Warunki użytkowania certyfikatów niekwalifikowanych

Wersja: 1.3
Data: 18 grudnia 2024
Status: aktualny

Asseco Data Systems S.A.
ul. Jana z Kolna 11
80-864 Gdańsk
Certum
ul. Bajeczna 13
71-838 Szczecin
www.certum.pl
www.certum.eu

Spis treści

§1 Definicje....2
§2 Zastosowanie....3
§3 Ograniczenia w użytkowaniu usługi....3
§4 Wydawanie i zarządzanie certyfikatami....3
4.1 Wniosek o wydanie certyfikatu....3
4.2 Weryfikacja....4
4.3 Akceptacja certyfikatu....4
4.4 Wydanie certyfikatu....4
4.5 Unieważnienie certyfikatu....4
4.6 Zawieszenie certyfikatu....6
§5 Zobowiązania....7
5.1 Zobowiązania ADS....7
5.2 Zobowiązania subskrybenta....7
§6 Oświadczenie subskrybenta....8
§7 Gwarancje ADS....8
§8 Zastrzeżenia....9
§9 Informacje kontaktowe....9

§1 Definicje

1. **Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates** – dokument stworzony przez konsorcjum opiniotwórcze CA/Browser Forum zrzeszające szereg urzędów certyfikacji oraz twórców przeglądarek internetowych, wyznaczający standardy opisujące standardy oraz wymagania jakie spełniać muszą urzędy certyfikacji, aby wydawać certyfikaty SSL/TSL. Dokument dostępny jest na stronie http://www.cabforum.org.
2. **Certum** – Powszechne Centrum Certyfikacji (Certum) – jednostka usługowa Asseco Data Systems SA (zwanym dalej ADS) będąca Urzędem Certyfikacji (ang. Certification Authority), świadcząca niekwalifikowane i kwalifikowane usługi certyfikacyjne. Kwalifikowane usługi certyfikacyjne świadczy w zakresie wydawania kwalifikowanych certyfikatów klucza publicznego oraz pozostałych usług certyfikacyjnych zgodnie z Ustawą z dnia 5 września 2016 r. o usługach zaufania oraz identyfikacji elektronicznej (Dz.U. 2016 poz. 1579). Niekwalifikowane usługi świadczy zgodnie w wymaganiami AICPA/CICA WebTrust Program for Certification Authorities oraz Principles and Criteria for Certification Authorities - Extended Validation Audit Criteria.
3. **Certyfikat** – elektroniczne zaświadczenie, które zawiera co najmniej nazwę lub identyfikator urzędu certyfikacji, identyfikator Subskrybenta, jego klucz publiczny, okres ważności certyfikatu, numer seryjny certyfikatu oraz jest podpisane przez Urząd Certyfikacji.
4. **Certyfikaty Code Signing** – certyfikaty wykorzystywane do zabezpieczania kodu źródłowego aplikacji. Przeznaczone dla programistów, służą do ochrony oprogramowania przed sfałszowaniem.
5. **Certyfikaty EV Code Signing** – certyfikat wydany zgodnie z wymaganiami określonymi w dokumencie *Baseline Requirements for the Issuance and Management of Publicly Trusted Code Signing Certificates,* wykorzystywane do zabezpieczania kodu źródłowego aplikacji. Przeznaczone dla programistów, służą do ochrony oprogramowania przed sfałszowaniem.
6. **Certyfikaty S/MIME** – certyfikaty, które umożliwiają szyfrowanie i podpisywanie poczty elektronicznej oraz znajdują zastosowanie w zabezpieczaniu dokumentów elektronicznych. Certyfikaty wydawane zgodnie z wymaganiami określonymi w dokumencie *Baseline Requirements for the Issuance and Management of Publicly-Trusted S/MIME Certificates.*
7. **Certyfikat Premium EV SSL** – certyfikat SSL będący elektronicznym zaświadczeniem wydanym zgodnie z wymaganiami określonymi w dokumencie *Guidelines for the issuance and management of Extended Validation Certificates*, który służy do zabezpieczania transmisji danych między użytkownikiem sieci Web a witryną Internetową, do której przyporządkowany jest certyfikat EV SSL oraz umożliwiający identyfikację właściciela tej witryny.
8. **Certyfikat SSL** – certyfikaty wykorzystywane do uwierzytelnienia subskrybentów (osób prawnych i fizycznych, urządzeń oraz serwisów) stosowane przez globalne oraz ekstranetowe serwisy usługowe pracujące w osłonie protokołu SSL/TLS/WTLS, wydawane zgodnie ze standardem *Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates*.
9. **Certyfikaty VPN** – certyfikaty umożliwiające tworzenie bezpiecznych kanałów komunikacji między użytkownikami sieci publicznych lub lokalnych.
10. **Kodeks Postępowania Certyfikacyjnego** – dokument opisujący szczegółowo proces certyfikacji klucza publicznego, uczestników tego procesu oraz określający obszary zastosowań uzyskanych w jego wyniku certyfikatów, opublikowany w Internecie pod adresem http://www.certum.pl.
11. **Polityka Certyfikacji** – dokument określający ogólne zasady stosowane przez Certum podczas procesu certyfikacji kluczy publicznych, definiujący uczestników tego procesu, ich

obowiązki i odpowiedzialność, typy certyfikatów, procedury weryfikacji tożsamości używane przy ich wydawaniu oraz obszary zastosowań, opublikowany w Internecie pod adresem http://www.certum.pl.

12. **Baseline Requirements for the Issuance and Management of Publicly Trusted Code Signing Certificates** – dokument stworzony przez konsorcjum opiniotwórcze CA/Browser Forum zrzeszające szereg urzędów certyfikacji oraz twórców przeglądarek internetowych, wyznaczający standardy opisujące zawartość certyfikatów Code Signing (w tym EV) oraz wymagania jakie spełniać muszą urzędy certyfikacji, aby wydawać certyfikaty Code Signing. Dokument dostępny jest na stronie http://www.cabforum.org.
13. **Subskrybent** – podmiot certyfikatu, osoba fizyczna, przedsiębiorstwo, podmiot administracji państwowej lub organizacja, której dane znajdują się w certyfikacie oraz jest właścicielem bądź wyłącznym użytkownikiem certyfikatu.
14. **Przedstawiciel Subskrybenta** – osoba fizyczna reprezentująca Subskrybenta, której dane przypisane są do konta internetowego w serwisie www.certum.pl lub konta programu partnerskiego. Przedstawicielem Subskrybenta może być pracownik zatrudniony przez Subskrybenta lub Zamawiającego a także autoryzowany przedstawiciel Subskrybenta lub Zamawiającego posiadający wyraźne pełnomocnictwo do działania w imieniu Subskrybenta. Przedstawiciel Subskrybenta jest osobą akceptującą niniejsze Warunki Użytkowania.
15. **Wniosek Certyfikacyjny** – elektroniczny wniosek dotyczący wydania lub odnowienia certyfikatu zawierający m.in. dane Subskrybenta oraz dane będące treścią certyfikatu.
16. **Zamawiający** – osoba fizyczna, prawna, jednostka organizacyjna nieposiadająca osobowości prawnej lub organ władzy publicznej, która w imieniu Subskrybenta składa Wniosek Certyfikacyjny.

§2 Zastosowanie

Niniejsze Warunki Użytkowania zakresem obejmują wszystkie certyfikaty niekwalifikowane wydawane przez Certum swoim subskrybentom oraz świadczenie usług certyfikacyjnych związanych z obsługą tych certyfikatów.

§3 Ograniczenia w użytkowaniu usługi

Certum nie wydaje certyfikatów osobom, które nie ukończyły 18 lat.

§4 Wydawanie i zarządzanie certyfikatami

4.1 Wniosek o wydanie certyfikatu

Zamawiający lub Przedstawiciel Subskrybenta mogą składać Wnioski Certyfikacyjne w formie elektronicznej za pośrednictwem indywidualnego konta w serwisie internetowym Certum na stronie www.certum.pl oraz za pośrednictwem dedykowanych kont usługowych udostępnianych w ramach programów partnerskich prowadzonych przez Certum. Zamawiający lub Przedstawiciel Subskrybenta mogą składać Wnioski Certyfikacyjne dotyczące wyłącznie certyfikatów, których nazwa wyróżniona (ang. Distinguished Name) a zwłaszcza zawartość pól CommonName oraz SubjectAlternativeName są własnością Subskrybenta lub jeśli Subskrybent upoważnił osobę/podmiot ubiegający się o certyfikat do posługiwania się nazwą wyróżnioną zawartą w certyfikacie. Wszystkie dane zawarte we Wniosku Certyfikacyjnym zostają włączone do niniejszego dokumentu jako część Warunków Użytkowania.

4.2 Weryfikacja

Certum weryfikuje otrzymane Wnioski Certyfikacyjne zgodnie z *Kodeksem Postępowania Certyfikacyjnego* oraz obowiązującymi wytycznymi (takimi jak *Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates, Guidelines for the Issuance and Management of Extended Validation Certificates, Baseline Requirements for the Issuance and Management of Publicly-Trusted Code Signing Certificates* oraz *Baseline Requirements for the Issuance and Management of Publicly- Trusted S/MIME Certificates).*

4.3 Akceptacja certyfikatu.

Zamawiający zobowiązany jest upoważnić osobę fizyczną, której dane zawarte są w koncie internetowym lub partnerskim do ubiegania się o certyfikat niekwalifikowany w imieniu Subskrybenta łącznie z prawem do jego akceptacji.

4.4 Wydanie certyfikatu

W przypadku pomyślnej weryfikacji Wniosku Certyfikacyjnego, Certum wydaje certyfikat niekwalifikowany o czym niezwłocznie informuje Subskrybenta certyfikatu.

4.5 Unieważnienie certyfikatu

Subskrybent posiada możliwość unieważnienia certyfikatu w każdym momencie okresu jego ważności samodzielnie lub za pośrednictwem Certum.

Certum unieważni certyfikat subskrybenta typu SSL lub Code Signing w ciągu 24 godzin w następujących okolicznościach:

- na każde pisemne żądanie subskrybenta wskazanego w certyfikacie,
- na podstawie powiadomienia pochodzącego od subskrybenta, o tym, że wniosek certyfikacyjny nie był przez niego autoryzowany i nie udziela autoryzacji z mocą wsteczną,
- gdy Certum uzyskuje dowód, że klucz prywatny subskrybenta został ujawniony[1],
- gdy Certum uzyskuje dowód na to, że weryfikacja wniosku została przeprowadzona na podstawie niepoprawnych informacji,
- gdy Subskrybent rezygnuje z podpisania dokumentów, które miał podpisać z wykorzystaniem usługi wydawania certyfikatów w procesie podpisywania;
- gdy Certum jest świadome, że istnieje zademonstrowana i sprawdzona metoda, która może łatwo obliczyć klucz prywatny subskrybenta na podstawie klucza publicznego zawartego w certyfikacie.

Certum unieważni certyfikat subskrybenta typu SSL lub Code Signing w ciągu 5 dni w następujących okolicznościach:

- gdy technologie zabezpieczeń kryptograficznych zdezaktualizują się, co może uczynić certyfikat subskrybenta podatnym na zagrożenia (np. zawartość lub format

[1] Ujawnienie klucza prywatnego oznacza: (1) nieuprawniony dostęp lub podejrzenie nieuprawnionego dostępu do klucza prywatnego, (2) zagubienie lub podejrzenie zagubienia klucza prywatnego, (3) kradzież lub podejrzenie kradzieży klucza prywatnego, (4) przypadkowe zniszczenie klucza prywatnego.

certyfikatu przedstawia ryzyko nieakceptowane przez strony ufające lub dostawców oprogramowania)

- gdy Certum otrzyma dowód na nieuprawnione lub niedozwolone użycie certyfikatu,
- wskutek nieprzestrzegania przez subskrybenta zaakceptowanej Polityki Certyfikacji oraz Kodeksu Postępowania Certyfikacyjnego lub postanowień innych dokumentów przywołanych w niniejszym dokumencie[2], których wymagań subskrybent certyfikatu zobowiązuje się przestrzegać,
- gdy Certum uzyskuje dowód, że użycie nazwy domeny lub adresu IP nie jest już dozwolone ze względów prawnych,
- gdy Certum uzyskuje dowód, że certyfikat typu Wildcard został użyty do wprowadzającego w błąd uwierzytelnienia podrzędnej domeny głównej,
- gdy jakakolwiek informacja zawarta w certyfikacie zdezaktualizuje się,
- gdy Certum jest świadome, że certyfikat nie został wydany zgodnie z postanowieniami Polityki Certyfikacji, Kodeksu Postępowania Certyfikacyjnego oraz postanowień innych dokumentów przywołanych w niniejszym dokumencie, których Certum przestrzega.
- gdy Certum ustali lub uzyska informacje, że jakakolwiek informacja zawarta w certyfikacie jest niepoprawna,
- w przypadku ustania prawa do wystawiania certyfikatów zgodnie z wymaganiami, lub zakończeniu działalności przez Certum, chyba, że Certum będzie utrzymywało repozytorium CRL/OCSP,
- gdy unieważnienie jest wymagane przez Politykę Certyfikacji lub Kodeks Postępowania Certyfikacyjnego,
- gdy Certum jest świadome dowiedzionej lub sprawdzonej metody, która naraża klucz prywatny na kompromitację, metody, według której klucz prywatny jest podatny na łatwe obliczenie na podstawie klucza publicznego lub gdy istnieją wyraźne dowody na to, że konkretna metoda używana do generowania klucza prywatnego była wadliwa,
- subskrybent nie wywiązuje się z zobowiązań płatniczych za usługi świadczone przez urząd certyfikacji lub innych zobowiązań, które podjął na rzecz Certum,
- subskrybent, będący pracownikiem organizacji po rozwiązaniu z nim umowy o pracę nie oddał kryptograficznej karty elektronicznej, na której przechowywany był certyfikat i komplementarny z nim klucz prywatny,
- inne przyczyny opóźniające lub uniemożliwiające subskrybentowi wypełnianie postanowień niniejszego Kodeksu Postępowania Certyfikacyjnego, powstałych wskutek klęsk żywiołowych, awarii systemu komputerowego lub sieci, zmian otoczenia prawnego, w którym działa subskrybent lub oficjalnych działań rządu lub jego agend.

Powyższe okoliczności mogą decydować także o unieważnieniu certyfikatu EV SSL.

[2] Przede wszystkim wymagania:

- Baseline Requirements for the Issuance and Management of Publicly Trusted TLS Server Certificates,
- Baseline Requirements for the Issuance and Management of Publicly Trusted Code Signing Certificates,
- Guidelines For The Issuance And Management Of Extended Validation Certificates,
- Baseline Requirements for the Issuance and Management of Publicly- Trusted S/MIME Certificates,

Certum unieważni certyfikat subskrybenta typu S/MIME tak szybko jak to możliwe w następujących okolicznościach:

- na podstawie powiadomienia pochodzącego od subskrybenta, o tym, że wniosek certyfikacyjny nie był przez niego autoryzowany i nie udziela autoryzacji z mocą wsteczną,
- gdy Certum uzyskuje dowód, że klucz prywatny subskrybenta został ujawniony,
- gdy Certum uzyska dowód, że certyfikat był używany do celów innych niż wskazany w certyfikacie lub w warunkach użytkowania,
- gdy Certum otrzyma powiadomienie lub w inny sposób uzyska informację, że subskrybent naruszył co najmniej jedno ze swoich istotnych zobowiązań wynikających z warunków użytkowania,
- gdy Certum otrzyma powiadomienie lub w inny sposób uzyska informacje o wszelkich okolicznościach wskazujących, że użycie adresu e-mail w certyfikacie nie jest już prawnie dozwolone,
- gdy Certum ustali lub otrzyma informację o istotnej zmianie informacji zawartych w certyfikacie,
- gdy Certum jest świadome, że certyfikat nie został wydany zgodnie z postanowieniami Polityki Certyfikacji, Kodeksu Postępowania Certyfikacyjnego oraz postanowień innych dokumentów przywołanych w niniejszym dokumencie, których Certum przestrzega.
- gdy Certum ustali, że jakakolwiek informacja zawarta w certyfikacie jest niedokładna,
- gdy Certum zaprzestanie działalności i nie przekaże innemu urzędowi certyfikacji wsparcia w zakresie unieważniania certyfikatu,
- gdy istnieje podejrzenie, że klucz prywatny CA użyty do wydania certyfikatu został naruszony;
- gdy Certum ustali, że certyfikat został wydany z naruszeniem obowiązujących wymagań,
- subskrybent nie wywiązuje się z zobowiązań płatniczych za usługi świadczone przez urząd certyfikacji lub innych zobowiązań, które podjął na rzecz Certum,
- subskrybent, będący pracownikiem organizacji po rozwiązaniu z nim umowy o pracę nie oddał kryptograficznej karty elektronicznej, na której przechowywany był certyfikat i komplementarny z nim klucz prywatny,
- inne przyczyny opóźniające lub uniemożliwiające subskrybentowi wypełnianie postanowień niniejszego Kodeksu Postępowania Certyfikacyjnego, powstałych wskutek klęsk żywiołowych, awarii systemu komputerowego lub sieci, zmian otoczenia prawnego, w którym działa subskrybent lub oficjalnych działań rządu lub jego agend.

4.6 Zawieszenie certyfikatu

Certum nie świadczy usługi zawieszenia certyfikatu.

§5 Zobowiązania

5.1 Zobowiązania ADS

W ramach niniejszych Warunków Użytkowania ADS zobowiązuje się do:

- wydania certyfikatów zgodnie z danymi określonymi we Wniosku Certyfikacyjnym oraz wymaganiami określonymi w *Baseline Requirements for the Issuance and Management of Publicly Trusted TLS Server Certificates, Baseline Requirements for the Issuance and Management of Publicly Trusted Code Signing Certificates, Guidelines For The Issuance And Management Of Extended Validation Certificates, Baseline Requirements for the Issuance and Management of Publicly Trusted S/MIME Certificates,* dostępnymi na stronie http://www.cabforum.org, w terminie nie przekraczającym 7 dni od daty złożenia wniosku o wydanie certyfikatu, lecz nie wcześniej niż po przekazaniu przez Subskrybenta do Certum kompletu wymaganych dokumentów i opłaceniu faktury VAT.
- weryfikacji prawdziwości i ścisłości udzielanych Certum informacji dotyczących danych podmiotu certyfikatu przez cały okres ważności certyfikatu.
- świadczenia na rzecz Subskrybenta usług certyfikacyjnych zgodnie z warunkami określonymi w *Polityce Certyfikacji, Kodeksie Postępowania Certyfikacyjnego, Baseline Requirements for the Issuance and Management of Publicly Trusted TLS Server Certificates, Baseline Requirements for the Issuance and Management of Publicly Trusted Code Signing Certificates, Guidelines For The Issuance And Management Of Extended Validation Certificates, Baseline Requirements for the Issuance and Management of Publicly Trusted S/MIME Certificates*, a w szczególności do:
  - unieważnienia certyfikatów w przypadku zaistnienia okoliczności uzasadniających ich unieważnienie, określonych w Kodeksie Postępowania Certyfikacyjnego,
  - opublikowania unieważnionego certyfikatu na liście certyfikatów odwołanych (CRL) w okresie nie dłuższym niż 7 dni,
  - zagwarantowania 24-godzinnej obsługi w zakresie unieważniania certyfikatów na każde złożone przez Subskrybenta żądanie.
  - opublikowania wydanych certyfikatów w repozytorium Certum.
  - powiadamiania drogą elektroniczną o konieczności odnowienia certyfikatu, co najmniej 7 dni przed upływem jego ważności.

5.2 Zobowiązania subskrybenta

W ramach niniejszych Warunków Użytkowania subskrybent zobowiązuje się do:

- dostarczania do Certum prawdziwych i ścisłych informacji dotyczących danych podmiotu certyfikatu przez cały okres ważności certyfikatu,

- ochrony klucza prywatnego - kontrolowania używania klucza prywatnego, powiązanego z kluczem publicznym umieszczonym w certyfikacie oraz do ochrony wszelkich informacji z nim związanych,
- instalacji certyfikatu tylko na serwerze obsługującym nazwę domeny wymienioną w certyfikacie,
- stosowania certyfikatu zgodnie z prawem, używania certyfikatu wyłącznie przez uprawniony do tego podmiot,
- niezwłocznego zaprzestania używania certyfikatu i związanego z nim klucza prywatnego oraz niezwłocznego zgłoszenia do Certum woli unieważnienia certyfikatu w następujących przypadkach:
    - nieprawidłowej lub nieprawdziwej informacji zawartej w certyfikacie;
    - podejrzeń nadużycia lub niewłaściwego wykorzystania certyfikatu;
    - kompromitacji klucza prywatnego.
- niezwłocznego zaprzestania używania klucza prywatnego powiązanego z kluczem publicznym umieszczonym w certyfikacie w chwili wygaśnięcia ważności certyfikatu lub jego unieważnienia.
- reagowania na instrukcje urzędu certyfikacji dotyczące naruszenia klucza lub niewłaściwego użycia certyfikatu w terminie nie dłuższym niż 24 godziny od momentu otrzymania powiadomienia.

§6 Oświadczenie subskrybenta

Subskrybent, akceptując wysłanie wniosku o wydanie certyfikatu niekwalifikowanego oświadcza, że:
zapoznał się z niniejszymi *Warunkami Użytkowania* i akceptuje treść *Polityki Certyfikacji Niekwalifikowanych Usług Certum* oraz *Kodeksu Postępowania Certyfikacyjnego Niekwalifikowanych Usług Certum*. Wszystkie podane przez niego informacje, które otrzymało Certum w związku z Wnioskiem Certyfikacyjnym, są zgodne z prawdą i zostały podane dobrowolnie oraz że administratorem tych danych będzie Asseco Data Systems S.A. z siedzibą w Gdańsku, ul. Jana z Kolna 11. Ponosi odpowiedzialność za szkody wynikające z podania nieprawdziwych lub fałszywych danych oraz za skutki nieprawidłowego użycia certyfikatu. Certyfikat może być publikowany w repozytorium Certum.

§7 Gwarancje ADS

ADS gwarantuje:
świadczenie usług będących przedmiotem niniejszej umowy z zachowaniem zasad należytej staranności zgodnie z postanowieniami niniejszej umowy, *Kodeksu Postępowania Certyfikacyjnego*, wytycznych *Baseline Requirements for the Issuance and Management of Publicly Trusted TLS Server Certificates, Baseline Requirements for the Issuance and Management of Publicly Trusted Code Signing Certificates, Guidelines For The Issuance And Management Of Extended Validation Certificates, Baseline Requirements for the Issuance and Management of Publicly Trusted S/MIME Certificates*. Okres gwarancji na świadczone przez ADS usługi certyfikacyjne jest tożsamy z okresem ważności certyfikatu. W przypadku zakończenia

działalności lub przekazania zadań przez Certum w trybie określonym przez *Kodeks Postępowania Certyfikacyjnego*, Subskrybent otrzyma zwrot kosztów wydanego certyfikatu proporcjonalnie do pozostałego okresu jego ważności. Wartość transakcji objętych gwarancją Certum jest ograniczona do kwot określonych w *Kodeksie Postępowania Certyfikacyjnego*.

§8 Zastrzeżenia

ADS zastrzega, że:

nie ponosi odpowiedzialności za szkody wyrządzone osobom trzecim przy użyciu niniejszego certyfikatu, za wyjątkiem szkód powstałych z winy umyślnej ADS, niniejszych certyfikatów wolno używać tylko zgodnie z zasadami określonymi prawem, wyłącznie przez uprawniony do tego podmiot oraz zgodnie z niniejszymi Warunkami Użytkowania, ADS nie ponosi odpowiedzialności za skutki działań Subskrybenta i osób trzecich, a w szczególności: wadliwą instalację i użytkowanie certyfikatu oraz straty wynikłe z jakości sprzętu stosowanego przez Subskrybenta i osoby trzecie, straty wynikłe z niewłaściwego stosowania i braku odpowiedniego zabezpieczania przez Subskrybenta i osoby trzecie kluczy lub wydanego certyfikatu. ADS nie ponosi odpowiedzialności również za straty poniesione na skutek działania siły wyższej.

§9 Informacje kontaktowe

Asseco Data Systems S.A.
ul. Jana z Kolna 11
80-864 Gdańsk
Strona internetowa: www.assecods.pl
e-mail: kontakt@assecods.pl

Certum
ul. Bajeczna 13
71-838 Szczecin
Strona internetowa: www.certum.pl
e-mail: infolinia@certum.pl

Historia zmian dokumentu		
23.05.2018	1.0	Opublikowanie dokumentu w repozytorium Certum
29.09.2021	1.1	Zmiana adresu spółki, zmiana czasu na wydanie certyfikatu, uaktualnienie nazewnictwa dokumentów CA/B Forum
27.09.2022	1.2	Drobne korekty edytorskie
18.12.2024	1.3	Drobne korekty edytorskie, naniesie poprawek po uwagach audytowych zgodności z Webtrust, uaktualnienie nazewnictwa dokumentów CA/B Forum