Polityka oraz deklaracja postępowania dla Kwalifikowanej Usługi Walidacji podpisów i pieczęci elektronicznych

Numer dokumentu	TSP - 003
Identyfikator dokumentu	OID: [1.2.616.1.113813.1.4.2.1.1]
Klasyfikacja dokumentu	publiczne
Właściciel dokumentu	Autenti S.A. (“Autenti”) ul. Święty Marcin 29/8, 61-806 Poznań KRS: 0001254852, NIP: 7831693251, REGON: 302246285
Wersja	Wersja nr 1.1

Spis treści

I. Postanowienia ogólne **4**
1. Wprowadzenie 4
2. Identyfikacja Dostawcy Usługi 4
3. Nazwa dokumentu oraz jego identyfikacja 4
II. Definicje i skróty **5**
III. Regulacje prawne oraz zgodność z normami **8**
1. Prawo powszechnie obowiązujące 8
2. Wzorce umowne i deklaracje praktyk 8
3. Normy 9
IV. Wstęp do Usługi oraz opis jej komponentów **9**
1. Opis Usługi 9
2. Uczestnicy Usługi Walidacji 10
3. Usługa Walidacji Kwalifikowanych Podpisów Elektronicznych oraz Kwalifikowanych Pieczęci Elektronicznych 11
4. Usługa Walidacji zaawansowanych podpisów elektronicznych oraz zaawansowanych pieczęci elektronicznych opartych o kwalifikowane certyfikaty 12
5. Usługa Walidacji e-Podpisu Autenti oraz Zaawansowanego e-Podpisu Autenti 13
V. Opis Usługi Walidacji **14**
1. Komponenty **14**
2. Interfejs i zasady świadczenia Usługi Walidacji 15
3. Proces walidacji oraz kryteria walidacji 15
2. Wskaźniki Walidacji 17
4. Raport Walidacji oraz Poświadczenie Walidacji 25
VI. Zarządzanie bezpieczeństwem **27**
1. Bezpieczeństwo organizacyjne 27
2. Dostęp fizyczny 27
3. Dostęp do systemów informatycznych 28
4. Zarządzanie incydentami 28
5. Personel Dostawcy Usługi 30
6. Zarządzanie dostawcami 30
7. Zarządzanie aktywami 31
8. Zarządzanie ryzykiem 31
9. Zarządzanie zmianą 32
10. Monitorowanie 32
11. Bezpieczeństwo transmisji oraz sieci 33

12. Audyty oraz przeglądu zarządzania bezpieczeństwem informacji 34
13. Kopie zapasowe 34
14. Ciągłość działania 35
15. Klucze kryptograficzne 35
16. Rejestracja zdarzeń 36
VII. Zakończenie działalności lub zaprzestanie świadczenia Usługi Walidacji 37
VIII. Warunki rozstrzygania sporów, reklamacje, wątpliwości 38
IX. Zarządzanie Polityką i jej zmiany 39
X. Mapowanie zgodności z wymogami Rozporządzenia eIDAS 39
HISTORIA ZMIAN 41

I. Postanowienia ogólne

1. Wprowadzenie

Niniejsza Polityka oraz deklaracja postępowania określa ogólne zasady oraz zbiór reguł świadczenia przez Autenti S.A., kwalifikowanej usługi zaufania walidacji certyfikatów podpisów oraz pieczęci elektronicznych (ang. Qualified Validation Service) w rozumieniu oraz zgodnie z art. 33 i 34 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 wraz z aktami wykonawczymi oraz właściwymi normami technicznymi wydanymi przez Europejski Instytut Norm Telekomunikacyjnych (ETSI), a także deklarację praktyk Autenti S.A. w tym zakresie.

2. Identyfikacja Dostawcy Usługi

Dostawcą kwalifikowanej usługi zaufania walidacji certyfikatów podpisów i pieczęci elektronicznych jest Autenti S.A. z siedzibą w Poznaniu, ul. Święty Marcin 29/8. Dostawca Usługi jest wpisany na listę dostawców usług kwalifikowanych prowadzoną przez Narodowe Centrum Certyfikacji oraz listę udostępnioną przez Komisję Europejską "Trusted List" pod adresem https://eidas.ec.europa.eu/efda/trust-services/browse/eidas/tls/tl/PL.

Dostawca Usługi świadczy również inne kwalifikowane i niekwalifikowane usługi zaufania zgodnie z eIDAS, w tym podpisy elektroniczne oraz rejestrowane doręczenia elektroniczne. Zasady świadczenia tych usług są opisane w odrębnych właściwych dla usług politykach i regulaminach. Usługi zaufania Dostawcy Usług są udostępniane za pośrednictwem Platformy Autenti.

3. Nazwa dokumentu oraz jego identyfikacja

Niniejszy dokument posiada nazwę własną "**Polityka oraz deklaracja postępowania dla Kwalifikowanej Usługi Walidacji podpisów i pieczęci elektronicznych",** w skrócie nazywana na potrzeby niniejszego dokumentu "Polityką".

Aktualna wersja Polityki oraz jej archiwalne wersje są udostępniane przez Dostawcę Usług w repozytorium, dostępnym na stronie internetowej pod adresem www.autenti.com/regulaminy.

Polityka posiada przypisany unikalny numer identyfikacyjny OID: 1.2.616.1.113813.1.4.2.1.x.x.

Dwie ostatnie cyfry numeru OID wskazują na wersję dokumentu.

Zasady zarządzania Polityką w tym dokonywanie i publikowanie jej zmian zostało określone w Rozdziale IX poniżej.

II. Definicje i skróty

1. Polityka posługuje się pojęciami, którym nadaje się następujące znaczenie:
   a. **Dane Walidacyjne** - oznaczają dane używane do walidacji podpisu lub pieczęci elektronicznej, w tym m.in. certyfikaty, informacje o unieważnieniu, atrybuty podpisu, znaczniki czasu oraz odpowiednie parametry kryptograficzne,
   b. **Dokument –** oznacza plik elektroniczny, zawierający certyfikaty podpisów elektronicznych lub pieczęci elektronicznych będących przedmiotem Usługi Walidacji,
   c. **Dostawca Usługi** - Autenti spółka akcyjna, świadcząca Usługę Walidacji zgodnie z Polityką oraz Regulaminem Walidacji,
   d. **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,
   e. **e-Podpis Autenti –** podpis elektroniczny (SES), stanowiący dane w postaci elektronicznej, które są dołączone lub logicznie powiązane z innymi danymi w postaci elektronicznej i które użyte są przez podpisującego jako podpis. Zasady świadczenia usługi opisuje dedykowana polityka Dostawcy Usług,
   f. **Zaawansowany e-Podpis Autenti –** zaawansowany podpis elektroniczny spełniający wymagania art 26 eIDAS, składany przy wykorzystaniu Platformy Autenti. Zasady świadczenia usługi opisuje dedykowana polityka Dostawcy Usług,
   g. **Kwalifikowany Certyfikat Podpisu –** Certyfikat podpisu elektronicznego wydany przez kwalifikowanego dostawcę usług zaufania i spełniający wymagania określone w załączniku I eIDAS,
   h. **Kwalifikowany Certyfikat Pieczęci –** Certyfikat pieczęci elektronicznej, wydany przez kwalifikowanego dostawcę usług zaufania i spełniający wymagania określone w załączniku III eIDAS,
   i. **Kwalifikowana Pieczęć Elektroniczna** - Zaawansowana pieczęć elektroniczna, która jest tworzona przez kwalifikowane urządzenie do tworzenia pieczęci elektronicznych i opiera się na Kwalifikowanym Certyfikacie Pieczęci elektronicznej, wydawanym zgodnie z wymogami eIDAS,

j. **Kwalifikowany Podpis Elektroniczny** - Zaawansowany podpis elektroniczny, który jest tworzony przez kwalifikowane urządzenie do tworzenia podpisów elektronicznych i opiera się na Kwalifikowanym Certyfikacie Podpisu elektronicznych, wydawanym zgodnie z wymogami eIDAS,

k. **Kwalifikowana Usługa Zaufania** - usługa zaufania, która spełnia odpowiednie wymagania określone eIDAS oraz jest świadczone przez kwalifikowanego dostawcę usług zaufania, wpisanego na europejską listę dostawców (Trusted List),

l. **Kwalifikowany Znacznik Czasu** - Kwalifikowana Usługa Zaufania spełniająca wymogi art. 42 eIDAS, korzystająca z domniemania dokładności daty i czasu, jakie wskazuje, oraz integralności danych, z którymi wskazywane data i czas są połączone,

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

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

o. **Polityka** - niniejsza Polityka oraz deklaracja postępowania dla Kwalifikowanej Usługi Walidacji,

p. **Poświadczenie Walidacji** - szczegółowy raport generowany przez Dostawcę Usługi po wykonaniu Usługi Walidacji, będący dokumentem towarzyszącym do Raportu Walidacji, prezentujący jej wynik w sposób możliwy do odczytu przez człowieka w formacie PDF,

q. **Raport Walidacji -** szczegółowy raport generowany przez Dostawcę Usługi po wykonaniu Usługi Walidacji, prezentujący jej wynik w formacie XML.

r. **Repozytorium -** strona internetowa Dostawcy Usług, dostępna pod adresem www.autenti.com/regulaminy, w ramach której udostępniane są aktualnie obowiązujące oraz archiwalne wersje Polityki, polityki innych usług oraz regulaminy.

s. **Regulamin Usługi Walidacji -** regulamin świadczenia usług drogą elektroniczną, regulujący korzystanie z Usługi Walidacji, którego treść dostępna jest na stronie internetowej Dostawcy Usług,

t. **Regulamin Platformy Autenti** – regulamin świadczenia usług drogą elektroniczną, regulujący korzystanie z Platformy Autenti, którego treść dostępna jest w Repozytorium.

u. **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 Walidacji,

v. **Usługa Walidacji** - Kwalifikowana usługa walidacji certyfikatów podpisów i pieczęci elektronicznych świadczona przez Dostawcę Usługi, polegająca na realizacji procesu weryfikacji i potwierdzania ważności podpisu elektronicznego lub pieczęci,

w. **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, która zawarła z Dostawcą Usługi umowę na świadczenie Usługi Walidacji. Użytkownik może być również Stroną Ufającą,

x. **Wskaźnik Walidacji -** jeden z następujących wyników Usługi Walidacji – WAŻNY (VALID - CAŁKOWICIE ZALICZONY), NIEWAŻNY (INVALID - CAŁKOWICIE NIEZALICZONY) lub NIEOKREŚLONY (INDETERMINATE - NIEPEWNY).

2. Polityka może posługiwać się skrótami, którym nadaje się następujące znaczenie:

a. **API** - Interfejs oprogramowania (ang. Application Program Interface),
b. **CA** - Urząd certyfikacji (ang. Certificate Authority),
c. **CAdES** - CMS Advanced Electronic Signatures [ETSI 101 733]
d. **CMS** - Cryptographic Message Syntax [RFC5652]
e. **CRL** - Lista certyfikatów unieważnionych
f. **ETSI** - Europejski Instytut Norm Telekomunikacyjnych
g. **GUI** - Graficzny interfejs użytkownika (ang. graphical user interface)
h. **OCSP** - Online Certificate Status Protocol [RFC2560]
i. **PDF** - Przenośny format dokumentu [PDF]
j. **PAdES** - PDF Advanced Electronic Signatures [ETSI 102 778]
k. **PKI** - Infrastruktura klucza publicznego
l. **PoE** - Dowód istnienia (ang. Proof of Existence)
m. **TLS** - Transport Layer Security [RFC4346]
n. **XAdES** - XML Advanced Electronic Signatures [ETSI 101 933]

III. Regulacje prawne oraz zgodność z normami

1. Prawo powszechnie obowiązujące

Dostawca Usługi świadczy Usługę Walidacji w oparciu o lub z uwzględnieniem przepisów 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 oraz zmieniającymi), 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, zwanym dalej "**RODO**",
c. Decyzja wykonawcza Komisji (UE) 2015/1506 z dnia 8 września 2015 r. ustanawiająca specyfikacje dotyczące formatów zaawansowanych podpisów elektronicznych oraz zaawansowanych pieczęci elektronicznych, które mają być uznane przez podmioty sektora publicznego, zgodnie z art. 27 ust. 5 i art. 37 ust. 5 rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 910/2014 w sprawie identyfikacji elektronicznej i usług zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznym (Dz. U. UE. L. z 2015 r. Nr 235, str. 37).

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

a. Ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych,
b. Ustawa z dnia 5 września 2016 r. o usługach zaufania oraz identyfikacji elektronicznej (łącznie z przepisami wykonawczymi),
c. Ustawa z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną.

2. Wzorce umowne i deklaracje praktyk

Dostawca Usługi świadczy Usługę Walidacji zgodnie niniejszą Polityką oraz w oparciu wzorce umowne (regulaminy lub polityki) udostępniane przez Dostawcę Usługi, w tym:

a. Regulamin Usługi Walidacji,
b. Regulamin Platformy Autenti,
c. Politykę Ochrony Prywatności,
d. Politykę Cookies,
e. Politykę Usług Zaufania Autenti dla podpisów elektronicznych Autenti oraz obsługi podpisywania dokumentów,

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

3. **Normy**

Dostawca Usługi świadczy Usługę Walidacji w zgodności z takimi normami referencyjnymi 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 TS 119 441 Electronic Signatures and Infrastructures (ESI); Policy requirements for TSP providing signature validation services - która definiuje m.in. wymagania techniczne i organizacyjne dla dostawców kwalifikowanej usługi walidacji,
c. ETSI EN 319 102-1 Procedures for Creation and Validation of AdES Digital Signatures; Part 1: Creation and Validation,
d. ETSI TS 119 102-2 Procedures for Creation and Validation of AdES Digital Signatures; Part 2: Signature Validation Report,
e. ETSI TS 119 442 Electronic Signatures and Infrastructures (ESI); Protocol profiles for trust service providers providing AdES digital signature validation services,
f. ETSI TS 119 101 Electronic Signatures and Infrastructures (ESI); Policy and security requirements for applications for signature creation and signature validation,
g. ETSI TS 119 172-4 Electronic Signatures and Infrastructures (ESI); Signature Policies; Signature applicability rules (validation policy) for European qualified electronic signatures/seals using trusted lists,
h. RFC 6960 X.509 Internet Public Key Infrastructure Online Certificate Status Protocol – OCSP.

IV. Wstęp do Usługi oraz opis jej komponentów

1. **Opis Usługi**

Kwalifikowana usługa walidacji certyfikatów podpisów i pieczęci elektronicznych (“Usługa Walidacji”) jest udostępniana przez Dostawcę Usług w ramach ekosystemu usług zaufania i identyfikacji elektronicznej dostępnych za pośrednictwem Platformy Autenti. Z Usługi Walidacji można korzystać na warunkach opisanych w Regulaminie Platformy Autenti i Regulaminie Usługi Walidacji, dostępnych w Repozytorium na stronie internetowej Dostawcy Usług www.autenti.com/regulaminy.

Usługa Walidacji umożliwia potwierdzenie ważności:

a. e-Podpisu Autenti,
b. Zaawansowanego e-Podpisu Autenti,
c. Kwalifikowanego Podpisu elektronicznego,
d. Kwalifikowanej Pieczęci Elektronicznej,
e. zaawansowanej pieczęci elektronicznej opartej o Kwalifikowany Certyfikat Pieczęci,
f. zaawansowanego podpisu elektronicznego opartego o Kwalifikowany Certyfikat Podpisu.

Przepisy ustanowione przez Unię Europejską opisują ramy prawne i operacyjne dla dostawców kwalifikowanej usługi walidacji certyfikatów, których przestrzeganie pozwala dostawcy uzyskać status "Kwalifikowanego dostawcy usług walidacji", a jego usługę uznać za "Kwalifikowaną usługę walidacji certyfikatów podpisów i pieczęci elektronicznych". Kwalifikowane usługi walidacji korzystają z domniemań opisanych w art. 32 Rozporządzenia eIDAS, a zatem nie wymagają dalszych dowodów, aby wykazać ważność Kwalifikowanego Certyfikatu Podpisu lub Kwalifikowanego Certyfikatu Pieczęci.

Usługa Walidacji przeznaczona jest dla osób fizycznych oraz prawnych, które chcą potwierdzić ważność złożonych w dokumencie Kwalifikowanych Certyfikatów Podpisów lub Kwalifikowanych Certyfikatów Pieczęci.

Usługa, w zakresie w jakim jest to możliwe, dostosowana jest również dla osób z niepełnosprawnościami.

2. Uczestnicy Usługi Walidacji

Uczestnikami Usługi Walidacji są:

a. Dostawca Usługi, świadcząc Usługę Walidacji lub świadcząc usługę e-Podpisu Autenti lub Zaawansowanego e-Podpisu Autenti,
b. Użytkownik korzystający z Usługi Walidacji,
c. Osoba, które złożyła podpis elektroniczny, jeżeli zastosowała ograniczenia w zakresie składanego podpisu elektronicznego, co może mieć wpływ na wynik Usługi Walidacji,
d. Podmiot, który złożył pieczęć elektroniczną, jeżeli zastosowane ograniczenia w zakresie składanej pieczęci elektronicznej, co może mieć wpływ na wynik Usługi Walidacji,
e. kwalifikowani dostawcy usług zaufania, wydający Kwalifikowane Certyfikaty Podpisu lub Kwalifikowane Certyfikaty Pieczęci,

f. kwalifikowany dostawca sług zaufania dostarczający i utrzymujący w imieniu podpisującego urządzenia do składania Kwalifikowanego Certyfikatu Podpisu lub Kwalifikowanego Certyfikatu Pieczęci,
g. kwalifikowany dostawca usług zaufania generujący Kwalifikowane Certyfikaty Podpisu lub Kwalifikowane Certyfikaty Pieczęci,
h. kwalifikowany dostawca usług zaufania, wydający Kwalifikowane Znaczniki Czasu powiązane ze złożonym podpisem lub pieczęcią elektroniczną,
i. Narodowe Centrum Certyfikacji, prowadzące polską listę dostawców usług zaufania,
j. Komisja Europejska, prowadzącą europejską listę dostawców usług zaufania (Trusted List).

3. **Usługa Walidacji Kwalifikowanych Podpisów Elektronicznych oraz Kwalifikowanych Pieczęci Elektronicznych**

Usługa Walidacji pozwala potwierdzić ważność Kwalifikowanego Podpisu Elektronicznego oraz Kwalifikowanej Pieczęci Elektronicznej w przypadku, gdy:

a. Kwalifikowany Certyfikat Podpisu lub Kwalifikowany Certyfikat Pieczęci, w momencie podpisywania był kwalifikowany zgodnie z załącznikiem 1 eIDAS,
b. Kwalifikowany Certyfikat Pieczęci lub Kwalifikowany Certyfikat Podpisu został wydany przez kwalifikowanego dostawcę usług zaufania i był ważny w momencie podpisywania,
c. Dane Walidacyjne Kwalifikowanego Podpisu Elektronicznego oraz Kwalifikowanej Pieczęci Elektronicznej odpowiadają danym przekazanym Stronie Ufającej,
d. unikalny zestaw danych reprezentujących podpisującego w Kwalifikowanym Certyfikacie Podpisu lub Kwalifikowanym Certyfikacie Pieczęci jest prawidłowy,
e. użycie pseudonimu jest wyraźnie wskazane Stronie Ufającej,
f. Kwalifikowany Podpis Elektroniczny lub Kwalifikowana Pieczęć Elektroniczna zostały utworzone przez kwalifikowane urządzenie do tworzenia Kwalifikowanych Certyfikatów Podpisu lub Kwalifikowanych Certyfikatów Pieczęci;
g. integralność podpisanych danych nie została naruszona,
h. w momencie podpisywania spełnione są wymagania dotyczące zaawansowanego podpisu elektronicznego (art. 26 eIDAS).

Usługa Walidacji umożliwia Stronom Ufającym otrzymanie Raportu Walidacji oraz Poświadczenia Walidacji w sposób zautomatyzowany, wraz ze Wskaźnikiem Walidacji, który jest wiarygodny i dokładny, oraz opatrzony Pieczęcią Elektroniczną Dostawcy Usługi. Ponadto, w przypadku korzystania z GUI, Użytkownik otrzymuje również skróconą informację o rezultacie Usługi Walidacji.

Usługa Walidacji weryfikuje techniczną ważność i poprawność ich certyfikatów, zgodnie z wymogami wskazanymi powyżej. Techniczna ważność jest sprawdzana zgodnie z procesem opisanym w ETSI TS 319 102-1 oraz potwierdzona poprzez podpisanie Raportu Walidacji oraz Poświadczenia Walidacji Pieczęcią Elektroniczną Dostawcy Usługi.

Obsługiwane formaty w Usłudze Walidacji to:

a. **XAdES** (XML Advanced Electronic Signatures),
b. **PAdES** (PDF Advanced Electronic Signatures),

Wszystkie certyfikaty i powiązane łańcuchy certyfikacji są weryfikowane w oparciu o europejską listę zaufanych certyfikatów (EU TSL – https://esignature.ec.europa.eu/efda/tl-browser/#/screen/home).

4. **Usługa Walidacji zaawansowanych podpisów elektronicznych oraz zaawansowanych pieczęci elektronicznych opartych o kwalifikowane certyfikaty**

Usługa Walidacji pozwala potwierdzić ważność zaawansowanego podpisu elektronicznego oraz zaawansowanej pieczęci elektronicznej opartej o kwalifikowany certyfikat w przypadku, gdy:

a. Kwalifikowany Certyfikat Podpisu lub Kwalifikowany Certyfikat Pieczęci, który towarzyszy podpisowi lub pieczęci zaawansowanej, był w momencie składania podpisu lub pieczęci Kwalifikowanym Certyfikatem Podpisu lub Kwalifikowanym Certyfikatem Pieczęci, zgodnym z załącznikiem I eIDAS,
b. Kwalifikowany Certyfikat Pieczęci lub Kwalifikowany Certyfikat Podpisu został wydany przez kwalifikowanego dostawcę usług zaufania i był ważny w momencie składania podpisu,
c. dane służące do walidacji Kwalifikowanego Certyfikatu Pieczęci lub Kwalifikowanego Certyfikatu Podpisu odpowiadają danym dostarczonym Stronie Ufającej,
d. niepowtarzalny zestaw danych reprezentujących podpisującego umieszczony w Kwalifikowanym Certyfikacie Pieczęci lub Kwalifikowanym Certyfikacie Podpisu jest prawidłowo dostarczony Stronie Ufającej,
e. jeżeli w momencie składania podpisu użyty został pseudonim, zostaje to wyraźnie wskazane Stronie Ufającej,
f. integralność podpisanych danych nie została skompromitowana,
g. wymogi przewidziane w art. 26 eIDAS zostały spełnione w momencie składania podpisu lub pieczęci elektronicznej.

Usługa Walidacji umożliwia Stronom Ufającym otrzymanie Raportu Walidacji oraz Poświadczenia Walidacji w sposób zautomatyzowany, wraz ze Wskaźnikiem Walidacji, który jest wiarygodny i dokładny, oraz opatrzony Pieczęcią Elektroniczną Dostawcy Usługi. Ponadto, w przypadku korzystania z GUI, Użytkownik otrzymuje również skróconą informację o rezultacie Usługi Walidacji.

Usługa Walidacji weryfikuje techniczną ważność i poprawność certyfikatów, zgodnie z wymogami wskazanymi powyżej. Techniczna ważność jest sprawdzana zgodnie z procesem opisanym w ETSI TS 319 102-1 oraz potwierdzona poprzez podpisanie Raportu Walidacji oraz Poświadczenia Walidacji Pieczęcią Elektroniczną Dostawcy Usługi.

Obsługiwane formaty w Usłudze Walidacji to:

c. **XAdES** (XML Advanced Electronic Signatures),
d. **PAdES** (PDF Advanced Electronic Signatures),

Wszystkie certyfikaty i powiązane łańcuchy certyfikacji są weryfikowane w oparciu o europejską listę zaufanych certyfikatów (EU TSL – https://esignature.ec.europa.eu/efda/tl-browser/#/screen/home).

5. **Usługa Walidacji e-Podpisu Autenti oraz Zaawansowanego e-Podpisu Autenti**

Usługa Walidacji e-Podpisu Autenti oraz Zaawansowanego e-Podpisu Autent potwierdza jego ważność pod warunkiem, że:

a. certyfikat, który towarzyszy e-Podpisowi Autenti oraz Zaawansowanemu e-Podpisowi Autenti, był w momencie jego składania certyfikatem Pieczęci Elektronicznej Dostawcy Usług,
b. Pieczęć Elektroniczna Dostawcy Usług została wydana przez kwalifikowanego dostawcę usług zaufania i była ważna w momencie składania e-Podpisu Autenti lub Zaawansowanego e-Podpisu Autenti,
c. dane służące do walidacji e-Podpisu Autenti oraz Zaawansowanego e-Podpisu Autenti, odpowiadają danym dostarczonym Stronie Ufającej,
d. niepowtarzalny zestaw danych reprezentujących podpisującego umieszczony w certyfikacie Pieczęci Elektronicznej Dostawcy Usług jest prawidłowo dostarczony Stronie Ufającej i zgodny z zasadami świadczenia e-Podpisu i Zaawansowanego e-Podpisu Autenti przez Dostawcę Usług,
e. jeżeli w momencie składania e-Podpisu Autenti lub Zaawansowanego e-Podpisu Autenti użyty został pseudonim, zostaje to wyraźnie wskazane Stronie Ufającej,
f. integralność podpisanych danych nie została skompromitowana,

g. dla Zaawansowanego e-Podpisu Autenti, Usługa Walidacji wskazuje również, że wymogi przewidziane w art. 26 eIDAS zostały spełnione w momencie jego składania.

Usługa Walidacji umożliwia Stronom Ufającym otrzymanie Raportu Walidacji oraz Poświadczenia Walidacji w sposób zautomatyzowany, wraz ze Wskaźnikiem Walidacji, który jest wiarygodny i dokładny, oraz opatrzony Pieczęcią Elektroniczną Dostawcy Usługi. Ponadto, w przypadku korzystania z GUI, Użytkownik otrzymuje również skróconą informację o rezultacie Usługi Walidacji. Z uwagi na fakt, że usługa e-Podpisu Autenti oraz Zaawansowanego e-Podpisu Autenti polega na powiązaniu danych podpisującego z dokumentem poprzez nałożenie certyfikatu Pieczęci Elektronicznej Dostawcy Usług oraz wpisanie danych podpisującego do certyfikatu Pieczęci Elektronicznej Dostawcy Usług (pole dotyczące powodu nałożenia pieczęci), Dostawca Usługi dostarcza:

a. Wskaźniki Walidacji dla Pieczęci Elektronicznej Dostawcy, prezentujący wynik Usługi Walidacji zarówno w Raporcie Walidacji, Poświadczeniu Walidacji oraz w przypadku korzystania z GUI, również skróconą informację o rezultacie Usługi Walidacji na GUI,
b. informacje o poprawności e-Podpisu Autenti lub Zaawansowanego e-Podpisu Autenti,
c. danych osobowych podpisującego, zawartych w certyfikacie Pieczęci Elektronicznej Dostawcy Usług, użytych do złożenia podpisu elektronicznego. Informacje są prezentowane na GUI oraz w Poświadczeniu Walidacji.

Usługa Walidacji e-Podpisu Autenti oraz Zaawansowanego e-Podpisu Autenti jest dostępna wyłącznie w formacie PAdES (PDF Advanced Electronic Signatures).

V. Opis Usługi Walidacji

1. Komponenty

Usługa Walidacji obejmuje następujące komponenty oprogramowania, zgodnie z ETSI EN 319 102-1:

a. Aplikacja do walidacji podpisu lub pieczęci elektronicznej (eng. *Driving Application*) – agent oprogramowania po stronie Użytkownika dostępny w GUI Platformy Autenti oraz API, który posiada następujące funkcje:
   - tworzy żądania walidacji;
   - wykonuje protokół walidacji przez stronę użytkownika;
   - udostępnia Użytkownikowi Raport Walidacji oraz Poświadczenie Walidacji.

b. Serwer walidacji – komponent implementujący protokół walidacji podpisów i pieczęci elektronicznych oraz w ramach którego działa aplikacja do walidacji podpisów i pieczęci elektronicznych po stronie Dostawcy Usług, a który wykonuje następujące funkcje:
   - odbiera podpisy elektroniczne, pieczęcie elektroniczne i inne dane wejściowe od Użytkownika do walidacji;
   - przeprowadza proces weryfikacji zgodnie z obowiązującą polityką dla walidowanych certyfikatów i ograniczeniami, wykorzystując procesy, algorytmy i protokoły weryfikacji zgodnie z ETSI EN 319 102-1 i ETSI TS 119 442; Techniczny opis wspieranych przez Dostawcę Usług wartości z normy ETSI TS 119 442 jest opublikowany na stronie developers.autenti.com,
   - Komunikuje się z wewnętrznymi i zewnętrznymi źródłami usługi – CRL/OCSP, urzędem certyfikacji, TSA, zaufaną listą UE;
   - Generuje Raport Walidacji oraz Poświadczenie Walidacji, zawierające Wskaźniki Walidacji dla zweryfikowanego podpisu lub pieczęci elektronicznej.

2. **Interfejs i zasady świadczenia Usługi Walidacji**

Dostawca Usług świadczy Usługę Walidacji za pośrednictwem Interfejsu użytkownika na Platformie Autenti, pod adresem - www.autenti.com (GUI), który wykorzystuje bezpieczny kanał komunikacyjny/bezpieczną sesję (protokół HTTPS / certyfikat uwierzytelniający stronę internetową) do połączenia się z serwerem walidacyjnym lub z wykorzystaniem API Po uzyskaniu dostępu do Usługi Walidacji, niezależnie od tego czy wykorzystywane jest GUI czy API, Użytkownik przesyła Dokument podpisany podpisem elektronicznym lub opatrzony pieczęcią elektroniczną, który chce zweryfikować i wysyła żądanie do serwera walidacyjnego.

Usługa Walidacji jest dostępna wyłącznie dla Użytkowników posiadających zarejestrowane Konto na Platformie Autenti.

3. **Proces walidacji oraz kryteria walidacji**

Żądanie walidacji podpisu elektronicznego lub pieczęci elektronicznej oraz odpowiedzi na te żądania wykorzystują komunikację klient-serwer. Protokół walidacji jest zgodny z normą ETSI TS 119 442.

Proces walidacji przebiega zgodnie z normą ETSI EN 319 102-1 i obejmuje następujące etapy:

a. Użytkownik generuje i wysyła żądanie walidacji, zawierające podpisany lub opieczętowany dokument lub wysyła dokument i podpis, w zależności od formatu;
b. Serwer walidacyjny waliduje podpis elektroniczny lub pieczęć przy użyciu wewnętrznych usług Dostawcy Usług, zewnętrznych usług innych dostawców lub zewnętrznych źródeł certyfikatów (np. europejska lista zaufanych certyfikatów).
c. Serwer walidacyjny generuje i wysyła Raport Walidacji oraz Poświadczenie Walidacji. Raport Walidacji oraz Poświadczenie Walidacji są opatrzone Pieczęcią Elektroniczną Dostawcy Usługi.
d. Użytkownik otrzymuje do pobrania Raport Walidacji oraz Poświadczenie Walidacji w formacie PDF, który można zapisać lokalnie na komputerze Użytkownika.

Usługa Walidacji obsługuje procesy walidacji Kwalifikowanych Podpisów Elektronicznych lub Kwalifikowanych Pieczęci Elektronicznych w następujących formatach:

a. proces walidacji podpisu i/lub pieczęci w podstawowym formacie BASELINE;
b. proces walidacji znacznika czasu;
c. proces walidacji podpisu i/lub pieczęci w profilu BASELINE_T i BASELINE_LT;
d. proces walidacji podpisu i/lub pieczęci w profilu BASELINE_LTA.

Dla każdego formatu podpisu elektronicznego oraz pieczęci elektronicznej Usługa Walidacji wykonuje następujące czynności:

a. Przeprowadza proces walidacji podpisu elektronicznego/pieczęci w formacie rozszerzonym – BASELINE_T, BASELINE_LT i BASELINE_LTA lub przeprowadza proces walidacji podpisu elektronicznego/pieczęci w formacie podstawowym – BASELINE;
b. Jeśli Wskaźnik Walidacji wybranego procesu walidacji to PASSED, zwracany jest wskaźnik statusu TOTAL-PASSED, Raport Walidacji i Poświadczenie Walidacji;
c. Jeśli Wskaźnik Walidacji wybranego procesu walidacji to FAILED, zwracany jest wskaźnik statusu TOTAL- FAILED, Raport Walidacji i Poświadczenie Walidacji;
d. Jeśli Wskaźnik Walidacji wybranego procesu walidacji nie jest ani VALID, ani FAILED, zwracany jest wskaźnik statusu UNDEFINED, Raport Walidacji i Poświadczenie Walidacji.

Użytkownik nie ma możliwości określenia kryteriów walidacji (signature validation policy) czy wyboru podpisów, wobec których ma zostać wykonana Usługa Walidacji. W ramach Usługi Walidacji weryfikowane są wszystkie podpisy i pieczęcie elektroniczne powiązane z Danymi Walidacyjnymi.

Kryteria walidacji stosowane przez Dostawcę Usług oraz ich aktualizacje są dostępne na stronie https://verify.autenti.com/public/signature-validation-policies (URI).

2. Wskaźniki Walidacji

a. Dla Usługi Walidacji, niezależnie od rodzaju weryfikowanego podpisu elektronicznego lub pieczęci elektronicznej, przewiduje się następujące Wskaźniki Walidacji:

Wskaźnik Walidacji	Informacje do Poświadczenia Walidacji	Znaczenie (Semantyka)
TOTAL–PASSED (WALIDACJA POZYTYWNA)	Proces walidacji powinien zwrócić zweryfikowany łańcuch certyfikatów, w tym certyfikat podpisujący użyty w procesie walidacji. Dodatkowo, proces walidacji może przedstawić wynik walidacji dla każdego z ograniczeń walidacyjnych. Proces walidacji powinien umożliwić dostęp aplikacji sterującej (DA) do podpisanych atrybutów obecnych w podpisie, tożsamości podpisującego, tożsamości podpisującego i daty i godziny walidacji.	Proces walidacji podpisu prowadzi do wyniku TOTAL–PASSED na podstawie następujących przesłanek: • sprawdzenie formatu zakończyło się sukcesem; • sprawdzenia kryptograficzne podpisu zakończyły się sukcesem (w tym sprawdzenie skrótów poszczególnych, pośrednio podpisanych danych); • wszelkie ograniczenia mające zastosowanie do certyfikatu podpisującego zostały pozytywnie zweryfikowane (np. certyfikat podpisujący został uznany za godny zaufania); • podpis został pozytywnie zweryfikowany względem przyjętych ograniczeń walidacyjnych i jest z nimi zgodny.

TOTAL–FAILED (WALIDACJA NEGATYWNA)	Proces walidacji powinien wygenerować dodatkowe informacje wyjaśniające wskazanie TOTAL-FAILED dla każdego z ograniczeń walidacji, które zostały uwzględnione i dla których wystąpił wynik negatywny.	Proces weryfikacji podpisu zakończył się wynikiem TOTAL-FAILED, ponieważ nie udało się sprawdzić formatu, nie udało się przeprowadzić kontroli kryptograficznej podpisu (w tym kontroli skrótów poszczególnych obiektów danych, które zostały podpisane pośrednio) lub udowodniono, że certyfikat podpisu był nieważny w momencie generowania podpisu.
INDETERMINATE (WALIDACJA NIEOKREŚLONA)	Proces walidacji powinien generować dodatkowe informacje wyjaśniające wskazanie statusu INDETERMINATE i pomagające Użytkownikowi w identyfikacji brakujących danych niezbędnych do zakończenia procesu walidacji. W szczególności powinien on dostarczać wskazania wyników walidacji dla tych ograniczeń walidacji, które zostały uwzględnione i dla których wystąpił wynik nieokreślony.	Dostępne informacje są niewystarczające, aby jednoznacznie stwierdzić, czy podpis może zostać uznany za TOTAL–PASSED czy TOTAL–FAILED.

b. Gdy status walidacji wynosi TOTAL-FAILED (Walidacja negatywna) i INDETERMINATE (nieokreślony), Poświadczenie Walidacji zawiera również dodatkowe wskaźniki, takie jak:

Główna Wskaźnik Walidacji	**Dodatkowy Wskaźnik Walidacji**	**Informacje wobec dodatkowego Wskaźnika Walidacji**	**Znaczenie (Semantyka)**
TOTAL-FAILED	FORMAT_FAILURE	Proces walidacji powinien dostarczyć wszelkich dostępnych informacji wyjaśniających, dlaczego analiza podpisu nie powiodła się.	Podpis nie jest zgodny z jedną z podstawowych norm w takim stopniu, że moduł weryfikacji kryptograficznej nie jest w stanie go przetworzyć.

TOTAL-FAILED	HASH_FAILURE	Proces walidacji powinien zapewniać identyfikator (identyfikatory) (np. URI lub OID) jednoznacznie identyfikujący element w podpisanym obiekcie danych (takim jak atrybuty podpisu lub SD), który spowodował niepowodzenie.	Proces weryfikacji podpisu zakończył się całkowitym niepowodzeniem, ponieważ co najmniej jeden skrót obiektu danych podpisanych, który został uwzględniony w procesie podpisywania, nie pasuje do odpowiedniej wartości skrótu w podpisie.
TOTAL-FAILED	SIG_CRYPTO_FAILURE	Proces walidacji powinien generować: Certyfikat podpisu użyty w procesie walidacji.	Proces weryfikacji podpisu zakończył się całkowitym niepowodzeniem, ponieważ nie udało się zweryfikować wartości podpisu przy użyciu klucza publicznego podpisującego zawartego w certyfikacie podpisu.
TOTAL-FAILED	REVOKED	Proces walidacji powinien zapewniać następujące informacje: • Łańcuchu certyfikatów użyty w procesie walidacji, • Czas i, jeśli to możliwe, powód unieważnienia certyfikatu podpisu.	Proces weryfikacji podpisu zakończył się całkowitym niepowodzeniem (TOTAL-FAILED) z następujących powodów: • certyfikat podpisu został unieważniony; oraz, • istnieją dowody na to, że podpis został utworzony po dacie unieważnienia.
TOTAL-FAILED	EXPIRED	Proces powinien zwrócić: Zweryfikowany łańcuch certyfikatów.	Proces weryfikacji podpisu zakończył się całkowitym niepowodzeniem, ponieważ istnieją dowody na to, że podpis został utworzony po upływie terminu ważności (notAfter) certyfikatu podpisu.
TOTAL-FAILED	NOT_YET_VALID		Proces weryfikacji podpisu zakończył się całkowitą niepowodzeniem (TOTAL-FAILED), ponieważ istnieją dowody na to, że podpis został utworzony

			przed datą wydania (notBefore) certyfikatu podpisu.
INDETERMINATE	SIG_CONSTRAINTS_FAILURE	Atrybuty podpisu nie spełniają wymagań ograniczeń walidacyjnych.	Proces weryfikacji podpisu zakończył się wynikiem INDETERMINATE, ponieważ co najmniej jeden atrybut podpisu nie spełnia ograniczeń weryfikacyjnych.
INDETERMINATE	CHAIN_CONSTRAINTS_FAILURE	Łańcuch certyfikatów nie spełnia ograniczeń walidacyjnych.	Proces weryfikacji podpisu zakończył się wynikiem INDETERMINATE, ponieważ łańcuch certyfikatów użyty w procesie weryfikacji nie spełnia ograniczeń weryfikacyjnych związanych z certyfikatem.
INDETERMINATE	CRYPTO_CONSTRAINTS_FAILURE	Użyto algorytmu lub długości klucza poniżej wymaganego poziomu bezpieczeństwa.	Proces weryfikacji podpisu zakończył się wynikiem INDETERMINATE, ponieważ zestaw certyfikatów dostępnych do weryfikacji łańcucha spowodował błąd z nieokreślonych przyczyn.
INDETERMINATE	CERTIFICATE_CHAIN_GENERAL_FAILURE	Proces powinien wygenerować dodatkowe informacje dotyczące przyczyny.	Proces weryfikacji podpisu zakończył się wynikiem INDETERMINATE, ponieważ zestaw certyfikatów dostępnych do weryfikacji łańcucha spowodował błąd z nieokreślonych przyczyn.
INDETERMINATE	CRYPTO_CONSTRAINTS_FAILURE	Proces powinien dostarczyć następujące wyniki: • Identyfikację materiału (podpis, certyfikat) wyprodukowanego przy użyciu algorytmu lub klucza o rozmiarze poniżej wymaganego poziomu	Proces weryfikacji podpisu daje wynik INDETERMINATE ponieważ co najmniej jeden z algorytmów użytych w materiale (np. wartość podpisu, certyfikat...), wykorzystanym do weryfikacji podpisu lub rozmiar klucza użytego w takim algorytmie jest poniżej wymaganego

		bezpieczeństwa kryptograficznego. • Jeśli jest to znane, czas, do którego algorytm lub rozmiar klucza były uważane za bezpieczne.	poziomu bezpieczeństwa kryptograficznego, a ponadto: • materiał ten został wyprodukowany po upływie czasu, do którego algorytm/klucz był uważany za bezpieczny (jeśli taki czas jest znany); oraz • materiał nie jest chroniony wystarczająco silnym znacznikiem czasu zastosowanym przed upływem czasu, do którego algorytm/klucz był uważany za bezpieczny (jeśli taki czas jest znany).
INDETERMINATE	POLICY_PROCESSING_ERROR	Proces walidacji dostarczy dodatkowych informacji na temat problemu.	Proces weryfikacji podpisu zakończył się wynikiem INDETERMINATE, ponieważ z jakiegoś powodu nie można było przetworzyć danego pliku z formalną polityką (np. brak dostępu, brak możliwości analizy, niezgodność skrótu itp.).
INDETERMINATE	SIGNATURE_POLICY_NOT_AVAILABLE		Proces weryfikacji podpisu zakończył się wynikiem INDETERMINATE, ponieważ dokument elektroniczny zawierający szczegóły polityki nie jest dostępny.
INDETERMINATE	TIMESTAMP_ORDER_FAILURE	Proces walidacji powinien wygenerować listę znaczników czasu, które nie spełniają ograniczeń dotyczących kolejności.	Proces weryfikacji podpisu zakończył się wynikiem INDETERMINATE, ponieważ niektóre ograniczenia dotyczące kolejności znaczników czasu podpisu i/lub znaczników czasu podpisanych obiektów danych nie zostały zachowane.

INDETERMINATE	NO_SIGNING_CERTIFICATE_FOUND		Proces weryfikacji podpisu zakończył się wynikiem INDETERMINATE, ponieważ nie można zidentyfikować certyfikatu podpisu.
INDETERMINATE	NO_CERTIFICATE_CHAIN_FOUND		Proces weryfikacji podpisu zakończył się wynikiem INDETERMINATE, ponieważ nie znaleziono łańcucha certyfikatów dla zidentyfikowanego certyfikatu podpisu.
INDETERMINATE	NO_CERTIFICATE_CHAIN_FOUND_NO_POE		Wyniki procesu sprawdzania podpisu to INDETERMINATE, ponieważ nie znaleziono łańcucha certyfikatów dla zidentyfikowanego certyfikatu podpisu, gdyż łańcuch certyfikatów nie był zaufany w momencie sprawdzania przez używaną politykę walidacji. Algorytm walidacji podpisu nie może jednak stwierdzić, czy czas podpisania był przed czy po momencie, kiedy łańcuch certyfikatów był zaufany przez używaną politykę walidacji.
INDETERMINATE	REVOKED_NO_POE		Proces weryfikacji podpisu zakończył się wynikiem INDETERMINATE, ponieważ certyfikat podpisu został unieważniony w dniu/godzinie weryfikacji. Jednak algorytm weryfikacji podpisu nie jest w stanie ustalić, czy czas podpisania nastąpił przed czy po unieważnieniu.
INDETERMINATE	REVOKED_CA_NO_POE	Proces walidacji powinien zapewniać następujące informacje:	Proces sprawdzania podpisu zakończył się wynikiem INDETERMINATE, ponieważ

		• Łańcuch certyfikatów zawierający unieważniony certyfikat CA. • Czas i powód unieważnienia certyfikatu.	znaleziono co najmniej jeden łańcuch certyfikatów, ale certyfikat pośredniego urzędu certyfikacji został unieważniony.
INDETERMINATE	OUT_OF_BOUNDS_NOT_REVOKED		Proces weryfikacji podpisu daje wynik INDETERMINATE, ponieważ certyfikat podpisu wygasł lub nie jest jeszcze ważny w dniu/godzinie weryfikacji, a algorytm weryfikacji podpisu nie może ustalić, czy czas podpisania mieści się w okresie ważności certyfikatu podpisu. Wiadomo, że certyfikat nie został unieważniony.
INDETERMINATE	OUT_OF_BOUNDS_NO_POE		Proces weryfikacji podpisu daje wynik INDETERMINATE, ponieważ certyfikat podpisu wygasł lub nie jest jeszcze ważny w dniu/godzinie weryfikacji, a algorytm weryfikacji podpisu nie może ustalić, czy czas podpisania mieści się w okresie ważności certyfikatu podpisu.
INDETERMINATE	REVOCATION_OUT_OF_BOUNDS_NO_POE	Proces walidacji powinien zapewniać następujące elementy: • Łańcuch certyfikatów wykorzystywany w procesie walidacji. • Dane dotyczące unieważnienia, których dotyczy niepowodzenie.	Proces walidacji podpisu kończy się wynikiem INDETERMINATE, ponieważ certyfikatużyty do podpisania danych unieważnienia (zawierających informację o statusie unieważnienia certyfikatu, którym podpisano podpis) wygasł albo nie był jeszcze ważny w chwili walidacji, a algorytm walidacji

			podpisu nie jest w stanie ustalić, że dane unieważnienia istniały w czasie mieszczącym się w okresie ważności certyfikatu, którym zostały podpisane.
INDETERMINATE	CRYPTO_CONSTRAINTS_FAILURE_NO_POE	Proces powinien dać następujące wyniki: Identyfikacja materiału (podpis, certyfikat) wyprodukowanego przy użyciu algorytmu lub klucza o rozmiarze poniżej wymaganego poziomu bezpieczeństwa kryptograficznego. Jeśli jest to znane, czas, do którego algorytm lub rozmiar klucza były uważane za bezpieczne.	Proces weryfikacji podpisu zakończył się wynikiem INDETERMINATE, ponieważ co najmniej jeden z algorytmów użytych w obiektach (np. wartość podpisu, certyfikat itp.) spowodował unieważnienie podpisu lub rozmiar klucza użytego w takim algorytmie jest poniżej wymaganego poziomu bezpieczeństwa kryptograficznego i nie ma dowodu, że materiał ten został wyprodukowany przed upływem czasu, do którego algorytm ten był używany.
INDETERMINATE	NO_POE	Proces walidacji powinien identyfikować co najmniej podpisane obiekty, dla których brakuje POE. Proces walidacji powinien dostarczać dodatkowych informacji na temat problemu.	Proces weryfikacji podpisu daje wynik INDETERMINATE, ponieważ brakuje dowodu potwierdzającego, że podpisany obiekt został wygenerowany przed wystąpieniem zdarzenia zagrażającego bezpieczeństwu (np. złamania algorytmu).
INDETERMINATE	TRY_LATER	Proces walidacji powinien wskazać moment, w którym spodziewane jest udostępnienie niezbędnych informacji dotyczących unieważnienia.	Proces weryfikacji podpisu daje wynik INDETERMINATE, ponieważ nie wszystkie ograniczenia mogą zostać spełnione przy użyciu dostępnych informacji. Jednakże może to być możliwe przy użyciu dodatkowych informacji dotyczących

			unieważnienia, które będą dostępne w późniejszym terminie.
INDETERMINATE	SIGNED_DATA_NOT_FOUND	Proces powinien wyświetlać następujące informacje, jeśli są dostępne: identyfikator(y) (np. URI) podpisanych danych, które spowodowały błąd.	Proces weryfikacji podpisu zakończył się wynikiem INDETERMINATE, ponieważ nie można uzyskać podpisanych danych.
INDETERMINATE	CUSTOM	Proces powinien generować informacje umożliwiające identyfikację przyczyny niestandardowego wyniku walidacji.	Proces walidacji podpisu kończy się wynikiem INDETERMINATE z powodu niestandardowego wyniku diagnostycznego, który nie został określony w niniejszym dokumencie.

4. Raport Walidacji oraz Poświadczenie Walidacji

Po przeprowadzeniu Usługi Walidacji, Użytkownikowi zwracana jest informacja o:

a. ogólnym wyniku Usługi Walidacji wobec Danych Walidacyjnych,
b. liście podpisów i pieczęci elektronicznych objętych Usługą Walidacji wraz ze wskazaniem Wskaźników Walidacji dla każdego z nich,
c. Szczegóły Usługi Walidacji, w tym:
   - data wygenerowania Raportu Walidacji,
   - Numer ID procesu walidacji,
   - skrót Danych Walidacyjnych,
   - nazwę Dostawcy Usługi,
   - OID Polityki.

Ponadto, w ramach Usługi Walidacji generowany jest Raport z Usługi Walidacji, zgodnie z ETSI TS 119 102-2 oraz Poświadczenie Walidacji w czytelnym dla Użytkownika formacie PDF, będące raportem, który zawiera informacje takie jak:

a. data i czas wygenerowania Poświadczenia Walidacji,
b. wersja Poświadczenia Walidacji,
c. nazwę walidowanego Dokumentu,
d. skrót walidowanego Dokumentu,

e. wskazanie podpisów i pieczęci elektronicznych objętych Usługą Walidacji, ich formatu, daty i czasu złożenia oraz Wskaźnikiem Walidacji dla każdego z nich,
f. szczegóły Usługi Walidacji, obejmujące dla każdego podpisu i pieczęci elektronicznej:
    - imię i nazwisko lub nazwę podmiotu składającego podpis lub pieczęć elektroniczną,
    - numer identyfikacyjny osoby lub podmiotu,
    - numer seryjny certyfikatu,
    - datę ważności certyfikatu,
    - datę wystawienia certyfikatu,
    - Wskaźnik Walidacji,
    - format podpisu lub pieczęci elektronicznej,
    - funkcję skrótu podpisu lub pieczęci elektronicznej,
    - informację o powodzie złożenia podpisu elektronicznego lub pieczęci elektronicznej, jeżeli istnieje,
    - informacje o znaczniku czasu, w tym jego wystawcy, dacie nałożenia oraz typie, jeżeli istnieje.

Dostawca Usług zapewnia, że treść Raportu Walidacji, Poświadczenie Walidacji oraz wynik prezentowany na GUI są spójne.

Wynik Usługi Walidacji dla Danych Walidacyjnych mogą się różnić w czasie, np. ze względu na upływy czasu poszczególnych certyfikatów.

Wskaźniki Walidacji są przez Dostawcę Usług określane i oznaczone odpowiednimi kolorami zgodnie z następującą klasyfikacją:

a. TOTAL–PASSED: Walidacja Pozytywna, oznaczona kolorem zielonym,
b. INDETERMINATE: Walidacja Nieokreślona, oznaczona kolorem pomarańczowym,
c. TOTAL–FAILED: Walidacja Negatywna, oznaczona kolorem czerwonym.

Każdy Raport Walidacji oraz Poświadczenie Walidacji zawierają również informację o numerze ID procesu walidacji oraz jest zabezpieczone Pieczęcią Elektroniczną Dostawcy Usługi. Numerem ID procesu należy się posługiwać w przypadku reklamacji lub pytań kierowanych do Działu Wsparcia Klienta.

VI. Zarządzanie bezpieczeństwem

1. Bezpieczeństwo organizacyjne

Działania podejmowane w zakresie ochrony informacji przez Dostawcę Usługi są elementem opracowanego i wdrożonego u Dostawcy Usługi systemu bezpieczeństwa informacji, zgodnego z wymaganiami normy ISO/IEC 27001:2022 oraz ETSI 319 401.

Działania związane z ochroną informacji, pomieszczeń, infrastruktury, systemów informatycznych oraz danych, które są z nimi powiązane, mają na celu zapobieganie w szczególności:

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

Infrastruktura Dostawcy Usługi niezbędna do świadczenia Usługi Walidacji 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,
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 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 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 tworzeniu, utrzymywaniu i monitorowaniu Usługi Walidacji oraz pełniący tzw. role zaufane posiada odpowiednie doświadczenie, umiejętności oraz kwalifikacje w zakresie pełnionych obowiązków oraz wykonywanych zadań.

Dostawca Usługi zapewnia również, że personel Dostawcy Usługi 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 Walidacji.

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.

Dostawca Usługi dla celów świadczenia Usługi Walidacji korzysta z takich podmiotów zewnętrznych jak:

a. dostawca chmury obliczeniowej Microsoft Ireland Operations Ltd.
b. dostawca kwalifikowanego znacznika czasu,
c. dostawca kwalifikowanej pieczęci elektronicznej.

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 Walidacji 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 Walidacji,

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 Walidacji 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. W ramach wdrażania zmian, Dostawca Usług weryfikuje również ich zgodność z właściwymi przepisami prawa oraz normami ETSI.

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 Walidacji 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:
    - bazy danych,
    - dzienników zdarzeń,
    - 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 72 godzin po ich wykryciu.

11. Bezpieczeństwo transmisji oraz sieci

Dostawca Usługi w ramach świadczenia Usługi Walidacji 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).

Stosowany przez Dostawcę Usług certyfikat TLS SSL, z uwagi na fakt, iż Raport Walidacji nie jest prezentowany na stronie internetowej, a wyłącznie w aplikacji Platformy Autenti działającej w domenie Dostawcy Usług, nie jest kwalifikowanym certyfikatem uwierzytelnienia stron internetowych (QWAC). Dostawca Usług stosuje certyfikat na poziomie DV (Domain Validation Certificate) umożliwiającym jego częstą rotację, a tym samym zwiększenie bezpieczeństwa użytkowników. Skuteczność kryptograficzna i bezpieczeństwo transmisji pozostają identyczne, a pozostałe kontrole bezpieczeństwa zapewniają pełną ochronę kanału komunikacji.

12. Audyty oraz przeglądu 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 oraz zgodności świadczonych usług. W przypadku Usługi Walidacji, Dostawca Usług między innymi przeprowadza audyty oraz testy poprawnego funkcjonowania, aby wykazać poprawność wdrożenia pod kątem sprawdzenia czy podpis lub pieczęć elektroniczna są prawidłowo walidowane. Przypadki testowe obejmują różne przypadki użycia, zarówno pozytywne jak i negatywne.

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.
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 Walidacji, 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 Walidacji 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 Walidacji 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 Walidacji.

15. Klucze kryptograficzne

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, przez cały cykl ich życia.

W ramach Usługi Walidacji, Dostawca Usługi posługuje się Pieczęcią Elektroniczną Dostawcy Usług, która służy do podpisywania Raportów Walidacji oraz Poświadczeń Walidacji. Klucz prywatny jest przechowywany i używany w bezpiecznym środowisku do wykonywania operacji kryptograficznych, który może zostać zapewniony przez dostawcę certyfikatu Pieczęci Elektronicznej Dostawcy Usług (kwalifikowane urządzenie do składania podpisu/pieczęci) lub w ramach infrastruktury własnej Dostawcy Usług. W przypadku, gdy klucz prywatny Pieczęci Elektronicznej Dostawcy Usług jest przechowywany w ramach infrastruktury własnej Dostawcy Usług, jest on przechowywany, przywracany i archiwizowany wyłącznie przez personel pełniący role zaufane, w fizycznie bezpiecznym środowisku. Liczba personelu upoważnionego do wykonywania czynności na urządzeniu oraz kluczach kryptograficznych jest ograniczona do niezbędnego minimum. W celu zabezpieczenia możliwości ciągłego generowania Raportów Walidacji oraz Poświadczeń Walidacji przez Dostawcę Usługi oraz podpisywania ich Pieczęcią Elektroniczną Dostawcy Usługi, w warunkach wystąpienia awarii (urządzeń, mediów, lub mechanizmów komunikacji niezbędnych do użycia urządzeń) zapewnia się jej redundancję.

Klucz prywatny certyfikatu Pieczęci Elektronicznej Dostawcy Usługi może zostać zmieniony w przypadku:

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

16. Rejestracja zdarzeń

Dostawca Usługi zbiera i archiwizuje następujące informacje:

a. rejestry zdarzeń (techniczne logi systemowe) ze świadczenia Usługi Walidacji, przez okres 3 miesięcy, zawierające następujące informacje:
   - adres IP, z które zainicjowano Usługę Walidacji,
   - nazwę oraz hash walidowanych dokumentów,
   - nazwy pól z podpisem,
b. zdarzenia (evidences) dla poprawnie ukończonych procesów walidacji, przez okres 6 lat, w sposób, który zabezpiecza przed ich modyfikacją takie jak:
   - informacja o ogólnym Wskaźniku Walidacji dla Danych Walidacyjnych,
   - informacje o użytkowniku,
   - informacja o Walidowanym dokumencie (nazwa, typ, rozmiar, suma kontrolna),
   - informacja o plikach źródłowych, jeżeli występowały (dot. XAdES),
   - czas wykonania Usługi Walidacji.

c. zdarzenia (events) dla procesów walidacji zakończonych błędem, przez okres 6 lat, takie jak:
   - informacja o błędzie,
   - informacja o użytkowniku,
   - informacja o Walidowanym dokumencie (nazwa, typ, rozmiar, suma kontrolna),
   - informacja o plikach źródłowych, jeżeli występowały (dot. XAdES),
   - czas wykonania Usługi Walidacji.

d. Poświadczenie Walidacji w formacie PDF, przez okres 24 godzin,
e. Raport Walidacji w formacie XML, przez okres 6 lat.

VII. Zakończenie działalności lub zaprzestanie świadczenia Usługi Walidacji

1. Dostawca Usługi dołoży wszelkich starań mających na celu zminimalizowanie negatywnych skutków podjęcia potencjalnej decyzji o zakończeniu świadczenia Usługi Walidacji lub zakończeniu działalności.
2. W tym celu Dostawca Usługi z odpowiednim wyprzedzeniem poinformuje o tym fakcie organ nadzoru, Użytkowników, na rzecz których Usługa Walidacji 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 Walidacji,
   b. informowania Użytkowników, organu nadzoru i stron trzecich o zakończeniu działalności lub zaprzestania świadczenia Usługi Walidacji. Informacje są przekazywane pocztą elektroniczną lub poprzez zamieszczenie na stronie internetowej Dostawcy Usługi,
   c. wycofania wszelkich upoważnień do wykonywania czynności związanych z Usługą Walidacji, w tym do przeprowadzania procesu weryfikacji tożsamości,
   d. przed zakończeniem działalności lub przed zakończeniem świadczenia Usługi Walidacji, 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 Walidacji zniszczyć lub usunąć z użycia w sposób uniemożliwiający odzyskanie wszelkie klucze kryptograficzne służące do świadczenia Usługi Walidacji, w tym ich kopie zapasowe - o ile ma to zastosowanie,
   f. zobowiązuje się do udostępnienia klucza publicznego stronom ufającym,

g. jeśli to możliwe, przekazać swoją działalność innemu kwalifikowanemu dostawcy usługi walidacji,
h. podjęcia wszelkich uzasadnionych wysiłków w celu zminimalizowania zakłócenia interesów konsumentów,
i. przechowywania lub przekazania przechowywania innej stronie dowodów z Usługi Walidacji, celem ich udostępniania przez czas wymagany Polityką lub przepisami prawa - o ile ma to zastosowanie.

Szczegółowy sposób postępowania w przypadku podjęcia decyzji o zakończeniu działalności Dostawcy Usług lub zakończeniu świadczenia Usługi Walidacji 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

VIII. Warunki rozstrzygania sporów, reklamacje, wątpliwości

1. Użytkownik korzystający z praw konsumenta oraz Klient może złożyć reklamację, jeżeli Usługa Walidacji 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.
3. Szczegółowe zasady rozpatrywania reklamacji oraz skarg zostały opisane i są realizowane zgodnie z pkt. VI oraz pkt IV.12-IV.13 Regulaminu, w zależności od przypadku.
4. Strona Ufająca może zgłosić wątpliwości dotyczące wykonania Usługi Walidacji 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.
5. W przypadku niezadowalającego Użytkownika postępowania reklamacyjnego spory związane z Usługą Walidacji świadczoną przez Dostawcę Usługi mogą być rozstrzygane przez właściwe sądy powszechne.

IX. Zarządzanie Polityką i jej zmiany

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 lub późniejszej daty wskazanej przez Dostawcę Usługi, zgodnie z przyjętą u Dostawcy Usługi procedurą. Dostawca Usług 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 Walidacji 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. Informacja o zmianie dotychczasowej wersji Polityki, zastąpieniu Polityki nową lub zaprzestaniu świadczenia Usługi Walidacji zostanie opublikowana w Repozytorium.

X. Mapowanie zgodności z wymogami Rozporządzenia eIDAS

Wymagania na podstawie art. 32 Rozporządzenia eIDAS	Spełnienie wymogu przez Usługę Walidacji
certyfikat wspierający podpis był w chwili podpisywania kwalifikowanym certyfikatem podpisu elektronicznego zgodnym z załącznikiem I eIDAS	Proces walidacji certyfikatów jest zgodny z wymaganiami określonymi w decyzji UE 2015/1505 oraz normie ETSI 319 412
kwalifikowany certyfikat został wydany przez kwalifikowanego dostawcę usług zaufania i był ważny w chwili podpisywania	Proces walidacji certyfikatów jest zgodny z wymaganiami określonymi w decyzji UE 2015/1505 oraz normie ETSI 319 412
dane walidacyjne podpisu odpowiadają danym przekazanym odbiorcy (relying party)	Proces walidacji dostarcza Użytkownikom raport zawierający certyfikat posiadacza, zawierający dane walidacyjne (klucz publiczny itp.)

unikatowy zestaw danych reprezentujący podpisującego w certyfikacie jest prawidłowo przekazany odbiorcy	Proces walidacji dostarcza Użytkownikom raport zawierający certyfikat posiadacza, zawierający dane walidacyjne (klucz publiczny itp.)
użycie jakiegokolwiek pseudonimu jest wyraźnie wskazane odbiorcy, jeśli pseudonim był użyty w momencie podpisu	Proces walidacji dostarcza Użytkownikom raport zawierający certyfikat posiadacza zawierający dane walidacyjne (klucz publiczny itp.)
podpis elektroniczny został utworzony za pomocą kwalifikowanego urządzenia do składania podpisu elektronicznego	Proces walidacji certyfikatów jest zgodny z wymaganiami opisanymi w decyzji UE 2015/1505 dla QTSP wydających certyfikaty kwalifikowane. Weryfikacja rodzaju urządzenia SSCD (QSCD) jest przeprowadzana.
integralność podpisanych danych nie została naruszona	Wykorzystywane przez Dostawcę Usług narzędzia, w tym bibliotek DSS i polityka walidacji podpisu (signature validation policy) gwarantują sprawdzenie integralności podpisanych danych
wymagania określone w art. 26 zostały spełnione w chwili składania podpisu	Proces walidacji podpisu lub pieczęci weryfikuje status i atrybuty certyfikatu w chwili składania podpisu

HISTORIA ZMIAN

Wersja	Data	Opis działania	Działanie*	Wykonawca działania
1.0	14.11.2025	Przyjęcie dokumentu Uchwałą Zarządu	N/P	Zarząd
1.1	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