POLITYKA ŚWIADCZENIA USŁUG ZAUFANIA

Poczta Prawnicza NOTA

Wersja 1.0

Wydawnictwo Kwantum Sp. z o.o.

1 Spis treści

1 Wstęp

1.1 Wprowadzenie

Polityka świadczenia usług zaufania, zwana dalej Polityką, określa szczegółowe rozwiązania, w tym techniczne i organizacyjne dotyczące świadczenia przez Wydawnictwo Kwantum Sp. z o.o. (dalej Kwantum) jako Operatora Poczty Prawniczej Nota (dalej PP Nota), usług zaufania polegających na:

1. wystawianiu i unieważnianiu niekwalifikowanych certyfikatów zaawansowanego podpisu elektronicznego oraz
2. wystawianiu dowodów wysłania oraz dowodów otrzymania dla świadczonych usług elektronicznych doręczeń.

Polityka definiuje strony biorące udział w procesie świadczenia powyższej określonych usług zaufania oraz ich prawa i obowiązki.

Certyfikaty zaawansowanego podpisu elektronicznego wydawane przez Kwantum służą potwierdzania tożsamości osób podpisujących pisma oraz do potwierdzania zlecenia wysyłki przesyłki elektronicznej w PP Nota.

Elektroniczne poświadczenia – dowody wysłania oraz dowody otrzymania – są wydawane przez Kwantum w celu potwierdzenia dokonania wysyłki elektronicznej przez jednego Subskrybenta (wysyłający) oraz w celu potwierdzenia jej doręczenia przez innych Subskrybentom (odbiorcy) za pośrednictwem PP Nota.

Usługi zaufania świadczone przez Kwantum na podstawie niniejszej Polityki spełniają wymagania:

- ustawy z dnia 29 września 2016 r. o usługach zaufania oraz identyfikacji elektronicznej oraz
- rozporządzenia Parlamentu Europejskiego i Rady (UE) Nr 910/2014 z dnia 23 lipca 2014 r. w sprawie identyfikacji elektronicznej i usług zaufania w odniesieniu do transakcji elektronicznych,

a także wymagania innych, obowiązujących norm prawnych oraz istniejących standardów międzynarodowych w zakresie tworzenia i funkcjonowania systemów PKI.

Struktura dokumentu została oparta na dokumencie RFC 3647 (*Internet X.509 Public Key Infrastructure Certification Policy and Certification Practices Framework*) i ma zaspokajać potrzeby informacyjne wszystkich uczestników infrastruktury PKI opisanej w niniejszym dokumencie i obsługiwanej przez Kwantum.

Polityka stanowi własność intelektualną Wydawnictwa Kwantum Sp. z o.o.

1.2 Definicje (słownik)

Algorytm ECDSA - (ang. Elliptic Curve Digital Signature Algorithm) - algorytm krzywych eliptycznych używany w procesie cyfrowego podpisu. Określony jest jednoznacznie przez identyfikator obiektu „{joint-iso-itu-t(2) international-organizations(23) set(42) vendor(9) 11 4 1}".

Certyfikat klucza publicznego - certyfikat klucza weryfikującego podpis lub certyfikat klucza szyfrującego.

Certyfikat klucza weryfikującego podpis - elektroniczne zaświadczenie, za pomocą którego klucz weryfikujący podpis jest przyporządkowany do osoby składającej podpis elektroniczny i które umożliwia identyfikację tej osoby; certyfikat klucza weryfikującego podpis jest certyfikatem.

Certyfikat pieczęci elektronicznej oznacza poświadczenie elektroniczne, które łączy dane służące do walidacji pieczęci elektronicznej z osobą prawną i potwierdza nazwę tej osoby.

Certyfikat podpisu elektronicznego oznacza poświadczenie elektroniczne, które przyporządkowuje dane służące do walidacji podpisu elektronicznego do osoby fizycznej i potwierdza co najmniej imię i nazwisko lub pseudonim tej osoby.

Dane identyfikujące osobę oznaczają zestaw danych umożliwiających ustalenie tożsamości osoby fizycznej lub prawnej, lub osoby fizycznej reprezentującej osobę prawną.

Dane służące do składania pieczęci elektronicznej oznaczają niepowtarzalne dane, które podmiot składający pieczęć wykorzystuje do złożenia pieczęci elektronicznej.

Dane służące do składania podpisu elektronicznego oznaczają unikalne dane, których podpisujący używa do składania podpisu elektronicznego.

Dane służące do walidacji oznaczają dane używane do walidacji podpisu elektronicznego lub pieczęci elektronicznej.

Dokument elektroniczny oznacza każdą treść przechowywaną w postaci elektronicznej, w szczególności tekst lub nagranie dźwiękowe, wizualne lub audiowizualne.

Dostawca usług zaufania oznacza osobę fizyczną lub prawną, która świadczy przynajmniej jedną usługę zaufania, jako kwalifikowany lub niekwalifikowany dostawca usług zaufania.

eIDAS - Rozporządzenie (UE) nr 910/2014 z dnia 23 lipca 2014 r. w sprawie identyfikacji elektronicznej i usług zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznym.

Elektroniczny znacznik czasu oznacza dane w postaci elektronicznej, które wiążą inne dane w postaci elektronicznej z określonym czasem, stanowiąc dowód na to, że te inne dane istniały w danym czasie.

Identyfikacja elektroniczna oznacza proces używania danych w postaci elektronicznej identyfikujących osobę, unikalnie reprezentujących osobę fizyczną lub prawną, lub osobę fizyczną reprezentującą osobę prawną.

Klucz - liczba, symbol lub ciąg liczb lub symboli jednoznacznie wyznaczający przekształcenie kryptograficzne spośród rodziny przekształceń zdefiniowanej przez algorytm kryptograficzny.

Klucze infrastruktury - klucze kryptograficzne algorytmów kryptograficznych stosowane do innych celów niż składanie lub weryfikacja kwalifikowanego podpisu elektronicznego lub poświadczenia elektronicznego, a w szczególności klucze stosowane:

a) w protokołach uzgadniania lub dystrybucji kluczy zapewniających poufność danych,
b) do zapewnienia, podczas transmisji lub przechowywania, poufności i integralności zgłoszeń certyfikacyjnych, kluczy użytkowników, rejestrów zdarzeń, 14.3. do weryfikacji dostępu do urządzeń, oprogramowania weryfikującego lub podpisującego.

Klucz prywatny są to dane służące do składania podpisów elektronicznych lub poświadczeń elektronicznych.

Klucz publiczny są to dane służące do weryfikacji podpisów elektronicznych lub poświadczeń elektronicznych.

Klucz podpisujący - klucz prywatny służący do składania podpisu elektronicznego; klucz podpisujący stanowi dane służące do składania podpisu elektronicznego.

Klucz weryfikujący podpis - klucz publiczny służący do weryfikowania podpisu elektronicznego; klucz weryfikujący podpis stanowi dane służące do weryfikacji podpisu elektronicznego lub dane służące do weryfikacji poświadczenia elektronicznego.

Komponent techniczny - sprzęt stosowany w celu wygenerowania lub użycia danych służących do składania bezpiecznego podpisu elektronicznego lub poświadczenia elektronicznego.

Kwalifikowany dostawca usług zaufania oznacza dostawcę usług zaufania, który świadczy przynajmniej jedną kwalifikowaną usługę zaufania i któremu status kwalifikowany nadał organ nadzoru.

Kwalifikowana pieczęć elektroniczna oznacza zaawansowaną pieczęć elektroniczną, która została złożona za pomocą kwalifikowanego urządzenia do składania pieczęci elektronicznej i która opiera się na kwalifikowanym certyfikacie pieczęci elektronicznej.

Kwalifikowany podpis elektroniczny oznacza zaawansowany podpis elektroniczny, który jest składany za pomocą kwalifikowanego urządzenia do składania podpisu elektronicznego i który opiera się na kwalifikowanym certyfikacie podpisu elektronicznego.

Lista CRL - lista unieważnionych i zawieszonych certyfikatów klucza publicznego wystawionych przez dany podmiot świadczący usługi certyfikacyjne oraz ewentualnie unieważnionych zaświadczeń certyfikacyjnych wystawionych przez ten podmiot. Lista jest poświadczona elektronicznie przez podmiot świadczący usługi certyfikacyjne.

Moduł kluczowy - urządzenie współpracujące z komponentem technicznym, przechowujące klucze infrastruktury lub dane służące do składania bezpiecznych podpisów elektronicznych lub poświadczeń elektronicznych, lub klucze chroniące te dane, lub przechowujące części tych kluczy lub danych.

OCSP - (ang. Online Certificate Status Protocol) - protokół komunikacyjny oraz serwis on-line zawierający wskazania na aktywne, zawieszone i unieważnione certyfikaty klucza publicznego wystawione przez dany podmiot świadczący usługi certyfikacyjne.

Pieczęć elektroniczna oznacza dane w postaci elektronicznej dodane do innych danych w postaci elektronicznej lub logicznie z nimi powiązane, aby zapewnić autentyczność pochodzenia oraz integralność powiązanych danych.

PKI - ang. Public Key Infrastructure - Infrastruktura Klucza Publicznego, jest to system, na który składają się polityka, procedury i systemy komputerowe niezbędne do świadczenia usług uwierzytelniania, szyfrowania, integralności i niezaprzeczalności za pośrednictwem kryptografii klucza publicznego, klucza prywatnego i certyfikatów elektronicznych.

Podmiot składający pieczęć oznacza osobę prawną, która składa pieczęć elektroniczną.

Podpisujący oznacza osobę fizyczną, która składa podpis elektroniczny.

Podpis elektroniczny oznacza dane w postaci elektronicznej, które są dołączone lub logicznie powiązane z innymi danymi w postaci elektronicznej, i które użyte są przez podpisującego jako podpis.

Polityka - niniejsza polityka usług zaufania.
Poświadczenie elektroniczne są to dane w postaci elektronicznej, które wraz z innymi danymi, do których zostały dołączone lub logicznie z nimi powiązane, umożliwiają identyfikację podmiotu świadczącego usługi certyfikacyjne oraz spełniają następujące warunki:

a) są sporządzone za pomocą podlegających wyłącznej kontroli podmiotu świadczącego usługi certyfikacyjne bezpiecznych urządzeń do składania podpisów i danych służących do składania poświadczenia elektronicznego,
b) jakakolwiek zmiana danych poświadczonych jest rozpoznawalna.

Produkt oznacza sprzęt lub oprogramowanie lub odpowiednie komponenty sprzętu lub oprogramowania, które są przeznaczone do wykorzystania w świadczeniu usług zaufania.

Strona ufająca oznacza osobę fizyczną lub prawną, która polega na identyfikacji elektronicznej lub usłudze zaufania.

System identyfikacji elektronicznej oznacza system identyfikacji elektronicznej, w ramach którego wydaje się środki identyfikacji elektronicznej osobom fizycznym lub prawnym, lub osobom fizycznym reprezentującym osoby prawne.

Ścieżka certyfikacji - uporządkowany ciąg zaświadczeń certyfikacyjnych lub zaświadczeń certyfikacyjnych i certyfikatu utworzony w ten sposób, że przy pomocy danych służących do weryfikacji poświadczenia elektronicznego i nazwy wydawcy pierwszego zaświadczenia certyfikacyjnego na ścieżce możliwe jest wykazanie, że dla każdych dwóch bezpośrednio po sobie występujących zaświadczeń certyfikacyjnych lub zaświadczenia certyfikacyjnego i certyfikatu poświadczenie elektroniczne zawarte w jednym z nich zostało sporządzone przy pomocy danych służących do składania poświadczenia elektronicznego związanych z drugim z nich; dane służące do weryfikacji pierwszego poświadczenia elektronicznego są dla weryfikującego „punktem zaufania".

Środek identyfikacji elektronicznej oznacza materialną lub niematerialną jednostkę zawierającą dane identyfikujące osobę i używaną do celów uwierzytelniania dla usługi online.

Subskrybent jest to osoba fizyczna używająca certyfikatów PP Nota, która jest uprawniona do zgłoszenia żądań o wydanie certyfikatu zaawansowanego podpisu elektronicznego oraz wydanie dowodu wysłania oraz dowodu otrzymania na podstawie Umowy.

TLS - (ang. Transport Layer Security). Jest to protokół, który służy do bezpiecznej wymiany danych za pośrednictwem Internetu.

TTP - W kryptografii zaufana strona trzecia (TTP) to podmiot ułatwiający interakcje między dwiema stronami, które ufają stronie trzeciej; strona trzecia dokonuje przeglądu wszystkich krytycznych komunikatów dotyczących transakcji między stronami, w oparciu o łatwość tworzenia fałszywych treści cyfrowych.

Umowa jest to umowa na świadczenie usług certyfikacyjnych zaawansowanego podpisu elektronicznego oraz elektronicznych doręczeń zawarta pomiędzy Wydawnictwem Kwantum Sp. z o.o., a Subskrybentem.

Urządzenie do składania pieczęci elektronicznej oznacza skonfigurowane oprogramowanie lub skonfigurowany sprzęt, które wykorzystuje się do składania pieczęci elektronicznej.

Urządzenie do składania podpisu elektronicznego oznacza skonfigurowane oprogramowanie lub skonfigurowany sprzęt, które wykorzystuje się do składania podpisu elektronicznego.

Usługi certyfikacyjne - szeroka klasa usług dotyczących TTP obejmująca działania polegające na poświadczeniu wybranych informacji przez wygenerowanie podpisanego elektronicznie zaświadczenia certyfikacyjnego, jak certyfikacja kluczy publicznych, certyfikacja istnienia danych elektronicznych w określonym czasie, certyfikacja przedstawienia danych elektronicznych przez określonych użytkowników w określonym czasie.

Usługa rejestrowanego doręczenia elektronicznego (niekwalifikowana) oznacza usługę umożliwiającą:

a) przesłanie danych między stronami trzecimi drogą elektroniczną,
b) zapewniającą dowody związane z posługiwaniem się przesyłanymi danymi, w tym dowód wysłania i otrzymania danych, oraz
c) chroniącą przesyłane dane przed ryzykiem utraty, kradzieży, uszkodzenia lub jakiejkolwiek nieupoważnionej zmiany.

Usługa rejestrowanego doręczenia elektronicznego (kwalifikowana) oznacza usługę rejestrowanego doręczenia elektronicznego, która spełnia następujące wymogi:

a) są świadczone przez co najmniej jednego kwalifikowanego dostawcę usług zaufania,
b) z dużą dozą pewności zapewniają identyfikację nadawcy,
c) zapewniają identyfikację adresata przed dostarczeniem danych,
d) wysłanie i otrzymanie danych jest zabezpieczone zaawansowanym podpisem elektronicznym lub zaawansowaną pieczęcią elektroniczną kwalifikowanego dostawcy usług zaufania w taki sposób, by wykluczyć możliwość niewykrywalnej zmiany danych,
e) każda zmiana danych niezbędna do celów wysłania lub otrzymania danych jest wyraźnie wskazana nadawcy i adresatowi danych,
f) data i czas wysłania, otrzymania i wszelkiej zmiany danych są wskazane za pomocą kwalifikowanego elektronicznego znacznika czasu.

Usługa zaufania oznacza usługę elektroniczną zazwyczaj świadczoną za wynagrodzeniem i obejmującą:

a) tworzenie, weryfikację i walidację podpisów elektronicznych, pieczęci elektronicznych lub elektronicznych znaczników czasu, usług rejestrowanego doręczenia elektronicznego oraz certyfikatów powiązanych z tymi usługami lub
b) tworzenie, weryfikację i walidację certyfikatów uwierzytelniania witryn internetowych lub
c) konserwację elektronicznych podpisów, pieczęci lub certyfikatów powiązanych z tymi usługami.

Ustawa o ochronie danych osobowych jest to ustawa z dnia 29 sierpnia 1997 roku o ochronie danych osobowych.

Uwierzytelnianie oznacza proces elektroniczny, który umożliwia identyfikację elektroniczną osoby fizycznej lub prawnej, lub potwierdzenie pochodzenia oraz integralności weryfikowanych danych w postaci elektronicznej.

Walidacja oznacza proces weryfikacji i potwierdzenia ważności podpisu elektronicznego lub pieczęci.

Zaawansowana pieczęć elektroniczna oznacza pieczęć elektroniczną, która spełnia następujące wymogi:

a) jest unikalnie przyporządkowana podmiotowi składającemu pieczęć,
b) umożliwia ustalenie tożsamości podmiotu składającego pieczęć,
c) jest składana przy użyciu danych służących do składania pieczęci elektronicznej, które podmiot składający pieczęć może, mając je z dużą dozą pewności pod swoją kontrolą, użyć do złożenia pieczęci elektronicznej oraz
d) jest powiązana z danymi, do których się odnosi, w taki sposób, że każda późniejsza zmiana danych jest rozpoznawalna.

Zaawansowany podpis elektroniczny oznacza podpis elektroniczny, który spełnia następujące wymogi:

a) jest unikalnie przyporządkowany podpisującemu,
b) umożliwia ustalenie tożsamości podpisującego,
c) jest składany przy użyciu danych służących do składania podpisu elektronicznego, których podpisujący może, z dużą dozą pewności, użyć pod wyłączną swoją kontrolą oraz
d) jest powiązany z danymi podpisanymi w taki sposób, że każda późniejsza zmiana danych jest rozpoznawalna.

Zaświadczenie certyfikacyjne - elektroniczne zaświadczenie, za pomocą którego dane służące do weryfikacji poświadczenia elektronicznego są przyporządkowane do podmiotu świadczącego usługi certyfikacyjne lub ministra właściwego do spraw gospodarki i które umożliwia identyfikację tego podmiotu lub organu.

X.509 - Standard definiujący konstrukcję certyfikatu klucza publicznego i listy certyfikatów unieważnionych.

1.3 Uczestnicy infrastruktury PKI opisanej w Polityce

Polityka opisuje całą infrastrukturę PKI niezbędną do świadczenia usług zaufania przez Kwantum. Jej głównymi uczestnikami są:

1) Ośrodek Certyfikacji Kwantum,
2) Subskrybenci,
3) Strony ufające.

W ramach Polityki Certyfikacyjnej Kwantum są wystawiane następujące certyfikaty:

Nazwa typu certyfikatu i zakres zastosowania	Poziom bezpieczeństwa i wiarygodności
Certyfikat dla zaawansowanego podpisu elektronicznego – podpis niekwalifikowany	Bardzo wysoki poziom wiarygodności tożsamości podmiotu certyfikatu. Certyfikaty wydawane są członkom korporacji prawniczych. Certyfikaty powinny być stosowane do składania zaawansowanych podpisów elektronicznych, zapewniających integralność oraz niezaprzeczalność podpisywanej informacji. Certyfikaty nie mogą być stosowane do szyfrowania danych lub kluczy kryptograficznych (ogólnie, w operacjach, których celem jest nadanie informacji cech poufności).
Certyfikat do potwierdzania dowodów wysłania i dowodów otrzymania elektronicznej przesyłki w PP Nota – doręczenie niekwalifikowane	Bardzo wysoki poziom wiarygodności tożsamości podmiotu certyfikatu. Certyfikat jest emitowany i użytkowany przez Kwantum, jako operatora PP Nota.

Kwantum jako operator PP Nota nie odpowiada za skutki użycia certyfikatów zaawansowanego podpisu elektronicznego do innych celów niż opisano w niniejszej Polityce. Ograniczenie to odnosi się zarówno do Subskrybentów, jak i Stron ufających.

1.3.1 Ośrodek certyfikacji Kwantum

Ośrodek Certyfikacji Kwantum wystawia certyfikaty zaawansowanego podpisu elektronicznego oraz dowody wysłania i dowody otrzymania dla Subskrybentów i udostępnia informacje niezbędne do weryfikacji ważności wydanych przez siebie certyfikatów.

1.3.2 Subskrybent

Subskrybent jest to osoba fizyczna używająca certyfikatów PP Nota, która jest uprawniona do zgłoszenia żądań o wydanie certyfikatu zaawansowanego podpisu elektronicznego oraz wydanie dowodu wysłania oraz dowodu otrzymania.

Subskrybentem są wyłącznie osoby fizyczne, członkowie korporacji prawniczych w Polsce (Krajowej Izby Radców Prawnych lub Krajowej Rady Adwokackiej) posiadający aktualne uprawnienia radcowskie lub adwokackie, którzy zawarli z Kwantum umowę na świadczenie usług zaufania.

1.3.3 Strony ufające

Przez osobę ufającą rozumie się osobę fizyczną, prawną lub jednostkę organizacyjną nieposiadającą osobowości prawnej, która podejmuje działania lub jakąkolwiek decyzję w zaufaniu do podpisanych elektronicznie lub cyfrowo lub poświadczonych elektronicznie danych z wykorzystaniem klucza publicznego zawartego w certyfikatach podpisów zaawansowanych, dowodach wysłania oraz dowodach otrzymania emitowanych przez Kwantum.

Strona ufająca powinna zwrócić uwagę na rodzaj certyfikatu / dowodu (wysłania lub otrzymania) oraz Politykę, według której zostały one wydane. W przypadku wątpliwości, czy dany certyfikat lub dowód został wydany poprawnie oraz czy jest używany przez upoważniony do tego podmiot strona ufająca jest zobowiązana do zgłoszenia wątpliwości do Kwantum. Zgłoszenie może być dokonane telefonicznie pod numerem infolinii w godzinach jej pracy lub całodobowo poprzez formularz kontaktowy dostępny na www.pocztaprawnicza.pl

1.4 Identyfikacja Polityki

Nazwa polityki	Polityka świadczenia usług zaufania Poczta Prawnicza NOTA
Status wersji	Aktualna
Identyfikator polityki OID (ang. *Object Identyfier*)	
Data wydania	25.10.2019 r.
Data ważności	Do odwołania

Aktualne oraz poprzednie wersje Polityki są publikowane na stronie internetowej www.pocztaprawnicza.pl

1.5 Historia zmian

Numer wersji	Status	Data wydania
1.0	Dokument zatwierdzony przez Zarząd Wydawnictwa Kwantum Sp. z o.o. – wersja obowiązująca od dnia wpisu Wydawnictwa Kwantum Sp. z o.o. z siedzibą w Sopocie do rejestru dostawców usług zaufania na podstawie na podstawie ustawy z dnia 5 września 2016 r. o usługach zaufania oraz identyfikacji elektronicznej	25.10.2019 r.

1.6 Zastosowanie dowodów wysłania oraz dowodów otrzymania

Dowód wysłania oraz dowód otrzymania służy poświadczeniu tożsamości nadawcy i adresata, daty i czasu oraz integralności danych, z którymi dana wysyłka lub odbiór są powiązane.

1.7 Zarządzanie polityką certyfikacji

Wszelkie zmiany niniejszej Polityki, z wyjątkiem takich, które naprawiają oczywiste błędy redakcyjne lub stylistyczne, wymagają nadania nowego numeru wersji.

1.7.1 Podmiot odpowiedzialny

Podmiotem uprawnionym do administrowania niniejszą polityką certyfikacji, w tym zatwierdzania zmian jest Zarząd Wydawnictwa Kwantum Sp. z o.o. z siedzibą w Sopocie

Wszelką korespondencję związaną ze świadczeniem usług zaufania elektronicznych doręczeń należy kierować na adres siedziby Kwantum:

Wydawnictwo Kwantum Sp. z o.o.
1 Maja 5
81-807 Sopot
Polska
Tel. +48 608 57 99 22
e-mail: kontakt@kwantum.com.pl

NIP 584 24 07 041
KRS 0000060215
Sąd Rejonowy Gdańsk-Północ VIII Wydział KRS

1.7.1 Procedury zatwierdzania Polityki

Polityka jest zatwierdzana przez Zarząd Kwantum. Po zatwierdzeniu otrzymuje status obowiązujący ze wskazaniem daty początku obowiązywania. Najpóźniej tego dnia jest ona publikowana na stronie internetowej www.pocztaprawnicza.pl

2 Publikowanie i repozytorium

2.1 Repozytorium

Informacje dotyczące usług zaufania świadczonych przez Kwantum, w tym informacje na temat sposobu zawierania umów, obsługi zamówień na usługi elektronicznych doręczeń są udostępniane wszystkim zainteresowanym na stronie internetowej Kwantum pod adresem www.pocztaprawnicza.pl.

2.2 Publikacja w repozytorium

W ramach swoich obowiązków Kwantum prowadzi repozytorium. Nowe wersje Polityk, regulaminów, umów itp. są publikowane elektronicznie w postaci plików pdf niezwłocznie po ich zatwierdzeniu. Do podstawowych informacji publikowanych w repozytorium należą:

1) obowiązującą wersję oraz wersje archiwalne Polityki,
2) regulamin PP Nota,
3) wzory umów i zamówień,
4) opisy procedur generowania oraz umarzania certyfikatów zaawansowanego podpisu elektronicznego,
5) opis zasad uzyskiwania dowodów wysłania oraz dowodów otrzymania dla usługi elektronicznych doręczeń oraz
6) certyfikaty podpisów elektronicznych klucza publicznego.

2.3 Dostęp do repozytorium

Informacje publikowane w repozytorium na stronach internetowych Kwantum są dostępne dla wszystkich zainteresowanych.

Informacje publikowane w repozytorium są zabezpieczone przed nieautoryzowanym zmienianiem, dodawaniem i usuwaniem oraz są przechowywane z zachowaniem kopii zapasowych.

Kwantum realizuje kontrolę dostępu uniemożliwiającą dokonywanie nieautoryzowanych zmian w dokumentach umieszczonych w repozytorium, a w przypadku jakichkolwiek działań ze strony nieuprawnionych podmiotów lub osób, które mogłyby naruszyć integralność publikowanych danych, Kwantum podejmie niezwłoczne działania prawne wobec takich podmiotów oraz dołoży wszelkich starań celem ponownego opublikowania właściwych danych w repozytorium

3 PP Nota – usługi elektronicznych doręczeń

3.1 Użytkownicy PP Nota

Poczta Prawnicza Nota zapewnia płatną obsługę elektronicznych doręczeń (usługa zaufania) dla członków korporacji prawniczych (Krajowa Izba Radców Prawnych oraz Krajowa Rada Adwokacka) posiadających aktualne uprawnienia radcy prawnego lub adwokata. Uprawnienia te są weryfikowane poprzez przyjętą procedurą zakładania konta na etapie jego aktywacji w PP Nota.

Usługi elektronicznych doręczeń w PP Nota są świadczona dla Użytkowników, którzy:

- aktywowali skrzynkę do doręczeń w PP Nota,
- zaakceptowali regulamin PP Nota podpisując go elektronicznie (wraz z kolejnymi wersjami regulaminu) oraz
- posiadają środki finansowe na koncie, które pozwalają na realizacje płatnej usługi elektronicznego doręczenia przez PP Nota.

Dla potrzeb potwierdzenia wysłania i odbioru przesyłek PP Nota wystawia elektroniczne poświadczenia tj.: dowody wysłania oraz dowody otrzymania.

3.2 Identyfikacja i uwierzytelnianie w PP Nota

W tej części opisano procedurę zakładania nowego konta w PP Nota przez uprawniona osobę (członka korporacji prawniczej posiadającego uprawnienia) oraz logowanie do PP Nota przez Użytkownika, który już posiada skrzynkę do doręczeń w PP Nota (wcześniej ją utworzył).

Kwantum okresowo do bazy danych potencjalnych Użytkowników PP Nota importuje z baz danych Krajowej Izby Radców Prawnych oraz Krajowej Rady Adwokackiej dane radców prawnych oraz adwokatów posiadających aktualne uprawnienia. Do bazy importowane są następujące dane:

- Imię
- Nazwisko

- Rodzaj (radca prawny , adwokat)
- Nr legitymacji (radcowskiej lub adwokackiej)
- Przynależność do izby (radcowskiej lub adwokackiej)

Aktualizacja jest dokonywana dwa razy w miesiącu oraz zawsze na żądanie radcy prawnego lub adwokata, który nie może aktywować konta z powodu braku jego danych w PP Nota i zwróci się z żądaniem aktualizacji do Kwantum. W efekcie, w bazie danych potencjalnych Użytkowników PP Nota znajduje się pełna lista radców prawnych i adwokatów uprawnionych do wykonywania zawodu.

Do PP Nota może się zalogować tylko i wyłącznie Użytkownik, który aktywował skrzynkę do doręczeń w PP Nota.

3.2.1 Aktywowanie skrzynki do doręczeń w PP Nota

Potencjalny Użytkownik chcąc aktywować skrzynkę do doręczeń w PP Nota musi wejść na stronę internetową www.pocztaprawnicza.pl oraz uruchomić funkcję Aktywuj skrzynkę. Uwierzytelnienie Użytkownika wymaga wpisania przez niego imienia, nazwiska, numeru legitymacji oraz złożenia elektronicznego podpisu zaawansowanego:

1) kwalifikowanego elektronicznego podpisu weryfikowanego certyfikatem kwalifikowanego dostawcy,
2) podpisania profilem zaufanym przy pomocy usługi „Podpisz dokument elektronicznie – wykorzystaj podpis zaufany" z serwisu obywatel.gov.pl

Na podstawie zgodności danych zaimportowanych i zapisanych w bazie danych PP Nota oraz danych wpisanych przez Użytkownika oraz danych pochodzących z certyfikatu podpisu elektronicznego następuje identyfikacja Użytkownika i jeżeli dane te są zgodne, to następuje aktywacja skrzynki do doręczeń Użytkownika w PP Nota.

Brak zgodności danych powoduje, że skrzynka do doręczeń nie zostaje aktywowana. W takiej sytuacji, uprawniony Użytkownik jest zobowiązany skierować swoje żądanie o aktywację skrzynki do doręczeń do Kwantum (zob. 1.7.1. Dane kontaktowe).

3.2.2 Logowanie Użytkownika do PP Nota

W trakcie procesu aktywacji skrzynki do doręczeń w PP Nota, Użytkownik jest zobowiązany wprowadzić swój elektroniczny klucz (login i hasło), którymi będzie się uwierzytelniał w PP Nota.

3.3 Przygotowanie, wysyłka i odbiór elektronicznej przesyłki

W celu wysyłki lub odebrania elektronicznej przesyłki Użytkownik musi się zalogować do PP Nota wykorzystują swój login i hasło, które otrzymał podczas procesu aktywacji skrzynki do doręczeń w PP Nota.

Kwantum, w celu potwierdzenia wysyłki wystawia elektroniczny Dowód wysłania, a w celu potwierdzenia otrzymania (doręczenia) wystawia elektroniczny Dowód otrzymania.

3.3.1 Wysyłanie przesyłek w PP Nota

Po zalogowaniu do PP Nota każdy aktywny Użytkownik (posiada aktywną skrzynkę do doręczeń w PP Nota) może dokonać elektronicznego doręczenia do innego aktywnego Użytkownika. Przedmiot doręczenia składa się z:

- pisma przewodniego przesyłki oraz
- plików stanowiących załączniki
- plik XML zawierający metadane przesyłki

Wysłanie przesyłki jest dokonywane przez PP Nota dopiero po podpisaniu przesyłki zaawansowanym podpisem elektronicznym (jak przy czynności aktywowania skrzynki do doręczeń w PP Nota).

Elektroniczna przesyłka jest zapisywana w bazie danych i udostępniana odbiorcy.

3.3.2 Odbieranie przesyłek w PP Nota – fikcja doręczenia

Elektroniczna przesyłka przesłana do aktywnego Użytkownika PP Nota jest zapisywana w bazie danych i udostępniana wszystkim adresatom przesyłki.

Fikcja doręczenia w PP Nota – przesyłkę uznaje się za doręczoną w momencie, gdy zostanie zapisana w bazie danych i udostępniona odbiorcy

3.3.3 Dowody wysłania

Kwantum, w momencie zapisania przesyłki w bazie danych PP Nota, wystawia Dowód wysłania. Dowód ten zawiera:

- informację o zawartości przesyłki,
- znacznik czasu oraz
- certyfikat e-Doręczenia wystawianym przez Kwantum i używanym do oznaczania dowodów wysłania (również dowodów otrzymania).

3.3.4 Dowody otrzymania

Dla potrzeb wystawiania Dowodu otrzymania przyjmuje się tzw. fikcję doręczenia, co Subskrybenci akceptują podpisując Regulamin. W związku z powyższym, Dowód otrzymania wystawiany przez Kwantum zawiera dokładnie ten sam zestaw informacji co Dowód wysłania.

4 PP Nota – zaawansowany podpis elektroniczny

Wydawnictwo Kwantum Sp. z o.o. jako Operator PP NOTA, świadczy płatną usługę zaufania polegającą na wydawaniu certyfikatów niekwalifikowanego podpisu elektronicznego.

Certyfikaty wydawane przez Wydawnictwo Kwantum Sp. z o.o. mają umożliwiać Subskrybentom podpisywanie zaawansowanym podpisem elektronicznym pism wysyłanych za pośrednictwem PP NOTA **[e-podpis PP NOTA]** .

Jako, że usługa doręczeń elektronicznych PP NOTA jest adresowana tylko do członków korporacji prawniczych również certyfikaty niekwalifikowanego podpisu elektronicznego będą wydawane wyłącznie członkom korporacji prawniczych (adwokatom i radcom prawnym).Certyfikaty są wydawane wyłączenie w celu podpisywania pism wysyłanych poprzez PP NOTA oraz potwierdzania elektronicznej wysyłki w PP NOTA

Wyżej wymienione certyfikaty są wydawane zgodnie z wymaganiami określonymi w Rozporządzenie Parlamentu Europejskiego i Rady (UE) NR 910/2014 w sprawie identyfikacji elektronicznej i usług zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznym oraz uchylające dyrektywę 1999/93/WE.

Podmiotem wydającym certyfikat jest Wydawnictw Kwantum Sp. z o.o. z siedzibą w Sopocie przy ul. 1 Maja 5.

Polityka Certyfikacji e-podpisu PP NOTA określa zasady stosowane przez Wydawnictwo Kwantum Sp. z o.o. w trakcie świadczenia usług zaufania w szczególności:

1. Wydawania certyfikatów dla zaawansowanego podpisu elektronicznego
2. Zawieszenia, cofnięcia zawieszenia i unieważnienia certyfikatów

PP NOTA, w zakresie wydawania certyfikatów niekwalifikowanych została zaprojektowana i wdrożona w taki sposób, aby spełnić wymagania nałożone przez krajową Ustawę o Usługach Zaufania i stosowne rozporządzenia, a także wymagania innych, obowiązujących norm prawnych oraz istniejących standardów międzynarodowych w zakresie tworzenia i funkcjonowania systemów PKI, w szczególności z uwzględnieniem zaleceń zawartych w RFC 3647 "Certificate Policy and Certification Practices Framework".

4.1 Identyfikacja i uwierzytelnianie

1. Wydanie certyfikatów e-podpisu PP NOTA jest możliwe tylko dla osób, które posiadają aktywne skrzynki do doręczeń w PP NOTA.
2. Procedura otwierania skrzynki do doręczeń w PP NOTA została opisana w dziale 3 „PP Nota – usługi elektronicznych doręczeń”
3. Certyfikaty [e-podpisu PP NOTA] wydawane są na wniosek zainteresowanego. Wydanie certyfikatu [e-podpisu PP NOTA] następuje po uruchomieniu funkcji „Generuj certyfikat e-podpisu” w PP NOTA.
4. Przy wydawaniu [e-podpisu PP NOTA] Wydawnictwo Kwantum, jako emitent certyfikatu e-podpisu, posługuje się danymi Subskrybenta zweryfikowanymi na etapie zakładania skrzynki do doręczeń w PP NOTA. Oznacza to, że nie prowadzi się osobnej procedury identyfikacji dla wydania certyfikatu e-podpisu.

4.2 Wystawienie kolejnego certyfikatu

Wydawnictwo Kwantum emituje certyfikaty [e-podpisu PP NOTA] według zasady, że jeden Subskrybent może posiadać tylko jeden ważny certyfikat [e-podpisu PP NOTA]. Oznacza to, że wystawienia kolejnego certyfikatu [e-podpisu PP NOTA], jest możliwe pod warunkiem umorzenia wcześniej wydanego certyfikatu.
W związku z powyższym, procedura wystawienia kolejnego certyfikatu [e-podpisu PP NOTA] jest, identyczna z procedurą wystawienia pierwszego certyfikatu.

4.3 Umorzenie certyfikatów

Procedura umorzenia certyfikatu jest uruchamiana poprzez wypełnienie przez Subskrybenta wniosku o umorzenie w PP NOTA. Wniosek dostępny jest po zalogowaniu do PP NOTA. Złożenie wniosku o umorzenie certyfikatu [e-podpisu PP NOTA] prowadzi do umorzenia certyfikatu [e-podpisu PP NOTA] wydanego Subskrybentowi.
Wydawnictwo Kwantum, jako Operator PP NOTA, opublikuje numery umorzonych certyfikatów na liście CRL dostępnej na stronie www.pocztaprawnicza.pl .

4.4 Zasady nadawania nazw

Certyfikaty wydawane w ramach PP NOTA są certyfikatami w standardzie x.509v3. Certyfikaty są tworzone w zgodzie z wymogami zawartymi w RFC 5280 Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile, z uwzględnieniem wymagań ze standardów europejskich ETSI EN 319 412-(1 do 2).

4.4.1 Typy nazw

Pole identyfikatora podmiotu ‘subject’ umożliwia zidentyfikowanie podmiotu związanego z kluczem publicznym, umieszczonym w polu klucza publicznego wydanego certyfikatu. Pole ‘subject’ musi zawierać niepustą nazwę wyróżniającą podmiotu. Zawartość pola Odbiorca certyfikatu będzie zgodna z wytycznymi rekomendacji ITU-T X.520.

4.4.2 Konieczność używania nazw znaczących

W celu zapewnienia możliwości jednoznacznej identyfikacji Odbiorcy certyfikatu, w polu identyfikatora podmiotu ‘subject’ wystąpią co najmniej atrybuty:

Zawartość certyfikatu dla zaawansowanego podpisu elektronicznego:

o Kraj (countryName)	pole obowiązkowe: wartość na podstawie danych dotyczących osoby - „Obywatelstwo”, 2 literowy kod zgodny z ISO 3166
o Nazwa wyróżniająca (commonName) -	pole obowiązkowe: Jest to połączenie pól „Imię/Imiona” +„ ” + „Nazwisko”
o Nazwisko (Surname) -	pole obowiązkowe: wartość na podstawie danych dotyczących osoby - „Nazwisko”
o Pierwsze Imię (givenName) –	pole obowiązkowe: wartość na podstawie danych dotyczących osoby - „Pierwsze imię”
o Drugie Imię (givenName) –	pole nie obowiązkowe: wartość na podstawie danych dotyczących osoby – „Drugie imię”
o Numer seryjny (serialNumber) -	pole obowiązkowe: numer legitymacji radcowskiej lub adwokackiej, będzie zawierać wartość na podstawie danych dotyczących posiadanej legitymacji - „numer uprawnień”. Składnia pola bazuje

	na Normie Europejskiej „ETSI EN 319 412-1 V1.1.1 Certificate Profiles Part 1: Overview and common data structures" Rozdział „5.1.3 Natural person semantics identifier". Pprzykładowa składnia to: AWDPL-WAW/Adw/500 Oznacza ona adwokata z warszawskiej Okręgowej Izby Adwokackiej wpisanego na listę na pozycji 500.

4.4.3 Unikalność nazw

Operator PP NOTA zapewnia unikalność nazw w domenie wystawcy certyfikatów, poprzez weryfikację już na poziomie rejestracji Użytkowników, że nie zostaną zarejestrowani różni odbiorcy z tym samym numerem uprawnień radcowskich lub adwokackich. Użytkownicy posiadają również unikalne w PP NOTA loginy. W nazwie wyróżniającej certyfikatu (DN) używany jest identyfikator Użytkownika w formacie login@pocztaprawnicza.pl oraz jego numer uprawnień, co pozwala jednoznacznie zidentyfikować właściciela certyfikatu spośród Subskrybentów PP NOTA. Raz wykorzystana nazwa DN, nie może być wykorzystana przez innego Odbiorcę certyfikatu przez cały okres życia wystawcy certyfikatów.

4.5 Wymagania dotyczące cyklu życia certyfikatów

PP NOTA działa w oparciu o zasadę, że jeden Użytkownik może posiadać tylko jeden aktualny certyfikat PP NOTA.

4.5.1 Wniosek o wydanie certyfikatu

Wniosek o wydanie certyfikatu nie ma formy wydzielonego dokumentu – procedura wydawania certyfikatu jest uruchamiana po zainicjowaniu funkcji odpowiedniej funkcji zawartej w PP NOTA.

Oznacza to, że:

- Uzyskanie certyfikatów PP NOTA dostępne jest tylko dla osób, które aktywowały skrzynkę do doręczeń w PP"NOTA.
- Tożsamość Użytkowników certyfikatów została zweryfikowana na etapie uruchamiania skrzynki do doręczeń w PP NOTA.
- Wydawanie certyfikatów odbywa się na wyraźne życzenie osoby, która będzie certyfikat wykorzystywała.

4.5.2 Obsługa wniosku o wydanie certyfikatu

Wydania certyfikatów obsługiwane jest automatycznie. Użycie przez zalogowanego Użytkownika PP NOTA funkcji „Generuj certyfikat" uruchamia proces generowanie certyfikatu. Certyfikat jest wytwarzany w oparciu o dane zalogowanego Użytkownika. Koniec procesu obsługi wniosku o wydanie certyfikatu sygnalizowany jest poprzez komunikat „Certyfikat został wygenerowany". Na tym etapie pojawia się hasło do wygenerowanego certyfikatu w formacie PFX.

4.5.3 Wydanie certyfikatu

Wydanie certyfikatu odbywa się zdalnie. Wydanie certyfikatu jest obsługiwane z poziomu PP NOTA za pomocą funkcji „Pobierz certyfikat". Funkcja „Pobierz certyfikat" jest dostępna tylko wówczas, kiedy dla Użytkownika zostały wygenerowane certyfikaty, które oczekują na pobranie. Funkcja „Pobierz certyfikat" uruchamia procedurę pobierania i instalacji certyfikatów. Procedura działa w oparciu o standardowe funkcje systemu operacyjnego Windows. Procedura jest realizowana w następujących krokach:

- Pobranie pliku z certyfikatem
- Instalacja certyfikatu w składzie certyfikatów przy użyciu otrzymanego hasła

4.5.4 Instalacja certyfikatu w składzie certyfikatów systemu operacyjnego „Windows". Zasady używania certyfikatu i pary kluczy

Użytkownik zobowiązuje się do:

1. wykorzystywania certyfikatu zgodnie z jego przeznaczeniem wskazanym w danym certyfikacie;
2. wykorzystywania certyfikatu tylko w okresie ważności certyfikatu w nim wskazanym;
3. ochrony swojego klucza prywatnego;
4. niezwłocznego zgłoszenia do Operatorowi PP NOTA żądania unieważnienia certyfikatu w przypadkach przewidzianych w prawie, umowie, Polityce Świadczenie Usług PP NOTA.

Umowa może określić bardziej szczegółowy zakres odpowiedzialności Użytkownika.

4.5.5 Odnowienie certyfikatu

PP NOTA nie przewiduje możliwości odnowienia certyfikatu. Oznacza to, że w każdej sytuacji, w której Użytkownik chciałby ponownie użytkować certyfikat PP NOTA należy w pierwszym kroku unieważnić aktualny certyfikat i złożyć zlecenie wydania nowego certyfikatu. Każdorazowo wydanie kolejnego certyfikatu jest realizowany tak jak proces wydania pierwszego certyfikatu, to jest łącznie z procesem pełnej identyfikacji i uwierzytelniania Użytkownika.

Użytkownik jest powiadamiany w systemie Nota o zbliżającym się końcu ważności swojego certyfikatu. Może wygenerować nowy?

4.5.6 Modyfikacja zawartości certyfikatu

PP NOTA nie przewiduje możliwości modyfikacji zawartości certyfikatu. Oznacza to, że zmiana danych Użytkownika zmusza do unieważnienia aktualnego certyfikatu i złożenia zlecenia wydania nowego certyfikatu. Każdorazowo wydanie kolejnego certyfikatu jest realizowany tak jak proces wydania pierwszego certyfikatu, to jest łącznie z procesem pełnej identyfikacji i uwierzytelniania Użytkownika.

4.6 Zawieszenie, cofnięcie zawieszenia

4.6.1 Unieważnienie certyfikatu

W przypadku utraty kontroli nad certyfikatem Użytkownik zobowiązany jest do natychmiastowego zlecenia unieważnienia certyfikatu. Zlecenie dostępne jest po zalogowaniu do PP NOTA. Operator zobowiązany jest do niezwłocznego unieważnienia certyfikatu.
Unieważnienie certyfikatu zostanie odnotowane poprzez umieszczenie unieważnionego certyfikatu na liście CRL. Dodatkowo unieważnienie certyfikatu będzie sygnalizowane poprzez zmianę statusu tego certyfikatu na liście certyfikatów dostępnych w PP NOTA.

5 Procedury bezpieczeństwa organizacyjnego, operacyjnego i fizycznego

5.1 Bezpieczeństwo fizyczne

1. Serwer wydający certyfikaty PP NOTA zlokalizowany jest w chmurze obliczeniowej „Microsoft Azure”
2. Chmura obliczeniowa „Microsoft Azure” została zaprojektowana i wykonana w oparciu o cztery podstawowe zasady:
    a. Zasada bezpieczeństwa
    b. Zasada zgodności z prawem i normami branżowymi
    c. Zasada zabezpieczenia prywatności użytkowników chmury
    d. Zasada transparentności działania chmury
3. Zgodnie z zasadą zgodności z prawem i normami branżowymi chmura obliczeniowa „Microsoft Azure” jest cyklicznie poddawana audytom, których celem jest potwierdzenie działania chmury zgodnie z normami branżowymi i zasadami prawa.
4. Zgodnie z zasadą transparentności wyniki audytów dostępne są na stronie: https://servicetrust.microsoft.com/ViewPage/MSComplianceGuideV3.

Podsumowując:
Wydawnictwo Kwantum jako operator PP NOTA, w zakresie:

- fizycznego zabezpieczenia serwera generującego certyfikaty PP NOTA oraz
- fizycznego zabezpieczenia danych zgromadzonych w związku z wydanymi certyfikatami

całkowicie opiera się na procedurach bezpieczeństwa stosowanych przez administratora Chmury Obliczeniowej „Microsoft Azure”.

5.2 Zabezpieczenia organizacyjne

5.2.1 Zaufane role

W Centrum Certyfikacji funkcjonują następujące role:

1. Inspektor Bezpieczeństwa Systemu, który nadzoruje wdrożenie i stosowanie wszystkich procedur bezpiecznej eksploatacji systemu teleinformatycznego Centrum Certyfikacji;

2. Administrator Systemu, który instaluje, konfiguruje i zarządza systemem teleinformatycznym oraz odtwarza dane z kopii zapasowej;
3. Inspektor ds. Audytu analizujący zapisy rejestrów zdarzeń mających miejsce w Centrum Certyfikacji.

5.2.2 Liczba osób wymaganych do realizacji zadań

Zgodnie z procedurami Centrum Certyfikacji nie występują czynności, które wymagają obecności więcej niż jednej osoby.

5.2.3 Identyfikacja oraz uwierzytelnianie każdej roli

Identyfikacja oraz uwierzytelnienie osób pełniących role jest dokonywane dzięki przydział indywidualnych imiennych kont w systemie i określony zakres uprawnień uzasadniony zakresem wykonywanych obowiązków.

5.2.4 Role, które nie mogą być łączone

Żadne role w Centrum Certyfikacji nie mogą być łączone.

5.3 Nadzorowanie personelu

5.3.1 Kwalifikacje, doświadczenie i poświadczenia bezpieczeństwa

Wydawnictwo Kwantum Sp. z o.o. jako operator PP NOTA gwarantuje, że osoby wykonujące zadania w ramach Centrum Certyfikacji:

- posiadają pełną zdolność do czynności prawnych;
- posiadają minimum wykształcenie średnie,
- zawarły umowę o pracę lub inną umowę cywilno-prawną precyzującą rolę, którą mają pełnić i określającą wynikające z niej prawa i obowiązki,
- przeszły niezbędne przeszkolenie z zakresu obowiązków, które będą wykonywały,
- zostały przeszkolone w zakresie ochrony danych osobowych,
- w umowie zawarto klauzule o nieujawnianiu informacji wrażliwych z punktu widzenia bezpieczeństwa urzędu certyfikacji lub poufności danych Subskrybenta,
- personel Centrum Certyfikacji, zwłaszcza osoby piastujące tzw. zaufane role, zobowiązane są postępować zgodnie z przepisami Rozporządzenia eIDAS i Ustawy z dnia 5 września o usługach zaufania oraz identyfikacji elektronicznej.

5.3.2 Wymagania szkoleniowe

Osoby pełniące role w Centrum Certyfikacji na bieżąco aktualizują swoją widzę niezbędną do zarządzania procesem certyfikacyjnym. Szkolenie odbywa się w trybie samokształcenia i prowadzone jest w oparciu o materiały udostępniane przez producentów oprogramowania. Samokształcenie obejmuje zakres wiedzy wymagany na danym stanowisku. Samokształcenie w szczególności dotyczy:

- technologii tworzenia certyfikatów

- obsługi sprzętu i oprogramowania stosowanego do elektronicznego przetwarzania danych, automatycznego przetwarzania danych w sieciach i systemach teleinformatycznych,
- przestrzegania zasad bezpieczeństwa systemów teleinformatycznych.

5.3.3 Częstotliwość i sekwencja rotacji zadań

Niniejsza Polityka nie określa wymagań w tym zakresie.

5.3.4 Kwestie dyscyplinarne

W przypadku wykrycia, że pracownik Centrum Certyfikacji wykonał nieuprawnione działania, może się on narazić na sankcje wynikające z Kodeksu Pracy oraz innych przepisów, w tym m.in. z Ustawy o podpisie elektronicznym czy Kodeksu Karnego.

5.3.5 Wymagania dla podwykonawców

Dopuszcza się pracę w systemie osób niebędących pracownikami Wydawnictwa Kwantum. W takim przypadku, wszelkie prace, które są wykonywane w Centrum Certyfikacji nadzorowane są przez osoby pełniące role w Centrum Certyfikacji Wydawnictwa Kwantum.

5.3.6 Dokumentacja dla personelu

W ramach realizacji obowiązków służbowych, udostępnia się pracownikom niezbędną dokumentację, wymaganą do realizacji obowiązków służbowych. W szczególności obejmuje ona:

- Politykę certyfikacji,
- wzory umów związanych ze świadczeniem usług certyfikacyjnych,
- zakres obowiązków i uprawnień wynikających z pełnionej roli

5.4 Rejestracja zdarzeń – do weryfikacji

5.4.1 Typy rejestrowanych zdarzeń

W celu zapewniania jak najwyższego poziomu bezpieczeństwa i zaufania do Centrum Certyfikacji, jest ono zobowiązane do archiwizowania wszystkich istotnych zdarzeń związanych z funkcjonowaniem systemu. W szczególności są to zdarzenia:

- Systemowe (generowane przez sprzęt i oprogramowanie Centrum Certyfikacji),
- Błędy (zdarzenia krytyczne dla funkcjonowania Centrum Certyfikacji),
- Audytu (związane z przeglądem rejestrów zdarzeń Centrum Certyfikacji).

Rejestry przechowywane są w postaci elektronicznej. Każdy z rejestrów powinien przechowywać przynajmniej następujące informacje:

- Miejsce wystąpienia zdarzenia,
- Rodzaj zdarzenia jakie wystąpiło,
- Dokładną datę i czas wystąpienia zdarzenia.

Rejestry zdarzeń tworzone są w oparciu o zdarzenia jakie miały miejsce w następujących elementach Architektury PKI:

- Centrum Certyfikacji (na warstwie sprzętowej, sieciowej i aplikacyjnej systemu),
- Centrum Certyfikacji (szczególnie zdarzenia związane z wystawieniem, zawieszeniem, unieważnieniem i odwieszeniem certyfikatu Subskrybenta),
- Zdarzenia wynikające z eksploatacji zabezpieczeń fizycznych i logicznych Centrum Certyfikacji).

5.4.2 Częstotliwość przeglądu rejestrów zdarzeń

Rejestry zdarzeń powinny być przeglądane nie rzadziej niż raz dziennie przez Administratora systemu.

5.4.3 Czas przechowywania archiwalnych kopii rejestrów zdarzeń

Archiwalne kopie rejestrów zdarzeń powinny być przechowywane przynajmniej przez okres 5 lat.

5.4.4 Ochrona zapisów rejestrowanych zdarzeń

Rejestry zdarzeń przechowywane są w środowisku zapewniającym odpowiedni poziom bezpieczeństwa. Zapewnia się integralność plików w rejestrach zdarzeń.

5.4.5 Procedury tworzenia kopii zapasowych

Kopie zapasowe tworzy się z wykorzystaniem technik zapewniających integralność danych.

5.4.6 Oszacowanie podatności na zagrożenia

Dokonuje się okresowej oceny poziomu ryzyka systemu, w celu identyfikacji zagrożeń, oszacowania prawdopodobieństwa ich wystąpienia oraz podatności na nie. Na podstawie wyników analizy ryzyka wprowadzone zostają rozwiązania mające na celu eliminację lub zmniejszenie podatności systemu na zagrożenia.

5.5 Archiwizacja danych

5.5.1 Rodzaje zasobów podlegających tworzeniu kopii zapasowych

Tworzenie kopii zapasowych ma na celu zapewnienie ciągłości działania Centrum Certyfikacji. Tworzeniu kopii zapasowych podlegają wszystkie istotne elementy infrastruktury informatycznej systemu Centrum Certyfikacji. W szczególności są to następujące elementy:

- Serwery Centrum Certyfikacji, w tym bazy danych przechowujące informacje o Użytkownikach i wystawionych certyfikatach.
- Serwery Repozytorium.

5.5.2 Częstotliwość tworzenia kopii zapasowych

Kopie zapasowe zasobów, o których mowa w rozdziale 5.5.1 tworzone są raz na tydzień.

5.5.3 Czas przechowywania kopii zapasowych

Tygodniowe kopie zapasowe przechowywane są przez okres jednego miesiąca. Wyjątkiem są kopie tworzone w ostatnim tygodniu miesiąca i roku kalendarzowego, które przechowywane są przez okres 5 lat.

5.5.4 Przechowywanie i dostęp do kopii zapasowych

Wszystkie nośniki danych przechowywane są w pomieszczeniach chroniących je przed wpływem czynników środowiskowych takich jak temperatura, wilgotność i pole magnetyczne.

5.5.5 Techniczna realizacja tworzenia kopii zapasowych

Kopie zapasowe tworzone są z użyciem narzędzi informatyczno-sprzętowych i podlegają zapisowi na magnetycznych nośnikach danych. Trwałość zapisu na wspomnianych nośnikach wynosi 5 lat. Tworząc kopie zapasowe, archiwizacji podlega cała zawartość dysków twardych serwerów Centrum Certyfikacji.

5.6 Wymiana kluczy urzędu

Niniejsza polityka nie opisuje przedmiotowego zakresu.

5.7 Naruszenie bezpieczeństwa kluczy urzędu i procedury odtwarzania po awarii (Compromise and Disaster Recovery)

5.7.1 Procedura postępowania po wystąpienie incydentu

W przypadku wykrycia incydentu naruszającego bezpieczeństwo Centrum Certyfikacji, podejmowane są działania mające na celu ich zidentyfikowanie i wyeliminowanie. Środkami zapobiegawczymi podejmowanymi w celu uniknięcia zaistnienia incydentu w Centrum Certyfikacji są odpowiednio wdrożone procedury awaryjne reagowania na zagrożenie. Procedury są uruchamiane w momencie zaistnienia zagrożenia. Dodatkowo zbierane są informacje na temat zasobów Centrum Certyfikacji, które uległy incydentowi, oraz przypadek poddawany jest analizie w celu przeciwdziałania jego wystąpieniu w przyszłości.

5.7.2 Postepowanie po uszkodzeniu zasobów sprzętowych, programowych i danych

W przypadku wystąpienia awarii zasobów Centrum Certyfikacji, zespół bezpieczeństwa w skład którego wchodzą Inspektor Bezpieczeństwa Systemu, Administrator Systemu oraz Operator Systemu zobowiązany jest do określenia i oszacowania zasobów, które uległy uszkodzeniu. Zasoby te obejmują sprzęt, oprogramowanie, środowisko sieciowe oraz środowisko fizyczne, w którym funkcjonuje Centrum Certyfikacji. Wystąpienie awarii zasobów uruchamia procedurę awaryjną pozwalającą na reagowanie na uszkodzenie odpowiednich zasobów. Działania podejmowane w tym zakresie zmierzają do jak najszybszego odtworzenia działalności Centrum Certyfikacji

5.7.3 Postępowanie po naruszeniu ochrony klucza prywatnego Centrum Certyfikacji

W przypadku wystąpienia incydentu naruszającego bezpieczeństwo klucza prywatnego Centrum Certyfikacji, personel Centrum Certyfikacji zobowiązany jest do podjęcia działań zmierzających w kierunku powiadomienia o zaistniałym incydencie kierownictwo Centrum Certyfikacji Wydawnictwa Kwantum oraz Użytkowników PP NOTA i Strony ufające. Następnie unieważnianie są wszystkie certyfikaty Subskrybentów (Użytkowników PP Nota) i Zaświadczenie certyfikacyjne Centrum Certyfikacji. W dalszej kolejności określane jest źródło, które spowodowało zagrożenie i podejmowane są działania zmierzające do zniwelowania zagrożeń wypływających z tegoż źródła. Po ich usunięciu następuje wygenerowanie nowej pary kluczy Centrum Certyfikacji. Subskrybenci zmuszeni są do wnioskowania o nowy certyfikat w PP NOTA

6 Zabezpieczenia techniczne

6.1 Generowanie pary kluczy i instalacja

6.1.1 Generowanie i instalacja par kluczy

Pary kluczy przekazywane Użytkownikom PP NOTA generowane są automatycznie przez serwer kluczy PP NOTA. Jako serwer kluczy wykorzystywana jest aplikacja CFSSL Cloud Flar's. Serwer kluczy PP NOTA zlokalizowany jest w chmurze obliczeniowej „Microsoft Azure". Po wygenerowaniu pary kluczy następuje instalacja pary kluczy oraz certyfikatu PP NOTA. Instalacja jest inicjowana przez Użytkownika PP NOTA. Instalowana para kluczy oraz certyfikat PP NOTA zostaną zapisane w magazynie certyfikatów prowadzonym przez system operacyjny.

6.1.2 Parametry kluczy

Urząd certyfikacji NOTA używa następujących kluczy:

Root CA:

- Klucze algorytmu ECDSA
- Typ: `secp521r1`
- Długość klucza: 521
- Algorytm podpisu: `ecdsa-with-SHA512`

SubCA:

- Klucze algorytmu ECDSA
- Typ: `secp521r1`
- Długość klucza: 521
- Algorytm podpisu: `ecdsa-with-SHA512`

Usługa OCSP używa następujących kluczy dla poszczególnych responderów:

Responder dla Root CA:

- Klucze algorytmu ECDSA
- Typ: prime256v1
- Długość klucza: 256
- Algorytm podpisu: ecdsa-with-SHA256

Responder dla certyfikatów do zaawansowanego podpisu elektronicznego:

- Klucze algorytmu ECDSA
- Typ: prime256v1
- Długość klucza: 256
- Algorytm podpisu: ecdsa-with-SHA256

6.1.3 Parametry generowania klucz publicznego

Klucze publiczne urzędów CA oraz Użytkowników końcowych generowane są za pomocą programowych modułów kryptograficznych, które zapewniają odpowiednią jakość otrzymanych kluczy.

6.1.4 Zastosowanie kluczy

Sposób użycia klucza zdefiniowany jest w polu KeyUsage oraz ExtendedKeyUsage rozszerzeń standardowych certyfikatu (X.509 v3). Pole jest weryfikowane przez PP NOTA i powinno być weryfikowane przez inne aplikacje korzystające z certyfikatu.

Klucze urzędu są używane wyłącznie do podpisywania certyfikatów Subskrybentów PP NOTA.

Klucze OCSP są używane wyłącznie do podpisywania odpowiedzi OCSP.

6.2 Ochrona, aktywacja, dezaktywacja i niszczenie kluczy

Klucze prywatne certyfikatów do zaawansowanego podpisu elektronicznego generowane są na serwerze certyfikacji PP NOTA w środowisku bezpiecznym, przy użyciu komponentu CFSSL. Certyfikaty przekazywane są użytkownikowi w formacie PFX zabezpieczonym losowym hasłem.

6.2.1 Deponowanie klucza prywatnego

PP NOTA nie przechowuje kluczy prywatnych Subskrybentów.

6.2.2 Kopia zapasowa klucza prywatnego

Centrum certyfikacji tworzy kopie kluczy prywatnych Urzędu Certyfikacji na wypadek awaryjnej procedury odzyskiwania kluczy. Kopie zapasowe kluczy przechowywane są w postaci zaszyfrowanej kluczem symetrycznym, który przechowywany jest w bezpiecznej lokalizacji.

Centrum certyfikacji nie tworzy kopii zapasowych kluczy prywatnych Subskrybentów.

6.2.3 Archiwizacja klucza prywatnego

Nie dopuszcza się archiwizacji kluczy prywatnych wydanych Subskrybentom.

6.2.4 Sposób aktywacji klucza prywatnego

Aktywacja klucza prywatnego Subskrybenta wymaga pobrania certyfikatu wygenerowanego w procesie wnioskowania o certyfikat Użytkownika PP NOTA w formacie PFX zabezpieczonego jednorazowym losowym hasłem. Hasło oraz certyfikat dostarczane są Użytkownikowi w bezpiecznym środowisku.

6.2.5 Archiwizacja klucza publicznego

Wszystkie klucze publiczne są archiwizowane przez PP NOTA. Certyfikaty, których okres ważności wygasł, są archiwizowane przez okres, co najmniej 10 lat od daty powstania, włącznie z kluczem publicznym

6.2.6 Okresy funkcjonowania certyfikatów i okresy funkcjonowania par kluczy

Okresy ważności certyfikatów Centrum Certyfikacji oraz certyfikatów Subskrybentów, wynoszą nie więcej niż:

- 25 lat dla głównego urzędu certyfikacji
- 10 lat dla certyfikatów pośrednich urzędów certyfikacji
- 5 lat dla certyfikatów Subskrybentów

6.3 Zarządzanie bezpieczeństwem systemu informatycznego

Zgodnie z polityką bezpieczeństwa PP NOTA, przepisami prawa powszechnego oraz wewnętrznymi regulacjami. W systemie teleinformatycznym PP NOTA wykorzystuje się wiarygodne oprogramowanie i sprzęt wdrożony na podstawie istniejących procedur zapewniających bezpieczną eksploatację. Funkcje zabezpieczające systemy komputerowe są realizowane na poziomie systemu operacyjnego, aplikacji oraz zabezpieczeń fizycznych.

Komputery funkcjonujące w Centrum Certyfikacji wyposażone są w następujące funkcje zabezpieczające:

- obligatoryjnie uwierzytelnione rejestrowanie się na poziomie systemu operacyjnego i aplikacji
- kontrola dostępu zarówno w zakresie dostępu do pomieszczeń jak i poszczególnych elementów systemu login, hasło (np. imienne konta w systemie operacyjnym i aplikacjach),
- możliwość prowadzenia audytu zabezpieczeń,
- pracownik, który pełni zaufaną role jest zobowiązany do blokowania swojej stacji roboczej zawsze, jeśli pozostają one poza jego nadzorem,
- wymuszanie separacji obowiązków, wynikające z pełnionych zaufanych ról,
- wymuszanie wylogowania Użytkownika po okresie bezczynności,
- kryptograficzną ochronę sesji wymiany informacji oraz zabezpieczenia baz danych,
- wykonywanie kopii zapasowych i archiwalnych,

- monitorowanie i alarmowanie w przypadku nieautoryzowanego dostępu do systemu teleinformatycznego.
- mechanizm monitorowani i alarmowania w przypadku wystąpienia zdarzenia przekroczenia parametrów wydajności systemów i dostępności usług.

7 Profil certyfikatu i list CRL

Profile certyfikatów są zgodne z formatami opisanymi normą ITU-T X.509. Dodatkowo certyfikaty są zgodne z profilami certyfikatów zdefiniowanych w normie ETSI-EN 319 412-2.

7.1 Struktura certyfikatu

W ramach Polityki Certyfikacji PP NOTA certyfikaty zawierają następujące elektroniczne struktury danych:

1. Treść certyfikatu (tbsCertificate),
2. Informacja o algorytmie użytym do podpisania certyfikatu (signatureAlgorithm),
3. Poświadczenie certyfikatu, składane przez organ wydający certyfikat (signatureValue).

7.1.1 Treść certyfikatu

L.p.	Pole	Opis	Zawartość
1	Version	wersja formatu certyfikatu zgodna z X.509	V3
2	SerialNumber	numer seryjny certyfikatu, unikalny w ramach urzędu wydającego certyfikat	-
3	SignatureAlgorithm	informacja o algorytmie użytym do podpisania certyfikatu	1.2.840.10045.4.3.2 (SHA256 with ECDSA Encryption)
4	Issuer	identyfikator (nazwa DN) wydającego certyfikat	CN = NOTA, Wydawnictwo Kwantum OU = pocztaprawnicza.pl O = Nota, Wydawnictwo Kwantum Sp. z o.o. L = Sopot C = PL
5	Validity	data ważności certyfikatu, określona jako data i czas początku okresu ważności certyfikatu (notBefore) oraz data i czas końca okresu ważności certyfikatu (notAfter)	
6	Subject	identyfikator (nazwa DN) posiadacza certyfikatu	C - pole obowiązkowe: wartość na podstawie danych dotyczących osoby - „Obywatelstwo” CN - pole obowiązkowe: Jest to połączenie pól

			„Imię/Imiona” +„ ” + „Nazwisko”; SURNAME - pole obowiązkowe: wartość na podstawie danych dotyczących osoby - „Nazwisko” z rozdziału 3.1.2 Zawartość warstwy graficznej; GIVENNAME – pole obowiązkowe: wartość na podstawie danych dotyczących osoby - „Imię pierwsze”; SN – pole obowiązkowe: numer legitymacji radcowskiej lub adwokackiej, będzie zawierać wartość na podstawie danych dotyczących posiadanej legitymacji - „numer uprawnień”. Składnia pola bazuje na Normie Europejskiej „ETSI EN 319 412-1 V1.1.1 Certificate Profiles Part 1: Overview and common data structures” Rozdział „5.1.3 Natural person semantics identifier”. Pprzykładowa składnia to: AWDPL-WAW/Adw/500 Oznacza ona adwokata z warszawskiej Okręgowej Izby Adwokackiej wpisanego na listę na pozycji 500.
7	SubjectPublicKeyInfo	określenie algorytmu używanego przez posiadacza certyfikatu oraz jego klucz publiczny	-

7.2 Struktura odpowiedzi OCSP

W ramach PP NOTA udostępniona jest usługa weryfikacji statusu certyfikatu w trybie online (OCSP). Umożliwia ona uzyskanie informacji zarówno o statusie certyfikatu wydanego w ramach PP NOTA, jak też informacji o statusie certyfikatu każdego z urzędów wchodzących w

skład infrastruktury Urzędu EDO. Zawartość i format odpowiedzi OCSP zgodny jest z zapisami normy RFC 6960.
Odpowiedź na zapytanie o status certyfikatu podpisywana jest kluczem usługi OCSP podpisanym przez ten Urząd Certyfikacji.

Odpowiedź OCSP jest zbiorem pól, których znaczenie przedstawiono poniżej:

- Informacja o statusie certyfikatu (**tbsResponseData**)
- Informacja o algorytmie użytym do podpisania odpowiedzi (**signatureAlgorithm**)
- Poświadczenie elektroniczne, składane przez organ wydający odpowiedź (**signature**)

7.2.1 Opis poszczególnych struktur

L.p.	Pole	Opis	Zawartość
1.	Version	wersja formatu usługi zgodna z RFC6990	V1
2.	Responder	identyfikator urzędu certyfikacji dostawcy usług	---
3.	ProducedAt	Data/czas wygenerowania odpowiedzi	---
4.	Responses	lista aktualnych statusów certyfikatów, pojedynczy certyfikat opisany jest następującymi atrybutami: numer seryjny unieważnionego certyfikatu (certID), status certyfikatu (certStatus), data/czas, dla której zweryfikowano status (thisUpdate), data/czas następnej aktualizacji statusu	---
5.	ResponseExtensions	rozszerzona informacja o odpowiedzi OCSP	---

8 Inne postanowienia

Rozdział ten przedstawia odpowiedzialność i zobowiązania Kwantum, Subskrybentów oraz Użytkowników certyfikatów (stron ufających).

8.1 Opłaty

Za wszystkie usługi doręczeń świadczone przez Kwantum pobierane są opłaty. Wysokość oraz rodzaje opłat opublikowane są na stronie pod adresem www.pocztaprawnicza.pl

8.2 Odpowiedzialność finansowa

Nie dotyczy.

8.3 Poufność informacji

Wszystkie dane, których nieuprawnione ujawnienie mogłoby narazić na szkodę Kwantum lub Subskrybenta usług zaufania traktowane są jako poufne i podlegają ochronie. Informacje

poufne opisane w niniejszym dokumencie nie są tym samym, co informacje poufne w znaczeniu Ustawy o Ochronie Informacji Niejawnych. Słowo „poufne" należy rozumieć jako „dyskrecja, udostępnianie czegoś tylko wybranym, niewielu osobom".

Subskrybenci są zobowiązani do ochrony poufności posiadanych kluczy kryptograficznych oraz innych danych z tym związanych (jak kody PIN).

Certyfikaty, zaświadczenia certyfikacyjne i listy CRL są traktowane jako informacje jawne, o ograniczonym dostępie. Dostęp do aktualnych certyfikatów, zaświadczeń certyfikacyjnych oraz list CRL ma personel obsługujący.

8.4 Ochrona danych osobowych

W ramach PP Nota ustanowiona jest polityka ochrony danych osobowych oraz wprowadzone mechanizmy ochrony danych osobowych zgodne z obowiązującymi przepisami.

8.5 Zabezpieczenie własności intelektualnej

Niniejsza polityka certyfikacji stanowi własność intelektualną Kwantum.

Certyfikaty wystawione przez CC Kwantum są jego własnością. Subskrybenci mają prawo do wykorzystywania certyfikatów w PP Nota, zgodnie z zasadami opisanymi w niniejszej polityce certyfikacji.

8.6 Udzielane gwarancje

Nie występują.

8.7 Zwolnienia z domyślnie udzielanych gwarancji

Wydawnictwo Kwantum Sp. z o.o. nie odpowiada wobec odbiorców usług certyfikacyjnych za:

a) szkody wynikające za użycia certyfikatu klucza publicznego poza zakresem określonym w Polityce,
b) szkodę wynikłą z powodu nieprawdziwych danych zawartych w certyfikacie klucza publicznego danych Zamawiającego.

8.8 Ograniczenia odpowiedzialności

Wydawnictwo Kwantum Sp. z o.o. nie odpowiada za jakiekolwiek szkody, które powstały lub mogły powstać u odbiorców usług certyfikacyjnych, wynikające z przyczyn innych niż niewykonanie lub nienależyte wykonanie obowiązków przez Kwantum.

W szczególności Wydawnictwo Kwantum Sp. z o.o. nie odpowiada za:

a) skutki nieprawidłowego użycia klucza prywatnego Subskrybenta,
b) skutki użycia klucza prywatnego Subskrybenta przez nieuprawnioną osobę,
c) skutki utraty bezpieczeństwa stosowanych przez Kwantum algorytmów kryptograficznych, chyba że użycie tych algorytmów nie jest zgodne z aktualnymi aktami wykonawczymi do Ustawy,

d) skutki nieprawidłowej, niezgodnej z Polityką, weryfikacji certyfikatów kluczy publicznych wystawionych przez Kwantum, w tym skutki wynikające ze stosowania przez Stronę ufającą uproszczonej procedury weryfikacji certyfikatów kluczy publicznych opisanej w Polityce.

8.9 Przenoszenie roszczeń odszkodowawczych

Nie występuje.

8.10 Przepisy przejściowe i okres obowiązywania polityki certyfikacji

Przepisy przejściowe nie występują.

Niniejsza polityka certyfikacji obowiązuje w stosunku do certyfikatów wystawionych zgodnie z nią do utraty ważności tych certyfikatów (z powodu zakończenia okresu ważności lub unieważnienia). Certyfikaty wykorzystywane w celach dochodzeniowych lub dowodowych po okresie ich ważności powinny być wykorzystywane zgodnie z polityką certyfikacji w ramach której zostały wystawione.

W stosunku do nowo wystawianych certyfikatów stosuje się najnowszą obowiązującą politykę certyfikacji zatwierdzoną przez Zarząd Kwantum.

8.11 Określanie trybu i adresów doręczania pism

Pisma związane ze sprawami niniejszej polityki certyfikacji i wystawianych w jej ramach certyfikatów mają być doręczane na adres skrzynki do doręczeń Wydawnictwa Kwantum znajdującej się w PP Nota.

8.12 Zmiany w polityce certyfikacji

Kwantum zastrzega sobie możliwość wprowadzania zmian w każdym czasie. Zmiany mogą wynikać w szczególności:

- ze zmian przepisów powszechnie obowiązującego prawa – zarówno europejskiego i polskiego,
- ze zmian wynikających ze sposobu świadczenia przez Kwantum usług, o których mowa w niniejszym dokumencie.

Zasady zarządzania polityką certyfikacji zostały opisane w rozdziale 1.7.

8.13 Rozstrzyganie sporów

W przypadku powstania sporu pomiędzy Kwantum a Subskrybentem strony podejmą próbę rozstrzygnięcia sporu w drodze polubownego porozumienia. W przypadku braku porozumienia rozstrzygnięcie sporu zostanie poddane sądowi powszechnemu właściwemu dla siedziby Wydawnictwa Kwantum Sp. z o.o..

8.14 Obowiązujące prawo

Umowa, jej wykonanie oraz wszelkie wynikające z niej stosunki prawne, podlegają prawu obowiązującemu na terenie Rzeczpospolitej Polski.

8.15 Podstawy prawne

Zasady działania Kwantum oraz PP Nota są zgodne z obowiązującym prawem, a w szczególności z przepisami zawartymi w następujących aktach prawnych:

- Ustawie z dnia 5 września 2016 r. o usługach zaufania oraz identyfikacji elektronicznej,
- Rozporządzenie Parlamentu Europejskiego i Rady (UE) Nr 910/2014 z dnia 23 lipca 2014 r. w sprawie identyfikacji elektronicznej i usług zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznym oraz uchylające dyrektywę 1999/93/WE
- Ustawie z dnia 4 lutego 1994 r. o prawie autorskim i prawach pokrewnych,
- Ustawie z dnia 29 sierpnia 1997 r. o ochronie danych osobowych.

8.16 Inne postanowienia

Nie występują.