór zasad i procedur regulujący procesy świadczenia usług certyfikacyjnych.

1.3. Identyfikacja.

Identyfikator OID niniejszej polityki - nie przydzielono.

Identyfikator DN (Distinguished Name) CC-PŁ:

Nazwa pola	Wartość
C	PL
O	Politechnika Lodzka

OU	Centrum Komputerowe
CN	Cert TU Lodz

oraz

Nazwa pola	Wartość
C	PL
O	Politechnika Lodzka
OU	Centrum Komputerowe
CN	Student TU Lodz

1.4. Zakres i podstawa działania.

CC-PŁ świadczy usługę certyfikacji dla pracowników i studentów PŁ.

CC-PŁ może również świadczyć usługi dla odbiorców spoza Politechniki Łódzkiej na podstawie odrębnych umów.

1.5. Struktura CC-PŁ.

Struktura CC-PŁ jest obecnie jednopoziomowa złożona z dwóch głównych urzędów odrębnym dla pracowników i studentów.

Certyfikat urzędu CC-PŁ jest certyfikatem samo podpisanym. Oznacza to, że CC-PŁ sam poświadcza autentyczność swojego certyfikatu.

2. Certyfikaty.

2.1. Zawartość certyfikatu.

Certyfikat jest ciągiem danych, który zawiera co najmniej: nazwę wydawcy, nazwę subskrybenta, klucz publiczny subskrybenta, okres ważności certyfikatu, podpis urzędu wydającego oraz dodatkowe opcje.

2.2. Typy certyfikatów.

CC-PŁ wydaje następujące typy certyfikatów do różnych zastosowań:

- Certyfikaty osobiste dla osób fizycznych o następujących właściwościach:
 - Certyfikaty służące do weryfikacji podpisów elektronicznych w poczcie elektronicznej,
 - Certyfikaty do zapewnienia poufności danych,
 - Certyfikaty do uwierzytelniania i zapewniania poufności w komunikacji z serwerem,
 - Certyfikaty do zestawiania połączeń VPN,
 - Certyfikaty służące do logowania się użytkowników do systemów informatycznych,

- Certyfikaty dla usług serwerowych SSL

2.3. Znaczenie certyfikatu i poziom wiarygodności.

Certyfikat wydany przez CC-PŁ stanowi dokument potwierdzający tożsamość subskrybenta lub jego dodatkowe dane jak np. adres e-mail. Ważny certyfikat (tzn. podpisany przez właściwego wydawcę, nie odwołany na liście CRL i posiadający datę ważności która jeszcze nie upłynęła) poświadcza również fakt, że klucz publiczny, którym posługuje się subskrybent w rzeczywistości należy do niego. Strona ufająca jest w stanie na podstawie otrzymanej podpisanej wiadomości zidentyfikować nadawcę i rozliczyć go z działań, których dokonał za pomocą certyfikatu.

Urząd wydaje certyfikaty na podstawie zawartości osobowych baz danych będących w posiadaniu Politechniki Łódzkiej, weryfikowanych w procesach rejestracji pracowników i studentów.

2.3.1. Certyfikat klasy "pracownik".

Certyfikaty klasy pracownik są wydawane przez główny urząd CC-PŁ i są przeznaczone dla pracowników Politechniki Łódzkiej do zastosowań produkcyjnych w zakresie podpisu elektronicznego wiadomości oraz do szyfrowania wiadomości lub łącza.

Certyfikat tej klasy może zostać również wydany osobom spoza Politechniki Łódzkiej, które znajdują się w relacji gospodarczej z uczelnią, określonej osobnymi umowami (np. są odbiorcą usługi świadczonej przez PŁ lub wykonują usługę na rzecz PŁ).

2.3.2. Certyfikat klasy "student".

Certyfikaty klasy student są wydawane przez główny urząd CC-PŁ i są przeznaczone dla studentów Politechniki Łódzkiej. Certyfikat służy do uwierzytelniania w wewnętrznych systemach korporacyjnych oraz do szyfrowania łącza lub danych związanych z tymi systemami.

3. Rejestracja i sprawdzenie tożsamości.

Subskrybentami usług certyfikacyjnych świadczonych przez CC-PŁ są pracownicy, studenci oraz inne osoby zarejestrowane w centralnej bazie katalogowej LDAP. Sprawdzenia tożsamości subskrybentów dokonują Biura Obsługi Klienta:

- w odniesieniu do pracowników oraz innych osób niebędących studentami – biuro w Centrum Komputerowym,
- w odniesieniu do studentów – biuro w Bibliotece.

4. Usługi certyfikacyjne.

CC-PŁ świadczy cztery podstawowe usługi certyfikacyjne:

- (1) wydanie certyfikatu,

- (2) odnowienie certyfikatu,
- (3) unieważnienie certyfikatu,
- (4) sprawdzenie statusu certyfikatu.

Wydawanie certyfikatu polega na przekazaniu subskrybentowi atrybutów w postaci certyfikatu i odpowiedniego klucza prywatnego, w postaci pliku w formacie PKCS#12.

Odnowienie ma miejsce wtedy, gdy subskrybent chce uzyskać certyfikat dla nowego klucza publicznego lub chce zmienić niektóre dane zawarte w dotychczasowym certyfikacie.

Unieważnienie certyfikatu następuje, gdy zostanie ujawniony klucz prywatny związany z kluczem publicznym zawartym w certyfikacie lub istnieje uzasadnione podejrzenie, że tak się stało.

Weryfikacja certyfikatu polega na stwierdzeniu przez CC-PŁ, że certyfikat został wydany przez CC-PŁ, czy znajduje się na liście certyfikatów unieważnionych i czy termin jego ważności upłynął.

Usługi certyfikacyjne są świadczone w sposób automatyczny przez stronę WWW pod adresem: <http://cert.p.lodz.pl> .

5. Gwarancje CC-PŁ.

Centrum Komputerowe oświadcza, że podjęło adekwatne kroki w celu weryfikacji danych zawartych w certyfikatach.

Centrum Komputerowe oświadcza, że nie ponosi odpowiedzialności finansowej z tytułu ewentualnych szkód wyrządzonych na skutek użycia wydanych przez CC-PŁ certyfikatów.

6. Akceptacja certyfikatu.

Odpowiedzialność oraz gwarancje CC-PŁ stają się obowiązujące od chwili zaakceptowania przez subskrybenta wydanego certyfikatu.

7. Strona ufająca.

Strona ufająca jest zobowiązana do rzetelnej weryfikacji podpisu cyfrowego umieszczonego na dokumencie, który do niej dotrze. W procesie weryfikacji strona ufająca powinna korzystać z zasobów i procedur udostępnianych przez CC-PŁ.

Każdy dokument z wykrytą wadą w podpisie cyfrowym powinien zostać odrzucony i ewentualnie poddany innym procedurom weryfikacji (np. weryfikacji prawnej).

8. Subskrybent.

Subskrybent jest zobowiązany do bezpiecznego przechowywania klucza prywatnego (zapobiegającego lub utrudniającego jego ujawnienie osobom postronnym). W przypadku ujawnienia klucza lub uzasadnionego podejrzenia, że takie zdarzenie miało miejsce, subskrybent musi niezwłocznie podjąć kroki w celu odwołania ważności certyfikatu lub

poinformować o tym urząd certyfikacyjny w sposób niebudzący wątpliwości co do tożsamości zgłaszającego.

9. Aktualizacja polityki certyfikacji.

Polityka certyfikacji CC-PŁ jest jawna i jest publikowana na stronach informacyjnych WWW. Polityka certyfikacji może podlegać okresowym modyfikacjom, dokonywanym przez zespół CC-PŁ. Wszystkie obowiązujące zmiany w polityce certyfikacji będą udostępniane subskrybentom, poprzez publikowanie. Subskrybenci, którzy nie zaakceptują zmian muszą zrezygnować z pobierania usług certyfikacyjnych.

10. Opłaty.

Usługi certyfikacyjne CC-PŁ są bezpłatne.

11. Postanowienia końcowe.

Niniejsza polityka certyfikacji jest dokumentem podstawowym dla działalności CC-PŁ. Inne dokumenty regulujące sposób świadczenia usług certyfikacyjnych przez CC-PŁ nie mogą stać z nią w sprzeczności.

Inne dokumenty podrzędne:

1. Regulamin świadczenia usług certyfikacyjnych – Kodeks Postępowania Certyfikacyjnego.