Polityka i Kodeks Kwalifikowanej Usługi Certum – rejestrowanego doręczenia elektronicznego eDoręczenia

Wersja 1.1

Ważny od: 26 luty 2024 r.

Asseco Data Systems S.A.
ul. Jana z Kolna 11
80-864 Gdańsk
www.assecods.pl

Certum
ul. Bajeczna 13
71-838 Szczecin
www.certum.pl
www.certum.eu

Klauzula: Prawa Autorskie

Spis treści

1. Wstęp

„Polityka i Kodeks Kwalifikowanej Usługi Certum – rejestrowanego doręczenia elektronicznego eDoręczenia" dalej zwana Polityką eDoręczenia jest dokumentem bazującym i uzupełniającym „Politykę Certyfikacji i Kodeks Postępowania Certyfikacyjnego Kwalifikowanych Usług Certum" zwaną dalej **Polityką Główną,** która określa ogólne zasady stosowane przez Certum w trakcie świadczenia kwalifikowanych usług zaufania. Niniejszy dokument pełni także rolę Polityki dla usługi zaufania eDoręczenia, obejmujący rejestrację usługobiorców oraz proces identyfikacji podmiotów korzystających z usługi.

Powyższa usługa jest świadczona zgodnie z:

- wdrożonym przez Asseco Data Systems S.A. Zintegrowanym Systemem Zarządzania, który obejmuje zwłaszcza wymagania standardów PN-EN ISO 9001oraz PN-ISO/IEC 27001,
- *Ustawą o usługach zaufania oraz identyfikacji elektronicznej z dnia 5 września 2016 r. (Dz.U. z 2021 r. poz. 1797, z późn. zm.) z późniejszymi zmianami*,
- *Ustawą o doręczeniach elektronicznych z dnia 18 listopada 2020 r.*,
- *Rozporządzeniem w sprawie sporządzania i doręczania dokumentów elektronicznych oraz udostępniania formularzy, wzorów i kopii dokumentów elektronicznych (Dz.U. 2011 nr 206 poz. 1216) z późniejszymi zmianami;*
- *Rozporządzeniem 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, zwanym dalej w treści niniejszego dokumentu Rozporządzeniem eIDAS;*
- *Standardem usługi RDE - Standard publicznej usługi rejestrowanego doręczenia elektronicznego świadczonej przez operatora wyznaczonego i kwalifikowanych dostawców usług zaufania świadczących kwalifikowane usługi rejestrowanego doręczenia elektronicznego w zakresie współpracy z publiczną usługą rejestrowanego doręczenia elektronicznego oraz skrzynki doręczeń*.

Niniejsza Polityka eDoręczenia oraz Polityka Główna definiuje także uczestników procesu, ich obowiązki i odpowiedzialność, procedury weryfikacji tożsamości oraz obszary zastosowań. Znajomość natury, celu oraz roli Polityk jest szczególnie istotna z punktu widzenia usługobiorcy.

Struktura i merytoryczna zawartość Polityki eDoręczenia są zgodne z zaleceniem RFC 3647 *Certificate Policy and Certification Practice Statement Framework*. Spełnia on również wymagania norm:

- *ETSI EN 319 401 Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers;*
- ETSI EN 319 521- *Electronic Signatures and Infrastructures (ESI); Policy and security for Electronic Registered Delivery Service Providers.*

Obowiązujące pojęcia, terminy i ich znaczenie są określone w **Słowniku pojęć** na końcu tego dokumentu.

1.1. Wprowadzenie

Polityka eDoręczenia opisuje zakres działania Certum (działającego w ramach Asseco Data Systems S.A.) oraz związanych z nim **punktów rejestracji, usługobiorców**. Określa także ogólne zasady świadczenia kwalifikowanej usługi zaufania eDoręczenia, zgodnej z *Ustawą o usługach zaufania oraz identyfikacji elektronicznej z dnia 5 września 2016 r. Dz.U. z 2021 r. poz. 1797, z późn. zm.),* dalej w tekście zwanej *Ustawą*, tj. **standard usługi rejestrowanego doręczenia elektronicznego** obejmującego rejestrację usługobiorców, wymagania techniczne przekazywania dokumentów

elektronicznych, sposób identyfikacji nadawcy i adresata, strukturę oraz formę i sposób wystawiania dowodów wysłania i otrzymania oraz utrwalania, zakres i strukturę danych dotyczących komunikacji pomiędzy adresami do doręczeń elektronicznych, wymagania funkcjonowania skrzynki doręczeń.

Certum świadczące kwalifikowaną usługę eDoręczenia świadczy usługę w oparciu o certyfikat dostawców usług zaufania, wystawiony przez ministra właściwego ds. informatyzacji lub upoważniony przez niego dostawca usług zaufania w trybie art. 10 ust. 1 *Ustawy o usługach zaufania oraz identyfikacji elektronicznej.* Dostawcą usług zaufania jest **Narodowe Centrum Certyfikacji** będące systemem informatycznym **Narodowego Banku Polskiego**.

Niniejszy dokument reguluje działalność usługi eDoręczenia i związanych z nim punktów rejestracji, a także usługobiorców tej usługi, korzystających z usługi lub wymieniających jakiekolwiek wiadomości usłudze.

Zakres związany pozostałymi usługami zaufania świadczonymi przez Certum zaadresowany został w Polityce Głównej.

Certum działa zgodnie z prawem obowiązującym na terytorium Rzeczypospolitej Polskiej oraz zasadami wynikającymi z przestrzegania, konstrukcji, interpretacji oraz ważności Polityki eDoręczenia.

Z Polityką eDoręczenia związany jest Regulamin Kwalifikowanej Usługi Zaufania Certum – rejestrowanego doręczenia elektronicznego eDoręczenia oraz inne dodatkowe dokumenty, które Certum jest obowiązane stosować w swoim działaniu. Dokumenty te wymienione zostały w Polityce Głównej.

Certum jest odpowiedzialne za przestrzeganie zgodności z procedurami opisanymi w niniejszym dokumencie.

Dodatkowe informacje oraz pomoc serwisową można uzyskać za pośrednictwem poczty elektronicznej: infolinia@certum.pl.

Zakres pozostałych usług związany z przedmiotowym punktem zaadresowany został w Polityce Głównej.

1.2. Nazwa dokumentu i jego identyfikacja

Niniejszemu dokumentowi przypisuje się nazwę własną o następującej postaci: **Polityka i Kodeks Kwalifikowanej Usługi Certum kwalifikowanego rejestrowanego doręczenia elektronicznego eDoręczenia** i jest on dostępny w postaci elektronicznej w serwisie internetowym urzędu certyfikacji dostępnym pod adresem www.certum.pl.

Z ww. dokumentem związane są następujące zarejestrowane identyfikatory obiektu:

(OID: 1.2.616.1.113527.2.4.1.0.4.1.1)[1]:

> **id-cck-kpc-v1 OBJECT IDENTIFIER ::= { iso(1) member-body(2) pl(616) organization(1) id-unizeto(113527) id-ccert(2) id-cck(4) id-cck-certum-certPolicy(1) id-certPolicy-doc(0) id-ccert-kpc(pc)(4) version(1) 1}**

w którym dwie ostatnie wartości liczbowe odnoszą się do aktualnej wersji i podwersji tego dokumentu.

[1] Identyfikatora dokumentu Polityka i Kodeksu eDoręczenia .

1.3. Strony Polityki eDoręczenia

Niniejszy dokument oraz Polityka Główna reguluje wszystkie najważniejsze relacje zachodzące pomiędzy podmiotami wchodzącymi w skład Certum, jego zespołami doradczymi (w tym audytorami) oraz klientami (użytkownikami dostarczanych usług). W szczególności regulacje te dotyczą:

- urzędów,
- Głównego Punktu Rejestracji (GPR),
- punktów rejestracji (PR),
- osób potwierdzających tożsamość,
- usługobiorców,
- stron ufających.

Certum świadczy usługi zaufania wszystkim osobom fizycznym, prawnym lub podmiotom nieposiadającym osobowości prawnej, akceptującym postanowienia niniejszego dokumentu oraz Polityki Głównej.

Certum w swoim działaniu zapewnia, że żaden z jego klientów ani stron ufających nie jest bezpośrednio lub pośrednio traktowany w sposób mniej korzystny niż inni, ani nie podlega ograniczeniom w korzystaniu ze swoich uprawnień, ze względu na wiek, kolor skóry, wyznanie, niepełnosprawność, pochodzenie etniczne lub narodowe, płeć, stan cywilny, stan zdrowia fizycznego, stan zdrowia psychicznego, narodowość, wygląd fizyczny ani polityczne przekonania.

Certum stosuje szczególne procedury obsługi osób niewidomych i niedowidzących ubiegających się o dostęp do usługi.

Certum świadczy kwalifikowaną usługę eDoręczenia w zakresie:

- rejestracji usługobiorców,
- identyfikacje nadawcy i adresata,
- „wskazanie użytkownika upoważnionego”,
- utworzenia adresu do doręczeń elektronicznych,
- aktywacji adresu do doręczeń elektronicznych,
- aktualizacji wpisu w rejestrze BAE,
- wniosek o wykreślenia adresu do doręczeń elektronicznych z rejestru BAE,
- przedłużenia ważności wpisu adresu do doręczeń elektronicznych w rejestrze BAE,
- odzyskania wykreślonego adresu do doręczeń elektronicznych,
- przeniesienia adresu do doręczeń elektronicznych do innego dostawcy,
- wysyłanie wiadomości i załączonych dokumentów/plików,
- zapewnienie dowodów związanych z przesyłanymi danymi.

1.3.1. Urzędy Usług Zaufania

Kwalifikowana usługa eDoręczenia świadczone przez urząd Certum QERDS 2023.

Pozostałe urzędy, usługi wchodzące w skład Certum świadczącego kwalifikowane usługi zaufania zdefiniowane zostały w Polityce Głównej.

1.3.1.1. Kwalifikowana usługa Certum eDoręczenia

Kwalifikowana usługa rejestrowanego doręczenia elektronicznego Certum eDoręczenia działa na podstawie wpisu Asseco Data Systems S.A. do rejestru kwalifikowanych dostawców usług zaufania. Nadzór nad usługą Certum eDoręczenia sprawuje minister właściwy ds. informatyzacji lub wskazany przez niego podmiot (narodowe centrum certyfikacji).

Kwalifikowana usługa rejestrowanego doręczenia elektronicznego Certum eDoręczenia zapewnienia możliwość wysyłania i odbierania korespondencji drogą elektroniczną, dowodów związanych z przesyłanymi danymi, w tym dowodu wysłania i otrzymania danych, ochrony przesyłanych danych przed ryzykiem utraty, kradzieży, uszkodzenia lub jakiejkolwiek nieupoważnionej zmiany. Poprzez wstępną identyfikację nadawcy i adresata zapewnia unikanie dostarczania wiadomości do nieuprawnionego użytkownika.

Kwalifikowana usługa eDoręczenia zapewnia znakowanie kwalifikowanym znacznikiem czasem oraz zabezpieczenie za pomocą kwalifikowanej pieczęci wysyłanej, odbieranej oraz wszelkich zmian korespondencji. Dowód zawiera informację, że w określonym momencie czasowym miało miejsce określone zdarzenie.

Usługa Certum eDoreczenia świadczy usługi dla:

- osób fizycznych, prawnym oraz podmiotom nie posiadającym osobowości prawnej.

1.3.2. Główny Punkt Rejestracji, Punkty Rejestracji oraz Punkty Potwierdzania Tożsamości

Z usługą eDoręczenia ściśle współpracują Główny Punkt Rejestracji, punkty rejestracji oraz punkty potwierdzania tożsamości. Punkty rejestracji oraz punkty potwierdzania tożsamości reprezentują eDoręczenia w kontaktach z usługobiorcą i działają w ramach oddelegowanych im uprawnień w zakresie rejestracji usługobiorcy oraz potwierdzania jego tożsamości.

Punkty rejestracji oraz punkty potwierdzania tożsamości przyjmują, weryfikują i następnie aprobują lub odrzucają – otrzymywane od wnioskodawców – wnioski o rejestrację usługi oraz inne wnioski związane z zarządzaniem usługą. Weryfikacja wniosków ma na celu uwierzytelnienie (na podstawie dokumentów dołączonych do wniosku) wnioskodawcy oraz danych, które zostały umieszczone we wniosku. Stopień dokładności potwierdzania tożsamości usługobiorcy oraz przypisywanych mu atrybutów wynika z ogólnych wymagań określonych w **Polityce eDoręczenia** (patrz rozdz. 3.2). Szczegółowy zakres obowiązków punktów rejestracji, punktów potwierdzania tożsamości oraz ich operatorów określany jest przez niniejszą Politykę eDoręczenia, Politykę Główną procedury funkcjonowania punkty rejestracji i punktów potwierdzania tożsamości oraz Regulamin Kwalifikowanej Usługi Zaufania Certum – rejestrowanego doręczenia elektronicznego eDoręczenia.

Pozostały zakres związany z przedmiotowym punktem zaadresowany został w Polityce Głównej.

1.3.3. Usługobiorca

Usługobiorcami Certum mogą być osoby fizyczne, prawne lub podmioty nieposiadające osobowości prawnej.

Organizacje pragnące uzyskać dla swoich pracowników dostęp do usługi, mogą to uczynić poprzez swoich upoważnionych przedstawicieli. Z kolei usługobiorca indywidualny występuje o dostęp do usługi, w swoim imieniu[2].

Usługobiorcy mogą korzystać z usługi eDoręczenia jako nadawcy i/lub adresaci.

[2] Niezależnie od tego czy usługobiorca występuje o dostęp do usługi indywidualnie czy też robi to w jego imieniu upoważniony przedstawiciel, to uzyskanie dostępu do usługi musi być poprzedzone akceptacją przez usługobiorcę warunków świadczenia usług eDoreczenia przez Asseco Data Systems S.A.

1.3.4. Strony ufające

Stroną ufającą, korzystającą z usługi jest dowolny podmiot, który podejmuje decyzję o jej ważności dowodowej.

W tym przypadku nie są to użytkownicy usługi eDoręczenia.

1.3.5. Inne Strony

Niezależnie jednostki oceniające zgodność z Rozporządzeniem eIDAS.

Organ nadzoru, tj. minister właściwy ds. informatyzacji lub wskazany przez niego podmiot (narodowe centrum certyfikacji).

1.4. Zakres stosowania usługi rejestrowanego doręczenia elektronicznego eDoręczenia

Usługa eDoręczenia służy do wysyłania i odbierania elektronicznych przesyłek.

Rejestrowane doręczenie elektroniczne stanowi elektroniczny dowód przesłania przez nadawcę dokumentu elektronicznego do adresata, zapewnia ochronę przesyłanych danych przed ryzykiem utraty, kradzieży, uszkodzenia lub jakiejkolwiek nieupoważnionej zmiany.

Pozostałe usługi wchodzące w skład Certum świadczącego kwalifikowane usługi zaufania zdefiniowane zostały w Polityce Głównej.

1.4.1. Certyfikat dostawcy usługi zaufania eDoręczenia

Certyfikat dostawcy usługi zaufania eDoręczenia wystawiane są tylko przez ministra właściwego ds. informatyzacji lub upoważnionego przez niego kwalifikowanego dostawcę usługi zaufania.

1.4.2. Nierekomendowane zastosowanie usługi eDoręczenia

Zabrania się używania usługi eDoręczenia z naruszeniem obowiązujących przepisów oraz niezgodnie z przeznaczeniem, określonym w niniejszym dokumencie.

1.5. Administracja Kodeksem Postępowania Certyfikacyjnego

Administrowanie niniejszą Polityką eDoręczenia odbywa się na zasadach opisanych w Polityce Głównej.

1.5.1. Organizacja odpowiedzialna za administrowanie dokumentem

Asseco Data Systems S.A.
ul. Jana z Kolna 11
80-864 Gdańsk
Polska
KRS: 0000421310 Sąd Rejonowy Gdańsk-Północ w Gdańsku

1.5.2. Kontakt

Asseco Data Systems S.A.
Certum
ul. Bajeczna 13
71-838 Szczecin
Polska
E-mail: infolinia@certum.pl
Numer telefonu: +48 91 4801 340

1.5.3. Podmioty określające aktualność zasad określonych w dokumencie

Ocena aktualności i przydatności niniejszej Polityki eDoręczenia odbywa się na zasadach opisanych w Polityce Głównej.

1.5.4. Procedura zatwierdzania Polityki i Kodeksu Kwalifikowanej Usługi Certum

Ocena aktualności i przydatności niniejszej Polityki eDoręczenia odbywa się na zasadach opisanych w Polityce Głównej.

1.6. Definicje i używane skróty

Zakres związany z przedmiotowym punktem zaadresowany został w Polityce Głównej, a specyficzne definicje dla Polityki eDoręczenia znajdują się na końcu niniejszego dokumentu.

2. Odpowiedzialność za publikację i repozytorium

2.1. Repozytorium

Zakres związany z przedmiotowym punktem zaadresowany został w Polityce Głównej

2.2. Informacje publikowane w repozytorium

Zakres związany z przedmiotowym punktem zaadresowany został w Polityce Głównej

Na stronie internetowej www.certum.pl w repozytorium dostępny jest również nieprzeterminowany i nieunieważniony certyfikat dostawców usług zaufania kwalifikowanej usługi Certum eDoręczenia.

2.3. Częstotliwość publikacji

Częstotliwość publikacji niniejszej Polityki eDoręczenia odbywa się na tych samych zasadach jak częstotliwość publikacji Polityki Głównej które zostały opisane w Polityce Głównej w rodz. 2.3.

2.4. Kontrola dostępu do repozytorium

Zakres związany z przedmiotowym punktem zaadresowany został w Polityce Głównej.

3. Adresu do doręczeń elektronicznych, identyfikacja i uwierzytelnienie usługobiorcy

Poniżej przedstawiono ogólne zasady weryfikacji tożsamości usługobiorców, które mogą być stosowane przez Certum. Weryfikacja przeprowadzana jest **obligatoryjnie** podczas rejestracji.

Certum oraz podległe mu podmioty potwierdzają tożsamość i wszelkie specjalne atrybuty osoby fizycznej lub osoby prawnej ubiegającej się o dostęp do usługi na podstawie ważnego dowodu osobistego, mDowodu[3], paszportu, polskiej kartu pobytu, polskiego lub stosując inną metodę z zastrzeżeniem art. 44 *Rozporządzenia eIDAS*.

3.1. Adres do doręczeń elektronicznych

3.1.1. Struktura adresu do doręczeń elektronicznych

Adres do doręczeń elektronicznych jest tworzony jako ciąg znaków zapewniających jego unikalność.

[3] Cyfrowy dokument tożsamości dostępny w aplikacji mobilnej mObywatel wydanej przez Kancelarię Prezesa Rady Ministrów .

Adres do doręczeń elektronicznych nie zawiera wprost, ani pośrednio, informacji dotyczących nazwy, ani innego identyfikatora podmiotu, którego dotyczy.

Adresu do doręczeń elektronicznych posiada strukturę zgodną z wymaganiami określonymi w normie [ETSI319412-1] w rozdziale 5.1 odpowiednio:

- Dla osób fizycznych w postaci identyfikatora semantycznego id-etsi-qcs-SemanticsId-Natural;
- Dla podmiotów publicznych oraz niepublicznych w postaci identyfikatora semantycznego id-etsi-qcs-SemanticsId-Legal.

Adres do doręczeń elektronicznych zawiera następującą strukturę:

- 3 znaki oznaczające rodzaj identyfikatora – oznaczające adres elektroniczny – "AE: ";
- 2 znaki kodu kraju zgodnie ze standardem ISO 3166 – oznaczające Polskę – "PL";
- myślnik "-" – kodowany (0x2D (ASCII), U+002D (UTF-8));
- co najmniej 20 znaków właściwego adresu elektronicznego składającego się z następujących grup znaków:
    - 5 znaków cyfr (0-9),
    - myślnik "-" – kodowany (0x2D (ASCII), U+002D (UTF-8)),
    - 5 znaków cyfr (0-9),
    - myślnik "-" – kodowany (0x2D (ASCII), U+002D (UTF-8)),
    - 5 znaków literowych (A-Z – tylko wielkie litery),
    - myślnik "-" – kodowany (0x2D (ASCII), U+002D (UTF-8)),
    - 2 znaki cyfr (0-9).

Ostatnie 2 znaki oznaczają sumę kontrolną.

Przykładowy adres zgodny z powyższą strukturą: "AE:PL-12345-67890-ABCDE-12".

3.1.2. Dane identyfikujące usługobiorcę

Usługa eDoręczenia zapewnia powiązanie danych osobowych i identyfikacyjnych nadawców i adresatów, aktualne i historyczne, z obsługiwanym w ramach danej usługi adresem do doręczeń elektronicznych.

- Zestaw danych zgodnie z normą *ETSI EN 319 522-2* w przypadku osób fizycznych:
    - imię, nazwisko,
    - miejsce urodzenia,
    - data urodzenia,
    - PESEL
- Zestaw danych zgodnie z normą *ETSI EN 319 522-2* w przypadku podmiotów nie będących osobami fizycznymi:
    - nazwa podmiotu a w przypadku komornika sądowego jego imię i nazwisko oraz tytuł,
    - siedziba i adres,
    - adres do korespondencji,
    - numer identyfikacyjny (REGON, NIP, KRS).

3.1.3. Anonimowość usługi

Wymagane jest aby adresy do doręczeń elektronicznych pozwalał na jednoznaczne wskazanie konkretnego adresata przesyłki.

3.1.4. Rola znaków towarowych

Zakres związany z przedmiotowym punktem zaadresowany został w Polityce Głównej.

3.2. Rejestracja początkowa, wstępna weryfikacja tożsamości

Rejestracja usługobiorcy ma miejsce zawsze wtedy, gdy składany jest wniosek o dostęp do usługi eDoręczenia oraz inne wnioski związane z zarządzaniem usługą.

Rejestracja obejmuje szereg wewnętrznych procedur, które jeszcze przed wydaniem dostępu do usługi eDoręczenia usługobiorcy mają na celu zgromadzenie przez punkt systemu rejestracji uwiarygodnionych danych o podmiocie, identyfikujących jego tożsamość oraz uprawnienia. Potwierdzenie tych danych realizowane jest zgodnie z standardem usługi RDE pkt. 5.1.17.1.

Usługobiorca składa wniosek (oświadczenie), które stanowi potwierdzenie prawdziwości jego danych i zgodę na przyporządkowanie do niego tych danych. Na podstawie tego wniosku Certum udziela dostępu do usługi przydzielając środek uwierzytelniający dla nadawcy lub adresata.

Usługobiorca jest zobowiązany potwierdzić zapoznanie się z „Regulamin Kwalifikowanej Usługi Zaufania eDoręczenia" poprzez zaakceptowanie warunków świadczenia usług zaufania.

Usługobiorca, jest zobowiązany udzielić w formularzu rejestracyjnym informacji pozwalających na jego identyfikację.

Wniosek o utworzenie adresu do doręczeń elektronicznych zgodnie z *Ustawą o doręczeniach elektronicznych* oraz normą *ETSI EN 319 522-2*, zawiera zestaw danych w przypadku osób fizycznych

- imię, nazwisko,
- firmę – w przypadku osoby fizycznej będącej przedsiębiorcą wpisanym do Centralnej Ewidencji i Informacji o Działalności Gospodarczej albo tytuł zawodowy – w przypadku osoby fizycznej będącej adwokatem, radcą prawnym, doradcą podatkowym, doradcą restrukturyzacyjnym, notariuszem, rzecznikiem patentowym lub radcą Prokuratorii Generalnej Rzeczypospolitej Polskiej,
- miejsce urodzenia,
- data urodzenia,
- PESEL
- numer identyfikacyjny (REGON, NIP) - jeżeli został nadany,
- adres do korespondencji – w przypadku osoby fizycznej niebędącej przedsiębiorcą wpisanym do Centralnej Ewidencji i Informacji o Działalności Gospodarczej,
- adres do doręczeń – w przypadku osoby fizycznej będącej przedsiębiorcą wpisanym do Centralnej Ewidencji i Informacji o Działalności Gospodarczej
- adres poczty elektronicznej, na który zostanie przesłana informacja o utworzeniu adresu do doręczeń elektronicznych oraz o sposobie aktywacji skrzynki doręczeń,
- w przypadku wyznaczenia administratora skrzynki doręczeń - imię i nazwisko administratora skrzynki doręczeń, jego adres poczty elektronicznej oraz numer PESEL.

Wniosek o utworzenie adresu do doręczeń elektronicznych zgodnie z *Ustawą o doręczeniach elektronicznych* oraz normą *ETSI EN 319 522-2* w przypadku podmiotów nie będących osobami fizycznymi:

- nazwa podmiotu a w przypadku komornika sądowego jego imię i nazwisko oraz tytuł,
- siedziba i adres,
- adres do korespondencji,
- numer identyfikacyjny (REGON, NIP, KRS),
- imię i nazwisko administratora skrzynki doręczeń, jego adres poczty elektronicznej oraz numer PESEL.

Każdy usługobiorca poddaje się procesowi rejestracji. Po wypełnieniu elektronicznego wniosku, poprawnym zweryfikowaniu dostarczonych danych, po zaakceptowaniu warunków świadczenia usług zaufania otrzymuje dostęp do usługi eDoręczenia, otrzymuje przydzielony środek uwierzytelniający.

Każdy wnioskodawca, ubiegający się o dostęp do usług eDoręczenia musi wykonać następujące podstawowe czynności:

- wypełnić elektroniczny wniosek,
- określić rodzaj usługi:
  - dla podmiotu niepublicznego będącego osobą fizyczną;
  - dla podmiotu niepublicznego będących osobą prawną.

Szczegółowy zakres uprawnień do występowania o określony rodzaj usługi powinno definiować dokument potwierdzający posiadanie tytułu, pełnomocnictwo lub inny dokument upoważniający do występowania w cudzym imieniu.

Wnioskodawca w trakcie procesu rejestracji informowany jest na piśmie lub w formie dokumentu elektronicznego, w sposób jasny i powszechnie zrozumiały o:

- warunkach użytkowania usługi eDoręczenia,
- zobowiązaniach usługobiorcy,
- informacjach dla stron ufających,
- informacjach o sposobie archiwizacji danych,
- zakresie i ograniczeniach odpowiedzialności Asseco Data Systems S.A.,
- zakresie i ograniczeniach świadczenia usługi eDoręczenia,
- zgodności świadczonych usług z *Rozporządzeniem eIDAS*, *Ustawą o usługach zaufania oraz identyfikacji elektronicznej i Ustawą o doręczeniach elektronicznych.*
- sposobie rozpatrywania skarg i sporów,
- sposobie audytowania usługi eDoręczenia,
- informacjach kontaktowych do Certum,
- dostępności usług,
- o procedurze zgłaszania wniosku w wyrejestrowanie usługobiorcy eDoręczenia.

Powyższe kwestie zawarte są w Regulamin Kwalifikowanej Usługi Zaufania Certum – rejestrowanego doręczenia elektronicznego eDoręczenia dostępnym na stronie internetowej pod adresem www.certum.pl.

Usługobiorca jest zobowiązany potwierdzić zapoznanie się z powyższymi informacjami poprzez zaakceptowanie warunków świadczenia usługi eDoręczenia.

Certum gwarantuje wersję językową polską i angielską przedstawionych dokumentów, co pokrywa obszar zainteresowania językowego naszych klientów. Przedstawione dokumenty są do pobrania w postaci plików PDF poprzez repozytorium Certum.

Akceptacja warunków świadczenia usług zaufania oznacza także, że:

- Usługobiorca wyraża zgodę na przetwarzanie przez Asseco Data Systems S.A. jego danych osobowych dla potrzeb niezbędnych do realizacji usługi,
- usługobiorca oświadcza, że informacje podane przez niego są zgodne z prawdą i zostały podane dobrowolnie.

Składając wniosek przyszły usługobiorca jest także zobowiązany do przedstawienia:

- pełnomocnictw do składania wniosku w imieniu upoważniającego go podmiotu,
- innych dokumentów, które są niezbędne do potwierdzenia danych zawartych we wniosku, np. tytułu.

Przy wypełnianiu wniosku przyszły usługobiorca wyraża w formie oświadczenia zgodę na:

- przetwarzanie swoich danych osobowych przez Asseco Data Systems S.A. i punkt systemu rejestracji, dla potrzeb niezbędnych do realizacji procesu.

Jeżeli usługobiorca przedstawił pełnomocnictwo, to podmiot go udzielający jest równocześnie zobowiązany do podpisania zawartej w nich dodatkowej części stanowiącej drugą część zgody na świadczenie kwalifikowanych usług zaufania, zawierającej następujące elementy, zgodne z punktem 6.3.4 e) ETSI EN 319 411-1:

- zgodę na świadczenie kwalifikowanych usługi eDoręczenia ,
- oświadczenie o zapoznaniu się z warunkami świadczenia usług zawartymi w Regulaminie Kwalifikowanej Usługi Zaufania eDoręczenia,
- wyraził zgodę na przechowywanie danych podmiotu użytych w procesie rejestracji przez wymagany przepisami *Ustawy o usługach zaufania oraz identyfikacji elektronicznej* okres.

3.2.1. Weryfikacja tożsamości osoby prawnej - uwierzytelnienie pełnomocnictw i innych atrybutów

Weryfikacja pełnomocnictw odbywa się zawsze wtedy, gdy usługobiorca wnioskuje o dostęp do usługi w imieniu organizacji, którego dane znajdują się we wniosku.

Uwierzytelnienie pełnomocnictw bądź uprawnień jest częścią procesu przetwarzania przez punkt systemu rejestracji i urząd certyfikacji wniosku o dostęp do usługi eDoręczenia, reprezentującej interesy innej osoby prawnej.

Proces uwierzytelniania pełnomocnictw stosowany w Certum oprócz weryfikacji samych pełnomocnictw obejmuje także uwierzytelnienie osoby fizycznej, która otrzymała pełnomocnictwo bądź upoważnienie.

Proces potwierdzania pełnomocnictw polega na weryfikacji dostarczonego pełnomocnictwa na podstawie:

- przedłożonych dokumentów upoważniających (np. notarialnie potwierdzonego dokumentu udzielenia pełnomocnictwa przez osobę fizyczną),
- sprawdzeniu czy dokument taki został podpisany przez osobę upoważnioną do reprezentacji,

- na sprawdzeniu zgodności danych podmiotu prawnego umieszczonych we wniosku z dostarczonymi dokumentami.

3.2.2. Weryfikacja tożsamości osób fizycznych

Weryfikacja tożsamości osoby fizycznej musi spełniać dwa cele. Po pierwsze musi wykazać, że podane we wniosku dane odnoszą się do istniejącej osoby fizycznej i po drugie, że wnioskodawca jest rzeczywiście tą osobą fizyczną, która została wymieniona we wniosku.

W przypadku, gdy usługobiorca jest osobą fizyczną (pracownikiem organizacji lub jej reprezentantem), dla której wydawany jest dostęp do usługi eDoręczenia weryfikacja może być realizowana dodatkowo na podstawie:

- stosownego upoważnienia wystawionego przez daną organizację do reprezentowania jej interesów,
- aktualnego wypisu z Krajowego Rejestru Sądowego lub wypisu z Centralnej Ewidencji i Informacji o Działalności Gospodarczej.

W przypadku, gdy usługobiorca jest osobą fizyczną (Komornikiem, Adwokatem lub Radcą Prawnym), dla której wydawany jest dostęp do usługi eDoręczenia weryfikacja dodatkowo realizowana jest na podstawie:

- dokumentu potwierdzającego posiadanie tytułu.

Inspektorzy ds. rejestracji Głównego Punktu Rejestracji, operatorzy punktów systemu rejestracji, zobligowane są do zweryfikowania poprawności oraz prawdziwości wszystkich danych zawartych we wniosku i dotyczących tożsamości wnioskodawcy oraz jego pełnomocnictw (patrz rozdz. 4.1).

Procedura weryfikacji tożsamości osoby fizycznej przeprowadzana przez operatora punktu systemu rejestracji, inspektora ds. rejestracji Głównego Punktu Rejestracji polega na szczegółowej weryfikacji wniosku i dokumentów okazanych przez usługobiorcę.

Po pozytywnym zakończeniu procedury weryfikacji operator punktu systemu rejestracji lub inna osoba weryfikująca tożsamość (poza notariuszem) akceptuje w imieniu Asseco Data Systems S.A. warunki świadczenia usługi eDoręczenia, wniosek oraz dokumenty są w systemie informatycznym przekazywane do Certum.

3.2.2.1. Weryfikacja tożsamości przez upoważnionego przedstawiciela Certum

Potwierdzenie tożsamości usługobiorcy realizowane jest na podstawie ważnego dowodu osobistego, mDowodu, paszportu lub polskiej karty pobytu za pośrednictwem Punktu Rejestracji lub Punktu Potwierdzania Tożsamości. Potwierdzenie tożsamości usługobiorcy może odbyć się:

- poprzez osobiste stawiennictwo w Punkcie Rejestracji lub Punkcie Potwierdzania Tożsamości,
- poprzez wizytę upoważnionego przedstawiciela Certum w lokalizacji, w której przebywa w danym momencie usługobiorca.

3.2.2.2. Weryfikacja tożsamości na podstawie kwalifikowanego podpisu elektronicznego

Weryfikacja tożsamości może nastąpić zdalnie, przy użyciu ważnego certyfikatu kwalifikowanego wydanego przez dowolnego polskiego dostawcę kwalifikowanych usług zaufania. Potwierdzenie tożsamości następuje na podstawie wniosku opatrzonego kwalifikowanym podpisem tej osoby.

3.2.3. Nieweryfikowane informacje usługobiorcy

Certum weryfikuje wszystkie informacje zawarte we wniosku.

3.2.4. Weryfikacja uprawnień

W przypadku, gdy wniosek o dostęp do usługi składany jest w imieniu organizacji, to należy to interpretować jako uprawnienie osoby składającej do działania w imieniu organizacji. Oznacza to jednocześnie, że Certum weryfikuje, czy osoba fizyczna, która złożyła wniosek była w momencie weryfikacji wniosku pracownikiem organizacji lub jej współpracownikiem i ma prawo do działania w imieniu organizacji; zakres tych uprawnień oraz okres ich ważności może być regulowany przez oddzielne przepisy, dane osoby fizycznej i jej uprawnienia Certum sprawdza w oparciu o dostępne zapisy lub bazy.

W przypadku cofnięcia uprawnień przez organizację osobie fizycznej wnioskującej o dostęp do usługi eDoręczenia należy poinformować Certum o tym oraz złożyć nowy wniosek wraz z wymaganym upoważnieniem dal nowej osoby fizycznej.

3.3. Uwierzytelnienie

Uwierzytelnienie tożsamości lub pełnomocnictw usługobiorcy, którzy posiadają już dostęp do usługi eDoręczenia realizowane jest:

- poprzez przydzielony środek uwierzytelniający dla nadawcy lub adresata, identyfikacja przeprowadzana jest za każdym razem, gdy przesyłka zostanie nadana lub doręczona;
- przesyłka przekazywana jest dopiero po udanej identyfikacji adresata.

4. Wymagania funkcjonalne

Poniżej przedstawiono sposób realizacji usługi eDoręczenia. Każdy etap rozpoczyna się od złożenia przez usługobiorcę stosownego wniosku. Certum podejmuje decyzję, co do dalszej realizacji wniosku, realizując żądaną usługę lub odmawiając jej realizacji. Składane wnioski powinny zawierać informacje, które są niezbędne do prawidłowego zidentyfikowania usługobiorcy oraz danych zawartych w składanym wniosku.

Usługa pozwala na przesyłane przesyłek w formie elektronicznej pomiędzy poszczególnymi nadawcami i adresatami. Usługa ta zapewnia dowód integralności i czasu przesyłanych danych, w tym dowód ich wysłania i odbioru. Usługa zabezpiecza dane przed utratą, kradzieżą, naruszeniem ich integralności lub nieuprawnioną modyfikacją, spełnia wymagania wynikające z *Rozporządzenia eIDAS*.

Przy korzystaniu z usługi eDoręczenia przestrzegana jest zasada, że moc prawna dokumentu elektronicznego nie może być kwestionowana z tego powodu, że ma on formę elektroniczną, co ma zapewnić, że transakcja elektroniczna nie zostanie odrzucona wyłącznie z tego powodu, że dokument ma formę elektroniczną. W związku z tym zakłada się, że dokumenty elektroniczne przesyłane i otrzymywane za pośrednictwem usługi eDoręczenia są wyczerpujące, wysłane przez nadawcę i otrzymane przez adresata oraz że data i godzina wysłania i otrzymania są dokładne.

4.1. Składanie wniosków

4.1.1. Kto może składać wnioski o dostęp do usługi

Z wnioskami o dostęp do usługi eDoręczenia może występować każdy podmiot należący do jednej z poniższych kategorii:

- osoba fizyczna, która jest lub będzie usługobiorcą, posiadająca polski identyfikator (PESEL),

- uprawniony przedstawiciel osoby prawnej lub instytucji nieposiadającej osobowości prawnej.

Certum nie udostępnia usługi eDoręczenia osobom niepełnoletnim (poniżej 18 roku życia), nawet prowadzącym działalność gospodarczą.

Certum nie wydaje dostępu do usługi eDoręczenia podmiotom wykonującym działalność gospodarczą w państwach, z którym prawo Rzeczpospolitej Polskiej zabrania prowadzenia wymiany handlowej.

4.1.2. Proces składania wniosków i związane z tym obowiązki

Wniosek o dostęp do usługo eDoręczenia składany jest przez wnioskodawcę w Punkcie Rejestracji, Partnerskim Punkcie Potwierdzania Tożsamości osobiście.

4.2. Przetwarzanie wniosków

Po zweryfikowaniu tożsamości wnioskodawcy przez operatora punktu systemu rejestracji, (patrz rozdz. 3.2.2) i otrzymaniu przez Certum wymaganych dokumentów, wniosek przekazywany jest do Głównego Punktu Rejestracji, gdzie inspektor ds. rejestracji przygotowuje **zgłoszenie** – przydzielenie lub przepisania od innego dostawcy adresu do doręczeń elektronicznych. Po otrzymaniu adresu do doręczeń Certum przesyła niezwłocznie informację o jego utworzeniu na adres poczty elektronicznej administratora skrzynki doręczeń jeżeli został wskazany, a w przypadku podmiotu niepublicznego będącego osobą fizyczną – także na adres poczty elektronicznej wnioskodawcy wskazany we wniosku.

4.2.1. Realizacja funkcji identyfikacji i uwierzytelnienia

Funkcje identyfikacji i uwierzytelniania wszystkich wymaganych danych usługobiorcy są realizowane przez Główny Punkt Rejestracji oraz współpracujące Punkty Rejestracji i Punkty Potwierdzania Tożsamości zgodnie z warunkami określonymi w rozdz. 1.3.2.

4.2.2. Przyjęcie lub odrzucenie wniosku

4.2.2.1. Procedura przyjęcia wniosku

Punkt Rejestracji lub Punkt Potwierdzania Tożsamości przyjmuje i weryfikuje wniosek o dostęp do usługi eDoręczenia i wraz z wymaganym kompletem dokumentów przekazuje go do Głównego Punktu Rejestracji skąd wniosek jest przekazywany do BAE (Bazie Adresów Elektronicznych) w celu nadania nowego lub przepisania od innego dostawcy adresu do doręczeń.

4.2.2.2. Odmowa przyjęcia wniosku

Certum może odmówić przyjęcia wniosku dowolnemu wnioskodawcy bez zaciągania jakichkolwiek zobowiązań lub narażania się na jakąkolwiek odpowiedzialność, które powstać mogą wskutek poniesionych przez wnioskodawcę (w wyniku odmowy) strat lub kosztów. Certum zwraca w takim przypadku wnioskodawcy wniesioną przez niego opłatę za dostęp do usługi eDoręczenia (jeśli dokonał stosownej przedpłaty), chyba że wnioskodawca we wniosku o dostęp do usługi umieścił sfałszowane lub nieprawdziwe dane.

Odmowa przyjęcia wniosku może nastąpić w następujących przypadkach:

- identyfikator usługobiorcy ubiegającego się o dostęp do usługi pokrywa się z identyfikatorem innego usługobiorcy,
- uzasadnionego podejrzenia, że usługobiorca sfałszował lub podał nieprawdziwe dane,

- niedostarczenia przez wnioskodawcę kompletu wymaganych dokumentów, stanowiących załącznik do wniosku o dostęp do usługi eDoręczenia,
- wykrycia odręcznych poprawek lub modyfikacji w przesłanych dokumentach formalnych,
- przekroczenia terminu ważności przesłanych dokumentów - za przedawnione uznaje się te dokumenty, których data podpisu przekroczyła termin 3 miesięcy na dzień wpłynięcia do Certum w formie elektronicznej,
- przekroczenia terminu ważności wniosku o dostęp do usługi - za przedawnione uznaje się te wioski, których data wypełnienia przekroczyła termin 3 miesięcy na dzień wpłynięcia do Certum w formie elektronicznej,
- innych, ważnych nie wymienionych powyżej przyczyn, po uprzednim uzgodnieniu odmowy z **inspektorem bezpieczeństwa**.

Informacja o odmowie udzielenia dostępu do usługi eDoręczenia przesyłana jest wnioskodawcy w postaci odpowiedniej decyzji z krótkim uzasadnieniem przyczyny odmowy. Od odmownej decyzji wnioskodawca może odwołać się do Certum w terminie 14 dni od daty otrzymania decyzji.

4.2.3. Okres oczekiwania na dostęp do usługi

Certum dokłada wszelkich starań, aby w jak najkrótszym czasie od momentu otrzymania wniosku o dostęp do usługi przeprowadzić jego weryfikację oraz udzielić dostęp do usługi.

Czas ten zależy głównie od dokładności dostarczonego wniosku oraz ewentualnych administracyjnych uzgodnień i wyjaśnień pomiędzy Certum a wnioskodawcą. Czasu oczekiwania na w BAE (Baza Adresów Elektronicznych) na nadania nowego lub przepisania od innego dostawcy adresu do doręczeń elektronicznych.

Jeśli przyczyny, ze względu na które mogą wystąpić ewentualne opóźnienia w wydaniu dostępu do usługi leżą tylko po stronie Certum, to czas ten nie powinien przekroczyć 7 dni roboczych od momentu zaakceptowania warunków świadczenia usługi eDoręczenia przez Asseco Data Systems S.A. i usługobiorcę.

4.3. Schematy procesu świadczenia usługi eDoręczenia

Usługa eDoręczenia wykorzystuje technologię, która po wstępnej identyfikacji nadawcy i jego uwierzytelnieniu umożliwia wysyłanie wiadomości i załączonych dokumentów/plików jako przesyłek. Wykorzystywany system zapewnia wysyłanie przesyłek w zabezpieczonym i zaszyfrowanym kanale.

Wysyłane i odbierane przesyłki nie są skanowane przez oprogramowanie antywirusowe.

Usługa eDoręczenia dostarcza dowodów zdarzeń, które zachodzą podczas procesu przesyłania (wiadomości, dokumentów, plików i innych elementów) pomiędzy stronami (np. informacji o tym, że dane zostały wysłane przez nadawcę lub dostarczone do adresata). Dowody takie mogą być wykorzystane do udowodnienia osobom trzecim, a także w postępowaniu sądowym, gdy jest to konieczne, że wymiana wiadomości lub dokumentów nastąpiła w określonym momencie czasu, co jest potwierdzone kwalifikowanym znacznikiem czasu.

Dowody dostarczane w ramach usługi eDoręczenia są podpisywane kwalifikowaną pieczęcią elektroniczną oraz kwalifikowanym znacznikiem czasu. Dowód zawiera informację, że w określonym momencie czasowym miało miejsce określone zdarzenie związane z procesem transmisji danych pomiędzy nadawcą a adresatem (np. wysłanie lub odebranie wiadomości). Dowód może być natychmiast dostarczony do nadawcy/adresata, ale jest również przechowywany przez okres 20 lat w celu późniejszego dostępu przez zainteresowane strony zgodnie z krajowym ustawodawstwem.

4.4. Proces świadczenia usługi eDoręczenia

Dostęp do usługi eDoręczenia odbywa się za pomocą portalu internetowego, poprzez udostępnianie API. Korzystanie z usługi wymaga wstępnej identyfikacji nadawcy i adresata dokonywanej zdalnie za pomocą aplikacji mobilnej lub poprzez osobiste stawiennictwo tych osób lub ich przedstawicieli w punkcie systemu rejestracji (patrz pkt. 3.2). Dane usługobiorców, które są gromadzone przez Certum to dane osobowe, dane kontaktowe, dane z dokumentów tożsamości i inne.

Usługa eDoręczenia udostępnia nadawcy wybranie jednej z trzech opcje przesłania przesyłek do odbiorcy:

- BASIC – przesyłka zwykła - treść przesyłki zostaje udostępniona adresatowi bez możliwości odrzucenia.
- CONSENTED – przesyłka awizowana – powiadomienie wysyłane jest do adresata przed przesyłką. Adresat jest zobowiązany do zaakceptowania lub odrzucenia treści przesyłki, treść przesyłki jest udostępniana dopiero po jej zaakceptowaniu przez adresata.
- CONSENTED SIGNED – jak w przypadku CONSENTED – z dodatkiem wymogu podpisu, wymagane jest cyfrowe podpisanie przez adresata potwierdzenia odbioru.

Przesyłki doręczane za pośrednictwem publicznej usługi eDoręczenia są obsługiwane jedynie w opcji BASIC.

Usługa eDoręczenia nie udostępnia innych opcji przesłania przesyłek od nadawcy do odbiorcy.

Usługa eDoręczenia umożliwia wysłanie przez usługobiorcę zaproszenia do skrzynki dla innych użytkowników.

Usługobiorca, czyli właściciel skrzynki samodzielnie nadzoruje i umożliwia dostęp do skrzynki innym użytkownikom. Użytkownicy tacy nie podlegają nadzorowi Certum. Usługobiorca jest administratorem danych osobowych innych użytkowników, które utrzymuje w swojej skrzynce.

4.5. Identyfikacja Nadawcy i Adresata

4.5.1. Identyfikacja Nadawcy

Certum dokonuje weryfikacji tożsamości nadawcy:

- przez fizyczną obecność osoby fizycznej lub upoważnionego przedstawiciela osoby prawnej (zgodnie z reprezentacją lub na podstawie pełnomocnictwa),
- za pomocą certyfikatu kwalifikowanego.

Zgodnie z informacją zawartą w pkt. 3.2..

Dopiero po pomyślnym uwierzytelnieniu nadawcy, przesyłka jest przekazywana z kontrolowanego przez niego systemu do usługi eDoręczenia.

Proces uwierzytelniania odbywa się w bezpiecznym i kontrolowanym środowisku. Wszystkie dowody uwierzytelnienia i nadania przesyłki są gromadzone i przechowywane w chronionym środowisku.

4.5.2. Identyfikacja Adresata

Certum dokonuje weryfikacji tożsamości adresata:

- przez fizyczną obecność osoby fizycznej lub upoważnionego przedstawiciela osoby prawnej (zgodnie z reprezentacją lub na podstawie pełnomocnictwa),
- za pomocą certyfikatu kwalifikowanego.

Zgodnie z informacją zawartą w pkt. 3.2..

Dopiero po pomyślnym uwierzytelnieniu adresata, przesyłka jest przekazywana z kontrolowanego przez niego systemu oraz do adresata.

Proces uwierzytelniania odbywa się w bezpiecznym i kontrolowanym środowisku. Wszystkie dowody uwierzytelnienia i odbioru przesyłki są gromadzone i przechowywane w chronionym środowisku.

4.6. Gromadzenie dowodów

Usługa eDoręczenia dostarcza dowodów na wysyłanie i odbieranie treści użytkownika.

Dowód jest dostarczany jako oddzielny dokument elektroniczny w ściśle określonym formacie, wskazujący dokładną datę i godzinę poprzez kwalifikowany znacznik czasu. Dowód jest podpisany elektronicznie przez urząd eDoręczenia.

Certum gromadzi i przechowuje dane dotyczące:

- wszystkich zdarzeniach związanych ze wstępną weryfikacją tożsamości nadawcy i jego identyfikacją;
- wszystkich zdarzeń związanych ze wstępną weryfikacją tożsamości adresata i jego identyfikacją;
- przy wstępnej weryfikacji tożsamości weryfikowane są dane dokumentu tożsamości osoby fizycznej (np. dowód osobisty, mDowód, paszport lub polskiej karta pobytu), dane identyfikacyjne osoby prawnej (np. dokumenty rejestrowe, pełnomocnictwa itp.) oraz wszystkie inne dane, które są niezbędne do jej poprawnej identyfikacji;
- dane służące do wstępnej identyfikacji nadawcy/adresata;
- dane dotyczące działania usługi potwierdzające uwierzytelnienie nadawcy i adresata oraz komunikacji między nimi;
- dowody w zakresie nadania, powiadomieniu o wysłaniu przesyłki oraz doręczenia;
- dowody potwierdzające, że treść przekazana przez nadawcę została odebrana przez adresata;
- dowód, że treść przekazana przez nadawcę nie została zmieniona w trakcie transmisji,
- dowody dotyczące przesyłek wykonywanych przez innych użytkowników zaproszonych przez usługobiorcę, przekazywane do usługi niebędącej usługą RDE. Dowody zawierają dane usługobiorcy (właściciela skrzynki).

Wszystkie gromadzone dowody są przechowywane w chronionym środowisku.

Wszystkie dowody są dostarczane za pośrednictwem:

a) Agent użytkownika QERDS – internetowy interfejs usługi QERDS;

b) API QERDS.

Dowody są udostępniane wyłącznie agentowi użytkownika QERDS.

4.6.1. Dowody związane z Nadawcą

Usługa generuje dowód wysłania, który może być również dostarczony stronie trzeciej. Dowód pokazuje dokładną datę i godzinę wysłania treści użytkownika przez nadawcę.

- Akceptacja nadania przesyłki

Nadawca pomyślnie przesyła przesyłkę do usługi eDoręczenia.

Generowany jest dowód z wstępnie ustaloną datą i godziną, wskazujący, że nadawca, złożył przesyłkę w usłudze eDoręczenia, która została zaakceptowana przez dostawcę, a ten podejmie wszelkie niezbędne działania w celu dostarczenia jej do odpowiedniego adresata(ów).

- Odrzucenie nadania przesyłki

Nadawca przesłał przesyłkę do usługi eDoręczenia, przesyłka nie została zaakceptowana przez usługę. Wygenerowany dowód wskazuje, że nadawca, przekazał przesyłkę do usługi w określonym dniu i czasie, a usługa eDoręczenia odmówiła wykonania niezbędnych czynności.

4.6.2. Dowody związane z Adresatem

Usługa generuje dowód odbioru, który może być również dostarczony stronie trzeciej. Dowód pokazuje dokładną datę i godzinę wysłania treści użytkownika przez nadawcę.

- Dostarczenie przesyłki

Treść przesyłki została dostarczona do adresata.

Powiązane dowody wykazują, że przesyłka została dostarczona do adresata w ustalonym czasie.

- Niepowodzenie w dostarczeniu przesyłki

Przesyłka nie może zostać dostarczona do adresata w ustalonym czasie z powodu błędów technicznych i/lub z innych powodów. Może nie być dowodów na dostarczenie treści w ustalonym czasie.

Niemożność dostarczenia przesyłki może być spowodowana różnymi zdarzeniami, takimi jak:

- Usługa eDoręczenia nie była w stanie przesłać treści od nadawcy do adresata.
- W czasie, gdy wiadomość znajdowała się w usłudze eDoręczenia system, w określonym czasie nie otrzymał żadnego dowodu pomyślnego doręczenia.

W takich przypadkach generowane są dowody przyczyny niedostarczenia zgodnie z normą *ETSI EN 319 522-1.*

4.6.3. Rodzaje generowanych dowodów

Certum gromadzi i przechowuje następujące rodzaje dowodów:

- Rodzaje gromadzonych dowodów dla poszczególnych zdarzeń zgodnie z normie *ETSI EN 319 522-1.*

ID	**Nazwa zdarzenia**
Zgłoszenie nadania przesyłki	
A.1	Akceptacja nadania przesyłki **(SubmissionAcceptance)**
A.2	Odrzucenie nadania przesyłki **(SubmissionRejection)**
Zdarzenia związane z przekazywaniem przesyłki między usługami RDE	
B.1	Akceptacja przekazania przesyłki pomiędzy usługami RDE **(RelayAcceptance)**
B.2	Odrzucenie przekazania przesyłki pomiędzy usługami RDE **(RelayRejection)**
B.3	Błąd przekazania **(RelayFailure)**
Zdarzenia związane z przyjęciem / odrzuceniem przez adresata	
C.1	Notyfikacja o akceptacji odbioru **(NotificationForAcceptance)**
C.2	Notyfikacja o błędzie akceptacji odbioru **(NotificationForAcceptanceFailure)**

C.3	Akceptacja preawizacji **(ConsignmentAcceptance)**
C.4	Odrzucenie preawizacji **(ConsignmentRejection)**
C.5	Wygaśnięcie czasu na akceptację/odrzucenie przesyłki **(AcceptanceRejectionExpiry)**
Zdarzenia związane z zawiadomieniem adresata (preawizacja) o nadejściu przesyłki	
D.1	Przesyłka przygotowana do odbioru **(ContentConsignment)**
D.2	Błąd przygotowania przesyłki do odbioru z powodu błędu technicznego **(ContentConsignmentFailure)**
D.3	Notyfikacja o przesyłce gotowej do odbioru **(ConsignmentNotification)**
D.4	Błąd notyfikacji o przesyłce gotowej do odbioru (**ConsignmentNotificationFailure)**
Zdarzenia związane z dostarczeniem przesyłki do adresata	
E.1	Dostarczenie przesyłki **(ContentHandover)**
E.2	Błąd dostarczenia przesyłki **(ContentHandoverFailure)**
Zdarzenia związane z połączeniami z systemami innymi niż usługa RDE	
F.1	Przekazanie do usługi niebędącej usługą RDE **(RelayToNonERDS)**
F.2	Błąd przekazania do usługi niebędącej usługą RDE **(RelayToNonERDSFailure)**
F.3	Odbiór przesyłki przez usługę niebędącą usługą RDE **(ReceivedFromNonERDS)**

- Rodzaje gromadzonych dowodów dla poszczególnych zdarzeń zgodnie z wymaganiami ustawy.

ID	**Nazwa zdarzenia**
KP.1	Potwierdzenie wysłania (**ShipingConfirmation)**
KP.2	Potwierdzenie otrzymania (**Delivery Confirmation)**

- Rodzaje gromadzonych wewnętrznych dowodów Certum dla poszczególnych zdarzeń - nie wymagane normą ETSI czy ustawą.

ID	**Nazwa zdarzenia**
CE.1	Potwierdzenie przyjęcia paczki korespondencji (**BatchMessagesRelayConfirmation)**
CE.2	Błąd przyjęcia paczki korespondencji (**BatchMessagesRelayFailure)**
CE.3	Oświadczenie woli odebrania preawizacji (**ConsignmentAcceptanceWillDeclaration)**
CE.4	Oświadczenie woli odrzucenia preawizacji (**ConsignmentRemovalWillDeclaration)**
CE.5	Usunięcie przesyłki (**ConsignmentRemoval)**

4.7. Ochrona przekazywanych danych przed ryzykiem utraty, kradzieży, uszkodzenia lub nieuprawnionej modyfikacji

Zabezpieczenia dotyczące przesyłek są zgodne z standardem usługi RDE.

Pozostałe zabezpieczenia patrz rozdział 5.

4.8. Odnowienie subskrypcji usługi eDoręczenia

Certum udostępnia możliwość odnowienia dostępu do usługi eDoręczenia przed upływem ważności skrzynki.

4.9. Zakończenie subskrypcji usługi eDoręczenia

Certum udostępnia możliwość wykreślenia adresu do doręczeń elektronicznych z rejestru BAE.

Za koniec świadczenia usługi eDoręczenia, pozwalającej na komunikację z podmiotami publicznymi (bez względu czy został on zgłoszony przez klienta czy zainicjowany przez system wskutek nieprzedłużenia abonamentu), Certum przyjmuje moment zgłoszenia do rejestru BAE, chęci rezygnacji z obsługi adresu ADE związanego ze skrzynką, niezależnie od tego jak przebiega faktyczny proces przekazywania/deaktywacji adresu ADE w samym rejestrze BAE.

4.9.1. Kto może wnioskować o zakończenie subskrypcji usługi eDoręczenia

Wniosek o zakończenie subskrypcji usługi eDoręczenia, wykreślenia adresu do doręczeń elektronicznych z rejestru BAE może być złożony:

- osobę fizyczną dla, której adres do doręczeń elektronicznych został założony,
- osobę prawną – upoważnionego przedstawiciela osoby prawnej dla, której adres do doręczeń elektronicznych został założony.

5. Zabezpieczenia techniczne, organizacyjne i operacyjne

W rozdziale opisano ogólne wymagania w zakresie nadzoru nad zabezpieczeniami fizycznymi, organizacyjnymi oraz działaniami personelu, stosowanymi w Certum.

5.1. Zabezpieczenia fizyczne

Zakres związany z przedmiotowym punktem zaadresowany został w Polityce Głównej.

5.1.1. Miejsce lokalizacji oraz budynek

Zakres związany z przedmiotowym punktem zaadresowany został w Polityce Głównej.

5.1.2. Dostęp fizyczny

Zakres związany z przedmiotowym punktem zaadresowany został w Polityce Głównej.

5.1.3. Zasilanie oraz klimatyzacja

Zakres związany z przedmiotowym punktem zaadresowany został w Polityce Głównej.

5.1.4. Zagrożenie zalaniem

Zakres związany z przedmiotowym punktem zaadresowany został w Polityce Głównej.

5.1.5. Ochrona przeciwpożarowa

Zakres związany z przedmiotowym punktem zaadresowany został w Polityce Głównej.

5.1.6. Nośniki informacji

Zakres związany z przedmiotowym punktem zaadresowany został w Polityce Głównej.

5.1.7. Niszczenie zbędnych nośników i informacji

Zakres związany z przedmiotowym punktem zaadresowany został w Polityce Głównej.

5.1.8. Przechowywanie kopii bezpieczeństwa

Zakres związany z przedmiotowym punktem zaadresowany został w Polityce Głównej.

5.1.9. Bezpieczeństwo punktów rejestracji

Zakres związany z przedmiotowym punktem zaadresowany został w Polityce Głównej.

5.1.9.1. Miejsce lokalizacji oraz budynek

Zakres związany z przedmiotowym punktem zaadresowany został w Polityce Głównej.

5.1.9.2. Dostęp fizyczny

Zakres związany z przedmiotowym punktem zaadresowany został w Polityce Głównej.

5.1.9.3. Zasilanie oraz klimatyzacja

Zakres związany z przedmiotowym punktem zaadresowany został w Polityce Głównej.

5.1.9.4. Zagrożenie wodne

Zakres związany z przedmiotowym punktem zaadresowany został w Polityce Głównej.

5.1.9.5. Ochrona przeciwpożarowa

Zakres związany z przedmiotowym punktem zaadresowany został w Polityce Głównej.

5.1.9.6. Nośniki informacji

Zakres związany z przedmiotowym punktem zaadresowany został w Polityce Głównej.

5.1.9.7. Niszczenie informacji

Zakres związany z przedmiotowym punktem zaadresowany został w Polityce Głównej.

5.1.9.8. Przechowywanie kopii bezpieczeństwa

Zakres związany z przedmiotowym punktem zaadresowany został w Polityce Głównej.

5.1.10. Bezpieczeństwo usługobiorcy

Usługobiorca powinien chronić swoje hasło dostępu do systemu oraz osobisty numer identyfikacyjny (PIN). Jeżeli używane hasło lub PIN są trudne do zapamiętania, mogą zostać zapisane jednak pod warunkiem przechowywania ich w sejfie, do którego dostęp ma tylko usługobiorca lub zaszyfrowaniu hasła (algorytmem znanym właścicielowi danego numeru PIN).

5.2. Zabezpieczenia organizacyjne

Zakres związany z przedmiotowym punktem zaadresowany został w Polityce Głównej.

Poniżej przedstawiono listę ról, które mogą pełnić pracownicy zatrudnieni w Certum, jest ona zgodna z wymogami opisanymi w *ETSI EN 319 401 Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers* oraz *ETSI EN 319 521 Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Electronic Registered Delivery Service Providers.*

5.2.1. Zaufane role

5.2.1.1. Zaufane role w Certum

Zakres związany z przedmiotowym punktem zaadresowany został w Polityce Głównej.

W Certum określono zaufane role opisane w Polityce Głównej oraz Inspektor ds. weryfikacji tożsamości:

- **Inspektor ds. weryfikacji tożsamości** - odpowiada za weryfikacji tożsamości usługobiorców (nadawcy i adresata) zgodne z określonym procesem wstępnej weryfikacji tożsamości zgodnie z normą *ETSI 319 521*.

Rolę inspektora ds. weryfikacji tożsamości pełni inspektor ds. rejestracji i on wykonuje wszystkie jego funkcje.

Poszczególne role oraz obowiązki z nimi związane udokumentowane są w wewnętrznych procedurach Certum, ponadto obowiązki są opisane w indywidualnych umowach z pracownikami (z uwzględnieniem pracowników tymczasowych).

5.2.1.2. Zaufane role w punkcie systemu rejestracji

Certum musi być pewne, że obsługa punktu systemu rejestracji rozumie swoją odpowiedzialność wynikającą z konieczności rzetelnej identyfikacji oraz uwierzytelniania usługobiorcy. Z tego powodu w punkcie systemu rejestracji wyróżnia się następujące role:

- **osoba potwierdzająca tożsamość wnioskodawcy** – weryfikuje tożsamość usługobiorcy oraz poprawność złożonego przez niego wniosku i w imieniu Asseco Data Systems S.A. akceptuje warunki świadczenia usługi eDoręczenia,
- **Partner prowadzący autoryzowany punktu rejestracji** – odpowiada za sprawne działanie punktu systemu rejestracji; jego rola polega na zapewnieniu finansowania pracowników, zarządzaniu pracą osób potwierdzających tożsamość usługobiorców.

Osoba potwierdzająca tożsamość usługobiorców musi posiadać akredytację Certum. Po jej uzyskaniu (na swój wniosek lub Partnera autoryzowanego punktu rejestracji) może potwierdzać tożsamość usługobiorców zarówno w siedzibie punktu systemu rejestracji jak też w miejscu pobytu usługobiorcy.

5.2.1.3. Zaufane role u usługobiorcy

Niniejsza Polityka eDoręczenia nie określa żadnych wymagań w tym zakresie.

5.2.2. Liczba osób wymaganych do realizacji zadania

Zakres związany z przedmiotowym punktem zaadresowany został w Polityce Głównej.

5.2.3. Identyfikacja oraz uwierzytelnianie ról

Zakres związany z przedmiotowym punktem zaadresowany został w Polityce Głównej.

5.2.4. Role, które nie mogą być łączone

Zakres związany z przedmiotowym punktem zaadresowany został w Polityce Głównej.

5.3. Nadzorowanie personelu

Zakres związany z przedmiotowym punktem zaadresowany został w Polityce Głównej.

5.3.1. Kwalifikacje, doświadczenie oraz upoważnienia

Zakres związany z przedmiotowym punktem zaadresowany został w Polityce Głównej.

5.3.2. Procedura weryfikacji personelu

Zakres związany z przedmiotowym punktem zaadresowany został w Polityce Głównej.

5.3.3. Wymagania dotyczące przeszkolenia

Zakres związany z przedmiotowym punktem zaadresowany został w Polityce Głównej.

Personel wykonujący czynności w ramach usługi eDoręczenia muszą być przeszkoleni w zakresie procedury weryfikacji tożsamości usługobiorców oraz obsługi systemu.

5.3.4. Częstotliwość powtarzania szkoleń oraz wymagania

Zakres związany z przedmiotowym punktem zaadresowany został w Polityce Głównej.

5.3.5. Częstotliwość rotacji stanowisk i jej kolejność

Zakres związany z przedmiotowym punktem zaadresowany został w Polityce Głównej.

5.3.6. Sankcje z tytułu nieuprawnionych działań

Zakres związany z przedmiotowym punktem zaadresowany został w Polityce Głównej.

5.3.7. Pracownicy kontraktowi

Zakres związany z przedmiotowym punktem zaadresowany został w Polityce Głównej.

5.3.8. Dokumentacja przekazana personelowi

Zakres związany z przedmiotowym punktem zaadresowany został w Polityce Głównej.

5.4. Rejestrowanie zdarzeń, zarządzanie incydentami bezpieczeństwa oraz audyty bezpieczeństwa

Zakres związany z przedmiotowym punktem zaadresowany został w Polityce Głównej.

5.4.1. Typy rejestrowanych zdarzeń

Zakres związany z przedmiotowym punktem zaadresowany został w Polityce Głównej.

5.4.2. Częstotliwość analizy zapisów rejestrowanych zdarzeń (logów)

Zakres związany z przedmiotowym punktem zaadresowany został w Polityce Głównej.

5.4.3. Okres przechowywania zapisów rejestrowanych zdarzeń

Zakres związany z przedmiotowym punktem zaadresowany został w Polityce Głównej.

5.4.4. Ochrona zapisów rejestrowanych zdarzeń

Zakres związany z przedmiotowym punktem zaadresowany został w Polityce Głównej.

5.4.5. Procedury tworzenia kopii zapisów rejestrowanych zdarzeń

Zakres związany z przedmiotowym punktem zaadresowany został w Polityce Głównej.

5.4.6. System gromadzenia danych na potrzeby audytu (wewnętrzny a zewnętrzny)

Zakres związany z przedmiotowym punktem zaadresowany został w Polityce Głównej.

5.4.7. Powiadamianie podmiotów odpowiedzialnych za zaistniałe zdarzenie

Zakres związany z przedmiotowym punktem zaadresowany został w Polityce Głównej.

5.4.8. Oszacowanie podatności na zagrożenia

Zakres związany z przedmiotowym punktem zaadresowany został w Polityce Głównej.

5.5. Archiwizowanie danych

Wymaga się, aby archiwizacji podlegały wszystkie dane i pliki dotyczące rejestrowanych danych o zabezpieczeniach systemu, wnioski napływające od usługobiorców, informacje o usługobiorcach, dowody ze zdarzeń zachodzących w ramach procesu doręczania.

Archiwalne kopie danych elektronicznych przechowywane są w ośrodku głównym oraz w ośrodku zapasowym Certum.

5.5.1. Rodzaje archiwizowanych danych

Archiwizacji podlegają następujące dane:

- dane potwierdzające tożsamość usługobiorcy (nadawcy i adresata),
- dokumenty wystawiane przez operatora systemu punktu rejestracji, potwierdzających tożsamość usługobiorców w imieniu Certum,
- zaakceptowane przez usługobiorcę warunki świadczenia usługi eDoręczenia,
- baza danych usługobiorców, w tym wszystkie informacje zebrane w procesie rejestracji usługobiorcy,
- pozostałe dokumenty i dane, związane ze świadczeniem usługi eDoręczenia.

Archiwizacji podlegają również dowody dotyczące usługi:

- zdarzenia, które mają miejsce podczas przesyłania danych między stronami,
- dowód z usługi, że określone zdarzenie związane z procesem przekazywania określonych danych między nadawcą a adresatem miało miejsce w określonym czasie,
- tokeny znaczników czasu odpowiadające dacie i godzinie wysłania i przekazania oraz modyfikacji przesyłki, stosownie do przypadku.

5.5.2. Okres przechowywania archiwum

Archiwizowane dane (w formie elektronicznej), wymienione w rozdz. 5.5.1 przechowywane są przez okres 20 lat. Po upływie przyjętego okresu archiwizacji dane są niszczone.

Zdarzenia związane ze składaniem, przesyłaniem i przekazywaniem przesyłki przechowywane są przez co najmniej 36 miesięcy w zależności od wykupionego pakietu biznesowego.

5.5.3. Ochrona archiwum

Zakres związany z przedmiotowym punktem zaadresowany został w Polityce Głównej.

5.5.4. Procedury tworzenia kopii zapasowych

Zakres związany z przedmiotowym punktem zaadresowany został w Polityce Głównej.

Kopie zapasowe umożliwiają całkowite odtworzenie (jeśli jest to konieczne, np. po awarii systemu) danych niezbędnych do normalnego funkcjonowania usługi.

Kopie zapasowe wykonywane są przez personel Certum pełniący zaufane role. Kopie zapasowe podlegają okresowej weryfikacji, odtworzeniu zgodnie z wewnętrznymi procedurami Certum.

Aby zapobiec utracie danych usługa eDoręczenia gwarantuje ich ochronę z wykorzystaniem mechanizmów backupu i replikacji danych conajmniej raz na 24h. Oznacza to, że odzyskanie danych w przypadku awarii oprogramowania lub infrastruktury realizowane jest zgodnie z następującymi wskaźnikami:

- RPO (Recovery Point Objective) dla usługi wynosi 24h.
- RTO (Recovery Time Objective) dla usługi wynosi 24h.

5.5.5. Wymaganie znakowania archiwizowanych danych elektronicznym znacznikiem czasu

Zakres związany z przedmiotowym punktem zaadresowany został w Polityce Głównej.

5.5.6. System gromadzenia danych archiwalnych (wewnętrzny a zewnętrzny)

Zakres związany z przedmiotowym punktem zaadresowany został w Polityce Głównej.

5.5.7. Procedury dostępu oraz weryfikacji zarchiwizowanej informacji

Zakres związany z przedmiotowym punktem zaadresowany został w Polityce Głównej.

5.6. Zmiana klucza

Procedura zmiany klucza odnosi się do klucza usługi eDoręczenia i dotyczy procesu aktualizacji klucza, który zastąpi klucz używany dotychczas do podpisywania dowodów z usługi.

Procedura aktualizacji klucza powyżej usługi eDoręczenia polega na wystąpieniu do narodowego centrum certyfikacji z wnioskiem o wydanie nowego certyfikatu dostawcy usług zaufania. Po otrzymaniu certyfikatu urząd ten wydaje narodowemu centrum certyfikacji wzajemne certyfikaty dostawców usług zaufania.

Każda zmiana klucza usługi eDoręczenia anonsowana jest odpowiednio wcześniej za pośrednictwem repozytorium Certum.

5.7. Naruszenie ochrony klucza i uruchamianie po awariach oraz klęskach żywiołowych

Zakres związany z przedmiotowym punktem zaadresowany został w Polityce Głównej.

5.7.1. Procedury obsługi incydentów i reagowania na zagrożenia

Zakres związany z przedmiotowym punktem zaadresowany został w Polityce Głównej.

5.7.2. Uszkodzenie zasobów obliczeniowych, oprogramowania i/lub danych

Zakres związany z przedmiotowym punktem zaadresowany został w Polityce Głównej.

5.7.3. Ujawnienie lub podejrzenie ujawnienia kluczy prywatnych urzędu certyfikacji

Zakres związany z przedmiotowym punktem zaadresowany został w Polityce Głównej.

5.7.4. Zapewnienie ciągłości działania po katastrofach

Zakres związany z przedmiotowym punktem zaadresowany został w Polityce Głównej.

5.8. Zakończenie działalności lub przekazanie zadań przez usługę eDoręczenia

Przedstawione poniżej obowiązki usługi eDoręczenia mają na uwadze redukcję wpływu skutków podjęcia przez Certum decyzji o zakończeniu swojej działalności i obejmują obowiązek odpowiednio wczesnego poinformowania o tym organu nadzoru, usługobiorców, kontrahentów, i Partnerów z którymi Centrum jest związane umowami handlowym oraz przekazania dokumentów i danych związanych ze świadczeniem usługi organowi nadzoru. Szczegółowy sposób postępowania w przypadku zakończenia działalności przez Centrum określa plan zakończenia działalności Centrum, stanowiący wewnętrzną procedurę Certum.

Organ nadzoru jest informowany o planach zakończenia działalności Certum, oraz każdorazowo o każdej znaczącej jego zmianie.

5.8.1. Wymagania związane z przekazaniem obowiązków

Po podjęciu decyzji o zakończeniu działalności Certum zobowiązane jest do wykonania następujących czynności:

- powiadomienia **narodowego centrum certyfikacji** o zamiarze zaprzestania działalności jako kwalifikowanego podmiotu świadczącego usługę eDoręczenia; na co najmniej na 90 dni przed planowanym zakończeniem działalności,
- zawiadomienia (co najmniej na 90 dni wcześniej) wszystkich usługobiorców o zamiarze zakończenia działalności,
- powiadomienia Partnerów handlowych oraz Partnerów prowadzących Punkty Potwierdzenia Tożsamości oraz powiadomienia Punktów Rejestracji,
- powiadomienia innych podmiotów, z którymi Certum jest związane umowami handlowymi na świadczenie usługi eDoręczenia,
- poinformowania wszystkich usługobiorców związanych z usługą eDoręczenia o zaprzestaniu działalności,
- unieważnienia wszystkich wydanych pełnomocnictw do potwierdzania tożsamości usługobiorców oraz podpisywania umów o świadczenie usługi eDoręczenia w imieniu Asseco Data Systems S.A.,
- przekazanie danych, bezpośrednio związanych z wykonywaniem usługi eDoręczenia organowi nadzoru lub wskazanemu przez niego podmiotowi, w tym kluczy usługi eDoręczenia, dokumentów rejestracji usługobiorców, logowania zdarzeń oraz wszystkich informacji, które są niezbędne do dostarczenia dowodów przesyłek, włączając w to obowiązek zapewnienia ich dostępności przez odpowiedni okres (przez okres 20 lat od ich wytworzenia),
- zawarcia umów niezbędnych do prawidłowego przekazania danych i usługi (o których mowa powyżej), z podmiotami je przejmującymi, zawierającymi zobowiązanie do ich przechowywania przez wskazany ustawowo okres, tj.: przez okres 20 lat od ich wytworzenia,

- zniszczenia kluczy usługi eDoręczenia i ich kopii zapasowych, w przypadku gdy nie przewiduje się dalszego wykorzystania lub w przypadku unieważnienia certyfikatu dostawcy usługi eDoręczenia powiązanego z usługą,
- zwrotu usługobiorcy lub podmiotowi reprezentowanemu przez usługobiorcę kosztów, proporcjonalnie do pozostałego okresu ważności usługi.

5.8.2. Postępowanie w przypadku zakończenia działalności

Szczegółowy sposób postępowania w przypadku zakończenia działalności przez Certum określa plan zakończenia działalności, stanowiący wewnętrzną procedurę Certum.

Wszystkie aktualnie ważne certyfikaty dostawcy usługi eDoręczenia muszą być unieważnione w dniu deklarowanego, definitywnego zaprzestania działalności i umieszczone na liście CRL. Klucze prywatne usługi eDoręczenia muszą być zniszczone.

6. Procedury bezpieczeństwa technicznego

Rozdział ten opisuje procedury tworzenia oraz zarządzania parami kluczy kryptograficznych Certum, wraz z towarzyszącymi temu uwarunkowaniami technicznymi.

6.1. Generowanie pary kluczy i jej instalowanie

6.1.1. Generowanie par kluczy

Procedury zarządzania kluczami dotyczą bezpiecznego przechowywania i używania kluczy, będących pod kontrolą Certum, od których zależy bezpieczeństwo funkcjonowania całej usługi. Klucz prywatny urzędu eDoręczenia jest generowany i zabezpieczony na takim samym poziomie jak klucze innych urzędów zgodnie z Polityką Główną.

Usługa eDoręczenia posiada przynajmniej jeden certyfikat dostawcy usług zaufania Certum QERDS 2023, który stosowany jest w procesie kwalifikowanego rejestrowanego doręczenia elektronicznego.

6.1.1.1. Generowanie klucza publicznego i prywatnego

Zakres związany z przedmiotowym punktem zaadresowany został w Polityce Głównej.

6.1.1.1.1 Procedury generowania początkowych kluczy urzędu certyfikacji

Zakres związany z przedmiotowym punktem zaadresowany został w Polityce Głównej.

6.1.1.1.2 Procedury aktualizacji kluczy urzędu eDoręczenia

Zakres związany z przedmiotowym punktem zaadresowany został w Polityce Głównej.

Klucze urzędu Certum QERDS 2023 mają skończony okres życia, przed upływem którego muszą zostać uaktualnione.

Urząd Certum QERDS 2023 pozostaje ważny tak długo jak długo algorytmy użyte do jego wytworzenia pozostają uważane za bezpieczne.

Maksymalny czas po którym certyfikat urzędu Certum QERDS 2023 będzie musiał zostać odnowiony na podstawie nowych algorytmów określany jest zgodnie z normą ETSI TS 119 312 (Recommended key sizes versus time).

6.1.2. Przekazywanie klucza prywatnego użytkownikowi końcowemu

Nie dotyczy.

6.1.3. Przekazywanie klucza publicznego do urzędu certyfikacji

Przekazanie odbywa się zgodnie z zasadami Narodowego Centrum Certyfikacji opisanymi w Polityce Certyfikacji Narodowego Centrum Certyfikacji.

6.1.4. Przekazywanie klucza publicznego urzędu certyfikacji stronom ufającym

Zakres związany z przedmiotowym punktem zaadresowany został w Polityce Głównej.

6.1.5. Długości kluczy

Zakres związany z przedmiotowym punktem zaadresowany został w Polityce Głównej.

6.1.6. Parametry generowania klucza publicznego oraz weryfikacja jakości klucza

Zakres związany z przedmiotowym punktem zaadresowany został w Polityce Głównej.

6.1.7. Zastosowania kluczy

Zakres związany z przedmiotowym punktem zaadresowany został w Polityce Głównej.

6.1.8. Sprzętowe i/lub programowe generowanie kluczy

Zakres związany z przedmiotowym punktem zaadresowany został w Polityce Głównej.

Dotyczy również usługi eDoręczenia.

6.2. Ochrona klucza prywatnego

Zakres związany z przedmiotowym punktem zaadresowany został w Polityce Głównej.

6.2.1. Standard modułu kryptograficznego

Zakres związany z przedmiotowym punktem zaadresowany został w Polityce Głównej.

Sprzętowe moduły kryptograficzne używane przez usługę eDoręczenia jest zgodny z wymaganiami normy FIPS 140, Common Criteria EAL 4+.

Minimalne wymagania nakładane na moduł kryptograficzny

Typ podmiotu certyfikatu / certyfikaty dostawców usług zaufania certyfikatu dostawcy usług zaufania	Wykorzystywany moduł kryptograficzny
Urząd certyfikacji Certum QERDS 2023	Sprzętowy FIPS 140-2 Level 3 i wyżej / EAL 4+

6.2.2. Podział klucza prywatnego na części

Zakres związany z przedmiotowym punktem zaadresowany został w Polityce Głównej.

Sekrety współdzielone zapisywane są na kartach elektronicznych, chronione numerem PIN i w uwierzytelniony sposób przekazywane posiadaczom sekretu współdzielonego.

Podział i dystrybucja sekretów współdzielonych usługi eDoręczenia

Nazwa podmiotu świadczącego usługi zaufania	Liczba sekretów współdzielonych wymagana do odtworzenia klucza prywatnego	Całkowita liczba dystrybuowanych sekretów
Certum QERDS 2023	3	5

Procedura przekazania sekretów musi przewidywać udział posiadacza sekretu w procesie generowania kluczy i ich podziału, obejmować akceptację przekazanego sekretu, akceptację odpowiedzialności za przechowywany sekret oraz określać warunki i zasady udostępniania sekretu współdzielonego upoważnionym do tego osobom.

6.2.2.1. Akceptacja sekretu współdzielonego przez posiadacza sekretu

Zakres związany z przedmiotowym punktem zaadresowany został w Polityce Głównej.

6.2.2.2. Zabezpieczenie sekretu współdzielonego

Zakres związany z przedmiotowym punktem zaadresowany został w Polityce Głównej.

6.2.2.3. Dostępność oraz usunięcie (przeniesienie) sekretu współdzielonego

Zakres związany z przedmiotowym punktem zaadresowany został w Polityce Głównej.

6.2.2.4. Odpowiedzialność posiadacza sekretu współdzielonego

Zakres związany z przedmiotowym punktem zaadresowany został w Polityce Głównej.

6.2.3. Deponowanie klucza prywatnego

Zakres związany z przedmiotowym punktem zaadresowany został w Polityce Głównej.

6.2.4. Kopie zapasowe klucza prywatnego

Zakres związany z przedmiotowym punktem zaadresowany został w Polityce Głównej.

6.2.5. Archiwizowanie klucza prywatnego

Zakres związany z przedmiotowym punktem zaadresowany został w Polityce Głównej.

Dotyczy również klucza prywatnego usługi eDoręczenia.

6.2.6. Wprowadzanie klucza prywatnego do modułu kryptograficznego

Zakres związany z przedmiotowym punktem zaadresowany został w Polityce Głównej.

Dotyczy również klucza prywatnego usługi eDoręczenia.

6.2.7. Przechowywanie klucza prywatnego w module kryptograficznym

Zakres związany z przedmiotowym punktem zaadresowany został w Polityce Głównej.

6.2.8. Metody aktywacji klucza prywatnego

Zakres związany z przedmiotowym punktem zaadresowany został w Polityce Głównej.

Zasady te dotyczę również klucza prywatnego usługi eDoręczenia.

6.2.9. Metody dezaktywacji klucza prywatnego

Zakres związany z przedmiotowym punktem zaadresowany został w Polityce Głównej.

Zasady te dotyczę również klucza prywatnego usługi eDoręczenia.

6.2.10. Metody niszczenia klucza prywatnego

Zakres związany z przedmiotowym punktem zaadresowany został w Polityce Głównej.

Zasady te dotyczę również klucza prywatnego usługi eDoręczenia.

6.2.11. Ocena modułu kryptograficznego

Zakres związany z przedmiotowym punktem zaadresowany został w Polityce Głównej.

6.3. Inne aspekty zarządzania kluczami

Zakres związany z przedmiotowym punktem zaadresowany został w Polityce Głównej.

6.3.1. Archiwizacja kluczy publicznych

Zakres związany z przedmiotowym punktem zaadresowany został w Polityce Głównej.

6.3.2. Okresy stosowania klucza publicznego i prywatnego

Zakres związany z przedmiotowym punktem zaadresowany został w Polityce Głównej.

Standardowe maksymalne okresy ważności kluczy prywatnych oraz związanych z nimi certyfikatów dostawcy usług zaufania urzędu eDoręczenia.

Typ właściciela klucza i rodzaj klucza		Główny rodzaj zastosowania klucza	
		RSA do podpisu certyfikatów i list CRL	RSA do podpisu tokenów
Certum QERDS 2023	certyfikat dostawcy	–	11 lat
	klucz prywatny	–	11 lat

6.4. Dane aktywujące

Zakres związany z przedmiotowym punktem zaadresowany został w Polityce Głównej.

Zasady te dotyczę również usługi eDoręczenia.

6.4.1. Generowanie danych aktywujących i ich instalowanie

Zakres związany z przedmiotowym punktem zaadresowany został w Polityce Głównej.

6.4.2. Ochrona danych aktywujących

Zakres związany z przedmiotowym punktem zaadresowany został w Polityce Głównej.

6.4.3. Inne aspekty związane z danymi aktywującymi

Zakres związany z przedmiotowym punktem zaadresowany został w Polityce Głównej.

6.5. Zabezpieczenia systemu komputerowego

Zakres związany z przedmiotowym punktem zaadresowany został w Polityce Głównej.

Zasady te dotyczę również usługi eDoręczenia.

6.5.1. Wymagania techniczne dotyczące specyficznych zabezpieczeń systemów komputerowych

Zakres związany z przedmiotowym punktem zaadresowany został w Polityce Głównej.

6.5.2. Ocena bezpieczeństwa systemów komputerowych

Zakres związany z przedmiotowym punktem zaadresowany został w Polityce Głównej.

6.6. Kontrola techniczna

Zakres związany z przedmiotowym punktem zaadresowany został w Polityce Głównej.

Zasady te dotyczę również usługi eDoręczenia.

6.6.1. Nadzorowanie rozwoju systemu

Zakres związany z przedmiotowym punktem zaadresowany został w Polityce Głównej.

6.6.2. Kontrola zarządzania bezpieczeństwem

Zakres związany z przedmiotowym punktem zaadresowany został w Polityce Głównej.

6.6.3. Ocena cyklu życia zabezpieczeń

Zakres związany z przedmiotowym punktem zaadresowany został w Polityce Głównej.

6.7. Zabezpieczenia sieci komputerowej

Zakres związany z przedmiotowym punktem zaadresowany został w Polityce Głównej.

6.8. Znakowanie czasem

Wszystkie przesyłki w ramach usługi eDoręczenia są oznaczone datą i godziną wysłania, odbioru i każdej zmiany przez kwalifikowany elektroniczny znacznik czasu.

Elektroniczny znaczniki czasu tworzone w ramach systemu Certum w wyżej wymienionych celach są zgodnie z ETSI EN 319 422 (patrz rozdz. 1.3.1.2 Polityki Głównej).

7. Profile certyfikatów i zaświadczeń certyfikacyjnych

7.1. Profil Usługi eDoręczenia

Usługa eDoręczenia wystawia elektroniczne dowody podpisywane certyfikatem urzędu Certum QERDS 2023. Dowód zawiera informację, że w określonym momencie czasowym miało miejsce

określone zdarzenie związane z procesem transmisji danych pomiędzy nadawcą a adresatem (np. wysłanie lub odebranie wiadomości).

Identyfikatory usługi umieszczane w poświadczeniach wydawanych przez Certum eDoręczenia:

Nazwa poświadczenia	Identyfikator usługi
Poświadczenie odbioru	1.2.616.1.113527.2.4.1.4.2
Poświadczenie przedłożenia	1.2.616.1.113527.2.4.1.4.4

7.2. Inne profile

7.2.1. Profil tokena elektronicznego znacznika czasu

Zakres związany z przedmiotowym punktem zaadresowany został w Polityce Głównej.

7.2.2. Profil tokena walidacji podpisów elektronicznych i pieczęci elektronicznych

Zakres związany z przedmiotowym punktem zaadresowany został w Polityce Głównej.

7.2.3. Profile tokenów weryfikacji statusu certyfikatów

Zakres związany z przedmiotowym punktem zaadresowany został w Polityce Głównej.

8. Audyt zgodności i inne oceny

Celem audytu jest określenie stopnia zgodności postępowania jednostki usługowej Certum lub wskazanych przez nią elementów z wdrożonym przez Asseco Data Systems S.A. Zintegrowanym Systemem Zarządzania w zakresie Jakości i Bezpieczeństwa Informacji, który obejmuje zwłaszcza wymagania standardów PN-EN ISO 9001 oraz PN-ISO/IEC 27001, oraz deklaracjami i procedurami wewnętrznymi Certum.

Audyty zgodności postępowania Certum z wymaganiami nałożonymi na dostawców usługi eDoręczenia określonych w Rozporządzeniu eIDAS, wymaganiami standardu usługi RDE oraz procedurami i procesami opisanymi w wewnętrznej dokumentacji Certum (z uwzględnieniem weryfikacji zaufanych ról określonych w Certum).

Audyt Certum może być prowadzony przez komórki wewnętrzne Asseco Data Systems S.A. (**audyt wewnętrzny**) oraz przez jednostki organizacyjne niezależne od Asseco Data Systems S.A. (**audyt zewnętrzny**).

8.1. Częstotliwość i okoliczności audytu

Zakres związany z przedmiotowym punktem zaadresowany został w Polityce Głównej.

8.2. Tożsamość/kwalifikacje audytora

Zakres związany z przedmiotowym punktem zaadresowany został w Polityce Głównej.

8.3. Związek audytora z audytowaną jednostką

Zakres związany z przedmiotowym punktem zaadresowany został w Polityce Głównej.

8.4. Zagadnienia obejmowane przez audyt

Zakres związany z przedmiotowym punktem zaadresowany został w Polityce Głównej.

8.5. Podejmowane działania w celu usunięcia rozbieżności wykrytych podczas audytu

Zakres związany z przedmiotowym punktem zaadresowany został w Polityce Głównej.

8.6. Informowanie o wynikach audytu

Publikacji podlega otrzymany certyfikat zgodności usługi eDoręczenia z wymaganiami w serwisie internetowym dostępnym pod adresem www.certum.pl..

9. Inne kwestie biznesowe i prawne

9.1. Opłaty

Za świadczone usługi Certum pobiera opłaty. Wysokości opłat oraz rodzaje usług objętych opłatami są opublikowane w cenniku, dostępnym w repozytorium urzędu certyfikacji Certum w serwisie internetowym pod adresem:

www.certum.pl

9.1.1. Opłaty za inne usługi

Zakres związany z przedmiotowym punktem zaadresowany został w Polityce Głównej pkt. 9.1.4.

9.1.2. Zwrot opłat

Certum dokłada wszelkich starań, aby świadczone usługi były na najwyższym poziomie. W każdym innym przypadku Usługobiorca może żądać zwrotu wniesionej opłaty, jeżeli usługa eDoręczenia była wykonana niezgodnie z zasadami wynikającymi z warunków świadczenia usług zaufania i postanowień niniejszego dokumentu.

Żądania o zwrot opłat należy kierować pod adres podany w rozdz. 1.5.2.

9.2. Odpowiedzialność finansowa

Odpowiedzialność Asseco Data Systems S.A. za pośrednictwem swojej jednostki organizacyjnej, działającej pod nazwą Certum oraz stron powiązanych poprzez usługi świadczone przez tę jednostkę wynika z rutynowych czynności wykonywanych przez te podmioty lub z czynności stron trzecich. Odpowiedzialność każdego z podmiotów jest określona w umowach dwustronnych lub wynika ze złożonych oświadczeń woli.

Certum ponosi odpowiedzialność za zaistnienie sytuacji wymienionych w rozdziale 9.9 niniejszego dokumentu.

Certum odpowiada finansowo wobec usługobiorców usługi eDoręczenia, którzy polegają na jej działalności.

Odpowiedzialność finansowa Certum ma zastosowanie tylko wówczas, jeśli szkody wystąpią z winy Certum lub z winy stron, z którymi Asseco Data Systems S.A. ma tak zawarte umowy, że wina ta przenosi się na Certum.

Certum nie ponosi odpowiedzialności finansowej zdefiniowanej w niniejszym dokumencie wobec innych osób trzecich, nie będących usługobiorcami usługi eDoręczenia.

W przypadku wystąpienia szkody usługobiorca musi zgłosić jej wystąpienie w ciągu 30 dni od jej zajścia. W przypadku zgłoszenie wystąpienia szkody w terminie późniejszym Certum nie ma obowiązku rozpatrzenia danej szkody.

Certum ponosi odpowiedzialność finansową tylko w okresie zabezpieczenia roszczeń zależnym od wykupionego pakietu biznesowego.

W przypadku potwierdzenia przez pracowników Certum wystąpienia szkody, Asseco Data Systems S.A. zobowiązuje się do wypłacenia odszkodowania. Wysokość odszkodowania dla pojedynczego szkody nie może być wyższa niż limit gwarancji finansowej dla pojedynczej szkody. Wielkość wypłaconego odszkodowania nie będzie wyższa niż udowodniona wartość szkody.

Asseco Data Systems S.A. wypłaca odszkodowania wobec zgłoszonych szkód według kolejności zgłoszenia wystąpienia szkody.

9.2.1. Zakres ubezpieczenia

Zakres związany z przedmiotowym punktem zaadresowany został w Polityce Głównej.

9.2.2. Inne aktywa

Zakres związany z przedmiotowym punktem zaadresowany został w Polityce Głównej.

9.2.3. Rozszerzony zakres gwarancji

Zakres związany z przedmiotowym punktem zaadresowany został w Polityce Głównej.

9.3. Poufność informacji biznesowej

Zakres związany z przedmiotowym punktem zaadresowany został w Polityce Głównej.

9.3.1. Zakres poufności informacji

Zakres związany z przedmiotowym punktem zaadresowany został w Polityce Głównej.

9.3.2. Informacje znajdujące się poza zakresem poufności informacji

Zakres związany z przedmiotowym punktem zaadresowany został w Polityce Głównej.

Ponadto wszystkie informacje, które niezbędne są w procesie prawidłowego funkcjonowania usługi eDoręczenia uważane są za informacje jawne.

Dodatkowo wymienione poniżej dokumenty traktowane są jako ogólnie dostępne za pośrednictwem serwisu internetowego Certum dostępnego pod adresem www.certum.pl:

- Regulamin Kwalifikowanej Usługi Zaufania Certum – rejestrowanego doręczenia elektronicznego eDoręczenia,
- Polityka i Kodeks Kwalifikowanej Usługi Certum – rejestrowanego doręczenia elektronicznego eDoręczenia.

9.3.3. Obowiązek ochrony poufności informacji

Zakres związany z przedmiotowym punktem zaadresowany został w Polityce Głównej.

9.4. Prywatność informacji osobowych

9.4.1. Zasady prywatności

Zakres związany z przedmiotowym punktem zaadresowany został w Polityce Głównej.

9.4.2. Informacje uważane za prywatne

Dowolna informacja dotycząca usługobiorcy, która nie jest niezbędna do poprawnego funkcjonowania usługi eDoręczenia.

9.4.3. Informacja nieuważana za prywatną

Wszystkie informacje udostępniane publicznie nie są uważane za informacje prywatne, o ile reguła ta nie narusza wymagań wynikających z *Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016r. sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE*..

9.4.4. Odpowiedzialność za ochronę informacji prywatnej

Zakres związany z przedmiotowym punktem zaadresowany został w Polityce Głównej.

9.4.5. Zastrzeżenia i zezwolenie na użycie informacji prywatnej

Zakres związany z przedmiotowym punktem zaadresowany został w Polityce Głównej.

9.4.6. Udostępnianie informacji zgodnie z nakazem sądowym lub administracyjnym

Zakres związany z przedmiotowym punktem zaadresowany został w Polityce Głównej.

9.4.7. Inne okoliczności ujawniania informacji

Zakres związany z przedmiotowym punktem zaadresowany został w Polityce Głównej.

9.5. Prawo do własności intelektualnej

Zakres związany z przedmiotowym punktem zaadresowany został w Polityce Głównej.

9.5.1. Znak towarowy

Zakres związany z przedmiotowym punktem zaadresowany został w Polityce Głównej.

9.6. Zobowiązania i gwarancje

W rozdziale tym przedstawione są zobowiązania i odpowiedzialność Certum, punktów rejestracji (w tym punktów potwierdzania tożsamości), użytkowników usługi eDoręczenia (usługobiorców i stron ufających). Zobowiązania te oraz odpowiedzialność regulowane są przez wzajemne umowy zawierane pomiędzy stronami.

Przedmiotem umowy zawartej pomiędzy Asseco Data Systems S.A. i usługobiorcą jest kwalifikowana usługa eDoręczenia udostępniana przez Certum, wzajemne zobowiązania oraz odpowiedzialności, w tym finansowe. Szczegółowy opis zawarty jest w Regulamin Kwalifikowanej Usługi Zaufania Certum – rejestrowanego doręczenia elektronicznego eDoręczenia.

9.6.1. Zobowiązania i gwarancje usługi eDoręczenia

Certum świadcząc kwalifikowaną usługę eDoręczenia gwarantuje, że:

- przestrzega i egzekwuje procedury opisane w niniejszym dokumencie,
- stosuje urządzenia i technologie zapewniające niezawodność systemu oraz bezpieczeństwo techniczne i kryptograficzne przy realizacji procesów,
- dostarczenia usługi eDoręczenia po zweryfikowaniu dostarczonych informacji za pomocą środków dozwolonych prawem,
- każda zmiana danych wymagana w celu wysłania lub odbioru danych jest wyraźnie wskazana nadawcy i adresatowi danych
- zapewnia dokładne określenie czasu wysyłania i odebrania przesyłki - usługi elektronicznego znacznika czasu,
- dostępność, integralność i poufność treści użytkownika jest zagwarantowana od momentu wysłania do momentu odbioru,
- chroniona jest integralność treści użytkownika, w szczególności przy wymianie między nadawcą/adresatem,
- dowody nadania wystawiane są po nadaniu przesyłki nie czekając na status zwrotny,
- dowody związane z czynnościami dostarczania treści użytkownika są chronione przez kwalifikowaną pieczęć elektroniczną, która wyklucza możliwość zmiany danych,
- każdemu adresowi do doręczeń elektronicznych przypisana jest jedna skrzynka o gwarantowanej pojemności,
- wielkość pojedynczej przesyłki nie może przekraczać 15 MB,
- usługa pozwala na jednoczesne dołączenie maksymalnie 25 załączników (wliczając w to treść przesyłki),
- przepełnienie pojemności skrzynki usługobiorcy spowoduje brak możliwości wysyłania i odbierania korespondencji do czasu zwolnienia przez usługobiorcę pojemności na skrzynce doręczeń,

- w przypadkach, gdy wymagana jest modyfikacja treści użytkownika, modyfikacje te są wyraźnie wskazane nadawcy, adresatowi i ewentualnym osobom trzecim,
- zapewnia podjęcie natychmiastowych działań w przypadku technicznych problemów bezpieczeństwa,
- zapewnia czas doręczenia zgodny z standardem usługi RDE,
- gwarantuje ochronę danych z wykorzystaniem mechanizmów backupu i replikacji danych co najmniej raz na 24h,
- zapewniony jest ciągły dostęp do serwisów świadczonych usług, w trybie 24/7/365 z wyłączeniem przerw:
    - zaplanowane i wcześniej zapowiedziane napraw technologicznych, związanych z konserwacją sprzętu i systemu;
    - nieplanowanych napraw technologicznych infrastruktury w wyniku nieprzewidzianych awarii;
    - konserwacji spowodowanej awariami infrastruktury poza jurysdykcją Certum;
    - niedostępność usługi w wyniku działania siły wyższej lub zdarzeń nadzwyczajnych.
- zgłoszenie konserwacji lub modernizacji swojej infrastruktury na co najmniej trzy dni przed rozpoczęciem naprawy,
- zapewnia ochronę danych osobowych usługobiorców zgodnie z *Rozporządzeniem Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016r. sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE* oraz dokumentami wykonawczymi do tej ustawy,
- zatrudnia pracowników posiadających wiedzę, kwalifikacje i doświadczenie odpowiednie do pełnienia funkcji związanych z usługą eDoręczenia, w tym w szczególności obejmujących dziedziny:
    - automatycznego przetwarzania danych w sieciach i systemach teleinformatycznych,
    - mechanizmów zabezpieczania sieci i systemów teleinformatycznych,
    - kryptografii, podpisów i pieczęci elektronicznych i infrastruktury klucza publicznego,
    - sprzętu i oprogramowania stosowanego do elektronicznego przetwarzania danych,

Ponadto Certum zobowiązuje się do:

- zachowania w tajemnicy informacji związanych ze świadczoną usługą eDoręczenia, których nieuprawnione ujawnienie mogłoby narazić na szkodę Asseco Data Systems S.A. lub odbiorcę usług zaufania przez okres 10 lat od ustania stosunków prawnych, o których mowa w art. 15 ust. 3 *Ustawy*, oraz do bezterminowego zachowania w tajemnicy danych służących do składania poświadczeń elektronicznych oraz do:
    a. przechowywania przez 20 lat wszystkich informacji dotyczących usługobiorców usługi eDoręczenia zebranych podczas procesu potwierdzania tożsamości,
    b. przechowywania przez 20 lat wszystkich poświadczeń wystawianych przez usługę eDoręczenia,

c. przechowywania przez co najmniej 36 miesięcy (zgodnie z standardem usługi RDE pkt. 5.1.12.9) wszystkie stworzonych przez siebie rejestrów zdarzeń w sposób umożliwiający ich elektroniczne przeglądanie.

Wszystkie zegary funkcjonujące w ramach systemu Certum świadczące kwalifikowane usługi wykorzystywane w trakcie świadczenia usług są synchronizowane z międzynarodowym wzorcem czasu UTC (Coordinated Universal Time), z dokładnością do 1 sekundy.

Certum nie udostępnia usługi eDoręczenia osobom niepełnoletnim (poniżej 18 roku życia), nawet prowadzącym działalność gospodarczą.

9.6.1.1. Zobowiązania repozytorium urzędu certyfikacji

Zakres związany z przedmiotowym punktem zaadresowany został w Polityce Głównej.

9.6.2. Zobowiązania i gwarancje Punktów Rejestracji

Zakres związany z przedmiotowym punktem zaadresowany został w Polityce Głównej.

9.6.3. Zobowiązania i gwarancje usługobiorcy

Poprzez złożenie wniosku o dostęp do usługi eDoręczenia oraz akceptację warunków świadczenia usługi usługobiorca wyraża zgodę na przystąpienie do usługi na zasadach określonych w warunkach świadczenia usługi eDoręczenia, Polityce Głównej, Polityce eDoręczenia oraz Regulamin Kwalifikowanej Usługi Zaufania eDoręczenia.

Usługobiorca zobowiązany jest do:

- przestrzegania warunków świadczonych usługi eDoręczenia świadczonej przez Asseco Data Systems S.A.,
- dostarczenia obsługującemu go punktowi sieci Systemu Rejestracji prawdziwych i poprawnych informacji na każdym etapie współpracy,
- dostarczenia dokumentów potwierdzających prawdziwość danych zawartych we wniosku w celu wypełnienia określonych w Polityce Głównej/Polityce eDoręczenia wymagań procesu rejestracji,
- niezwłocznego poinformowania Certum o jakichkolwiek błędach lub o zmianach danych,
- korzystania z usługi eDoręczenia wyłącznie w celach zgodnych z prawem,
- zobowiązany jest do przesyłania plików wolnych od wirusów i złośliwego oprogramowania.

Usługobiorca ponosi odpowiedzialność za szkody wynikające z przesłania zainfekowanych przesyłek.

Usługobiorca samodzielnie nadzoruje poprawność wpisów w swojej książce adresowej (kontaktach). Wpisy w książce adresowej usługobiorcy nie podlegają nadzorowi Certum. Usługobiorca jest administratorem danych osobowych, które utrzymuje w książce adresowej (kontaktach).

Usługobiorca, czyli właściciel usługi samodzielnie nadzoruje i umożliwia dostęp do usługi innym użytkownikom. Użytkownicy tacy nie podlegają nadzorowi Certum. Usługobiorca jest administratorem danych osobowych innych użytkowników, które utrzymuje w swojej usłudze.

9.6.4. Zobowiązania i gwarancje stron ufających

W zależności od wzajemnych relacji pomiędzy stroną ufającą a Certum lub usługobiorcą, zobowiązania strony ufającej mogą być wyrażone w postaci umowy z Asseco Data Systems S.A. lub usługobiorcą lub mogą mieć charakter akceptacji warunków świadczenia usług zaufania.

Niezależnie od charakteru umowy strona ufająca zobowiązana jest do:

- rzetelnej weryfikacji każdego poświadczenia które do niej dotrze w celu zweryfikowania poświadczenia strona ufająca powinna:
    - sprawdzić, czy wszystkie certyfikaty dostawców usług zaufania wchodzące w skład ścieżki certyfikacji należą do urzędów certyfikacji oraz czy nadano im prawo poświadczania rejestrowanych doręczeń elektronicznych,
    - określić datę oraz czas poświadczenia. Jest to możliwe za pomocą kwalifikowanego elektronicznego znacznika czasu umieszczonego w poświadczeniu.

Jeśli dokument lub podpis elektroniczny jest oznakowany czasem lub w jakikolwiek sposób powiązany z innymi tokenami, poświadczeniami wystawianymi przez Certum, to w celu racjonalnego zbudowania zaufania do weryfikowanego tokena lub poświadczenia strona ufająca powinna dodatkowo:

- zweryfikować, czy token, poświadczenie został prawidłowo poświadczone elektronicznie oraz czy klucz prywatny użyty przez kwalifikowany urząd elektronicznego znacznika czasu Certum QTST 2017, nie był ujawniony aż do momentu weryfikacji tokena, poświadczenia (chyba, że zawarty w nich czas spełnia wymagania daty pewnej); status klucza prywatnego można zweryfikować w oparciu o weryfikację komplementarnego z nim klucza publicznego,
- sprawdzić ograniczenia w stosowaniu usługi w niniejszym dokumencie Polityce eDoręczenia oraz warunkach świadczenia usług zaufania przez Certum.

9.6.5. Zobowiązania i gwarancje innych użytkowników

Niniejsza Polityka eDoręczenia nie określa żadnych wymagań w tym zakresie.

9.7. Wyłączenie odpowiedzialności z tytułu gwarancji

Gwarancje Certum oparte są na ogólnych zasadach zawartych w niniejszej Polityce eDoręczenia oraz są zgodne z obowiązującymi aktualnie na terenie Rzeczypospolitej Polskiej nadrzędnymi aktami prawnymi. Wyłączenia odpowiedzialności z tytułu gwarancji Certum umieszczane są w warunkach świadczenia usług zaufania przez Certum.

9.8. Ograniczenia odpowiedzialności

Certum, działając w ramach umocowań Asseco Data Systems S.A., ponosi odpowiedzialność za skutki działań usługi eDoręczenia, Głównego Punktu Rejestracji i innych punktów systemu rejestracji oraz osób potwierdzających tożsamość w zakresie określonym w warunkach świadczenia usługi eDoręczenia.

Działalność Certum wspomagana jest przez inne działy Asseco Data Systems S.A na zasadzie wyspecjalizowanego outsourcingu wewnętrznego.

Przedstawione poniżej zapisy o odpowiedzialności stron nie eliminują lub nie zastępują odpowiedzialności wynikającej z odrębnych przepisów prawa.

9.8.1. Odpowiedzialność Certum

9.8.1.1. Odpowiedzialność usługi eDoręczenia

Usługa eDoręczenia ponosi odpowiedzialność w przypadkach, gdy bezpośrednie i pośrednie szkody poniesione przez użytkownika:

- powstały pomimo przestrzegania przez nich zasad określonych w Polityce eDoręczenia oraz Polityce Głównej,
- są wynikiem udowodnionych błędów popełnionych przez usługę eDoręczenia,
- powstały wskutek naruszenia innych gwarancji, określonych w 9.6.1.

Certum zleca podmiotom zewnętrznym usługi świadczone w ramach prowadzenia tzw. Punkty Potwierdzania Tożsamości. Mimo, że punkt rejestracji związany jest z Asseco Data Systems S.A. umową, to pełną odpowiedzialność za tę część jego pracy, która związana jest ze świadczeniem przez Certum usług zaufania, ponosi Certum.

Certum nie ponosi odpowiedzialności za nie działanie lub nierzetelne działanie serwisów po stronie Partnera.

Certum nie zleca podmiotom zewnętrznym żadnych innych usług poza usługami rejestracji.

Certum nie ponosi odpowiedzialności za niedostępność usługi z powodu braku dostępności bazy BAE oraz OW – operatora wyznaczonego.

Jednocześnie Certum nie ponosi odpowiedzialności za działania stron trzecich, usługobiorców oraz innych stron nie związanych z Certum. W szczególności nie odpowiada:

- za szkody powstałe na skutek działania siły wyższej lub innych, za których wystąpienie nie ponosi odpowiedzialności, tj.: pożaru, powodzi, wichury, wojny, aktów terroru, epidemii oraz innych klęsk naturalnych lub spowodowanych przez człowieka,
- za szkody powstałe na skutek instalacji, użytkowania oraz zarządzania aplikacjami innymi niż dostarczone przez Certum,
- w przypadku podania przez usługobiorcę fałszywych danych i – mimo zachowania przez Certum należytej staranności – umieszczenie ich na jego wniosek zarówno w bazach Certum, jak też w usłudze eDoręczenia.

9.8.1.2. Odpowiedzialność repozytorium urzędu certyfikacji

Zakres związany z przedmiotowym punktem zaadresowany został w Polityce Głównej.

9.8.1.3. Odpowiedzialność usługobiorcy

Odpowiedzialność usługobiorcy wynika ze zobowiązań i ograniczeń określonych w rozdz. 9.6.3 niniejszego dokumentu.

9.8.1.4. Odpowiedzialność strony ufającej

Odpowiedzialność strony ufającej wynika ze zobowiązań i gwarancji określonych w rozdz. 9.6.4. Warunki tej odpowiedzialności może również regulować umowa zawarta z usługobiorcą oraz z Asseco Data Systems S.A lub akceptacja warunków świadczenia usługi eDoręczenia.

9.9. Odszkodowania

9.9.1. Odszkodowanie z tytułu odpowiedzialności cywilnej usługobiorcy

Odszkodowanie z tytułu odpowiedzialności cywilnej usługobiorcy wynika ze zobowiązań i gwarancji określonych w rozdz. 9.6.3 niniejszego dokumentu.

9.9.2. Odszkodowanie z tytułu odpowiedzialności cywilnej strony ufającej

Odszkodowanie z tytułu odpowiedzialności cywilnej strony ufającej wynika ze zobowiązań i gwarancji określonych w rozdz. 9.6.4 niniejszego dokumentu.

9.10. Okres obowiązywania Polityki i Kodeksu Kwalifikowanej usługi eDoręczenia oraz jego ważność

9.10.1. Okres obowiązywania

Niniejsza Polityka i Kodeks Kwalifikowanej usługi eDoręczenia obowiązuje od momentu nadania jej statusu aktualny i opublikowania jej w repozytorium Certum do momentu opublikowanie kolejnej aktualnej wersji.

9.10.2. Wygaśnięcie ważności

Niniejszy dokument obowiązuje do momentu zastąpienia go nową wersją. Data rozpoczęcia ważności nowej wersji Polityka i Kodeks Kwalifikowanej usługi eDoręczenia jest jednocześnie datą zakończenia ważności niniejszej Polityki.

9.10.3. Skutki wygaśnięcia ważności Polityki i Kodeksu Kwalifikowanej usługi eDoręczenia i okres przejściowy

Po wygaśnięciu ważności poprzedniej wersji dokumentu użytkownicy usługi eDoręczenia są obowiązani do stosowania się do zapisów niniejszego dokumentu aż do momentu zakończenia jego obowiązywania.

9.11. Indywidualne powiadamianie i komunikowanie się z użytkownikami

Zakres związany z przedmiotowym punktem zaadresowany został w Polityce Głównej.

9.12. Procedura wprowadzania zmian

Zakres związany z przedmiotowym punktem zaadresowany został w Polityce Głównej.

9.12.1. Procedura wnoszenia poprawek

Zakres związany z przedmiotowym punktem zaadresowany został w Polityce Głównej.

9.12.1.1. Zmiany nie wymagające informowania

Zakres związany z przedmiotowym punktem zaadresowany został w Polityce Głównej.

9.12.2. Mechanizm powiadamiania oraz okres oczekiwania na komentarze

Zakres związany z przedmiotowym punktem zaadresowany został w Polityce Głównej.

9.12.2.1. Okres oczekiwania na komentarze

Zakres związany z przedmiotowym punktem zaadresowany został w Polityce Głównej.

9.12.3. Okoliczności wymagające zdefiniowania nowego identyfikatora polityki

Zakres związany z przedmiotowym punktem zaadresowany został w Polityce Głównej.

9.12.4. Dystrybucja nowej wersji Polityki i Kodeksu Kwalifikowanej usługi eDoręczenia oraz Regulaminu Kwalifikowanej Usługi Zaufania eDoręczenia

Zakres związany z przedmiotowym punktem zaadresowany został w Polityce Głównej.

Dotyczy również usługi eDoręczenia.

9.12.5. Elementy nie publikowane w Polityce i Kodeksie Kwalifikowanej usługi eDoręczenia

Zakres związany z przedmiotowym punktem zaadresowany został w Polityce Głównej.

Dotyczy również usługi eDoręczenia.

9.13. Warunki rozstrzygania sporów, reklamacje

Przedmiotem rozstrzygania sporów, w tym reklamacji, mogą być jedynie rozbieżności bądź konflikty powstałe pomiędzy stronami w zakresie usługi eDoręczenia w oparciu o regulacje Polityki eDoręczenia, Polityki Głównej oraz zawartych umów.

Spory, reklamacje bądź zażalenia powstałe na tle użytkowania usługi, będą rozstrzygane na podstawie pisemnych informacji w drodze mediacji. Skargi należy kierować w formie pisemnej na adres:

Asseco Data Systems S.A.

ul. Królowej Korony Polskiej 21

70-486 Szczecin

Spory związane z usługą eDoręczenia będą w pierwszej kolejności rozstrzygane na drodze postępowania pojednawczego.

Skargi podlegają pisemnemu rozpatrzeniu w terminie 21 dni od dnia ich doręczenia na wskazany wyżej adres. W przypadku braku rozstrzygnięcia sporu w terminie 45 dni od rozpoczęcia postępowania pojednawczego, stronom przysługuje prawo do wystąpienia na drogę sądową. Sądem właściwym do rozpoznania sprawy będzie Sąd Powszechny miejscowo właściwy dla pozwanego.

W przypadku wystąpienia innych sporów będących konsekwencją użycia usługi świadczonej przez Certum, usługobiorca zobowiązuje się pisemnie poinformować Certum o przedmiocie powstałego sporu.

9.14. Prawa właściwe

9.14.1. Ciągłość postanowień

Zakres związany z przedmiotowym punktem zaadresowany został w Polityce Głównej.

Dotyczy również usługi eDoręczenia.

9.14.2. Łączenie postanowień

Zakres związany z przedmiotowym punktem zaadresowany został w Polityce Głównej.

Dotyczy również usługi eDoręczenia.

9.15. Zgodność z obowiązującym prawem

Funkcjonowanie Certum oparte jest na zasadach zawartych w niniejszej Polityce eDoręczenia Polityce Głównej oraz obowiązujących na terytorium Polski przepisach prawa.

9.16. Przepisy różne

Niniejsza Polityka eDoręczenia oraz Polityka Główna nie określają żadnych wymagań w tym zakresie.

9.16.1. Kompletność warunków umowy

Niniejsza Polityka eDoręczenia oraz Polityka Główna nie określają żadnych wymagań w tym zakresie.

9.16.2. Cesja praw

Niniejsza Polityka eDoręczenia oraz Polityka Główna nie określają żadnych wymagań w tym zakresie.

9.16.3. Rozłączność postanowień

Zakres związany z przedmiotowym punktem zaadresowany został w Polityce Głównej.

9.16.4. Klauzula wykonalności

Zakres związany z przedmiotowym punktem zaadresowany został w Polityce Głównej.

9.16.5. Siła wyższa

Zakres związany z przedmiotowym punktem zaadresowany został w Polityce Głównej.

9.17. Postanowienia dodatkowe

Niniejsza Polityka eDoręczenia oraz Polityka Główna nie określają żadnych wymagań w tym zakresie.

Historia dokumentu

Historia zmian dokumentu		
1.0	15 listopada 2022	Opracowanie dokumentu.
1.1	26 luty 2024	Dodanie informacji na temat częstotliwości tworzenia kopii zapasowych, maksymalnej ilości załączników oraz możliwości potwierdzenia tożsamości na podstawie mDowodu i polskiej karty pobytu.

Dodatek 1: Słownik pojęć

Adres do doręczeń elektronicznych (ADE) - adres elektroniczny, o którym mowa w art. 2 pkt 1 ustawy z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną, podmiotu korzystającego z publicznej usługi rejestrowanego doręczenia elektronicznego lub publicznej usługi hybrydowej albo z kwalifikowanej usługi rejestrowanego doręczenia elektronicznego, umożliwiający jednoznaczną identyfikację nadawcy lub adresata danych przesyłanych w ramach tych usług. Adres do doręczeń elektronicznych tworzony przez ministra właściwego do spraw informatyzacji, w sposób zapewniający jego unikalność oraz jednoznaczne przypisanie do podmiotu publicznego, podmiotu niepublicznego, w tym osoby fizycznej.

Adresat – podmiot określony przez nadawcę jako odbiorca przesyłki.

API (Application Programming Interface) – interfejs programowania aplikacji, czyli określony zestaw reguł, umożliwiający dostęp do usługi.

Certum – jednostka organizacyjna firmy Asseco Data Systems S.A. wpisanej do rejestru kwalifikowanych dostawców usług zaufania prowadzonego w imieniu ministra właściwego ds. informatyzacji przez Narodowy Bank Polski. Rejestr ten jest publikowany pod adresem internetowym: www.nccert.pl.

BAE – baza adresów elektronicznych, będąca rejestrem publicznym, w którym gromadzone są adresy do doręczeń elektronicznych, prowadzonym przez ministra właściwego do spraw informatyzacji.

Dane identyfikacyjne – dane jednoznacznie identyfikujące Usługobiorcę, których prawdziwość można potwierdzić na podstawie dokumentu tożsamości Usługobiorcy.

Nadawca - osoba fizyczna lub prawna dostarczająca treści przesyłki.

Polityka certyfikacji – „Polityka i Kodeks Kwalifikowanej Usługi Zaufania Certum – rejestrowanego doręczenia elektronicznego eDoręczenia" to zestaw reguł określających w szczególności zasady świadczenia usługi zaufania, odpowiedzialność stron, dostępny w formie elektronicznej na stronie www.certum.pl.

Punkt systemu rejestracji - jest to punkt - Punkt Potwierdzania Tożsamości (PPT) i Punkt Rejestracji (PR) – jego funkcją jest potwierdzanie tożsamości usługobiorców i akceptacja warunków świadczenia usług zaufania w procesie wnioskowania o dostęp do wybranej usługi.

Rozporządzenie UE 910/2014 (eIDAS) – 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. Rozporządzenie stanowi akt prawny w całości obowiązujący w systemie prawnym Polski oraz we wszystkich państwach Unii Europejskiej.

Rozporządzenie w sprawie sporządzania i doręczania dokumentów elektronicznych oraz udostępniania formularzy, wzorów i kopii dokumentów elektronicznych – z dnia 5 stycznia 2018 r. (Dz.U. 2018 poz. 180).

Rozporządzenie w sprawie gwarantowanych dostępności i pojemności skrzynek doręczeń dla podmiotów publicznych i niepublicznych korzystających z publicznej usługi rejestrowanego doręczenia elektronicznego - z dnia 24 czerwca 2021 r. (Dz.U. 2021 poz. 1202)

Skrzynka doręczeń – narzędzie umożliwiające wysyłanie, odbieranie i przechowywanie danych w ramach usługi eDoręczenia.

Usługa eDoręczenia - kwalifikowanego rejestrowanego doręczenia elektronicznego – świadczone przez urząd Certum QERDS 2023. Oznacza usługę umożliwiającą przesłanie danych między stronami trzecimi drogą elektroniczną i zapewniającą dowody związane z posługiwaniem się przesyłanymi danymi, w tym dowód wysłania i otrzymania danych,

oraz chroniącą przesyłane dane przed ryzykiem utraty, kradzieży, uszkodzenia lub jakiejkolwiek nieupoważnionej zmiany.

Usługobiorca – osoba fizyczna wnioskująca o dostęp do usługi i dla której dostęp został udzielony.

Ustawa o usługach zaufania oraz identyfikacji elektronicznej – Ustawa z dnia 5 września 2016 r. o usługach zaufania oraz identyfikacji elektronicznej (Dz.U. z 2021 r. poz. 1797, z późn. zm.).

Ustawa o doręczeniach elektronicznych - z dnia 18 listopada 2020 r. o doręczeniach elektronicznych (Dz.U. 2020 poz. 2320).