Polityka kwalifikowanej usługi walidacji i kwalifikowanej usługi konserwacji kwalifikowanych podpisów i pieczęci elektronicznych (Certum QESValidationQ)

Wersja 1.3

Ważna od 1 marca 2020

Asseco Data Systems S.A.
ul. Podolska 21
81-321 Gdynia
Certum
ul. Bajeczna 13
71-838 Szczecin
https://certum.pl

Klauzula: Prawa Autorskie

Spis Treści

1 Wstęp, zakres i założenia

Polityka walidacji i konserwacji kwalifikowanej usługi walidacji i konserwacji Certum dla kwalifikowanego podpisu elektronicznego oraz kwalifikowanej pieczęci elektronicznej przedstawia zbiór reguł wymaganych do wydawania kwalifikowanych tokenów walidacji i konserwacji (dawniej znanych jako walidacja danych oraz poświadczenia), zgodnie z wymogami określonymi w Rozporządzeniu Parlamentu Europejskiego i Rady (EU) nr 910/2014 z dnia 23 lipca 2014 w sprawie identyfikacji elektronicznej i usług zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznym oraz uchylające dyrektywę 1999/93/WE, wraz z załączonymi aktami delegowanymi i wykonawczymi, oraz w normach europejskich wytworzonych przez Komitet Techniczny ESI ETSI.

Zbiór zasad opisanych w niniejszym dokumencie odzwierciedla wymagania biznesowe, prawne i wymagania polityk bezpieczeństwa.

Na podstawie Wersji 6 decyzji wykonawczej Komisji UE [EU 2015/1506]:

"Zaawansowane podpisy elektroniczne i zaawansowane pieczęcie elektroniczne są podobne pod względem technicznym. W związku z tym normy dotyczące formatów zaawansowanych podpisów elektronicznych powinny mieć zastosowanie *mutatis mutandis* do formatów zaawansowanych pieczęci elektronicznych."

wszystkie zasady opisane w niniejszym dokumencie dotyczące podpisów elektronicznych mają również odpowiednio zastosowanie dla pieczęci elektronicznych.

1.1 Nazwa dokumentu i jego identyfikacja

Niniejszemu dokumentowi przypisuje się nazwę własną o następującej postaci: **Polityka kwalifikowanej usługi walidacji i kwalifikowanej usługi konserwacji kwalifikowanych podpisów i pieczęci elektronicznych (Certum QESValidationQ)** i jest on dostępny w postaci elektronicznej w serwisie internetowym urzędu certyfikacji dostępnym pod adresem www.certum.pl.

Z niniejszym dokumentem związane są następujące zarejestrowane identyfikatory obiektu (OID: Z dokumentem Polityki Certyfikacji i Kodeksu Postępowania Certyfikacyjnego związane są następujące zarejestrowane identyfikatory obiektu (OID: OID: 1.2.616.1.113527.2.4.1.0.5.1.3):

> **id-cck-kpc-v1 OBJECT IDENTIFIER ::= { iso(1) member-body(2) pl(616) organization(1) id-unizeto(113527) id-ccert(2) id-cck(4) id-cck-certum-certPolicy(1) id-certPolicy-doc(0) id-ccert-ESSVP(5) version(1) 3}**

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

2 Odniesienia

Odniesienia mogą opierać się na wybranych wersjach/edycjach dokumentów (ze wskazaną datą publikacji i/lub numerem edycji lub numerem wersji) lub na wersjach uwzględniających naniesione zmiany. Dla wymienionych na początku dokumentów obowiązuje jedynie dokładnie wskazana wersja. Dla pozostałych obowiązuje ostatnia wersja dokumentu (wraz ze zmianami).

2.1 Odniesienia normatywne

[1] ETSI TS 103 171 V2.1.1 (2012-03) Electronic Signatures and Infrastructures (ESI); XAdES Baseline Profile

[2] ETSI TS 103 173 V2.2.1 (2013-04) Electronic Signatures and Infrastructures (ESI); CAdES Baseline Profile

[3] ETSI TS 103 172 V2.2.2 (2013-04) Electronic Signatures and Infrastructures (ESI); PAdES Baseline Profile

[4] ETSI TS 103 174 V2.2.1 (2013-06) Electronic Signatures and Infrastructures (ESI); ASiC Baseline Profile

2.2 Odniesienia informacyjne

[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

[EU 2015/1505] Decyzja wykonawcza Komisji (UE) 2015/1505 z dnia 8 września 2015 r. ustanawiająca specyfikacje techniczne i formaty dotyczące zaufanych list zgodnie z art. 22 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

[EU 2015/1506] 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

[ETSI-119-102] ETSI TS 119 102-1 Electronic Signatures and Infrastructures (ESI); Procedures for Creation and Validation of AdES Digital Signatures; Part 1: Creation and Validation

[ETSI-119-101] ETSI TS 119 101 Electronic Signatures and Infrastructures (ESI); Policy and security requirements for applications for signature creation and signature validation

[ETSI 119 172-1] ETSI TS 119 172-1 V1.1.1 (2015-07) Electronic Signatures and Infrastructures (ESI); Signature Policies; Part 1: Building blocks and table of contents for human readable signature policy documents

[ETSI 119 312] ETSI TS 119 312 V1.1.1 (2014-11) Electronic Signatures and Infrastructures (ESI); Cryptographic Suites

[ETSI 119 412-2] ETSI TS 119 412-2 V2.1.1 (2016-02) Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 2: Certificate profile for certificates issued to natural persons

[ETSI 119 412-5] ETSI TS 119 412-5 V2.1.1 (2016-02) Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 5: QCStatements

[ETSI-101-733] ETSI TS 101 733 V.1.7.4 (2008-07) Electronic Signature and Infrastructure (ESI) – CMS Advanced Electronic Signature (CAdES).

[ETSI-101-903] ETSI TS 101 903 V.1.3.2 (2006-03) XML Advanced Electronic Signatures (XAdES).

[ETSI-102-778] ETSI TS 102 778 (2009-07) Electronic Signature and Infrastructure (ESI) – PDF Advanced Electronic Signature (PAdES).

[RFC2315] B.Kaliski, PKCS#7: Cryptographic Message Syntax Standard - Version 1.5. RFC2315. 1998. http://datatracker.ietf.org/doc/rfc2315

[RFC5652] R.Housley. Cryptographic Message Syntax (CMS). RFC5652. 2009. http://datatracker.ietf.org/doc/rfc5652

[RFC3275] D.Eastlake, J.Reagle, D.Solo, (Extensible Markup Language) XML-Signature Syntax and Processing, RFC3275. 2002. http://datatracker.ietf.org/doc/rfc3275

[ETSI-11-612] ETSI TS 119 612 V2.1.1 (2015-07) Electronic Signatures and Infrastructures (ESI); Trusted Lists

[OASIS-DSS-Core] S.Drees et al., Digital Signature Service Core Protocols and Elements OASIS. 2007. http://docs.oasis-open.org/dss/v1.0/oasis-dss-core-spec-v1.0-os.html

[OASIS-DSS-Gateway] OASIS Digital Signature Service Signature Gateway Profile. 2007. http://docs.oasis-open.org/dss/v1.0/oasis-dss-profiles-SignatureGateway-spec-v1.0-os.html

[OASIS-DSS-X] OASIS Digital Signature Service eXtended Technical Committee draft documents. http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=dss-x

[PDF] Adobe Systems Inc., PDF Reference – Fifth Edition – Adobe Portable Document Format Version 1.6. 2004. http://partners.adobe.com/public/developer/en/pdf/PDFReference16.pdf

[RFC 3029] Internet X.509 Public Key Infrastructure; Data Validation and Certification Server Protocols https://tools.ietf.org/html/rfc3029

[RFC2560] M.Myers, R.Ankney, A.Malpani, S.Galperin, C.Adams. Internet X.509 Public Key Infrastructure Online Certificate Status Protocol – OCSP, RFC2560. 1999. http://datatracker.ietf.org/doc/rfc5055

[RFC3377] J.Hodges, R.Morgan. Lightweight Directory Access Protocol (v3): Technical Specification. RFC3377. 2002. http://datatracker.ietf.org/doc/rfc3377

[RFC4346] T.Dierks, E.Rescorla. The Transport Layer Security (TLS) Protocol Version 1.1. RFC4346. 2006. http://datatracker.ietf.org/doc/rfc4346

[SOAP] Simple Object Access Protocol v1.2 (second edition), parts 0-3. W3C Recommendations. 2007. http://www.w3.org/TR/2007/REC-soap12-part0-20070427 http://www.w3.org/TR/2007/REC-soap12-part1-20070427 http://www.w3.org/TR/2007/REC-soap12-part2-20070427

[TSL-HR] EU Trust Status List of national TSL issuer, human readable (PDF) format. 2010. https://ec.europa.eu/information_society/policy/esignature/trusted-list/tl-hr.pdf

[TSL-MP] EU Trust Status List of national TSL issuer, machine processable (XML) format. 2010. https://ec.europa.eu/information_society/policy/esignature/trusted-list/tl-mp.xml

[XKMS] XML Key Management Specification (XKMS 2.0) Version 2.0, W3C Recommendation. 2005. http://www.w3.org/TR/2005/REC-xkms2-20050628 http://www.w3.org/TR/2005/REC-xkms2-bindings-20050628

[Validation model] How to avoid the Breakdown of Public Key Infrastructures Forward Secure Signatures for Certificate Authorities, J. Braun, A. Hulsing, A. Wiesmaier, M. Vigil, J. Buchmann

3 Definicje i skróty

Certum QESValidationQ – oznaczenie kwalifikowanej usługi walidacji i konserwacji kwalifikowanych podpisów elektronicznych i pieczęci elektronicznych świadczonej przez Certum

API	Interfejs oprogramowania
CA	Urząd certyfikacji
CAdES	CMS Advanced Electronic Signatures [ETSI-101-733]
CMS	Cryptographic Message Syntax [RFC5652]
CRL	Lista certyfikatów unieważnionych
DSS	Digital Signature Standard (OASIS) [OASIS-DSS-Core]
eID	Tożsamość elektroniczna
eIDAS	Rozporządzenie Parlamentu Europejskiego (EU) nr 910/2014
EU	Unia Europejska
ETSI	Europejski Instytut Norm Telekomunikacyjnych
ESI	Komitet Techniczny Podpisów Elektrocznicznych i Infrastruktury w ETSI.
GUI	Graficzny interfejs użytkownika
OASIS	Organization for the Advancement of Structured Information Standards
OCSP	Online Certificate Status Protocol [RFC2560]
PDF	Przenośny format dokumentu [PDF]
PDS	Konserwacja podpisów elektronicznych (ang. Preservation of Digital Signatures)
PAdES	PDF Advanced Electronic Signatures [ETSI-102-778]
PEPPOL	Pan European Public Procurement On-Line [PEPPOL]
PKI	Infrastruktura klucza publicznego
PKCS	Zbiór standardów kryptografii klucza publicznego
PoE	Proof of Evidence
RFC	Request For Comments (Internet publication)
SOAP	Simple Object Access Protocol [SOAP]
TC ESI	Technical Committee Electronic Signatures and Infrastructures
TLS	Transport Layer Security [RFC4346]
TSA	Urząd znacznika czasu [RFC3628]
TSL	Trust Status List [ETSI-102-231]
WST	Usługa konserwacji z przechowywaniem (ang. Preservation Service with storage)
VA	Urząd walidacji danych
VS	Usługa walidacji
XAdES	XML Advanced Electronic Signatures [ETSI-101-933]
XKMS	XML Key Management Specification [XKMS]
XML	Rozszerzalny Język Znaczników [XML]
XML DSIG	XML Digital Signature [RFC3275]

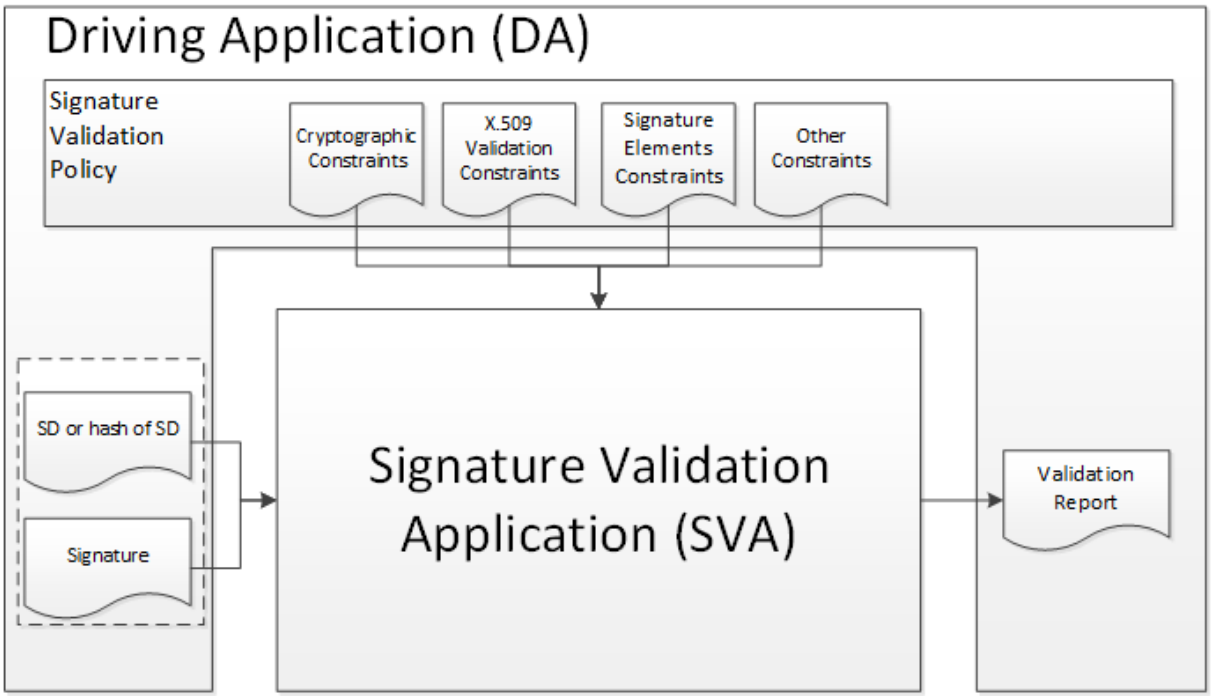
4 Walidacja i konserwacja podpisu

Zbiór procedur usługa walidacji i konserwacji Certum umożliwiających sprawdzenie czy podpis elektroniczny lub pieczęć elektroniczna jest technicznie ważny oparty jest o proces opisany w ETSI 119 120 [ETSI-119-102].

W przypadku gdy poniższy dokument nie zawiera opisu szczególnych wymagań, zakłada się, że wymagania i zasady z dokumentu ETSI TS 119 102 Pkt 5 są spełnione w całości. W przypadku gdy poniższy dokument zawiera opis wymagań i zasad oznacza to, że mają one pierwszeństwo przed odpowiadającymi im wymaganiami z ETSI TS 119 102. W przypadku rozbieżności między poniższym dokumentem, a dokumentem ETSI TS 119 102 w pozostałych kwestiach poniższy dokument ma pierwszeństwo.

Niniejszy dokument zawiera opis mechanizmów konserwacji, które można wykorzystać do zachowania długookresowej ważności dowodowej podpisów elektronicznych lub do konserwacji obiektów przy użyciu technik podpisu elektronicznego. Mechanizmy te wspierają kwalifikowaną usługę konserwacji zgodnie z Artykułem 34 oraz 40 Rozporządzenia (EU) No 910/2014.

4.1 Model walidacji podpisu



Schemat 1 Model koncepcyjny aplikacji do walidacji podpisu

Powyższy schemat modelu koncepcyjnego aplikacji do walidacji podpisu został zaproponowany w specyfikacji technicznej ETSI 319 102. Poszczególne elementy schematu oznaczają:

- Driving Application (DA) – aplikacja sterująca; aplikacja wykorzystująca system walidacji podpisów w celu walidacji podpisów
- Signature Validation Policy – polityka walidacji podpisu; zbiór zasad mających zastosowanie do co najmniej jednego podpisu elektronicznego, który definiuje techniczne i proceduralne wymagania dotyczące ich walidacji, w celu spełnienia określonej potrzeby biznesowej, w ramach której podpis elektroniczny można uznać za ważny
- Cryptographic Constraints – zasady kryptograficzne; zbiór stosowanych reguł, wartości, zakresów i wyników obliczeń w dziedzinie kryptografii, według których jest walidowany podpis
- X.509 Validation Constraints – zasady dotyczące walidacji X.509
- Signature Elements Constraints – zasady dla elementów podpisu
- Other Constraints – inne zasady
- SD or hash of SD – dane podpisane bądź skrót z danych podpisanych
- Signature - podpis
- Signature Validation Application (SVA) – aplikacja walidująca podpisy
- Validation Report – raport z walidacji

Zgodnie z modelem koncepcyjnym aplikacji do walidacji podpisu usługa Certum jest komponentem SVA. SVA jest wywoływana przez aplikację sterującą (DA), do której zwracany jest następnie wynik procesu walidacji w formie raportu z procesu walidacji. Aplikacje sterująca (DA) dla usługi CERTUM występuje pod postacią:

- Aplikacji webowej z graficznym interfejsem użytkownika,
- Klienta zgodnego z protokołem DVCS,
- Klienta zgodnego z protokołem OASIS-DSS,
- Klienta zgodnego z protokołem XKMS,
- Bramki walidacji,

Wyżej wymienione aplikacje sterujące (DA) realizowane są w postaci interfejsu webowego lub Bramki Walidacji opisanej w rozdziale 7..

4.1.1 Wybór procesu walidacji

Usługa Certum QESValidationQ wspiera proces walidacji kwalifikowanych podpisów w następujących przypadkach: podpisów standardowych, podpisów oznakowanych czasem oraz podpisów z długoterminową wartością dowodową.

Nie ma możliwości wyboru przypadku, według którego ma zostać wykonana walidacja przez Aplikację Sterującą (DA) .

4.1.2 Opis wyników procesu walidacji podpisu oraz raportu z procesu walidacji

Usługa Certum dostarcza pełny raport z procesu walidacji, umożliwiający DA sprawdzanie poszczególnych kroków podjętych w procesie walidacji wraz z możliwością sprawdzenia przyczyny zwrócenia takiego, a nie innego wyniku procesu.

W przypadku korzystania przez użytkownika z aplikacji webowej dostarczonej wraz z usługą Certum, bądź z Bramki Walidacji (opisanej w rozdziale 7), raport z procesu walidacji przedstawiany jest w czytelnej dla użytkownika formie pliku PDF.

Wynik procesu walidacji podpisu składa się z:

- statusu procesu walidacji,
- unikalnego identyfikatora wydanego poświadczenia,
- daty wraz z godziną, dla której wskazany wynik procesu walidacji jest obowiązujący, wraz z informacją jaka data została wykorzystana w procesie walidacji,
- dodatkowych danych opisanych w tabeli poniżej,
- powodu złożenia podpisu, jeżeli został on dołączony do sprawdzanego podpisu

Tabela 1 Statusy procesu walidacji podpisu

Status	**Opis**	**Informacje dodatkowe załączone w raporcie**
TOTAL-PASSED	Wynik TOTAL-PASSED (CAŁKOWICIE POZYTYWNY) w procesie walidacji zwracany jest, gdy: • weryfikacja kryptograficzna podpisu powiodła się (w tym kontrola wartości skrótów poszczególnych obiektów danych, które zostały podpisane pośrednio); • wszelkie wymogi dotyczące poświadczenia tożsamości osoby podpisującej zostały zweryfikowane pozytywnie (np. certyfikat podpisującego został uznany za zaufany) • podpis został pozytywnie oceniony pod kątem	W wyniku procesu walidacji wyświetlana jest ścieżka zaufania certyfikatu użytego w procesie podpisywania dokumentu wraz z szczególnymi atrybutami podpisanymi, jeżeli wystąpiły i zostały uznane za dowód walidacji.

	wymagań w procesie walidacji, tym samym uznaje się go za zgodny z tymi wymaganiami	
TOTAL-FAILED	Wynik TOTAL-FAILED (CAŁKOWICIE NEGATYWNY) w procesie walidacji otrzymujemy w przypadku gdy weryfikacja kryptograficzna podpisu nie powiodła się (w tym kontrola wartości skrótów poszczególnych obiektów danych, które zostały podpisane) lub zostało udowodnione, że podpis został złożony po dacie odwołania powiązanego z nim certyfikatu.	W wyniku procesu walidacji podane są dodatkowe informacje, w celu wyjaśnienia przyczyny wystąpienia statusu CAŁKOWICIE NEGATYWNY
INDETERMINATE	Dostępne informacje są niewystarczające do stwierdzenia czy certyfikat powinien mieć status CAŁKOWICIE POZYTYWNY lub CAŁKOWICIE NEGATYWNY	W wyniku procesu walidacji podane są dodatkowe informacje, w celu wyjaśnienia przyczyny wystąpienia statusu NIEOKREŚLONY wraz z informacją, dla strony weryfikującej, jakich danych brakuje do poprawnego przejścia pełnego procesu weryfikacji.

Tabela 2 Struktura i opis raportu walidacji

Status	**Status podrzędny**	**Opis**	**Informacje dodatkowe załączone w raporcie**
TOTAL-FAILED	HASH_FAILURE	Proces walidacji podpisu zwraca w wyniku status CAŁKOWICIE NEGATYWNY, jeśli co najmniej jedna z wartości skrótów podpisanych danych załączonych w procesie składania podpisu nie jest równa odpowiadającej wartości skrótu w weryfikowanym podpisie.	Proces walidacji podpisu jednoznaczne wskazanie, który z elementów podpisanych danych spowodował negatywny wynik weryfikacji podpisu.
	FORMAT_FAILURE	Podpis nie jest zgodny z żadnym ze wspieranych standardów do tego	Proces walidacji dostarcza informacji wskazujących,

		stopnia, że niemożliwym jest przeprowadzenie weryfikacji kryptograficznej podpisu.	dlaczego analiza podpisu nie powiodła się.
	SIG_CRYPTO_FAILURE	Proces walidacji podpisu zwraca w wyniku status CAŁKOWICIE NEGATYWNY, jeśli wartość podpisu nie może zostać zweryfikowana za pomocą klucza publicznego zawartego w certyfikacie podpisującego.	Proces walidacji zwraca wykorzystany do weryfikacji certyfikat podpisującego.
	REVOKED	Proces walidacji podpisu zwraca w wyniku • CAŁKOWICIE NEGATYWNY, jeśli certyfikat podpisującego został odwołany oraz • gdy istnieje dowód na to, że moment złożenia podpisu nastąpił po odwołaniu certyfikatu podpisującego	Proces walidacji zwraca następujące informacje: • Ścieżkę certyfikacji użytą w procesie weryfikacji • Czas oraz jeśli jest dostępny powód odwołania certyfikatu podpisującego • Listę CRL, jeśli jest dostępna, na której certyfikat otrzymał status odwołany • Znacznik czasu z podpisu, z niepodpisanych atrybutów, jeśli są dostępne, które mogą wskazywać na najstarszy moment istnienia złożonego podpisu
NIEOKREŚLONY	SIG_CONSTRAINTS_FAILURE	Proces walidacji podpisu zwraca w wyniku status NIEOKREŚLONY, jeśli jeden lub więcej atrybutów podpisu nie spełniają wymogów procesu walidacji	Proces walidacji zwraca następujące informacje: • Ścieżkę zaufania użytą w procesie weryfikacji • Dodatkowe informacje na temat przyczyny

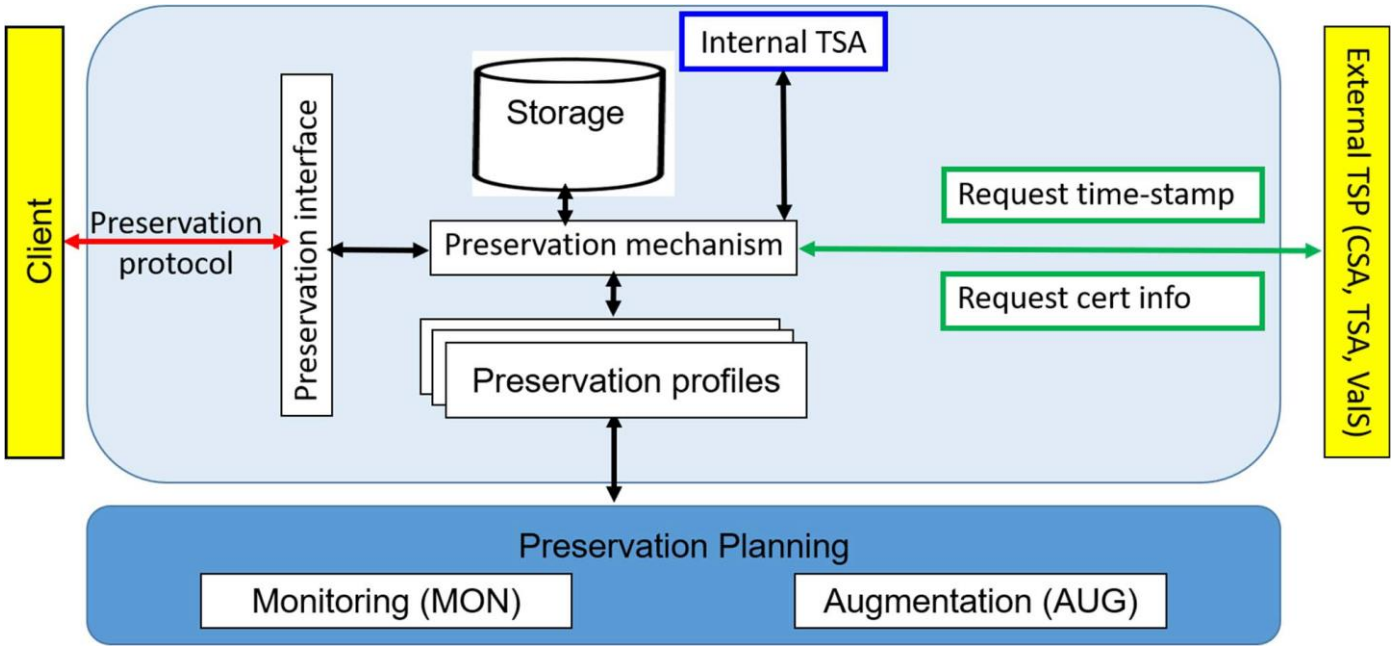
	CHAIN_CONSTRAINTS_FAILURE	Proces walidacji podpisu zwraca w wyniku status NIEOKREŚLONY, jeśli ścieżka zaufania wykorzystana w procesie walidacji nie jest zgodna z wymaganiami procesu walidacji związanymi z certyfikatem podpisującego	Proces walidacji wraca następujące informacje: • Ścieżkę zaufania użytą w procesie weryfikacji • Dodatkowe informacje na temat przyczyny
	CERTIFICATE_CHAIN_GENERAL_FAILURE	Proces walidacji podpisu zwraca w wyniku status NIEOKREŚLONY, jeśli zbiór dostępnych certyfikatów przeznaczonych do weryfikacji ścieżki zaufania zwraca błąd z nieznanego powodu	Proces walidacji wraca następujące informacje: • Dodatkowe informacje na temat przyczyny
	CRYPTO_CONSTRAINTS_FAILURE	Proces walidacji podpisu zwraca w wyniku status NIEOKREŚLONY, jeśli co najmniej jeden z użytych algorytmów w elementach podpisu lub długość klucza algorytmu jest poniżej wymaganego poziomu bezpieczeństwa, oraz: • element ten wygenerowano po okresie czasu, w którym dany algorytm / klucz był uznawany za bezpieczny (na przykład, gdy data wygenerowania jest znana); • element ten nie jest chroniony przez wystarczająco silny znacznik czasu zastosowany w okresie czasu, w	Proces walidacji zwraca następujące informacje: • Identyfikacja elementu (podpis, certyfikat), który jest wygenerowany przy użyciu algorytmu lub klucza kryptograficznego o długości poniżej wymaganego poziomu bezpieczeństwa.

		którym algorytm / klucz uznawano za bezpieczny.	
	EXPIRED	Proces walidacji podpisu zwraca w wyniku status NIEOKREŚLONY, jeśli data złożenia podpisu jest późniejsza niż data wygaśnięcia (Ważny do) certyfikatu podpisującego	Proces walidacji wraca następujące informacje: • Ścieżkę zaufania użytą w procesie weryfikacji
	NOT_YET_VALID	Proces walidacji podpisu zwraca w wyniku status NIEOKREŚLONY, jeśli data złożenia podpisu jest wcześniejsza niż data obowiązywania certyfikatu podpisującego	
	NO_SIGNING_CERTIFICATE_FOUND	Proces walidacji podpisu zwraca w wyniku status NIEOKREŚLONY w przypadku, gdy certyfikat podpisującego nie może zostać zidentyfikowany.	
	NO_CERTIFICATE_CHAIN_FOUND	Proces walidacji podpisu zwraca w wyniku status NIEOKREŚLONY w przypadku, gdy dla wskazanego certyfikatu podpisującego nie udało się zbudować ścieżki zaufania.	
	REVOKED_NO_POE	Proces walidacji podpisu zwraca w wyniku status NIEOKREŚLONY w przypadku, gdy certyfikat podpisującego został odwołany w momencie walidacji podpisu. Jednakże algorytm walidacji podpisu nie może stwierdzić czy data złożenia podpisu znajduje się przed czy po	Proces walidacji zwraca następujące informacje: • Ścieżkę zaufania użytą w procesie weryfikacji • Czas oraz jeśli jest dostępny powód odwołania certyfikatu podpisującego

		dacie odwołania certyfikatu.	
	OUT_OF_BOUNDS_NO_POE	Proces walidacji podpisu zwraca w wyniku status NIEOKREŚLONY w przypadku, gdy certyfikat podpisującego jest przedawniony lub nie jest jeszcze aktywny w czasie procesu walidacji oraz algorytm walidacji podpisu nie może stwierdzić czy data złożenia podpisu znajduje się w przedziale ważności certyfikatu podpisującego.	
	CRYPTO_CONSTRAINTS_FAILURE_NO_POE	Proces walidacji podpisu zwraca w wyniku status NIEOKREŚLONY, jeśli co najmniej jeden z użytych algorytmów w elementach podpisu lub długość klucza algorytmu jest poniżej wymaganego poziomu bezpieczeństwa oraz nie istnieje dowód, że wskazane elementy podpisu zostały wygenerowane w okresie czasu, w którym dany algorytm / klucz był uznawany za bezpieczny	Proces walidacji wraca następujące informacje: • Identyfikacja elementu (podpis, certyfikat), który jest wygenerowany przy użyciu algorytmu lub klucza kryptograficznego o długości poniżej wymaganego poziomu bezpieczeństwa.
	NO_POE	Proces walidacji podpisu zwraca w wyniku status NIEOKREŚLONY jeśli brakuje dowodu umożliwiającego jednoznacznie stwierdzić, że obiekt został podpisany zanim nastąpiło zdarzenie kompromitujące (np. złamanie algorytmu).	Proces walidacji identyfikuje co najmniej jeden obiekt dla którego POE jest niedostępne. Proces walidacji dostarcza dodatkowych informacji o występującym błędzie.

	TRY_LATER	Proces walidacji podpisu zwraca w wyniku status NIEOKREŚLONY, jeśli wszystkie wymogi nie mogą zostać spełnione ze względu na brak informacji. Jednakże istnieje możliwość ponownego wykonania procesu walidacji z wykorzystaniem dodatkowych informacji dotyczących odwołania certyfikatu, które będą dostępne w późniejszym czasie.	
	SIGNED_DATA_NOT_FOUND	Proces walidacji podpisu zwraca w wyniku status NIEOKREŚLONY, jeśli podpisane dane nie mogą zostać pobrane.	Proces walidacji wraca następujące informacje: • Identyfikacja miejsca, w którym znajdowały się dane których nie można było pobrać (np. URL)
	GENERIC	Proces walidacji podpisu zwraca w wyniku status NIEOKREŚLONY w przypadku, gdy wystąpił jakikolwiek inny błąd nie opisany w tej tabeli	Proces walidacji zwraca następujące informacje: • Dodatkowe informacje, dlaczego status walidacji został uznany jako nieokreślony

4.2 Model Konserwacji Podpisu



Rysunek 2 Model koncepcyjny usługi konserwacji z przechowywaniem

Powyższy schemat modelu koncepcyjnego usługi konserwacji z przechowywaniem został zaproponowany w specyfikacji technicznej ETSI 119 511. Poszczególne elementy schematu oznaczają:

- Client – Subskrybent usługi; osoba prawna lub fizyczna przekazujące dane usłudze w celu ich konserwacji
- Preservation protocol – protokół do komunikacji pomiędzy Subskrybentem a usługą;
- Preservation interface – komponent implementujący protokół konserwacji po stronie usługi;
- Storage – magazyn danych;
- Preservation mechanism – mechanizm konserwacji; mechanizm stosowany do utrzymania długoterminowej ważności dowodowej konserwowanych obiektów;
- Preservation profiles – profil konserwacji; unikalnie zidentyfikowany zestaw szczegółów implementacji związanych z modelem konserwacji, który określa m.in. sposób generowania i walidacji dowodów konserwacji;
- Internal TSA – wewnętrzny urząd znakowania czasem;
- Preservation Planning – planowanie konserwacji; komponent odpowiedzialny za monitorowanie i augmentację dowodów konserwacji;
- Monitoring (MON) – monitorowanie algorytmów kryptograficznych;
- Augumentation (AUG) – augmentacja dowodów konserwacji;
- Request time-stamp – żądanie znakowania czasem;
- Request cert info – żądanie informacji o certyfikacie;
- External TSP (CSA, TSA, ValS) – zewnętrzne usługi zaufania CSA Certificate Status Authorities, TSA TimeStamp Authorities, ValS Validation Service.

Wymagania nakładane na usługę konserwacji przez rozporządzenie eIDAS ściśle wiążą tę usługę z usługą walidacji.

Do najważniejszych wymagań należą:

- Usługa konserwacji waliduje przedłożone dane zgodnie z polityką walidacji podpisu i weryfikuje czy przedłożone dane są odpowiednie,
- Usługa konserwacji dostarcza dowodu istnienia podpisu i danych walidacyjnych niezbędnych w procesie walidacji podpisu z użyciem technik podpisu elektronicznego,
- Usługa konserwacji dostarcza dowodu istnienia podpisu i danych walidacyjnych niezbędnych w procesie walidacji podpisu i dowodu istnienia podpisanych danych, jeżeli podpisane dane zostały dostarczone do usługi,
- W przypadku podpisów zewnętrznych bądź jeżeli Subskrybent używa Bramki Walidacji, usługa konserwacji pozwala Subskrybentowi na dostarczenie tylko skrótu z podpisanych danych zamiast pełnych podpisanych danych – QTSP zaznacza w profilu konserwacji funkcje skrótu, które mogą być użyte.

Usługa Certum działając jako usługa konserwacji, wykorzystuje usługę walidacji do sprawdzenia poprawności przesłanych podpisów. Następnie zbiera dowody konserwacji. Dowody są zabezpieczone kryptograficznie i przechowywane przez okres określony w profilu konserwacji.
Dowody zabezpieczane są za pomocą kwalifikowanego znacznika czasu dostarczanego przez Certum QTSA.

5 Polityka Walidacji i Konserwacji

Usługa Certum QESValidationQ działa zgodnie z domyślną polityką walidacji i konserwacji.

Nie ma możliwości skonfigurowania osobnych wymogów dla procesu walidacji i konserwacji dla każdej ze stron ufających.

5.1 Zasady procesu walidacji

Wymogi dla procesu walidacji w usłudze Certum QESValidationQ są definiowane w danych kontrolnych systemu oraz przez samą implementację usługi.

Wszelkie zasady walidacji, które nie wynikają z implementacji, wynikają bezpośrednio z samej treści podpisu (zawartej w atrybutach podpisanych) lub pośrednio, tj. przez odwołanie do zewnętrznego dokumentu, dostarczonego w formie przetwarzalnej maszynowo.

5.1.1 Zasady ogólne

Usługa Certum QESValidationQ działa według następujących zasad:

Tabela 1

Zasada (a)	Wartość
Usługa TSA wykorzystana do znakowania czasem poświadczeń walidacji	CERTUM QTST
Maksymalny rozmiar pliku obsługiwanych dokumentów	10MB

5.1.2 Zasady procesu walidacji odniesione do standardu X.509

UsługaCertum QESValidationQ wspiera następujące wymagania w procesie walidacji X.509, znajdujące się w dokumencie ETSI TS 119 172-1 [ETSI 119 172-1], pkt A.4.2.1, tabela A.2 wiersz m.

Tabela 2

Zasada (a)	Wartość
(m)1.1. SetOfTrustAnchors: Zbiór punktów zaufania (ang. TA Trust Anchors) wymaganych w procesie walidacji	EU TSL
• (m)1.3. user-initial-policy-set: Wymaganie opisane w domumencie IETF RFC 5280 pkt 6.1.1 podpunkt (c) • (m)1.4. initial-policy-mapping-inhibit: Wymaganie opisane w domumencie IETF RFC 5280 pkt 6.1.1 podpunkt (e) • (m)1.5. initial-explicit-policy: Wymaganie opisane w domumencie IETF RFC 5280 pkt 6.1.1 podpunkt (f) • (m)1.6. initial-any-policy-inhibit: Wymaganie opisane w domumencie IETF RFC 5280 pkt 6.1.1 podpunkt (g) • (m)1.7. initial-permitted-subtrees: Wymaganie opisane w domumencie IETF RFC 5280 pkt 6.1.1 podpunkt (h) • (m)1.8. initial-excluded-subtrees: Wymaganie opisane w domumencie IETF RFC 5280 pkt 6.1.1 podpunkt (i) • (m)1.9. path-length-constraints: Wymaganie określające maksymalną ilość certyfikatów	Brak

CA w ścieżce certyfikacji. Może wystąpić potrzeba określenia wartości początkowych w celu obsłużenia pozostałych przypadków (np. zignorowanie wymagania) • (m)1.10. policy-constraints: Wymaganie dotyczące polityki certyfikacji zawartej w certyfikacie. Może wystąpić potrzeba określenia wartości początkowych w celu obsłużeniu pozostałych przypadków (np. zignorowanie wymagania)	
(m)2.1. RevocationCheckingConstraints: Wymaganie związane ze sprawdzaniem odwołania weryfikowanego certyfikatu. Określa czy w przypadku czy wymagane jest sprawdzenie odwołania certyfikatu oraz czy sprawdzane jest za pomocą odpowiedzi z OCSP czy należy wykorzystać listę CRL. Poniżej opis wymagań: – clrCheck: Weryfikacja powinna odbywać na podstawie aktualnej listy CRL (or Authority Revocation Lists); – ocspCheck: Do weryfikacji status(odwołania) certyfikatu powinien zostać wykorzystany OCSP IETF RFC 6960; – bothCheck: Powinna zostać przeprowadzona weryfikacja OCSP oraz CRL – eitherCheck: Powinna zostać przeprowadzona weryfikacja OCSP lub CRL – noCheck: Weryfikacja nie jest obowiązkowa.	eitherCheck (sprawdzenie jednego z wymagań)
(m)2.2. RevocationFreshnessConstraints: Wymaganie dotyczące informacji o odwołaniu certyfikatu i związanych z nimi zakresów dat. Wymagania określające maksymalną akceptowalną różnicę między datą wydania informacji o statusie odwołania certyfikatu oraz datą uprawomocnienia się odwołania. Wymaganie pozwalające SVA akceptować jedynie informacje dotyczące odwołania certyfikatu stworzone po dacie złożenia podpisu elektronicznego.	Nie
(m)2.3. RevocationInfoOnExpiredCerts: Wymaganie dotyczące certyfikatu podpisującego stosowanego w walidacji podpisu wydanego przez urząd certyfikacji, który zachowuje	Nie

informacje dotyczące unieważnionych certyfikatów przez dłuższy niż wymagany minimalny okres czasu na ich przechowywanie.	
(m)3. LoAOnTSPPractices: wskazuje wymagany poziom LoA dla praktyk stosowanych przez TSP wydających certyfikaty	Nie
EUQualifiedCertificateRequired	Tak
EUQualifiedCertificateSigRequired	Tak
EUQualifiedCertificateSealRequired	Tak
PKIX Certification Path Validation Model	Chain model
Cache dla list CRL włączony	Tak
Czas życia pamięci podręczne list CRL Maksymalny okres czasu, w którym lista CRL może być przechowywana w pamięci podręcznej	30 sekund
TSLUnavilable W przypadku gdy TSL jest niedostępne	Ostatni dostępny
Wpływ znaczników czasu na wynik walidacji	Tylko kwalifikowane znaczniki czasu

5.1.3 Zasady Kryptograficzne

Usługa Certum QESValidationQ obsługuje następujące wymagania kryptograficzne, które dotyczącą algorytmów i parametrów stosowanych podczas tworzenia podpisów lub użytych w procesie walidacji podpisanego obiektu, określone w ETSI TS 119 172-1 [ETSI 119 172-1], pkt A.4.2.1, tabela A.2 wiersz p.

Tabela 3

Zasada	Wartość
(p)1. CryptographicSuitesConstraints: wskazuje wymagania dla algorytmów i parametrów używanych podczas tworzenia podpisów bądź używanych podczas walidacji podpisanych obiektów występujących w procesie walidacji bądź augmentacji (np. podpis, certyfikaty, listy CRL, odpowiedzi OCSP, znaczniki czasu).	Zgodnie z ETSI TS 119 312 [ETSI 119 312]

5.1.4 Zasady dotyczące elementów podpisu elektronicznego

Usługa CERTUM QESValidationQ obsługuje następujące wymagania dla elementów podpisu dotyczące DTBS znajdujące się w ETSI TS 119 172-1 119 172-1 ETSI [ETSI 119 172-1], pkt A.4.2.1, tabela A.2 wiersz B.

Tabela 4

Zasada(s)	Constraint value at signature validation (SVA or DA)
(b)1. ConstraintOnDTBS - wskazuje wymagania dla typu danych, jakie można podpisać	Brak
(b)2. ContentRelatedConstraintsAsPartOfSignatureElements: Ten zbiór zasad wskazuje wymagane elementy informacji związane z treścią w postaci podpisanych bądź niepodpisanych atrybutów, które mają być obecne w podpisie. Zbiór zawiera: (b)2.1 MandatedSignedQProperties-DataObjectFormat wymaga określonego formatu treści podpisywanej przez osobę podpisującą (b)2.2 MandatedSignedQProperties-content-hints wymaga określonych informacji opisujących najbardziej wewnętrzną podpisaną treść wielowarstwowej wiadomości, w której jedna treść jest umieszczona w innej dla treści podpisywanej przez osobę podpisującą (b)2.3 MandatedSignedQProperties-content-reference wymaga włączenia informacji o sposobie łączenia żądań i odpowiedzi między dwiema stronami bądź o sposobie w jaki należy utworzyć takie łącze, itp. (b)2.4 MandatedSignedQProperties-content-identifier wymaga obecności i opcjonalnej wartości identyfikatora, którego można uzyć później w atrybucie „content-reference”.	Brak
(b)3. DOTBSAsAWholeOrInParts: wskazuje, czy wszystkie dane, czy tylko niektóre z nich, muszą być podpisane. Semantyka dla możliwego zbioru wartości to: • całość: całe dane musza być podpisane, • część: tylko niektóre części danych muszą być podpisane. W tym przypadku należy użyć dodatkowych informacji, aby określić, które części mają zostać podpisane.	Brak

5.2 Wspierane formaty podpisów i pieczęci elektronicznych wraz z ich poziomami

Formaty podpisów i pieczęci elektronicznych obsługiwanych przez usługę Certum QESValidationQ zgodne są dyrektywami UE [EU 2015/1506]:

[1] ETSI TS 103 171 V2.1.1 (2012-03) Electronic Signatures and Infrastructures (ESI); XAdES Baseline Profile

[2] ETSI TS 103 173 V2.2.1 (2013-04) Electronic Signatures and Infrastructures (ESI); CAdES Baseline Profile

[3] ETSI TS 103 172 V2.2.2 (2013-04) Electronic Signatures and Infrastructures (ESI); PAdES Baseline Profile

[4] ETSI TS 103 174 V2.2.1 (2013-06) Electronic Signatures and Infrastructures (ESI); ASiC Baseline Profile

5.2.1 Ograniczenia dotyczące wspieranych formatów podpisów i pieczęci elektronicznych

Tabela 5

Położenie podpisu oraz podpisanych danych Liczba podpisów oraz podpisanych danych	Wartość
Podpisy otaczane	tak
Podpisy otaczające	tak
Podpisy zewnętrzne	tak
Jednoczesne występowanie wielu pozycji względnych	tak
Jeden dokument z więcej niż jednym podpisem	tak

5.3 Kwalifikowany podpis/pieczęć elektroniczna oparta na długookresowej dostępności danych walidacyjnych

Usługa Certum pozwala na konserwację zaawansowanych podpisów bądź zaawansowanych pieczęci elektronicznych złożonych z użyciem kwalifikowanego certyfikatu jak zdefiniowano w Rozporządzeniu eIDAS poprzez znakowanie czasem dla uzyskania dowodu istnienia. Zgromadzone dowody są sukcesywnie znakowane czasem, przed wygaśnięciem certyfikatu wcześniejszego znacznika czasu bądź kiedy algorytmy

zostaną uznane za zbyt słabe dla długookresowej ochrony. Rekomendację dla zbioru wspieranych algorytmów oparte są na ETSI TS 119 312.

5.3.1 Profil konserwacji

Usługa konserwacji oparta jest na usłudze walidacji, która przechowuje lokalnie dane walidacyjne dla kwalifikowanych urzędów certyfikacji. Dane walidacyjne zbierane są codziennie. Takie podejście uniezależnia usługę od dostępności danych walidacyjnych dla całego przedziału czasowego konserwacji.

Przez cały okres konserwacji stosowana będzie ta sama polityka konserwacji.

Po upływie okresu obowiązywania umowy Subskrybent, przez 1 miesiąc ma możliwość pobrania pełnego zestawu konserwowanych danych, po czym dane te będą trwale usuwane.

Usługa Certum QESValidationQ implementuje jeden Profil konserwacji, opisany poniżej:

a) Identyfikator: http://uri.etsi.org/19512/scheme/pds+wst+ers
b) Wspierane operacje:
    i. PreservePO
        1. Formaty wejściowe:
            a. Zgodnie z 5.2
            b. Dozwolone funkcje skrótu: zgodnie z 5.1.3
    ii. VerifyRequest
        1. Formaty wejściowe:
            a. Zgodnie z 5.2
            b. Dozwolone funkcje skrótu: zgodnie z 5.1.3
c) Polityka:
    i. Polityka dotycząca zabezpieczenia dowodów: zgodnie z 5.3.2
    ii. Polityka walidacji: zgodnie z rozdziałami 4, 5.1, 5.2.
d) Okres ważności profilu:
    i. Ważny od: z dniem umieszczenia usługi na liście TSL
e) Model przechowywania: konserwacja z przechowywaniem danych (Preservation services with storage (WST))
f) Cel konserwacji: konserwacja podpisów elektronicznych (Preservation of digital signatures (PDS))

g) Format zabezpieczeń: znaczniki czasu

5.3.2 Polityka dotycząca dowodów konserwacji

Polityka dotycząca dowodów konserwacji opisana jest przez następujące zasady:

a) Wersja: 1

b) Użyte algorytmy: RSA-PKCSv1, SHA-512

c) **Punkty zaufania używane do walidacji podpisu elektronicznego pod dowodem konserwacji:** QEsValidationQ identyfikowany przez:

Certificate serial
190776352711112402811911134056768917207409779927

Digest algorithm
SHA512

Issuer
OID.2.5.4.97=VATPL-5250008198, CN=Narodowe Centrum Certyfikacji, O=Narodowy Bank Polski, C=PL

Subject
OID.2.5.4.97=VATPL-5170359458, CN=Certum QESValidationQ 2017, O=Asseco Data Systems S.A., C=PL

Validity
2017-03-15 11:25:12 - 2028-03-16 00:59:59

d) **Punkt zaufania do zweryfikowania znaczników czasu dla dowodów konserwacji:** Certum QTST identyfikowany przez:

Certificate serial
100341102919473197820118384675833212695201296873

Digest algorithm
SHA512

Issuer
OID.2.5.4.97=VATPL-5250008198, CN=Narodowe Centrum Certyfikacji, O=Narodowy Bank Polski, C=PL

Subject
OID.2.5.4.97=VATPL-5170359458, CN=Certum QTST 2017, O=Asseco Data Systems S.A., C=PL

Validity
2017-03-15 11:23:18 - 2028-03-16 00:59:59

h) **Sposób w jaki przedłużana jest ważność dowodów konserwacji:** odnawianie znaczników czasu zgodnie z IETF RFC 4998

i) **Przewidywany okres przechowywania dowodów:** 30 lat

5.3.3 Polityka dla pakietów export-import

Dostęp do konserwowanych podpisów elektronicznych odbywa się według poniższych zasad:

- Dostępne tylko dla uwierzytelnionych Subskrybentów
- Struktura paczki exportu oparta jest o odpowiedź RetrievePOResponse, gdzie znajdziemy żądanie walidacji danych (zawierające podpisane dane, bądź skrót z podpisanych danych), poświadczenie walidacyjne i łańcuch znaczników czasu.
- Usługa konserwacji przechowuje rejestr zdarzeń eksportu paczki zawierający:
  - Datę zdarzenia,
  - Kryteria użyte do wybrania zbioru danych dodawanych do paczki exportu

6 Obsługiwane API

Usługa Certum QESValidationQ dostępna jest dla przetwarzania maszynowego poprzez różne rodzaje API, zarówno oparte na strukturach XML jak i ASN.1. Wspierana jest tylko komunikacja synchroniczna. Poniżej wymieniono wspierane interfejsy:

- OASIS-DSS

Usługa wspiera profil zdefiniowany przez projekt PEPPOL [PEPPOL-D1.3], oparty jest o struktury XML. Protokół pozwala na wysłanie żądań walidacji i konserwacji dla podpisów i pieczęci elektronicznych.

- DVCS

Protokół zdefiniowany w [RFC3029], oparty o struktury ASN.1. Pozwala na walidację podpisów i pieczęci elektronicznych oraz certyfikatów klucza publicznego x.509.

- XKMS

Usługa wspiera profil zdefiniowany w projekcie PEPPOL [PEPPOL-D1.3], oparty jest o struktury XML. Protokół pozwala na wysyłanie żądań weryfikacji certyfikatów klucza publicznego x.509.

7 Opcje dodatkowe

Ten rozdział zawiera opis funkcjonalności, które Certum oferuje dodatkowo.

7.1 Bramka walidacji i konserwacji

Bramka walidacji i konserwacji pozwala na uniknięcie przesyłania do usługi całych podpisanych dokumentów, które mogą zawierać informacje poufne bądź być dużych rozmiarów.

Bramka walidacji jest instalowana (jako pakiet oprogramowania) po stronie infrastruktury informatycznej subskrybenta. Wspiera taki sam interfejs API dla walidacji podpisów i pieczęci elektronicznych jak usługa walidacji.

Do zalet wykorzystania bramki należą:

- zwiększenie wydajności usługi walidacji i konserwacji, w związku z brakiem potrzeby przesyłania dużych całych dokumentów
- bramka zapewnia pojedynczy punkt egzekwowania polityki, ponieważ posiada możliwość określania wymagań dotyczących polityki (parametry żądania) dla wszystkich żądań przechodzących przez nią samą.
- klucze i certyfikaty TLS przeznaczone do uwierzytelnienia i podpisania żądania wysyłanego do usługi, mogą zostać zainstalowane w bramce, zamiast być instalowane, w każdym systemie subskrybenta, który powinien korzystać z usługi
- dwa powyższe punkty dotyczą rownież procesu z wykorzystaniem XKMS, co oznacza, że możliwe jest wykorzystanie bramki wraz z interfejsem XKMS.

7.2 Graficzny interfejs webowy

W ramach usługi Certum dostępny jest graficzny interfejs webowy (GUI), dostępny bezpośrednio dla usługi walidacji lub poprzez Bramkę Walidacji. Poprzez GUI użytkownik może przesłać dokument lub certyfikat, wybrać parametry żądania oraz odpowiedzi, a następnie wysłać żądanie do usługi.

Załącznik A: Związek z Rozporządzeniem Parlamentu Europejskiego i Rady (UE) nr 910/2014

A.1 Walidacja kwalifikowanych podpisów elektronicznych: Artykuł 26, 28 i 32 rozporządzenia eIDAS

Wymagania wymienione w Artykule 32 i 28 pochodzące z Rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 910/2014	Spełnienie wymagań przez usługę walidacji i konserwacji CERTUM
Artykuł 32: Wymogi dla walidacji kwalifikowanych podpisów elektronicznych 1. Proces walidacji kwalifikowanego podpisu elektronicznego potwierdza ważność kwalifikowanego podpisu elektronicznego, pod warunkiem, że:	
(a) certyfikat, który towarzyszy podpisowi, był w momencie składania podpisu kwalifikowanym certyfikatem podpisu elektronicznego zgodnym z załącznikiem I;	Proces walidacji certyfikatu spełnia wymagania opisane w [EU 2015/1505] dla kwalifikowanych dostawców usług zaufania wystawiających certyfikaty kwalifikowane dla podpisów elektronicznych. Ponad zachowano zgodność z załącznikiem A.1 ETSI 119 412-5 [ETSI 119 412-5]
(b) kwalifikowany certyfikat został wydany przez kwalifikowanego dostawcę usług zaufania i był ważny w momencie składania podpisu;	
(c) dane służące do walidacji podpisu odpowiadają danym dostarczonym stronie ufającej;	Gwarantowana poprawnością obsługi formatów podpisu opisanych w 5.2
(d) unikalny zestaw danych reprezentujących podpisującego umieszczony w certyfikacie jest prawidłowo dostarczony stronie ufającej;	Certyfikat podpisującego jest załączony do raportu z przeprowadzonego procesu walidacji dla każdego z protokołów opisanych w Tabela 2 Struktura i opis raportu walidacji
(e) jeżeli w momencie składania podpisu użyty został pseudonim, zostaje to wyraźnie wskazane stronie ufającej;	Zgodnie z [ETSI 119 412-2] użycie pseudonimu jest jawnie wskazywane w polu Podmiot certyfikatu. Dane certyfikatu osoby podpisującej są dostarczane w raporcie z walidacji (Tabela 2 Struktura i opis raportu walidacji)
(f) podpis elektroniczny został złożony za pomocą kwalifikowanego urządzenia do składania podpisu elektronicznego;	Proces walidacji certyfikatu spełnia wymagania opisane w [EU 2015/1505] dla dostawców usług zaufania oraz wystawców certyfikatów

	kwalifikowanych wykorzystywanych do podpisów elektronicznych. W szczególności sprawdzane jest prawidłowe wskazanie charakteru wspieranego SSCD.
(g) integralność podpisanych danych nie została naruszona;	Gwarantowana obsługą modelu walidacji podpisu, opisanym w 4.1
(h) wymogi przewidziane w art. 26 zostały spełnione w momencie składania podpisu.	Przedstawiono poniżej.
2. System wykorzystany do walidacji kwalifikowanego podpisu elektronicznego zapewnia stronie ufającej prawidłowy wynik procesu walidacji i umożliwia stronie ufającej wykrycie wszelkich problemów związanych z bezpieczeństwem.	Proces walidacji podpisu wraz z oznaczeniami statusów opisany w 4.1
Artykuł 28: Kwalifikowane certyfikaty podpisów elektronicznych	
1. Kwalifikowane certyfikaty podpisów elektronicznych muszą spełniać wymogi określone w załączniku I.	Zachowano zgodność z Załącznikiem A.1 ETSI 119 412-5 [ETSI 119 412-5]
2. Kwalifikowane certyfikaty podpisów elektronicznych nie podlegają żadnym obowiązkowym wymogom wykraczającym poza wymogi określone w załączniku I.	Proces walidacji certyfikatu spełnia wymagania opisane w [EU 2015/1505] dla dostawców usług zaufania oraz wystawców certyfikatów kwalifikowanych wykorzystywanych do podpisów elektronicznych. Brak dodatkowej kontroli wykraczającej poza wymagania opisane w załączniku I.
3. Kwalifikowane certyfikaty podpisów elektronicznych mogą zawierać nieobowiązkowe dodatkowe szczególne atrybuty. Atrybuty te nie mogą wpływać na interoperacyjność i uznawanie kwalifikowanych podpisów elektronicznych.	Brak dodatkowej kontroli wykraczającej poza wymagania opisane w załączniku I.
4. Jeżeli kwalifikowany certyfikat podpisów elektronicznych został unieważniony po początkowej aktywacji, traci on ważność od momentu jego unieważnienia i w żadnym przypadku nie	Wymagania dla kwalifikowanych usług zaufania wystawiających kwalifikowane certyfikat do składania podpisów elektronicznych.

można przywrócić jego poprzedniego statusu.	
5. Państwa członkowskie mogą ustanawiać przepisy krajowe dotyczące tymczasowego zawieszenia kwalifikowanego certyfikatu podpisu elektronicznego z zastrzeżeniem następujących warunków: (a)jeżeli kwalifikowany certyfikat podpisu elektronicznego został czasowo zawieszony, certyfikat ten traci ważność na okres zawieszenia; (b)okres zawieszenia jest jasno wskazywany w bazie danych dotyczącej certyfikatów i informacja o zawieszeniu jest widoczna, w okresie zawieszenia, na podstawie usługi informawania o statusie certyfikatu.	Według [ETSI TS 110 102-1] jeśli weryfikacji ścieżki certyfikatu nie powiodą się ponieważ certyfikat podpisującego został czasowo zawieszony usługa CERTUM przerywa proces walidacji i zwraca status NIEOKREŚLONY, z podstatusem TRY_LATER, datą zawieszenia certyfikatu, oraz jeśli dostępna jest zawartość pola nextUpdate – z listy CRL lub odpowiedzi OCSP wykorzystywana będzie jako sugestia kiedy można ponowić próbę weryfikacji.
Artykuł 26: Wymogi dla zaawansowanych podpisów elektronicznych Zaawansowany podpis elektroniczny musi spełniać następujące wymogi:	
(a)jest unikalnie przyporządkowany podpisującemu;	Gwarantowana poprawnością obsługi formatów podpisu 5.2
(b) umożliwia ustalenie tożsamości podpisującego;	
(c)jest składany przy użyciu danych służących do składania podpisu elektronicznego, których podpisujący może, z dużą dozą pewności, użyć pod wyłączną swoją kontrolą; oraz	
(d)jest powiązany z danymi podpisanymi w taki sposób, że każda późniejsza zmiana danych jest rozpoznawalna.	

A.2 Walidacja kwalifikowanych pieczęci elektronicznych: Artykuł 38 i 40 rozporządzenia eIDAS

Wymagania wymienione w Artykule 38 i 40 pochodzące z Rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 910/2014	Spełnienie wymagań przez usługę walidacji i konserwacji CERTUM
Artykuł 38: Kwalifikowane certyfikaty pieczęci elektronicznej	
1. Kwalifikowane certyfikaty pieczęci elektronicznych muszą spełniać wymogi określone w załączniku III.	Zachowano zgodność z Załącznikiem A.2 ETSI 119 412-5 [ETSI 119 412-5]
2. Kwalifikowane certyfikaty pieczęci elektronicznych nie podlegają żadnym obowiązkowym wymogom wykraczającym poza wymogi określone w załączniku III.	Proces walidacji certyfikatu spełnia wymagania opisane w [EU 2015/1505] dla dostawców usług zaufania oraz wystawców certyfikatów kwalifikowanych wykorzystywanych do pieczęci elektronicznych. Brak dodatkowej kontroli wykraczającej poza wymagania opisane w załączniku III.
3. Kwalifikowane certyfikaty pieczęci elektronicznych mogą zawierać nieobowiązkowe dodatkowe szczególne atrybuty. Atrybuty te nie mogą wpływać na interoperacyjność i uznawanie kwalifikowanych pieczęci elektronicznych.	Brak dodatkowej kontroli wykraczającej poza wymagania opisane w załączniku III.
4. Jeżeli kwalifikowany certyfikat pieczęci elektronicznej został unieważniony po początkowej aktywacji, traci on ważność od momentu jego unieważnienia i w żadnym przypadku nie można przywrócić jego poprzedniego statusu.	Wymagania dla kwalifikowanych usług zaufania wystawiających kwalifikowane certyfikat do składania pieczęci elektronicznych.
5. Państwa członkowskie mogą ustanawiać przepisy krajowe dotyczące tymczasowego zawieszenia kwalifikowanych certyfikatów pieczęci elektronicznych z zastrzeżeniem następujących warunków: (a)jeżeli kwalifikowany certyfikat pieczęci elektronicznej został czasowo zawieszony, certyfikat ten traci ważność na okres zawieszenia; (b)okres zawieszenia jest jasno wskazywany w bazie danych dotyczącej certyfikatów i podmiot udzielający	Według [ETSI TS 110 102-1] jeśli weryfikacji ścieżki certyfikatu nie powiodą się ponieważ certyfikat pieczęci został czasowo zawieszony usługa CERTUM przerywa proces walidacji i zwraca status NIEOKREŚLONY, z podstatusem TRY_LATER, datą zawieszenia pieczęci, oraz jeśli dostępna jest zawartość pola nextUpdate – z listy CRL lub odpowiedzi OCSP wykorzystywana będzie jako sugestia kiedy można ponowić próbę weryfikacji.

informacji o statusie certyfikatu zapewnia widoczność statusu zawieszenia podczas okresu zawieszenia.	
Artykuł 40: Walidacja i konserwacja kwalifikowanych pieczęci elektronicznych	
Art. 32, 33 i 34 stosuje się odpowiednio do walidacji i konserwacji kwalifikowanych pieczęci elektronicznych.	

A.3 Kwalifikowana usługa konserwacji kwalifikowanych podpisów elektronicznych: Artykuł 34

Wymagania wymienione w Artykule 34 pochodzące z Rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 910/2014	Spełnienie wymagań przez usługę walidacji i konserwacji CERTUM
Kwalifikowana usługa konserwacji kwalifikowanych podpisów elektronicznych	
Kwalifikowaną usługę konserwacji kwalifikowanych podpisów elektronicznych może świadczyć wyłącznie kwalifikowany dostawca usług zaufania, który stosuje procedury i technologie umożliwiające przedłużenie wiarygodności kwalifikowanego podpisu elektronicznego poza techniczny okres ważności.	Zachowano zgodność z ETSI TS 119 511 V1.1.1 (2019-06).

Załącznik B: Wyjątki dla procesu walidacji podpisów/pieczęci i certyfikatów elektronicznych

B.1 Walidacja kwalifikowanych certyfikatów wydanych przed eIDAS

Zgodnie z punktem 2 Artykułu 51 Rozporządzenia eIDAS

„2. Kwalifikowane certyfikaty wydane osobom fizycznym na mocy dyrektywy 1999/93/WE uznaje się za kwalifikowane certyfikaty podpisów elektronicznych na mocy niniejszego rozporządzenia do czasu ich wygaśnięcia.”

Usługa Certum przyjmuje certyfikaty wydane przed eIDAS za kwalifikowane.

Opis wyjątku	Akt prawny pozwalający na wyjątek
1. polskie kwalifikowane certyfikaty wydane przez 01.07.2016	Dyrektywa 1999/93/WE i Ustawa o Podpisie Elektronicznym z 21.09.2001

Historia

Historia dokumentu		
1.0	03 czerwca 2016 r.	Wersja wstępna
1.1	1 sierpnia 2018	Zmiana adresu Asseco Data Systems S.A.
1.2	1 sierpnia 2019	Dodanie załącznika B Dodanie informacji w punkcie Tabeli 4 na temat akceptacji niekwalifikowanych znaczników czasu
1.3	01 marca 2020	Dodanie w opisie kwalifikowanej usługi konserwacji w rozdziałach 1, 4 i 5. Nowe rozdziały 5.3 i A.3