Polityka Certyfikacji i Kodeks Postępowania Certyfikacyjnego dla Certyfikatów TLS

Certum

Asseco Data Systems S.A.
ul. Jana z Kolna 11
80-864 Gdańsk
Poland

Wersja: 1.1.0

Data publikacji: 2026-10-05

Spis treści

Polityka Certyfikacji i Kodeks Postępowania Certyfikacyjnego dla Certyfikatów TLS 1
1. WPROWADZENIE 5
1.1 Przegląd 5
1.2 Nazwa i identyfikacja dokumentu 6
1.3 Uczestnicy PKI 6
1.4 Użycie certyfikatu 11
1.5 Zarządzanie polityką 12
1.6 Definicje i akronimy 13
2. PUBLIKACJA I OBOWIĄZKI ZWIĄZANE Z REPOZYTORIUM 14
2.1 Repozytoria 14
2.2 Publikacja informacji certyfikacyjnych 14
2.3 Czas lub częstotliwość publikacji 14
2.4 Kontrole dostępu do repozytoriów 15
3. IDENTYFIKACJA I UWIERZYTELNIENIE 16
3.1 Nazewnictwo 16
3.2 Początkowa walidacja tożsamości 17
3.3 Identyfikacja i uwierzytelnienie dla wniosków o re-key 20
3.4 Identyfikacja i uwierzytelnienie dla wniosku o unieważnienie 21
4. WYMAGANIA OPERACYJNE DOTYCZĄCE CYKLU ŻYCIA CERTYFIKATU 22
4.1 Wniosek o certyfikat 22
4.2 Przetwarzanie wniosku o certyfikat 22
4.3 Wydanie certyfikatu 25
4.4 Akceptacja certyfikatu 25
4.5 Użycie pary kluczy i certyfikatu 26
4.6 Odnowienie certyfikatu 27
4.7 Re-key certyfikatu 28
4.8 Modyfikacja certyfikatu 28
4.9 Unieważnienie i zawieszenie certyfikatu 29
4.10 Usługi statusu certyfikatu 33
4.11 Koniec subskrypcji 33
4.12 Escrow i odzyskiwanie kluczy 34

5. KONTROLE FIZYCZNE, ZARZĄDCZE I OPERACYJNE 35
5.1 Kontrole fizyczne 35
5.2 Kontrole proceduralne 37
5.3 Kontrole personelu 38
5.4 Procedury rejestrowania zdarzeń 41
5.5 Archiwizacja danych 42
5.6 Zmiana klucza 43
5.7 Kompromitacja i odtwarzanie po awarii 43
5.8 Zakończenie działania CA lub RA 46
6. TECHNICZNE KONTROLE BEZPIECZEŃSTWA 47
6.1 Generowanie i instalacja pary kluczy 47
6.2 Ochrona klucza prywatnego i kontrole inżynieryjne modułów kryptograficznych 48
6.3 Inne aspekty zarządzania parami kluczy 50
6.4 Dane aktywacyjne 51
6.5 Kontrole bezpieczeństwa komputerowego 51
6.6 Kontrole techniczne cyklu życia 51
6.7 Kontrole bezpieczeństwa sieciowego 53
6.8 Znakowanie czasem 53
7. PROFILE CERTYFIKATÓW, CRL I OCSP 54
7.1 Profil certyfikatu 54
7.2 Profil CRL 58
7.3 Profil OCSP 60
8. AUDYT ZGODNOŚCI I INNE OCENY 61
8.1 Częstotliwość lub okoliczności oceny 61
8.2 Tożsamość/kwalifikacje oceniającego 61
8.3 Relacja oceniającego z ocenianym podmiotem 61
8.4 Zakres tematyczny objęty oceną 61
8.5 Działania podejmowane w wyniku niezgodności 62
8.6 Komunikacja wyników 62
8.7 Samoaudyty 62
9. INNE SPRAWY BIZNESOWE I PRAWNE 63
9.1 Opłaty 63
9.2 Odpowiedzialność finansowa 63

9.3 Poufność informacji biznesowych 64
9.4 Prywatność informacji osobowych 65
9.5 Prawa własności intelektualnej 66
9.6 Oświadczenia i gwarancje 67
9.7 Wyłączenia gwarancji 69
9.8 Ograniczenia odpowiedzialności 70
9.9 Zwolnienie z odpowiedzialności 70
9.10 Okres obowiązywania i zakończenie 70
9.10.3 Skutek zakończenia i dalsze obowiązywanie 71
9.11 Indywidualne zawiadomienia i komunikacja z uczestnikami 71
9.12 Zmiany 71
9.13 Postanowienia dotyczące rozstrzygania sporów 72
9.14 Prawo właściwe 72
9.15 Zgodność z mającym zastosowanie prawem 72
9.16 Postanowienia różne 72
9.17 Inne postanowienia 73
ANEKS A - Historia zmian 74
ANEKS B - Definicje, akronimy i referencje 75
Definicje 75
Skróty 78
Referencje 79

1. WPROWADZENIE

Asseco Data Systems S.A. działająca pod marką Certum, będąca następcą prawnym Unizeto Technologies S.A., jest urzędem certyfikacji (Certification Authority, CA) świadczącym usługi dla wszystkich podstawowych operacji infrastruktury klucza publicznego (Public Key Infrastructure, PKI), w tym przyjmowania żądań certyfikacyjnych, wydawania certyfikatów, unieważniania certyfikatów, publikowania list unieważnionych certyfikatów (Certificate Revocation Lists, CRLs) oraz zapewniania weryfikacji statusu w czasie rzeczywistym za pośrednictwem usług OCSP.

1.1 Przegląd

Niniejszy łączny dokument Polityki certyfikacji (Certificate Policy, CP) i Kodeksu Postępowania Certyfikacyjnego (Certification Practice Statement, CPS) (CP/CPS) określa polityki, zasady i praktyki związane z publicznie zaufanymi usługami certyfikacyjnymi TLS świadczonymi przez Certum.

Infrastruktura klucza publicznego Certum (Certum Public Key Infrastructure, Certum PKI) wydaje publicznie zaufane certyfikaty TLS na następujących poziomach zapewnienia: Domain Validated (DV), Organization Validated (OV) oraz Extended Validation (EV), zgodnie z mającymi zastosowanie wymaganiami CA/B Forum.

Certum jest zgodne z najnowszą opublikowaną wersją wymagań CA/B Forum Baseline Requirements:

- CA/B Forum Baseline Requirements for the Issuance and Management of Publicly-Trusted TLS Server Certificates (TLS BR) - https://cabforum.org/working-groups/server/baseline-requirements/documents/
- CA/B Forum Guidelines for the Issuance and Management of Extended Validation Certificates (EV Guidelines) - https://cabforum.org/extended-validation
- CA/B Forum Network and Certificate System Security Requirements - https://cabforum.org/network-security-requirements

Certum jest zgodne z najnowszą opublikowaną wersją polityk repozytoriów zaufanych głównych dostawców oprogramowania aplikacyjnego, w tym:

- Apple Root Store Program - https://github.com/apple/apple-root-program/blob/main/policy.md
- CCADB Policy - https://www.ccadb.org/policy
- Chrome Root Program Policy - https://googlechrome.github.io/chromerootprogram/crp/policy/
- Microsoft Root Program Requirements - https://github.com/TrustedRootProgram/Program-Requirements/blob/main/Requirements.md

- Mozilla Root Store Policy - https://www.mozilla.org/en-US/about/governance/policies/security-group/certs/policy/

W przypadku jakiejkolwiek niespójności pomiędzy niniejszym dokumentem a normatywnymi postanowieniami mających zastosowanie wytycznych lub norm branżowych (applicable requirements), pierwszeństwo mają applicable requirements.

W przypadku jakiejkolwiek niespójności pomiędzy niniejszym dokumentem (mającym zastosowanie do certyfikatów TLS) a *Polityką Certyfikacji Niekwalifikowanych Usług Certum* lub *Kodeksem Postępowania Certyfikacyjnego Niekwalifikowanych Usług Certum*, które regulują wszystkie certyfikaty wydawane przez Certum (i które są stopniowo zastępowane przez dedykowane dokumenty CP/CPS o określonym zakresie), pierwszeństwo ma niniejszy dokument.

1.2 Nazwa i identyfikacja dokumentu

Niniejszy dokument nosi tytuł *Polityka Certyfikacji i Kodeks Postępowania Certyfikacyjnego dla certyfikatów TLS* (zwany dalej CP/CPS). Jest to dokument publiczny opisujący praktyki i polityki Certum dotyczące publicznie zaufanych usług certyfikacyjnych TLS.

Niniejszy dokument jest zorganizowany zgodnie ze standardem Internet Engineering Task Force (IETF) RFC 3647.

OID dla Certum to 1.2.616.1.113527.2.

```
{iso(1) member-body(2) pl(616) organization(1) unizeto(113527) 2(2)}
```

Zob. Sekcja 7.1 w zakresie identyfikatorów obiektów Certificate Policy.

Zob. Aneks A w zakresie wykazu zmian niniejszego dokumentu.

1.3 Uczestnicy PKI

1.3.1 Urzędy certyfikacji

Certum jest jedynym operatorem wszystkich głównych urzędów certyfikacji (Root Certification Authorities, Root CAs) i podrzędnych urzędów certyfikacji (Subordinate Certification Authorities, Subordinate CAs) przeznaczonych dla publicznie zaufanych usług certyfikacyjnych TLS Certum.

- Root CAs są wykorzystywane do wydawania Subordinate CAs
- Subordinate CAs są wykorzystywane do wydawania certyfikatów końcowych (end-entity certificates)

Wszystkie urzędy certyfikacji działają w ramach swojej PKI, w tym w zakresie wydawania certyfikatów, unieważniania oraz utrzymywania CRL i usług OCSP.

1.3.1.1 Główny urząd certyfikacji Certum (Certum Root CA)

Certum Trusted Network CA (G1)

- Klucz: RSA 2048
- Numer seryjny: 279744 (0x444c0)
- Odcisk SHA-256: 5C:58:46:8D:55:F5:8E:49:7E:74:39:82:D2:B5:00:10:B6:D1:65:37:4A:CF:83:A7:D4:A3:2D:B7:68:C4:40:8E
- Ważny do: 2029-12-31

Certum Trusted Network CA 2 (G1)

- Klucz: RSA 4096
- Numer seryjny: 21:d6:d0:4a:4f:25:0f:c9:32:37:fc:aa:5e:12:8d:e9
- Odcisk SHA-256: B6:76:F2:ED:DA:E8:77:5C:D3:6C:B0:F6:3C:D1:D4:60:39:61:F4:9E:62:65:BA:01:3A:2F:03:07:B6:D0:B8:04
- Ważny do: 2046-10-06

Certum Trusted Root CA (G2)

- Klucz: RSA 4096
- Numer seryjny: 1e:bf:59:50:b8:c9:80:37:4c:06:f7:eb:55:4f:b5:ed
- Odcisk SHA-256: FE:76:96:57:38:55:77:3E:37:A9:5E:7A:D4:D9:CC:96:C3:01:57:C1:5D:31:76:5B:A9:B1:57:04:E1:AE:78:FD
- Ważny do: 2043-03-16

Certum EC-384 CA (G2)

- Klucz: ECC 384
- Numer seryjny: 78:8f:27:5c:81:12:52:20:a5:04:d0:2d:dd:ba:73:f4
- Odcisk SHA-256: 6B:32:80:85:62:53:18:AA:50:D1:73:C9:8D:8B:DA:09:D5:7E:27:41:3D:11:4C:F7:87:A0:F5:D0:6C:03:0C:F6
- Ważny do: 2043-03-26

Certum TLS RSA Root CA (G3)

- Klucz: RSA 4096
- Numer seryjny: e7:dd:21:38:a2:c9:41:46:ff:5f:12:17:89:95:05:53
- Odcisk SHA-256: ED:12:A6:E9:28:92:39:D6:6C:A1:D2:44:CE:90:C6:23:AC:30:5A:D0:56:02:DA:35:2B:CF:C5:FE:F2:C4:45:8D
- Ważny do: 2048-01-26

Certum TLS ECC Root CA (G3)

- Klucz: ECC 384
- Numer seryjny: b0:7e:c0:cb:2e:05:e6:3c:71:da:0d:7f:99:79:71:f3
- Odcisk SHA-256: 63:0C:CB:83:B0:18:0A:99:24:95:E0:39:D2:61:3C:32:87:A8:10:2F:8A:8D:70:3D:B1:33:0A:3E:86:D4:E6:53
- Ważny do: 2048-01-26

1.3.1.2 Certum cross-signed CA

W celu zapewnienia kompatybilności wstecznej ze starszymi wersjami magazynów głównych certyfikatów (root stores) głównych dostawców oprogramowania, Certum wydał certyfikaty krzyżowe pomiędzy własnymi głównymi urzędami certyfikacji (Root CA):

G1 → G1

Certum Trusted Network CA (G1) → Certum Trusted Network CA 2 (G1)

- Klucz: RSA 4096
- Numer seryjny: 1b:b5:8f:25:2a:df:23:00:49:28:c9:ae:3d:7e:ed:27
- Odcisk SHA-256: 08:E7:EA:C9:98:A6:2C:41:55:CC:4C:BC:5E:DA:32:F5:B4:1A:12:C0:12:F2:9A:B3:43:3B:D3:66:34:81:49:F0
- Ważny do: 2029-09-17

G1 → G2

Certum Trusted Network CA (G1) → Certum Trusted Root CA (G2)

- Klucz: RSA 4096
- Numer seryjny: d8:e0:74:4b:58:24:91:9f:bd:08:84:7d:f7:20:20:fa
- Odcisk SHA-256: FB:13:89:0C:7A:B1:4F:F7:B9:4B:27:14:50:3E:31:12:3B:FD:D3:40:FC:4D:97:97:43:16:6E:04:69:B4:7A:88
- Ważny do: 2028-09-19

Certum Trusted Network CA (G1) → Certum EC-384 CA (G2)

- Klucz: ECC 384
- Numer seryjny: da:fd:4b:f5:41:21:e0:27:d6:86:96:22:5f:1f:ce:e8
- Odcisk SHA-256: B7:24:50:AB:F5:04:7A:8A:F6:3E:C9:D8:7E:33:14:84:85:0B:18:49:A2:55:0A:82:A8:6D:B6:B4:1E:D3:87:60
- Ważny do: 2028-09-19

G1 → G3

Certum Trusted Network CA (G1) → Certum TLS RSA Root CA (G3)

- Klucz: RSA 4096
- Numer seryjny: f3:a6:f6:60:2e:d9:3e:8a:c2:71:63:18:8e:c0:5b:8f
- Odcisk SHA-256: 58:06:D9:DE:DA:84:AE:85:8E:6F:3D:13:71:E2:BD:65:D0:97:8F:D2:4A:1A:97:8C:A3:51:0F:47:21:73:55:D9
- Ważny do: 2029-12-30

Certum Trusted Network CA (G1) → Certum TLS ECC Root CA (G3)

- Klucz: ECC 384
- Numer seryjny: aa:34:75:7c:53:26:f6:50:14:94:ef:95:03:a5:3a:f6
- Odcisk SHA-256: BC:6C:77:55:69:75:94:59:2C:22:CE:1F:8C:70:85:D3:C4:9B:F4:1B:12:6A:66:71:FE:5E:F1:0F:9D:E8:EF:D6
- Ważny do: 2029-12-30

G2 → G3

Certum Trusted Root CA (G2) → Certum TLS RSA Root CA (G3)

- Klucz: RSA 4096
- Numer seryjny: dd:29:cf:13:fe:68:a3:21:6e:47:dc:61:a3:4a:62:b1
- Odcisk SHA-256: 98:D8:8F:84:15:95:87:EF:C8:30:BA:17:AC:8E:0C:80:7B:7A:59:D5:60:DE:49:C8:59:29:12:25:1C:3E:C1:27
- Ważny do: 2036-04-15

Certum EC-384 CA (G2) → Certum TLS ECC Root CA (G3)

- Klucz: ECC 384
- Numer seryjny: 68:61:04:73:ed:c5:5e:86:16:a9:e3:95:ef:d9:ba:5c
- Odcisk SHA-256: 83:C1:8A:F3:F7:BC:E7:DC:7C:5A:3A:51:D0:01:A5:AB:74:C3:59:F7:47:6D:5B:EE:D8:A3:07:30:FC:9A:6C:26
- Ważny do: 2036-04-15

1.3.1.3 Podrzędne urzędy certyfikacji Certum (Certum Subordinate CA)

Podrzędne urzędy certyfikacji Certum w hierarchiach G2 i G3 są wydawane w następującej strukturze, w celu rozdzielenia różnych poziomów zapewnienia dla certyfikatów TLS:

- Subordinate CA dla DV TLS
- Subordinate CA dla OV TLS
- Subordinate CA dla EV TLS

1.3.2 Urzędy rejestracji

Urzędy rejestracji (Registration Authorities, RAs) są podmiotami, które wykonują identyfikację i uwierzytelnienie Wnioskodawców certyfikatów, weryfikują ich upoważnienie do żądania certyfikatów oraz wspierają zatwierdzanie wydania i unieważnienia certyfikatów.

Certum działa jako jedyny urząd rejestracji (Registration Authority, RA) i wykonuje wszystkie czynności identyfikacji i uwierzytelnienia bezpośrednio, w tym walidację nazw domen i adresów IP. Certum nie deleguje tych funkcji walidacyjnych stronom trzecim.

Certum może wykorzystywać zaufane procesy weryfikacyjne realizowane przez podmioty trzecie w celu wsparcia walidacji tożsamości Wnioskodawcy tam, gdzie jest to wymagane. Takie procesy nie stanowią odrębnych RA. Certum analizuje wszystkie zebrane informacje i podejmuje ostateczną decyzję dotyczącą walidacji i wydania certyfikatu.

1.3.3 Subskrybenci

Subskrybentem jest osoba fizyczna lub osoba prawna, której wydano certyfikat i która posiada lub kontroluje klucz prywatny (private key).

Subskrybenci są zobowiązani działać zgodnie z mającą zastosowanie umową Subskrybenta (Subscriber Agreement) lub Warunkami użytkowania (Terms of Use), w tym do:

- Podawania dokładnych i prawdziwych informacji
- Niezwłocznego powiadamiania Certum o każdej zmianie informacji zawartych w certyfikacie
- Zapewnienia ochrony klucza prywatnego
- Używania certyfikatu zgodnie z niniejszym CP/CPS
- Niezwłocznego powiadamiania Certum o każdym podejrzeniu kompromitacji klucza (key compromise)
- Natychmiastowego zaprzestania używania certyfikatu po jego wygaśnięciu lub unieważnieniu

1.3.4 Strony ufające

Stroną ufającą (relying party) jest każda osoba fizyczna lub osoba prawna, która polega na certyfikacie TLS wydanym przez Certum w celu zweryfikowania tożsamości serwera lub ustanowienia bezpiecznego, szyfrowanego kanału komunikacji.

Przed oparciem się na jakimkolwiek certyfikacie strona ufająca powinna:

- Zweryfikować status certyfikatu i wszystkich certyfikatów w jego łańcuchu przy użyciu odpowiednich usług CRL lub OCSP udostępnianych przez Certum
- Przeczytać i zrozumieć warunki niniejszego CP/CPS

1.3.5 Inni uczestnicy

Innymi uczestnikami są podmioty świadczące usługi wspierające PKI Certum, które nie działają jako urzędy certyfikacji, urzędy rejestracji, Subskrybenci ani strony ufające.

Tacy uczestnicy mogą obejmować między innymi:

- Dostawców usług statusu certyfikatów (np. responderów OCSP i usług dystrybucji CRL)
- Dostawców repozytoriów i usług publikacyjnych
- Dostawców infrastruktury i usług wspierających operacje PKI
- partnerów biznesowych, w tym autoryzowanych resellerów

Wszyscy inni uczestnicy są zobowiązani działać zgodnie z mającymi zastosowanie umowami i niniejszym CP/CPS.

1.4 Użycie certyfikatu

1.4.1. Dozwolone zastosowania certyfikatów

Certyfikaty TLS wydawane na podstawie niniejszego CP/CPS będą wykorzystywane do następujących celów:

- Uwierzytelnienie serwera (server authentication) - ustanowienie bezpiecznego kanału TLS pomiędzy serwerem Subskrybenta a stronami ufającymi
- Uwierzytelnienie klienta (client authentication) - weryfikacja tożsamości osób, organizacji lub urządzeń w scenariuszach mutual TLS (mTLS), jeżeli zezwala na to właściwy profil certyfikatu

Dozwolone użycie musi być zgodne z rozszerzeniami Key Usage (KU) i Extended Key Usage (EKU) zdefiniowanymi w profilu certyfikatu, a także z mającymi zastosowanie przepisami prawa i umową Subskrybenta (Subscriber Agreement) lub Warunkami użytkowania (Terms of Use).

Poziom zapewnienia zależy od typu walidacji:

- Certyfikaty TLS Domain Validation (DV) są odpowiednie dla środowisk niskiego ryzyka, ponieważ tożsamość Subskrybenta nie jest weryfikowana poza potwierdzeniem jego kontroli nad domeną
- Certyfikaty TLS Organization Validation (OV) są odpowiednie dla środowisk średniego ryzyka, w których wymagane jest zapewnienie zarówno kontroli nad domeną, jak i prawnego istnienia organizacji
- Certyfikaty TLS Extended Validation (EV) są odpowiednie dla środowisk wysokiego ryzyka i zapewniają najwyższy poziom zapewnienia, zgodnie z EV Guidelines, w celu weryfikacji prawnego, fizycznego i operacyjnego istnienia podmiotu

1.4.2 Zabronione zastosowania certyfikatów

Certyfikaty wydawane na podstawie niniejszego CP/CPS nie mogą być wykorzystywane do żadnego z poniższych celów:

- Infrastruktura wysokiego ryzyka (fail-safe) - jakiekolwiek zastosowanie wymagające bezawaryjnego działania, w którym awaria certyfikatu mogłaby prowadzić do śmierci, obrażeń ciała lub katastrofalnych szkód środowiskowych
- Nieuprawnione przechwytywanie - cele typu Man-in-the-Middle (MITM) lub skryte przechwytywanie ruchu bez wyraźnej zgody abonenta domeny
- Niewłaściwe zapewnienie tożsamości - wykorzystywanie certyfikatów TLS Domain Validated (DV) jako dowodu prawnego istnienia lub tożsamości organizacyjnej Subskrybenta
- Role infrastruktury PKI - działanie jako urząd certyfikacji (Certification Authority, CA) lub używanie certyfikatów końcowych do podpisywania albo wydawania innych certyfikatów lub CRL
- Technicznie niezamierzone użycie - jakiekolwiek zastosowanie wykraczające poza zakres określony przez rozszerzenia Key Usage (KU) i Extended Key Usage (EKU) w profilu certyfikatu
- Działania niezgodne z prawem - jakikolwiek cel sprzeczny z mającymi zastosowanie przepisami prawa, regulacjami lub ograniczeniami eksportowymi/importowymi

Zastrzeżenie: Wydając certyfikat, Certum potwierdza wyłącznie, że informacje zostały zweryfikowane w chwili wydania, i nie udziela gwarancji co do dalszej uczciwości, rzetelności ani wiarygodności Subskrybenta.

1.5 Zarządzanie polityką

1.5.1 Organizacja administrująca dokumentem

Niniejszy CP/CPS jest administrowany przez Certum Policy Authority.

Oficjalny adres organizacji to:

Asseco Data Systems S.A.
ul. Jana z Kolna 11
80-864 Gdańsk
Poland

1.5.2 Osoba kontaktowa

Pytania, uwagi lub wnioski dotyczące niniejszego CP/CPS należy kierować do Certum, korzystając z następujących danych kontaktowych:

Certum Certification Authority
Certum Policy Authority
ul. Bajeczna 13

71-838 Szczecin
Poland

Email: policy.pki@certum.pl

W celu zgłaszania problemów związanych z certyfikatami, w tym wniosków o unieważnienie lub zastrzeżeń dotyczących niniejszego CP/CPS, Certum udostępnia Certificate Problem Report pod adresem:

https://problemreport.certum.pl

Kanał ten powinien być wykorzystywany do składania Certificate Problem Reports, w tym zgłoszeń podejrzenia niewłaściwego użycia certyfikatu, kompromitacji lub niezgodności.

1.5.3 Osoba określająca przydatność CPS dla polityki

Certum Policy Authority określa zakres stosowania oraz przeznaczenie niniejszego CP/CPS.

1.5.4 Procedury zatwierdzania CPS

Niniejszy CP/CPS jest zatwierdzany i zmieniany przez Certum Policy Authority.

Niniejszy CP/CPS wchodzi w życie z chwilą jego publikacji w oficjalnym repozytorium Certum.

Wszystkie modyfikacje, w tym aktualizacje redakcyjne i zmiany wymagane przez regulacje lub standardy branżowe, są odnotowywane w historii zmian niniejszego dokumentu.

1.6 Definicje i akronimy

Zob. Aneks B w zakresie wykazu definicji i akronimów.

1.6.1 Definicje zgodnie z RFC 2119

W niniejszym CP/CPS stosowane są sformułowania normatywne odpowiadające znaczeniu słów kluczowych “MUST”, “MUST NOT”, “REQUIRED”, “SHALL”, “SHALL NOT”, “SHOULD”, “SHOULD NOT”, “RECOMMENDED”, “MAY” oraz “OPTIONAL” zdefiniowanych w RFC 2119.

2. PUBLIKACJA I OBOWIĄZKI ZWIĄZANE Z REPOZYTORIUM

2.1 Repozytoria

Certum prowadzi i utrzymuje publicznie dostępne Repozytorium dostępne pod adresem:

https://www.certum.pl/pl/repozytorium oraz https://repository.certum.pl/

Audit Attestation Letters są publikowane pod adresem:

https://pomoc.certum.pl/pl/wspolpraca-certum-i-webtrust

2.2 Publikacja informacji certyfikacyjnych

Certum publikuje kompleksowy zestaw dokumentacji, który obejmuje między innymi:

- Niniejszy dokument CP/CPS oraz dokumenty CP i CPS dla innych usług
- Publicznie zaufane certyfikaty Root CA, certyfikaty cross-signed CA i certyfikaty Subordinate CA
- Warunki użytkowania (Terms of Use)
- Politykę prywatności
- Zaufane źródła danych
- Wzory dokumentów

Listy unieważnionych certyfikatów (Certificate Revocation Lists, CRLs) dostępne w punktach dystrybucji wskazanych w każdym certyfikacie są dostępne pod adresem:

https://crl.certum.pl

Sprawdzanie statusu za pomocą protokołu Online Certificate Status Protocol (OCSP) jest dostępne pod adresem:

https://ocsp.certum.pl

2.3 Czas lub częstotliwość publikacji

CP/CPS jest przeglądany co najmniej raz na 365 dni lub za każdym razem, gdy zmiany standardów branżowych (takich jak wymagania CA/B Forum) powodują konieczność aktualizacji, i jest publikowany po zatwierdzeniu, zazwyczaj w terminie 7 dni od zatwierdzenia.

Publicznie zaufane certyfikaty Root CA, certyfikaty cross-signed CA i certyfikaty Subordinate CA są publikowane tak szybko, jak to możliwe po wydaniu.

Audit Attestation Letters są publikowane zgodnie z Sekcją 8.6.

CRL są publikowane zgodnie z Sekcją 4.9.7.

Inne aktualizacje są publikowane tak szybko, jak to możliwe po ich utworzeniu lub aktualizacji, zazwyczaj w terminie 7 dni od zatwierdzenia.

2.4 Kontrole dostępu do repozytoriów

Informacje publikowane w Repozytorium Certum są publicznie dostępne, nieograniczone i stale dostępne.

Certum stosuje zarówno logiczne, jak i fizyczne środki bezpieczeństwa, aby zapobiec nieuprawnionej modyfikacji, usunięciu lub naruszeniu integralności zawartości Repozytorium.

3. IDENTYFIKACJA I UWIERZYTELNIENIE

3.1 Nazewnictwo

3.1.1 Typy nazw

W przypadku certyfikatów TLS Domain Validation (DV) informacje Distinguished Name (DN) muszą być ograniczone do identyfikatorów związanych z domeną i nie mogą zawierać informacji o tożsamości organizacji.

W przypadku certyfikatów TLS Organization Validation (OV) i Extended Validation (EV) Distinguished Name (DN) musi zawierać zweryfikowane informacje o tożsamości organizacji zgodnie z odpowiednim profilem certyfikatu opisanym w Sekcji 7.1.

Rozszerzenie Subject Alternative Names (SAN) musi zawierać w pełni kwalifikowaną nazwę domenową (Fully-Qualified Domain Name, FQDN) i/lub adres IP.

3.1.2 Wymóg, aby nazwy były znaczące

Certum wymaga, aby nazwy zawarte w certyfikatach były znaczące i umożliwiały identyfikację podmiotu.

Żądania certyfikacyjne zawierające nazwy, które są mylące, niejednoznaczne, wykraczają poza zakres przeprowadzonej walidacji lub nie mogą zostać zwalidowane, będą odrzucane.

3.1.3 Anonimowość lub pseudonimowość Subskrybentów

Certum nie wydaje certyfikatów zawierających anonimowe lub pseudonimowe informacje o podmiocie.

3.1.4 Zasady interpretacji różnych form nazw

Distinguished Names w certyfikatach są interpretowane z wykorzystaniem standardów X.500 i składni ASN.1.

Nazwy domen są interpretowane zgodnie z mającymi zastosowanie standardami DNS.

Informacje o tożsamości organizacji zawierające znaki spoza ASCII mogą być normalizowane lub transliterowane do odpowiedników ASCII (np. zastąpienie znaków takich jak “ę” przez “e” albo “ö” przez “oe”).

Powszechnie uznawane warianty językowe lub tłumaczenia nazw geograficznych mogą być akceptowane (np. “Warsaw” zamiast “Warszawa”).

3.1.5 Unikalność nazw

Unikalność nazw podmiotu nie jest wymagana.

3.1.6 Rozpoznawanie, uwierzytelnianie i rola znaków towarowych

Certum nie wydaje certyfikatów zawierających nazwy, znaki towarowe ani inne identyfikatory, do których używania Wnioskodawca nie jest uprawniony.

Spory dotyczące znaków towarowych lub praw do nazewnictwa nie są rozstrzygane. W przypadku konfliktu lub niepewności żądania certyfikacyjne mogą zostać odrzucone lub wydane certyfikaty mogą zostać unieważnione.

3.2 Początkowa walidacja tożsamości

Certum może żądać od Wnioskodawcy dokumentacji wspierającej walidację żądania certyfikatu zgodnie z wymaganiami mającymi zastosowanie do żądanego typu certyfikatu.

Jakiekolwiek oznaki modyfikacji dokumentu, fałszerstwa lub wprowadzenia w błąd co do tożsamości albo statusu stanowią podstawę do odrzucenia żądania certyfikatu i mogą skutkować unieważnieniem wszelkich certyfikatów wydanych na podstawie takich informacji.

3.2.1 Metoda udowodnienia posiadania klucza prywatnego

Wnioskodawca potwierdza posiadanie klucza prywatnego odpowiadającego kluczowi publicznemu zawartemu w żądaniu certyfikatu poprzez złożenie żądania podpisania certyfikatu (Certificate Signing Request, CSR) w formacie PKCS#10.

3.2.2 Uwierzytelnienie tożsamości organizacji

3.2.2.1 Tożsamość

Certum weryfikuje prawną tożsamość organizacji dla wszystkich certyfikatów TLS OV i EV, wykorzystując wiarygodne i niezależne źródła, takie jak rejestry państwowe lub kwalifikowane bazy danych gospodarczych.

Lista zatwierdzonych źródeł jest utrzymywana pod adresem:

https://www.certum.pl/pl/zrodla-weryfikacji-certyfikatow/

Weryfikacja potwierdza:

- Prawne istnienie organizacji
- Pełną nazwę prawną ujawnioną w oficjalnych rejestrach
- Adres rejestrowy lub adres istnienia/prowadzenia działalności

W przypadku certyfikatów TLS EV stosowane są rozszerzone procedury weryfikacyjne. Procedury te obejmują dodatkową weryfikację:

- Prawnego istnienia organizacji w jej jurysdykcji
- Operacyjnego istnienia organizacji
- Fizycznego adresu organizacji

Wszystkie czynności weryfikacyjne i dowody są rejestrowane i przechowywane do celów audytowych. Informacje wykorzystywane do walidacji organizacji pozostają ważne przez maksymalny okres zgodnie z Sekcją 4.2.1.

Certum może zażądać lub zaakceptować dodatkową dokumentację niewymienioną powyżej, jeżeli jest to konieczne do zapewnienia rzetelnej i dokładnej weryfikacji informacji zawartych we wniosku o wydanie certyfikatu.

3.2.2.2 DBA/Nazwa handlowa

Wnioskodawca może zażądać umieszczenia w certyfikacie nazwy handlowej (określanej również jako “Doing Business As” lub nazwa DBA).

Certum weryfikuje prawo Wnioskodawcy do używania zgłoszonej nazwy handlowej przy użyciu metod opisanych w Sekcji 3.2.2.1 lub na podstawie jednego z poniższych dokumentów:

- listu poświadczającego (Attestation Letter) wraz z dokumentami potwierdzającymi lub innego dokumentu identyfikacyjnego uznanego przez Certum za wiarygodny

- rachunku za media, wyciągu bankowego, wyciągu z karty kredytowej, dokumentu podatkowego wydanego przez organ państwowy lub innego dokumentu uznanego za wiarygodny

Taka weryfikacja potwierdza, że nazwa handlowa jest zarejestrowana, prawnie uznana lub w inny sposób powiązana z Wnioskodawcą.

3.2.2.3 Weryfikacja kraju

Certum weryfikuje kraj poprzez weryfikację adresu z wykorzystaniem metod opisanych w Sekcji 3.2.2.1.

3.2.2.4 Walidacja upoważnienia do domeny lub kontroli nad domeną

Certum weryfikuje kontrolę Wnioskodawcy nad każdą nazwą domeny ujętą w żądaniu certyfikatu. Weryfikacja ta jest przeprowadzana przed wydaniem certyfikatu, wyłącznie w ramach Systemów Certum, i nie jest delegowana stronom trzecim.

Certum obsługuje następujące metody zdefiniowane w TLS BR:

- 3.2.2.4.4 Email to a Constructed Address
- 3.2.2.4.7 DNS Change
- 3.2.2.4.18 Agreed-Upon Change to Website v2
- 3.2.2.4.19 Agreed-Upon Change to Website - ACME

Dodatkowo Certum może przeprowadzać procedurę walidacji z wykorzystaniem kontroli względem dodatkowych źródeł danych i czarnych list (blacklists).

3.2.2.5 Uwierzytelnienie dla adresu IP

Certum weryfikuje kontrolę Wnioskodawcy nad każdym adresem IP ujętym w żądaniu certyfikatu. Weryfikacja ta jest przeprowadzana przed wydaniem certyfikatu, wyłącznie w ramach Systemów Certum, i nie jest delegowana stronom trzecim.

Certum obsługuje następujące metody zdefiniowane w TLS BR:

- 3.2.2.5.1 Agreed-Upon Change to Website
- 3.2.2.5.6 ACME “http-01” method for IP Addresses

Dodatkowo Certum może przeprowadzać procedurę walidacji z wykorzystaniem kontroli względem dodatkowych źródeł danych i czarnych list (blacklists).

3.2.2.6 Walidacja domen wieloznacznych (wildcard)

Domena typu wildcard jest zdefiniowana jako ciąg rozpoczynający się od gwiazdki i kropki (*.), po których następuje w pełni kwalifikowana nazwa domenowa (Fully-Qualified Domain Name, FQDN).

Jeżeli część FQDN dowolnej nazwy domeny wildcard jest etykietą “registry-controlled” lub “public suffix”, taką jak *.com lub *.pl, Certum musi odrzucić żądanie certyfikatu, chyba że Wnioskodawca wykaże swoje uprawnione prawo do kontroli całej przestrzeni nazw domeny (Domain Namespace).

Nazwy domen wildcard są bezwzględnie zabronione dla certyfikatów TLS EV.

3.2.2.7 Dokładność źródła danych

Zanim jakiekolwiek źródło danych zostanie wykorzystane jako zaufane źródło danych (Reliable Data Source), Certum ocenia to źródło pod względem wiarygodności, dokładności oraz odporności na modyfikację lub fałszerstwo.

Lista zatwierdzonych źródeł danych jest przeglądana co najmniej raz w roku. Po każdym przeglądzie zaktualizowana wersja listy jest publikowana na stronie internetowej Certum.

3.2.2.8 Rekordy CAA

Certum musi pobierać i przetwarzać rekordy CAA zgodnie z RFC 8659 dla każdej wartości dNSName w rozszerzeniu subjectAltName, która nie zawiera nazwy domeny onion.

Kontrola rekordów CAA jest wykonywana łącznie z procesem walidacji kontroli domeny i musi zostać pomyślnie zakończona przed jakimkolwiek wydaniem certyfikatu.

3.2.2.9. Potwierdzenie wydania z wielu perspektyw (Multi-Perspective Issuance Corroboration)

Certum wdraża Multi-Perspective Issuance Corroboration (MPIC) w celu potwierdzenia ustaleń dokonanych podczas walidacji domeny (Sekcja 3.2.2.4) oraz sprawdzania CAA (Sekcja 3.2.2.8) z wielu zdalnych perspektyw sieciowych przed wydaniem certyfikatu.

Perspektywy sieciowe są dobierane w celu zapewnienia różnorodności geograficznej, z zachowaniem odległości w linii prostej co najmniej 500 km pomiędzy nimi.

3.2.3 Uwierzytelnienie tożsamości osoby fizycznej

Certum nie wydaje certyfikatów TLS osobom fizycznym.

3.2.4 Nieweryfikowane informacje Subskrybenta

Certum nie umieszcza nieweryfikowanych informacji w certyfikatach TLS.

3.2.5 Walidacja uprawnień

W przypadku żądań certyfikatów zawierających nazwę organizacji Certum weryfikuje, że Wnioskodawca jest upoważniony do działania w imieniu wskazanego podmiotu prawnego w chwili wydania i posiada prawo do reprezentowania tego podmiotu.

Weryfikacja tożsamości osoby oraz jej umocowania jest przeprowadzana z wykorzystaniem zaufanych źródeł danych (Reliable Data Sources), dokumentów (takich jak upoważnienia, pełnomocnictwa lub zaświadczenia o zatrudnieniu) lub za pomocą zaufanej metody komunikacji (takiej jak telefon lub e-mail) z autorytatywnym źródłem w ramach organizacji.

3.2.6 Kryteria interoperacyjności

Certum może świadczyć usługi interoperacyjności w celu certyfikacji zewnętrznych urzędów certyfikacji (Certification Authorities, CAs). Taka interoperacyjność może obejmować cross-certification lub inne formy ustanowienia zaufania.

Interoperacyjność jest dozwolona wyłącznie wtedy, gdy spełnione są następujące kryteria:

- Zewnętrzny CA działa na podstawie Certificate Policy (CP) i Certification Practice Statement (CPS), które są zgodne z niniejszym CP/CPS lub co najmniej równie rygorystyczne
- Certum przeprowadza ocenę due diligence zewnętrznego CA w celu zapewnienia, że spełnia on wymogi bezpieczeństwa i operacyjne Certum
- Pomiędzy Certum a zewnętrznym CA obowiązuje formalna umowa określająca wzajemne prawa i obowiązki stron

Wszystkie certyfikaty cross-certificate wydane przez Certum są ujawniane w Repozytorium Certum oraz w Common CA Database (CCADB).

3.3 Identyfikacja i uwierzytelnienie dla wniosków o re-key

3.3.1 Identyfikacja i uwierzytelnienie dla rutynowego re-key

Subskrybenci mogą zażądać re-key certyfikatu. Autoryzacja dla re-key może zostać ustanowiona poprzez złożenie żądania certyfikatu z wykorzystaniem Systemu Certum.

W przypadku żądań re-key Certum może przeprowadzić ponowną walidację Wnioskodawcy, ale może również oprzeć się na informacjach uzyskanych podczas poprzedniego procesu identyfikacji.

3.3.2 Identyfikacja i uwierzytelnienie dla re-key po unieważnieniu

Jeżeli certyfikat został unieważniony, a unieważnienie nie jest związane z incydentami bezpieczeństwa, Subskrybenci mogą złożyć nowe żądanie re-key. Takie żądanie jest traktowane jako rutynowy re-key i podlega tym samym wymaganiom dotyczącym identyfikacji i uwierzytelnienia, jak opisano w Sekcji 3.3.1.

3.4 Identyfikacja i uwierzytelnienie dla wniosku o unieważnienie

Strona zarządzająca kontem Systemu Certum, do którego wydano certyfikat, może zażądać unieważnienia przez uwierzytelnienie się w Systemie Certum i zgłoszenie unieważnienia za pośrednictwem tego systemu.

Każdy może zażądać unieważnienia za pomocą formularza webowego Certificate Problem Report. Wymaga to przejścia dodatkowych etapów weryfikacyjnych przeprowadzanych przez Certum przy użyciu metod opisanych w Sekcji 3.2.

4. WYMAGANIA OPERACYJNE DOTYCZĄCE CYKLU ŻYCIA CERTYFIKATU

4.1 Wniosek o certyfikat

4.1.1 Kto może złożyć wniosek o certyfikat

Wniosek o certyfikat może zostać złożony przez Wnioskodawcę lub przez osobę upoważnioną do działania w jego imieniu. Wnioskodawca odpowiada za dokładność wszystkich przekazanych informacji.

Certum nie wydaje certyfikatów Wnioskodawcom zlokalizowanym w jurysdykcjach, w których wydanie naruszałoby przepisy prawa Rzeczypospolitej Polskiej lub mające zastosowanie sankcje Unii Europejskiej.

4.1.2 Proces rejestracji i odpowiedzialności

Proces rejestracji może obejmować:

- Złożenie wniosku o certyfikat (certificate Application)
- Wygenerowanie pary kluczy (key pair)
- Przekazanie klucza publicznego
- Akceptację mających zastosowanie Warunków użytkowania (Terms of Use) lub umowy Subskrybenta (Subscriber Agreement)
- Dostarczenie dokumentacji uzupełniającej, jeśli jest wymagana
- Uiszczenie mających zastosowanie opłat

Wnioskodawca odpowiada za przekazanie dokładnych i kompletnych informacji we wniosku o certyfikat oraz za spełnienie wszystkich wymagań procesu rejestracji.

Niedostarczenie dokładnych informacji lub niespełnienie tych wymagań może skutkować odrzuceniem wniosku o certyfikat.

4.2 Przetwarzanie wniosku o certyfikat

4.2.1 Wykonywanie czynności identyfikacji i uwierzytelnienia

Certum wykonuje procedury identyfikacji i uwierzytelnienia podczas przetwarzania każdego wniosku o certyfikat, aby zweryfikować tożsamość i umocowanie Wnioskodawcy zgodnie z metodami opisanymi w Sekcji 3.2.

Wszystkie procedury identyfikacji i uwierzytelnienia MUSZĄ zostać pomyślnie zakończone przed wydaniem certyfikatu.

Jeżeli niezbędne dane nie są dostępne z zaufanych źródeł wewnętrznych, Certum pozyskuje je bezpośrednio od Wnioskodawcy lub z Reliable Data Sources.

Certum może ponownie wykorzystać dane walidacyjne i dokumentację uzyskaną podczas poprzednich procesów identyfikacji, pod warunkiem że takie informacje pozostają dokładne i zostały uzyskane nie wcześniej niż 398 dni przed datą wydania.

Certum utrzymuje udokumentowane procedury identyfikowania żądań certyfikatów wysokiego ryzyka, które wymagają dodatkowych czynności weryfikacyjnych przed zatwierdzeniem. Procedury te obejmują utrzymywanie wewnętrznej bazy danych wcześniej unieważnionych certyfikatów i odrzuconych wniosków związanych z podejrzeniem phishingu, oszustwa lub innych złośliwych działań. Certum może odrzucać wnioski o certyfikaty na podstawie tych danych.

4.2.2 Zatwierdzanie lub odrzucanie wniosków o certyfikat

Certum może zatwierdzać wnioski o certyfikat wyłącznie wtedy, gdy wszystkie przekazane informacje zostały pomyślnie zwalidowane.

Certum nie może wydawać certyfikatu zawierającego nazwy wewnętrzne lub adresy IP oznaczone przez IANA jako zastrzeżone.

Certum może odrzucić wniosek o certyfikat z dowolnego powodu, w tym między innymi gdy:

- Wniosek o certyfikat zawiera nową gTLD, która nadal jest rozpatrywana przez ICANN
- Wnioskodawca podaje fałszywe lub wprowadzające w błąd informacje albo składa zmienioną lub sfałszowaną dokumentację
- Wniosek o certyfikat zostaje zidentyfikowany jako wysokiego ryzyka lub potencjalnie oszukańczy
- Wydanie certyfikatu stwarzałoby ryzyko prawne, regulacyjne, bezpieczeństwa lub reputacyjne dla CA albo dla ekosystemu zaufania
- Wnioskodawca nie ukończy procedur identyfikacji i uwierzytelnienia w ciągu 30 dni od złożenia wniosku o certyfikat

Wnioskodawcy, których wnioski zostały odrzucone, mogą następnie ponownie złożyć wniosek.

Wnioskodawca nie jest uprawniony do żadnego zwrotu ani odszkodowania, jeżeli zostały przekazane fałszywe lub wprowadzające w błąd informacje albo złożono sfałszowaną dokumentację.

4.2.3 Czas przetwarzania wniosków o certyfikat

Certum dokłada należytej staranności, aby od momentu otrzymania kompletnego wniosku o wydanie certyfikatu przetworzyć wniosek oraz wydać certyfikat w terminie do 7 dni roboczych, przy czym czas wydania danego rodzaju certyfikatu określony jest na stronie internetowej Certum.

Rzeczywisty czas przetwarzania zależy przede wszystkim od:

- Szybkości reakcji Wnioskodawcy w zakresie dostarczenia niezbędnych szczegółów i wyjaśnień
- Kompletności i poprawności złożonego wniosku
- Dostępności informacji z Reliable Data Sources

Certum może wydłużyć czas przetwarzania lub odrzucić wniosek, jeżeli Wnioskodawca nie dostarczy wymaganej dokumentacji w rozsądnym terminie albo jeżeli podczas procesu weryfikacji pojawią się komplikacje.

Certum nie ponosi odpowiedzialności za opóźnienia wynikające ze zdarzeń pozostających poza jego uzasadnioną kontrolą.

4.2.4 Certificate Authority Authorization (CAA)

W procesie wydawania certyfikatów TLS Certum weryfikuje rekordy DNS Certification Authority Authorization (CAA) dla każdej nazwy `dNSName` wskazanej w rozszerzeniu `subjectAltName` certyfikatu przeznaczonego do wydania.

Weryfikacja rekordów CAA jest realizowana zgodnie z: - RFC 8659 oraz sekcją 3.2.2.8 TLS BR

Certum uznaje następujące nazwy domen wystawcy w tagach właściwości CAA “issue” lub “issuewild” za przyznające upoważnienie do wydawania certyfikatów przez Certum:

- certum.pl
- certum.eu

Certum rozpoznaje parametry `accounturi` oraz `validationmethods` zgodnie z RFC 8657.

Parametr `accounturi` musi mieć postać URL: - Dla wniosków certyfikacyjnych złożonych przez ACME: - `https://acme.certum.pl/account/{identyfikator konta}` - For certificate requests not issued by ACME: - `https://certmanager.certum.pl/account/{identyfikator konta}`

Parametr `validationmethods` musi mieć wartość: - Dla wniosków certyfikacyjnych złożonych przez ACME:

Metody weryfikacji domen	Obsługiwane wartości
Agreed-Upon Change to Website - ACME	http-01ca-tbr-19
DNS Change	dns-01ca-tbr-7

- Dla wniosków certyfikacyjnych nie złożonych przez ACME:

Metody weryfikacji domen	Obsługiwane wartości
Agreed-Upon Change to Website v2	ca-tbr-18
DNS Change	ca-tbr-7
Constructed Email to Domain Contact	ca-tbr-4

Certyfikat nie zostanie wydany, jeżeli spełniony jest którykolwiek z poniższych warunków: - Rekord CAA nie zezwala na wydanie certyfikatu przez Certum - Rekord CAA zawiera nierozpoznaną właściwość oznaczoną flagą critical - Rekord CAA nie pozwala na wydanie certyfikatu przez wnioskujące konto - Rekord CAA nie pozwala na użycie wybranej metody weryfikacji domeny do wydania certyfikatu - Rekord CAA zawiera parametr `accounturi` i/lub `validationmethods` w formacie niezgodnym z RFC 8657

Błędy podczas wyszukiwania lub walidacji rekordów CAA nie stanowią autoryzacji do wydania certyfikatu.

4.3 Wydanie certyfikatu

4.3.1 Działania CA podczas wydawania certyfikatu

Certum będzie wykonywać wydanie certyfikatu wyłącznie po pomyślnym zakończeniu procedur walidacyjnych mających zastosowanie do danego typu certyfikatu, jak określono w Sekcji 3 i Sekcji 4.2.

Precertyfikaty (precertificates) podlegają lintingowi przedwydaniowemu (pre-issuance linting) w celu weryfikacji zgodności technicznej. Linting przedwydaniowy wykorzystuje uznane w branży narzędzia, w tym ZLint i pkilint. Jeżeli zostanie wykryta niezgodność, wydanie jest wstrzymywane.

Proces lintingu może być wykorzystywany do weryfikacji zgodności technicznej certyfikatów końcowych.

Precertyfikaty są przekazywane do logów Certificate Transparency zgodnie z mającymi zastosowanie wymaganiami.

Wydanie certyfikatu przez Root CA wymaga świadomego działania upoważnionego personelu pełniącego Role Zaufane (Trusted Roles) w celu wykonania operacji podpisania certyfikatu.

4.3.2 Powiadomienie Subskrybenta przez CA o wydaniu certyfikatu

Certum może powiadomić Wnioskodawcę o wydaniu certyfikatu pocztą elektroniczną lub innymi środkami, wskazując sposób uzyskania certyfikatu. Powiadomienie to nie zawiera samego certyfikatu.

4.4 Akceptacja certyfikatu

4.4.1 Zachowanie stanowiące akceptację certyfikatu

Subskrybent odpowiada za sprawdzenie treści wydanego certyfikatu, w tym weryfikację poprawności zawartych w nim informacji oraz zgodności klucza publicznego z odpowiadającym mu kluczem prywatnym.

Certyfikat uznaje się za zaakceptowany, gdy Subskrybent:

- Pobierze i zainstaluje certyfikat na serwerze albo użyje certyfikatu w dowolnej operacji kryptograficznej, albo
- Uplynie 7 dni od daty udostępnienia certyfikatu

Akceptacja certyfikatu stanowi oświadczenie Subskrybenta, że przed użyciem certyfikatu zapoznał się on z niniejszym CP/CPS i zobowiązuje się do jego przestrzegania oraz do przestrzegania mających zastosowanie Warunków użytkowania (Terms of Use) lub umowy Subskrybenta (Subscriber Agreement).

4.4.2 Publikacja certyfikatu przez CA

Wszystkie publicznie zaufane certyfikaty Root CA, certyfikaty cross-signed CA i certyfikaty Subordinate CA są publikowane w Repozytorium Certum opisanym w Sekcji 2.1.

Certum udostępnia certyfikaty końcowe Subskrybentom za pośrednictwem Systemów Certum.

4.4.3 Powiadomienie innych podmiotów przez CA o wydaniu certyfikatu

Informacja o certyfikatach przeznaczonych do wykorzystania jest udostępniana publicznie poprzez publikację precertyfikatów w logach Certificate Transparency. Certum nie gwarantuje wydania certyfikatu końcowego dla każdego wygenerowanego precertyfikatu.

Certum może powiadamiać inne podmioty uczestniczące w procesie rejestracji o wydaniu certyfikatu.

4.5 Użycie pary kluczy i certyfikatu

4.5.1 Użycie klucza prywatnego i certyfikatu przez Subskrybenta

Subskrybenci powinni:

- Używać certyfikatu wyłącznie zgodnie z jego przeznaczeniem oraz zgodnie z mającymi zastosowanie przepisami prawa, niniejszym CP/CPS i mającymi zastosowanie Warunkami użytkowania (Terms of Use) lub umową Subskrybenta (Subscriber Agreement)
- Chronić swoje klucze prywatne przed nieuprawnionym dostępem, ujawnieniem lub użyciem
- Natychmiast zaprzestać używania klucza prywatnego i powiązanego certyfikatu po unieważnieniu lub wygaśnięciu certyfikatu

Certyfikaty powinny być używane wyłącznie w okresie ich ważności i zgodnie z rozszerzeniami Key Usage (KU) i Extended Key Usage (EKU) określonymi w certyfikacie.

4.5.2 Użycie klucza publicznego i certyfikatu przez stronę ufającą

Strony ufające powinny:

- Weryfikować status certyfikatu przed poleganiem na nim, w tym sprawdzać informacje o unieważnieniu
- Upewniać się, że certyfikat jest wykorzystywany wyłącznie zgodnie z jego przeznaczeniem i w okresie jego ważności
- Polegać na certyfikacie wyłącznie w zakresie dozwolonym przez niniejszy CP/CPS i mające zastosowanie umowy

Decyzja o poleganiu na certyfikacie pozostaje wyłączną odpowiedzialnością strony ufającej.

4.6 Odnowienie certyfikatu

Odnowienie certyfikatu skutkuje wydaniem Subskrybentowi nowego certyfikatu bez zmiany klucza publicznego Subskrybenta lub innego uczestnika ani jakiejkolwiek innej informacji zawartej w certyfikacie.

4.6.1 Okoliczności odnowienia certyfikatu

Certum nie obsługuje odnowienia certyfikatu z ponownym użyciem klucza.

Termin “renewal” w ofercie Certum i Systemach Certum ma charakter komercyjny i nie odzwierciedla formalnego procesu odnowienia zdefiniowanego w niniejszym CP/CPS. Każde takie żądanie “renewal” wymaga wygenerowania nowej pary kluczy i złożenia odpowiadającego jej klucza publicznego.

4.6.2 Kto może zażądać odnowienia

Nie dotyczy.

4.6.3 Przetwarzanie wniosków o odnowienie certyfikatu

Nie dotyczy.

4.6.4 Powiadomienie Subskrybenta o wydaniu nowego certyfikatu

Nie dotyczy.

4.6.5 Zachowanie stanowiące akceptację odnowionego certyfikatu

Nie dotyczy.

4.6.6 Publikacja odnowionego certyfikatu przez CA

Nie dotyczy.

4.6.7 Powiadomienie innych podmiotów przez CA o wydaniu certyfikatu

Nie dotyczy.

4.7 Re-key certyfikatu

Re-key skutkuje wydaniem Subskrybentowi nowego certyfikatu z nowo wygenerowanym kluczem publicznym i nowym numerem seryjnym.

4.7.1 Okoliczności re-key certyfikatu

Subskrybenci mogą zażądać re-key z dowolnego powodu.

Subskrybent może dodać nazwę domeny lub adres IP do SAN nowego certyfikatu, ale pozostałe informacje w subject muszą pozostać niezmienione. Nowe nazwy domen lub adresy IP muszą zostać zwalidowane zgodnie z mającymi zastosowanie procedurami opisanymi w Sekcji 3.2.

4.7.2 Kto może zażądać certyfikacji nowego klucza publicznego

Wiele certyfikatów może zostać wydanych temu samemu Subskrybentowi w ramach jednego okresu subskrypcji.

Zob. Sekcja 4.1.1.

4.7.3 Przetwarzanie wniosków o re-key certyfikatu

Certum może polegać na wcześniej zwalidowanych informacjach, jeżeli pozostają one ważne. W przeciwnym razie Certum będzie przeprowadzać walidację zgodnie z Sekcją 4.1 i Sekcją 4.2.

4.7.4 Powiadomienie Subskrybenta o wydaniu nowego certyfikatu

Zob. Sekcja 4.3.2.

4.7.5 Zachowanie stanowiące akceptację certyfikatu po re-key

Zob. Sekcja 4.4.1.

4.7.6 Publikacja certyfikatu po re-key przez CA

Zob. Sekcja 4.4.2.

4.7.7 Powiadomienie innych podmiotów przez CA o wydaniu certyfikatu

Zob. Sekcja 4.4.3.

4.8 Modyfikacja certyfikatu

Modyfikacja certyfikatu skutkuje wydaniem Subskrybentowi nowego certyfikatu z powodu zmian informacji zawartych w certyfikacie innych niż klucz publiczny Subskrybenta.

4.8.1 Okoliczności modyfikacji certyfikatu

Certum nie obsługuje modyfikacji certyfikatu. Każde żądanie certyfikatu wymaga wygenerowania nowej pary kluczy i złożenia odpowiadającego jej klucza publicznego.

4.8.2 Kto może zażądać modyfikacji certyfikatu

Nie dotyczy.

4.8.3 Przetwarzanie wniosków o modyfikację certyfikatu

Nie dotyczy.

4.8.4 Powiadomienie Subskrybenta o wydaniu nowego certyfikatu

Nie dotyczy.

4.8.5 Zachowanie stanowiące akceptację zmodyfikowanego certyfikatu

Nie dotyczy.

4.8.6 Publikacja zmodyfikowanego certyfikatu przez CA

Nie dotyczy.

4.8.7 Powiadomienie innych podmiotów przez CA o wydaniu certyfikatu

Nie dotyczy.

4.9 Unieważnienie i zawieszenie certyfikatu

Unieważnienie certyfikatu trwale kończy okres operacyjny certyfikatu przed pierwotną datą jego wygaśnięcia. Certyfikaty, które wygasły, nie mogą zostać unieważnione. Certum nie obsługuje zawieszenia certyfikatu.

4.9.1 Okoliczności unieważnienia

4.9.1.1 Powody unieważnienia certyfikatu Subskrybenta

Subskrybent może w dowolnym momencie zażądać unieważnienia swojego certyfikatu. Składając żądanie unieważnienia, Subskrybent powinien wybrać powód unieważnienia najlepiej odpowiadający jego sytuacji:

- Kompromitacja klucza (key compromise): Subskrybent ma podstawy sądzić, że jego klucz prywatny został skompromitowany (CRLReason #1, keyCompromise)
- Zaprzestanie działalności (cessation of operation): Subskrybent nie kontroluje już nazw domen wymienionych w certyfikacie lub nie używa już certyfikatu z powodu zaprzestania korzystania z powiązanej domeny lub usługi (CRLReason #2, cessationOfOperation)
- Zmiana powiązania (affiliation changed): nazwa organizacji lub inne informacje o tożsamości podmiotu zawarte w certyfikacie uległy zmianie (CRLReason #3, affiliationChanged)
- Zastąpienie (superseded): certyfikat został zastąpiony nowym certyfikatem (CRLReason #4, superseded)

Jeżeli żaden z wymienionych powodów nie ma zastosowania do żądania unieważnienia, Subskrybent nie powinien wskazywać innego powodu niż “unspecified”. Bez wskazania CRLreason Certum może unieważnić certyfikat (CRLReason “unspecified (0)”, co skutkuje brakiem rozszerzenia reasonCode w CRL);

Powyższe powody stanowią przyczyny unieważnienia dostępne dla Subskrybenta przy składaniu wniosku o unieważnienie certyfikatu. Pełna lista przyczyn unieważnienia stosowanych przez Certum jest określona w sekcji 7.2.2.

Certum unieważnia certyfikat Subskrybenta w terminie 24 godzin lub 5 dni, w zależności od przypadku, dla wszystkich przesłanek określonych w sekcji 4.9.1.1 TLS Baseline Requirements.

4.9.1.2 Powody unieważnienia Subordinate CA

Certum unieważnia certyfikat Subordinate CA w ciągu 7 dni dla wszystkich przesłanek określonych w TLS BR Sekcja 4.9.1.2.

4.9.2 Kto może zażądać unieważnienia

Unieważnienia certyfikatu mogą żądać:

- Subskrybent lub jego upoważniony przedstawiciel
- Strona zarządzająca kontem Systemu Certum, do którego wydano certyfikat
- Inne strony trzecie w przypadku problemów związanych z kompromitacją, oszustwem, niewłaściwym użyciem lub jakąkolwiek inną kwestią związaną z certyfikatem
- Certum może unieważnić certyfikat bez otrzymania wniosku i bez podania przyczyny

4.9.3 Procedura wniosku o unieważnienie

Certum zapewnia ciągłą, całodobową (24/7) zdolność do przyjmowania i obsługi wniosków o unieważnienie certyfikatów oraz zgłoszeń problemów z certyfikatami (Certificate Problem Reports).

Wniosek o unieważnienie może zostać zainicjowany przez konto Systemu Certum, do którego wydano certyfikat. Metoda ta jest przeznaczona wyłącznie dla certyfikatów zarządzanych w ramach tego konta.

- Wymagane informacje obejmują identyfikator certyfikatu oraz powód unieważnienia
- Wniosek o unieważnienie certyfikatu jest przetwarzany niezwłocznie
- Subskrybent jest informowany o unieważnieniu pocztą elektroniczną lub innymi odpowiednimi środkami

Wniosek o unieważnienie może również zostać złożony za pośrednictwem Certificate Problem Report, jak opisano w Sekcji 1.5.2. Metoda ta może zostać użyta do żądania unieważnienia dowolnego certyfikatu wydanego przez CA.

- Wymagane informacje obejmują między innymi identyfikator certyfikatu, powód unieważnienia oraz wystarczające informacje kontaktowe pozwalające CA uwierzytelnić zgłaszającego i uzyskać dodatkowe informacje, jeżeli będzie to konieczne
- Certum przetwarza wniosek o unieważnienie i może przeprowadzić procedury weryfikacyjne zgodnie z Sekcją 3.2
- Certum może skontaktować się z Subskrybentem lub innymi właściwymi stronami w celu zweryfikowania wniosku i uzyskania wszelkich dodatkowych informacji niezbędnych do jego przetworzenia
- Po pomyślnej weryfikacji CA unieważnia certyfikat i powiadamia Subskrybenta o unieważnieniu pocztą elektroniczną lub innymi odpowiednimi środkami

4.9.4 Okres karencji dla wniosku o unieważnienie

Subskrybenci powinni zgłaszać wszelkie okoliczności stanowiące podstawę do unieważnienia certyfikatu bez zbędnej zwłoki, jednak nie później niż 24 godziny po wykryciu incydentu. Obowiązek ten dotyczy w szczególności podejrzenia lub potwierdzenia kompromitacji klucza prywatnego (private key compromise).

4.9.5 Czas, w jakim CA musi przetworzyć wniosek o unieważnienie

Certum przetwarza wnioski o unieważnienie w terminie do 24 godzin od otrzymania zgłoszenia problemu z certyfikatem (Certificate Problem Report), zgodnie z sekcją 4.9.5 TLS Baseline Requirements.

Po przeprowadzeniu analizy i potwierdzeniu zasadności zgłoszenia Certum unieważnia certyfikat w terminie 24 godzin lub 5 dni, w zależności od przypadku, nie przekraczając terminów określonych w Sekcji 4.9.1.1.

Status unieważnionego certyfikatu jest odzwierciedlony w odpowiedziach OCSP w ciągu 1 godziny, a w CRL w ciągu 24 godzin.

4.9.6 Wymóg sprawdzania unieważnienia dla stron ufających

Strony ufające powinny sprawdzać ważność każdego certyfikatu w łańcuchu certyfikacji przed poleganiem na certyfikacie, w tym weryfikować informacje o unieważnieniu z użyciem odpowiedniego OCSP lub CRL.

4.9.7 Częstotliwość wydawania CRL

W przypadku CA wydających certyfikaty Subskrybentów Certum:

- Aktualizuje i publikuje nową CRL co najmniej co 7 dni
- Aktualizuje i publikuje nową CRL w ciągu 24 godzin od odnotowania unieważnienia certyfikatu

W przypadku CA wydających certyfikaty CA Certum:

- Aktualizuje i publikuje nową CRL co najmniej co 12 miesięcy
- Aktualizuje i publikuje nową CRL w ciągu 24 godzin od odnotowania unieważnienia certyfikatu

4.9.8 Maksymalne opóźnienie publikacji CRL

CRL są publikowane do repozytorium CRL automatycznie, zazwyczaj w ciągu 10 minut od wygenerowania i nie później niż w ciągu 24 godzin.

4.9.9 Dostępność sprawdzania unieważnienia/statusu online

Lokalizacje responderów OCSP (URL) muszą być zawarte w rozszerzeniu Authority Information Access (AIA) odpowiednich certyfikatów.

Odpowiedzi OCSP muszą być zgodne z RFC 6960 i/lub RFC 5019.

Odpowiedzi OCSP muszą być podpisywane cyfrowo przez responder OCSP, którego certyfikat jest podpisany przez issuing CA.

Certyfikat podpisujący respondera musi zawierać rozszerzenie typu `id-pkix-ocsp-nocheck`, zgodnie z definicją w RFC 6960.

4.9.10 Wymagania dotyczące sprawdzania unieważnienia online

Responder OCSP Certum:

- Musi obsługiwać metodę HTTP GET do odbierania żądań statusowych
- Nie może zwracać statusu “good” dla numeru seryjnego certyfikatu, który jest “unused” lub “unassigned”

W odniesieniu do statusu certyfikatów Subskrybentów Certum:

- Musi zapewniać, że odpowiedzi OCSP mają okres ważności co najmniej 8 godzin, ale nie dłuższy niż 10 dni
- Musi udostępniać autorytatywną odpowiedź OCSP nie później niż w ciągu 15 minut od momentu pierwszej publikacji lub innego udostępnienia certyfikatu albo precertyfikatu

W odniesieniu do statusu certyfikatów Subordinate CA Certum:

- Musi aktualizować informacje OCSP co najmniej co 12 miesięcy
- Musi aktualizować informacje OCSP w ciągu 24 godzin od unieważnienia certyfikatu Subordinate CA

4.9.11 Inne dostępne formy ogłaszania unieważnień

Nie dotyczy.

4.9.12 Szczególne wymagania dotyczące kompromitacji klucza

Kompromitacja klucza (key compromise) może zostać wykazana na jeden z następujących sposobów:

- Złożenie CSR, którego Common Name zawiera tekst “This key is compromised” lub podobny, podpisanego skompromitowanym kluczem, albo
- Złożenie samego klucza prywatnego

4.9.13 Okoliczności zawieszenia

Certum nie obsługuje zawieszenia certyfikatu.

4.9.14 Kto może zażądać zawieszenia

Nie dotyczy.

4.9.15 Procedura wniosku o zawieszenie

Nie dotyczy.

4.9.16 Ograniczenia okresu zawieszenia

Nie dotyczy.

4.10 Usługi statusu certyfikatu

4.10.1 Charakterystyka operacyjna

Informacja o statusie certyfikatu jest dostępna za pośrednictwem CRL i respondera OCSP.

Wpis unieważnienia w CRL lub odpowiedzi OCSP nie może zostać usunięty przed upływem daty wygaśnięcia unieważnionego certyfikatu.

4.10.2 Dostępność usług

Certum utrzymuje zdolność CRL i OCSP przy wykorzystaniu zasobów wystarczających do zapewnienia czasu odpowiedzi wynoszącego 10 sekund lub mniej w normalnych warunkach operacyjnych.

Usługi statusu certyfikatów są dostępne 24x7, chyba że są czasowo niedostępne z powodu prac utrzymaniowych lub awarii usługi.

4.10.3 Funkcje opcjonalne

Nie dotyczy.

4.11 Koniec subskrypcji

Subskrypcja usług certyfikatowych Subskrybenta kończy się, gdy:

- certyfikat wygasa i nie zostaje zastąpiony

- certyfikat zostaje unieważniony i nie zostaje zastąpiony
- Certum zaprzestaje świadczenia usług certyfikatowych

4.12 Escrow i odzyskiwanie kluczy

Certum nie obsługuje escrow kluczy.

4.12.1 Polityka i praktyki escrow oraz odzyskiwania kluczy

Nie dotyczy.

4.12.2 Polityka i praktyki enkapsulacji oraz odzyskiwania kluczy sesyjnych

Nie dotyczy.

5. KONTROLE FIZYCZNE, ZARZĄDCZE I OPERACYJNE

5.1 Kontrole fizyczne

Certum wdraża fizyczne i środowiskowe kontrole bezpieczeństwa jako część ogólnego programu bezpieczeństwa w celu ochrony danych certyfikatów oraz procesów zarządzania certyfikatami przed nieuprawnionym dostępem, uszkodzeniem i zakłóceniem. Kontrole te są wdrażane w sposób współmierny do wrażliwości chronionych systemów i danych.

5.1.1 Lokalizacja i konstrukcja obiektu

Certum działa w obiektach Asseco Data Systems S.A. wybranych i utrzymywanych na podstawie kryteriów bezpieczeństwa, operacyjnych i ryzyka. Wszystkie obiekty mają solidną konstrukcję zapobiegającą nieuprawnionemu wejściu i znajdują się w wybranym zestawie lokalizacji ocenionych pod kątem bezpieczeństwa fizycznego.

Krytyczne systemy PKI, w tym systemy CA i moduły kryptograficzne, są zlokalizowane w wydzielonych, fizycznie chronionych strefach wysokiego bezpieczeństwa, oddzielonych od ogólnych środowisk biurowych. Obszary te są zaprojektowane i utrzymywane w sposób zapobiegający nieuprawnionemu dostępowi, uszkodzeniu i zakłóceniom oraz zapewniający odpowiednią ochronę danych certyfikatów i procesów zarządzania certyfikatami.

5.1.2 Dostęp fizyczny

Fizyczny dostęp do obiektów Certum jest ograniczony do upoważnionego personelu i kontrolowany za pośrednictwem systemów kontroli dostępu. Wszystkie wejścia i wyjścia są zabezpieczone lub monitorowane przez ochronę albo systemy monitoringu/kontroli.

Prawa dostępu są przydzielane na podstawie ról i odpowiedzialności oraz podlegają mechanizmom uwierzytelniania i monitorowania. Wejście do obszarów chronionych jest kontrolowane z wykorzystaniem systemów kontroli dostępu, w tym kart mikroprocesorowych lub równoważnych mechanizmów.

Dostęp do stref wysokiego bezpieczeństwa, w których znajdują się krytyczne systemy PKI, jest ograniczony do szczególnie upoważnionego personelu pełniącego Trusted Roles. Dodatkowe ograniczenia mogą mieć zastosowanie do operacji wrażliwych, w tym kontrola wieloosobowa tam, gdzie jest wymagana.

Cały dostęp do obszarów chronionych jest monitorowany, a zdarzenia wejścia i wyjścia są rejestrowane. Goście, audytorzy i personel serwisowy mogą uzyskać dostęp do obszarów chronionych wyłącznie po uzyskaniu upoważnienia oraz, tam gdzie jest to wymagane, pod nadzorem lub w asyście upoważnionego personelu Certum.

5.1.3 Zasilanie i klimatyzacja

Obiekty Certum są wyposażone w systemy zasilania zaprojektowane tak, aby zapewnić ciągłe działanie systemów krytycznych. Obejmują one systemy zasilania bezprzerwowego (uninterruptible power supply, UPS) oraz zapasowe generatory prądu.

Kontrole środowiskowe, w tym klimatyzacja i monitorowanie temperatury, są wdrożone w celu zapewnienia niezawodnego działania 24/7.

5.1.4 Zagrożenia związane z wodą

Obiekty Certum są chronione przed ryzykami związanymi z wodą dzięki wykorzystaniu czujników wilgotności i wykrywania wody zainstalowanych w strefach wysokiego bezpieczeństwa.

Czujniki te są zintegrowane z systemem bezpieczeństwa budynku. W przypadku wykrycia odpowiedni personel jest powiadamiany i uruchamiane są procedury reakcji, w tym eskalacja do zarządzania obiektem, personelu bezpieczeństwa i administratorów systemów, stosownie do sytuacji.

5.1.5 Zapobieganie pożarom i ochrona przeciwpożarowa

Obiekty Certum są wyposażone w systemy wykrywania i gaszenia pożaru zgodne z lokalnymi standardami i przepisami bezpieczeństwa pożarowego.

Serwerownie i obszary, w których znajdują się systemy krytyczne, są chronione przez automatyczne systemy wykrywania pożaru oraz gazowe systemy gaszenia pożaru zaprojektowane tak, aby minimalizować szkody w sprzęcie i zapewniać ciągłość działania.

5.1.6 Przechowywanie nośników

Nośniki zawierające informacje wrażliwe, w tym nośniki kopii zapasowych i dane systemowe, są przechowywane w bezpiecznych lokalizacjach z dostępem ograniczonym do upoważnionego personelu.

Miejsca przechowywania są chronione przed nieuprawnionym dostępem, zagrożeniami środowiskowymi i uszkodzeniem.

5.1.7 Utylizacja odpadów

Nośniki i materiały zawierające informacje wrażliwe są utylizowane w bezpieczny sposób, aby zapobiec nieuprawnionemu dostępowi do danych:

- Dokumenty papierowe zawierające informacje wrażliwe są niszczone na miejscu przez rozdrabnianie
- Urządzenia pamięci masowej są fizycznie niszczone lub bezpiecznie wymazywane z wykorzystaniem zatwierdzonych narzędzi w celu uniemożliwienia odzyskania danych, zgodnie z NIST SP 800-88 lub równoważnymi standardami
- Klucze prywatne przechowywane w HSM są wymazywane (zeroized) po wycofaniu urządzenia z użycia w sposób uniemożliwiający ich odzyskanie

5.1.8 Kopia zapasowa poza lokalizacją podstawową

Certum utrzymuje kopie zapasowe danych krytycznych i konfiguracji systemów. Nośniki kopii zapasowych są przechowywane w bezpiecznych obiektach poza lokalizacją

podstawową, geograficznie odmiennych od lokalizacji podstawowej, w celu zapewnienia dostępności w przypadku katastrofy regionalnej.

Dostęp do nośników kopii zapasowych jest ograniczony do upoważnionego personelu. Procesy tworzenia kopii zapasowych są zaprojektowane tak, aby zapewnić integralność i dostępność przechowywanych danych.

Kopie zapasowe są okresowo testowane poprzez odtworzenie w celu weryfikacji ich niezawodności.

5.2 Kontrole proceduralne

Certum wdraża kontrole proceduralne, aby zapewnić, że krytyczne operacje urzędu certyfikacji są wykonywane w sposób bezpieczny, zgodnie ze zdefiniowanymi rolami, odpowiedzialnościami i zasadami rozdziału obowiązków.

5.2.1 Trusted Roles

Role w Certum, które obejmują dostęp do Danych Certyfikatowych (Certificate Data), operacji kryptograficznych lub Procesów Zarządzania Certyfikatami (Certificate Management Processes), są wyznaczane jako Trusted Roles. Role te są ustanowione w celu współdzielenia odpowiedzialności, ograniczenia działań indywidualnych oraz zapewnienia, że żadna pojedyncza osoba nie może obejść środków bezpieczeństwa.

Trusted Roles obejmują między innymi:

- Personel kierowniczy - odpowiedzialny za usługi certyfikacyjne
- Administratorów systemów i operatorów systemów (System Administrator, System Operator) - odpowiedzialnych za instalację, konfigurację i utrzymanie systemów PKI
- Inspektorów bezpieczeństwa (Security Officers) - odpowiedzialnych za administrowanie i wdrażanie praktyk bezpieczeństwa
- Inspektorów audytu (Audit Officers) - odpowiedzialnych za przegląd i archiwizację audit logs oraz nadzór nad zgodnością
- Inspektorów rejestracji (Validation Officers) - odpowiedzialnych za weryfikację tożsamości oraz zatwierdzanie wydania lub unieważnienia certyfikatu

Trusted Roles są przydzielane zgodnie z zasadą najmniejszych uprawnień (least privilege) i wymagają odpowiedniego upoważnienia przed uzyskaniem dostępu do systemów lub obiektów.

5.2.2 Liczba osób wymagana do wykonania zadania

Wrażliwe operacje PKI są wykonywane pod kontrolą wieloosobową (multi-person control, dual control), aby zapewnić, że żadna pojedyncza osoba nie może obejść środków bezpieczeństwa.

Takie operacje wymagają udziału co najmniej dwóch upoważnionych osób pełniących wyznaczone Trusted Roles, w tym:

- Security Officer (lub równoważna rola kontrolna)
- Operator Hardware Security Module (HSM)
- Posiadacze współdzielonych sekretów (Shared Secret Holders), tam gdzie ma to zastosowanie

Obserwatorzy, tacy jak audytorzy, mogą być obecni podczas takich operacji.

5.2.3 Identyfikacja i uwierzytelnienie dla każdej roli

Cały personel działający w Trusted Roles podlega procedurom identyfikacji i uwierzytelnienia przed uzyskaniem dostępu do systemów lub obiektów.

Dostęp do Systemów Certum jest ograniczony do upoważnionego personelu i kontrolowany za pośrednictwem mechanizmów uwierzytelniania.

Konta użytkowników są jednoznacznie przypisane do osób, powiązane z określonymi rolami i ograniczone zgodnie z funkcjami wymaganymi dla tych ról.

5.2.4 Role wymagające rozdziału obowiązków

Certum egzekwuje rozdział obowiązków w celu ograniczenia ryzyka działań nieuprawnionych lub niewłaściwych.

Prawa dostępu są przyznawane ściśle zgodnie z przypisanymi rolami.

Zabronione są następujące połączenia ról:

- Rola Security Officer nie może być łączona z rolą System Administrator
- Personel odpowiedzialny za funkcje audytowe lub kontrolne nie może wykonywać ról operacyjnych związanych z wydawaniem certyfikatów, administracją systemami lub zarządzaniem bezpieczeństwem

Mechanizmy wylogowania po okresie bezczynności (inactivity time-outs) i polityki blokowania kont (account lockout policies) są egzekwowane, aby zapobiegać nieuprawnionemu dostępowi. Certum regularnie dokonuje przeglądu wszystkich kont systemowych i zapewnia cofnięcie praw dostępu w ciągu 24 godzin od ustania zatrudnienia danej osoby lub zmiany jej obowiązków służbowych.

5.3 Kontrole personelu

5.3.1 Wymagania dotyczące kwalifikacji, doświadczenia i poświadczeń

Personel pełniący Trusted Roles lub wykonujący inne funkcje związane z usługami certyfikacyjnymi musi posiadać odpowiednie kwalifikacje, doświadczenie i kompetencje właściwe dla swoich obowiązków.

Certum wymaga, aby taki personel spełniał następujące wymagania:

- Personel posiada co najmniej wykształcenie średnie oraz wiedzę, doświadczenie i kompetencje niezbędne do wykonywania konkretnych funkcji służbowych

- Personel jest zaangażowany na podstawie umów o pracę lub innych umów cywilnoprawnych, które określają przypisane role, prawa i obowiązki
- Personel kończy obowiązkowe szkolenia właściwe dla swoich obowiązków przed rozpoczęciem ich wykonywania, w tym szkolenia z bezpieczeństwa, ochrony danych osobowych i polityk prywatności
- Personel jest wolny od konfliktów interesów, które mogłyby wpływać na bezstronność usług certyfikacyjnych
- Personel działa zgodnie z politykami Certum wdrażającymi CA/Browser Forum Baseline Requirements oraz inne mające zastosowanie standardy branżowe

Dostęp do systemów i obiektów jest przyznawany wyłącznie po uzyskaniu odpowiedniego upoważnienia i przypisaniu odpowiedzialności.

5.3.2 Procedury weryfikacji personelu

Przed uzyskaniem dostępu do systemów lub obiektów związanych z usługami certyfikacyjnymi personel podlega procedurom weryfikacji, w zakresie dozwolonym przez mające zastosowanie przepisy prawa.

Zakres i intensywność takiej weryfikacji są współmierne do wrażliwości danej roli.

Weryfikacja personelu dla ról zaufanych (Trusted Roles) obejmuje:

- Potwierdzenie tożsamości danej osoby
- Sprawdzenie karalności
- Potwierdzenie poprzedniego zatrudnienia
- Weryfikację referencji i uprawnień zawodowych
- Weryfikację najwyższego poziomu wykształcenia istotnego dla danej roli
- W przypadku ograniczeń wynikających z przepisów prawa, Certum stosuje alternatywne metody weryfikacji zapewniające zasadniczo równoważny zakres informacji

Certum może odrzucić kandydata lub podjąć działania dyscyplinarne wobec pracownika pełniącego rolę zaufaną (Trusted Role), jeżeli zostanie ustalone, że dana osoba:

- Przekazała nieprawdziwe lub wprowadzające w błąd informacje podczas procesu weryfikacji
- Posiada istotnie negatywne lub niewiarygodne referencje zawodowe

W takich przypadkach dalsze działania są prowadzone zgodnie z wewnętrznymi procedurami bezpieczeństwa Asseco Data Systems S.A. oraz mającymi zastosowanie przepisami prawa.

5.3.3 Wymagania szkoleniowe

Personel wykonujący obowiązki w ramach usług certyfikacyjnych Certum lub procesów weryfikacji tożsamości jest zobowiązany ukończyć szkolenia odpowiednie do swoich ról.

Szkolenie obejmuje:

- Wszystkie właściwe dokumenty CP, CPS oraz CP/CPS
- Procedury i dokumentację właściwe dla danej roli
- Mechanizmy i procedury bezpieczeństwa
- Systemy i oprogramowanie wykorzystywane w procesach certyfikacyjnych
- Procedury reagowania na incydenty i sytuacje awaryjne
- Typowe zagrożenia dla procesu weryfikacji informacji, w tym phishing i techniki socjotechniczne (social engineering)
- Mające zastosowanie standardy branżowe, takie jak CA/Browser Forum Baseline Requirements
- Dodatkowe szkolenia dla personelu zaangażowanego w procesy weryfikacji tożsamości, odpowiednie do wymagań walidacji tożsamości

5.3.4 Częstotliwość i wymagania dotyczące szkoleń okresowych

Personel przechodzi okresowe szkolenia uzupełniające (retraining) w celu utrzymania i aktualizacji wiedzy oraz umiejętności.

Programy szkoleń okresowych są opracowywane tak, aby odzwierciedlać i obejmować wszelkie istotne zmiany w operacjach Certum PKI. Personel jest również informowany o nowych zdarzeniach w branży PKI, w tym o incydentach związanych z bezpieczeństwem u innych Dostawców Usług Zaufania (Trust Service Providers) oraz o dobrych praktykach zidentyfikowanych przez organizacje normalizacyjne.

5.3.5 Częstotliwość i sekwencja rotacji stanowisk

Brak postanowień.

5.3.6 Sankcje za działania nieuprawnione

Certum stosuje środki dyscyplinarne za działania nieuprawnione lub naruszenia mających zastosowanie polityk i procedur.

Środki takie są stosowane zgodnie z wewnętrznymi politykami personalnymi i mającym zastosowanie prawem i obejmują między innymi ograniczenie lub cofnięcie praw dostępu, zawieszenie oraz rozwiązanie stosunku pracy.

5.3.7 Wymagania dotyczące niezależnych wykonawców

Jeżeli niezależni wykonawcy są angażowani w działania związane z usługami certyfikacyjnymi, są oni zobowiązani do przestrzegania mających zastosowanie wymagań szkoleniowych, bezpieczeństwa i proceduralnych właściwych dla wykonywanych ról.

Niezależni wykonawcy nie są uprawnieni do wykonywania krytycznych operacji certyfikacyjnych, chyba że zostali wyraźnie zatwierdzeni i podlegają takim samym kontrolom jak personel Certum wykonujący porównywalne funkcje.

Personel zewnętrzny, który nie ukończył mających zastosowanie procedur weryfikacyjnych, może uzyskać dostęp do obiektów Certum wyłącznie pod nadzorem lub w asyście upoważnionego personelu Certum.

5.3.8 Dokumentacja przekazywana personelowi

Personelowi przekazywana jest dokumentacja niezbędna do bezpiecznego i skutecznego wykonywania obowiązków.

Obejmuje ona polityki, procedury, instrukcje specyficzne dla roli oraz inną właściwą dokumentację dotyczącą usług certyfikacyjnych.

5.4 Procedury rejestrowania zdarzeń

Certum wdraża procedury rejestrowania zdarzeń (audit logging) w celu rejestrowania, monitorowania i analizowania zdarzeń istotnych dla bezpieczeństwa danych certyfikatów i procesów zarządzania certyfikatami.

Rejestry zdarzeń (audit logs) są wykorzystywane do wspierania wykrywania działań nieuprawnionych, problemów operacyjnych i incydentów bezpieczeństwa.

5.4.1 Typy rejestrowanych zdarzeń

Certum rejestruje zdarzenia związane z działaniem i bezpieczeństwem usług certyfikacyjnych, w tym między innymi:

- Dostęp do systemów wspierających operacje certyfikacyjne
- Zdarzenia systemowe oraz zdarzenia związane z bezpieczeństwem
- Działania administracyjne wykonywane przez upoważniony personel
- Operacje cyklu życia certyfikatu (w tym wydanie i unieważnienie)
- Zmiany konfiguracji systemów, jeżeli mają znaczenie dla usług certyfikacyjnych

5.4.2 Częstotliwość przeglądu rejestrów zdarzeń

Rejestry zdarzeń (audit logs) są przeglądane w sposób regularny oraz każdorazowo w przypadku wykrycia anomalii, incydentów lub potrzeb operacyjnych.

5.4.3 Okres przechowywania rejestrów zdarzeń

Certum przechowuje rejestry zdarzeń (audit logs) zgodnie z następującymi zasadami:

- Zdarzenia dotyczące kluczy CA oraz cyklu życia certyfikatów – przez co najmniej 2 lata od momentu zniszczenia klucza prywatnego CA lub unieważnienia albo wygaśnięcia końcowego certyfikatu CA powiązanego z tym kluczem

- Zdarzenia dotyczące zarządzania cyklem życia certyfikatów Subskrybentów – przez co najmniej 2 lata od momentu unieważnienia lub wygaśnięcia certyfikatu Subskrybenta
- Rejestry zdarzeń bezpieczeństwa – przez co najmniej 2 lata od momentu wystąpienia zdarzenia

5.4.4 Ochrona rejestrów zdarzeń

Rejestry zdarzeń (audit logs) są chronione przed nieuprawnionym dostępem, modyfikacją i usunięciem.

Dostęp do rejestrów zdarzeń (audit logs) jest ograniczony do upoważnionego personelu.

5.4.5 Procedury tworzenia kopii zapasowych rejestrów zdarzeń

Rejestry zdarzeń (audit logs) są objęte procesami tworzenia kopii zapasowych w celu zapewnienia ich dostępności w przypadku awarii systemu lub utraty danych.

5.4.6 System gromadzenia rejestrów zdarzeń (wewnętrzny vs. zewnętrzny)

Rejestry zdarzeń (audit logs) są gromadzone i utrzymywane z wykorzystaniem systemów zarządzanych przez Certum.

5.4.7 Powiadamianie podmiotu powodującego zdarzenie

Brak postanowień.

5.4.8 Oceny podatności

Certum wdraża proces zarządzania podatnościami w celu identyfikacji, oceny i usuwania podatności bezpieczeństwa wpływających na systemy wspierające usługi certyfikacyjne.

Oceny podatności są przeprowadzane corocznie oraz w odpowiedzi na istotne zmiany systemów lub infrastruktury.

Oceny te obejmują skanowanie podatności, przeglądy konfiguracji oraz inne działania oceny bezpieczeństwa odpowiednie dla danych systemów.

Zidentyfikowane podatności są oceniane i usuwane zgodnie z przypisanym im ryzykiem i mającymi zastosowanie procedurami.

5.5 Archiwizacja danych

Certum utrzymuje dane związane z usługami certyfikacyjnymi w celu wspierania wymagań operacyjnych, bezpieczeństwa, audytowych i prawnych.

Zarchiwizowane dane są przechowywane, chronione i udostępniane zgodnie z mającymi zastosowanie politykami i wymaganiami regulacyjnymi.

5.5.1 Rodzaje archiwizowanych danych

Certum archiwizuje zapisy istotne dla usług certyfikacyjnych, w tym między innymi:

- Dane wniosku o certyfikat oraz dane rejestracyjne
- Informacje dotyczące weryfikacji tożsamości
- Zdarzenia związane z cyklem życia certyfikatu (w tym wydanie i unieważnienie)
- Rejestry zdarzeń (audit logs)
- Rejestry systemowe oraz rejestry związane z bezpieczeństwem istotne dla operacji certyfikacyjnych
- Umowy oraz dokumentację związaną z usługami certyfikacyjnymi

5.5.2 Okres przechowywania archiwum

Wszystkie dane opisane w Sekcji 5.5.1 są przechowywane przez co najmniej 2 lata.

5.5.3 Ochrona archiwum

Zarchiwizowane dane są chronione przed nieuprawnionym dostępem, modyfikacją i zniszczeniem.

Dostęp do zarchiwizowanych zapisów jest ograniczony do upoważnionego personelu.

5.5.4 Procedury tworzenia kopii zapasowych archiwum

Zarchiwizowane dane podlegają procedurom tworzenia kopii zapasowych w celu zapewnienia ich dostępności i integralności w przypadku utraty danych lub awarii systemu.

5.5.5 Wymagania dotyczące znakowania czasem

W stosownych przypadkach dane są opatrywane informacją o dacie i czasie w celu zapewnienia ich integralności oraz możliwości śledzenia.

5.5.6 System archiwizacji (wewnętrzny lub zewnętrzny)

Brak postanowień.

5.5.7 Procedury uzyskiwania i weryfikacji informacji archiwalnych

Brak postanowień.

5.6 Zmiana klucza

Certum wykorzystuje nowo wygenerowane pary kluczy (key pairs) dla nowo wydawanych certyfikatów CA i Subskrybentów.

5.7 Kompromitacja i odtwarzanie po awarii

Certum utrzymuje procedury wewnętrzne obejmujące Plan ciągłości działania (Business Continuity Plan, BCP) oraz Plan odtwarzania po awarii (Disaster Recovery Plan, DRP) w celu

zapewnienia odtworzenia gwarantowanych poziomów usług w przypadku okoliczności wyjątkowych, takich jak klęski żywiołowe lub zdarzenia katastrofalne.

5.7.1 Procedury obsługi incydentów i kompromitacji

Certum utrzymuje procedury obsługi incydentów oraz reagowania na zagrożenia bezpieczeństwa jako część Planu ciągłości działania (BCP).

BCP określa warunki jego uruchomienia, procedury reagowania awaryjnego, procedury ciągłości działania oraz procedury przywracania usług certyfikacyjnych. Obejmuje również wymagania dotyczące świadomości personelu, ról i odpowiedzialności oraz regularnego przeglądu i utrzymania planu.

Certum testuje skuteczność BCP co najmniej raz w roku oraz każdorazowo po wprowadzeniu istotnych zmian.

Certum utrzymuje plan masowego unieważnienia certyfikatów (Mass Revocation Plan), który określa działania podejmowane w przypadku konieczności szybkiego, skoordynowanego i bezpiecznego unieważnienia znacznej liczby certyfikatów.

Plan masowego unieważnienia certyfikatów obejmuje:

- Kryteria uruchomienia planu
- Role i odpowiedzialności personelu
- Wymagania szkoleniowe
- Procedury powiadamiania Subskrybentów i stron ufających
- Docelowe ramy czasowe rozpoczęcia i zakończenia czynności unieważnienia

Skuteczność planu masowego unieważnienia certyfikatów jest testowana w ramach testów BCP oraz po istotnych zmianach procesowych.

BCP obejmuje również:

- Cele odtworzeniowe dla krytycznych procesów certyfikacyjnych
- Tworzenie kopii zapasowych oraz odtwarzanie krytycznych systemów i danych
- Wymagania dotyczące bezpiecznego przechowywania materiałów kryptograficznych w lokalizacjach zapasowych
- Geograficzne rozdzielenie lokalizacji podstawowych i zapasowych
- Procedury zabezpieczania zasobów w trakcie zakłóceń
- Dopuszczalne poziomy niedostępności oraz warunki odtworzenia systemów

5.7.2 Uszkodzenie zasobów obliczeniowych, oprogramowania i/lub danych

W przypadku uszkodzenia zasobów obliczeniowych, oprogramowania lub danych Certum wdraża procedury identyfikacji i oceny skali incydentu oraz jego wpływu na usługi certyfikacyjne.

Podejmowane są odpowiednie działania mające na celu ograniczenie problemu i przywrócenie dotkniętych systemów i danych z zaufanych źródeł, w tym z kopii zapasowych oraz systemów redundantnych lub alternatywnych.

Przywrócone systemy i dane są weryfikowane przed wznowieniem normalnej pracy.

Jeżeli uszkodzenie wpływa na procesy certyfikacyjne lub wydane certyfikaty, Certum może podjąć odpowiednie działania, w tym unieważnienie dotkniętych certyfikatów i wydanie certyfikatów zastępczych.

Tam, gdzie jest to konieczne, uruchamiane są procedury zdefiniowane w BCP i Disaster Recovery Plan.

5.7.3 Procedury kompromitacji klucza prywatnego podmiotu

Certum utrzymuje procedury reagowania na kompromitację lub podejrzenie kompromitacji kluczy prywatnych związanych z usługami certyfikacyjnymi.

W przypadku takiej kompromitacji Certum wdraża działania odpowiednie do charakteru i zakresu incydentu, które mogą obejmować:

- Natychmiastowe zaprzestanie używania skompromitowanego klucza prywatnego
- Unieważnienie certyfikatów powiązanych ze skompromitowanym kluczem
- Powiadomienie stron, których to dotyczy, w tym Subskrybentów i stron ufających, stosownie do wymagań
- Wygenerowanie i wdrożenie zastępczych par kluczy i certyfikatów
- Wdrożenie dodatkowych środków ograniczających wpływ kompromitacji

Tam, gdzie ma to zastosowanie, Certum podejmuje również działania w celu przywrócenia bezpiecznego działania usług certyfikacyjnych i ponownego ustanowienia zaufania do wydanych certyfikatów.

5.7.4 Zdolności ciągłości działania po katastrofie

Certum utrzymuje zdolności ciągłości działania i odtwarzania po awarii w celu zapewnienia dostępności i ciągłości usług certyfikacyjnych po katastrofie lub poważnym zakłóceniu.

Zdolności te obejmują wykorzystanie systemów zapasowych, obiektów przetwarzania redundantnych lub alternatywnych oraz procedur przywracania systemów i danych krytycznych.

Certum wdraża środki ochrony systemów certyfikacyjnych i materiałów wrażliwych przed utratą, nieuprawnionym dostępem lub dalszym uszkodzeniem w trakcie i po zdarzeniu zakłócającym.

Procedury odtworzeniowe są zaprojektowane tak, aby przywracać usługi certyfikacyjne w sposób kontrolowany i bezpieczny, w tym poprzez odtworzenie systemów, danych i materiałów kryptograficznych.

Certum przeprowadza okresowe testy i przeglądy swoich rozwiązań w zakresie ciągłości działania i odtwarzania po awarii w celu zapewnienia ich skuteczności.

5.8 Zakończenie działania CA lub RA

Gdy konieczne jest zakończenie działania CA Certum, Certum zobowiązuje się minimalizować wpływ takiego zakończenia na Subskrybentów i strony ufające.

Przed zakończeniem świadczenia swoich usług certyfikacyjnych:

- Certum powiadamia wszystkich Subskrybentów posiadających aktywne certyfikaty co najmniej 90 dni przed planowaną datą zakończenia pocztą elektroniczną oraz za pośrednictwem swojej oficjalnej strony internetowej, aby umożliwić im przejście do innego Dostawcy Usług Zaufania (Trust Service Provider)
- Certum dokłada uzasadnionych handlowo starań, aby zminimalizować zakłócenia, oraz zapewnia rekompensatę opłat za certyfikaty proporcjonalnie do niewykorzystanego okresu ważności, zgodnie z mającymi zastosowanie umowami o świadczenie usług i politykami wewnętrznymi
- W dniu ostatecznego zakończenia Certum unieważnia wszystkie certyfikaty, które pozostają ważne i niewygasłe, wydaje końcową CRL z polem nextUpdate wskazującym koniec działalności oraz unieważnia własne certyfikaty CA
- Certum niszczy wszystkie klucze prywatne

W celu utrzymania ciągłości działania Certum jest uprawnione do przeniesienia swoich obowiązków na podmiot sukcesora.

6. TECHNICZNE KONTROLE BEZPIECZEŃSTWA

6.1 Generowanie i instalacja pary kluczy

6.1.1 Generowanie pary kluczy

Pary kluczy dla CA Certum są generowane w bezpiecznym środowisku z wykorzystaniem Hardware Security Modules (HSMs), zgodnie z Sekcją 6.2.1.

Proces generowania jest przeprowadzany przez personel pełniący Trusted Roles podczas formalnej ceremonii generowania kluczy (key generation ceremony) zgodnie z udokumentowanym scenariuszem.

W szczególności podczas generowania pary kluczy CA przeznaczonej dla certyfikatu Root CA procedura jest obserwowana przez niezależnego audytora zewnętrznego. Certum utrzymuje audytowalne dowody, że ceremonia była prowadzona zgodnie z niniejszym CP/CPS oraz zapewniała integralność i poufność par kluczy.

Pary kluczy Subskrybenta są generowane przez Subskrybenta.

6.1.2 Dostarczenie klucza prywatnego Subskrybentowi

Certum nie generuje kluczy prywatnych Subskrybenta.

6.1.3 Dostarczenie klucza publicznego wystawcy certyfikatu

Subskrybenci mogą dostarczać swój klucz publiczny do Certum w formie Certificate Signing Request (CSR) w formacie PKCS#10. Zgłoszenie jest składane elektronicznie za pośrednictwem Systemów Certum.

6.1.4 Dostarczenie klucza publicznego CA stronom ufającym

Klucze publiczne CA Certum są udostępniane z Repozytorium Certum (zob. Sekcja 2.1).

Klucze publiczne CA Certum są również udostępniane jako kotwice zaufania (trust anchors) w przeglądarkach, systemach operacyjnych lub innych zaufanych repozytoriach głównych (trusted root stores) oprogramowania.

6.1.5 Rozmiary kluczy

Następujące algorytmy i długości kluczy są dopuszczalne dla Root CAs Certum, Subordinate CAs oraz certyfikatów Subskrybentów:

Certum Root CA

- RSA: 2048b, 3072b, 4096b
- ECDSA: NIST P-256, P-384

Certum Subordinate CA

- RSA: 2048b, 3072b, 4096b

- ECDSA: NIST P-256, P-384

Certyfikaty Subskrybentów Certum

- RSA: 2048b, 3072b, 4096b
- ECDSA: NIST P-256, P-384

6.1.6 Generowanie parametrów klucza publicznego i kontrola jakości

Dla kluczy RSA wymagane są następujące dodatkowe kryteria (na podstawie Sekcji 5.3.3, NIST SP 800-89):

- Wykładnik publiczny musi być liczbą nieparzystą równą 3 lub większą
- Wykładnik publiczny mieści się w zakresie od 2^16 + 1 do 2^256 - 1
- Moduł jest liczbą nieparzystą
- Moduł nie jest potęgą liczby pierwszej, oraz
- Moduł nie ma dzielników mniejszych niż 752

Dla kluczy ECDSA wymagane są następujące dodatkowe kryteria (na podstawie Sekcji 5.6.2.3.2 i 5.6.2.3.3 dokumentu NIST SP 800-56A, Revision 2). Poprawność wszystkich kluczy ECDSA jest weryfikowana przy użyciu jednej z następujących metod: - ECC Full Public Key Validation Routine - ECC Partial Public Key Validation Routine

6.1.7 Cele użycia kluczy (zgodnie z polem X.509 v3 key usage)

Certum przypisuje użycia kluczy certyfikatu zgodnie z ich zamierzonym przeznaczeniem poprzez pole X.509 v3 Key Usage.

Klucze prywatne odpowiadające certyfikatom Root CA Certum nie mogą być używane do podpisywania certyfikatów, z wyjątkiem następujących przypadków:

- Certyfikatów self-signed reprezentujących sam Root CA
- Certyfikatów dla Subordinate CAs oraz certyfikatów cross-certificate
- Certyfikatów do celów infrastrukturalnych (wewnętrzne certyfikaty urządzeń operacyjnych CA)
- Certyfikatów do weryfikacji odpowiedzi OCSP

6.2 Ochrona klucza prywatnego i kontrole inżynieryjne modułów kryptograficznych

Certum wdraża fizyczne i logiczne zabezpieczenia w celu zapobiegania nieuprawnionemu wydawaniu certyfikatów. Ochrona klucza prywatnego CA poza zwalidowanym systemem lub urządzeniem określonym w Sekcji 6.2.7 polega na bezpieczeństwie fizycznym, szyfrowaniu lub połączeniu obu tych środków, wdrożonych w sposób zapobiegający ujawnieniu klucza prywatnego.

Certum szyfruje swój klucz prywatny przy użyciu algorytmu i długości klucza, które zgodnie ze stanem wiedzy technicznej są zdolne wytrzymać ataki kryptoanalityczne przez pozostały okres życia zaszyfrowanego klucza lub jego części.

6.2.1 Standardy i kontrole modułów kryptograficznych

Wszystkie Systemy Certum podpisujące certyfikaty, CRL lub generujące odpowiedzi OCSP wykorzystują specyfikacje bezpieczeństwa FIPS 140-2 Level 3 lub wyższe albo Common Criteria EAL4+.

Klucze prywatne CA Certum są utrzymywane w fizycznie bezpiecznych środowiskach i nigdy nie są przechowywane w postaci niezaszyfrowanej poza HSM.

6.2.2 Wieloosobowa kontrola klucza prywatnego (n z m)

Wszelki dostęp do kluczy prywatnych CA Certum, zarówno fizyczny, jak i logiczny, wymaga udziału wielu osób pełniących Trusted Roles. Dotyczy to wszystkich instancji kluczy prywatnych, w tym kopii produkcyjnych i zapasowych, zarówno na miejscu, jak i poza lokalizacją podstawową.

6.2.3 Escrow klucza prywatnego

Klucze prywatne CA Certum nie są objęte escrow.

6.2.4 Kopia zapasowa klucza prywatnego

Kopie zapasowe kluczy prywatnych CA Certum są przechowywane w bezpieczny sposób zgodnie z mającą zastosowanie polityką backupową Certum.

Klucze prywatne CA Certum są archiwizowane w kopiach zapasowych, przechowywane i odzyskiwane wyłącznie przez personel pełniący Trusted Roles z zastosowaniem co najmniej dual control w fizycznie zabezpieczonym środowisku.

6.2.5 Archiwizacja klucza prywatnego

Klucze prywatne należące do Certum nie są archiwizowane przez podmioty inne niż Certum.

6.2.6 Przenoszenie klucza prywatnego do modułu kryptograficznego lub z niego

Klucze prywatne CA Certum są generowane w HSM i eksportowane wyłącznie do celów redundancji lub kopii zapasowej. Przy eksporcie klucze są szyfrowane przed opuszczeniem HSM i odszyfrowywane wyłącznie wewnątrz docelowego HSM, przy użyciu procesu, który zawsze wymaga kontroli wieloosobowej.

Wszelkie transfery kluczy prywatnych CA Certum do modułu kryptograficznego lub z niego są wykonywane zgodnie z procedurami zdefiniowanymi przez producenta danego modułu.

6.2.7 Przechowywanie klucza prywatnego w module kryptograficznym

Certum przechowuje klucze prywatne CA na sprzętowym module kryptograficznym zgodnie z Sekcją 6.2.1.

6.2.8 Metoda aktywacji klucza prywatnego

Certum aktywuje klucze prywatne CA zgodnie z instrukcjami i dokumentacją dostarczonymi przez producenta sprzętowego modułu bezpieczeństwa.

6.2.9 Metoda dezaktywacji klucza prywatnego

Certum dezaktywuje klucze prywatne CA zgodnie z instrukcjami i dokumentacją dostarczonymi przez producenta sprzętowego modułu bezpieczeństwa.

6.2.10 Metoda niszczenia klucza prywatnego

Certum niszczy klucze prywatne CA zgodnie z instrukcjami i dokumentacją dostarczonymi przez producenta sprzętowego modułu bezpieczeństwa.

6.2.11 Ocena modułu kryptograficznego

Zob. Sekcja 6.2.1.

6.3 Inne aspekty zarządzania parami kluczy

6.3.1 Archiwizacja klucza publicznego

Zob. Sekcja 5.5.

6.3.2 Okresy operacyjne certyfikatu i okresy użycia pary kluczy

Pary kluczy Root CA i Subordinate CA Certum mają okres życia odpowiadający ich certyfikatom:

- Maksymalny okres ważności Root CA wynosi 25 lat
- Maksymalny okres ważności Subordinate CA wynosi 15 lat

Typ	Maksymalny okres użycia klucza	Maksymalny okres ważności certyfikatu
Certum Root CA	25 lat	25 lat
Certum Subordinate CA	15 lat	15 lat

Maksymalny okres ważności certyfikatów TLS Subskrybentów zależy od daty ich wydania:

- Maksymalny okres ważności certyfikatów Subskrybenta wydanych przed 15 marca 2026 r. wynosi 398 dni;
- Maksymalny okres ważności certyfikatów Subskrybenta wydanych 15 marca 2026 r. lub później i przed 15 marca 2027 r. wynosi 200 dni;

- Maksymalny okres ważności certyfikatów Subskrybenta wydanych 15 marca 2027 r. lub później i przed 15 marca 2029 r. wynosi 100 dni;
- Maksymalny okres ważności certyfikatów Subskrybenta wydanych 15 marca 2029 r. lub później wynosi 47 dni.

Certyfikat Subskrybenta wydany w dniu lub po dniu	Certyfikat wydany przed dniem	Maksymalny okres ważności
N/A	2026-03-15	398 dni
2026-03-15	2027-03-15	200 dni
2027-03-15	2029-03-15	100 dni
2029-03-15	N/A	47 dni

6.4 Dane aktywacyjne

6.4.1 Generowanie i instalacja danych aktywacyjnych

Dane aktywacyjne wykorzystywane do aktywacji kluczy prywatnych CA Certum są generowane podczas ceremonii klucza opisanej w Sekcji 6.1.1. Dane aktywacyjne są przekazywane personelowi pełniącemu Trusted Role w celu ich użycia lub przechowywania.

6.4.2 Ochrona danych aktywacyjnych

Dane aktywacyjne są chronione przed nieuprawnionym ujawnieniem zarówno środkami fizycznymi, jak i logicznymi.

6.4.3 Inne aspekty danych aktywacyjnych

Brak postanowień.

6.5 Kontrole bezpieczeństwa komputerowego

6.5.1 Szczegółowe techniczne wymagania bezpieczeństwa komputerowego

Systemy Certum są chronione w celu zapobiegania nieuprawnionemu dostępowi lub modyfikacji oprogramowania CA i danych. Dla dostępu do systemu stosowane jest uwierzytelnianie wieloskładnikowe (multifactor authentication). Poprawki bezpieczeństwa są wdrażane terminowo, a skanowania podatności są wykonywane regularnie.

6.5.2 Ocena bezpieczeństwa komputerowego

Brak postanowień.

6.6 Kontrole techniczne cyklu życia

6.6.1 Kontrole rozwoju systemu

Certum utrzymuje udokumentowane procedury regulujące pozyskiwanie i rozwój swoich systemów CA, zapewniając, że wszystkie komponenty spełniają wymagania

bezpieczeństwa, wydajności i niezawodności. Dedykowany sprzęt i oprogramowanie są utrzymywane wyłącznie do działania funkcji CA.

Certum wykorzystuje oprogramowanie, które przeszło formalne testy w celu zapewnienia jego przydatności i adekwatności do celu. Sprzęt jest nabywany w ramach kontrolowanego procesu zakupowego wykorzystującego renomowanych dostawców branżowych. Wszystkie dostawy sprzętu są odbierane przez osoby pełniące Trusted Roles i kontrolowane pod kątem oznak manipulacji. Hardware Security Modules (HSMs) są dostarczane w opakowaniach z zabezpieczeniem przed naruszeniem (tamper-evident packaging), a numery seryjne toreb zabezpieczających są weryfikowane z dostawcą przy odbiorze. Każdy HSM jest testowany zgodnie z ustalonymi procedurami przed dopuszczeniem do użycia produkcyjnego.

Certum utrzymuje dedykowane środowisko testowe CA, logicznie i fizycznie oddzielone od środowiska produkcyjnego. Platforma testowa jest zaprojektowana tak, aby możliwie najwierniej odtwarzać środowisko produkcyjne, bez dostępu do kluczy prywatnych CA używanych dla zaufanych certyfikatów. Środowisko to wspiera kompleksowe testowanie oprogramowania i systemów przed wdrożeniem na produkcję, zapewniając bezpieczeństwo i stabilność.

Certum ustanowiło i egzekwuje formalne polityki i procedury kontroli zmian, które muszą być stosowane przy każdej modyfikacji systemów CA. Wszystkie proponowane zmiany muszą być przeglądane i zatwierdzane przez osoby pełniące Trusted Roles, niezależne od osoby wnioskującej o zmianę. Każdy wniosek o zmianę wraz z powiązanymi przeglądami i zatwierdzeniami jest w pełni dokumentowany.

Gdy Certum rozwija oprogramowanie do wykorzystania w operacjach CA, rozwój odbywa się zgodnie ze zdefiniowanymi politykami i metodykami promującymi jakość, bezpieczeństwo i integralność oprogramowania. Praktyki te obejmują peer review, ustrukturyzowane testowanie i dokumentowanie wszystkich modyfikacji kodu.

W odniesieniu do oprogramowania do lintingu opracowanego przez strony trzecie Certum monitoruje pojawianie się nowych wersji takiego oprogramowania i planuje wdrożenie aktualizacji w ciągu trzech miesięcy od ich publicznego wydania. Certum może wykonywać linting na zbiorze swoich niewygasłych i nieunieważnionych certyfikatów Subskrybentów przy każdej aktualizacji oprogramowania do lintingu w celu weryfikacji dalszej zgodności z mającymi zastosowanie profilami certyfikatów i politykami wydawania.

6.6.2 Kontrole zarządzania bezpieczeństwem

Aktualna konfiguracja Systemu Certum, jak również wszystkie modyfikacje i aktualizacje, jest rejestrowana i podlega formalnym procedurom kontroli zmian. Kontrole zarządzania konfiguracją wdrożone w Systemie Certum zapewniają ciągłą weryfikację integralności aplikacji i wersji.

6.6.3 Kontrole bezpieczeństwa cyklu życia

Brak postanowień.

6.7 Kontrole bezpieczeństwa sieciowego

Certum przestrzega CA/Browser Forum Network and Certificate System Security Requirements.

Certum wdraża odpowiednie kontrole i zabezpieczenia bezpieczeństwa sieciowego zaprojektowane w celu zapobiegania nieuprawnionemu dostępowi do swoich systemów CA.

Architektura sieciowa Certum ma charakter wielowarstwowy i segmentowany. Firewalle są konfigurowane zgodnie z polityką najmniejszych uprawnień (least-privilege), opartą na allowlist, dopuszczającą wyłącznie niezbędny ruch sieciowy wszędzie tam, gdzie jest to wykonalne.

Klucze prywatne Root CA Certum są utrzymywane offline w bezpiecznym i kontrolowanym środowisku.

Certum przyjmuje następujące terminy usuwania podatności:

- Wysoki priorytet w ciągu 96 godzin
- Średni priorytet w ciągu 7 dni
- Niski priorytet w ciągu 30 dni

6.8 Znakowanie czasem

Certum zapewnia, że źródła czasu wykorzystywane we wszystkich operacjach znakowania czasem pozostają dokładne, niezawodne i weryfikowalne za pośrednictwem NTP (Network Time Protocol).

7. PROFILE CERTYFIKATÓW, CRL I OCSP

7.1 Profil certyfikatu

Certyfikaty Certum są wydawane zgodnie z RFC 5280. Rozszerzenia certyfikatów, ich ustawienia krytyczności oraz identyfikatory obiektów algorytmów kryptograficznych są wdrażane zgodnie ze specyfikacjami określonymi w RFC 5280. Certum jest zgodne z wymaganiami technicznymi określonymi w Sekcji 6.1.5 i Sekcji 6.1.6 niniejszego dokumentu.

W przypadku konfliktu pomiędzy postanowieniami RFC 5280 a mającymi zastosowanie wymaganiami CA/Browser Forum, Certum przestrzega wymagań CA/Browser Forum.

Profil certyfikatu Root CA

Pole lub rozszerzenie	Wartość
`version`	Zob. Sekcja 7.1.1
`serialNumber`	Liczba niesekwencyjna większa od zera (0) i mniejsza niż 2^{159}, zawierająca co najmniej 64 bity wyjścia z CSPRNG
`issuer`	Zawiera `countryName`, `organizationName` i `commonName`
`validity`	Zob. Sekcja 6.3.2
`subject`	Taki sam jak DN wystawcy (Issuer DN)
`subjectPublicKeyInfo`	Zob. Sekcja 6.1.5, Sekcja 6.1.6 oraz Sekcja 7.1.3
`signatureAlgorithm`	Zob. Sekcja 6.1.5, Sekcja 6.1.6 oraz Sekcja 7.1.3
`basicConstraints` (critical)	`cA=True`
`keyUsage` (critical)	`keyCertSign`, `cRLSign`
`subjectKeyIdentifier`	Skrót SHA-1 z `subjectPublicKeyInfo`

Uwaga: Stare certyfikaty Root CA Certum nie są zgodne z obecnym profilem certyfikatu Root CA, ponieważ pochodzą sprzed obecnych standardów.

Profil certyfikatu Subordinate CA

Pole lub rozszerzenie	Wartość
`version`	Zob. Sekcja 7.1.1
`serialNumber`	Liczba niesekwencyjna większa od zera (0) i mniejsza niż 2^{159}, zawierająca co najmniej 64 bity wyjścia z CSPRNG
`issuer`	Zawiera `countryName`, `organizationName` i `commonName`
`validity`	Zob. Sekcja 6.3.2
`subject`	Taki sam jak DN wystawcy (Issuer DN)
`subjectPublicKeyInfo`	Zob. Sekcja 6.1.5, Sekcja 6.1.6 oraz Sekcja 7.1.3
`signatureAlgorithm`	Zob. Sekcja 6.1.5, Sekcja 6.1.6 oraz Sekcja 7.1.3

Pole lub rozszerzenie	Wartość
authorityKeyIdentifier	Identyczne z polem subjectKeyIdentifier issuing CA
basicConstraints (critical)	cA=True, pathLenConstraint (opcjonalnie)
certificatePolicies	anyPolicy
crlDistributionPoints	HTTP URL usługi CRL issuing CA dla tego certyfikatu
keyUsage (critical)	keyCertSign, cRLSign
subjectKeyIdentifier	Skrót SHA-1 z subjectPublicKeyInfo
extKeyUsage	id-kp-serverAuth, id-kp-clientAuth (opcjonalnie)
authorityInformationAccess	HTTP URL respondera OCSP issuing CA oraz HTTP URL certyfikatu issuing CA

Uwaga 1: Stare certyfikaty Subordinate CA Certum nie są zgodne z obecnym profilem certyfikatu Root CA, ponieważ pochodzą sprzed obecnych standardów.

Uwaga 2: Profil certyfikatu cross-certified Subordinate CA, który jest szczególnym typem certyfikatu Subordinate CA, jest wydawany zgodnie z TLS BR Sekcja 7.1.2.2.

Certyfikat końcowy serwera TLS (DV)

Pole lub rozszerzenie	Wartość
version	Zob. Sekcja 7.1.1
serialNumber	Liczba niesekwencyjna większa od zera (0) i mniejsza niż 2^{159}, zawierająca co najmniej 64 bity wyjścia z CSPRNG
issuer	Wywiedzione z issuing CA
validity	Zob. Sekcja 6.3.2
subject	Zawiera commonName
subjectPublicKeyInfo	Zob. Sekcja 6.1.5, Sekcja 6.1.6 oraz Sekcja 7.1.3
signatureAlgorithm	Zob. Sekcja 6.1.5, Sekcja 6.1.6 oraz Sekcja 7.1.3
authorityInformationAccess	HTTP URL respondera OCSP issuing CA oraz HTTP URL certyfikatu issuing CA
authorityKeyIdentifier	Identyczne z polem subjectKeyIdentifier issuing CA
certificatePolicies	2.23.140.1.2.1, 1.2.616.1.113527.2.101.1 (opcjonalnie)
extKeyUsage	id-kp-serverAuth, id-kp-clientAuth (opcjonalnie)
subjectAltName	Sekwencja jednej lub większej liczby dNSNames lub ipAddresses.
keyUsage (critical)	digitalSignature, keyEncipherment (opcjonalnie)
basicConstraints (critical)	cA=False
crlDistributionPoints	HTTP URL usługi CRL issuing CA dla tego certyfikatu
Signed Certificate Timestamp	Zgodnie z RFC 6962.

Pole lub rozszerzenie	Wartość
List	
`subjectKeyIdentifier`	Skrót SHA-1 z `subjectPublicKeyInfo` (opcjonalnie)
Precertificate poison	Zgodnie z RFC 6962 (wyłącznie w precertyfikatach)

Certyfikat końcowy serwera TLS (OV)

Pole lub rozszerzenie	Wartość
`version`	Zob. Sekcja 7.1.1
`serialNumber`	Liczba niesekwencyjna większa od zera (0) i mniejsza niż 2^{159}, zawierająca co najmniej 64 bity wyjścia z CSPRNG.
`issuer`	Wywiedzione z issuing CA
`validity`	Zob. Sekcja 6.3.2
`subject`	Zawiera `countryName`, `stateOrProvinceName` (opcjonalnie), `localityName` (opcjonalnie), `organizationName`, `commonName`
`subjectPublicKeyInfo`	Zob. Sekcja 6.1.5, Sekcja 6.1.6 oraz Sekcja 7.1.3
`signatureAlgorithm`	Zob. Sekcja 6.1.5, Sekcja 6.1.6 oraz Sekcja 7.1.3
`authorityInformationAccess`	HTTP URL respondera OCSP issuing CA oraz HTTP URL certyfikatu issuing CA
`authorityKeyIdentifier`	Identyczne z polem `subjectKeyIdentifier` issuing CA
`certificatePolicies`	2.23.140.1.2.2, 1.2.616.1.113527.2.101.2 (opcjonalnie)
`extKeyUsage`	`id-kp-serverAuth`, `id-kp-clientAuth` (opcjonalnie)
`subjectAltName`	Sekwencja jednej lub większej liczby `dNSNames` lub `ipAddresses`
`keyUsage` (critical)	`digitalSignature`, `keyEncipherment` (opcjonalnie)
`basicConstraints` (critical)	`cA=False`
`crlDistributionPoints`	HTTP URL usługi CRL issuing CA dla tego certyfikatu
Signed Certificate Timestamp List	Zgodnie z RFC 6962.
`subjectKeyIdentifier`	Skrót SHA-1 z `subjectPublicKeyInfo` (opcjonalnie)
Precertificate poison	Zgodnie z RFC 6962 (wyłącznie w precertyfikatach)

Certyfikat końcowy serwera TLS (EV)

Pole lub rozszerzenie	Wartość
`version`	Zob. Sekcja 7.1.1
`serialNumber`	Liczba niesekwencyjna większa od zera (0) i mniejsza niż 2^{159}, zawierająca co najmniej 64 bity wyjścia z CSPRNG

Pole lub rozszerzenie	Wartość
issuer	Wywiedzione z issuing CA
validity	Zob. Sekcja 6.3.2
subject	Zawiera businessCategory, jurisdictionCountryName, jurisdictionStateOrProvinceName(opcjonalnie), jurisdictionLocalityName(opcjonalnie), serialNumber, countryName, stateOrProvinceName (opcjonalnie), localityName (opcjonalnie), postalCode (opcjonalnie), streetAddress (opcjonalnie), organizationName, commonName
subjectPublicKeyInfo	Zob. Sekcja 6.1.5, Sekcja 6.1.6 oraz Sekcja 7.1.3
signatureAlgorithm	Zob. Sekcja 6.1.5, Sekcja 6.1.6 oraz Sekcja 7.1.3
authorityInformationAccess	HTTP URL respondera OCSP issuing CA oraz HTTP URL certyfikatu issuing CA.
authorityKeyIdentifier	Identyczne z polem subjectKeyIdentifier issuing CA
certificatePolicies	2.23.140.1.1, 1.2.616.1.113527.2.101.3
extKeyUsage	id-kp-serverAuth, id-kp-clientAuth (opcjonalnie)
subjectAltName	Sekwencja jednej lub większej liczby dNSNames lub ipAddresses
keyUsage (critical)	digitalSignature, keyEncipherment (opcjonalnie)
basicConstraints (critical)	cA=False
crlDistributionPoints	HTTP URL usługi CRL issuing CA dla tego certyfikatu.
Signed Certificate Timestamp List	Zgodnie z RFC 6962.
subjectKeyIdentifier	Skrót SHA-1 z subjectPublicKeyInfo (opcjonalnie)
Precertificate poison	Zgodnie z RFC 6962 (wyłącznie w precertyfikatach)

7.1.1 Numer(y) wersji

Wszystkie certyfikaty używają X.509 wersja 3.

7.1.2. Rozszerzenia certyfikatu

Rozszerzenia certyfikatu są zgodne z RFC 5280 oraz TLS BR.

Niniejsza sekcja określa dodatkowe wymagania dotyczące zawartości i rozszerzeń certyfikatów.

7.1.3 Identyfikatory obiektów algorytmów

Certum wydaje certyfikaty przy użyciu algorytmów identyfikowanych następującymi OID:

Nazwa algorytmu	OID

Nazwa algorytmu	OID
sha256WithRSAEncryption	1.2.840.113549.1.1.11
sha384WithRSAEncryption	1.2.840.113549.1.1.12
sha512WithRSAEncryption	1.2.840.113549.1.1.13
ecdsa-with-SHA256	1.2.840.10045.4.3.2
ecdsa-with-SHA384	1.2.840.10045.4.3.3
ecdsa-with-SHA512	1.2.840.10045.4.3.4

7.1.4 Formy nazw

Certum wydaje certyfikaty, których konwencje nazewnicze są zgodne z RFC 5280 oraz wytycznymi określonymi w Sekcji 7.1.4 TLS BR.

7.1.5 Ograniczenia nazw

Certum nie tworzy Subordinate CAs zawierających ograniczenia nazw (name constraints).

7.1.6 Identyfikator obiektu polityki certyfikatu

Zob. Sekcja 7.1.

7.1.7 Użycie rozszerzenia Policy Constraints

Nie dotyczy.

7.1.8 Składnia i semantyka kwalifikatorów polityki

Zob. Sekcja 7.1.

7.1.9 Semantyka przetwarzania krytycznego rozszerzenia Certificate Policies

Brak postanowień.

7.2 Profil CRL

Profil CRL

Pole lub rozszerzenie	Wartość
version	v2
signature	Zob. Sekcja 7.1.3.
issuer	Bajt do bajtu identyczne z polem subject issuing CA
thisUpdate	Data i czas wydania CRL
nextUpdate	Zob. Sekcja 4.9.7
revokedCertificates	Certyfikaty, które zostały unieważnione
authorityKeyIdentifier	Identyczne z polem subjectKeyIdentifier issuing CA

Pole lub rozszerzenie	Wartość
`CRLNumber`	Numer seryjny tej CRL w inkrementalnie rosnącej sekwencji CRL

7.2.1 Numer(y) wersji

CRL używają X.509 wersja 2.

7.2.2 Rozszerzenia CRL i wpisów CRL

W zakresie rozszerzeń CRL zob. Sekcja 7.2.

Rozszerzenia wpisów CRL (`revokedCertificates` components)

Składnik	Wartość
`serialNumber`	`serialNumber` zawarty w unieważnionym certyfikacie.
`revocationDate`	Data i czas unieważnienia. Data unieważnienia może być cofnięta w czasie (backdated), jeżeli `reasonCode` to `keyCompromise`.
`crlEntryExtensions`	Zawiera `reasonCode`.

Rozszerzenie CRL `reasonCode` dla certyfikatów końcowych (wartość RFC 5280 `reasonCode` w nawiasie):

- `unspecified` (0) - Reprezentowane przez pominięcie reasonCode. musi zostać pominięte, jeżeli wpis CRL dotyczy certyfikatu technicznie niezdolnego do powodowania wydania, chyba że wpis CRL dotyczy certyfikatu Subskrybenta objętego niniejszymi Requirements unieważnionego przed 15 lipca 2023 r.
- `keyCompromise` (1) - Wskazuje, że wiadomo lub podejrzewa się, iż klucz prywatny Subskrybenta został skompromitowany.
- `affiliationChanged` (3) - Wskazuje, że nazwa Subject lub inne informacje o tożsamości Subject w certyfikacie uległy zmianie, ale nie ma podstaw, by podejrzewać kompromitację klucza prywatnego certyfikatu.
- `superseded` (4) - Wskazuje, że certyfikat jest zastępowany, ponieważ: Subskrybent zażądał nowego certyfikatu, CA posiada uzasadnione dowody, że nie należy polegać na walidacji upoważnienia lub kontroli domeny dla jakiejkolwiek w pełni kwalifikowanej nazwy domenowej lub adresu IP w certyfikacie, lub CA unieważnił certyfikat z powodów zgodności, takich jak niezgodność certyfikatu z niniejszymi CA/Browser Forum Baseline Requirements albo z CP lub CPS CA.
- `cessationOfOperation` (5) - Wskazuje, że strona internetowa korzystająca z certyfikatu została zamknięta przed wygaśnięciem certyfikatu lub że Subskrybent nie jest już właścicielem ani nie kontroluje nazwy domeny zawartej w certyfikacie przed wygaśnięciem certyfikatu.
- `privilegeWithdrawn` (9) - Wskazuje, że po stronie Subskrybenta wystąpiło naruszenie, które nie skutkowało keyCompromise, takie jak przekazanie przez Subskrybenta certyfikatu mylących informacji w jego żądaniu certyfikatu albo niewywiązanie się z istotnych obowiązków wynikających z mającej zastosowanie

umowy Subskrybenta (Subscriber Agreement) lub Warunkami użytkowania (Terms of Use). Ten kod nie jest udostępniany Subskrybentom do wyboru i jest stosowany wyłącznie przez Certum, w uzasadnionych przypadkach.

7.3 Profil OCSP

Certum świadczy usługę OCSP zgodną ze standardem RFC 6960.

7.3.1 Numer(y) wersji

Brak postanowień.

7.3.2 Rozszerzenia OCSP

`singleExtensions` odpowiedzi OCSP nie zawierają rozszerzenia wpisu CRL `reasonCode`.

8. AUDYT ZGODNOŚCI I INNE OCENY

8.1 Częstotliwość lub okoliczności oceny

Audyty zgodności są przeprowadzane co najmniej raz w roku. Okres, w którym Certum wydaje publicznie zaufane certyfikaty, jest podzielony na nieprzerwany ciąg kolejnych okresów audytowych. Żaden okres audytowy nie przekracza 1 roku.

8.2 Tożsamość/kwalifikacje oceniającego

Zewnętrzne audyty są przeprowadzane przez niezależny podmiot upoważniony do przeprowadzania audytów WebTrust.

Taki podmiot:

- Jest niezależny od Certum i wolny od konfliktów interesów
- Jest upoważniony do przeprowadzania audytów WebTrust mających zastosowanie do publicznie zaufanych usług Certum
- Zatrudnia personel z wykazaną wiedzą ekspercką w zakresie technologii infrastruktury klucza publicznego (Public Key Infrastructure, PKI), kontroli bezpieczeństwa informacji i audytu IT
- Jest związany mającym zastosowanie prawem, regulacją lub zawodowym kodeksem etyki
- Utrzymuje odpowiednie ubezpieczenie odpowiedzialności zawodowej

8.3 Relacja oceniającego z ocenianym podmiotem

Audytor zewnętrzny jest niezależny od Certum i nie posiada interesu finansowego, relacji biznesowej ani innego układu, który mógłby tworzyć konflikt interesów lub stronniczość.

8.4 Zakres tematyczny objęty oceną

Coroczny audyt zewnętrzny jest przeprowadzany zgodnie z aktualnymi wersjami mających zastosowanie WebTrust Principles and Criteria, opublikowanymi przez CPA Canada i dostępnymi pod adresem:

https://www.cpacanada.ca/en/business-and-accounting-resources/audit-and-assurance/overview-of-webtrust-services/principles-and-criteria

Audyt obejmuje programy WebTrust mające zastosowanie do publicznie zaufanych usług TLS Certum, w tym, w odpowiednim zakresie:

- WebTrust for Certification Authorities
- WebTrust for Certification Authorities – TLS Baseline Requirements
- WebTrust for Certification Authorities – Extended Validation (TLS)
- WebTrust for Certification Authorities – Network Security

Audyt ocenia, czy Certum utrzymuje skuteczne kontrole zapewniające uzasadnioną pewność, że jego praktyki są właściwie ujawnione oraz że usługi certyfikacyjne TLS działają zgodnie z niniejszym CP/CPS i mającymi zastosowanie wymaganiami.

8.5 Działania podejmowane w wyniku niezgodności

Jeżeli podczas audytu zostanie zidentyfikowana niezgodność, audytor dokumentuje ustalenie i powiadamia Certum.

W zależności od charakteru i wagi niezgodności Certum:

- Opracuje i udokumentuje plan naprawczy
- Wdroży działania korygujące w komercyjnie uzasadnionym terminie
- Zaktualizuje swoje polityki, procedury lub kontrole techniczne tam, gdzie będzie to konieczne

Tam, gdzie ma to zastosowanie, audytor może zweryfikować, czy zidentyfikowana niezgodność została należycie usunięta.

Certum ocenia, czy w odniesieniu do wcześniej wydanych certyfikatów wymagane jest jakiekolwiek działanie korygujące, i podejmuje odpowiednie środki zgodnie z mającymi zastosowanie wymaganiami.

8.6 Komunikacja wyników

Certum udostępnia publicznie swój coroczny Audit Report nie później niż 3 miesiące po zakończeniu okresu audytowego.

Audit Reports są publikowane w formacie PDF w publicznym repozytorium i umożliwiają przeszukiwanie tekstu (zob. Sekcja 2.1).

Certum nie jest zobowiązane do publicznego udostępniania ustaleń audytowych, które nie wpływają na ogólną opinię z audytu.

8.7 Samoaudyty

Certum przeprowadza wewnętrzne samoaudyty co najmniej raz na kwartał zgodnie z mającymi zastosowanie wymaganiami CA/Browser Forum. Audyty te są prowadzone na losowo wybranej próbie obejmującej większą z wartości: 1 certyfikat albo co najmniej 3% certyfikatów wydanych w audytowanym okresie.

Samoaudyty oceniają, czy czynności związane z wydawaniem certyfikatów i zarządzaniem ich cyklem życia są wykonywane zgodnie z niniejszym CP/CPS i mającymi zastosowanie wymaganiami.

Wyniki samoaudytów są dokumentowane i przeglądane przez upoważniony personel. Zidentyfikowane niezgodności są usuwane zgodnie z Sekcją 8.5.

9. INNE SPRAWY BIZNESOWE I PRAWNE

9.1 Opłaty

9.1.1 Opłaty za wydanie lub odnowienie certyfikatu

Certum jest uprawnione do pobierania od Subskrybentów opłat za weryfikację i wydanie certyfikatów. Wszystkie mające zastosowanie opłaty są jasno komunikowane Wnioskodawcom w trakcie procesu składania wniosku.

Certum nie pobiera opłat za unieważnienie certyfikatu.

9.1.2 Opłaty za dostęp do certyfikatów

Certum nie pobiera opłat za dostęp do certyfikatów ani certyfikatów dostawcy usług zaufania.

9.1.3 Opłaty za dostęp do informacji o unieważnieniu lub statusie

Certum nie pobiera opłaty za unieważnienie certyfikatów.

Certum nie pobiera opłaty za dostęp do standardowych informacji o statusie certyfikatów za pośrednictwem CRL lub OCSP.

Certum może pobierać opłaty za dostarczanie niestandardowych informacji o unieważnieniu lub innych usług statusowych o wartości dodanej.

9.1.4 Opłaty za inne usługi

Certum może pobierać opłaty za usługi wykraczające poza standardowy proces wydania.

9.1.5 Polityka zwrotów

Subskrybent ma prawo żądać zwrotu uiszczonej opłaty w terminie 14 dni od dnia wydania certyfikatu, jeżeli usługa została wykonana niezgodnie z niniejszym CP/CPS oraz mającą zastosowanie umową Subskrybenta (Subscriber Agreement) lub Warunkami użytkowania (Terms of Use). Certum jest upoważnione do unieważnienia certyfikatu po przyznaniu zwrotu.

W przypadku rozwiązania umowy w związku z koniecznym unieważnieniem certyfikatu z powodu naruszenia przez Subskrybenta, Subskrybentowi nie przysługuje zwrot.

9.2 Odpowiedzialność finansowa

9.2.1 Zakres ochrony ubezpieczeniowej

Certum utrzymuje ochronę ubezpieczeniową z tytułu odpowiedzialności zawodowej (Professional Indemnity, Errors and Omissions) oraz ubezpieczenie Commercial General Liability.

Ubezpieczenie Professional Indemnity zapewnia ochronę z limitem polisy w wysokości 10 000 000 USD na jedno roszczenie oraz łącznie w okresie ubezpieczenia.

Utrzymywana ochrona ubezpieczeniowa spełnia lub przewyższa wymagania określone w aktualnych EV Guidelines.

Gwarancja finansowa Asseco Data Systems S.A. dotycząca wydawania certyfikatów EV podlega ograniczeniom odpowiedzialności określonym w niniejszym CP/CPS i mających zastosowanie umowach.

9.2.2 Inne aktywa

Brak postanowień.

9.2.3 Ubezpieczenie lub gwarancja dla podmiotów końcowych

Brak dodatkowych postanowień. Postanowienia dotyczące odpowiedzialności i gwarancji są określone w niniejszym CP/CPS oraz w mających zastosowanie umowach.

9.3 Poufność informacji biznesowych

9.3.1 Zakres informacji poufnych

Certum traktuje jako poufne wszystkie niepubliczne informacje uzyskane w toku świadczenia usług certyfikacyjnych i chroni takie informacje zgodnie z mającym zastosowanie prawem oraz wewnętrznymi politykami bezpieczeństwa.

Informacje poufne obejmują między innymi:

- Klucze prywatne
- Zapisy wniosków o certyfikat i dokumentację uzupełniającą
- Umowy z Subskrybentami i stronami ufającymi
- Logi transakcyjne i audit logs
- Wewnętrzne raporty audytowe i oceny bezpieczeństwa
- Plany ciągłości działania i odtwarzania po awarii
- Wewnętrzną dokumentację operacyjną dotyczącą systemów CA i RA
- Wszelkie inne informacje niepubliczne uzyskane w związku ze świadczeniem usług certyfikacyjnych

Certum nie gromadzi, nie przechowuje ani nie obejmuje escrow kluczy prywatnych Subskrybentów.

9.3.2 Informacje nieobjęte zakresem informacji poufnych

Za poufne nie uważa się następujących informacji:

- Informacje zawarte w wydanych certyfikatach
- Informacje o statusie certyfikatów i unieważnieniach (CRL, odpowiedzi OCSP)

- Niniejszy CP/CPS i inne publicznie dostępne dokumenty polityk
- Informacje, które muszą zostać ujawnione zgodnie z mającym zastosowanie prawem lub wiążącym orzeczeniem sądu albo organu administracji

9.3.3 Odpowiedzialność za ochronę informacji poufnych

Certum wdraża odpowiednie środki techniczne i organizacyjne w celu ochrony informacji poufnych przed nieuprawnionym dostępem, ujawnieniem, modyfikacją lub zniszczeniem.

Personel pełniący Trusted Roles jest związany obowiązkami zachowania poufności.

9.4 Prywatność informacji osobowych

9.4.1 Zasady prywatności

Dane osobowe przekazywane Certum przez Subskrybentów są objęte ochroną określoną przez:

- 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 oraz w sprawie swobodnego przepływu takich danych i uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) oraz
- Ustawę o ochronie danych osobowych

Zakres danych osobowych gromadzonych i przetwarzanych przez Certum odpowiada celom, do których dane te są potrzebne. Dane osobowe będą przetwarzane w celu: - zawarcia i realizacji umowy o wydanie certyfikatu niekwalifikowanego - na podstawie art. 6 ust. 1 lit b RODO, - realizacji obowiązków prawnych nałożonych na administratora - na podstawie art. 6 ust. 1 lit. c RODO w związku z właściwymi przepisami Ustawy o usługach zaufania i identyfikacji elektronicznej, - zapewnienia przestrzegania właściwych standardów branżowych - na podstawie prawnie uzasadnionego interesu administratora, jakim jest zapewnienie najwyżej jakości świadczonych usług (art. 6 ust. 1 lit. f RODO) - zdalnej weryfikacji tożsamości na podstawie odrębnie wyrażonej zgody - na podstawie art. 6 ust. 1 lit. a i art. 9 ust. 2 lit. a RODO, Szczegóły związane z wyrażeniem samej zgody zostaną podane przy jej wyrażaniu. Dane osobowe są wykorzystywane wyłącznie w związku ze świadczeniem usług certyfikacyjnych.

Dane osobowe są chronione zgodnie z zasadami ochrony prywatności określonymi w polityce bezpieczeństwa Asseco Data Systems S.A.

9.4.2 Informacje traktowane jako prywatne

Za informacje prywatne uważa się dane dotyczące subskrybenta pozyskane w toku składania wniosku lub procesu weryfikacji, które nie są udostępniane publicznie, w szczególności nie są zawarte w certyfikacie, repozytorium, na listach CRL.

9.4.3 Informacje nieuznawane za prywatne

Informacje dostępne w certyfikatach, CRL lub OCSP nie są uznawane za prywatne.

Każdy dokument opublikowany w Repozytorium Certum (Sekcja 2.1) nie jest uznawany za prywatny.

9.4.4 Odpowiedzialność za ochronę informacji prywatnych

Każdy pracownik Certum lub osoba upoważniona, która ma dostęp do danych osobowych gromadzonych w związku z wydawaniem certyfikatów, jest związana obowiązkami zachowania poufności.

Certum wdraża odpowiednie środki techniczne i organizacyjne w celu ochrony danych osobowych przed nieuprawnionym dostępem, ujawnieniem, modyfikacją lub zniszczeniem.

9.4.5 Powiadomienie i zgoda na wykorzystanie informacji prywatnych

O ile niniejszy CP/CPS lub mająca zastosowanie umowa nie stanowią inaczej, dane osobowe nie mogą być przetwarzane poza celami opisanymi w niniejszym dokumencie bez ważnej podstawy prawnej wynikającej z mającego zastosowanie prawa, w tym, tam gdzie jest to wymagane, zgody osoby, której dane dotyczą.

Dodatkowe informacje dotyczące przetwarzania danych osobowych są dostępne w Polityce Prywatności Asseco Data Systems S.A. opublikowanej pod adresem:

https://www.assecods.pl/en/privacy-policy

9.4.6 Ujawnienie na podstawie postępowania sądowego lub administracyjnego

Informacje poufne lub dane osobowe mogą być ujawnione sądom, organom ścigania lub organom administracyjnym wyłącznie wtedy, gdy wymaga tego mające zastosowanie prawo i po spełnieniu wszystkich wymogów prawnych obowiązujących w Rzeczypospolitej Polskiej.

9.4.7 Inne okoliczności ujawnienia informacji

Brak postanowień.

9.5 Prawa własności intelektualnej

Asseco Data Systems S.A. działająca pod marką Certum zachowuje wszelkie prawa własności intelektualnej do:

- Niniejszego CP/CPS i powiązanych dokumentów polityk
- Certyfikatów i informacji o unieważnieniach wydawanych przez Certum
- Znaków towarowych, znaków usługowych, logotypów i innych elementów identyfikacji marki Certum
- Systemów Certum, oprogramowania, dokumentacji i powiązanych materiałów

Certyfikaty i informacje o unieważnieniach pozostają wyłączną własnością Certum. Certum udziela zgody na reprodukcję i dystrybucję certyfikatów w całości, pod warunkiem że nie są modyfikowane ani wykorzystywane w sposób wprowadzający w błąd.

Klucze prywatne i publiczne powiązane z certyfikatem pozostają własnością Subskrybenta wskazanego w certyfikacie.

Wszelkie pozostałe prawa własności intelektualnej pozostają przy ich odpowiednich właścicielach.

9.6 Oświadczenia i gwarancje

Certum składa wszystkim Subskrybentom i stronom ufającym określone oświadczenia dotyczące jego publicznych usług certyfikacyjnych, opisane poniżej.

Certum zastrzega sobie prawo do modyfikowania takich oświadczeń według własnego uznania lub zgodnie z wymogami prawa.

Z wyjątkiem przypadków wyraźnie wskazanych w niniejszym dokumencie lub w odrębnej umowie z Subskrybentem, w zakresie określonym w odpowiednich sekcjach niniejszego dokumentu, Certum oświadcza, we wszystkich istotnych aspektach, że:

- Będzie przestrzegać niniejszego dokumentu oraz swoich wewnętrznych lub opublikowanych polityk i procedur, w szczególności z niniejszym CP/CPS
- Udostępni kopię niniejszego dokumentu i mających zastosowanie polityk zainteresowanym stronom za pośrednictwem Repozytorium Certum
- Będzie przestrzegać mających zastosowanie przepisów prawa i regulacji, w tym przepisów o ochronie danych osobowych, takich jak RODO
- Będzie zapewniać infrastrukturę i usługi certyfikacyjne, w tym między innymi ustanowienie i prowadzenie Repozytorium Certum dla zarządzania usługami PKI
- Niezwłocznie powiadomi wszystkich dotkniętych Subskrybentów w przypadku kompromitacji własnych kluczy prywatnych
- Będzie zapewniać i weryfikować procedury wnioskowania dla różnych typów certyfikatów, które udostępnia, weryfikując tożsamość Subskrybenta oraz jego prawo do używania lub kontrolowania nazw domen albo adresów IP
- W przypadku certyfikatów Extended Validation (EV) będzie weryfikować i potwierdzać prawne istnienie oraz tożsamość organizacji zgodnie z EV Guidelines
- Będzie wydawać certyfikaty cyfrowe zgodnie z niniejszym dokumentem oraz wykonywać zobowiązania w nim przedstawione
- Będzie unieważniać certyfikaty z każdego szczególnego powodu i w terminach (24 godziny lub 5 dni) zdefiniowanych w niniejszym dokumencie oraz TLS BR
- Będzie publikować zaakceptowane certyfikaty oraz listy unieważnionych certyfikatów (CRLs)

- Będzie zapewniać wsparcie Subskrybentom i stronom ufającym zgodnie z opisem w niniejszym dokumencie, w tym świadczenie usług weryfikacji statusu online za pośrednictwem OCSP

Subskrybent przyjmuje również do wiadomości, że Certum nie ma dalszych obowiązków poza tymi, które zostały wyraźnie wskazane w niniejszym dokumencie.

9.6.1 Oświadczenia i gwarancje CA

Nie dotyczy.

9.6.2 Oświadczenia i gwarancje RA

Nie dotyczy.

9.6.3 Oświadczenia i gwarancje Subskrybenta

Certum wymaga, aby każdy Wnioskodawca potwierdził i zaakceptował Subscriber Agreement lub Terms of Use, które są prawnie egzekwowalne wobec Subskrybenta. Akceptując certyfikat, Subskrybent oświadcza i gwarantuje wobec Certum oraz beneficjentów certyfikatu, że:

- Wszystkie informacje przekazane Certum podczas składania wniosku, rejestracji i przez cały cykl życia certyfikatu są dokładne, kompletne i prawdziwe
- Subskrybent sprawuje wyłączną kontrolę, zachowuje poufność i podejmuje wszelkie rozsądne środki w celu ochrony klucza prywatnego
- Subskrybent sprawdzi i zweryfikuje poprawność informacji zawartych w certyfikacie przed jego instalacją i użyciem
- Certyfikat jest używany wyłącznie do celów uprawnionych i zgodnych z prawem, zgodnych z przeznaczeniem zdefiniowanym w niniejszym CP/CPS oraz mającą zastosowanie umową Subskrybenta (Subscriber Agreement) lub Warunkami użytkowania (Terms of Use)
- Subskrybent niezwłocznie powiadomi Certum i zażąda unieważnienia, jeżeli jakakolwiek informacja w certyfikacie stanie się nieprawidłowa albo jeżeli wystąpi rzeczywista lub podejrzewana kompromitacja klucza prywatnego
- Subskrybent niezwłocznie zaprzestanie wszelkiego używania certyfikatu oraz powiązanego z nim klucza prywatnego po jego wygaśnięciu lub unieważnieniu
- Subskrybent nie będzie używać klucza prywatnego do podpisywania żadnego innego certyfikatu ani CRL jako urząd certyfikacji
- Wykorzystanie informacji przekazanych przez Subskrybenta (np. nazw domen, nazw organizacji) nie narusza praw własności intelektualnej ani praw majątkowych osób trzecich
- Subskrybent odpowie na instrukcje Certum dotyczące niewłaściwego użycia certyfikatu lub kompromitacji klucza w terminie określonym przez CA

- Certyfikat nie będzie wykorzystywany w systemach lub zastosowaniach wysokiego ryzyka wymagających bezawaryjnego działania (fail-safe), w których awaria certyfikatu mogłaby prowadzić do śmierci, obrażeń ciała lub poważnych szkód środowiskowych

9.6.4 Oświadczenia i gwarancje strony ufającej

Strony ufające oświadczają i gwarantują, że przed poleganiem na certyfikacie wydanym przez Certum przeczytały, rozumieją i akceptują niniejszy CP/CPS oraz mającą zastosowanie umowę strony ufającej.

Aby poleganie było rozsądne, strona ufająca odpowiada za:

- Uzyskanie wystarczającej wiedzy na temat użycia certyfikatów cyfrowych i PKI, aby podjąć świadomą decyzję co do stopnia polegania
- Potwierdzenie ważności każdego certyfikatu w ścieżce certyfikacji (aż do Root CA) przez sprawdzenie bieżącego statusu unieważnienia za pośrednictwem CRL lub OCSP przed jakimkolwiek aktem polegania
- Upewnienie się, że certyfikat nie wygasł i nie został unieważniony w chwili polegania
- Zweryfikowanie, że certyfikat jest używany wyłącznie zgodnie z jego przeznaczeniem i w granicach określonych przez rozszerzenia Key Usage (KU) i Extended Key Usage (EKU)
- Podjęcie wszelkich rozsądnych kroków w celu minimalizacji ryzyka poprzez uwzględnienie wartości ekonomicznej transakcji, potencjalnej straty lub szkody wynikającej z błędnej identyfikacji oraz wszelkich innych przesłanek wiarygodności odnoszących się do Subskrybenta
- Uznanie, że ostateczna decyzja o poleganiu na certyfikacie spoczywa wyłącznie na stronie ufającej, która ponosi wszelkie konsekwencje, w tym odpowiedzialność prawną, za jakiekolwiek niewypełnienie tych obowiązków

Jakiekolwiek poleganie na certyfikacie w sposób niezgodny z tymi wymaganiami odbywa się na własne ryzyko strony ufającej.

9.6.5 Oświadczenia i gwarancje innych uczestników

Brak postanowień.

9.7 Wyłączenia gwarancji

Gwarancje Certum opierają się na ogólnych zasadach określonych w niniejszym CP/CPS i są zgodne z nadrzędnymi aktami prawnymi obowiązującymi w Rzeczypospolitej Polskiej. Wyłączenie gwarancji powinno być określone w umowach pomiędzy Subskrybentami a Certum.

9.8 Ograniczenia odpowiedzialności

Jeżeli szkody powstały z winy Certum lub stron, z którymi Asseco Data Systems S.A. zawarła umowę w taki sposób, że wina jest przeniesiona na Certum, łączne gwarancje finansowe (całkowita odpowiedzialność odszkodowawcza) Certum wobec wszystkich stron (w tym stron ufających) nie mogą przekroczyć (w pojedynczym przypadku) łącznej kwoty sum dla poziomu wiarygodności:

Certyfikaty DV TLS

- Łączny limit odpowiedzialności Certum 200 000 EUR
- Limit odpowiedzialności Certum za jedną objętą szkodę 600 EUR

Certyfikaty OV TLS

- Łączny limit odpowiedzialności Certum 400 000 EUR
- Limit odpowiedzialności Certum za jedną objętą szkodę 15 000 EUR

Certyfikaty EV TLS

- Łączny limit odpowiedzialności Certum 1 000 000 EUR
- Limit odpowiedzialności Certum za jedną objętą szkodę 15 000 EUR

9.9 Zwolnienie z odpowiedzialności

9.9.1 Odpowiedzialność Subskrybenta

Odpowiedzialność Subskrybenta wynika z obowiązków i gwarancji określonych w Sekcji 9.6.3. Warunki odpowiedzialności reguluje umowa z Asseco Data Systems S.A.

9.9.2 Odpowiedzialność strony ufającej

Odpowiedzialność strony ufającej wynika z obowiązków i gwarancji określonych w Sekcji 9.6.4. Warunki odpowiedzialności mogą być regulowane umową z Certum i Subskrybentem.

Umowy z Subskrybentami i Certum wymagają, aby strony ufające posiadały wystarczającą ilość informacji do podjęcia decyzji o zatwierdzeniu lub odrzuceniu podpisu elektronicznego podczas jego weryfikacji.

Strony powinny określić wartość finansową transakcji, która zostanie przez nie zatwierdzona wyłącznie na podstawie informacji zawartych w certyfikacie, oraz zapoznać się z informacjami określonymi w Sekcji 9.6.4.

9.10 Okres obowiązywania i zakończenie

9.10.1 Okres obowiązywania

Niniejszy CP/CPS wchodzi w życie z chwilą oznaczenia go statusem ważny i publikacji w Repozytorium Certum.

Aneksy do niniejszego CP/CPS wchodzą w życie z chwilą publikacji w Repozytorium Certum.

9.10.2 Zakończenie

Niniejszy CP/CPS obowiązuje (ma status aktualny) do chwili oznaczenia statusem ważny, publikacji i zatwierdzenia jego nowej wersji.

9.10.3 Skutek zakończenia i dalsze obowiązywanie

Po zakończeniu obowiązywania niniejszego CP/CPS Subskrybenci i strony ufające pozostają związani jego postanowieniami w odniesieniu do wszystkich certyfikatów wydanych na pozostały okres ważności takich certyfikatów.

9.11 Indywidualne zawiadomienia i komunikacja z uczestnikami

O ile umowa pomiędzy stronami nie stanowi inaczej, uczestnicy będą korzystać z komercyjnie uzasadnionych metod komunikacji z uwzględnieniem krytyczności i przedmiotu komunikacji.

Metody te obejmują między innymi:

- Zawiadomienia wysyłane na adresy email przekazane przez uczestnika
- Komunikację wykorzystującą informacje kontaktowe zebrane i zwalidowane podczas procesu składania wniosku i weryfikacji tożsamości

Ogólne ogłoszenia przeznaczone dla wszystkich uczestników, takie jak publikacja CRL lub zmiany niniejszego CP/CPS, są obsługiwane przez Repozytorium Certum, a nie poprzez indywidualne zawiadomienia.

9.12 Zmiany

9.12.1 Procedura zmiany

Certum dokonuje przeglądu niniejszego CP/CPS co najmniej raz w roku i jest upoważnione do wprowadzania zmian według uznania. Zmiany są zatwierdzane przez Certum Policy Authority i potwierdzane nowym numerem wersji oraz zaktualizowaną datą publikacji w historii dokumentu.

9.12.2 Mechanizm i okres powiadamiania

Certum publikuje wszystkie zaktualizowane wersje niniejszego CP/CPS w swoim publicznym Repozytorium Certum (zob. Sekcja 2.1).:

- Istotne zmiany, które mają materialny wpływ na uczestników, podlegają powiadomieniu
- Zmiany redakcyjne, takie jak poprawki pisowni, gramatyki lub odesłań wewnętrznych, mogą być wprowadzane bez powiadomienia

9.12.3 Okoliczności, w których OID musi zostać zmieniony

Certum Policy Authority zachowuje wyłączne uprawnienie do ustalenia, czy zmiana niniejszego CP/CPS wymaga zmiany identyfikatora obiektu polityki (Object Identifier, OID).

9.13 Postanowienia dotyczące rozstrzygania sporów

Brak postanowień.

9.14 Prawo właściwe

Niniejszy CP/CPS oraz wszelkie związane z nim umowy podlegają prawu obowiązującemu w Rzeczypospolitej Polskiej i zgodnie z nim powinny być interpretowane.

9.15 Zgodność z mającym zastosowanie prawem

Certum działa i świadczy swoje usługi z pełną zgodnością ze wszystkimi mającymi zastosowanie krajowymi, lokalnymi i zagranicznymi przepisami prawa, regułami, regulacjami, zarządzeniami, dekretami i nakazami.

Aby zapewnić integralność prawną we wszystkich jurysdykcjach:

- Certum i wszyscy Uczestnicy przestrzegają wszystkich mających zastosowanie ograniczeń dotyczących eksportu lub importu oprogramowania, sprzętu lub informacji technicznych, w szczególności odnoszących się do produktów kryptograficznych
- Certum spełnia wymagania mających zastosowanie przepisów o ochronie danych, w tym europejskiego General Data Protection Regulation (GDPR) oraz polskiego prawa ochrony danych osobowych, wdrażając odpowiednie środki techniczne i organizacyjne w celu ochrony danych osobowych
- Certum utrzymuje wszystkie niezbędne licencje i upoważnienia wymagane przez prawo jurysdykcji, w których działa, dla wydawania i zarządzania certyfikatami.
- Świadcząc usługi PKI, Certum jest zgodne we wszystkich istotnych aspektach z wysokopoziomowymi standardami międzynarodowymi oraz odpowiednimi przepisami regulującymi certyfikaty TLS

9.16 Postanowienia różne

9.16.1 Całość porozumienia

Niniejszy CP/CPS oraz dokumenty włączone do niego przez odesłanie stanowią całość porozumienia pomiędzy stronami, zastępując wszelkie wcześniejsze uzgodnienia lub oświadczenia dotyczące tego przedmiotu. W przypadku sprzeczności pomiędzy postanowieniami niniejszego CP/CPS a konkretną umową z uczestnikiem, postanowienia tej konkretnej umowy mają pierwszeństwo wobec odpowiedniej strony.

9.16.2 Cesja

Uczestnicy nie mogą przenieść swoich praw ani obowiązków wynikających z niniejszego CP/CPS bez uprzedniej pisemnej zgody Certum. Każda próba dokonania cesji bez takiej zgody jest nieważna. Niniejszy dokument wiąże strony oraz ich odpowiednich następców prawnych i dopuszczalnych cesjonariuszy i działa na ich korzyść.

9.16.3 Rozdzielność postanowień

Jeżeli poszczególne części niniejszego dokumentu lub umów zawartych na jego podstawie zostaną uznane za naruszające obowiązujące prawo lub sprzeczne z prawem, właściwy sąd może nakazać respektowanie pozostałej części CP/CPS lub już zawartych umów (tj. zgodnej z prawem), chyba że zakwestionowane części nie mają znaczenia z punktu widzenia wymiany (np. transakcji handlowej), którą strony uzgodniły.

Postanowienie o rozdzielności jest szczególnie istotne w umowach wskazanych w rozdziale 9.6. Jeżeli klauzula rozdzielności nie została zawarta w umowie, cała umowa może być sprzeczna z prawem, nawet jeżeli nie taki był zamiar stron.

9.16.4 Egzekwowanie (honoraria adwokackie i zrzeczenie się praw)

Certum może dochodzić zwolnienia z odpowiedzialności oraz dochodzić uzasadnionych honorariów adwokackich, kosztów i wydatków od każdego Uczestnika z tytułu szkód i strat związanych z działaniem tego Uczestnika lub naruszeniem niniejszego CP/CPS.

Niniejszy dokument być egzekwowany jako całość, przy czym niewyegzekwowanie przez jakąkolwiek osobę któregokolwiek postanowienia niniejszego dokumentu nie oznacza zrzeczenia się prawa do przyszłego egzekwowania tego lub jakiegokolwiek innego postanowienia. Żadne naruszenie któregokolwiek postanowienia niniejszego CP/CPS nie będzie uznawane za objęte zrzeczeniem, chyba że zrzeczenie zostanie sporządzone na piśmie i podpisane przez upoważnionego przedstawiciela Certum.

9.16.5 Siła wyższa

Certum nie ponosi odpowiedzialności za niewykonanie lub opóźnienie wykonania swoich obowiązków, jeżeli takie niewykonanie lub opóźnienie wynika ze zdarzeń pozostających poza jego uzasadnioną kontrolą oraz bez jego winy lub zaniedbania.

9.17 Inne postanowienia

Brak postanowień.

ANEKS A - Historia zmian

Wersja	Opis zmian	Data
1.0.0	Pierwsze wydanie.	2026-04-29
1.0.1	Zaktualizowano informacje dotyczące certyfikatów krzyżowych Certum w sekcji 1.3.1.2.	2026-07-20
1.1.0	Zaktualizowano sekcję 4.1.1 w celu doprecyzowania sankcji mających zastosowanie do Certum; zaktualizowano odnośniki do programów głównych certyfikatów Chrome i Apple; skorygowano opis rozszerzenia Certificate Policies dla certyfikatów EV.	2026-10-05

ANEKS B - Definicje, akronimy i referencje

Definicje

Applicant (Wnioskodawca) - Osoba fizyczna lub osoba prawna, która składa wniosek o wydanie (lub odnowienie) certyfikatu. Po wydaniu certyfikatu Wnioskodawca jest określany jako Subskrybent (Subscriber). W przypadku certyfikatów wydawanych dla urządzeń, Wnioskodawcą jest podmiot, który kontroluje lub obsługuje urządzenie wskazane w certyfikacie, nawet jeśli to urządzenie wysyła faktyczne żądanie certyfikatu.

Attestation Letter (List poświadczający) - Dokument potwierdzający poprawność informacji o Podmiocie (Subject Information), sporządzony przez księgowego, prawnika, urzędnika państwowego lub inny zaufany podmiot trzeci, na którego opinii zwyczajowo się polega.

Audit Period (Okres audytu) - W audycie obejmującym określony przedział czasu, okres pomiędzy pierwszym dniem (początek) a ostatnim dniem działalności (koniec) objętym badaniem audytora.

Audit Report (Raport z audytu) - Raport sporządzony przez Kwalifikowanego Audytora, zawierający jego opinię na temat zgodności procesów i mechanizmów kontrolnych danego podmiotu z obowiązkowymi wymaganiami.

CAA (Certification Authority Authorization – autoryzacja urzędu certyfikacji) - Zgodnie z RFC8659: rekord DNS umożliwiający właścicielowi domeny określenie, które urzędy certyfikacji są uprawnione do wydawania certyfikatów dla tej domeny.

Certificate (Certyfikat) - Dokument elektroniczny wykorzystujący podpis cyfrowy do powiązania klucza publicznego z tożsamością.

Certificate Data (Dane certyfikatu) - Wnioski o certyfikaty oraz powiązane z nimi dane, będące w posiadaniu lub pod kontrolą CA.

Certificate Policy (Polityka certyfikacji) - Zbiór zasad określających zastosowanie certyfikatu dla określonej społeczności lub implementacji PKI o wspólnych wymaganiach bezpieczeństwa.

Certificate Problem Report (Zgłoszenie problemu z certyfikatem) - Zgłoszenie dotyczące podejrzenia kompromitacji klucza, niewłaściwego użycia certyfikatu lub innych form nadużyć.

Certificate Profile (Profil certyfikatu) - Zestaw dokumentów lub plików definiujących zawartość certyfikatu i jego rozszerzenia.

Certificate Revocation List (CRL – lista unieważnionych certyfikatów) - Regularnie aktualizowana, oznaczona czasem lista unieważnionych certyfikatów podpisana cyfrowo przez CA.

Certification Authority (CA – urząd certyfikacji) - Podmiot odpowiedzialny za tworzenie, wydawanie, unieważnianie i zarządzanie certyfikatami.

Certification Practice Statement (CPS – kodeks postępowania certyfikacyjnego) - Dokument opisujący zasady funkcjonowania usług certyfikacyjnych.

Certum Systems (Systemy Certum) - Systemy i interfejsy techniczne wykorzystywane przez Certum do świadczenia usług certyfikacyjnych, w tym CertManager, API i ACME.

Control (Kontrola) - Posiadanie, bezpośrednio lub pośrednio, możliwości kierowania działalnością podmiotu lub sprawowania nad nim kontroli.

Country (Kraj) - Państwo będące członkiem ONZ lub jednostka uznana za suwerenne państwo przez co najmniej dwa państwa członkowskie ONZ.

CSPRNG (Kryptograficznie bezpieczny generator liczb losowych) - Generator liczb losowych przeznaczony do zastosowań kryptograficznych.

Domain Contact (Kontakt domeny) - Właściciel domeny lub kontakt techniczny/administracyjny wskazany w WHOIS lub DNS.

Domain Label (Etykieta domeny) - Część nazwy domeny zgodnie z RFC8499.

Domain Name (Nazwa domeny) - Ciąg etykiet domenowych tworzący nazwę w systemie DNS.

Expiry Date (Data wygaśnięcia) - Data „Not After" określająca koniec ważności certyfikatu.

Internal Name (Nazwa wewnętrzna) - Nazwa niebędąca publicznie rozpoznawalną nazwą domenową.

IP Address (Adres IP) - 32- lub 128-bitowy identyfikator urządzenia w sieci.

Issuing CA (CA wydający) - Urząd certyfikacji, który wydał dany certyfikat.

Key Compromise (Kompromitacja klucza) - Sytuacja, w której klucz prywatny został ujawniony lub dostęp do niego uzyskała osoba nieuprawniona.

Key Pair (Para kluczy) - Klucz prywatny i odpowiadający mu klucz publiczny.

Legal Entity (Osoba prawna) - Podmiot posiadający osobowość prawną.

Linting (Linting – walidacja techniczna) - Proces sprawdzania zgodności danych podpisanych cyfrowo z wymaganiami standardów.

Network Perspective (Perspektywa sieciowa) - Punkt widzenia sieci wykorzystywany do walidacji kontroli domeny.

Object Identifier (OID – identyfikator obiektu) - Unikalny identyfikator przypisany obiektowi zgodnie z normami ISO.

OCSP Responder (Responder OCSP) - Serwer dostarczający informacje o statusie certyfikatu.

Onion Domain Name (Nazwa domeny .onion) - Nazwa domeny kończąca się na „.onion”.

Online Certificate Status Protocol (OCSP – protokół sprawdzania statusu certyfikatu) - Protokół umożliwiający sprawdzenie statusu certyfikatu.

Precertificate (Precertyfikat) - Struktura danych przesyłana do logów Certificate Transparency.

Private Key (Klucz prywatny) - Klucz używany do podpisu i odszyfrowywania danych.

Public Key (Klucz publiczny) - Klucz używany do weryfikacji podpisu i szyfrowania.

Public Key Infrastructure (PKI – infrastruktura klucza publicznego) - Zestaw komponentów umożliwiających zarządzanie certyfikatami i kluczami.

Random Value (Wartość losowa) - Wartość o wysokiej entropii wykorzystywana w procesach weryfikacyjnych.

Registration Authority (RA – urząd rejestracji) - Podmiot odpowiedzialny za identyfikację i uwierzytelnienie Wnioskodawców.

Reliable Data Source (Zaufane źródło danych) - Źródło danych uznawane za wiarygodne.

Reliable Method of Communication (Zaufana metoda komunikacji) - Metoda komunikacji zweryfikowana niezależnie od Wnioskodawcy.

Relying Party (Strona ufająca) - Podmiot polegający na ważnym certyfikacie.

Repository (Repozytorium) - Publicznie dostępna baza danych PKI.

Requirements (Wymagania) - Baseline Requirements.

Reserved IP Address (Zastrzeżony adres IP) - Adres IP zarejestrowany jako specjalny w IANA.

Root CA (Główny urząd certyfikacji) - Najwyższy poziom CA.

Subject (Podmiot certyfikatu) - Podmiot wskazany w certyfikacie.

Subject Identity Information (Dane identyfikujące podmiot) - Dane identyfikujące podmiot certyfikatu.

Subordinate CA (Podrzędny urząd certyfikacji) - CA podpisany przez Root CA.

Subscriber (Subskrybent) - Podmiot, któremu wydano certyfikat.

Subscriber Agreement (Umowa Subskrybenta) - Umowa określająca prawa i obowiązki.

Terms of Use (Warunki użytkowania) - Warunki korzystania z certyfikatu.

Trusted Root Store (Zaufany magazyn certyfikatów głównych) - Zbiór zaufanych certyfikatów głównych urzędów certyfikacji (Root CA Certificates), utrzymywany i dystrybuowany przez dostawcę oprogramowania, systemu operacyjnego, przeglądarki internetowej lub innej platformy, wykorzystywany przez aplikacje do ustalania zaufania do łańcuchów certyfikacji. Certyfikat urzędu certyfikacji umieszczony w Trusted Root Store jest traktowany jako punkt odniesienia zaufania (trust anchor) podczas weryfikacji certyfikatów TLS i innych certyfikatów X.509.

Validity Period (Okres ważności) - Okres od „notBefore" do „notAfter".

WHOIS (WHOIS – system informacji o domenach) - Dane o domenie uzyskane z WHOIS lub RDAP.

Skróty

CA (Certification Authority – urząd certyfikacji)

CAA (Certification Authority Authorization – autoryzacja urzędu certyfikacji)

CP (Certificate Policy – polityka certyfikacji)

CPS (Certification Practice Statement – kodeks postępowania certyfikacyjnego)

CRL (Certificate Revocation List – lista unieważnionych certyfikatów)

DBA (Doing Business As – nazwa handlowa)

FIPS (Federal Information Processing Standards – federalne standardy przetwarzania informacji)

FQDN (Fully Qualified Domain Name – w pełni kwalifikowana nazwa domenowa)

HSM (Hardware Security Module – sprzętowy moduł bezpieczeństwa kryptograficznego)

IANA (Internet Assigned Numbers Authority – organizacja przydzielająca numery internetowe)

ICANN (Internet Corporation for Assigned Names and Numbers – organizacja zarządzająca nazwami domen)

ISO (International Organization for Standardization – Międzynarodowa Organizacja Normalizacyjna)

OCSP (Online Certificate Status Protocol – protokół sprawdzania statusu certyfikatu)

PKI (Public Key Infrastructure – infrastruktura klucza publicznego)

RA (Registration Authority – urząd rejestracji)

SSL (Secure Sockets Layer – protokół bezpiecznej komunikacji)

TLS (Transport Layer Security – protokół bezpieczeństwa warstwy transportowej)

Referencje

RFC 2119, *Słowa kluczowe używane w RFC do określania poziomów wymagań*. S. Bradner, marzec 1997.

RFC 5280, *Infrastruktura klucza publicznego X.509 w Internecie – Profil certyfikatów i list unieważnień certyfikatów (CRL)*. D. Cooper i in., maj 2008.

RFC 6962, *Certificate Transparency*. B. Laurie i in., czerwiec 2013.

RFC 7686, *Nazwa domenowa specjalnego przeznaczenia „.onion”*. J. Appelbaum i in., październik 2015.

RFC 8499, *Terminologia DNS*. P. Hoffman i in., styczeń 2019.

RFC 8659, *Rekord DNS Certification Authority Authorization (CAA)*. P. Hallam-Baker i in., listopad 2019.

ITU-T X.509, Międzynarodowy Związek Telekomunikacyjny. *Technologia informacyjna – Otwarte systemy połączeń – Katalog: Ramy certyfikatów klucza publicznego i certyfikatów atrybutów*.

ISO/IEC 9594-8, Międzynarodowa Organizacja Normalizacyjna, *Technologia informacyjna – Otwarte systemy połączeń – Katalog: Ramy certyfikatów klucza publicznego i certyfikatów atrybutów*.

CA/Browser Forum Baseline Requirements, Wymagania podstawowe dotyczące wydawania i zarządzania publicznie zaufanymi certyfikatami TLS, https://cabforum.org/working-groups/server/baseline-requirements/documents/

CA/Browser Forum Extended Validation Guidelines, Wytyczne dotyczące wydawania i zarządzania certyfikatami Extended Validation (EV), https://cabforum.org/working-groups/server/extended-validation/documents/

CA/Browser Forum Network and Certificate System Security Requirements, Wymagania bezpieczeństwa sieci i systemów certyfikacyjnych, https://cabforum.org/working-groups/netsec/documents/

WebTrust for Certification Authorities, Program audytowy WebTrust dla urzędów certyfikacji, https://www.cpacanada.ca/business-and-accounting-resources/audit-and-assurance/overview-of-webtrust-services/principles-and-criteria

WebTrust for Certification Authorities – TLS Baseline Requirements, Program WebTrust obejmujący wymagania podstawowe TLS. https://www.cpacanada.ca/business-and-accounting-resources/audit-and-assurance/overview-of-webtrust-services/principles-and-criteria

WebTrust for Certification Authorities – Extended Validation, Program WebTrust obejmujący certyfikaty Extended Validation. https://www.cpacanada.ca/business-and-accounting-resources/audit-and-assurance/overview-of-webtrust-services/principles-and-criteria

WebTrust for Certification Authorities – Network Security, Program WebTrust dotyczący bezpieczeństwa sieci. https://www.cpacanada.ca/business-and-accounting-resources/audit-and-assurance/overview-of-webtrust-services/principles-and-criteria