Polityka oraz deklaracja postępowania dla Kwalifikowanej Usługi Zaufania Rejestrowanych Doręczeń Elektronicznych

Numer dokumentu	TSP – 002
Identyfikator dokumentu	OID: [1.2.616.1.113813.1.4.1.1.2]
Klasyfikacja dokumentu	publiczne
Właściciel dokumentu	Autenti S.A. (“Autenti”) ul. Święty Marcin 29/8, 61-806 Poznań KRS: 0001254852, nr NIP: 7831693251, REGON: 302246285
Wersja	Wersja nr 1.2

Spis treści

I. Postanowienia ogólne ... 4
1. Wprowadzenie ... 4
2. Wstęp do usługi ... 4
3. Regulacje prawne oraz zgodność z normami ... 5
4. Definicje ... 7
5. Definicje Stron Usługi QDS: ... 9
II. Zarządzanie Polityką i Repozytorium ... 9
1. Zarządzanie Polityką: ... 9
2. Repozytorium i publikacja: ... 10
III. Identyfikacja i uwierzytelnienie ... 11
1. Wstęp ... 11
2. Zasady ustalenia tożsamości osób fizycznych ... 11
3. Zasady ustalenia tożsamości osoby fizycznej uprawnionej do reprezentacji oraz potwierdzenie danych osoby prawnej lub innych jednostek organizacyjnych ... 13
4. Zasady ustalania tożsamości innych osób uprawnionych do reprezentacji osoby prawnej lub innej jednostki organizacyjnej ... 15
5. Uwierzytelnienie ... 16
6. Zasady przetwarzania Danych identyfikujących osobę ... 17
IV. Dowody z Usługi QDS ... 17
1. Dowody powiązane z Nadawcą ... 18
2. Dowody odnoszące się do Odbiorcy ... 19
3. Dowody dotyczące czynności wykonywanych przez Dostawcę Usługi ... 19
4. Dowody związane z doręczeniem e-Przesyłki ... 20
5. Dowody związane z akceptacją lub odmową akceptacji e-Przesyłki przez Odbiorcę dla usługi doręczenia przewidującej taką możliwość ... 21
6. Dowody przewidziane dla realizacji Usługi QDS ze Standardem RDE ... 22
V. Zakres Usługi QDS ... 23
1. Zakres ... 23
2. Opis świadczenia Usługi QDS ... 23
3. Szczegółowy opis przebiegu Usługi QDS ... 25
VI. Bezpieczeństwo informacji ... 27
1. Zabezpieczenia fizyczne ... 27
2. Dostęp fizyczny ... 28
3. Dostęp do systemów informatycznych ... 28
4. Zarządzanie incydentami ... 29
5. Personel Dostawcy Usługi ... 31

6. Zarządzanie dostawcami....31
7. Zarządzanie aktywami....32
8. Zarządzanie ryzykiem....32
9. Zarządzanie zmianą....33
10. Monitorowanie....33
11. Bezpieczeństwo transmisji oraz sieci....34
12. Audyty oraz przeglądu zarządzania bezpieczeństwem informacji....34
13. Kopie zapasowe....35
14. Ciągłość działania....35
15. Klucze kryptograficzne niezbędne do świadczenia Usługi QDS....36
16. Rejestracja zdarzeń....37
VII. Archiwizacja istotnych zdarzeń....38
VIII. Inne postanowienia....40
1. Opłaty....40
2. Niedyskryminujące zastosowanie....40
3. Odpowiedzialność finansowa....40
4. Poufność informacji....40
5. Źródło czasu....41
6. Ochrona danych osobowych....41
7. Zobowiązania i gwarancje....42
a. Zobowiązania i gwarancje Dostawcy Usługi:....42
8. Zobowiązania Użytkowników:....43
10. Ograniczenie odpowiedzialności....44
11. Odszkodowania....46
12. Dostawcy usług zaufania zaangażowani w świadczenie Usługi QDS....46
IX. Warunki rozstrzygania sporów, reklamacje, wątpliwości....46
X. Zakończenie działalności lub zaprzestanie świadczenia Usługi QDS....47
XI. Obowiązywanie i procedura wprowadzania zmian....49
HISTORIA ZMIAN....51

I. Postanowienia ogólne

1. Wprowadzenie

Niniejsza Polityka oraz deklaracja postępowania określa ogólne zasady świadczenia przez Autenti S.A. kwalifikowanej usługi zaufania rejestrowanego doręczenia elektronicznego (ang. Qualified Registered Electronic Delivery Service) w rozumieniu Rozporządzenia Parlamentu Europejskiego i Rady (UE) NR 910/2014 z dnia 23 lipca 2014 r. w sprawie identyfikacji elektronicznej i usług zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznym oraz uchylające dyrektywę 1999/93/WE, a także deklarację praktyk Autenti S.A. w tym zakresie.

2. Wstęp do usługi

Kwalifikowana usługa zaufania rejestrowanego doręczenia elektronicznego jest udostępniana przez Autenti w ramach ekosystemu usług zaufania i identyfikacji elektronicznej dostępnych za pośrednictwem Platformy Autenti. Z usługi można korzystać na warunkach opisanych w Regulaminie Platformy Autenti i Regulaminie eDelivery Autenti, dostępnych na stronie internetowej Autenti.

Kwalifikowana usługa zaufania rejestrowanego doręczenia elektronicznego umożliwia wysyłanie i/lub odbieranie treści oraz bezpieczne i długoterminowe przechowywanie dowodów z realizacji tych procesów.

Przepisy ustanowione przez Unię Europejską opisują ramy prawne i operacyjne dla dostawców kwalifikowanej usługi rejestrowanego doręczenia, których przestrzeganie pozwala dostawcy uzyskać status "Kwalifikowanego dostawcy usług rejestrowanego doręczenia elektronicznego", a jego usługę uznać za "Kwalifikowaną usługę rejestrowanego doręczenia elektronicznego". Kwalifikowane usługi elektronicznego rejestrowanego doręczenia korzystają z domniemań opisanych w art. 43 rozporządzenia eIDAS, a zatem nie wymagają dalszych dowodów, aby wywoływać skutki prawne zwykle zarezerwowane dla nieelektronicznych przesyłek poleconych.

Kwalifikowana usługa elektronicznego rejestrowanego doręczenia zapewnia bezpieczeństwo i ochronę komunikacji, poświadczenie czasu wysłania Zawartości przesyłki od Nadawcy oraz poświadczenie czasu postawienia e-Przesyłki do dyspozycji Odbiorcy, a także dowody z komunikacji. Ponadto, kwalifikowana usługa rejestrowanego doręczenia zapewnia Identyfikację Odbiorcy i Nadawcy oraz ich powiązanie z treścią e-Przesyłki.

Dostawca Usługi uczestniczy w realizacji usługi publicznych doręczeń elektronicznych, określonych w Standardzie RDE, we współpracy z Operatorem Wyznaczonym na potrzeby wymiany rejestrowanych wiadomości elektronicznych pomiędzy Użytkownikami Dostawcy Usługi, a instytucjami państwowymi (publicznymi), których Adresy do doręczeń elektronicznych będą utrzymywane przez Operatora Wyznaczonego.

Usługa przeznaczona jest dla osób fizycznych oraz prawnych, w tym do komunikacji z organami administracji publicznej. Usługa QDS, w zakresie w jakim jest to możliwe, dostosowana jest również dla osób z niepełnosprawnościami.

3. Regulacje prawne oraz zgodność z normami

[Prawo powszechnie obowiązujące] Dostawca Usługi świadczy Usługę QDS w oparciu o przepisy prawa Unii Europejskiej, w szczególności:

a. 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, (łącznie z przepisami wykonawczymi), zwanym dalej "**eIDAS**",

b. Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE, (łącznie z przepisami wykonawczymi), zwanym dalej "**RODO**".

W zakresie w jakim Usługa QDS jest świadczona na terenie lub w oparciu o przepisy prawa Rzeczypospolitej Polskiej, zastosowanie mają również, w szczególności:

a. Ustawa o doręczeniach elektronicznych z dnia 18 listopada 2020 r.; (łącznie z przepisami wykonawczymi, jeżeli mają zastosowanie),

b. Ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych, (łącznie z przepisami wykonawczymi),

c. Ustawa z dnia 5 września 2016 r. o usługach zaufania oraz identyfikacji elektronicznej (łącznie z przepisami wykonawczymi),

d. Ustawa z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną (łącznie z przepisami wykonawczymi).

[Wzorce umowne] Dostawca Usługi świadczy Usługę QDS zgodnie niniejszą Polityką oraz w oparciu wzorce umowne (regulaminy) udostępniane przez Dostawcę Usługi, w tym:

a. Regulamin Autenti eDelivery,
b. Regulamin Platformy Autenti,
c. Politykę Ochrony Prywatności,
d. Politykę Cookies,

których każdorazowo aktualna treść jest udostępniona pod adresem https://autenti.com/regulaminy/

[Normy] Dostawca Usługi świadczy Usługę QDS w zgodności z takimi normami jak:

a. ETSI EN 319 401 Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers - która definiuje ogólne wymagania dla dostawców usług zaufania,
b. ETSI EN 319 521 Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Electronic Registered Delivery Service Providers - która definiuje zasady i wymagania bezpieczeństwa dla dostawców usługi rejestrowanego doręczenia elektronicznego,
c. ETSI EN 319 522-1 Electronic Signatures and Infrastructures (ESI); Electronic Registered Delivery Services Part 1: Framework and Architecture,
d. ETSI EN 319 522-2 Electronic Signatures and Infrastructures (ESI); Electronic Registered Delivery Services Part 2 Semantic Contents,
e. ETSI EN 319 522-3 Electronic Signatures and Infrastructures (ESI); Electronic Registered Delivery Services Part 3: Formats,
f. ETSI EN 319 522-4-1 Electronic Signatures and Infrastructures (ESI); Electronic Registered Delivery Services Part 4-1: Message delivery bindings,
g. ETSI EN 319 522-4-2 Electronic Signatures and Infrastructures (ESI); Electronic Registered Delivery Services Part 4-2: Evidence and identification bindings,
h. 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 - Wersja: 1.4 (12.01.2024) określonym i udostępniony w Biuletynie Informacji Publicznej przez ministra właściwego do spraw informatyzacji, o ile Usługa QDS służy do realizacji doręczeń w ramach usługi publicznej.

4. Definicje

Polityka posługuje się pojęciami, którym nadaje się następujące znaczenie:

a. **Adres do doręczeń elektronicznych -** adres elektroniczny Nadawcy lub Odbiorcy korzystającego z usługi rejestrowanego doręczenia elektronicznego, będący identyfikatorem jednoznacznie przypisanym Nadawcy lub Odbiorcy e-Przesyłek, umożliwiającym porozumiewanie się za pomocą środków komunikacji elektronicznej.

b. **BAE (Baza Adresów Elektronicznych)** - rejestr publiczny prowadzony przez ministra właściwego do spraw informatyzacji przeznaczony do ujawniania adresów do doręczeń elektronicznych podmiotu korzystającego z publicznej usługi rejestrowanego doręczenia elektronicznego oraz adresu do doręczeń elektronicznych podmiotu niepublicznego korzystającego z kwalifikowanej usługi rejestrowanego doręczenia elektronicznego. Ujawnieniu w BAE podlegają adresy do doręczeń elektronicznych według definicji w Ustawie o doręczeniach elektronicznych z dnia 18 listopada 2020 r. (ADE).

c. **Dostawca Usługi** - Autenti Spółka Akcyjna, świadcząca kwalifikowaną usługę zaufania doręczenia elektronicznego zgodnie z Polityką oraz Regulaminem Autenti eDelivery.

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

e. **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.

f. **e-Przesyłka** - Zawartość przesyłki oraz jej metadane, w tym dane określające Nadawcę i Odbiorcę, przekazana celem jej doręczenia w ramach Usługi QDS.

g. **HSM (ang. *Hardware Security Module*)** - sprzętowy moduł bezpieczeństwa, stanowiący w pełni zabezpieczone urządzenie do przechowywania i zarządzania kluczami kryptograficznymi, do krytycznej autoryzacji i przetwarzania kryptograficznego.

h. **Identyfikacja -** proces używania danych w postaci elektronicznej identyfikujących osobę fizyczną lub osobę prawną, lub osobę fizyczną

reprezentującą osobę prawnę, w celu ustalenia jej tożsamości na potrzeby skorzystania z Usługi QDS.

i. **Operator Wyznaczony -** operator wyznaczony, o którym mowa w art. 3 pkt. 13 Ustawy z dnia 23 listopada 2012 r. Prawo pocztowe.

j. **Pieczęć Elektroniczna** – kwalifikowana lub zaawansowana pieczęć elektroniczna weryfikowana kwalifikowanym certyfikatem, złożona w imieniu Dostawcy Usługi.

k. **Platforma Autenti** – platforma technologiczna, dostępna drogą elektroniczną zgodnie z Regulaminem Platformy Autenti, za pośrednictwem której możliwe jest korzystanie z Usługi QDS.

l. **Polityka** - niniejsza Polityka Świadczenia Usługi QDS.

m. **Polityka Weryfikacji Tożsamości** - dokument Dostawcy Usług opisujący w sposób szczegółowy proces weryfikacji tożsamości dla Usługi QDS.

n. **Regulamin Autenti eDelivery -** regulamin świadczenia usług drogą elektroniczną, regulujący korzystanie z Usługi QDS, którego treść dostępna jest na stronie internetowej Dostawcy Usług.

o. **Regulamin Platformy Autenti** – regulamin świadczenia usług drogą elektroniczną, regulujący korzystanie z Platformy Autenti, którego treść dostępna jest na stronie internetowej pod adresem https://autenti.com/regulamin/.

p. **Usługa Nadawcy** - usługa realizująca odebranie Zawartości przesyłki od Nadawcy, określenie przez Nadawcę danych Odbiorcy oraz wskazanie parametrów usługi (w zakresie udostępnionym do decyzji Nadawcy), odpowiedzialna za przekazanie Zawartości przesyłki Usłudze Odbiorcy, oraz umożliwienie Nadawcy dostępu do dowodów z realizacji usługi, zarówno wytworzonych przez Usługę Nadawcy jak i otrzymanych od Usługi Odbiorcy.

q. **Usługa Odbiorcy -** usługa realizująca doręczenie Zawartości przesyłki. Doręczenie Zawartości przesyłki może być realizowane bezpośrednio przez Dostawcę Usługi lub innego dostawcę kwalifikowanej usługi rejestrowanego doręczenia elektronicznego.

r. **Usługa QDS (ang. *Qualified Delivery Service*) -** kwalifikowana usługa rejestrowanego doręczenia elektronicznego w rozumieniu art. 3 pkt. 37) i art. 44 eIDAS, świadczona przez Autenti za pośrednictwem Platformy Autenti.

s. **Uwierzytelnienie** - proces potwierdzenia że dany podmiot jest osobą, za którą się podaje, przy użyciu danych posiadanych przez Dostawcę Usługi.

t. **Wstępna weryfikacja tożsamości** - Identyfikacja Odbiorcy lub Nadawcy wykonana przed udostępnieniem Usługi QDS, wykonana celem przydzielenia Użytkownikowi środków uwierzytelniających lub powiązania wydanych wcześniej środków uwierzytelniających z daną tożsamością, lub też celem umożliwienia jednorazowego wykorzystania Usługi QDS.

u. **Znacznik czasu -** kwalifikowany elektroniczny znacznik czasu, wykorzystywany przez Dostawcę Usługi**.**

v. **Zawartość przesyłki (ang. *"User Content")*** - źródłowe dane pochodzące lub utworzone przez Nadawcę, które mają zostać przekazane Odbiorcy.

5. Definicje Stron Usługi QDS:

a. **Dostawca Usługi** - Autenti Spółka Akcyjna z siedzibą w Poznaniu, przy ul. Święty Marcin 29/8, wpisana do rejestru przedsiębiorców przez Sąd Rejonowy Poznań Nowe Miasto i Wilda w Poznaniu, VIII Wydział Gospodarczy pod numerem KRS: 0001254852, posiadającą NIP: 7831693251.

b. **Użytkownik** - osoba fizyczna (działająca w imieniu własnym albo jako reprezentant osoby prawnej lub jednostki organizacyjnej nieposiadającej osobowości prawnej), osoba prawna lub jednostka organizacyjna nieposiadająca osobowości prawnej (dalej również jako "Inna jednostka organizacyjna"), która zawarła z Dostawcą Usługi umowę na świadczenie Usługi QDS. Użytkownik może występować w roli Nadawcy lub Odbiorcy w związku z korzystaniem z Usługi QDS.

c. **Nadawca** - osoba fizyczna (działająca w imieniu własnym albo jako reprezentant osoby prawnej lub jednostki organizacyjnej nieposiadającej osobowości prawnej), osoba prawna lub jednostka organizacyjna nieposiadająca osobowości prawnej, która przekazuje Zawartość przesyłki celem jej doręczenia do Odbiorcy, korzystając z Usługi QDS.

d. **Odbiorca** – osoba fizyczna, osoba prawna lub jednostka organizacyjna nieposiadająca osobowości prawnej, której dane zostały wskazane przez Nadawcę w celu odbioru e-Przesyłki.

e. **Strona ufająca** - osoba fizyczna, osoba prawna, jednostka organizacyjna nieposiadająca osobowości prawnej lub inny podmiot, w tym organ państwowy, który polega na dowodach dostarczonych przez Dostawcę Usługi w związku ze świadczeniem Usługi QDS.

II. Zarządzanie Polityką i Repozytorium

1. **Zarządzanie Polityką:**
    a. Polityka jest dokumentem publicznym.
    b. W metryce Polityki na pierwszej stronie wskazywana jest aktualna wersja oraz numer OID. W metryce na ostatniej stronie Polityki wskazana jest data przyjęcia właściwej wersji dokumentu przez właściwe organy Dostawcy Usługi.
    c. Dostawca Usługi jest odpowiedzialny za zarządzanie Polityką. Za zarządzanie Polityką u Dostawcy Usługi, w tym ocenę jej aktualności, odpowiedzialny jest Information Security Compliance Officer.
    d. Każda wersja Polityki obowiązuje po jej zatwierdzeniu w sposób określony przez Dostawcę Usługi, zgodnie z postanowieniami Rozdziału XI ust 2 Polityki.
    e. Każda zmiana Polityki jest zatwierdzana przez Zarząd Dostawcy Usługi.
    f. Użytkownicy są zobowiązani do przestrzegania wersji Polityki, która jest obowiązująca w momencie rozpoczęcia świadczenia Usługi QDS.
    g. Dostawca Usługi dokonuje cyklicznych przeglądów praktyk, które obejmują obowiązki w zakresie utrzymania deklaracji postępowania wskazanych w Polityce, zgodnie z przyjętymi procedurami wewnętrznymi Dostawcy Usługi, związanymi z procesem zarzadzania zgodnością.

2. **Repozytorium i publikacja:**

    a. Dostawca Usługi udostępnia treść Polityki, Regulaminu Autenti eDelivery oraz inne dokumenty niezbędne do wykazania zgodności z Polityką w repozytorium. Repozytorium zawiera informacje o:
        - aktualnej i obowiązującej wersji Polityki,
        - historycznych wersjach Polityki,
    b. Wszystkie informacje umieszczone w repozytorium są ogólnie dostępne za pośrednictwem strony internetowej w domenie Dostawcy Usługi pod adresem www.autenti.com/regulaminy. Repozytorium jest stale dostępne dla wszystkich Użytkowników oraz Stron Ufających z wyjątkiem zdarzeń lub sytuacji, które pozostają poza kontrolą Dostawcy Usługi.
    c. Treść Polityki oraz innych opublikowanych dokumentów w ramach repozytorium, pozwalających na wykazanie zgodności z Polityką jest zabezpieczona przez Dostawcę Usługi w taki sposób, aby zapobiegać nieautoryzowanym zmianom.

d. Wszelkie zmiany Polityki są publikowane w repozytorium niezwłocznie po ich zaakceptowaniu przez Zarząd Dostawcy Uslugi.
e. Użytkownicy są powiadamiani o zmianach drogą elektroniczną z odpowiednim wyprzedzeniem, z tym że powiadomienie następuję na co najmniej 7 dni przed jej wejściem w życie.
f. Informowanie właściwego organu nadzoru odbywa się zgodnie z przyjętą u Dostawcy Usługi procedurą informowania organu nadzoru.
g. Użytkownicy są informowani o treści Polityki oraz Regulaminu Autenti eDelivery przed rozpoczęciem korzystania z Usługi QDS.

III. Identyfikacja i uwierzytelnienie

1. Wstęp

a. Zgodnie z wymogami art. 44 eIDAS, dostawca kwalifikowanej usługi rejestrowanego doręczenia elektronicznego zobowiązany jest do zapewnienia identyfikacji Nadawcy przed udostępnieniem Usługi QDS oraz zapewnienia identyfikacji Odbiorcy przed doręczeniem e-Przesyłki. W związku z tym, Dostawca Usługi wdrożył odpowiednie procedury oraz mechanizmy pozwalające na potwierdzenie tożsamości Użytkowników.
b. Identyfikacja jest obowiązkowa na etapie rejestracji Użytkownika do Usługi QDS oraz na żądanie Dostawcy Usługi.
c. Dostawca Usługi weryfikuje tożsamość Nadawcy i Odbiorcy bezpośrednio lub za pośrednictwem strony trzeciej, zgodnie z przyjętą przez Dostawcę Usługi Polityką Weryfikacji Tożsamości.
d. Polityka Weryfikacji Tożsamości opisuje w sposób szczegółowy sposób zbierania oraz oceny dowodów z procesu Identyfikacji, w tym przede wszystkim Dane identyfikujące osobę.

2. Zasady ustalenia tożsamości osób fizycznych

a. Dla celów skorzystania z Usługi QDS Dostawca Usługi przeprowadza weryfikację tożsamości osób fizycznych z zastosowaniem jednej z procedur przewidzianych dla kontekstu Usługi QDS, zgodnie z Polityką Weryfikacji Tożsamości Dostawcy Usługi.
b. Weryfikacja tożsamości osób fizycznych odbywa się przede wszystkim w sposób zdalny i zautomatyzowany w zabezpieczonym i nadzorowanym przez Dostawcę Usługi środowisku.
c. Identyfikacja osoby fizycznej w trybie zdalnym jest realizowana z wykorzystaniem jednej z przyjętych przez Dostawcę Usługi procedur:

- Identyfikacja w notyfikowanym systemie identyfikacji elektronicznej (eID) uznanym przez Unię Europejską za zapewniający co najmniej "znaczący" (“substantial”) poziom pewności;
- Identyfikacja i udostępnienie Danych identyfikujących osobę przez aplikacje, których administratorem są organy administracji państwowej lub instytucje zaufania publicznego;
- przekazanie Danych identyfikujących osobę przez podmioty podlegające obowiązkom wynikającym z właściwych przepisów prawa dotyczących przeciwdziałania praniu pieniędzy oraz finansowaniu terroryzmu (AML);
- przekazanie Danych identyfikujących osobę przez osoby uprawnione do reprezentacji osoby prawnej lub innej jednostki organizacyjnej oraz dokonanie Uwierzytelnienia przez osobę, której dane zostały przekazane;
- pozyskanie Danych identyfikujących osobę ze złożonego podpisu zaufanego, w rozumieniu Ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne;
- pozyskanie Danych identyfikujących osobę z certyfikatu kwalifikowanego podpisu elektronicznego lub zaawansowanego podpisu elektronicznego;
- pozyskanie Danych identyfikujących osobę z procesu walidacji elektronicznego dokumentu tożsamości;
- identyfikację schematem identyfikacji elektronicznej (eID), który Dostawca Usługi uznaje za zapewniający pewność równoważną "znaczącemu" (“substantial”) poziomowi pewności, na podstawie oceny zgodności przeprowadzonej przez Dostawcę Usługi.

d. W przypadku nieudanej identyfikacji automatycznej, na wniosek Użytkownika, Dostawca Usługi przeprowadza zdalną weryfikację tożsamości Użytkownika za pośrednictwem wideokonferencji z udziałem operatora umocowanego przez Dostawcę Usługi, przy użyciu metodologii weryfikacji określonych Danych identyfikujących osobę z dokumentem tożsamości oraz weryfikacji wizualnej osoby fizycznej z przedstawionym dokumentem tożsamości.
e. W przypadku niepomyślnej weryfikacji tożsamości w sposób zdalny, osobie umożliwia się wizytę w biurze Dostawcy Usługi lub spotkanie z osobą uprawnioną przez Dostawcę Usługi w celu identyfikacji osobistej, po wcześniejszych ustaleniach z Dostawcą Usługi. Dostawca Usługi przeprowadza weryfikację autentyczności informacji przy użyciu prawnie dozwolonych oraz dostępnych środków.
f. Minimalny zakres Danych identyfikujących osobę pozyskiwanych w trakcie weryfikacji tożsamości to:

- imię (imiona) i nazwisko,
- unikalny identyfikator krajowy (w przypadku Polski jest to PESEL lub numer dokumentu tożsamości) lub inny identyfikator unikalnie powiązany z osobą fizyczną, nadany przez właściwe organy administracji publicznej.

Dopuszcza się zastąpienie unikalnego identyfikatora kombinacją imienia i nazwiska oraz danych dodatkowych wymienionych w punkcie "g" poniżej, przy zachowaniu unikalności takiego zestawu Danych identyfikujących osobę oraz możliwości potwierdzenia tych danych w stosunku do osoby identyfikowanej.

g. Zakres Danych identyfikujących osobę może się różnić w zależności od wybranej procedury Identyfikacji. Dodatkowymi danymi mogą być w szczególności:
   - data urodzenia,
   - miejsce zamieszkania,
   - wizerunek oraz inne dane biometryczne.
h. Przed rozpoczęciem świadczenia Usługi QDS, w zależności od wybranej procedury, od osoby fizycznej dla celów Identyfikacji wymagane jest:
   - zainicjowanie procesu rejestracji do Usługi QDS oraz identyfikacji, w celu zawarcia umowy na świadczenie Usługi QDS,
   - zaakceptowanie regulaminów oraz polityk, niezbędnych do świadczenia Usługi QDS lub niezbędnych do przeprowadzenia weryfikacji tożsamości,
   - posiadanie ważnego dokumentu tożsamości, środka identyfikacji elektronicznej, kwalifikowanego podpisu elektronicznego zgodnego z eIDAS lub innego dokumentu pozwalającego na weryfikację tożsamości, przewidzianego Polityką Weryfikacji Tożsamości.

3. Zasady ustalenia tożsamości osoby fizycznej uprawnionej do reprezentacji oraz potwierdzenie danych osoby prawnej lub innych jednostek organizacyjnych

a. Weryfikacja Danych identyfikujących osobę wobec osoby prawnej lub innej jednostki organizacyjnej jest przeprowadzana po pozytywnej weryfikacji tożsamości osoby lub osób fizycznych, które ją reprezentują.
b. Weryfikacja Danych identyfikujących osobę wobec osoby prawnej lub innej jednostki organizacyjnej ma na celu udowodnienie, że przed udostępnieniem Usługi QDS osoba prawna lub inna jednostka organizacyjna istnieje, oraz że przedstawiciel, który ubiega się o korzystanie z Usługi QDS, ma uprawnienia do reprezentacji.

c. Weryfikacja tożsamości osoby fizycznej odbywa się w sposób określony w rozdziale III pkt. 2 powyżej.
d. Weryfikacja tożsamości osoby prawnej lub innej jednostki organizacyjnej odbywa się sposób zdalny i zautomatyzowany, poprzez złożenie przez osoby uprawnione do reprezentacji danej osoby prawnej lub innej jednostki organizacyjnej (pełnomocnicy, prokurenci, zarząd), oświadczenia o poprawności i prawdziwości danych reprezentowanego podmiotu oraz o prawie do reprezentacji w wymaganym zakresie.
e. W celu ustalenia tożsamości osoby fizycznej, która jest przedstawicielem osoby prawnej lub innej jednostki organizacyjnej oraz potwierdzenia jej praw do reprezentacji:
    - w przypadku, gdy jej uprawnienia do reprezentacji wynikają z przepisów prawa lub innych dokumentów w szczególności takich jak umowa spółki, statut, uchwała czy wypis z właściwego rejestru, Użytkownik przed udostępnieniem Usługi QDS składa Dostawcy Usługi oświadczenie o uprawnieniu do samodzielnej reprezentacji i potwierdzeniu danych,
    - w przypadku, gdy uprawnienie do reprezentacji wynika z upoważnienia do reprezentacji, upoważnienie to musi pochodzić od osoby lub osób posiadających prawo do reprezentacji. Użytkownik działający w oparciu o upoważnienie, przed udostępnieniem Usługi QDS składa Dostawcy Usługi treść upoważnienia podpisanego przez osoby uprawnione do reprezentacji wraz z jednoczesnym potwierdzeniem danych.
f. W przypadku, gdy upoważnienie nie może zostać ustanowione zgodnie z procedurą opisaną w punkcie powyżej, pierwotna tożsamość osoby prawnej zostanie zweryfikowana na podstawie dokumentów przedłożonych uprawnionemu przedstawicielowi Dostawcy Usługi. W takim przypadku Dostawca Usługi może zażądać takich dokumentów jak:
    - pełnomocnictwo poświadczone przez notariusza, a w przypadku cudzoziemców z appostile, z którego wynika umocowanie do reprezentacji,
    - pełnomocnictwo podpisane kwalifikowanym podpisem elektronicznym przez osoby upoważnione do reprezentacji,
    - dowód osobisty lub inne dokumenty potwierdzające tożsamość reprezentanta,
    - wykaz z rejestru potwierdzającego umocowanie do reprezentacji.
g. Dopuszcza się przeprowadzenie weryfikacji ex post, w oparciu o zebrane dowody (w szczególności: dowody fizyczne lub zapisy będą weryfikowane ex

post). W tym celu Dostawca Usługi dokonuje cyklicznych sprawdzeń prawdziwości przekazanych Danych identyfikujących osobę oraz dowodów na wykazanie umocowania do reprezentacji, w tym poprzez ich weryfikację w rejestrach publicznych, jeżeli jest to możliwe.

h. Weryfikacja dowodów potwierdzających może być zautomatyzowana, jeśli jest to możliwe i opłacalne ekonomicznie.
i. W przypadku stwierdzenia, iż oświadczenie złożone przez osoby uprawnione do reprezentacji jest nieprawdziwe lub niekompletne, Dostawca Usług jest uprawniony do zawieszenia Usługi QDS do czasu wyjaśnienia sprawy. Ponadto, Dostawca Usług będzie uprawniony do powiadomienia organów ścigania.
j. Dokonanie weryfikacji tożsamości osoby prawnej lub innych jednostek organizacyjnych może być również przeprowadzone przez uprawnionego przedstawiciela Dostawcy Usługi, w tym na etapie zawierania umowy na Usługę QDS.
k. Minimalny zakres Danych identyfikujących osobę, pozyskanych w trakcie weryfikacji tożsamości to:
    - nazwa osoby prawnej lub innej jednostki organizacyjnej,
    - numer identyfikacji podatkowej lub inny niepowtarzalny identyfikator, o ile zostały wydane.
l. Zakres Danych identyfikujących osobę pozyskanych w trakcie weryfikacji tożsamości może również zawierać dodatkowe dane, takie jak adres siedziby, inne numery identyfikacyjne.
m. Dostawca Usługi podejmuje kroki w celu zminimalizowania ryzyka, że tożsamość osoby prawnej lub innej jednostki organizacyjnej nie jest zgodna z podaną.

4. Zasady ustalania tożsamości innych osób uprawnionych do reprezentacji osoby prawnej lub innej jednostki organizacyjnej

a. Nadawcą i Odbiorcą w ramach Usługi QDS może być zarówno osoba fizyczna działająca we własnym imieniu, jak również osoba fizyczna reprezentująca osobę prawną lub inną jednostkę organizacyjną, która zawarła z Dostawcą Usług umowę na świadczenie Usługi QDS.
b. Weryfikacja tożsamości osób fizycznych jest realizowana zgodnie z zasadami wskazanymi w rozdziale III ust 2 powyżej.
c. W ramach świadczenia Usługi QDS dla osoby prawnej lub innej jednostki organizacyjnej, Nadawcą lub Odbiorcą może być również osoba fizyczna, która została wskazana do jej reprezentacji przy korzystaniu z Usługi QDS, poprzez

nadanie jej odpowiedniej roli Usłudze QDS na Platformie Autenti. Użytkownik wskazany przez osobę uprawnioną do reprezentacji osoby prawnej lub innej jednostki organizacyjnej jako upoważniony do wysyłania lub odbierania e-Przesyłek nie może przekazać swojego prawa innemu Użytkownikowi, z wyłączeniem sytuacji, gdy pełni również rolę administratora w Usłudze QDS..

d. W przypadku wskazania przez osobę reprezentującą osobę prawną lub inną jednostkę organizacyjną innych osób uprawnionych do korzystania z Usługi QDS, nie jest wymagane przeprowadzenie dodatkowej Identyfikacji z zastosowaniem procedur opisanych w pkt 2 i 3 powyżej.
e. Źródłem tożsamości osób wskazanych jako uprawnionych do korzystania z Usługi QDS jest osoba prawna lub inna jednostka organizacyjna, reprezentowana przez uprawnioną osobę fizyczną.
f. Osoba prawna lub inna jednostka organizacyjna ponosi odpowiedzialność za prawdziwość przekazanych Danych identyfikujących osobę.

5. Uwierzytelnienie

a. Wstępna weryfikacja tożsamości Użytkownika nie jest wymagana w przypadku ponownego użycia Usługi QDS.
b. Użytkownicy celem ponownego użycia Usługi QDS dokonują Uwierzytelnienia za pomocą wydanych Użytkownikom środków uwierzytelniających.
c. Proces Uwierzytelnienia jest realizowany w taki sposób, aby zapewnić znaczny poziom pewności, że tożsamość osoby dokonującej Uwierzytelnienia jest poprawna.
d. Uwierzytelnienie jest realizowane w zależności od sposobu dostarczania Usługi QDS do Użytkownika:
    - w przypadku korzystania z aplikacji mobilnej Dostawcy QDS, Użytkownik używa do Uwierzytelniania kluczy kryptograficznych (sekretów), które są powiązane z aplikacją mobilną w sposób dający wysoką pewność, że nie mogą być wykorzystane przez inne aplikacje, np. przez umieszczenie w chronionym kontenerze systemu operacyjnego (np. keychain). Klucze generowane są w procesie aktywacji aplikacji,, w trakcie którego Użytkownik przechodzi Wstępną weryfikację tożsamości lub Uwierzytelnia się za pomocą wydanych środków uwierzytelniających, przy czym wymagane jest Uwierzytelnienie dwuskładnikowe. Każda instancja aplikacji mobilnej podlega osobnej aktywacji i jest odróżnialna od innych, korzystając z wygenerowanych specyficznie dla niej kluczy

kryptograficznych. Klucze prywatne nie opuszczają urządzenia, na którym były generowane.

- Jeśli Użytkownik korzysta z interfejsu API, Uwierzytelnia się przyznanymi mu wcześniej czynnikami uwierzytelnienia, zaś aplikacja (klient API) żądający tego Uwierzytelnienia musi być wcześniej zarejestrowana i skonfigurowana przez administratora na Platformie Autenti, w sposób umożliwiający żądanie od Użytkownika uprawnień do wywołania API Usługi QDS w jego imieniu. Żądanie Uwierzytelnienia Użytkownika API musi być zabezpieczone przed przedstawieniem go przez inną aplikację, poprzez zastosowanie metod kryptograficznych, w szczególności na poziomie kanału komunikacji, np. Mutual TLS, lub też poprzez kryptograficzne zabezpieczenie całości lub części żądania (np. przez wykorzystanie tokenów podpisanych, zgodnie RFC 7523, sekcja 2.2, zastosowanie podpisu żądania zgodnie z RFC 7515 lub podobny mechanizm gwarantujący pochodzenie żądania i jego integralność). Żądania Uwierzytelnienia dla potrzeb API powinny być zabezpieczone przed ponownym przedstawieniem przez stronę nieuprawnioną, w razie ich wycieku. Dopuszcza się, za wiedzą i zgodą Użytkownika, działanie przez API w jego imieniu w czasie, gdy nie wykorzystuje on interaktywnie Usługi QDS, poprzez wydawanie tokenów uwierzytelniających o dłuższym czasie ważności, oraz zastosowanie mechanizmów trwałej autoryzacji do działania, takich jak np. OAuth2 Refresh Token flow (RFC 6749).. Dopuszcza się działanie zautomatyzowanych aplikacji zewnętrznych korzystających z interfejsu API, nie działających w imieniu konkretnego Użytkownika, tj, działających w imieniu Nadawcy lub Odbiorcy jako podmiotu, uwierzytelnionych za pomocą wydanych specyficznie dla nich danych uwierzytelniających, skonfigurowanych przez administratora na Platformie Autenti, w szczególności sekretów współdzielonych, tzw. API key lub kluczy kryptograficznych. Dopuszczalne jest także autoryzowanie żądań takich aplikacji w oparciu o kryptograficznie zabezpieczony kanał ustanowiony za pomocą kluczy zarejestrowanych specyficznie dla danej aplikacji.
- w przypadku korzystania z aplikacji dostępnej za pośrednictwem przeglądarki internetowej, Użytkownik Uwierzytelnia się wybranym przez siebie sposobem, obejmującym co najmniej Uwierzytelnienie dwuskładnikowe, lub korzysta z ponownej identyfikacji.

e. Poza opisanymi sposobami Uwierzytelniania, Dostawca Usługi stosuje dodatkowe mechanizmy w celu osiągnięcia maksymalnego bezpieczeństwa i ochrony procesu.

6. Zasady przetwarzania Danych identyfikujących osobę

a. Po Wstępnej weryfikacji tożsamości realizowanej zdalnie w sposób automatyczny, Dostawca Usługi zachowuje takie dane jak:
   - Dane identyfikujące osobę,
   - dowód, że tożsamość Użytkownika została zweryfikowana.

b. Po Wstępnej weryfikacji tożsamości realizowanej przez upoważnionych pracowników Dostawcy Usługi, zarówno w formie zdalnej jak i poprzez fizyczną obecność, Dostawca Usługi wystawia dowody na potwierdzenie, że tożsamość Użytkownika została zweryfikowana.

c. Wskazane powyżej dane są przechowywane przez Dostawcę Usługi przez okres 20 lat, zgodnie z art. 17 ust 2 Ustawy z dnia 5 września 2016 r. o usługach zaufania oraz identyfikacji elektronicznej.

IV. Dowody z Usługi QDS

Dostawca Usługi zapewnia wystawianie dowodów z realizacji Usługi QDS, w tym zdarzeń które mają miejsce podczas przesyłania Zawartości przesyłki między Nadawcą a Odbiorcą. Dowody wystawiane przez Dostawcę Usługi mogą zostać wykorzystane dla celów dowodowych, w tym także w postępowaniu sądowym, w tym na potrzeby wykazania, że czynność w ramach Usługi QDS została dokonana w określonym momencie, co zostanie potwierdzone Znacznikiem czasu oraz zabezpieczone Pieczęcią elektroniczną.

Dowodem Usługi QDS jest oświadczenie o fakcie, podpisane Pieczęcią elektroniczną. Dowód jest generowany i dostarczony Nadawcy oraz Odbiorcy (jeżeli Zawartość przesyłki została przyjęta lub doręczona) niezwłocznie po wykonaniu czynności, jak również przechowywany przez Dostawcę Usług przez okres co najmniej 36 miesięcy.

Źródłem czasu dla generowanych dowodów jest (zgodnie z art. 44 eIDAS) usługa kwalifikowanego dostawcy znaczników czasu, z którym Dostawca Usługi zawarł umowę o świadczenie usług.

Dowody są pozostawiane do wglądu i dyspozycji Użytkowników, w tym możliwość ich pobrania w postaci dokumentów elektronicznych poza Usługę QDS w obrębie interfejsu

Użytkownika Usługi QDS lub poprzez wykonanie dedykowanej operacji pobrania dowodów przez API.

1. Dowody powiązane z Nadawcą

a. Dowód Identyfikacji Nadawcy

Dowód Identyfikacji Nadawcy jest wydawany w formie podpisanego tokena identyfikacyjnego, zawierającego zestaw elementów danych identyfikacyjnych i odniesienie do weryfikowalnej ścieżki audytu procesu Identyfikacji.

Domyślną formą dowodu jest podpisany JSON Web Token (JWT) zgodny ze specyfikacją OpenID Connect for Identity Assurance 1.0, dopuszcza się użycie innych form reprezentacji dowodu o tożsamej użyteczności, w szczególności zmiany dostosowujące formę dowodu do wymogów standardów uznanych w domenie, lub wprowadzonych wymogami prawa w przyszłości.

Dowody będą jednoznacznie identyfikowalne, a czas ich utworzenia będzie rejestrowany. Wymaganie to, w przypadku stosowania dowodów w postaci tokenów JWT spełnione będzie przez zastosowanie oświadczeń (ang: claim, patrz RFC 7519, sekcja 2 “Terminologia” https://datatracker.ietf.org/doc/html/rfc7519#section-2) “iat” oraz “jti”.

Dowód Identyfikacji Nadawcy nie jest postawiony do dyspozycji Użytkownika i w związku z tym, jego integralność nie jest zabezpieczona Pieczęcią elektroniczną służącą do podpisywania dowodów z Usługi QDS.

b. Dowód Uwierzytelnienia Nadawcy

Uwierzytelnienie Nadawcy wobec Usługi QDS skutkuje wydaniem asercji tożsamości Nadawcy w postaci podpisanego (lub zaszyfrowanego) tokena sieciowego JSON, zawierającego co najmniej unikalny identyfikator użytkownika (dwie różne asercje odwołujące się do tego samego unikalnego identyfikatora dowodzą, że podmiot, dla którego wydano asercje, był tym samym podmiotem w obu przypadkach), unikalny identyfikator asercji oraz czas wydania.

Sama asercja będzie służyć jako dowód i zostanie zapisana w formie dosłownej w systemie wydającym oraz w formie dosłownej lub jako odniesienie poprzez zacytowanie unikalnego identyfikatora asercji w systemie Usługi QDS.

Asercja Uwierzytelnienia Nadawcy zawiera informacje o użytych środkach uwierzytelniających.

Dowód Uwierzytelnienia Nadawcy nie jest postawiony do dyspozycji Użytkownika i w związku z tym, jego integralność nie jest zabezpieczona Pieczęcią elektroniczną służącą do podpisywania dowodów z Usługi QDS.

2. Dowody odnoszące się do Odbiorcy

a. Dowód Identyfikacji Odbiorcy

Dowód Identyfikacji Odbiorcy jest wydawany w tożsamy sposób jak przewidziano dla dowodu Identyfikacji Nadawcy (*vide* pkt 1 lit a powyżej).

b. Dowód Uwierzytelnienia Odbiorcy

Dowód Uwierzytelnienia Odbiorcy jest wydawany w tożsamy sposób jak przewidziano dla dowodu Uwierzytelnienia Nadawcy (*vide* pkt 1 lit b powyżej).

3. Dowody dotyczące czynności wykonywanych przez Dostawcę Usługi

a. Przyjęcie do doręczenia (Submission Acceptance)

W momencie pomyślnego przesłania Zawartości przesyłki do systemu Usługi QDS przez Nadawcę, generowany jest dowód z dokładną datą i godziną wskazujący, że Nadawca, który został zidentyfikowany, przesłał Zawartość przesyłki do systemu Usługi QDS, która została następnie zaakceptowana przez Dostawcę Usługi, po weryfikacji żądanych parametrów usługi (w tym trybu doręczenia), adresu lub innego określenia Odbiorcy (pod kątem przynajmniej możliwości dostarczenia pod żądany Adres do doręczeń elektronicznych) oraz innych warunków świadczenia usługi. Po otrzymaniu Zawartości przesyłki Dostawca Usługi podejmuje wszelkie niezbędne działania w celu dostarczenia Zawartości przesyłki do Odbiorcy.

b. Odmowa przyjęcia do doręczenia (Submission Rejection)

W przypadku braku zaakceptowania Zawartości przesyłki lub wskazanych przez nadawcę parametrów usługi, Usługa QDS wystawia dowód odmowy przyjęcia do doręczenia, poświadczający, że Usługa QDS odmówił dalszych czynności zmierzających do przekazania Zawartości przesyłki do Odbiorcy. Wygenerowane dowody wskazują, że Nadawca, który został początkowo zidentyfikowany i prawidłowo uwierzytelniony, przesłał

Zawartość przesyłki do Usługi QDS w określonym dniu i czasie, a system Usługi QDS odmówił wykonania dalszych czynności zmierzających do doręczenia.

4. Dowody związane z doręczeniem e-Przesyłki

Dowody związane z dostarczeniem e-Przesyłki służą wykazaniu, iż Zawartość przesyłki Nadawcy została dostarczona do Odbiorcy, lub, jeżeli do doręczenia nie doszło, opisują przyczyny takiej sytuacji. Powiązane dowody wskazują, że e-Przesyłka została dostarczona do Odbiorcy w ustalonym czasie po uprzedniej Identyfikacji Odbiorcy.

a. Akceptacja Zawartości przesyłki do doręczenia przez Usługę Odbiorcy (Relay Acceptance)

Dowód wskazuje, że Zawartość przesyłki została z powodzeniem przekazana do Usługi Odbiorcy, a Usługa Odbiorcy zaakceptowała ją do doręczenia.

b. Odmowa akceptacji Zawartości przesyłki do doręczenia przez Usługę Odbiorcy (Relay Rejection)

Dowód wskazuje, że Usługa Odbiorcy odmawia podjęcia próby doręczenia Zawartości przesyłki do Odbiorcy.

c. Niepowodzenie próby przekazania Zawartości przesyłki do Usługi Odbiorcy (Relay Failure)

Dowód wskazuje, że próba przekazania Zawartości przesyłki do Usługi Odbiorcy nie powiodła się pomimo podjęcia przewidzianych protokołem technicznym lub wzajemnymi ustaleniami środków zaradczych.

d. Dostarczenie Zawartości przesyłki (Content Consignment)

Dowód wskazuje, że Zawartość przesyłki została postawiona do dyspozycji Odbiorcy w obrębie systemu Usługi Odbiorcy.

e. Niepowodzenie dostarczenia Zawartości przesyłki (Content Consignment Failure)

Dowód wskazuje, że Zawartość przesyłki Nadawcy nie mogła zostać postawiona do dyspozycji Odbiorcy w obrębie systemu Usługi Odbiorcy w określonym czasie z powodu błędów technicznych i/lub z innych przyczyn.

f. Powiadomienie o postawieniu e-Przesyłki do dyspozycji Odbiorcy (Consignment Notification)

Dowód wskazuje, że Usługa Odbiorcy powiadomiła Odbiorcę za pomocą ustalonego kanału komunikacji o postawieniu e-Przesyłki do dyspozycji Odbiorcy.

g. Niepowodzenie powiadomienia o postawieniu e-Przesyłki do dyspozycji Odbiorcy (Consignment Notification Failure)

Dowód wskazuje, że Usługa Odbiorcy podjęła próbę powiadomienia Odbiorcy za pomocą ustalonego kanału komunikacji, ale próba ta nie powiodła się.

h. Przekazanie Zawartości przesyłki (Content Handover)

Dowód wskazuje, że e-Przesyłka została pomyślnie przekazana z Usługi Odbiorcy do systemów zewnętrznych wskazanych przez Odbiorcę do odbioru e-Przesyłki.

W przypadku publicznej usługi rejestrowanego doręczenia elektronicznego (tzw. PURDE), dowód ten potwierdza zakończone powodzeniem przekazanie e-Przesyłki do systemu zewnętrznego skonfigurowanego przez Odbiorcę do automatycznego odbioru lub przesunięcie e-Przesyłki z systemów Usługi Odbiorcy do skrzynki odbiorczej po dyspozycji tego przesunięcia odebranej od Odbiorcy.

i. Niepowodzenie przekazania Zawartości przesyłki (Content Handover Failure)

Dowód wskazuje, że podjęta próba przekazania e-Przesyłki z Usługi Odbiorcy do wskazanego przez Odbiorcę systemu zewnętrznego nie powiodła się.

5. Dowody związane z akceptacją lub odmową akceptacji e-Przesyłki przez Odbiorcę dla usługi doręczenia przewidującej taką możliwość

Dowody z tej grupy nie są wystawiane dla realizacji publicznej usługi doręczenia elektronicznego.

a. Powiadomienie o oczekiwaniu na akceptację odbioru e-Przesyłki (Notification for Acceptance)

Dowód wskazuje, że Usługa Odbiorcy powiadomiła Odbiorcę za pomocą ustalonego kanału komunikacji o otrzymaniu e-Przesyłki, której doręczenie wymaga jego akceptacji.

Dowód zawiera informacje czy próba powiadomienia była pierwszą czy powtórną

b. Niepowodzenie powiadomienia o oczekiwaniu na akceptację odbioru e-Przesyłki (Notification for Acceptance Failure)

Dowód wskazuje, że próba powiadomienia Odbiorcy za pomocą ustalonego kanału komunikacji o otrzymaniu e-Przesyłki, której doręczenie wymaga akceptacji Odbiorcy podjęta przez Usługę Odbiorcy zakończyła się niepowodzeniem.

c. Akceptacja e-Przesyłki przez Odbiorcę (Consignment Acceptance)

Dowód wskazuje, że Odbiorca e-Przesyłki wydał dyspozycję doręczenia e-Przesyłki w trybie przewidującym jej akceptację.

d. Odrzucenie e-Przesyłki przez Odbiorcę (Consignment Rejection)

Dowód wskazuje, że Odbiorca e-Przesyłki odrzucił doręczenie e-Przesyłki wysłanej w trybie przewidującym taką możliwość.

e. Wygaśnięcie możliwości akceptacji lub odrzucenia e-Przesyłki przez Odbiorcę (Acceptance Rejection Expiry)

Dowód wskazuje, że w czasie przewidzianym warunkami świadczenia usługi, Odbiorca e-Przesyłki wymagającej akceptacji przed jej doręczeniem nie podjął żadnych decyzji.

6. Dowody przewidziane dla realizacji Usługi QDS ze Standardem RDE

a. Potwierdzenie wysłania

Potwierdzenie wysłania jest dodatkowym dowodem zdefiniowanym przez Standard RDE dla usługi publicznego rejestrowanego doręczenia elektronicznego wystawianym na podstawie i w oparciu o to samo zdarzenie co do dowód Submission Acceptance norm ETSI.

Potwierdzenie wysłania jest wystawiane przez Dostawcę Usługi zgodnie z wymogami punktu 6.6 Standardu RDE.

b. Potwierdzenie otrzymania

Potwierdzenie otrzymania jest dodatkowym dowodem zdefiniowanym przez Standard RDE dla usługi publicznego rejestrowanego doręczenia elektronicznego. Potwierdzenie otrzymania jest wystawiane przez Usługę Nadawcy zgodnie z wymogami punktu 6.7 Standardu RDE.

V. Zakres Usługi QDS

1. Zakres

a. Usługa QDS umożliwia przesyłanie Zawartości przesyłki między określonym Nadawcą i Odbiorcą ze skutkiem rejestrowanego doręczenia elektronicznego, tj. z domniemaniem określonym art. 43 eIDAS. W związku z tym zakłada się, że Zawartość przesyłki przesyłana i otrzymywana za pośrednictwem Usługi QDS jest integralna, wysłana przez Nadawcę i otrzymana przez Odbiorcę oraz że data i godzina wysłania i otrzymania są dokładne.

b. Usługa QDS realizowana jest w ramach usługi świadczonej drogą elektroniczną na podstawie Regulaminu Autenti eDelivery

c. Dostęp do Usługi QDS odbywa się za pośrednictwem interfejsu UI Platformy Autenti lub API.

d. Usługa QDS może być realizowana samodzielnie przez Dostawcę Usługi lub poprzez interoperacyjność z innymi dostawcami usługi rejestrowanego doręczenia elektronicznego, w tym Operatorem Wyznaczonym.

e. Ograniczenia dotyczące korzystania z Usługi QDS, w tym przede wszystkim rodzaje akceptowanych przez Usługę QDS formatów plików elektronicznych wskazane zostały w treści Regulaminu Autenti eDelivery.

2. Tryby świadczenia Usługi QDS

Dostawca Usługi QDS może świadczyć usługę w jednym z trybów doręczenia przewidzianym w Standardzie ETSI 319 522 tj.:

- Basic - czyli przesyłka zwykła, gdzie treść przesyłki zostaje udostępniona Odbiorcy bez możliwości odrzucenia,
- Consented - powiadomienie o e-Przesyłce wysyłane jest do Odbiorcy przed postawieniem e-Przesyłki do dyspozycji Odbiorcy. Odbiorca ma możliwość zaakceptowania lub odrzucenia e-Przesyłki.
- Consented Signed - tryb analogiczny do Consented, z dodatkowym wymogiem elektronicznego podpisania poświadczenia decyzji o odebraniu e-Przesyłki.

Udostępnienie Usługi QDS w danym trybie, jeżeli nie wynika z właściwych przepisów prawa (np. wobec publicznej usługi doręczeń elektronicznych) lub możliwości technicznych innych dostawców kwalifikowanej usługi doręczeń elektronicznych, pozostaje do decyzji biznesowej pomiędzy Dostawcą Usługi QDS a Użytkownikiem. W przypadku udostępnienia Użytkownikowi przez Dostawcę Usługi wielu trybów, ostateczny wybór trybu doręczenia należy do Użytkownika.

3. Opis świadczenia Usługi QDS

Usługa QDS daje Nadawcy możliwość przekazania Zawartości przesyłki przeznaczonej do doręczenia do wskazanego przez Nadawcę Odbiorcy, oraz określenia przez Nadawcę istotnych parametrów doręczenia (takich jak tryb doręczenia, dane Odbiorcy do weryfikacji itp.). Usługa QDS przyjmuje Zawartość przesyłki do doręczenia, lub odmawia podjęcia się próby doręczenia, na podstawie weryfikacji zgodności cech przekazanej Zawartości przesyłki oraz wskazanych przez Nadawcę parametrów z warunkami świadczenia Usługi QDS lub warunkami świadczenia Usługi Odbiorcy, w szczególności w zakresie weryfikacji możliwości technicznych wykonania Usługi QDS, istnienia stosownych ustaleń komercyjnych oraz zgodności z wymogami prawa. Przyjęcie lub odmowa przyjęcia Zawartości przesyłki do doręczenia dokumentowane jest odpowiednimi dowodami, które zostają udostępnione Nadawcy.

Usługa QDS może też być Usługą Odbiorcy (tj. Odbiorca korzysta z Usługi QDS jako obsługującej Adres do doręczeń elektronicznych dla Odbiorcy, a Zawartość przesyłki do doręczenia została przekazana do Usługi QDS przez Usługę Nadawcy lub samego Nadawcę). W takim wypadku, Usługa QDS przyjmuje Zawartość przesyłki do doręczenia od Usługi Nadawcy lub samego Nadawcy, i weryfikuje możliwość doręczenia jej do Odbiorcy, w szczególności pod kątem zgodności wskazanych parametrów usługi z warunkami świadczenia Usługi QDS, postanowieniami prawa i ustaleniami komercyjnymi z Usługą Nadawcy. Stosownie do wyników tej weryfikacji Usługa QDS podejmuje się próby doręczenia Zawartości przesyłki do Odbiorcy, lub odrzuca Zawartość przesyłki, co dokumentuje wystawieniem stosownych dowodów, które udostępniane są (z wykorzystaniem ustalonych środków technicznych) Usłudze Nadawcy, lub samemu Nadawcy. Usługa QDS stawia Zawartość przesyłki do dyspozycji Odbiorcy w obrębie Usługi QDS, i powiadamia o tym fakcie Odbiorcę z użyciem ustalonego kanału powiadomień. Oba zdarzenia dokumentowane są wystawieniem przez Usługę QDS stosownych dowodów, a przypadku niepowodzenia którejś z tych czynności - wystawieniem dowodów niepowodzenia, które przekazuje Usłudze Nadawcy (lub samemu Nadawcy).

Jeżeli Zawartość przesyłki powinna zostać doręczona w trybie przewidującym możliwość odmowy jej przyjęcia przez Odbiorcę (tryb Consented) lub uzależniającym postawienie e-Przesyłki do dyspozycji Odbiorcy od jego świadomej decyzji (tryb Consented Signed),przed postawieniem e-Przesyłki do dyspozycji Odbiorcy w obrębie Usługi Odbiorcy lub przed przekazaniem do ustalonego systemu zewnętrznego (np. API), Usługa QDS powiadamia Odbiorcę ustalonym kanałem, o oczekiwaniu na zaakceptowanie

e-Przesyłki, i odbiera od niego decyzję, które to czynności dokumentuje stosownymi dowodami. W razie niepowodzenia powiadomienia Odbiorcy, Usługa QDS wystawia dowód niepowodzenia. W przypadku, gdy pomimo powiadomienia wymaganą liczbę razy (ustaloną danym reżimem obowiązującym w przypadku danej e-Przesyłki na podstawie ustaleń umownych, warunków świadczenia usługi lub przepisów prawa) Odbiorca nie podejmuje decyzji o przyjęciu e-Przesyłki (lub odrzuceniu jeśli reżim daje mu taką możliwość), Usługa QDS wystawia dowód nie podjęcia decyzji przez Odbiorcę w ustalonym czasie. Dowody z powyższych czynności Usługa QDS przekazuje Usłudze Nadawcy lub samemu Nadawcy. Wskazane powyżej tryby nie mają zastosowania do realizacji publicznej usługi doręczeń elektronicznych [tzw. PURDE].

W przypadku gdy Usługa QDS realizuje zadania Usługi Odbiorcy w toku realizacji publicznej usługi doręczeń elektronicznych w rozumieniu "*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",* Usługa QDS przekazuje Zawartość przesyłki do uzgodnionego systemu zewnętrznego, lub w przypadku gdy nie został on wskazany lub niezwłoczne przekazanie do tego systemu nie jest możliwe, stawia e-Przesyłkę do dyspozycji Odbiorcy w obrębie Usługi QDS i powiadamia ustalonym kanałem, wystawiając stosowne dowody na potwierdzenie podjętych czynności, lub ich niepowodzenia, które to dowody przekazuje Usłudze Nadawcy lub samemu Nadawcy.

Dowody wystawiane przez Usługę QDS są podpisane Pieczęcią elektroniczną i opatrzone Znacznikiem czasu.

4. Szczegółowy opis przebiegu Usługi QDS

a. Nadanie Zawartości przesyłki

Proces nadania Zawartości przesyłki obejmuje:

- Proces identyfikacji Nadawcy

W celu nadania Zawartości przesyłki Nadawca zobowiązany jest do dokonania Identyfikacji lub Uwierzytelnienia, w zakresie i na warunkach opisanych w rozdziale IV niniejszej Polityki.

- Wskazanie przez Nadawcę danych Odbiorcy

W przypadku osoby fizycznej:

- dane podawane obligatoryjnie to: Adres do doręczeń elektronicznych albo imię i nazwisko, oraz jeżeli nie jest podany Adres do doręczeń elektronicznych, adres e-mail, numer telefonu lub inny adres pozwalający na komunikację elektroniczną,
- opcjonalnie Usługa QDS może żądać inne dane pozwalające na weryfikację Odbiorcy pod kątem tożsamości Odbiorcy oraz możliwości realizacji Usługi QDS.

W przypadku osoby prawnej:

- dane podawane obligatoryjnie to: nazwa, numer identyfikacji podatkowej lub inny wymagany identyfikator oraz Adres do doręczeń elektronicznych, a jeżeli nie jest on podany, dane reprezentanta Odbiorcy, w tym imię i nazwisko, do którego ma zostać skierowana komunikacja związana z realizacją Usługi QDS.
- opcjonalnie Usługa QDS może żądać inne dane pozwalające na weryfikację Odbiorcy pod kątem tożsamości Odbiorcy oraz możliwości realizacji Usługi QDS.

- Przekazanie Dostawcy Usług przez Nadawcę Zawartości przesyłki przeznaczonej do doręczenia Odbiorcy.
- Ustalenie przez Dostawcę Usługi Adresu do doręczeń elektronicznych Odbiorcy (w przypadku przesyłek adresowanych do Odbiorców, których Adres do doręczeń elektronicznych nie jest znany Nadawcy) skutkujące jego potwierdzeniem lub informacją zwrotną o braku możliwości jego ustalenia.
- Po potwierdzeniu przez Dostawcę Usługi Adresu do doręczeń elektronicznych Odbiorcy, rozpoczyna się proces przekazania Zawartości przesyłki przez Dostawcę Usługi do właściwej Usługi Odbiorcy, obsługującej Adres do doręczeń elektronicznych Odbiorcy.

b. Przekazanie e-Przesyłki do Usługi Odbiorcy

W procesie przekazania e-Przesyłki następuje weryfikacja możliwości doręczenia Zawartości przesyłki wskazanemu Odbiorcy.

Potwierdzenie możliwości doręczenia e-Przesyłki jest warunkiem koniecznym do poprawnej realizacji Usługi QDS.

W przypadkach, w których Dostawca Usługi Nadawcy nie obsługuje Adresu do doręczeń Odbiorcy, proces weryfikacji możliwości doręczenia e-Przesyłki występuje na każdym etapie doręczenia i wygląda następująco:

- Dostawca Usługi przekazuje do Usługi Odbiorcy za pomocą uzgodnionego mechanizmu technicznego e-Przesyłkę wraz z ustalonymi informacjami określającymi Odbiorcę, np. Adres do doręczeń elektronicznych.
- Usługa Odbiorcy, do której został przypisany Adres do doręczeń elektronicznych, weryfikuje możliwość doręczenia e-Przesyłki do wskazanego Odbiorcy, w tym m.in. poprzez zgodność wskazanego trybu doręczenia, ważność Adresu do doręczeń elektronicznych. W efekcie powyższej weryfikacji, Usługa Odbiorcy przyjmuje do doręczenia lub odrzuca e-Przesyłkę, informując o tym Dostawcę Usługi Nadawcy.
- Dostawca Usługi Nadawcy może nie przyjąć do doręczenia lub odmówić doręczenie e-Przesyłki, w szczególności z przyczyn technicznych, w tym m.in. z powodu niezgodności określonych parametrów e-Przesyłki z warunkami świadczenia Usługi QDS (w szczególności komercyjnymi), niezgodności trybów doręczenia lub niedostępności Usługi Odbiorcy.

Jeżeli Dostawca Usługi Nadawcy jest jednocześnie Dostawcą Usługi Odbiorcy, e-Przesyłka jest przekazywana do doręczenia w ramach systemu Dostawcy Usług.

5. Doręczenie e-Przesyłki

Jeżeli Dostawca Usługi obsługuje Adres do doręczeń elektronicznych Odbiorcy, proces doręczania e-Przesyłki obejmuje:

a. jeżeli tryb doręczenia wskazany przez dostawcę Usługi Nadawcy (i obsługiwany przez dostawcę Usługi Odbiorcy zgodnie z obowiązującymi w chwili otrzymania e-Przesyłki ustaleniami wzajemnymi lub przepisami prawa) przewiduje przyznanie Odbiorcy prawa do odmowy przyjęcia e-Przesyłki (w szczególności w przypadku przesyłek ze wskazaniem trybu odbioru Consented, Odbiorca jest powiadamiany o fakcie otrzymania przez Usługę Odbiorcy e-Przesyłki adresowanej do danego Odbiorcy, i udostępniony jest mu mechanizm pozwalający na wyrażenie swojej decyzji co do jej odbioru. Ewentualna decyzja odmowna, lub brak decyzji w określonym przepisami lub warunkami swiadczenia usługi czasie zostają udokumentowane stosownymi dowodami.
b. Powiadomienie Odbiorcy o nadanej do Odbiorcy e-Przesyłce.

Odbiorca jest powiadamiany za pośrednictwem ustalonego kanału powiadomień, np. wiadomości e-mail oraz sms, Usługa Odbiorcy przekazuje Odbiorcy informację o gotowej do odbioru e-Przesyłce. Przekazana wiadomość może zawierać kod odbioru, informacje o rodzaju przesyłki i danych Nadawcy.

c. Proces identyfikacji Odbiorcy.
   W celu odebrania e-Przesyłki, Odbiorca zobowiązany jest do identyfikacji lub Uwierzytelnienia, zgodnie z rozdziałem IV Polityki.
d. Działania Odbiorcy.
   Dostawca Usług oczekuje na działanie Odbiorcy. Jeżeli Odbiorca nie podejmie działań zmierzających do odbioru e-Przesyłki we wskazanym czasie, podejmowana jest ponowna próba powiadomienia. Odbiorca może e-Przesyłkę zaakceptować lub odmówić jej akceptacji. Odmowa odbioru e-Przesyłki może nastąpić także poprzez zaniechanie i upływ wskazanego przez Dostawcę Usługi terminu.

VI. Bezpieczeństwo informacji

1. Zabezpieczenia fizyczne

Działania podejmowane w zakresie ochrony fizycznej przez Dostawcę Usługi są elementem opracowanego i wdrożonego u Dostawcy Usługi systemu bezpieczeństwa informacji, zgodnego z wymaganiami normy ISO/IEC 27001. Działania związane z fizyczną ochroną pomieszczeń i powiązaną z nimi infrastrukturą, systemami informatycznymi oraz informacjami mają na celu zapobieganie:

a. nieuprawnionemu dostępowi fizycznemu,
b. uszkodzeniu lub utracie, w tym kradzieży aktywów,
c. zakłóceniom w ciągłości działania lub dostępności informacji,
d. kradzieży informacji lub infrastruktury służącej do ich przetwarzania.

Infrastruktura Dostawcy Usługi niezbędna do świadczenia Usługi QDS jest fizycznie lub logicznie wydzielona od pozostałych usług świadczonych przez Dostawcę Usługi.

2. Dostęp fizyczny

Dostęp fizyczny do infrastruktury sprzętowej obsługującej systemy informatyczne oraz inne aktywa, w tym informacje takie jak dane osobowe, jest zabezpieczony zgodnie z zaleceniami międzynarodowych norm i standardów. Bezpieczeństwo fizyczne infrastruktury sprzętowej jest zapewnione między innymi poprzez:

a. kontrolę dostępu do pomieszczeń,

b. całodobową ochronę fizyczną,
c. kontrolę dostępu do szafy, w której znajduje się infrastruktura sprzętowa, gdzie zgodnie z wewnętrzną procedurą, dostęp jest możliwy wyłącznie dla co najmniej dwóch upoważnionych osób,
d. dokumentowanie dostępu do infrastruktury krytycznej (np. HSM).

Budynek z pomieszczeniami biurowymi Dostawcy Usługi oraz budynki serwerowni, w których znajduje się krytyczna infrastruktura sprzętowa, są chronione przez całodobową ochronę, system alarmowy, system monitoringu wizyjnego, system sygnalizacji pożaru oraz system kontroli dostępu. Dodatkowo pomieszczenia, w których znajduje się infrastruktura krytyczna, posiadają wbudowane systemy zasilania i wentylacji, ochrony przeciwpowodziowej i przeciwpożarowej.

Dostęp do wszystkich obszarów jest monitorowany i ograniczony wyłącznie do osób upoważnionych przez Dostawcę Usługi.

3. Dostęp do systemów informatycznych

Dla celów zapewnienia odpowiedniego poziomu bezpieczeństwa przetwarzanych informacji, w tym danych osobowych, Dostawca Usługi wdrożył zasady zarządzania uprawnieniami i dostępem, w oparciu o zasadę minimalizacji oraz wiedzy koniecznej, oraz wdrożył formalny proces zarządzania uprawnieniami, zgodnie z wewnętrznymi procedurami.

Dostęp do każdego systemu informatycznego odbywa się na podstawie identyfikatorów nadawanych osobom upoważnionym przez Dostawcę Usługi lub grupie takich osób, posiadających ten sam poziom uprawnień.

Osoby upoważnione do dostępu są zobowiązane do pracy tylko i wyłącznie na indywidualnie przydzielonych kontach użytkowników. Zabronione jest zezwalanie innym osobom na pracę na swoim koncie użytkownika, w tym przede wszystkim ujawnianie swoich danych dostępowych lub udostępnianie sprzętu.

Dokonywanie czynności administratorskich takich jak konfiguracja kluczowego systemu informatycznego, wykonywane są wyłącznie przez osoby pełniące role zaufane u Dostawcy Usługi, stosując do wykonania zadania narzędzia tymczasowo podnoszące poziom uprawnień lub bezpośrednio z poziomu uprawnień administratorskich, przy czym operacje takie wymagają współdziałania co najmniej dwóch administratorów.

Zarządzanie dostępami oraz uprawnieniami odbywa się na bieżąco. Proces zarządzania dostępami i uprawnieniami podlega nadzorowi poprzez przeprowadzanie cyklicznych audytów.

4. Zarządzanie incydentami

Zarządzanie incydentami u Dostawcy Usługi odbywa się zgodnie z przyjętą procedurą zarządzania incydentami, która ma na celu zapewnienie ciągłości operacyjnej oraz ograniczenie wpływu zdarzeń, które mogą mieć charakter incydentu związanego z bezpieczeństwem informacji oraz skutkować naruszeniem ochrony danych osobowych. Celem procedury zarządzania incydentami jest również zapewnienie zgodnego z przepisami prawa informowania o wystąpieniu incydentu wszystkich stron zainteresowanych.

Dostawca Usługi wyodrębnia następujące kategorie zdarzeń podlegających formalnemu zgłoszeniu:

a. Zdarzenie, jako nieoczekiwany lub niepożądany stan systemu informatycznego lub infrastruktury, który wskazuje na możliwe naruszenie bezpieczeństwa informacji,
b. Incydent, jako zdarzenie lub kilka powiązanych ze sobą zdarzeń, które zakłócają lub mogą z wysokim prawdopodobieństwem zakłócić działalność Dostawcy Usług oraz zagrażają bezpieczeństwu informacji, w tym ochronie danych osobowych,
c. Poważny Incydent, jako zdarzenie lub kilka powiązanych ze sobą zdarzeń, których skutkiem jest zatrzymanie działalności Autenti, w tym przede wszystkim utrata integralności, dostępności lub inne naruszenie bezpieczeństwa Informacji, które mają znaczący wpływ na świadczoną Usługę QDS lub przetwarzane w jej ramach dane osobowe.

Klasyfikacja zdarzeń następuje po ich zgłoszeniu do osób odpowiedzialnych u Dostawcy Usługi za proces zarządzania incydentami.

W ramach przyjętej procedury:

d. każda osoba, która jest świadkiem zdarzenia lub podejrzewa jego wystąpienie zobowiązana jest do jego niezwłocznego zgłoszenia,

e. zgłoszenie zdarzeń jest możliwe w każdy dostępny sposób, w tym poprzez dedykowany formularz dostępny dla personelu Dostawcy Usługi, tak aby umożliwić jak najszybsze powiadomienie odpowiednich osób,
f. każde zdarzenie będące incydentem lub poważnym incydentem jest odnotowywane w rejestrze incydentów,
g. każde zdarzenie jest oceniane przez osoby odpowiedzialne za zarządzanie incydentami pod względem zakresu zdarzenia, jego skutków, krytyczności, znaczenia wobec aktywów (np. infrastruktury), kosztów oraz ryzyka naruszenia ochrony danych osobowych,
h. podejmowane są działania zapobiegawcze oraz minimalizujące ryzyko, związane z rozprzestrzenieniem się incydentu lub jego skutków,
i. ustalone są zasady zgłaszania incydentów do właściwych organów nadzoru, Użytkowników lub innych osób zainteresowanych w czasie i sposób przewidziany właściwymi przepisami prawa.

W ramach procedury u Dostawcy Usług funkcjonuje również ciało kolegialne - Information Security Council, odpowiedzialna przede wszystkim za rekomendowanie sposobów postępowania w zakresie eliminacji przyczyn i skutków Incydentu, trybu zawiadamiania organów ścigania, komunikacji z organami nadzoru.

5. Personel Dostawcy Usługi

Dostawca Usługi wdrożył odpowiednie procedury związane z rekrutacją, wdrażaniem oraz zakończeniem współpracy, tak aby zapewnić odpowiedni poziom bezpieczeństwa informacji na każdym z etapów, w tym procedury związane informowaniem o zasadach bezpieczeństwa obowiązujących u Dostawcy Usługi oraz informowania o ich zmianach.

Dostawca Usługi zapewnia, że personel Dostawcy Usługi biorący udział w świadczeniu Usługi QDS oraz pełniący role zaufane posiada odpowiednie doświadczenie, umiejętności oraz kwalifikacje w zakresie pełnionych obowiązków oraz wykonywanych zadań.

Dostawca Usługi zapewnia również, że personel Dostawcy Usługi biorący udział w świadczeniu Usługi QDS oraz pełniący role zaufane został przeszkolony z ustanowionymi politykami i procedurami bezpieczeństwa informacji, a wiedza jest uzupełniana w ramach cyklicznych szkoleń z zakresu bezpieczeństwa informacji oraz ochrony danych osobowych, tak aby zapewnić odpowiedni poziom wiedzy. Procedury

obowiązujące u Dostawcy Usługi przewidują także odpowiednie postępowanie dyscyplinarne w przypadku złamania zasad bezpieczeństwa informacji.

W ramach obowiązującego u Dostawcy Usługi systemu zarządzania bezpieczeństwem informacji powołane zostały role zaufane, odpowiedzialne za realizację celów związanych z bezpieczeństwem informacji. Role i odpowiedzialności w zakresie bezpieczeństwa informacji zostały przez Dostawcę Usług określone oraz formalnie przypisane w taki sposób, aby wyeliminować konflikty interesów oraz zagwarantować bezstronność działalności Dostawcy Usługi. Nazwy ról zaufanych oraz ich odpowiedzialności zostały określone w dokumencie wewnętrznym Dostawcy Usługi.

6. Zarządzanie dostawcami

Dostawca Usługi wdrożył i opracował zasady bezpieczeństwa w relacjach z dostawcami, tak aby zapewnić odpowiedni poziom bezpieczeństwa prawnego oraz bezpieczeństwa informacji w zakresie, w jakim dostawcy świadczą usługi niezbędne do realizacji Usługi QDS. Pełna lista dostawców jest udostępniana w repozytorium na stronie internetowej Dostawcy Usługi.

W ramach procedury Dostawca Usługi zapewnia, aby:

a. każda relacja z dostawcą była odpowiednio udokumentowana, w tym zawierała odpowiednie postanowienia w zakresie bezpieczeństwa informacji oraz funkcjonowania i poziomu SLA (w tym dostępności usług), jeżeli jest to wymagane,
b. każdy dostawca dawał rękojmię odpowiedniego poziomu bezpieczeństwa informacji oraz jakości usług.

Dostawcy są poddawani cyklicznym audytom pod względem między innymi bezpieczeństwa informacji oraz dostępności i jakości usług.

7. Zarządzanie aktywami

Dostawca Usługi opracował i wdrożył zasady postępowania z aktywami, w szczególności takimi jak:

a. infrastruktura sprzętowa, aby zapewnić odpowiedni poziom bezpieczeństwa ich eksploatacji,

b. informacje, w tym dane osobowe, tak aby zapewnić odpowiedni poziom bezpieczeństwa w zakresie ich przetwarzania, w tym przechowywania i udostępniania.

Dostawca Usługi prowadzi rejestr kluczowych aktywów, który obejmuje między innymi takie informacje jak krytyczność aktywów oraz ich właścicieli.

Aktywa informacje są klasyfikowane zgodnie z przyjętą u Dostawcy Usługi klasyfikacją informacji. Każdy rodzaj klasyfikacji posiada określone zasady postępowania z aktywami informacyjnymi.

8. Zarządzanie ryzykiem

Dostawca Usługi wdrożył i opracował procedurę zarządzania ryzykiem, względem zagrożeń oraz podatności, tak aby zapewnić odpowiedni poziom identyfikowania ryzyk dla Usługi QDS oraz ich mitygacji, poprzez określanie i zarządzanie planami postępowania z ryzykiem.

Analiza ryzyka jest przeprowadzana przynajmniej raz w roku lub częściej, w przypadkach takich jak:

a. wdrażanie istotnych zmian w Usłudze QDS,
b. wdrażanie nowego systemu lub aplikacji służącej do przetwarzania informacji, w tym przede wszystkim danych osobowych,
c. zmiany lokalizacji dla krytycznej infrastruktury sprzętowej (np. zmiana serwerowni),
d. wystąpienie poważnego incydentu bezpieczeństwa.

9. Zarządzanie zmianą

Dostawca Usługi wdrożył i opracował procedurę zarządzania zmianą, której celem jest zapewnienie, że zmiany wprowadzane na środowisku produkcyjnym dla Usługi QDS w tym infrastrukturze sprzętowej, zostaną ocenione, autoryzowane, zarejestrowane i przetestowane.

W ramach zarządzania zmianą, Dostawca Usługi przeprowadza analizę wymogów bezpieczeństwa, która jest przeprowadzana na etapie projektowania i specyfikacji wymagań dla każdego projektu rozwoju systemów, tak aby zapewnić, że bezpieczeństwo jest wbudowane w systemy informatyczne.

Dostawca Usługi oddziela systemy produkcyjne od systemów wykorzystywanych w fazie rozwoju i testowania (np. Systemy rozwoju, testowania).

Dostawca Usługi określa również zasady informowania organu nadzoru w przypadku dokonania zmian w świadczeniu Usługi QDS lub skutkujących zmianą Polityki.

10. Monitorowanie

Dostawca Usługi wdrożył procedury związane z monitorowaniem systemów informatycznych oraz infrastruktury sprzętowej dla celów systematycznego pozyskiwania informacji, analizie bieżących oraz przeszłych zdarzeń, tak aby zapewnić odpowiedni poziom zarządzania bezpieczeństwem informacji i podejmowania odpowiednich decyzji w tym zakresie.

Regularne monitorowanie, w tym obserwacja sieci oraz dzienników zdarzeń w systemach informatycznych, jest wspierane przez szereg działań lub narzędzi z zakresu bezpieczeństwa, w szczególności:

a. system wykrywania prób włamań,
b. programy antywirusowe,
c. działania zmierzające do wykrywania podatności na zagrożenia,
d. testy bezpieczeństwa aplikacji (DAST, SAST, testy penetracyjne),
e. systemy bezpieczeństwa sieci – w tym zapory, przełączniki, routery,
f. kontrola dostępu do krytycznych aktywów określonych na podstawie analizy ryzyka, w szczególności:
a. bazy danych,
b. dzienników zdarzeń,
c. nośników przechowujących klucze kryptograficzne,
g. środki bezpieczeństwa fizycznego (np. dostęp do szaf HSM, pomieszczeń o ograniczonym dostępie, serwerownie).

Monitorowaniu podlegają również wszelkie nośniki oraz infrastruktura sprzętowa pod względem ich zużycia, wydajności oraz pojemności.

Dostawca Usługi obsługuje wszelkie krytyczne podatności w zabezpieczeniach, które nie zostały wcześniej obsłużone w ciągu 48 godzin po ich wykryciu.

11. Bezpieczeństwo transmisji oraz sieci

Dostawca Usługi w ramach świadczenia Usługi QDS zapewnia stosowanie odpowiednich zabezpieczeń, które zapewniają bezpieczeństwo transmisji informacji przed ryzykiem utraty, kradzieży, uszkodzenia lub wszelkich nieautoryzowanych zmian.

Dostawca Usługi stosuje w szczególności takie środki bezpieczeństwa jak:

a. segmentacja sieci,
b. zabezpieczenie dostępu do sieci wydzielonych,
c. zabezpieczenie odpowiednich środków kryptograficznych w przesyle (TLS SSL w standardzie nie niższym niż 1.2),
d. stosowanie szyfrowanych połączeń tunelowych (VPN),
e. stosowanie zapór sieciowych (firewall),
f. stosowanie Oprogramowania antywirusowego,
g. działania hardeningowe,
h. redundancja łączy internetowych dla krytycznej infrastruktury sprzętowej lub lokalizacji centrów przetwarzania. (geo-redundancja).

12. Audyty oraz przegląd zarządzania bezpieczeństwem informacji

Dostawca Usługi przeprowadza cykliczne audyty wewnętrzne w oparciu o przyjętą procedurę audytu wewnętrznego oraz zgodnie z przyjętym harmonogramem, a które dotyczą kluczowych procedur oraz procesów związanych z bezpieczeństwem informacji. Maksymalny odstęp między audytami wewnętrznymi pod kątem zmian, które mogą naruszać polityki bezpieczeństwa informacji Autenti wynosi 12 miesięcy.

Dostawca Usługi podlega również pod coroczne audyty przeprowadzone przez firmę zewnętrzną, a które związane są z utrzymaniem certyfikatu zgodności z normą ISO/IEC 27001. Dodatkowo, Dostawca Usług zobowiązany jest do przeprowadzania corocznych audytów oceny zgodności przez zewnętrzną jednostkę oceniającą zgodność z eIDAS oraz standardami ETSI EN 319 401 oraz ETSI EN 319 521.

Audyty są przeprowadzane przez jednostki oceniające zgodność co najmniej raz na 24 miesiące.

Raporty z audytów, zarówno wewnętrznych jak i zewnętrznych są przedkładane Zarządowi Dostawcy Usługi. Raport jednostki oceniającej zgodność z eIDAS oraz standardami ETSI jest przekazywany do organu nadzoru w ciągu trzech dni roboczych od

dnia przekazania go Zarządowi Dostawcy Usługi. Organ nadzoru po analizie raportu z audytu podejmuje decyzję o pozostawieniu lub cofnięciu statusu kwalifikowanego dostawcy wobec Dostawcy Usługi. Na podstawie ocen dokonanych w raportach, Zarząd oraz wyznaczone osoby określają środki i terminy usunięcia wszelkich stwierdzonych niezgodności lub zastrzeżeń.

13. Kopie zapasowe

Dostawca Usługi ustanowił zasady w zakresie wykonywania, przechowywania, testowania oraz odzyskiwania kopii zapasowych informacji oraz systemów informatycznych krytycznych dla Usługi QDS, tak aby zapewnić ich integralność oraz dostępność.

14. Ciągłość działania

Dostawca Usługi opracował, wdrożył i utrzymuje plan ciągłości działania oraz scenariusze postępowania w celu zapewnienia niezbędnego poziomu ciągłości działania i bezpieczeństwa informacji w przypadku wystąpienia zdarzeń niepożądanych.

Dostawca Usługi zapewnia:

a. odpowiednią strukturę zarządzania oraz personel posiadający odpowiednie uprawnienia, doświadczenie i kompetencje w celu przygotowania, złagodzenia i reagowania zdarzenia zakłócające ciągłość działania, w tym zdarzenia o charakterze katastrofy,
b. opracowanie scenariuszy postępowania, opisujących w jaki sposób postępować i zarządzać zdarzeniem niepożądanym, w tym o charakterze katastrofy, tak aby utrzymywać ciągłość działania Usługi QDS oraz informacji lub infrastruktury niezbędnych do jej świadczenia,
c. mechanizmy kontroli bezpieczeństwa informacji w ramach procedur oraz systemów i narzędzi wspierających ciągłość działania, w tym stosowanie ośrodków zapasowych lub nadmiarowość,
d. odzyskiwanie działalności, w tym przywracanie działania Usługi QDS po utracie ciągłości działania.

Dostawca Usługi w regularnych odstępach czasu dokonuje przeglądu stworzonych mechanizmów kontroli ciągłości działania, w celu zapewnienia ich skuteczności i efektywności podczas zdarzeń niepożądanych. Dostawca Usługi regularnie tworzy kopie zapasowe krytycznych aktywów oraz zapewnia możliwość ich odtworzenia z kopii

zapasowej. Mechanizmy odzyskiwania danych są regularnie weryfikowane w celu zapewnienia, że spełniają one wymagania planu ciągłości działania.

Kopie zapasowe niezbędne do przywrócenia działalności Dostawcy Usługi w przypadku incydentu lub katastrofy są utrzymywane i przechowywane w bezpiecznych lokalizacjach. Dostawca Usługi informuje Użytkowników, właściwe organy nadzoru oraz inne zainteresowane strony o wystąpieniu przerw w ciągłości działania oraz poważnych incydentach w działalności związanej ze świadczeniem Usługi QDS.

15. Klucze kryptograficzne niezbędne do świadczenia Usługi QDS

Dostawca Usługi opracował oraz utrzymuje procedury związane z zarządzaniem kluczami kryptograficznymi, tak aby zapewnić bezpieczne generowanie, przechowywanie oraz używanie kluczy kryptograficznych będących pod kontrolą Dostawcy Usługi, od których zależy bezpieczeństwo funkcjonowania Usługi QDS, przez cały cykl ich życia.

Dostawca Usługi generuje Pieczęć elektroniczną, która służy do podpisywania dowodów wystawianych w ramach Usługi QDS. Klucz prywatny certyfikatu Pieczęci elektronicznej jest przechowywany w fizycznie odizolowanym miejscu, do którego ma dostęp wyłącznie upoważniony personel. Klucz prywatny jest przechowywany i używany w bezpiecznym środowisku do wykonywania operacji kryptograficznych (HSM). Klucz prywatny jest przechowywany, przywracany i archiwizowany wyłącznie przez personel pełniący role zaufane w fizycznie bezpiecznym środowisku. Liczba personelu upoważnionego do wykonywania czynności na HSM oraz kluczach kryptograficznych jest ograniczona do niezbędnego minimum.
W celu zabezpieczenia możliwości ciągłego wydawania dowodów przez Dostawcę Usługi z realizacji Usługi QDS oraz podpisywania ich Pieczęcią elektroniczną, w warunkach wystąpienia awarii (urządzeń, mediów, lub mechanizmów komunikacji niezbędnych do użycia urządzeń) zapewnia się redundancję Pieczęci elektronicznych a klucz prywatny potrzebny do nałożenia Pieczęci elektronicznej zabezpiecza się co najmniej dwoma niezależnymi HSM, skonfigurowanych na jeden z dwóch opisanych niżej sposobów:

a. każde HSM chroni odrębną Pieczęć elektroniczną, przy czym wszystkie Pieczęcie elektroniczne potwierdzają tożsamość Dostawcy Usługi i są zarejestrowane na liście zaufanych usług, dzięki czemu dowody opieczętowane dowolną z Pieczęci elektronicznych zachowują ten sam poziom wiarygodności, lub

b. HSM są skonfigurowane jako zespół urządzeń chroniących ten sam klucz prywatny, tj. dla trybu wysokiej dostępności - jeśli urządzenie jest w stanie i jest certyfikowane do działania w takim trybie.

Klucz prywatny certyfikatu Pieczęci elektronicznej może zostać zmieniony w przypadku:

a. wygaśnięcia ważności certyfikatu,
b. zmiany atrybutów prywatności klucza prywatnego i wymogu stosowania nowych s kombinacji kryptograficznych i algorytmów,
c. w przypadku podejrzenia kompromitacji.

W przypadku utraty możliwości zastosowania Pieczęci elektronicznej z innych powodów niż wskazane powyżej, Pieczęć elektroniczną powinna zostać przywrócona poprzez zastosowanie środków technicznych i operacyjnych niewiążących się z wydawaniem nowych Pieczęci elektronicznych, takich jak:

a. przywrócenie kopii zapasowej klucza prywatnego, jeśli HSM umożliwia tworzenie kopii zapasowych materiału klucza prywatnego przy jednoczesnym zachowaniu gwarancji braku możliwości eksportu materiału klucza kryptograficznego w postaci użytkowej poza granicę kwalifikowanej strefy wysokiego bezpieczeństwa,
b. przełączenie na HSM w ośrodku zapasowym, w przypadku wystąpienia awarii lub czasowej niedostępności HSM obecnie funkcjonującego.

16. Rejestracja zdarzeń

Dostawca Usługi przechowuje zapisy dotyczące:

a. zdarzeń związanych z weryfikacją tożsamości Nadawcy i/lub dodatkowym Uwierzytelnianiem,
b. zdarzeń związanych z Identyfikacją Odbiorcy i/lub dodatkowym Uwierzytelnianiem,
c. dokumentację zawierającą dowody przedłożone lub opis przedłożonych dowodów przez osobę, która się Identyfikuje (np. dokument tożsamości, pełnomocnictwo itp.), a także dane dotyczące unikalnych danych identyfikacyjnych, numerów lub ich kombinacji lub kopii wniosków i dokumentów tożsamości, w tym podpisanej umowy na świadczenie Usługi QDS,
d. zdarzeń związanych z wysyłką Zawartości przesyłki i odbiorem e-Przesyłki,
e. zdarzeń związanych z zarządzaniem bezpieczeństwem, w tym zmiany polityki bezpieczeństwa lub innych dokumentów z systemu zarządzania

bezpieczeństwem informacji, informacje o awariach systemu lub awariach sprzętowych, incydentach oraz informacje dotyczące zarządzania kluczami kryptograficznymi,

f. dowody dotyczące realizacji Usługi QDS.

Zdarzenia są rejestrowane w sposób uniemożliwiający ich łatwe usunięcie lub zniszczenie. Dostawca Usługi rejestruje zdarzenia, które mają istotny wpływ na bezpieczeństwo i niezawodność systemu technologicznego, kontrolę pracowników i klientów oraz wpływ na bezpieczeństwo świadczonej Usługi QDS.

Dowody generowane przez Dostawcę Usługi oraz wybrane zdarzenia związane ze świadczeniem Usługi QDS mogą być udostępniane np. jako dowody w postępowaniu sądowym. Dostawca Usługi zapewnia prywatność, integralność i dostępność dzienników zdarzeń. Dzienniki zdarzeń dla systemów informatycznych oraz generowanych dowodów z Usługi QDS, w tym z Identyfikacji, są generowane automatycznie. Dostęp do dzienników zdarzeń jest ograniczony wyłącznie dla upoważnionego personelu Dostawcy Usługi. Po tym okresie rejestry zdarzeń są archiwizowane.

VII. Archiwizacja istotnych zdarzeń

Wymaga się, aby archiwizacji podlegały wszystkie dane i pliki dotyczące rejestrowanych danych o zabezpieczeniach systemu, wnioski napływające od Użytkowników lub Stron Ufających, informacje o Użytkownikach, dowody ze zdarzeń zachodzących w ramach Usługi QDS.

W związku z powyższym, archiwizacji podlegają:

a. dane potwierdzające tożsamość Nadawcy i/lub dodatkowym Uwierzytelnianiem,
b. dane potwierdzające tożsamość Odbiorcy i/lub dodatkowym Uwierzytelnianiem,
c. dokumentacja zawierająca dowody przedłożone lub opis przedłożonych dowodów przez osobę, która się Identyfikuje (np. dokument tożsamości, pełnomocnictwo itp.), a także dane dotyczące unikalnych danych identyfikacyjnych, numerów lub ich kombinacji lub kopii wniosków i dokumentów tożsamości (archiwizowane w postaci elektronicznej),
d. warunki świadczenia usług, w tym przede wszystkim Regulamin Autenti eDelivery oraz Polityka,
e. pozostałe dokumenty związane ze świadczeniem Usługi QDS,

f. zdarzenia związane z zarządzaniem bezpieczeństwem, w tym zmiany polityki bezpieczeństwa lub innych dokumentów z systemu zarządzania bezpieczeństwem informacji, informacje o awariach systemu lub awariach sprzętowych, incydentach oraz informacje dotyczące zarządzania kluczami kryptograficznymi,
g. żądania złożone przez Użytkowników, które są związane z realizacją ich praw, rezygnacji z Usługi QDS lub zastrzeżeń,
h. korespondencja między Dostawcą Usługi, a Użytkownikami lub Stronami Ufającym związana ze świadczeniem Usługi QDS,
i. dowody dotyczące realizacji Usługi QDS, w tym:
    - zdarzenia, które mają miejsce podczas przesyłania danych między Nadawcą a Odbiorcą,
    - dowody z Usługi QDS, potwierdzające że określone zdarzenie związane z procesem przekazywania e-Przesyłki między Nadawcą a Odbiorcą miało miejsce w określonym czasie,
    - tokeny znaczników czasu odpowiadające dacie i godzinie wysłania i przekazania oraz modyfikacji e-Przesyłki, stosownie do przypadku.

Dane wskazane powyżej w pkt od a. do e są przechowywane przez Dostawcę Usług przez okres 20 lat, w tym po zakończeniu działalności Dostawcy Usług lub zaprzestaniu świadczenia Usługi QDS. Pozostałe dane są przechowywane przez okres niezbędny do obrony roszczeń.

Dowody z realizacji Usługi QDS przechowywane są przez 36 miesięcy.

Po upływie przyjętych okresów archiwizacji, dane zostają usunięte lub zniszczone.

Długoterminowe przechowywanie danych odbywa się w bezpiecznym i chronionym środowisku chmurowym. Dostęp do długoterminowo przechowywanych danych mają wyłącznie osoby upoważnione przez Dostawcę Usługi.

VIII. Inne postanowienia

1. Opłaty

Z tytułu świadczonych usług Dostawca Usługi pobiera opłaty, które są określone w cenniku lub indywidualnie uzgodnionej ofercie. Aktualny cennik usług dostępny jest na stronie internetowej www.autenti.com.

2. **Niedyskryminujące zastosowanie**

Praktyki w zakresie Usługi QDS, w ramach których Dostawca Usługi funkcjonuje, są niedyskryminujące.

3. **Odpowiedzialność finansowa**

a. Dostawca Usługi posiada obowiązkowe ubezpieczenie od odpowiedzialności cywilnej, o którym mowa w art. 13 Ustawy o usługach zaufania oraz identyfikacji elektronicznej oraz przepisach wykonawczych. za szkody wyrządzone Użytkownikom Usługi QDS, powstałe w okresie świadczenia Usługi QDS,
b. Odpowiedzialność finansowa Dostawcy Usługi ma zastosowanie wyłącznie wówczas gdy szkoda z tytułu korzystania z Usługi QDS wystąpi z winy Dostawcy Usługi.
c. Dostawca Usługi nie ponosi odpowiedzialności finansowej wobec osób trzecich nie będących Użytkownikami.

4. **Poufność informacji**

Dostawca Usługi zobowiązany jest do zapewnienia oraz przestrzegania poufności wszelkich informacji, w tym danych osobowych oraz treści otrzymanych od Użytkowników w ramach świadczenia Usługi QDS. Do zachowania poufności zobowiązany jest również personel Dostawcy Usług oraz inne podmioty, z którymi Dostawca Usługi współpracuje w związku ze świadczeniem Usługi QDS.

5. **Źródło czasu**

Czas systemowy dla Usługi QDS, używany do rejestrowania momentu zajścia istotnych zdarzeń w dziennikach zdarzeń, oparty jest o czas UTC i synchronizowany ze źródłem czasu UTC nie rzadziej niż dwukrotnie w ciągu doby.

6. **Ochrona danych osobowych**

Dostawca Usługi w zakresie danych osobowych Użytkowników przetwarzanych dla celów realizacji Usługi QDS pełni rolę administratora w rozumieniu RODO.

Jako administrator danych osobowych Dostawca Usługi zobowiązuje się przestrzegać wymogów dotyczących poufności i nieujawniania danych osobowych osób fizycznych,

które przetwarza w ramach wykonywania swojej działalności jako kwalifikowany dostawca usług zaufania.

Dostawca Usługi wdraża odpowiednie środki techniczne i organizacyjne, w tym wdraża odpowiednie polityki uwzględniając charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie i wadze, tak aby przetwarzanie danych osobowych odbywało się zgodnie z RODO. Środki te są w razie potrzeby poddawane przeglądom i uaktualniane.

Dostawca Usługi:

a. stosuje domyślną ochronę danych osobowych ("*privacy by default*") poprzez przetwarzanie tylko takich danych osobowych, które są wymagane lub niezbędne do świadczenia Usługi QDS,
b. uwzględnia ochronę danych w fazie projektowania ("*privacy by design*") Usługi QDS oraz jej zmian,
c. korzysta wyłącznie z takich dostawców, którzy zapewniają odpowiedni poziom ochrony danych osobowych,
d. dopuszcza do przetwarzania danych osobowych wyłącznie taki personel, który został do tego upoważniony,
e. przeprowadza cykliczne szkolenia personelu celem zapewnienia odpowiedniej wiedzy z zakresu ochrony danych osobowych oraz stosowanych przez Dostawcę Usługi procedur i polityk związanych z bezpieczeństwem informacji,
f. wdraża odpowiednie środki techniczne i organizacyjne, aby zapewnić stopień bezpieczeństwa odpowiadający ryzyku, w tym między innymi w stosownym przypadku Dostawca Usługi stosuje:
    - pseudonimizację,
    - szyfrowanie,
    - zdolność do ciągłego zapewnienia poufności, integralności, dostępności i odporności systemów informatycznych,
    - zdolność do szybkiego przywrócenia dostępności danych osobowych i dostępu do nich w razie incydentu fizycznego lub technicznego,
    - regularne testowanie, mierzenie i ocenianie skuteczności wdrożonych środków technicznych i organizacyjnych, mających zapewnić bezpieczeństwo przetwarzania danych osobowych,

g. zapewnia obsługę i realizację praw osób fizycznych, których dane osobowe dotyczą zgodnie z RODO,
h. współpracuje z organem właściwym w sprawie ochrony danych osobowych.

Za nadzór oraz monitorowanie właściwego przestrzegania przepisów prawa dotyczących ochrony danych osobowych u Dostawcy Usługi odpowiada powołany inspektor ochrony danych osobowych, który pełni rolę zaufaną. Dane kontaktowe inspektora ochrony danych osobowych są dostępne na stronie internetowej Dostawcy Usługi oraz w Polityce prywatności.

7. Zobowiązania i gwarancje

a. Zobowiązania i gwarancje Dostawcy Usługi:

Dostawca Usługi świadcząc Usługę Autenti QDS, gwarantuje i zapewnia, że:

- Usługa QDS jest świadczona i oferowana zgodnie z obowiązującymi przepisami prawa,
- stosuje się do zasad określonych w niniejszej Polityce i jej postanowień, a także wskazanych w Polityce przepisów prawa, w tym eIDAS,
- wdrożył i stosuje wskazane w Polityce europejskie normy w obszarze usług zaufania, w tym ETSI EN 319 401 oraz ETSI 319 521 oraz Standard usługi RDE,
- stosuje zadeklarowane w Polityce zabezpieczenia fizyczne, organizacyjne i techniczne oraz korzysta z urządzeń i technologii zapewniające bezpieczeństwo techniczne oraz kryptograficzne przy realizacji objętych nią procesów,
- przetwarza dane osobowe zgodnie z przepisami obowiązującego prawa, w szczególności zgodnie z przepisami 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 oraz dokumentami wykonawczymi do tej ustawy i zapewnia ochronę tych danych zgodnie z tymi regulacjami,
- personel uczestniczący w świadczeniu Usługi posiada wiedzę, doświadczenie i kwalifikacje odpowiednie do pełnienia funkcji

związanych z usługami zaufania oraz przeszedł szkolenie w zakresie bezpieczeństwa i zasad ochrony danych osobowych,
- przeprowadza w sposób cykliczny audyty na zgodność świadczonej Usługi QDS z deklaracją wskazaną w Polityce,
- świadcząc Usługę QDS nie narusza praw własności intelektualnej innych podmiotów,
- zapewnia dostęp do Usługi QDS w trybie ciągłym,, z wyjątkiem następujących przypadków: zaplanowane i wcześniej zapowiedziane przerwy techniczne, naprawy techniczne infrastruktury, nieplanowane naprawy techniczne infrastruktury wynikające z nadzwyczajnych okoliczności, w tym siły wyższej. Dostawca Usługi z wyprzedzeniem udostępnia informacje o planowanych oknach serwisowych, faktycznej niedostępności i zakresie niedostępności,
- odpowiada za działania oraz zaniechania swoich podwykonawców, z których korzysta w ramach świadczenia Usługi QDS oraz za spełnienie przez nich wymogów w zakresie bezpieczeństwa i jakości usługi, zgodnie z Rozdziałem VI ust. 6 Polityki.
- nie ingeruje w treść Zawartości przesyłki oraz e-Przesyłki w trakcie świadczenia Usługi QDS.

8. Zobowiązania Użytkowników:

Użytkownik zobowiązany jest do:

a. zapoznania się i akceptacji Polityki przed rozpoczęciem korzystania z Usługi QDS,
b. przestrzegania warunków i zasad świadczonej przez Dostawcę Usług Usługi QDS określonych w Regulaminie Autenti eDelivery i Regulaminie Platformy Autenti,
c. podawania prawdziwych i niewprowadzających w błąd danych, danych osobowych, aktualnych dokumentów oraz składania prawdziwych oświadczeń,
d. korzystania z Usługi QDS w celach zgodnych z przepisami prawa i nie naruszających dobrych obyczajów,
e. przechowywania lub używania danych dostępowych do Usługi QDS w sposób zapewniający ich ochronę przed nieuprawnionym wykorzystaniem,

f. w odniesieniu do Usługi QDS realizowanej w zakresie współpracy z publiczną usługą rejestrowanego doręczenia elektronicznego, Użytkownicy Usługi QDS zobowiązani są do akceptacji przyjmowania notyfikacji o gotowości e-Przesyłki do odbioru,
g. w odniesieniu do Usługi QDS realizowanej w zakresie współpracy z publiczną usługą rejestrowanego doręczenia elektronicznego, Użytkownicy są zobowiązani do powiadamiania Dostawcy Usługi o utracie dostępu do Usługi QDS lub zmianie zadeklarowanego sposobu notyfikacji.

9. Zobowiązania Stron Ufających

Strona Ufająca zobowiązana jest do zgłaszania Dostawcy Usług wszelkich zastrzeżeń oraz nadużyć w zakresie dowodów lub innych informacji, które otrzymała, a które dotyczą zrealizowanej Usługi QDS. Zgłoszenia należy dokonać za pomocą formularza kontaktowego, poczty elektronicznej na adres: support@autenti.com lub pisemnie na adres: Autenti S.A., ul. Święty Marcin 29/8, 61-806 Poznań.

10. Ograniczenie odpowiedzialności

a. Dostawca Usługi nie odpowiada za szkody wynikające z nieprzestrzegania przez Użytkownika zobowiązań wskazanych w Polityce oraz zasad określonych w Regulaminie Autenti eDelivery i Regulaminie Platformy Autenti, w szczególności za szkody wynikające z:
    - podania nieaktualnych, nieprawdziwych, niepoprawnych lub wprowadzających w błąd danych lub informacji, w tym danych osobowych lub Adresu do doręczeń elektronicznych Odbiorcy, ani jego zdolności do czynności prawnych, w tym również przesłania treści nieprzeznaczonej do Odbiorcy,
    - przechowywania przez Użytkownika danych dostępowych do Usługi QDS w sposób nie zapewniający ich ochrony przed nieuprawnionym dostęp i ich wykorzystaniem,
    - użycia danych dostępowych do Usługi QDS przez osoby nieuprawnione, wskutek działania lub zaniechania Użytkownika (m.in. braku ochrony haseł dostępowych),
    - korzystania przez Użytkownika z Usługi QDS w sposób niezgodny z postanowieniami Regulaminu Autenti eDelivery, odnoszącymi się do wymagań technicznych dla systemu teleinformatycznego.

- z braku odbioru notyfikacji za pomocą zadeklarowanego mechanizmu notyfikowania, w tym nie poinformowania Dostawcy Usługi o utracie dostępu lub zmianę zadeklarowanego mechanizmu notyfikacji.

b. Dostawca Usługi nie ponosi odpowiedzialności za niedostępność Usługi QDS z powodu braku dostępności bazy BAE, Operatora Wyznaczonego lub innego dostawcy usług niezależnego od Dostawcy Usługi, biorącego udział w procesie doręczenia e-Przesyłki.
c. Dostawca Usługi nie ponosi odpowiedzialności za szkody powstałe w skutek zdarzenia o charakterze siły wyższej.
d. Dostawca Usług nie ponosi odpowiedzialności za szkody powstałe w wyniku korzystania z Usługi QDS w zakresie w jakim Użytkownicy zostali wcześniej poinformowani o ograniczeniach w świadczeniu Usługi QDS.
e. Dostawca Usługi nie ponosi odpowiedzialności za zachowania Użytkowników lub osób trzecich, ani za nienależyte wykonanie bądź niewykonanie przez nich czynności faktycznych bądź prawnych w związku z e-Przesyłką przetwarzaną w ramach Usługi QDS, jak również nie ponosi odpowiedzialności za następstwa działań podjętych przez Użytkowników oraz osoby trzecie, a stanowiących naruszenie postanowień Polityki lub Regulaminu Autenti eDelivery lub przepisów prawa. W szczególności Dostawca Usług nie ponosi odpowiedzialności za skutki prawne nie doręczenia e-Przesyłki, w przypadku, jeżeli jest to wynikiem działań bądź zaniechań Użytkowników lub osób trzecich.
f. Dostawca Usługi nie ponosi odpowiedzialności za skutki niewłaściwego lub niezgodnego z prawem lub wewnętrznymi procedurami lub zasadami obowiązującymi u Użytkownika nadania uprawnień, o których mowa w rozdziale III ust 4 Polityki.
g. Dostawca Usługi nie odpowiada za szkody wynikające z nieprzestrzegania przez Użytkownika przepisów prawa, w szczególności za szkody wynikające z korzystania z Usługi QDS niezgodnie z jej przeznaczeniem lub w celu naruszenia przepisów prawa.
h. Dostawca Usługi nie odpowiada za brak pełnej zgodności Usługi QDS z usługami innych dostawców kwalifikowanej usługi doręczenia elektronicznego oraz Operatora Wyznaczonego, w ramach interoperacyjności, w szczególności w wyniku dokonania przez tych dostawców zmian funkcjonalnych.

i. O ile z powszechnie obowiązujących przepisów prawa nie wynika nic innego, odpowiedzialność Dostawcy Usługi wobec Użytkowników ograniczona jest wyłącznie do szkód rzeczywistych wyrządzonych umyślnie lub z powodu rażącego zaniedbania.

11. Odszkodowania

Odszkodowania z tytułu odpowiedzialności cywilnej wobec Użytkowników wynikają z zobowiązań oraz gwarancji określonych w Polityce.

12. Dostawcy usług zaufania zaangażowani w świadczenie Usługi QDS

a. Wystawca Pieczęci elektronicznej, służącej do podpisywania dowodów i identyfikacji Dostawcy Usług w ramach realizacji Usługi QDS,
b. Kwalifikowany dostawca usług zaufania Znacznika czasu,
c. Inni dostawcy kwalifikowanej usługi rejestrowanego doręczenia elektronicznego według listy zaufanej.

Pełna i aktualna lista dostawców usług zaufania zaangażowanych w świadczenie Usługi QDS, o których mowa powyżej, dostępna jest na stronie internetowej Dostawcy Usług.

IX. Warunki rozstrzygania sporów, reklamacje, wątpliwości

1. Użytkownik może złożyć reklamację, jeżeli Usługa QDS opisana w niniejszej Polityce nie jest realizowana przez Dostawcę Usługi lub jest realizowana niezgodnie z Polityką.
2. Reklamację można złożyć w postaci elektronicznej za pomocą formularza kontaktowego, poczty elektronicznej na adres: support@autenti.com lub pisemnie na adres: Autenti S.A., ul. Święty Marcin 29/8, 61-806 Poznań. Reklamacja powinna zawierać co najmniej adres e-mail, opis zgłaszanych zastrzeżeń oraz oczekiwany sposób rozstrzygnięcia sprawy.
3. Jeżeli podane w reklamacji dane lub informacje wymagają uzupełnienia, dla prawidłowego rozpatrzenia reklamacji i uczynienia zadość żądaniu Użytkownika, przed rozpatrzeniem reklamacji Dostawca Usługi zwróci się do składającego reklamację o jej uzupełnienie we wskazanym zakresie i terminie. Bezskuteczny upływ terminu powoduje, że reklamacja nie może zostać rozpatrzona i podlega oddaleniu. Czynność wezwania Użytkownika do uzupełnienia reklamacji przerywa bieg terminu do jej rozpatrzenia. Postanowienie to nie uchybia przepisom prawa

bezwzględnie obowiązującym w zakresie, w jakim przyznają one konsumentom szerszą ochronę.

4. Dostawca Usługi rozpoznaje reklamację w terminie 14 dni od daty jej otrzymania w prawidłowej postaci, z zastrzeżeniem, że odmawia uznania reklamacji złożonych po upływie 90 dni od ujawnienia się przyczyn reklamacji.
5. Odpowiedź na reklamację wysyłana jest wyłącznie na adres e-mail wskazany przez danego Użytkownika.
6. Strona Ufająca może zgłosić wątpliwości dotyczące wykonania Usługi QDS do Dostawcy Usługi. Zgłoszenie może być dokonane pisemnie, drogą poczty elektronicznej na adres: support@autenti.com lub poprzez formularz kontaktowy udostępniony w domenie autenti.com.
7. Prawem właściwym dla umów zawieranych pomiędzy Użytkownikiem a Dostawcą Usługi, których przedmiotem jest Usługa QDS opisana w niniejszej Polityce, jest prawo polskie, o ile prawo w Unii Europejskiej w odniesieniu do konsumenta nie przewiduje innej właściwości. W przypadku niezadowalającego Użytkownika postępowania reklamacyjnego spory związane z Usługą QDS świadczoną przez Dostawcę Usługi mogą być rozstrzygane przez właściwe sądy powszechne.

X. Zakończenie działalności lub zaprzestanie świadczenia Usługi QDS

1. Dostawca Usługi dołoży wszelkich starań mających na celu zminimalizowanie negatywnych skutków podjęcia potencjalnej decyzji o zakończeniu świadczenia Usługi QDS lub zakończeniu działalności.
2. W tym celu Dostawca Usługi z odpowiednim wyprzedzeniem poinformuje o tym fakcie organ nadzoru, Użytkowników, na rzecz których Usługa QDS jest świadczona oraz inne podmioty, z którymi Dostawca Usługi ma zawarte umowy, jeżeli jest to wymagane.
3. Po podjęciu decyzji o zakończeniu działalności, Dostawca Usługi zobowiązany jest do:
    a. postępowania zgodnie z aktualnym planem zakończenia działalności lub zaprzestania świadczenia Usługi QDS,
    b. informowania Użytkowników, organu nadzoru i stron trzecich o zakończeniu działalności lub zaprzestania świadczenia Usługi QDS. Informacje są przekazywane pocztą elektroniczną lub poprzez zamieszczenie na stronie internetowej Dostawcy Usługi,
    c. wycofania wszelkich upoważnień do wykonywania czynności związanych z Usługą QDS, w tym do przeprowadzania procesu weryfikacji tożsamości,

d. przed zakończeniem działalności lub przed zakończeniem świadczenia Usługi QDS, w rozsądnym terminie, przenieść swoje obowiązki w zakresie przechowywania wszystkich informacji, które są niezbędne do dostarczenia dowodów, na wiarygodną stronę,
e. przed zakończeniem działalności lub w dniu zaprzestania świadczenia Usługi QDS zniszczyć lub usunąć z użycia w sposób uniemożliwiający odzyskanie wszelkie klucze kryptograficzne służące do świadczenia Usługi QDS, w tym ich kopie zapasowe,
f. zobowiązuje się do udostępnienia klucza publicznego stronom ufającym,
g. jeśli to możliwe, przekazać swoją działalność innemu kwalifikowanemu dostawcy usługi doręczenia elektronicznego,
h. podjęcia wszelkich uzasadnionych wysiłków w celu zminimalizowania zakłócenia interesów konsumentów.
i. przechowywania lub przekazania przechowywania innej stronie dowodów z Usługi QDS, celem ich udostępniania przez czas wymagany Polityką lub przepisami prawa.

Szczegółowy sposób postępowania w przypadku podjęcia decyzji o zakończeniu działalności Dostawcy Usług lub zakończeniu świadczenia Usługi QDS przez Dostawcę Usług, zostanie określony szczegółowym planem zakończenia działalności, zatwierdzonym przez Zarząd. Szczegółowy plan zakończenia działalności zostanie przedstawiony organowi nadzoru oraz pozostałym zainteresowanym stronom, w tym przede wszystkim Użytkownikom.

Dostawca Usługi zapewnia odpowiednie środki na pokrycie kosztów w przypadku ogłoszenia upadłości lub z innych powodów zakończenia działalności. W przypadku, gdy nie jest w stanie samodzielnie pokryć kosztów, Dostawca Usługi przewiduje środki w ramach obowiązujących przepisów prawa.

XI. Obowiązywanie i procedura wprowadzania zmian

1. Niniejsza Polityka obowiązuje przez czas nieokreślony.
2. Każda zmiana treści Polityki obowiązuje po upływie co najmniej 7 dni od dnia jej publikacji w repozytorium Autenti lub późniejszej daty wskazanej w zaktualizowanej treści Polityki, zgodnie z przyjętą u Dostawcy Usługi procedurą. Autenti każdorazowo powiadamia Użytkowników o zakresie zmian oraz czasie, w którym zaczną one obowiązywać.

3. Poza cyklicznymi audytami na zgodność świadczonej usługi z deklaracją wskazaną w Polityce, Dostawca Usługi raz w roku dokonuje przeglądu obowiązującej wersji Polityki pod kątem jej zgodności z wdrożonymi procedurami wewnętrznymi Dostawcy Usługi oraz wymaganiami przepisów prawa, norm i standardów.
4. Zmiany w Polityce mogą być wynikiem zauważonych błędów, uaktualnień oraz sugestii zainteresowanych stron. Propozycje zmian do aktualnej wersji Polityki mogą wnieść strony zainteresowane, w tym m.in. wszystkie strony Usługi QDS oraz organy państwowe.
5. Propozycje zmian można złożyć w postaci elektronicznej za pomocą formularza kontaktowego, poczty elektronicznej na adres: support@autenti.com lub pisemnie na adres: Autenti S.A., ul. Święty Marcin 29/8, 61-806 Poznań. Propozycja zmian powinna zawierać co najmniej adres e-mail, uzasadnienie i opis zgłaszanych zastrzeżeń oraz ich zakres.
6. W przypadku zmian, które nie mają znaczącego wpływu na treść Polityki, takich jak: zmiana adresu kontaktowego osoby odpowiedzialnej za zarządzanie dokumentem oraz poprawa błędów redakcyjnych (korekta edycyjna), Dostawca Usługi zastrzega sobie prawo do wprowadzania tych zmian bez wcześniejszego informowania stron.
7. W przypadku pozostałych zmian, informacja o zmianie dotychczasowej wersji Polityki publikowana jest w repozytorium, o którym mowa w rozdziale II Polityki.

HISTORIA ZMIAN

Wersja	Data	Opis działania	Działanie*	Wykonawca działania
1.0	25.10.2023	Przyjęcie dokumentu Uchwałą Zarządu	N/P	Zarząd
1.1	22.11.2024	Przyjęcie dokumentu uchwałą Zarządu	Z/P	Zarząd
1.2	31.07.2026	Przyjęcie dokumentu uchwałą Zarządu - zmiana dotycząca aktualizacji danych Dostawcy Usług	Z/P	Zarząd

(*) Działanie: N-Nowy, Z-Zmiana, W-Weryfikacja, P- przyjęcie / zatwierdzenie