



ZARZĄDZENIE nr 33/2016
REKTORA UNIWERSYTETU PAPIESKIEGO JANA PAWŁA II W KRAKOWIE
z dnia 23 czerwca 2016 r.

w sprawie

stosowania kwalifikowanego podpisu elektronicznego
na Uniwersytecie Papieskim Jana Pawła II w Krakowie

Na podstawie art. 66 ust. 1 ustawy z dnia 27 lipca 2005 r. Prawo o szkolnictwie wyższym (Dz. U. z 2012 r., poz. 572 z późn. zm.) oraz § 31 Statutu UPJPII, zarządzam, co następuje:

I. POSTANOWIENIA OGÓLNE

§1

- 1 W Uniwersytecie Papieskim Jana Pawła II w Krakowie stosuje się kwalifikowany podpis elektroniczny do podpisywania dokumentów wchodzących w zakres spraw poszczególnych komórek organizacyjnych, wydawany zgodnie z ustawą z dnia 18 września 2001 r. o podpisie elektronicznym (Dz. U. z 2013 r. poz. 262 z późn. zm).
- 2 Subskrybentami podpisu elektronicznego w Uniwersytecie Papieskim Jana Pawła II w Krakowie są:
 - 1) Rektor;
 - 2) Prorektorzy;
 - 3) Kanclerz;
 - 4) Kwestor;
 - 5) Dziekani Wydziałów.
- 3 Pozostali pracownicy UPJPII na podstawie zgody Rektora lub Kanclerza.

§2

1. Subskrybent może stosować kwalifikowany podpis elektroniczny tylko zgodnie z przepisami prawa, wyłącznie w celach służbowych oraz w granicach udzielonych mu pełnomocnictw i upoważnień.
2. Subskrybent jest zobowiązany chronić kartę kryptograficzną przed jej utratą, zniszczeniem lub uszkodzeniem oraz przed dostępem do niej osób nieupoważnionych.
3. Kod PIN zabezpieczający kartę kryptograficzną jest poufny i jest przeznaczony do używania wyłącznie przez Użytkownika Karty i nie może być udostępniany innym osobom.

II. WYDAWANIE CERTYFIKATU KWALIFIKOWANEGO

§3

1. Certyfikat kwalifikowany zamawia uprawniony pracownik Działu Uczelnianej Sieci Komputerowej, pełniący funkcję Administratora Podpisu Kwalifikowanego (Administrator PK):
 - 1) pracownikom określonym w § 1 ust. 2 - na podstawie formularza zgłoszenia certyfikacyjnego; określonego przez Centrum Certyfikacji, świadczące usługi certyfikacyjne,
 - 2) pracownikom określonym w § 1 ust. 3 - na podstawie złożonego przez bezpośredniego przełożonego pracownika wniosku o wydanie certyfikatu kwalifikowanego, określonego w załączniku nr 1 oraz formularza zgłoszenia certyfikacyjnego.
2. Formularz zgłoszenia certyfikacyjnego wypełnia pracownik ubiegający się o wydanie mu certyfikatu kwalifikowanego i wraz z wnioskiem zaakceptowanym przez Rektora lub Kanclerza (dla pracowników o których mowa w § 1 ust. 3) przesyła go Administratorowi PK w formie pisemnej.
3. Administrator PK niezwłocznie, to jest po wystąpieniu zdarzenia, informuje Dział Spraw Osobowych, Płac i Spraw Socjalnych o przydzieleniu certyfikatu kwalifikowanego dla pracownika.

§4

Pracownik osobiście odbiera certyfikat kwalifikowany od przedstawiciela Centrum Certyfikacji, po podpisaniu Umowy z Centrum Certyfikacji.

§5

Niezwłocznie po odebraniu certyfikatu kwalifikowanego pracownik składa oświadczenie subskrybenta według wzoru, o którym mowa w załączniku nr 2 do niniejszego zarządzenia, o:

- 1) odebraniu zestawu do podpisu elektronicznego lub karty kryptograficznej;
- 2) zapoznaniu się z przepisami Ustawy z dnia 18 września 2001 r. o podpisie elektronicznym (Dz. U. z 2013 r. poz. 262 z późn. zm)
- 3) zapoznaniu się z treścią niniejszego Zarządzenia;
- 4) podpisaniu Umowy z Centrum Certyfikacji;
- 5) zobowiązaniu się w szczególności do:
 - a. przestrzegania zasad niniejszego zarządzenia,
 - b. stosowania kwalifikowanego podpisu elektronicznego zgodnie z przepisami prawa, wyłącznie w celach służbowych oraz w granicach udzielonych mu pełnomocnictw i upoważnień,
 - c. nieudostępniania osobom nieupoważnionym karty kryptograficznej i kodu PIN zabezpieczającego tę kartę.

III. ODNOWIENIE CERTYFIKATU KWALIFIKOWANEGO

§6

1. W uzasadnionych przypadkach kwalifikowany podpis elektroniczny może być odnowiony dla pracowników zobowiązanych do jego stosowania na podstawie obowiązujących przepisów prawa lub wykonywania innych czynności wynikających z zakresu obowiązków na zajmowanym stanowisku.
2. Osoby, o których mowa w ust. 1, składają do Administratora PK wniosek w formie pisemnej według wzoru określonego w załączniku nr 3 do zarządzenia.
3. Odnowienie certyfikatu odbywa się zgodnie z zasadami obowiązującymi w Centrum Certyfikacji.

IV. UNIEWAŻNIANIE CERTYFIKATU KWALIFIKOWANEGO

§7

1. Unieważnienie certyfikatu kwalifikowanego może nastąpić na wniosek subskrybenta, kierownika jednostki organizacyjnej, w której pracuje subskrybent, uprawnionego pracownika Działu Spraw Osobowych, Płac i Spraw Socjalnych, Kanclerza oraz w szczególnych przypadkach, o których mowa w § 9 pkt. 4 na wniosek Administratora PK.
2. Wniosek kierownika jednostki organizacyjnej, uprawnionego pracownika Działu Spraw Osobowych, Płac i Spraw Socjalnych oraz wniosek Administratora PK w oparciu o § 9 pkt. 4 wymagają akceptacji Kanclerza.
3. Administrator PK niezwłocznie, to jest po wystąpieniu zdarzenia, informuje Dział Spraw Osobowych, Płac i Spraw Socjalnych o każdorazowym unieważnieniu certyfikatu.

§8

1. W razie utraty lub kradzieży karty kryptograficznej subskrybent zobowiązany jest do powiadomienia Administratora PK o utracie lub kradzieży tej karty oraz do niezwłocznego wystąpienia do Administratora PK z wnioskiem o unieważnienie certyfikatu kwalifikowanego, a w razie kradzieży, także do niezwłocznego zgłoszenia kradzieży w komisariacie Policji.
2. Po otrzymaniu informacji o utracie lub kradzieży karty kryptograficznej Administrator PK niezwłocznie występuje do Centrum Certyfikacji o unieważnienie certyfikatu kwalifikowanego.

§9

Administrator PK występuje do Centrum Certyfikacji o unieważnienie certyfikatu kwalifikowanego w szczególności w przypadku:

- 1) zmiany stanowiska pracy subskrybenta lub innej przyczyny, skutkującej brakiem konieczności stosowania przez niego kwalifikowanego podpisu elektronicznego – na podstawie wniosku kierownika jednostki organizacyjnej, w której pracuje subskrybent;

- 2) rozwiązania stosunku pracy z subskrybentem lub zmian na stanowisku pracy – na podstawie wniosku uprawnionego pracownika Działu Spraw Osobowych, Płac i Spraw Socjalnych;
- 3) odwołania lub wygaśnięcia udzielonego subskrybentowi pełnomocnictwa lub upoważnienia, skutkującego brakiem konieczności stosowania przez niego kwalifikowanego podpisu elektronicznego – na podstawie wniosku uprawnionego pracownika Działu Spraw Osobowych, Płac i Spraw Socjalnych;
- 4) uzyskania potwierdzonej informacji o stosowaniu przez subskrybenta kwalifikowanego podpisu elektronicznego niezgodnie z § 2.

V. ADMINISTROWANIE CERTYFIKATAMI KWALIFIKOWANYMI I KARTAMI KRYPTOGRAFICZNYMI

§10

Administrator PK prowadzi sprawy związane z administrowaniem certyfikatami kwalifikowanymi, a w szczególności związane z:

- 1) zamawianiem certyfikatów kwalifikowanych w Centrum Certyfikacji;
- 2) wydawaniem certyfikatów kwalifikowanych;
- 3) prowadzeniem ewidencji wydanych i unieważnionych certyfikatów kwalifikowanych;
- 4) występowaniem do Centrum Certyfikacji z wnioskami o odnowienie i unieważnienie certyfikatów kwalifikowanych.

§11

W celu aktualizacji danych przez Administratora PK, Dział Spraw Osobowych, Płac i Spraw Socjalnych przekazuje niezwłocznie, tj. po zaistnieniu zdarzenia, Administratorowi PK, w formie pisemnej, informacje o pracownikach określonych w § 1 dotyczące w szczególności:

- 1) zatrudnienia w UPJPII;
- 2) zmiany danych występujących w formularzu zgłoszenia certyfikacyjnego;
- 3) rozwiązania stosunku pracy;
- 4) udzielenia, odwołania lub wygaśnięcia pełnomocnictwa lub upoważnienia skutkujące powstaniem lub brakiem konieczności stosowania przez pracownika kwalifikowanego podpisu elektronicznego.

§12

1. Za procedurę wyboru odpowiedniego Centrum Certyfikacji, zamówienia związane z realizacją zarządzenia oraz ich zgodność z odrębnymi przepisami UPJPII odpowiada Administrator PK.
2. Przekazywanie i odbieranie od pracowników zestawów do podpisu elektronicznego oraz prowadzenie ewidencji w tym zakresie należy do zadań Administratora PK.
3. Prowadzenie wszystkich spraw związanych z przygotowaniem infrastruktury informatycznej do składania podpisu elektronicznego, a w szczególności:

instalacja i konfiguracja zestawów do podpisu elektronicznego należy do zadań Działu Uczelnianej Sieci Komputerowej. W odniesieniu do Systemu ProAkademia w porozumieniu z administratorem Systemu ProAkademia.

§13

1. Tworzy się rejestr subskrybentów podpisu kwalifikowanego w UPJPII zawierający następujące dane:

- 1) Imię i nazwisko pracownika,
- 2) Stanowisko pracownika,
- 3) Data złożenia wniosku o certyfikat,
- 4) Daty obowiązywania podpisu,
- 5) Szczegółowy cel stosowania podpisu,
- 6) Informację o Centrum Certyfikacji,
- 7) Informację o dacie unieważnienia certyfikatu,
- 8) Informację o przyczynie unieważnienia certyfikatu.

2. Rejestr prowadzi Administrator PK.

§14

Pracownicy, posiadający nieaktualny podpis kwalifikowany zobowiązani są do dostarczenia kart kryptograficznych do Administratora PK do 14 dni od ogłoszenia zarządzenia.

§15

Zarządzenie wchodzi w życie z dniem ogłoszenia.

WYKAZ ZAŁĄCZNIKÓW

1. Wniosek o wydanie certyfikatu kwalifikowanego
2. Oświadczenie subskrybenta
3. Wniosek o odnowienie certyfikatu kwalifikowanego
4. Wniosek o unieważnienie certyfikatu kwalifikowanego



ks. prof. dr hab. Wojciech Zyzak
REKTOR