Podręcznik obsługi

Polityka certyfikacji i kodeks postępowania certyfikacyjnego – Certificate Policy Certificate Practice Statement

NUMER DOKUMENTU	ICERT-INDI-MO*
WERSJA	4.11
DATA	15.05.2024

* z wersji 4.0, w niniejszym dokumencie zostały połączone dokumenty ICERT-INDI-MO i ICERT- INDI-MO-ENT


INFOCERT
TINEXTA GROUP

SPIS TREŚCI

1 WPROWADZENIE

1.1 Zagadnienia ogólne

Certyfikat łączy klucz publiczny z zestawem informacji identyfikujących podmiot posiadający odpowiedni klucz prywatny: osoba ta, fizyczna lub prawna, jest **posiadaczem** certyfikatu. Certyfikat używany jest przez inne osoby w celu uzyskania klucza publicznego, rozpowszechnianego wraz z certyfikatem, oraz weryfikacji kwalifikowanego podpisu elektronicznego, dołączonego do dokumentu lub z nim związanego. Certyfikat gwarantuje zgodność między kluczem publicznym a posiadaczem. Stopień wiarygodności
tego powiązania zależy od kilku czynników: sposobu, w jaki urząd certyfikacji (Certification Authority) wydał certyfikat, zastosowanych środków bezpieczeństwa, zobowiązań przyjętych przez posiadacza w celu ochrony jego klucza prywatnego, oferowanych gwarancji.
Niniejszy dokument jest Podręcznikiem obsługi **Dostawcy usług zaufania**
InfoCert (*Trust Service Provider*), który, w ramach swoich usług zaufania, świadczy również usługi kwalifikowanego podpisu elektronicznego. Podręcznik obsługi zawiera zasady i praktyki stosowane w procesie identyfikacji i wydawania certyfikatu kwalifikowanego, przyjęte środki bezpieczeństwa, obowiązki, gwarancje i zakresy odpowiedzialności oraz, ogólnie, opisuje wszystko to, co czyni certyfikat kwalifikowany wiarygodnym, zgodnie z obowiązującymi przepisami w zakresie usług zaufania, kwalifikowanego podpisu elektronicznego i podpisu cyfrowego.
Publikując niniejszy dokument i umieszczając odniesienia do niego w certyfikatach, umożliwia się użytkownikom dokonanie oceny charakterystyki i wiarygodności usługi certyfikacyjnej, a tym samym związku pomiędzy kluczem a posiadaczem.
Treść oparta jest na normach obowiązujących w dniu wydania i jest zgodna z zaleceniami dokumentu: „Request for Comments: 3647 – Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework” © Internet Society 2003.

Niniejszy Podręcznik obsługi zawiera również zasady i praktyki stosowane przez InfoCert S.p.A. (zwaną dalej również po prostu „**InfoCert**”) w procesie kontroli wniosków, identyfikacji wnioskodawców i wystawiania certyfikatów do uwierzytelniania stron internetowych, o których mowa w art. 34 Rozporządzenia delegowanego (UE) 2018/389 [12], wdrażającego Dyrektywę (UE) 2015/2366 (PSD2) [11], zgodnie z wymogami określonymi w normie ETSI TS 119 495 (określonymi w dalszej części jako „Certyfikaty PSD2”).

1.2 Nazwa i identyfikacja dokumentu

Dokument ten nosi nazwę „Dostawca usług zaufania InfoCert – Podręcznik obsługi” i oznakowany został kodem dokumentu: ICERT-INDI-MO. Wersja i

poziom wydania widoczne są w nagłówku każdej strony.
Wersja 4.0 niniejszego dokumentu stanowi kontynuację i zastępuje poprzednie Podręczniki obsługi posiadające następujące kody:

- ICERT-INDI-MO, wersja 3.5 z dnia 30.11.2018 r. dotycząca wydawania kwalifikowanych certyfikatów dla osób fizycznych za pośrednictwem systemu CMS
- ICERT-INDI-MO-ENT, wersja 3.5 z dnia 30.11.2018 r. dotycząca wydawania dla osób fizycznych kwalifikowanych certyfikatów typu LongTerm i OneShot,

opisując w jednym dokumencie zasady i procedury zarządzania certyfikatami kwalifikowanymi zgodnie z rozporządzeniem eIDAS [1].
Do dokumentu przypisane są opisane poniżej identyfikatory obiektu (Object Identifier – OID), do których odwołanie znajduje się w rozszerzeniu Certificate Policy certyfikatów, zgodnie z ich przeznaczeniem użytkowym. Znaczenie OID jest następujące:

Identyfikatorem obiektu (OID) identyfikującym InfoCert jest 1.3.76.36. Polityki dotyczące certyfikatów kwalifikowanych są następujące:

Opis	**OID**
Podręcznik obsługi dla certyfikatu kwalifikowanego wydawanego osobie fizycznej	1.3.76.36.1.1.48.1 zgodna z polityką QCP-n 0.4.0.194112.1.0
Podręcznik obsługi dla certyfikatu kwalifikowanego wydawanego osobie fizycznej i kluczy na urządzeniu (SSCD)	1.3.76.36.1.1.48.2 zgodna z polityką QCP-n 0.4.0.194112.1.0
Podręcznik obsługi dla certyfikatu kwalifikowanego wydawanego osobie prawnej również na urządzeniu (SSCD) Dostępny również dla PSD2 (QSealC)	1.3.76.36.1.1.47 zgodna z polityką QCP-l 0.4.0.194112.1.1

Polityki dotyczące certyfikatów kwalifikowanych na urządzeniu kwalifikowanym są następujące:

Opis	OID
Podręcznik obsługi dla certyfikatu kwalifikowanego wydawanego osobie fizycznej i kluczy na urządzeniu kwalifikowanym (QSCD)	1.3.76.36.1.1.1/1.3.76.36.1.1.61 zgodna z polityką QCP-n-qscd 0.4.0.194112.1.2
Podręcznik obsługi dla certyfikatu kwalifikowanego wydawanego osobie fizycznej do automatycznego zdalnego podpisu na urządzeniu kwalifikowanym (QSCD)	1.3.76.36.1.1.2/1.3.76.36.1.1.62 zgodna z polityką QCP-n-qscd 0.4.0.194112.1.2
Podręcznik obsługi dla certyfikatu kwalifikowanego wydawanego osobie fizycznej do zdalnego podpisu na urządzeniu kwalifikowanym (QSCD)	1.3.76.36.1.1.22/1.3.76.36.1.1.63 zgodna z polityką QCP-n-qscd 0.4.0.194112.1.2
Podręcznik obsługi dla certyfikatu kwalifikowanego wydawanego osobie fizycznej za pośrednictwem systemu CMS na urządzeniu kwalifikowanym (QSCD)	1.3.76.36.1.1.32/1.3.76.36.1.1.66 zgodna z polityką QCP-n-qscd 0.4.0.194112.1.2
Podręcznik obsługi dla certyfikatu kwalifikowanego wydawanego osobie prawnej na urządzeniu (QSCD) Dostępna również dla PSD2 (QSealC)	1.3.76.36.1.1.46 zgodna z polityką QCP-l-qscd 0.4.0.194112.1.3
Podręcznik obsługi dla certyfikatu kwalifikowanego wydawanego osobie fizycznej do zdalnego podpisu na na urządzeniu kwalifikowanym (QSCD) typu LongTerm	1.3.76.36.1.1.35/1.3.76.36.1.1.65 zgodna z polityką QCP-n-qscd 0.4.0.194112.1.2
Podręcznik obsługi dla certyfikatu kwalifikowanego wydawanego osobie fizycznej do zdalnego podpisu na na urządzeniu kwalifikowanym (QSCD) typu OneShot	1.3.76.36.1.1.34/1.3.76.36.1.1.64 zgodna z polityką QCP-n-qscd 0.4.0.194112.1.2

Podręcznik obsługi dla certyfikatu kwalifikowanego „Obywatela Hiszpanii” wydawanego osobie fizycznej i kluczy na urządzeniu kwalifikowanym (QSCD)	1.3.76.36.1.1.10.16.1.1.1 zgodna z polityką QCP-n-qscd 0.4.0.194112.1.2

Poniżej zostały wymienione polityki dotyczące wydawania kwalifikowanych certyfikatów na urządzeniu kwalifikowanym określone wraz z ustawieniami użycia kluczy typu B lub F, jak określono w punkcie 4.3.2 normy ETSI EN 319 412-2. Ponieważ połączenie bitu niezaprzeczalności z bitami

podpisu cyfrowego i szyfrowania klucza może mieć wpływ na bezpieczeństwo, używanie tych OID jest ograniczone i każdy wniosek jest rozpatrywany osobno.

Opis	OID
Podręcznik obsługi dla certyfikatu kwalifikowanego wydawanego osobie fizycznej i kluczy na urządzeniu kwalifikowanym (QSCD) z ustawieniami użycia kluczy typu B lub F	1.3.76.36.1.1.61.1 zgodna z polityką QCP-n-qscd 0.4.0.194112.1.2
Podręcznik obsługi dla certyfikatu kwalifikowanego wydawanego osobie fizycznej do zdalnego podpisu na urządzeniu kwalifikowanym (QSCD) z ustawieniami użycia kluczy typu B lub F	1.3.76.36.1.1.63.1 zgodna z polityką QCP-n-qscd 0.4.0.194112.1.2
Podręcznik obsługi dla certyfikatu kwalifikowanego wydawanego osobie fizycznej do zdalnego podpisu na urządzeniu kwalifikowanym (QSCD) typu LongTerm z ustawieniami użycia kluczy typu B lub F	1.3.76.36.1.1.65.1 zgodna z polityką QCP-n-qscd 0.4.0.194112.1.2
Podręcznik obsługi dla certyfikatu kwalifikowanego wydawanego osobie fizycznej do zdalnego podpisu na urządzeniu kwalifikowanym (QSCD) typu OneShot z ustawieniami użycia kluczy typu B lub F	1.3.76.36.1.1.64.1 zgodna z polityką QCP-n-qscd 0.4.0.194112.1.2

Dodatkowe OID mogą być obecne w certyfikacie w celu wskazania istnienia ograniczeń stosowania. Tego rodzaju OID są wymienione w punkcie 4.5.3. Obecność ograniczeń stosowania nie zmienia w żaden sposób zasad określonych w pozostałej części niniejszego Podręcznik obsługi.
Ponadto, wszystkie certyfikaty zgodne z zaleceniami Decyzji AgID [Agencji ds. Cyfryzacji Włoch] nr 121/2019 wraz z poprawkami późniejszej Decyzji AgID nr 147/2019 [13], z dnia 5 lipca 2019 r. będą zawierać dodatkowy element PolicyIdentifier o wartości agIDcert (OID 1.3.76.16.6) w polu CertificatePolicies (OID 2.5.29.32).[1]Dokument ten jest opublikowany w formie elektronicznej na stronie internetowej Dostawcy usług zaufania pod adresem: https://www.firma.infocert.it lub na

stronie internetowej instytucji: https://www.infocert.it, w zakładce „Dokumentacja”.

---

[1] Brak takiego OID może spowodować, że oferowane usługi sieciowe nie będą odpowiednie dla specyficznego kontekstu włoskiego. Jednym z przykładów jest brak obowiązku podawania w certyfikacie kwalifikowanym do generowania podpisu kodu identyfikacji podatkowej posiadacza, co jest niezbędne dla wielu włoskich organów administracji publicznej.

1.3 Uczestnicy i ich obowiązki

1.3.1 Certification Authority – Urząd certyfikacji

Urząd certyfikacji (CA, ang. Certification Authority) jest zaufanym podmiotem trzecim, który wydaje kwalifikowane certyfikaty kwalifikowanego podpisu elektronicznego, podpisując je własnym kluczem prywatnym, zwanym kluczem CA lub kluczem root.
InfoCert jest urzędem certyfikacji (dalej zwanym po prostu **CA**), który
wydaje, publikuje w rejestrze i unieważnia certyfikaty kwalifikowane, działając zgodnie z przepisami technicznymi wydanymi przez organ nadzoru oraz zgodnie z wytycznymi Rozporządzenia eIDAS [1] i z włoskim kodeksem administracji cyfrowej [2].

Pełne dane organizacji pełniącej funkcję CA są następujące:

Nazwa firmy: InfoCert – spółka akcyjna – Spółka podlegająca zarządowi i koordynacji Tinexta S.p.A.
Siedziba statutowa: Piazza Sallustio n. 9, 00187 Rzym (RM)
Siedziby operacyjne:

- Via Marco e Marcelliano n. 45, 00147 Rzym (RM)
- Via Fernanda Wittgens n. 2, 20123 Mediolan (MI)
- Piazza Luigi da Porto n. 3, 35131 Padwa (PD)

Przedstawiciel prawny: Danilo Cattaneo jako pełnomocny członek zarządu
Numer telefonu: 06 836691
Numer identyfikacji podatkowej i numer wpisu do Rejestru Przedsiębiorstw: 07945211006
Numer wpisu do Rejestru Gospodarczo-Administracyjnego (REA): RM – 1064345
Numer VAT: 07945211006
Strona internetowa: https://www.infocert.it

1.3.2 Registration authority – Punkt rejestracji (RA)

Punkty rejestracji (RA, ang. Registration Authority) (dalej zwane po prostu **„RA”**) to podmioty, którym CA udzielił określonego umocowania z prawem do reprezentacji, w którym powierza wykonywanie jednej lub więcej czynności właściwych
dla procesu rejestracji, takich jak na przykład:

- identyfikacja posiadacza lub wnioskodawcy,
- rejestrowanie danych posiadacza,
- przekazywanie danych posiadacza do systemów CA,
- przyjmowanie wniosku o wydanie certyfikatu kwalifikowanego,

- dystrybucja i/lub inicjalizacja bezpiecznego urządzenia do składania podpisu, o ile zostało przewidziane,
- uruchomienie procedury certyfikacji klucza publicznego,

- udzielanie wsparcia posiadaczowi, wnioskodawcy i CA na wszystkich etapach odnawiania, unieważniania lub zawieszania certyfikatów.

Punkt rejestracji zasadniczo wykonuje wszystkie czynności związane z kontaktami między urzędem certyfikacji a posiadaczem lub wnioskodawcą, zgodnie z zawartymi porozumieniami. Umocowanie z prawem do reprezentacji reguluje rodzaj działalności powierzonej RA przez CA oraz procedury operacyjne jej wykonywania.
RA aktywowane są przez CA po odpowiednim przeszkoleniu zatrudnionego personelu. CA sprawdza zgodność stosowanych procedur z postanowieniami niniejszego dokumentu.

1.3.2.1 Operator punktu rejestracji

RA może wyznaczyć, przy użyciu odpowiednich formularzy, osoby fizyczne lub prawne, którym powierza wykonywanie czynności związanych z identyfikacją posiadacza. **Operatorzy punktu rejestracji** lub Registration Authority Officer działają na podstawie
instrukcji otrzymanych od RA, któremu podlegają i którego zadaniem jest nadzorowanie poprawności wdrożonych procedur. W dalszej części niniejszego dokumentu podmioty te będą określane wyłącznie jako operatorzy punktu rejestracji.

1.3.3 Posiadacz

Posiadaczem jest osobą fizyczną lub prawną będącą posiadaczem certyfikatu kwalifikowanego, do którego wprowadzone są podstawowe dane identyfikacyjne. W niektórych częściach niniejszego Podręcznika obsługi w niektórych ograniczeniach stosowania może być również zdefiniowany jako posiadacz certyfikatu.

1.3.4 Użytkownik

Jest to podmiot, który otrzymuje dokument elektroniczny podpisany certyfikatem cyfrowym posiadacza i który opiera się na ważności samego certyfikatu (i/lub na kwalifikowanym podpisie elektronicznym, który w nim występuje) w celu dokonania oceny poprawności i ważności dokumentu w kontekstach, w których jest on używany.

1.3.5 Wnioskodawca

Jest to osoba fizyczna lub prawna, która występuje do CA o wydanie certyfikatów cyfrowych dla posiadacza, ewentualnie ponosząc odnośne koszty, i której przysługuje prawo do zawieszenia lub unieważnienia takich certyfikatów. Rola ta, o ile jest przewidziana, może być również pełniona przez RA.
W szczególności określono następujące przypadki:

- może pokrywać się z posiadaczem, o ile jest on osobą fizyczną,

- może to być osoba fizyczna, która jest uprawniona do ubiegania się o certyfikat dla osoby prawnej,
- może to być osoba prawna ubiegająca się o certyfikat dla osób fizycznych związanych z nią stosunkami handlowymi lub w ramach organizacji,
- może to być rodzic lub opiekun prawny w przypadku osoby niepełnoletniej w wieku powyżej 14 lat.

Wnioskodawcą może być osoba fizyczna lub prawna, od której pochodzą uprawnienia do reprezentacji i rola posiadacza. W tym przypadku, w którym wnioskodawca określany jest również jako *zainteresowana strona trzecia*, certyfikat powinien zawierać wskazanie organizacji, z którą posiadacz jest powiązany, i/lub roli.
O ile w dokumentacji umownej nie określono inaczej, wnioskodawca jest tożsamy z posiadaczem.

1.3.6 Organy

1.3.6.1 Agencja ds. Cyfryzacji Włoch – AgID

Agencja ds. Cyfryzacji Włoch (**AgID**) jest organem nadzoru dostawców usług zaufania, zgodnie z art. 17 Rozporządzenia eIDAS. W tym charakterze AgID nadzoruje dostawców kwalifikowanych usług zaufania mających siedzibę na terenie Włoch w celu zagwarantowania, że spełniają one wymogi ustanowione w rozporządzeniu.

1.3.6.2 Jednostka oceniająca zgodność – Conformity Assessment Body

Jednostka oceniająca zgodność (**CAB**, ang. Conformity Assessment Body) jest organem akredytowanym zgodnie z Rozporządzeniem eIDAS, właściwym do przeprowadzania oceny zgodności kwalifikowanego dostawcy usług zaufania i świadczonych przez niego kwalifikowanych usług zaufania z obowiązującymi przepisami i normami.

1.3.6.3 Właściwy organ krajowy (NCA)

W przypadku PSD2 [11], krajowy organ nadzoru pośredników finansowych jest organem odpowiedzialnym za udzielanie zezwolenia PSP w każdym państwie członkowskim. Jeżeli zezwolenie zostało udzielone, właściwy organ krajowy (dalej zwany po prostu „**NCA**”) wydaje numer zezwolenia i publikuje tę informację w swoich rejestrach publicznych.

1.3.6.4 Europejski Urząd Nadzoru Bankowego (EBA)

Europejski Urząd Nadzoru Bankowego (dalej zwany po prostu „**EBA**”) działa w celu zapewnienia określonego poziomu regulacji i jednolitego nadzoru w

europejskim sektorze bankowym. W przypadku PSD2 [11], monitoruje i zapewnia przejrzystość działalności dostawców usług płatniczych (PSP), którzy uzyskali zezwolenie od NCA właściwych dla każdego państwa członkowskiego. Jest on odpowiedzialny za opracowanie i obsługę „Elektronicznego centralnego rejestru", w którym każdy NCA musi publikować listę nazwisk i informacji dotyczących uprawnionych podmiotów.

1.4 Zastosowanie certyfikatu

1.4.1 Dopuszczalne zastosowania

Certyfikaty wydawane przez CA InfoCert, zgodnie z trybami wskazanymi w niniejszej Polityce, są certyfikatami kwalifikowanymi w rozumieniu przepisów CAD i rozporządzenia eIDAS.
Certyfikat wydany przez CA będzie wykorzystywany do weryfikacji kwalifikowanego podpisu lub pieczęci elektronicznej posiadacza, do którego należy certyfikat.
CA InfoCert udostępnia do weryfikacji podpisów kilka produktów dostępnych na stronie internetowej InfoCert. Na rynku mogą być dostępne inne produkty do weryfikacji, z funkcjami i ograniczeniami wskazanymi przez dostawcę.

1.4.2 Niedozwolone zastosowania

Zabronione jest korzystanie z certyfikatu w sposób wykraczający poza ograniczenia i zakres stosowania określony w niniejszej Polityce i w umowach, a w każdym przypadku w sposób naruszający ograniczenia stosowania i limity kwotowe (*key usage*, *extended key usage, user notice*) wskazane w certyfikacie.

1.5 Zarządzanie Podręcznikiem obsługi

1.5.1 Dane kontaktowe

InfoCert jest odpowiedzialna za opracowanie, publikację i aktualizację niniejszego dokumentu. Pytania, reklamacje, uwagi i prośby o udzielenie wyjaśnień dotyczące niniejszego Podręcznika obsługi należy kierować na adres i do osoby, które zostały wskazane poniżej:

InfoCert S.p.A.
Responsabile del Servizio di Certificazione Digitale
(Kierownik ds. usług certyfikacyjnych) Piazza Luigi da
Porto n.3
35131 Padwa

Telefon: 06 836691
Call Center: consultare il link https://help.infocert.it/contatti/ w celu uzyskania szczegółowych informacji strona internetowa: https://www.firma.infocert.it, https://www.infocert.it
e-mail: firma.digitale@legalmail.it

Posiadacz lub wnioskodawca mogą żądać wydania kopii dotyczącej ich dokumentacji poprzez wypełnienie i wysłanie formularza dostępnego na stronie internetowej www.firma.infocert.it oraz zastosowanie się do wskazanej procedury. Dokumentacja zostanie przesłana w formie elektronicznej, na adres e-mail podany w formularzu.

1.5.2 Podmioty odpowiedzialne za zatwierdzenie Podręcznika obsługi

Niniejszy Podręcznik obsługi jest weryfikowany przez kierownika ds. bezpieczeństwa i polityk, kierownika ds. ochrony danych osobowych, kierownika ds. usług certyfikacyjnych, kierownika ds. prawnych i kierownika odpowiedzialnego za kwestie regulacyjne oraz zatwierdzany przez zarząd firmy.

1.5.3 Procedury zatwierdzania

Podręcznik obsługi jest sporządzany i zatwierdzany zgodnie z procedurami przewidzianymi w
Systemie zarządzania jakością w przedsiębiorstwie według normy ISO 9001:2015.
Nie częściej niż raz w roku, dostawca usług zaufania sprawdza zgodność niniejszego Podręcznika obsługi z własnym procesem świadczenia usług certyfikacyjnych.

1.6 Definicje i skróty

1.6.1 Definicje

Poniżej podano definicje terminów użytych przy sporządzaniu niniejszego dokumentu. W celu zrozumienia znaczenia terminów zdefiniowanych w rozporządzeniu eIDAS [1] i w CAD [2] należy zapoznać się z odnośnymi definicjami. W stosownych przypadkach w nawiasach kwadratowych podawane jest odpowiednie określenie w języku angielskim, powszechnie używane w publikacjach, normach i dokumentach technicznych.

Termin	Definicja

Samocertyfikacja	Jest to oświadczenie skierowane do CA, złożone osobiście przez podmiot, który będzie posiadaczem certyfikatu cyfrowego, w którym podmiot ten potwierdza określone fakty, cechy lub stan prawny, przyjmując na siebie odpowiedzialność określoną ustawowo.
Termin	**Definicja**
Conformity Assessment Body (jednostka oceniająca zgodność) (CAB)	Jednostka akredytowana zgodnie z rozporządzeniem eIDAS jako właściwa do przeprowadzania oceny zgodności kwalifikowanego dostawcy usług zaufania i świadczonych przez niego kwalifikowanych usług zaufania. Sporządza CAR.
Conformity Assessment Raport (raport z oceny zgodności) (CAR)	Raport, w którym jednostka oceniająca zgodność potwierdza, że dostawca kwalifikowanych usług zaufania i same usługi zaufania spełniają wymogi rozporządzenia (patrz eIDAS [1]).
Card Management System (CMS)	Instrument uwierzytelniania, identyfikacji, gromadzenia i przechowywania danych dotyczących posiadaczy lub wnioskodawców.
Certyfikat podpisu elektronicznego	Poświadczenie elektroniczne, które przyporządkowuje dane służące do walidacji podpisu elektronicznego do danej osoby fizycznej i potwierdza co najmniej imię i nazwisko lub pseudonim tej osoby (patrz eIDAS [1]).
Certyfikat pieczęci elektronicznej	Poświadczenie elektroniczne, które przyporządkowuje dane służące do walidacji pieczęci elektronicznej do danej osoby prawnej i potwierdza nazwę tej osoby (patrz eIDAS [1]).
Kwalifikowany certyfikat podpisu elektronicznego	Certyfikat podpisu elektronicznego, który jest wydawany przez kwalifikowanego dostawcę usług zaufania i spełnia wymogi określone w załączniku I rozporządzenia eIDAS (patrz eIDAS [1]).

Kwalifikowany certyfikat pieczęci elektronicznej (QSealC)	Certyfikat pieczęci elektronicznej, który jest wydawany przez kwalifikowanego dostawcę usług zaufania i spełnia wymogi określone w załączniku III rozporządzenia eIDAS (patrz eIDAS [1]).
Kwalifikowany certyfikat pieczęci elektronicznej dla PSD2 (QSealC PSD2)	QSealC, o którym mowa w art. 34 Rozporządzenia delegowanego (UE) 2018/389 [12], wdrażającego Dyrektywę (UE) 2015/2366 (PSD2) [11], zgodnie z wymogami określonymi w normie ETSI TS 119 495 (określone w dalszej części jako „QSealC PSD2”).

Termin	Definicja
Certyfikat LongTerm	Szczególny kwalifikowany certyfikat kwalifikowanego podpisu elektronicznego do procedury zdalnego podpisywania, którego użycie jest ograniczone wyłącznie do domeny informatycznej, dla której został wydany.
Certyfikat OneShot	Jest to kwalifikowany certyfikat kwalifikowanego podpisu elektronicznego do procedury zdalnego podpisywania regulowany w niniejszej Polityce, którego klucze po wygenerowaniu są dostępne wyłącznie do transakcji złożenia podpisu, do której został on wydany. Natychmiast po użyciu klucz prywatny jest zniszczony. Ta kategoria obejmuje również certyfikaty zwane short-term w ETSI 319 411-1, dla których okres ważności jest krótszy od maksymalnego czasu na złożenie wniosku o unieważnienie jak podano w niniejszym dokumencie.
Klucz certyfikacyjny lub klucz root	Para kluczy kryptograficznych używanych przez CA do podpisywania certyfikatów i list certyfikatów unieważnionych lub zawieszonych.
Klucz prywatny	Element pary kluczy asymetrycznych używany przez posiadacza, za pomocą którego kwalifikowany podpis elektroniczny umieszczany jest na dokumencie informatycznym (patrz CAD [2]).
Klucz publiczny	Element pary kluczy asymetrycznych, który ma być podany do wiadomości publicznej i za pomocą którego weryfikuje się kwalifikowany podpis elektroniczny umieszczony na dokumencie informatycznym przez posiadacza (patrz CAD [2]).
Klient	Podmiot, z którym InfoCert zawarła umowę na dostawę usług za opłatą.
Kod awaryjny (ERC)	Kod bezpieczeństwa przekazywany posiadaczowi w celu złożenia wniosku o zawieszenie certyfikatu na portalach TSP.
Walidacja	Proces weryfikacji i potwierdzania ważności podpisu elektronicznego (patrz eIDAS [1]).
	Dane używane do walidacji podpisu elektronicznego

Termin	Definicja
Dane identyfikujące osobę	Zestaw danych umożliwiających ustalenie tożsamości osoby fizycznej lub prawnej, lub osoby fizycznej reprezentującej osobę prawną (patrz eIDAS [1]).
Dane służące do składania podpisu elektronicznego	Unikalne dane, których podpisujący używa do składania podpisu elektronicznego (patrz eIDAS [1]).
Urządzenie do składania podpisu elektronicznego (SSCD secure system creation device)	Skonfigurowane oprogramowanie lub skonfigurowany sprzęt wykorzystywany do składania podpisu elektronicznego (patrz eIDAS [1]).
Kwalifikowane urządzenie do składania kwalifikowanego podpisu elektronicznego (QSCD)	Urządzenie do składania podpisu elektronicznego, które spełnia wymogi określone w załączniku II rozporządzenia eIDAS (patrz eIDAS [1]).
Dokument elektroniczny	Każda treść przechowywana w postaci elektronicznej, w szczególności tekst lub nagranie dźwiękowe, wizualne lub audiowizualne (patrz eIDAS [1]).
Domena informatyczna	Jest tożsama z aplikacjami, za pośrednictwem których posiadaczowi wydawany jest certyfikat kwalifikowany i w których posiadacz może używać certyfikatu do podpisywania dokumentów elektronicznych. Aplikacje mogą być zarządzane bezpośrednio przez podmiot certyfikujący lub przez wnioskodawcę, a także mogą zawierać dodatkowe szczegółowe przepisy w zależności od procedury identyfikacji przyjętej do wydania kwalifikowanego certyfikatu.
Podpis automatyczny	Szczególna procedura informatyczna podpisu elektronicznego wykonana po uprzednim upoważnieniu podpisującego, który zachowuje wyłączną kontrolę nad swoimi kluczami podpisu, w przypadku braku odpowiedniego i stałego nadzoru z jego strony.

Termin	Definicja
Podpis cyfrowy (digital signature)	Szczególny rodzaj zaawansowanego podpisu elektronicznego opartego na certyfikacie kwalifikowanym i na systemie wzajemnie powiązanych kluczy kryptograficznych, jednego publicznego i jednego prywatnego, który umożliwia odpowiednio posiadaczowi za pomocą klucza prywatnego oraz odbiorcy za pomocą klucza publicznego ujawnienie i weryfikację pochodzenia oraz integralności dokumentu informatycznego lub zestawu dokumentów informatycznych (patrz CAD [2]).
Podpis elektroniczny	Dane w postaci elektronicznej, które są dołączone lub logicznie powiązane z innymi danymi elektronicznymi, i które użyte są przez podpisującego jako podpis (patrz eIDAS [1]).
Zaawansowany podpis elektroniczny	Podpis elektroniczny, który spełnia wymogi określone w art. 26 rozporządzenia eIDAS (patrz eIDAS [1]).
Kwalifikowany podpis elektroniczny	Zaawansowany podpis elektroniczny, który jest składany za pomocą urządzenia do składania kwalifikowanego podpisu elektronicznego i który opiera się na kwalifikowanym certyfikacie do podpisów elektronicznych (patrz eIDAS [1]).
Zdalny podpis	Specjalna procedura kwalifikowanego podpisu elektronicznego lub podpisu cyfrowego, wygenerowanego na urządzeniu HSM, która umożliwia zapewnienie wyłącznej kontroli kluczy prywatnych przez ich posiadaczy.
Podpisujący	Osoba fizyczna, która składa podpis elektroniczny (patrz eIDAS [1]).
Dziennik kontrolny	Zawiera zbiór zapisów, wykonywanych automatycznie lub ręcznie, dotyczących zdarzeń przewidzianych w przepisach technicznych [9].

Identyfikacja elektroniczna	Proces używania danych identyfikujących osobę w formie elektronicznej, w sposób jednoznaczny reprezentujący osobę fizyczną lub prawną lub lub osobę fizyczną reprezentującą osobę prawną (patrz eIDAS [1]).
Termin	**Definicja**
Lista certyfikatów unieważnionych lub zawieszonych (Certificate Revocation List –CRL)	Lista certyfikatów, które straciły ważność przed upływem ich naturalnej daty ważności. Operacja ta nazywana jest unieważnieniem, jeżeli jest trwała, lub zawieszeniem, jeżeli jest tymczasowa. W przypadku unieważnienia lub zawieszenia certyfikatu, jego numer seryjny jest dodawany do listy CRL, która jest następnie publikowana w rejestrze publicznym.
Podręcznik obsługi (certificate practice statement – CPS)	Określa procedury, które CA stosuje przy świadczeniu usługi. Podczas opracowywania Podręcznika obsługi uwzględniono wskazówki podane przez organ nadzoru oraz zawarte w literaturze międzynarodowej.
Środek identyfikacji elektronicznej	Materialna lub niematerialna jednostka zawierająca dane identyfikujące osobę i używana do celów uwierzytelniania dla usługi online (patrz eIDAS [1]).
Online Certificate Status Protocol (OCSP)	Protokół zdefiniowany przez IETF w RFC 6960, umożliwiający aplikacjom szybszą i dokładniejszą weryfikację ważności certyfikatu w porównaniu z listą CRL, z którą współdzieli dane.
One Time Password (OTP)	One-Time Password (hasło jednorazowe) to hasło, które jest ważne tylko dla jednej transakcji. OTP jest generowany i udostępniany posiadaczowi bezpośrednio przed złożeniem kwalifikowanego podpisu elektronicznego. Może opierać się na urządzeniach sprzętowych lub procedurach programowych.

Strona ufająca	Osoba fizyczna lub prawna, która polega na identyfikacji elektronicznej lub usłudze zaufania (patrz eIDAS [1]).
Dostawca usług zaufania	Osoba fizyczna lub prawna, która świadczy jedną usługę zaufania lub więcej takich usług, jako kwalifikowany lub niekwalifikowany dostawca usług zaufania (patrz eIDAS [1]).
Termin	**Definicja**
Kwalifikowany dostawca usług zaufania	Dostawca usług zaufania, który świadczy jedną usługę lub więcej takich usług i któremu organ nadzoru nadał status kwalifikowanego dostawcy usług zaufania (patrz eIDAS [1]).
Produkt	Sprzęt lub oprogramowanie lub odpowiednie komponenty sprzętu lub oprogramowania, które są przeznaczone do wykorzystania w świadczeniu usług zaufania (patrz eIDAS [1]).
Funkcjonariusz publiczny	Podmiot, który w zakresie prowadzonej działalności jest upoważniony przez odnośne prawo do poświadczania tożsamości osób fizycznych.
Rejestr publiczny (Directory)	Archiwum, które zawiera: wszystkie certyfikaty wydane przez CA, o których publikację wnioskował posiadacz; listę certyfikatów unieważnionych i zawieszonych (CRL).
Unieważnienie lub zawieszenie certyfikatu	Czynność, w wyniku której CA unieważnia certyfikat przed upływem jego naturalnej daty ważności.
Rola	Oznacza zasadniczo tytuł i/lub kwalifikacje zawodowe posiadacza, lub wszelkie uprawnienia do reprezentowania osób fizycznych lub podmiotów prawa prywatnego lub publicznego, lub przynależność do takich podmiotów, jak również pełnienie funkcji publicznych.

Usługa zaufania	Usługa elektroniczna zazwyczaj świadczona za wynagrodzeniem i obejmująca następujące elementy: tworzenie, weryfikację i walidację podpisów elektronicznych, pieczęci elektronicznych lub elektronicznych znaczników czasu, usług rejestrowanego doręczenia elektronicznego oraz certyfikatów powiązanych z tymi usługami; lub tworzenie, weryfikację i walidację certyfikatów uwierzytelniania witryn internetowych; lub przechowywanie elektronicznych podpisów, pieczęci lub certyfikatów powiązanych z tymi usługami (patrz eIDAS [1]).
Kwalifikowana usługa zaufania	Usługa zaufania, która spełnia stosowne wymogi określone w rozporządzeniu (patrz eIDAS [1]).
Termin	**Definicja**
Pieczęć elektroniczna	Dane w postaci elektronicznej, które są dołączone lub logicznie powiązane z innymi danymi elektronicznymi, w celu zagwarantowania pochodzenia i integralności tych ostatnich (patrz eIDAS [1]).
Zaawansowana pieczęć elektroniczna	Pieczęć elektroniczna, która spełnia wymogi określone w art. 36 rozporządzenia EIDAS (patrz eIDAS [1]).
Kwalifikowana pieczęć elektroniczna	Zaawansowana pieczęć elektroniczna, która jest składana za pomocą urządzenia do składania pieczęci elektronicznej i która opiera się na kwalifikowanym certyfikacie pieczęci elektronicznych (patrz eIDAS [1]).
Państwo członkowskie	Państwo członkowskie Unii Europejskiej.
Uniwersalny czas koordynowany (Coordinated Universal Time)	Skala czasowa z dokładnością do sekundy, zgodnie z definicją w ITU-R Recommendation TF.460-5.
Elektroniczny znacznik czasu	Dane w postaci elektronicznej, które wiążą inne dane w postaci elektronicznej z określonym czasem, stanowiąc dowód na to, że te inne dane istniały w danym momencie (patrz eIDAS [1]).

Kwalifikowany elektroniczny znacznik czasu	Elektroniczny znacznik czasu spełniający wymogi art. 42 rozporządzenia (patrz eIDAS [1]).
WebCam	Kamera wideo o małych rozmiarach, przeznaczona do strumieniowego przesyłania obrazów przez Internet i przechwytywania obrazów fotograficznych. Podłączona do komputera lub zintegrowana z urządzeniami przenośnymi używana jest do rozmów wideo lub wideokonferencji.

1.6.2 Akronimy i skróty

Akronim	Definicja
AgID	Agenzia per l'Italia Digitale – Agencja ds. Cyfryzacji Włoch – organ nadzoru nad dostawcami usług zaufania
CA	Certification Authority – urząd certyfikacji
CAB	Conformity Assessment Body – jednostka oceniająca zgodność
CAD	Codice dell'Amministrazione Digitale – włoski kodeks administracji cyfrowej
CAR	Conformity Assessment Raport – raport z oceny zgodności
CC	Common Criteria
CIE	Carta di Identità Elettronica – elektroniczny dowód osobisty
CMS	Card Management System – system zarządzania kartami
CNS – TS-CNS	Carta Nazionale dei Servizi – Krajowa karta usług Tessera Sanitaria-Carta Nazionale dei Servizi – Karta ubezpieczenia zdrowotnego- Krajowa karta usług
CRL	Certificate Revocation List – lista unieważnionych certyfikatów
DMZ	Demilitarized Zone – strefa zdemilitaryzowana

DN	Distinguish Name – nazwa wyróżniająca
EAL	Evaluation Assurance Level – poziom uzasadnionego zaufania
EBA	European Banking Authority – Europejski Urząd Nadzoru Bankowego
eID	Electronic Identity – tożsamość elektroniczna
eIDAS	Electronic Identification and Signature Regulation
ERC	Emergency Request Code – kod awaryjny
ETSI	European Telecommunications Standards Institute – Europejski Instytut Norm Telekomunikacyjnych
FIPS	Federal Information Processing Standard – Federalne Standardy Przetwarzania Informacji
HSM	Hardware Secure Module – moduł bezpieczeństwa sprzętu – bezpieczne urządzenie do składania podpisu, z funkcjami podobnymi do funkcji kart elektronicznych, ale o lepszych parametrach pamięci i wydajności
HTTP	HyperText Transfer Protocol
IETF	Internet Engineering Task Force
IR	Incaricato alla Registrazione – Operator punktu rejestracji lub Registration Authority Officer
ISO	International Organization for Standardization – Międzynarodowa Organizacja Normalizacyjna założona w 1946 roku jest międzynarodową organizacją złożoną z krajowych organów normalizacyjnych
ITU	International Telecommunication Union – Międzynarodowy Związek Telekomunikacyjny założony w
Akronim	**Definicja**
	1865 roku jest międzynarodową organizacją zajmującą się ustanawianiem standardów w telekomunikacji
IUT	Identificativo Univoco del Titolare – unikalny identyfikator posiadacza – kod przypisany do posiadacza, który jednoznacznie identyfikuje go przed CA; posiadacz ma różne kody dla każdego posiadanego certyfikatu

LDAP	Lightweight Directory Access Protocol – protokół wykorzystywany do uzyskania dostępu do rejestru certyfikatów
LoA	Level of Assurance – poziom pewności
NCA	National Competent Authority – właściwy organ krajowy
NTR Code	National Trade Register Code – kod krajowego rejestru handlowego
OID	Object Identifier – identyfikator obiektu – składa się z sekwencji liczb, zarejestrowanej zgodnie z procedurą określoną w ISO/IEC 6523, która identyfikuje określony obiekt w ramach danej hierarchii
OTP	OneTime Password – hasło jednorazowe
PEC	Posta Elettronica Certificata – certyfikowana poczta elektroniczna
PIN	Personal Identification Number – osobisty numer identyfikacyjny – numer przypisany do bezpiecznego urządzenia do składania podpisu, używany przez posiadacza w celu uzyskania dostępu do funkcji danego urządzenia
PKCS	Public-Key Cryptography Standards – standardy kryptografii klucza publicznego
PKI	Public Key Infrastructure (infrastruktura klucza publicznego) – zbiór zasobów, procesów i środków technologicznych umożliwiających zaufanym stronom trzecim weryfikację i/lub zagwarantowanie tożsamości danego podmiotu, jak również przypisanie klucza publicznego danemu podmiotowi
PSD2	Payment Services Directive 2 – dyrektywa o usługach płatniczych 2
PSP	Service Payment Provider – dostawca usług płatniczych
QSealC	Qualified electronic Seal Certificate – kwalifikowany certyfikat pieczęci elektronicznej
RA	Registration Authority – Punkt rejestracji
RFC	Request for Comment – prośba o komentarz – dokument zawierający informacje lub specyfikacje dotyczące nowych badań,

Akronim	Definicja
	innowacji i metodologii w dziedzinie IT, przekazany przez autorów do oceny społecznej
RSA	Pochodzi od inicjałów wynalazców algorytmu: River, Shamir, Adleman
SGSI	Sistema di Gestione per la Sicurezza delle Informazioni – System zarządzania bezpieczeństwem informacji
SPID	Sistema Pubblico di Identità Digitale – włoski publiczny system tożsamości cyfrowej
SSCD – QSSCD	Secure Signature Creation Device – bezpieczne urządzenie do składania podpisu elektronicznego Qualified Secure Signature Creation Device – kwalifikowane urządzenie do składania podpisu elektronicznego
TIN	Tax Identification Number – numer identyfikacji podatkowej
UUID	Universally unique identifier – uniwersalny unikalny identyfikator
URL	Uniform Resource Locator – uniwersalny lokalizator zasobów
VAT Code	Value Added Tax Code – numer VAT
X500	Standard ITU-T dla usług LDAP i directory
X509	Standard ITU-T dla PKI

2 PUBLIKACJA I ARCHIWIZACJA

2.1 Archiwizacja

Opublikowane certyfikaty, listy CRL i podręczniki obsługi są publikowane i dostępne 24 godziny na dobę przez 7 dni w tygodniu.

2.2 Publikacja informacji dotyczących certyfikacji

2.2.1 Publikacja Podręcznika obsługi

Niniejszy Podręcznik obsługi, lista certyfikatów kluczy certyfikacyjnych oraz inne wymagane prawem informacje na temat CA publikowane są na liście podmiotów certyfikujących (pod adresem https://eidas.agid.gov.it/TL/TSL-IT.xml) oraz na stronie internetowej urzędu certyfikacji (patrz punkt 1.5.1).

2.2.2 Publikacja certyfikatów

Posiadacz lub wnioskodawca reprezentujący osobę prawną, chcący złożyć wniosek o upublicznienie własnego certyfikatu, może przesłać do InfoCert odpowiedni formularz (dostępny na stronie internetowej www.firma.infocert.it), wypełniony i podpisany cyfrowo kluczem odpowiadającym certyfikatowi, o którego upublicznienie wnioskuje. Wniosek należy wysłać pocztą elektroniczną na adres richiesta.pubblicazione@cert.legalmail.it zgodnie z procedurą opisaną na stronie internetowej. Nie ma takiej możliwości w przypadku certyfikatów LongTerm i OneShot.

2.2.3 Publikacja list certyfikatów unieważnionych i zawieszonych

Listy certyfikatów unieważnionych i zawieszonych publikowane są w publicznym rejestrze certyfikatów dostępnym za pośrednictwem protokołu LDAP lub za pośrednictwem protokołu HTTP pod adresem wskazanym w atrybucie „CRL Distribution Points” (punkty dystrybucji CRL) certyfikatu. Dostęp można uzyskać za pomocą oprogramowania dostarczonego przez CA i/lub korzystając z funkcji występujących w produktach dostępnych na rynku, które obsługują protokół LDAP i/lub HTTP.
Oprócz wyżej wskazanej metody CA może udostępnić inne metody zapoznawania się z listą opublikowanych certyfikatów i ich ważnością.

2.3 Okres lub częstotliwość publikacji

2.3.1 Częstotliwość publikacji Podręcznika obsługi

Podręcznik obsługi publikowany jest, jak wskazano w punkcie 1.5.1 ze zmienną częstotliwością, po wprowadzeniu w niej zmian. Jeśli zmiany są istotne, CA musi zostać skontrolowany przez akredytowaną jednostkę CAB, przedłożyć organowi nadzoru (AgID) raport z oceny zgodności (*CAR – Conformity Assessment Report*) i Podręcznik obsługi oraz poczekać na pozwolenie na publikację.

2.3.2 Częstotliwość publikacji list certyfikatów unieważnionych i zawieszonych

Listy CRL są publikowane co godzinę, jak wskazano w punkcie 2.2.3.

2.4 Kontrola dostępu do archiwów publicznych

Informacje na temat opublikowanych certyfikatów, list CRL i podręczników obsługi są informacjami publicznymi. CA nie ograniczył dostępu do treści do odczytu i wdrożył wszystkie środki zaradcze zapobiegające nieupoważnionym modyfikacjom lub usunięciom.

3 IDENTYFIKACJA I UWIERZYTELNIENIE

3.1 Nazwa

3.1.1 Rodzaje nazw

Posiadacz identyfikowany jest w certyfikacie atrybutem Distinguished Name (DN), który w związku z tym nie może być pusty i musi być zgodny z normą X500. Certyfikaty wydawane są zgodnie z przepisami specyfikacji RFC-5280 i treścią norm ETSI EN 319 412 od 1 do 5.
Jednak normy ETSI EN 319 412-2 punkt 4.2.4 i 319 412-3 punkt 4.2.1 dopuszczają, zarówno w przypadku certyfikatów dla osoby fizycznej, jak i dla osoby prawnej, dłuższą długość niż określona w specyfikacji RFC 5280 dla pól *givenName, surname, commonName.*
Zgodnie z tym odstępstwem ustalono następujące limity: *givenName* i *surname* 40 znaków, *commonName* 81 znaków.

W zależności od kontekstu należy stosować wskazania Decyzji AgID 147/2019 [13] lub innych państw pod warunkiem, że nie są one sprzeczne z rozporządzeniem eIDAS [1].

3.1.2 Konieczność używania nazw znaczących

Atrybut certyfikatu Distinguished Name (DN) jednoznacznie identyfikuje posiadacza, któremu wydawany jest certyfikat.

3.1.3 Anonimowość i pseudonimizacja wnioskodawców

Jedynie w przypadku identyfikacji zgodnie z trybem 1_LiveID (patrz punkt 3.2.3.1) posiadacz ma prawo do zażądania od CA, aby certyfikat zawierał pseudonim zamiast rzeczywistych danych. Nie ma takiej możliwości w przypadku certyfikatów LongTerm i OneShot. Ponieważ certyfikat jest kwalifikowany, CA będzie przechowywać informacje na temat rzeczywistej tożsamości osoby przez co najmniej dwadzieścia (20) lat od daty ważności certyfikatu, do maksymalnie 23 (dwudziestu trzech) lat od daty wydania.

3.1.4 Zasady interpretacji rodzajów nazw

InfoCert spełnia wymagania normy X500.

3.1.5 Jednoznaczność nazw

Posiadacz będący osobą fizyczną:
Aby zapewnić jednoznaczną identyfikację posiadacza, certyfikat musi zawierać imię i nazwisko oraz unikalny kod identyfikacyjny.
Zazwyczaj używany jest Tax Identification Number (TIN). TIN nadawany jest przez organy państwa, którego obywatelem jest posiadacz, lub przez państwo, w którym siedzibę ma organizacja, w której pracuje posiadacz. Dla obywateli włoskich unikalnym kodem identyfikacyjnym jest kod identyfikacji podatkowej.
W przypadku braku TIN lub kodu identyfikacji podatkowej certyfikat może zawierać

- kod identyfikacyjny uzyskany z ważnego dokumentu tożsamości używanego w procedurach potwierdzania tożsamości. Należy stosować format przewidziany w normie ETSI 319 412-1,
- unikalny identyfikator określony przez CA. W tym wypadku używany jest UUID (Identificativo Univoco Universale – uniwersalny unikalny identyfikator) typu 4 opisany w RFC4122,
- unikalny identyfikator opisany w profilu EIDAS eID w ramach EIDAS cooperation network. Dokumentem odniesienia jest „eIDAS SAML AttributeProfileVersion" wer. 1.2. (https://ec.europa.eu/digital-building-blocks/sites/display/DIGITAL/eIDAS+eID+Profile),
- inny unikalny identyfikator przypisany w obrębie izby, stowarzyszenia lub ogólnie własnej organizacji.

Jednakże, ponieważ kod identyfikacji podatkowej jest używany przez wszystkie organy administracji publicznej jako identyfikator obywatela i podatnika, jego brak w certyfikacie podpisu sprawia, że certyfikat nieodpowiedni dla włoskiej administracji publicznej.

Posiadacz będący osobą prawną:
W przypadku osoby prawnej, w celu zapewnienia jednoznacznej identyfikacji posiadacza, certyfikat musi zawierać nazwę organizacji i unikalny kod identyfikacyjny, do wyboru spośród poniższych:

- VAT (Value Added Tax Code)
- NTR (National Trade Register)
- LEI (Legal Entity Identifier) – identyfikator podmiotu prawnego

W przypadku włoskich osób prawnych kod identyfikacyjny wykorzystuje numer identyfikacyjny VAT lub numer w rejestrze handlowym. Jeżeli organizacja nie posiada ani numeru identyfikacyjnego VAT, ani numeru NTR, lecz tylko kod identyfikacji podatkowej można używać dwóch znaków „CF", po których występuje „:IT-" (np. CF:IT-

97735020584), jak przewidziano w Decyzji AgID 147/2019 [13].

W przypadku użycia kodu LEI, w rozszerzeniu country code (kod państwa) certyfikatu należy podać „XG” zgodnie z normą ETSI 319 412-1.
Ponadto stwierdza się, że możliwe są wyjątki w przypadku wydawania certyfikatów dotyczących poszczególnych układów.

3.1.6 Potwierdzanie tożsamości, uwierzytelnianie i rola zarejestrowanych znaków towarowych

Wnioskując do CA o wydanie certyfikatu, posiadacz i wnioskodawca gwarantują, że ich działalność jest całkowicie zgodna z krajowymi i międzynarodowymi przepisami dotyczącymi własności intelektualnej.
W commonName certyfikatu pieczęci można użyć zarejestrowanego znaku towarowego.
CA nie weryfikuje wykorzystania znaków towarowych, dlatego posiadacz i wnioskodawca przyjmują pełną odpowiedzialność za korzystanie z zarejestrowanych znaków towarowych w ramach certyfikatu.
CA może ponadto odmówić wygenerowania lub zażądać unieważnienia certyfikatu będącego przedmiotem sporu.

3.2 Wstępna walidacja tożsamości

W niniejszym rozdziale opisano procedury stosowane w celu identyfikacji posiadacza lub
wnioskodawcy w momencie składania wniosku o wydanie certyfikatu kwalifikowanego.
Procedura identyfikacji prowadzi do uznania posiadacza przez CA, również za pośrednictwem RA lub jego operatora, który sprawdzi jego tożsamość za pomocą jednej z metod określonych w niniejszej Polityce.

3.2.1 Metoda udowodnienia posiadania klucza prywatnego

InfoCert ustala, że wnioskodawca posiada lub kontroluje klucz prywatny odpowiadający kluczowi publicznemu, który ma być certyfikowany, weryfikując podpis we wniosku o certyfikat za pomocą klucza prywatnego odpowiadającego kluczowi publicznemu, który ma być certyfikowany.

3.2.2 Uwierzytelnienie tożsamości organizacji

Wniosek o certyfikat dla osoby prawnej musi być złożony przez osobę fizyczną zidentyfikowaną w jeden ze sposobów opisanych w punkcie 3.2.3.
Powinien również przedłożyć dokumentację dotyczącą osoby prawnej oraz dokumentację potwierdzającą uprawnienie do składania wniosku w imieniu osoby prawnej.

Osoba prawna może być dostawcą usług płatniczych (PSP) objętym zakresem dyrektywy PSD2.

CA weryfikuje nazwę organizacji i jej istnienie, korzystając z rządowych lub zewnętrznych baz danych lub poprzez bezpośrednie kontakty z podmiotem nadzorującym tworzenie i uznawanie podmiotów prawnych w państwie, w którym organizacja ma siedzibę.

W szczególności,

- w przypadku prywatnych włoskich lub zagranicznych przedsiębiorstw, weryfikacje opierają się na wypisach uzyskanych z rejestru handlowego, w którym zarejestrowany jest podmiot prawny. Dostęp do danych z rejestrów handlowych jest udostępniany za pośrednictwem usługi świadczonej przez Innolva do przeglądania rejestru handlowego za pomocą linku: https://areainterna.assicom.com/area_interna/ lub za pomocą portalu https://e-justice.europa.eu/content_business_registers_in_member_states-106-en.do;
- w przypadku włoskich organów administracji publicznej, weryfikacje prowadzone są za pomocą portalu IPA https://indicepa.gov.it/ipa-portale/.

3.2.3 Uwierzytelnienie osoby fizycznej

Bez uszczerbku dla odpowiedzialności CA, tożsamość posiadacza może zostać ustalona przez podmioty upoważnione do potwierdzania tożsamości, z wykorzystaniem następujących procedur zgodnych z treścią art. 24 eIDAS:

Tryb	Podmioty upoważnione do przeprowadzania identyfikacji	Narzędzia uwierzytelniania wspierające fazę identyfikacji
1 LiveID	• Urząd certyfikacji (CA) • Punkt rejestracji (RA) • Operator punktu rejestracji • Funkcjonariusz publiczny • Pracodawca, w zakresie identyfikacji własnych pracowników, współpracowników, agentów	Nie dotyczy
2 AMLID	• Adresaci obowiązków w zakresie przeciwdziałania praniu pieniędzy zgodnie z przepisami transponującymi dyrektywę 2005/60/WE Parlamentu Europejskiego i Rady w sprawie przeciwdziałania korzystaniu z systemu finansowego w celu prania pieniędzy oraz finansowania ter roryzmu, wraz z późniejszymi wspólnotowymi przepisami wykonawczymi	Nie dotyczy
3 SignID	• Urząd certyfikacji (CA) • Punkt rejestracji (RA) • Operator punktu rejestracji	Używanie kwalifikowanego podpisu elektronicznego wydanego przez kwalifikowanego dostawcę usług zaufania

4 AutID	• Urząd certyfikacji (CA) • Punkt rejestracji (RA) • Operator punktu rejestracji	Wykorzystanie istniejącego środka identyfikacji elektronicznej

Tryb	Podmioty upoważnione do przeprowadzania identyfikacji	Narzędzia uwierzytelniania wspierające fazę identyfikacji
5.1 VideoID z udziałem operatora (attended)	• Urząd certyfikacji (CA) • Punkt rejestracji (RA) • Operator punktu rejestracji	Nie dotyczy
5.2 VideoID bez udziału operatora (unattended)	• Urząd certyfikacji (CA) • Punkt rejestracji (RA) • Operator punktu rejestracji	Nie dotyczy
5.3 VideoID półautomatyczne (SelfQ)	• Urząd certyfikacji (CA) • Punkt rejestracji (RA) • Operator punktu rejestracji	Nie dotyczy
6 eDocId	• Urząd certyfikacji (CA) • Punkt rejestracji (RA) • Operator punktu rejestracji	Wykorzystanie istniejącego środka identyfikacji elektronicznej
7 ContoID	• Urząd certyfikacji (CA)	Strong Customer Authentication – silne uwierzytelnianie klienta w celu uzyskania dostępu do konta bankowego

W Aneksie [14] wymieniono włoskie i zagraniczne dokumenty tożsamości uznawane za dopuszczalne do celów prawidłowej identyfikacji posiadacza w ramach procesów wydawania kwalifikowanych certyfikatów podpisu elektronicznego.

3.2.3.1 Potwierdzanie tożsamości zgodnie z trybem 1 – LiveID

Tryb identyfikacji **LiveID** przewiduje osobiste spotkanie posiadacza z jednym z podmiotów upoważnionych do potwierdzania tożsamości.
Posiadacz okazuje specjalnie przeszkolonej i upoważnionej przez CA osobie jeden lub więcej oryginalnych i ważnych dokumentów tożsamości, znajdujących się na liście akceptowanych dokumentów, opublikowanej na stronie internetowej CA: https://www.firma.infocert.it lub na stronie internetowej instytucji:

https://www.infocert.it[2].

W celu zagwarantowania jednoznacznej identyfikacji posiadacza i jego nazwy, musi on również

posiadać unikalny kod identyfikacyjny, o którym mowa w punkcie 3.1.5 Podmiot uprawniony

[2] Lista akceptowanych dokumentów identyfikacyjnych sporządzana jest przez CA po przeanalizowaniu dokumentów i ich obiektywnych cech gwarantujących pewność tożsamości i bezpieczeństwo w procesie wydawania przez organy wydające. Lista jest przekazywana do AgID i aktualizowana po każdej zmianie.

do potwierdzania tożsamości może zażądać okazania dokumentacji potwierdzającej posiadanie takiego unikalnego kodu identyfikacyjnego w przypadku stwierdzenia niezgodności z deklaracją wnioskodawcy.
Punkty rejestracji działające za granicą, lub które w każdym razie identyfikują posiadaczy mieszkających za granicą, mogą być upoważnione przez InfoCert do akceptowania dokumentów tożsamości wydanych przez organy państw należących do Unii Europejskiej, znajdujących się na liście akceptowanych dokumentów, opublikowanej na stronie internetowej CA https://www.firma.infocert.it lub na stronie internetowej instytucji: https://www.infocert.it.
Identyfikacji może również dokonać funkcjonariusz publiczny, zgodnie z przepisami regulującymi jego działalność. Posiadacz wypełnia wniosek o wydanie certyfikatu i podpisuje go przed funkcjonariuszem publicznym, uwierzytelniając swój podpis zgodnie z obowiązującymi przepisami. Wniosek jest następnie składany do CA w jednym ze związanych umową punktów rejestracji. Szczególna identyfikacja LiveID, po uprzedniej weryfikacji procedur operacyjnych w zakresie identyfikacji i uwierzytelniania, jest przeprowadzana przez pracodawcę w celu zawarcia umowy o pracę i określana jest jako Employee ID. Podobnie uznawana jest za ważną, zgodnie z opisanym poniżej trybem potwierdzania tożsamości, identyfikacja przeprowadzana przez pracodawcę w ramach nawiązania stosunków agencyjnych, po uprzedniej weryfikacji procedur operacyjnych identyfikacji i uwierzytelniania.
Ten tryb identyfikacji przewiduje udzielenie przez CA umocowania z prawem do reprezentacji pracodawcy, który występuje zatem w charakterze punktu rejestracji RA[3].
Certyfikaty wydane zgodnie z tym trybem identyfikacji mogą być używane wyłącznie do celów służbowych, dla których zostały wydane, i są objęte określonym ograniczeniem stosowania.
Dane rejestracyjne do identyfikacji w trybie LiveID przechowywane są przez CA w formacie analogowym lub elektronicznym.

3.2.3.2 *Potwierdzanie tożsamości zgodnie z trybem 2 – AMLID*

W **trybie 2 – AMLID** CA korzysta z identyfikacji dokonywanej przez jednego z adresatów obowiązków w zakresie identyfikacji i odpowiedniej weryfikacji, zgodnie z obowiązującymi w danym okresie przepisami transponującymi dyrektywę 2005/60/WE Parlamentu Europejskiego i Rady w sprawie przeciwdziałania korzystaniu z systemu finansowego w celu prania pieniędzy oraz finansowania terroryzmu, wraz z późniejszymi wspólnotowymi przepisami aktualizującymi i wykonawczymi.

[3] Przed udzieleniem umocowania CA dokonuje dokładnej oceny bezpieczeństwa procedur identyfikacji pracownika oraz trybu przypisywania i zarządzania narzędziami identyfikacji osobistej do systemów informatycznych, do których pracownik (lub agent lub emerytowany pracownik) uzyskuje dostęp w celu wnioskowania do CA o certyfikat podpisu cyfrowego.

W kontekście Włoch posiadacz podaje dane wykorzystywane do potwierdzania tożsamości w myśl [włoskiego] dekretu ustawodawczego 231/2007 z późniejszymi zmianami i uzupełnieniami, zgodnie z którym klienci zobowiązani są do dostarczenia – na własną odpowiedzialność – wszelkich aktualnych i niezbędnych informacji, aby umożliwić adresatom obowiązków wywiązanie się z obowiązków w zakresie identyfikacji klientów.
Ten tryb identyfikacji przewiduje udzielenie przez CA umocowania z prawem do reprezentacji adresatowi obowiązków, który występuje zatem w charakterze RA. Dane identyfikacyjne posiadacza zgromadzone w momencie potwierdzania tożsamości są zazwyczaj przechowywane przez CA w formie elektronicznej i mogą być również przechowywane w formie analogowej.

3.2.3.3 Potwierdzanie tożsamości zgodnie z trybem 3 – SignID

W **trybie 3 SignID** CA InfoCert opiera się na potwierdzaniu tożsamości przeprowadzonym już przez inny CA wydający certyfikaty kwalifikowane (QTSP)**.** Posiadacz posiada już ważny certyfikat kwalifikowany, który wykorzystuje w stosunku do InfoCert. W takim przypadku dane rejestracyjne przechowywane są wyłącznie w formacie elektronicznym.
Wniosek o certyfikat może być złożony w trybie SignID wyłącznie wtedy, gdy certyfikat kwalifikowany używany do podpisania takiego wniosku nie został z kolei wydany w trybie SignID.

3.2.3.4 Potwierdzanie tożsamości zgodnie z trybem 4 – AUTID

W **trybie 4 AutID** CA opiera się na istniejącym środku identyfikacji elektronicznej, który nie wygasł, nie został unieważniony ani zawieszony:

- notyfikowanym przez państwo członkowskie w myśl art. 9 rozporządzenia eIDAS, o *wysokim* poziomie bezpieczeństwa;
- notyfikowanym przez państwo członkowskie w myśl art. 9 rozporządzenia eIDAS, o *średnim* poziomie bezpieczeństwa pod warunkiem, że zapewnia on pewność równoważną pod względem wiarygodności fizycznej obecności;
- nienotyfikowanym i wydanym przez organ publiczny lub podmiot prywatny, pod warunkiem, że zapewnia on pewność równoważną obecności fizycznej pod względem wiarygodności, oraz że została ona potwierdzona przez jednostkę oceniającą zgodność;
- wydanym przez organ publiczny lub podmiot prywatny, następnie potwierdzonym przez posiadacza poprzez uwierzytelnienie dostępu do jego rachunku płatniczego wykonane za pomocą silnego uwierzytelnienia (Strong Customer Authentication – SCA) przez dostawcę usług płatniczych (Payment Service Provider – PSP), zgodnie z Dyrektywą (UE) 2015/2366 (PSD2).

Ze szczególnym uwzględnieniem ram interoperacyjności określonych w art. 12

Rozporządzenia eIDAS, wiadomość zwrócona przez węzeł EIDAS z tytułu korzystania z notyfikowanego krajowego systemu identyfikacji, co najmniej o średnim poziomie, uznaje się za wystarczającą do wydania certyfikatu kwalifikowanego. Wiadomość typu SAML przewidziana w specyfikacjach CEF (Connecting Europe Facility – Instrument „Łącząc Europę") ramach programu CEF eID[4], i wysłany do CA przez administratora węzła krajowego lub przez jeden z podmiotów upoważnionych do korzystania z tego węzła. CA sprawdza integralność otrzymanej wiadomości SAML i uważa podmiot za zidentyfikowany na podstawie danych zawartych w tej wiadomości.

W kontekście Włoch są to środki identyfikacji elektronicznej takie jak CNS (Krajowa karta usług) lub TS-CNS (Karta ubezpieczenia zdrowotnego – Krajowa karta usług), CIE (elektroniczny dowód osobisty), elektroniczne pozwolenie na pobyt oraz tożsamości wydane w kontekście systemu SPID.

Środki identyfikacji elektronicznej, z których może korzystać CA i RA, wymienione są na liście opublikowanej na stronie internetowej CA i zgłoszonej do AgID.
InfoCert oceni możliwość skorzystania z identyfikacji przeprowadzonych przez posiadaczy posiadających certyfikację wydaną przez CAB poświadczającą, że zastosowany tryb identyfikacji jest zgodny z art. 24 lit. d) eIDAS.

W takim przypadku dane rejestracyjne przechowywane są wyłącznie w formacie elektronicznym.

3.2.3.5 Potwierdzanie tożsamości zgodnie z trybem 5 – VideoID

W **trybie 5 VideoID** wymagane jest, aby posiadacz posiadał urządzenie umożliwiające połączenie z Internetem (komputer, smartfon, tablet itp.), kamerę internetową oraz działający system audio.

Tryb identyfikacji 5 – VideoID można skonfigurować ewentualnie:

5.1 W obecności operatora punktu rejestracji i posiadacza lub wnioskodawcy w ramach tej samej sesji audiowizualnej (VideoID z udziałem operatora); odpowiednio przeszkolony operator punktu rejestracji sprawdza tożsamość posiadacza lub wnioskodawcy poprzez dopasowanie jednego lub kilku ważnych dokumentów identyfikacyjnych zawierających aktualne wyraźne zdjęcie i umieszczonych na liście akceptowanych dokumentów opublikowanych na stronie internetowej CA[5].

[4] Specyfikacje te są dostępne pod adresem: https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/eIDAS+eID+Profile
[5] Lista akceptowanych dokumentów identyfikacyjnych sporządzana jest przez CA po przeanalizowaniu dokumentów i ich obiektywnych cech
gwarantujących pewność tożsamości i bezpieczeństwo w procesie wydawania przez organy wydające. Lista jest przekazywana

5.2 Bez równoczesnej obecności operatora punktu rejestracji i posiadacza lub wnioskodawcy w ramach sesji audiowizualnej. W tej konfiguracji, posiadacz samodzielnie przeprowadza sesję audiowizualną, a ponadto w celu potwierdzenia swojej tożsamości wysyła transakcję bankową z rachunku bieżącego, którego jest właścicielem lub współwłaścicielem, wskazując w opisie specjalny kod powiązania przekazany przez CA lub RA. Następnie na etapie backoffice, operator punktu rejestracji ogląda sesję audiowizualną, sprawdza zbieżność między beneficjentem przelewu i danymi posiadacza a prawidłowością kodu powiązania, i w przypadku pozytywnego wyniku kontroli zatwierdza tożsamość (VideoID bez udziału operatora).

5.3 Bez równoczesnej obecności operatora punktu rejestracji i posiadacza lub wnioskodawcy w ramach sesji audiowizualnej, z użyciem zautomatyzowanych narzędzi walidacji (SelfQ). W tej konfiguracji, posiadacz otrzymuje instrukcje w ramach procedury pobierania kopii dokumentu tożsamości i automatycznej procedury fotografowania twarzy (tzw. „wideo selfie"), w trakcie której wykonuje losowe czynności wzmacniające. CA stosuje technologie weryfikacji dokumentów w celu ustalenia autentyczności przedłożonego dokumentu tożsamości, pozyskuje z niego dane i zdjęcie oraz sprawdza jego rzeczywistą przynależność do posiadacza, przy użyciu jednej lub kilku technologii biometrycznych porównujących zdjęcie pozyskane z pobranym wideo selfie. Jeśli wskaźnik zgodności (tzw. „scoring") nie osiągnął wystarczających wartości, operator punktu rejestracji przeprowadza kolejny etap weryfikacji tożsamości w backoffice.

Ponadto, identyfikacja wideo może nastąpić zgodnie z metodami operacyjnymi i procedurami zatwierdzonymi przez inny organ nadzoru, zgłoszony Komisji zgodnie z art. 17 rozporządzenia eIDAS zgodnie z odpowiednimi przepisami krajowymi wdrażającymi art. 24 rozporządzenia pod warunkiem, że nie naruszają one prawa włoskiego[6].

RA działające za granicą, lub w każdym razie identyfikujące posiadaczy mieszkających za granicą, mogą być upoważnione przez InfoCert do przyjmowania akceptowania dokumentów tożsamości wydanych przez organy państw należących do Unii Europejskiej, po przeanalizowaniu dokumentów i ich obiektywnych cech gwarantujących pewność tożsamości i bezpieczeństwo w procesie wydawania przez organy wydające, a także po przeprowadzeniu specjalnego szkolenia[7].
Operatora punktu rejestracji ma prawo wykluczyć dopuszczalność dokumentu użytego przez posiadacza lub wnioskodawcę, jeżeli uzna, że posiada wymienionych cech. Dane rejestracyjne złożone z plików audiowizualnych i ustrukturyzowanych metadanych

jest przekazywana do AgID i aktualizowana po każdej zmianie. Ze względu na bezpieczeństwo i procedury przeciwdziałania oszustwom, rodzaj dokumentów akceptowanych w tym trybie jest ograniczony do najbardziej rozpowszechnionych dokumentów tożsamości

6 Takie przypadki będą zgłaszane organowi nadzoru.
7 Takie przypadki będą zgłaszane organowi nadzoru.

w formacie elektronicznym są przechowywane w sposób chroniony.

3.2.3.6 *Potwierdzanie tożsamości zgodnie z trybem 6 – eDocID*

W trybie 6 eDocID, posiadacz posiada urządzenie podłączone do Internetu, wyposażone w kamerę internetową i czujnik zbliżeniowy oraz przedkłada do identyfikacji mechanicznie czytelny dokument tożsamości, który może być użyty do identyfikacji biometrycznej[8].
Kadrując dokument kamerą i zbliżając go do czytnika zbliżeniowego, posiadacz umożliwia dostęp do pamięci elektronicznej chipa, z której pozyskiwane są zawarte w nim dane identyfikacyjne i zdjęcie. Posiadacz otrzymuje również instrukcje w ramach automatycznej procedury fotografowania twarzy (tzw. wideo selfie"), w trakcie której wykonuje losowe czynności wzmacniające, zgodnie z instrukcjami procedury określonymi przez CA.
CA sprawdza autentyczność podpisu technicznego znajdującego się na danych i zdjęciach pozyskanych z dokumentu tożsamości oraz sprawdza jego rzeczywistą przynależność do posiadacza, przy użyciu jednej lub kilku technologii biometrycznych porównujących zdjęcie pozyskane z uzyskanym wideo selfie. Jeśli wskaźnik zgodności (tzw. „scoring") nie osiągnął wystarczających wartości, operator punktu rejestracji przeprowadza kolejny etap weryfikacji tożsamości w backoffice.
Dane rejestracyjne złożone z plików audiowizualnych i ustrukturyzowanych metadanych w formacie elektronicznym są przechowywane w sposób chroniony.

3.2.3.7 *Potwierdzanie tożsamości zgodnie z trybem 7 – ContoID*

W trybie 7 ContoID, posiadacz posiada urządzenie podłączone do Internetu i wyposażone w kamerę internetową oraz przedkłada do identyfikacji ważny dokument tożsamości.
Kadrując dokument kamerą, posiadacz otrzymuje instrukcje w ramach procedury pobierania kopii dokumentu tożsamości, aby umożliwić pozyskanie z niego stosownych danych identyfikacyjnych i zdjęcia. Posiadacz otrzymuje instrukcje w ramach automatycznej procedury fotografowania twarzy (tzw. wideo selfie"), w trakcie której wykonuje losowe czynności wzmacniające, zgodnie z instrukcjami procedury określonymi przez CA.
CA sprawdza rzeczywistą przynależność dokumentu do posiadacza, przy użyciu jednej lub kilku technologii biometrycznych porównujących zdjęcie pozyskane z uzyskanym wideo selfie. Sprawdza również, czy dane właściciela konta są zgodne z danymi posiadacza.
Posiadacz potwierdza swoje dane poprzez uwierzytelnienie dostępu do swojego konta

[8] Chodzi o dokumenty spełniające wymagania norm ICAO z MRZ lub w każdym razie posiadające porównywalne cechy bezpieczeństwa

Płatniczego wykonane za pomocą silnego uwierzytelnienia (Strong Customer Authentication – SCA) przez dostawcę usług płatniczych (Payment Service Provider – PSP), zgodnie z Dyrektywą (UE) 2015/2366 (PSD2).
Dane rejestracyjne złożone z plików audiowizualnych i ustrukturyzowanych metadanych w formacie elektronicznym są przechowywane w sposób chroniony.

3.2.4 Niezweryfikowane informacje dotyczące posiadacza lub wnioskodawcy

Posiadacz może uzyskać, bezpośrednio lub za zgodą zainteresowanej strony trzeciej, umieszczenie w certyfikacie informacji dotyczących:

- tytułów i/lub kwalifikacji zawodowych;
- uprawnień do reprezentacji osób fizycznych;
- uprawnień do reprezentacji osób prawnych lub przynależności do nich;
- pełnienia funkcji publicznych, uprawnień do reprezentacji organizacji i podmiotów prawa publicznego lub przynależności do nich.

Certyfikat z informacją o **roli** jest zgodny z zapisami Decyzji AgID 147/2019 [13].
Posiadacz zobowiązany jest przedstawić odpowiednie oświadczenie wykazujące rzeczywiste istnienie danej roli, również w drodze samocertyfikacji[9]. CA nie ponosi żadnej odpowiedzialności, z wyjątkiem przypadków zamierzonego działania lub niedbalstwa, za umieszczenie w certyfikacie informacji poświadczonych przez posiadacza w drodze samocertyfikacji.
Nazwa przedsiębiorstwa lub nazwa i kod identyfikacyjny **organizacji** zostaną natomiast wskazane w certyfikacie, jeśli organizacja upoważniła do wydania certyfikatu posiadaczowi, również bez wyraźnego wskazania roli. W takim przypadku, CA sprawdza formalną prawidłowość dokumentacji przedłożonej przez posiadacza. Wniosek o wydanie certyfikatów ze wskazaniem roli i/lub organizacji mogą złożyć wyłącznie organizacje posiadające określoną formę prawną.

3.2.5 Walidacja wniosku

CA lub RA weryfikują informacje określone w punktach 3.2.2 , 3.2.3 i 3.2.4 i wymagane do celów identyfikacji, oraz zatwierdzają wniosek.
CA lub RA, jeżeli zostało to przewidziane lub jest konieczne, może korzystać z publicznych baz danych w celu potwierdzenia informacji przekazanych przez wnioskodawcę.

W przypadku wniosku QSealC PSD2, CA lub RA sprawdza specyficzne atrybuty dostarczone przez wnioskodawcę (numer upoważnienia, nazwę i status NCA, rolę

[9] W przypadku, gdy wniosek o umieszczenie roli w certyfikacie został złożony przez posiadacza tylko w drodze samocertyfikacji, certyfikat nie będzie podawać informacji dotyczących organizacji, z którą rola mogłaby być ewentualnie powiązana.

PSP), korzystając z prawdziwych informacji udostępnionych przez EBA w jego centralnym rejestrze lub, w stosownych przypadkach, w rejestrach udostępnionych przez NCA każdego państwa członkowskiego.
Jeżeli krajowy NCA dostarczył zasady dotyczące walidacji tych atrybutów, TSP stosuje wskazane zasady.

3.3 Identyfikacja i uwierzytelnianie w celu odnowienia lub ponownego wydania nowych kluczy

Niniejszy punkt opisuje procedury stosowane do uwierzytelniania i identyfikacji posiadacza w przypadku, gdy wnioskuje o odnowienie swojego certyfikatu lub ponownego wydania certyfikatu z nowymi i innymi kluczami kryptograficznymi.

3.3.1 Identyfikacja i uwierzytelnianie posiadacza w celu ponownego wydania nowych kluczy

Ponowne wydanie certyfikatu z nowymi kluczami może nastąpić przed wygaśnięciem certyfikatu, tj. gdy „ważny do dnia” (not after) jest późniejszy od daty wniosku. Korzystając z narzędzi udostępnionych przez CA, posiadacz może złożyć wniosek podpisany kluczem prywatnym odpowiadającym kluczowi publicznemu zawartemu w certyfikacie, który jest w jego posiadaniu. W tym przypadku można to również określić jako **odnowienie z ponowną certyfikacją nowych kluczy.**
Posiadacz może wnioskować o ponowne wydanie certyfikatu również po wygaśnięciu poprzedniego certyfikatu, czyli gdy „ważny do dnia” (not after) jest wcześniejszy niż data wniosku. Podmiot certyfikujący może skorzystać z wcześniej wykonanego potwierdzenia tożsamości posiadacza i z uprzednio ustalonego bezpiecznego powiązania między uprawnieniami posiadacza a potwierdzeniem jego tożsamości. Powiązanie to jest zapewnione przez uwierzytelnianie dwuetapowe, które w fazie potwierdzania tożsamości zostało powiązane z posiadaczem.
Potwierdzenie tożsamości zachowuje ważność maksymalnie przez okres czterech lat i tylko wtedy, gdy w międzyczasie dokumenty tożsamości wnioskodawcy lub inne atrybuty związane z tożsamością posiadaczy nie straciły ważności.
Podmiot certyfikujący, w przypadku stwierdzenia problemów związanych z bezpieczeństwem informacji lub problemów związanych z oszustwami, może podjąć decyzję o unieważnieniu potwierdzenia tożsamości przed upływem czterech lat.

3.3.2 Identyfikacja i uwierzytelnianie posiadacza w celu ponownego wydania nowych klucz po ich unieważnieniu

Nie dotyczy

3.3.3 Identyfikacja i uwierzytelnianie posiadacza w celu odnowienia

certyfikatów

Niniejszy punkt opisuje procedury stosowane do uwierzytelniania i identyfikacji posiadacza przypadku odnowienia kwalifikowanego certyfikatu podpisu z tymi samymi kluczami kryptograficznymi.
Certyfikat zawiera wskazanie okresu ważności w polu „termin ważności" (validity) z atrybutami „ważny od dnia" (not before) i „ważny do dnia" (not after). Poza tym zakresem dat, obejmującym godziny, minuty i sekundy, certyfikat należy uważać za nieważny.
Posiadacz może jednak odnowić go przed upływem terminu ważności, korzystając z narzędzi udostępnionych przez CA, które przedstawiają wniosek o odnowienie podpisany kluczem prywatnym odpowiadającym kluczowi publicznemu zawartemu w certyfikacie, który ma być odnowiony. Po unieważnieniu lub wygaśnięciu ważności certyfikatu nie można go odnowić, a zatem wymagane jest wydanie nowego certyfikatu.

3.4 Identyfikacja i uwierzytelnianie wniosków o unieważnienie lub zawieszenie

Unieważnienie lub zawieszenie certyfikatu może nastąpić na wniosek posiadacza lub wnioskodawcy (zainteresowanej strony trzeciej w przypadku, gdy wyraziła ona zgodę na umieszczenie roli) lub z inicjatywy CA.

3.4.1 Wniosek ze strony posiadacza

Posiadacz może złożyć wniosek o unieważnienie lub zawieszenie certyfikatu, wypełniając i podpisując, w tym cyfrowo, formularz dostępny na stronie internetowej CA (patrz punkt 4.9).
Wniosek o zawieszenie certyfikatu może zostać złożony za pomocą formularza internetowego. W takim przypadku, posiadacz dokonuje uwierzytelnienia, podając kod awaryjny dostarczony w momencie wydania certyfikatu lub za pomocą innego systemu uwierzytelniania opisanego w dokumentacji umownej dostarczonej w momencie rejestracji. Posiadacz posiadający zdalny podpis może zawnioskować o unieważnienie, korzystając również ze swojego prywatnego obszaru, do którego uzyskuje dostęp za pośrednictwem dwuetapowego systemu uwierzytelniania (punkt 4.2.2)

W przypadku składania wniosku w punkcie rejestracji, uwierzytelnienie posiadacza odbywa się zgodnie z trybami przewidzianymi dla identyfikacji.

Jeżeli posiadacz jest osobą prawną, wniosek o zawieszenie lub unieważnienie certyfikatu powinien zostać złożony przez przedstawiciela prawnego lub podmiot posiadający odpowiednie pełnomocnictwo.

3.4.2 Wniosek ze strony wnioskodawcy

Wnioskodawca lub zainteresowana strona trzecia wnosząca o unieważnienie lub zawieszenie certyfikatu posiadacza dokonuje uwierzytelnienia, podpisując odpowiedni formularz wniosku o unieważnienie lub zawieszenie certyfikatu, udostępniony przez CA. Wniosek należy przesłać w sposób określony w punktach 4.9.3 lub 4.9.15.2. CA zastrzega sobie prawo do określenia dodatkowych sposobów składania wniosku o unieważnienie lub zawieszenie certyfikatu przez wnioskodawcę w odpowiednich porozumieniach zawieranych z wnioskodawcą.

4 WYMAGANIA FUNKCJONALNE

4.1 Wnioskowanie o wydanie certyfikatu

4.1.1 Kto może wnioskować o wydanie certyfikatu?

O wydanie certyfikatu kwalifikowanego dla osoby fizycznej może wnioskować:

- posiadacz,
  - zwracając się w tym celu bezpośrednio do CA za pośrednictwemstrony www.firma.infocert.it lub www.infocert.it, lub
  - zwracając się do punktu rejestracji
- wnioskodawca w imieniu posiadacza,
  - zwracając się w tym celu bezpośrednio do CA za pośrednictwem strony internetowej www.firma.infocert.it lub www.infocert.it lub zawierając z CA odpowiednie porozumienie handlowe
  - zwracając się do punktu rejestracji
  - udzielając CA umocowanie z prawem do reprezentacji i stając się punktem rejestracji w ramach domeny informatycznej.

O wydanie certyfikatu kwalifikowanego dla osoby prawnej może wnioskować:

- wnioskodawca reprezentujący osobę prawną,
  - zwracając się w tym celu bezpośrednio do CA za pośrednictwem strony internetowej www.firma.infocert.it lub www.infocert.it lub zawierając z CA odpowiednie porozumienie handlowe
  - zwracając się do określonych punktów rejestracji specjalnie przeszkolonych w zakresie wydawania tego typu certyfikatów.

4.1.2 Proces rejestracji i związane z nim obowiązki

Proces rejestracji obejmuje złożenie wniosku przez posiadacza, wygenerowanie pary kluczy, złożenie wniosku o wydanie certyfikatu klucza publicznego oraz podpisanie

umów, przy czym czynności te niekoniecznie muszą odbywać się w tej kolejności.

Poszczególni uczestnicy procesu mają różne obowiązki, których łączne wypełnienie umożliwia jego pozytywne zakończenie:

- obowiązkiem posiadacza jest dostarczenie prawidłowych oraz prawdziwych informacji na temat własnej tożsamości, dokładne zapoznanie się z udostępnionym przez CA materiałem, również za pośrednictwem RA, a także realizacja zaleceń CA i/lub RA w trakcie procedowania wniosku o wydanie kwalifikowanego certyfikatu. Jeśli posiadaczem jest osoba prawna, powyższe obowiązki spadają na jego prawnego przedstawiciela lub podmiot posiadający odpowiednie pełnomocnictwo, który wnioskuje o wydanie kwalifikowanego certyfikatu w imieniu danej osoby prawnej;
- wnioskodawca, jeśli występuje, ma obowiązek poinformować posiadacza, w imieniu którego wnioskuje o wydanie certyfikatu, o obowiązkach wynikających z certyfikatu, dostarczyć prawidłowe i prawdziwe informacje dotyczące tożsamości posiadacza, a także realizować procedury i wykonywać instrukcje CA i/lub RA;
- punkt rejestracji, jeśli występuje, również za pośrednictwem operatora punktu rejestracji, ma obowiązek jednoznacznie zidentyfikować posiadacza i wnioskodawcę, poinformować poszczególne podmioty o obowiązkach wynikających z certyfikatu, a także dokładnie realizować procedury określone przez CA;
- urząd certyfikacji jako ostatni jest odpowiedzialny za identyfikację posiadacza, a także za pozytywne zakończenie procesu rejestracji certyfikatu kwalifikowanego.

W przypadku, gdy posiadaczem jest osoba prawna, a klucze są generowane przez urządzenie posiadacza, wnioskodawca musi wysłać wniosek również w formacie PKCS#10 podpisany przez samego wnioskodawcę.

4.2 Przetwarzanie wniosku

W celu uzyskania certyfikatu podpisu, posiadacz i/lub wnioskodawca musi:

- zapoznać się z dokumentacją umowną i wszelką dodatkową dokumentacją informacyjną;
- postępować zgodnie z procedurami identyfikacji przyjętymi przez urząd certyfikacji, zgodnie z opisem zawartym w punkcie 3.2.3;
- dostarczyć wszelkie informacje niezbędne do identyfikacji, uzupełnione, gdy istnieje taka potrzeba, o odpowiednią dokumentację;
- podpisać wniosek o rejestrację i wydanie certyfikatu, akceptując warunki umowne regulujące korzystanie z usługi, wypełniając w tym celu odpowiednie formularze, w wersji analogowej lub elektronicznej, przygotowane przez CA.

4.2.1 Realizacja czynności związanych z identyfikacją i uwierzytelnianiem

4.2.1.1 Osoba fizyczna

W celu złożenia wniosku o wydanie kwalifikowanego certyfikatu podpisu, posiadacz lub

Wnioskodawca, który wnioskuje o wydanie certyfikatu dla osoby fizycznej musi obowiązkowo dostarczyć następujące informacje:

- nazwisko i imię;
- datę i miejsce urodzenia;
- kod TIN (we Włoszech kod identyfikacji podatkowej) lub, w razie jego braku, analogiczny kod identyfikujący osobę, jak np. numer dokumentu tożsamości; w przypadkach, w których przepisy krajowe nie pozwalają na publiczne wykorzystanie tych informacji, InfoCert nie umieści ich w certyfikacie.
- dane dokumentu tożsamości okazanego do identyfikacji, takie jak typ lub numer;
- przynajmniej jedną z informacji kontaktowych służących CA do przesyłania wiadomości posiadaczowi :
  - adres zamieszkania;
  - adres e-mail;
- numer telefonu komórkowego do kontaktu w sytuacjach awaryjnych i do przesyłania haseł OTP, jeśli jest stosowana ta technologia.

Adres e-mail i numer telefonu komórkowego podany RA muszą istnieć i jednoznacznie identyfikować podmiot. Adres e-mail będzie używany do wszelkich wiadomości od CA oraz do wysyłania kodów awaryjnych (ERC) i zawiadomień o wygaśnięciu. Uwaga ta nie ma zastosowania w przypadku certyfikatów LongTerm i OneShot.

Opcjonalnie, posiadacz (lub wnioskodawca) może podać inną nazwę, pod którą jest powszechnie znany, a która zostanie wprowadzona do odpowiedniego pola o nazwie commonName (nazwa powszechnie znana) w SubjectDN certyfikatu. W przypadku, gdy posiadać lub wnioskodawca nie podał żadnej dodatkowej nazwy, pole commonName uzupełnione zostanie imieniem i nazwiskiem posiadacza.

4.2.1.2 Osoba prawna

W przypadku wniosku o wydanie kwalifikowanego certyfikatu dla osoby prawnej, wnioskodawca, zidentyfikowany w osobie prawnego przedstawiciela lub osoby fizycznej posiadającej pełnomocnictwo, musi obowiązkowo dostarczyć następujące informacje:

- nazwisko i imię wnioskodawcy;
- kod TIN lub analogiczny kod identyfikujący wnioskodawcę (we Włoszech kod identyfikacji podatkowej);
- dane dokumentu tożsamości okazanego do identyfikacji wnioskodawcy, takie jak typ, numer, nazwę organu wydającego i datę jego wydania;

- adres e-mail służący CA do przesyłania wiadomości wnioskodawcy;

- nazwę posiadacza będącego osobą prawną;
- numer VAT lub NTR (numer identyfikacyjny VAT lub numer w Rejestrze Przedsiębiorstw w przypadku podmiotów włoskich).

Gdyby osoba prawna chciała uzyskać certyfikat dla własnych par kluczy, wnioskodawca musi dostarczyć również plik w formacie PKCS#10 zawierający wniosek podpisany przez wnioskodawcę.
Przekazane informacje zapisywane są w archiwach CA (etap rejestracji) i stanowić będą podstawę do wygenerowania certyfikatu kwalifikowanego.

W przypadku wniosku QSealC PSD2, posiadacz (PSP), zidentyfikowany w osobie prawnego przedstawiciela lub osoby fizycznej posiadającej pełnomocnictwo, **musi dostarczyć następujące dodatkowe informacje:**

- numer upoważnienia, który jednoznacznie identyfikuje dostawcę usług płatniczych (PSP);
- rolę(-e) dostawcy usług płatniczych (PSP);
- nazwę i status właściwego organu krajowego (NCA), który upoważnił dostawcę usług płatniczych (PSP) i wydał numer upoważnienia.

4.2.1.3 Rejestracja

W początkowej fazie rejestracji oraz przyjmowania wniosku o rejestrację i wydanie certyfikatu posiadaczowi lub wnioskodawcy, będącemu prawnym przedstawicielem osoby prawnej, przekazane są kody bezpieczeństwa, które umożliwiają mu aktywację urządzenia do składania podpisu lub uruchomienie procedury podpisu, jeśli jest ona zdalna, i/lub złożenie ewentualnego wniosku o zawieszenie certyfikatu (kod ERC lub analogiczny kod, jeśli jest to przewidziane w umowie). Kody bezpieczeństwa dostarczane są drogą elektroniczną w zaszyfrowanych plikach.
Wystawione kody bezpieczeństwa nie są już dostarczane w zaciemnionej kopercie. Może być ona używana tylko w rzadkich przypadkach, gdy nie będzie możliwe korzystanie z trybu elektronicznego.
CA może postanowić, aby posiadacz lub wnioskodawca będący prawnym przedstawicielem osoby prawnej sam wybrał kod PIN potrzebny do podpisu. W takich przypadkach, obowiązek zapamiętania PIN-u leży po stronie posiadacza lub wnioskodawcy.
CA może również postanowić o stosowaniu certyfikatu podpisu w procedurze zdalnej za pośrednictwem systemu uwierzytelniania oferowanego przez RA, którego poziom bezpieczeństwa jest co najmniej średni lub wysoki, po wcześniejszym przeanalizowaniu jego cech, w ramach certyfikacji bezpiecznego urządzenia do składania podpisu. W takich przypadkach system uwierzytelniania może być również wykorzystywany do ewentualnego wniosku o zawieszenie i unieważnienie certyfikatu.

4.2.2 Przyjęcie lub odrzucenie wniosku o wydanie certyfikatu

Po wstępnej rejestracji, CA lub RA może odmówić wydania certyfikatu podpisu w razie stwierdzenia braku lub niekompletności informacji, kontroli spójności i zgodności przekazanych informacji, kontroli pod kątem zwalczania nadużyć finansowych lub wątpliwości co do tożsamości posiadacza bądź wnioskodawcy itd.

4.2.3 Maksymalny czas przetwarzania wniosku o wydanie certyfikatu

Czas od chwili złożenia wniosku o rejestrację do momentu wydania certyfikatu zależy od trybu składania wniosku wybranego przez posiadacza (lub wnioskodawcę) oraz od ewentualnej konieczności zebrania dodatkowych informacji lub fizycznego dostarczenia urządzenia.

4.3 Wydanie certyfikatu

4.3.1 Działania CA w trakcie procesu wystawiania certyfikatu

4.3.1.1 Wystawienie certyfikatu na urządzeniu do składania podpisu (karta elektroniczna lub token)

Para kluczy kryptograficznych jest generowana przez RA bezpośrednio na bezpiecznych urządzeniach do składania podpisu, z wykorzystaniem aplikacji udostępnionych przez CA po wcześniejszym bezpiecznym uwierzytelnieniu.
RA przesyła do CA wniosek o wydanie certyfikatu dla klucza publicznego w formacie PKCS#10, podpisany elektronicznie przy użyciu specjalnie do tego celu wygenerowanego kwalifikowanego certyfikatu podpisu.
CA, po zweryfikowaniu ważności podpisu na PKCS#10 i prawa podmiotu do przesłania wniosku, generuje certyfikat kwalifikowany, który jest przesłany do urządzenia z użyciem bezpiecznego kanału.

4.3.1.2 Wystawienie certyfikatu na urządzeniu do zdalnego składania podpisu (HSM)

Posiadacz lub wnioskodawca uwierzytelniają swój dostęp do usług lub aplikacji udostępnionych przez RA.
Para kluczy kryptograficznych jest generowana na HSM znajdującym się w siedzibie QTSP. RA przesyła zatem do CA wniosek o wydanie certyfikatu klucza publicznego z użyciem bezpiecznego kanału.
CA, po zweryfikowaniu prawa podmiotu do przesłania wniosku, generuje certyfikat kwalifikowany, który jest zapisany w HSM.

4.3.1.3 *Wystawienie certyfikatu przy użyciu systemu Card Management System*

Para kluczy kryptograficznych jest generowana przez RA bezpośrednio na urządzeniach z wykorzystaniem uwierzytelnionego systemu Card Management System. System zarządza pełnym cyklem życia urządzenia kryptograficznego, przesyłając do CA wniosek o wydanie certyfikatu klucza publicznego w formacie PKCS#10, podpisany elektronicznie z użyciem bezpiecznego kanału.

CA, po zweryfikowaniu ważności podpisu na PKCS#10 i prawa podmiotu do przesłania wniosku, generuje certyfikat kwalifikowany, który jest przesłany do urządzenia z użyciem bezpiecznego kanału.

4.3.1.4 *Wystawienie certyfikatu dla osoby prawnej*

Para kluczy kryptograficznych jest generowana przez RA bezpośrednio na HSM.RA przesyła zatem do CA wniosek o wydanie certyfikatu dla klucza publicznego w formacie PKCS#10, który jest podpisany elektronicznie przy użyciu automatycznej procedury specjalnie do tego celu wygenerowanego kwalifikowanego certyfikatu podpisu.

CA, po zweryfikowaniu ważności podpisu na PKCS#10 i prawa podmiotu do przesłania wniosku, generuje certyfikat kwalifikowany, który jest zapisany w HSM.
W przypadku, gdy para kluczy generowana jest w urządzeniu HSM posiadacza, posiadacz powinien wysłać podpisany PKCS#10, a CA, po zweryfikowaniu ważności podpisu na PKCS#10 i prawa podmiotu do przesłania wniosku, generuje certyfikat kwalifikowany, który jest zapisany w HSM.

4.3.1.5 *Wystawienie certyfikatu do celów testowych*

Czasami potrzebne są certyfikaty w celu przeprowadzenia testów w warunkach produkcyjnych.
W takich przypadkach, przed rozpoczęciem procedury wystawiania certyfikatu, należy dokonać rejestracji danych. Rejestracja musi zostać zatwierdzona przez Kierownika CA.
W określonych przypadkach, punktem rejestracji musi być urząd wykorzystywany przez InfoCert do wystawiania wewnętrznych certyfikatów lub urząd wykorzystywany przez procedurę klienta, która jest przedmiotem sesji testowej.
Dane użyte do rejestracji muszą jednoznacznie wskazywać w Subject, że jest to certyfikat badania, a nie certyfikat rzeczywisty.
Procedura ta nie może być stosowana do badań obciążeniowych lub cyklicznych w odniesieniu do rejestracji i emisji.
Gdy certyfikat przestaje już być potrzebny (np. po zakończeniu danej sesji

testowej), musi zostać unieważniony z urzędu.

4.3.2 Zawiadomienie wnioskodawców o wystawieniu certyfikatu

W przypadku wystawienia certyfikatu na urządzeniu kryptograficznym, posiadacz (lub wnioskodawca) nie potrzebuje zawiadomienia, ponieważ certyfikat jest dostępny na otrzymanym przez niego urządzeniu.
W przypadku certyfikatów LongTerm i OneShot, CA zawiadamia wnioskodawcę za pomocą automatycznej procedury, że certyfikat podmiotu został wydany. Wnioskodawca informuje posiadacza w sposób i według metod określonych w umowie.
W pozostałych przypadkach posiadacz otrzyma zawiadomienie na adres mailowy podany w chwili rejestracji. Informacja ta jest również przekazane wnioskodawcy.

4.3.3 Aktywacja

4.3.3.1 Aktywacja urządzenia do składania podpisu (karta elektroniczna lub token)

Po otrzymaniu urządzenia, posiadacz, korzystając z otrzymanych w poufny sposób kodów aktywacyjnych i odpowiedniego oprogramowania udostępnionego przez CA, uruchamia urządzenie, wybierając jednocześnie PIN podpisu, zastrzeżoną ilość zabezpieczeń, których przechowywanie i ochrona leży wyłącznie w gestii posiadacza.

4.3.3.2 Uruchomienie urządzenia do zdalnego składania podpisu (HSM)

Posiadacz lub wnioskodawca w imieniu podmiotu prawnego, posiadający uprawnienia dostępu do portali CA za pośrednictwem otrzymanych w sposób poufny kodów aktywacyjnych, wybiera PIN podpisu, zastrzeżoną ilość zabezpieczeń, których przechowywanie i ochrona leży wyłącznie w gestii posiadacza, co jest potwierdzane wpisaniem hasła OneTime Password otrzymanego w wiadomości SMS lub wygenerowanego na tokenie lub w aplikacji tokenowej powiązanej z certyfikatem.
W niektórych przypadkach może być wydany już aktywny i możliwy do użycia certyfikat.

4.4 Akceptacja certyfikatu

4.4.1 Kroki kończące proces akceptacji certyfikatu

Nie dotyczy

4.4.2 Publikacja certyfikatu przez urząd

certyfikacji

W chwili pozytywnego zakończenia procedury certyfikacji, certyfikat zostanie wprowadzony do rejestru certyfikatów, bez podawania go do publicznej wiadomości. Posiadacz zainteresowany upublicznieniem swojego certyfikatu może się o to zwrócić w drodze procedury opisanej w punkcie
2.2.2. Wniosek zostanie rozpatrzony w ciągu trzech dni roboczych. Nie ma takiej możliwości w przypadku certyfikatów LongTerm i OneShot.

4.4.3 Zawiadomienie wnioskodawców o upublicznieniu certyfikatu

Nie dotyczy

4.5 Korzystanie z pary kluczy i certyfikatu

4.5.1 Korzystanie z prywatnego klucza i certyfikatu przez posiadacza

Posiadacz zobowiązany jest do bezpiecznego przechowywania urządzenia do składania podpisu, jeśli występuje, lub innych narzędzi uwierzytelniających dla procedury zdalnego składania podpisu; musi również przechowywać informacje umożliwiające korzystanie z prywatnego klucza z dala od samego urządzenia, jeżeli występuje, lub narzędzi albo kodów aktywacyjnych. Musi zapewnić w tajemnicy i przechowywać kod awaryjny niezbędny do zawieszenia certyfikatu, w stosownych przypadkach. Musi korzystać z certyfikatu tylko do celów przewidzianych w Polityce oraz zgodnie z obowiązującymi, krajowymi i międzynarodowymi przepisami prawa. Nie może składać podpisów elektronicznych, korzystając z prywatnych kluczy, dla których certyfikat został unieważniony lub zawieszony, ani też składać podpisów elektronicznych, korzystając z certyfikatu wydanego przez CA, któremu cofnięto uprawnienia.
W przypadku domeny zamkniętej, certyfikat LongTerm i OneShot musi być używany tylko do podpisywania dokumentów dotyczących specyficznego związku między wnioskodawcą i posiadaczem.

4.5.2 Korzystanie z publicznego klucza i certyfikatu przez użytkowników końcowych

Użytkownik końcowy musi zapoznać się z zakresem stosowania certyfikatu opisanym w Polityce i w samym certyfikacie. Musi również zweryfikować ważność certyfikatu przez użyciem zawartego w nim klucza publicznego, a także zweryfikować, czy

certyfikat nie został zawieszony lub unieważniony, sprawdzając w tym celu zapisy w odpowiednich rejestrach; musi ponadto zweryfikować istnienie i zakres ewentualnych ograniczeń stosowania pary kluczy, uprawnień do reprezentacji oraz kwalifikacji zawodowych.

4.5.3 Ograniczenia stosowania i limity kwotowe

Przedkładając odpowiednią dokumentację pomocniczą, można zwrócić się do RA o umieszczenie w kwalifikowanym certyfikacie podpisu następujących ograniczeń stosowania określonych przez AgID:

- Posiadacze korzystają z certyfikatu wyłącznie do celów służbowych, dla których został on wydany. The certificate holder must use the certificate only for the purposes for which it is issued.
- Korzystanie z certyfikatu ograniczone jest do kontaktów z (*wskazać podmiot*). The certificate may be used only for relations with the (*declare the subject*).

Kwalifikowane certyfikaty do składania podpisów **w procedurze automatycznej** zawierają
ograniczenie stosowania określone przez AgiD:

Niniejszy certyfikat jest ważny jedynie dla podpisów składanych w procedurze automatycznej. The certificate may only be used for unattended/automatic digital signature.

Certyfikaty wystawione na podstawie **identyfikacji typu 4 – AutID** z wykorzystaniem **węzła eIDAS** lub na podstawie identyfikacji typu **eDocID** zawierają OID 1.3.76.16.5 i następujące ograniczenie jego stosowania:

- Certificate not usable to require SPID digital identity [Certyfikat nie może być stosowany do wnioskowania o cyfrowe tożsamości SPID]

Certyfikaty wystawione na podstawie **identyfikacji typu 4 – AutID** z wykorzystaniem **tożsamości cyfrowej SPID** zgodnie z zawiadomieniem nr 17 z dnia 24 stycznia 2019 roku, zawierają OID 1.3.76.16.5 i następujące ograniczenie stosowania:

- Certificate issued through Sistema Pubblico di Identità Digitale (SPID) digital identity, not usable to require other SPID digital identity [Certyfikat wystawiony przy użyciu Publicznego systemu tożsamości cyfrowej (SPID), nie może być stosowany do wnioskowania o cyfrowe tożsamości SPID]

Certyfikaty dla osoby prawnej z kodem LEI wystawione dla PoC (Proof of Concepts – weryfikacji poprawności)
zawierają następujące ograniczenie stosowania:

- The use of the certificate is limited for sealing the documents used in the Proof of Concepts about the incorporation of the LEI codes in the electronic seal certificates

[Stosowanie certyfikatu jest ograniczone do pieczętowania dokumentów wykorzystywanych w weryfikacji poprawności dotyczącej włączenia kodów LEI do certyfikat pieczęci elektronicznej]

Ponadto posiadacz lub wnioskodawca mają prawo zwrócić się do urzędu certyfikacji o umieszczenie w certyfikacie indywidualnych ograniczeń stosowania (maks. 200 znaków) lub limitów kwotowych. Wniosek o wprowadzenie innych, szczególnych ograniczeń stosowania certyfikatu analizowany jest przez CA pod kątem prawnym, technicznym oraz ze względu na ich interoperacyjność, a następnie rozpatrywany.

Odnośnie ograniczeń stosowania przewidzianych dla hiszpańskich organów administracji publicznej, obowiązują uwagi podane w Aneksie C i w odniesieniach prawnych [17], [18], [19].

Ograniczenia stosowania certyfikatów LongTerm i OneShot

Certyfikaty typu LongTerm mogą być ograniczone wyłącznie do stosowania w domenie informatycznej określonej w umowie, do podpisywania dokumentów informatycznych udostępnionych podmiotowi przez CA lub przez wnioskodawcę. W takim wypadku, dokumenty informatyczne mogą być nierozerwalnie związane z kontaktami między wnioskodawcą i posiadaczem.
W **certyfikacie LongTerm** podawane jest zatem jedno z następujących ograniczeń stosowania:

- Korzystanie z certyfikatu ograniczone jest do kontaktów posiadacza z wnioskodawcą. The certificate can be used only in the relationships between the holder and the requestor (max 200 caratteri).
- Certyfikat do podpisywania produktów i usług udostępnionych przez [Nazwa posiadacza]. Certificate to subscribe product and services made available by [Nome Soggetto] (max 200 caratteri).

Certyfikat OneShot wskazuje następujące ograniczenie stosowania:

- Korzystanie z certyfikatu ograniczone jest do podpisywania dokumentów, na których umieszczany jest podpis. The use of the certificate is technically limited to the signature of the underlying documents.

Z zastrzeżeniem odpowiedzialności CA, o której mowa w CAD (art. 30), za weryfikację ograniczeń stosowania certyfikatu i limitów kwotowych z nim związanych odpowiedzialny jest użytkownik (osoba, która otrzymuje podpisany dokument). W związku z tym, CA nie odpowiada za szkody wynikające z korzystania z kwalifikowanego certyfikatu w zakresie przekraczającym wprowadzone w nim ograniczenia lub wynikające z przekroczenia dopuszczalnych limitów kwotowych.

4.6 Odnowienie certyfikatu

4.6.1 Przyczyny odnowienia

Odnowienie certyfikatu umożliwia otrzymanie nowego certyfikatu na podstawie posiadanego certyfikatu ze zbliżającym się terminem ważności. Odnowienie oznacza, że nowy certyfikat będzie zawierać te same dane identyfikacyjne podmiotu, ten sam klucz publiczny i nowy termin ważności. Dla certyfikatu LongTerm i OneShot oraz dla

certyfikatów wystawionych dla osoby prawnej nie przewidziano odnowienia, lecz nowe potwierdzenie tożsamości i wystawienie nowego certyfikatu.

4.6.2 Kto może zwrócić się o odnowienie certyfikatu?

Posiadacz może zwrócić się o odnowienie certyfikatu przed upływem terminu jego ważności tylko wtedy, gdy nie został unieważniony i jeżeli wszystkie informacje podane w momencie jego poprzedniego wystawienia są wciąż aktualne. Odnowienie certyfikatu nie będzie możliwe po upływie terminu jego ważności, lecz konieczne jest złożenie wniosku o wydanie nowego certyfikatu.
Procedura odnowienia stosowana jest wyłącznie dla certyfikatów wystawionych przez InfoCert.

4.6.3 Przetwarzanie wniosku o odnowienie certyfikatu

Odnowienie certyfikatu odbywa się przy użyciu funkcji udostępnionej przez CA w ramach kontaktów handlowych i umownych określonych z posiadaczem i z RA, jeśli występuje.

4.7 Ponowne wystawienie certyfikatu z nowymi kluczami

4.7.1 Przyczyny ponownego wystawienia certyfikatu z nowymi kluczami

Ponowne wystawienie certyfikatu z nowym kluczem (re-key) umożliwia już zidentyfikowanemu i posiadającemu certyfikat posiadaczowi uzyskanie certyfikatu dla innej pary kluczy przy zachowaniu tych samych danych identyfikacyjnych. Termin ważności nowego certyfikatu jest określony w umowie.
Niewyczerpujący wykaz przykładów może obejmować ponowną certyfikację nowej pary kluczy na urządzeniu zdalnym ze zbliżającym się terminem ważności certyfikatu lub na urządzeniu wycofywanym z użytku, lub zastąpienie słabych kluczy kryptograficznych kluczami kryptograficznymi wygenerowanymi za pomocą bardziej solidnych algorytmów.

Procedura stosowana jest wyłącznie dla certyfikatów wystawionych przez InfoCert.

4.7.2 Kto może wnioskować o ponowne wystawienie certyfikatu z nowymi kluczami

Wniosek może być złożony przez posiadacz lub wnioskodawcę przed upływem terminu ważności certyfikatu lub później pod warunkiem, że wszystkie informacje dostarczone w momencie wystawienia poprzedniego certyfikatu i dowody zebrane na etapie potwierdzania tożsamości są nadal aktualne. W przypadku, gdy dokument tożsamości nie jest już ważny, certyfikat nie może być ponownie wystawiony.

4.7.3 Przetwarzanie wniosku o ponowne wystawienie certyfikatu z nowymi kluczami

Ponowne wystawienie certyfikatu z nowymi kluczami odbywa się przy użyciu funkcji udostępnionej przez CA w ramach kontaktów handlowych i umownych określonych z posiadaczem i z RA, jeśli występuje.

4.8 Zmiany certyfikatu

Nie dotyczy

4.9 Unieważnienie i zawieszenie certyfikatu

Unieważnienie lub zawieszenie certyfikatu powoduje wygaśnięcie ustalonego terminu ważności certyfikatu oraz unieważnienie podpisów złożonych po opublikowaniu informacji o unieważnieniu certyfikatu. Unieważnione lub zawieszone certyfikaty wpisywane są na listę unieważnionych i zawieszonych certyfikatów (CRL) podpisaną przez CA, który je wystawił, i publikowaną w rejestrze certyfikatów z wcześniej ustaloną częstotliwością. W szczególnych okolicznościach CA może nalegać na nieplanowane opublikowanie listy CRL. Unieważnienie lub zawieszenie certyfikatu staje się skuteczne w chwili opublikowania listy, co jest poświadczone datą rejestracji zdarzenia w dzienniku kontrolnym prowadzonym przez urząd certyfikacji.

Informacja na temat stanu unieważnienia jest dostępna w urzędzie certyfikacji przez 20 lat od wygaśnięcia certyfikatu root poprzez wydanie i przechowywanie przy użyciu serwisu przechowywania danych InfoCert zgodnie z ostatnią listą CRL.

4.9.1 Przyczyny unieważnienia certyfikatu

Wniosek o unieważnienie certyfikatu musi zostać złożony w momencie wystąpienia poniższych okoliczności:

1. naruszony został prywatny klucz, tj. wystąpił jeden z poniższych przypadków:
   - zostało zagubione bezpieczne urządzenie do składania podpisu zawierające klucz;
   - została naruszona poufność klucza lub jego kodu aktywacyjnego (PIN) lub też, w przypadku certyfikatów do zdalnego składania podpisu, zostało naruszone lub zagubione urządzenie OTP;
   - wystąpiło jakiekolwiek inne zdarzenie naruszające poziom wiarygodności klucza;
2. posiadacz nie jest w stanie dalej korzystać z bezpiecznego urządzenia do składania podpisu będącego w jego posiadaniu, np. z powodu awarii;
3. nastąpiła zmiana danych posiadacza zawartych w certyfikacie, w tym danych dotyczących roli, w zakresie powodującym, iż powyższe dane przestały być poprawne i/lub prawdziwe;
4. uległy zakończeniu stosunki między posiadaczem a CA lub między wnioskodawcą a CA;
5. doszło do istotnego naruszenia niniejszego Podręcznika obsługi.

4.9.2 Kto może zwrócić się o unieważnienie certyfikatu?

O unieważnienie certyfikatu może zwrócić się:

- posiadacz certyfikatu;
- wnioskodawca lub zainteresowana strona trzecia;
- CA z urzędu;
- NCA w przypadku wniosku o unieważnienie QSealC PSD2.

4.9.3 Procedury wnioskowania o unieważnienie certyfikatu

Poniżej przedstawiono procedury, za pomocą których osoby uprawnione do unieważnienia mogą złożyć wniosek o unieważnienie certyfikatu.

Unieważnienie wnioskowane przez posiadacza: wniosek o unieważnienie może zostać złożony poprzez podpisanie formularza znajdującego się na stronie internetowej InfoCert. Powyższy formularz można przekazać do RA lub przesłać bezpośrednio do CA listem poleconym i certyfikowaną pocztą elektroniczną, wraz z fotokopią ważnego dokumentu tożsamości. Ponadto, CA lub RA mogą udostępnić dodatkowe sposoby składania wniosku o unieważnienie certyfikatu pod warunkiem, że umożliwiają one prawidłową identyfikację posiadacza. CA lub RA poinformuje o tym odpowiednio posiadacza.

CA lub RA weryfikuje autentyczność wniosku, a następnie przystępuje do unieważnienia certyfikatu, informując niezwłocznie o podjętej decyzji posiadacza i jeśli występuje, wnioskodawcę.

Jeżeli certyfikat będący przedmiotem wniosku o unieważnienie zawiera informacje dotyczące roli posiadacza, CA podejmie kroki mające na celu poinformowanie o dokonaniu unieważnienia certyfikatu ewentualnej zainteresowanej strony trzeciej, z którą zostały zawarte określone porozumienia. Jeżeli certyfikat będący przedmiotem wniosku o unieważnienie zawiera dane organizacji, CA podejmie kroki mające na celu poinformowanie tego podmiotu o dokonaniu unieważnienia. Dodatkowe sposoby składania wniosku o unieważnienie certyfikatu przez posiadacza mogą być określone w ewentualnych umowach zawartych przez posiadacza i CA.

W przypadku wniosku o unieważnienie certyfikatów LongTerm i OneShot, z wyłączeniem certyfikatów short-term, posiadacz może zwrócić się o unieważnienie certyfikatu poprzez uwierzytelnienie się w systemach udostępnionych przez RA i/lub CA, przy użyciu usług aplikacyjnych, działając w sposób opisany w dokumentacji umownej. Ze względu na sam charakter certyfikatu short-term, nie została przewidziana możliwość złożenia wniosku o unieważnienie przez posiadacza.

Unieważnienie wnioskowane przez wnioskodawcę lub zainteresowaną stronę trzecią: wnioskodawca lub zainteresowana strona trzecia może zwrócić się o unieważnienie

certyfikatu posiadacza w taki sam sposób, w jaki może to zrobić posiadacz, pod warunkiem, że jest odpowiednio uprawniony. Musi również podać dane posiadacza certyfikatu przekazane CA w momencie wystawiania certyfikatu.

CA lub RA weryfikuje autentyczność wniosku, aby CA mógł podjąć kroki zmierzające do unieważnienia certyfikatu, a następnie niezwłocznie informuje o tym fakcie posiadacza, korzystając w tym celu ze środka komunikacji ustalonego w momencie złożenia wniosku o wydanie certyfikatu. Dodatkowe sposoby składania wniosku o unieważnienie certyfikatu przez posiadacza mogą być określone w ewentualnych umowach zawartych przez posiadacza i CA lub RA.

W przypadku wniosku o unieważnienie certyfikatów LongTerm i OneShot, z wyłączeniem certyfikatów short-term, wnioskodawca może zwrócić się o unieważnienie certyfikatu posiadacza poprzez uwierzytelnienie się w systemach udostępnionych przez CA, przy użyciu usług aplikacyjnych, działając w sposób opisany w dokumentacji umownej.
Ze względu na sam charakter certyfikatu short-term, nie została przewidziana możliwość złożenia wniosku o unieważnienie przez wnioskodawcę.

Unieważnienie certyfikatu z inicjatywy urzędu CA/RA: w przypadku zaistnienia takiej konieczności, CA ma prawo unieważnić certyfikat, wcześniej uprzedzając o tym fakcie posiadacza i podając uzasadnienie unieważnienia, a także datę i godzinę, kiedy to nastąpi.

Jeżeli certyfikat będący przedmiotem unieważnienia zawiera informacje dotyczące roli posiadacza, CA lub RA podejmie kroki mające na celu poinformowanie o dokonaniu unieważnienia certyfikatu ewentualnej zainteresowanej strony trzeciej, z którą zostały zawarte określone porozumienia. Jeżeli certyfikat będący przedmiotem wniosku o unieważnienie zawiera dane organizacji, CA podejmie kroki mające na celu poinformowanie tego podmiotu o dokonaniu unieważnienia. CA lub RA poinformuje o dokonaniu unieważnienia również wnioskodawcę.

W wyjątkowych przypadkach, CA może unieważnić również certyfikaty short-term, wcześniej informując o tym posiadacza i wnioskodawcę, podając uzasadnienie unieważnienia, a także datę i godzinę, kiedy to nastąpi.

Wniosek NCA: w przypadku wniosku o unieważnienie QSealC PSD2, o unieważnienie może się zwrócić również NCA, który wydał numer upoważnienia dostawcy usług płatniczych (PSP) znajdujący się w certyfikacie.

4.9.4 Okres karencji dla wniosku o unieważnienie certyfikatu

Okres karencji dla listy CRL obejmuje czas między opublikowaniem przez CA kolejnej listy CRL a terminem obowiązywania

bieżącej listy CRL. Aby zapobiec zakłóceniom w świadczeniu usług przez którąkolwiek z zaangażowanych stron, okres ten jest dłuższy od czasu, jaki CA potrzebuje na wygenerowanie i opublikowanie nowej listy CRL. W ten sposób bieżąca lista CRL obowiązuje przynajmniej do chwili zastąpienia jej przez nową listę CRL.

4.9.5 Maksymalny czas przetwarzania wniosku o unieważnienie certyfikatu

Wniosek o unieważnienie certyfikatu jest przetworzony i nowy certyfikat wydany w ciągu 24 (dwudziestu czterech) godzin, chyba że istnieją wątpliwości co do autentyczności wniosku. W takich wypadkach CA zastrzega sobie prawo do przeprowadzenia dodatkowych weryfikacji w celu ustalenia tożsamości wnioskodawcy. W tym ostatnim przypadku następuje zawieszenie certyfikatu w oczekiwaniu na przeprowadzenie dalszych kontroli dotyczących autentyczności otrzymanego wniosku.

4.9.6 Wymagania dotyczące kontroli unieważnienia certyfikatu

Nie dotyczy

4.9.7 Częstotliwość publikacji listy CRL

Unieważnione lub zawieszone certyfikaty wpisywane są na listę unieważnionych lub zawieszonych certyfikatów (CRL), podpisaną przez CA i opublikowaną w publicznym rejestrze. Lista CRL publikowana jest regularnie co godzinę (emisja zwyczajna). W szczególnych przypadkach CA może nalegać na nieplanowane opublikowanie listy CRL (natychmiastowa nadzwyczajna emisja), np. gdy unieważnienie lub zawieszenie certyfikatu następuje w wyniku podejrzenia naruszenia poufności prywatnego klucza (natychmiastowe unieważnienie lub zawieszenie). Lista CRL publikowana jest zawsze w całości. Za moment publikacji listy CRL uznaje się datę podawaną przez system Time Stamping Authority InfoCert i taki zapis jest umieszczany w dzienniku kontrolnym. Każdy element listy CRL zawiera datę i godzinę unieważnienia lub zawieszenia podane w odpowiednim formacie. W celu odciążenia sieci CA zastrzega sobie prawo do odrębnego publikowania innych list CRL stanowiących podzbiory głównej listy CRL. Uzyskanie listy CRL i zapoznanie się z nią leży w gestii użytkowników. Lista CRL, z którą należy się zapoznać w związku z konkretnym certyfikatem, jest wskazana w takim certyfikacie zgodnie z obowiązującymi przepisami prawa.

4.9.8 Maksymalne opóźnienie listy CRL

Po sprawdzeniu autentyczności wniosku o unieważnienie lub zawieszenie certyfikatu, czas oczekiwania pomiędzy przekazaniem wniosku do CA a jego realizacją poprzez opublikowanie listy CRL wynosi maksymalnie godzinę.

4.9.9 Usługi kontroli online statusu wniosku o unieważnienie certyfikatu

Oprócz publikacji listy CRL w rejestrach LDAP i HTTP, InfoCert udostępnia także usługę OCSP umożliwiającą kontrolę statusu certyfikatu. Adres URL usługi podany jest w certyfikacie. Usługa jest dostępna 24 godziny na dobę przez 7 dni w tygodniu.

Zgodność pomiędzy usługą OCSP i listą CRL jest zagwarantowana maksymalnie w ciągu godziny. Zgodność pomiędzy usługą OCSP i zaktualizowanymi informacjami podanymi przez usługę w związku z aktualizacjami listy CRL zależy od czasu oczekiwania potrzebnego do zaktualizowania listy CRL zgodnie z treścią poprzedniego punktu.
Informacje na temat statusu certyfikatu będą udostępniane do czasu wygaśnięcia certyfikatu root CA.

4.9.10 Wymagania dotyczące usług kontroli online

Patrz Aneks A

4.9.11 Inne formy unieważnienia

Nie dotyczy

4.9.12 Szczególne wymagania rekey w przypadku naruszeń

Nie dotyczy

4.9.13 Przyczyny zawieszenia certyfikatu

Procedura zawieszenia certyfikatu musi zostać przeprowadzona w przypadku wystąpienia następujących okoliczności:

1. został złożony wniosek o unieważnienie certyfikatu bez możliwości ustalenia w odpowiednim czasie autentyczności wniosku;
2. posiadacz, wnioskodawca lub zainteresowana strona trzecia, RA lub CA weszli w posiadanie elementów rodzących wątpliwości co do ważności certyfikatu lub tożsamości posiadacza bądź wnioskodawcy (np. w przypadku podejrzenia lub zgłoszenia kradzieży bądź oszustwa dotyczącego tożsamości);
3. pojawiły się wątpliwości co do bezpieczeństwa urządzenia do składania podpisu lub urządzenia OTP, jeżeli występuje;
4. konieczne jest tymczasowe przerwanie ważności certyfikatu.

W powyższych przypadkach wnioskuje się o zawieszenie certyfikatu, podając ewentualnie okres, na jaki ma on zostać zawieszony. Po upływie okresu zawieszenia lub na wniosek

o przywrócenie certyfikatu nastąpi albo ostateczne unieważnienie certyfikatu, albo przywrócenie jego ważności.
W przypadku podejrzenia kradzieży tożsamości, CA może bez uprzedniego powiadomienia dokonać zawieszenia zapobiegawczego.

4.9.14 Kto może zwrócić się o zawieszenie certyfikatu?

O zawieszenie certyfikatu, z jakiegokolwiek powodu i w dowolnym momencie, może zwrócić posiadacz. Ponadto, wniosek o zawieszenie certyfikatu może złożyć również wnioskodawca lub zainteresowana strona trzecia, z powodów oraz w trybie ustalonym w niniejszej Polityce. Wreszcie, certyfikat może zostać zawieszony z urzędu przez CA.

4.9.15 Procedury wnioskowania o zawieszenie certyfikatu

Wniosek o zawieszenie certyfikatu należy złożyć w odpowiedniej sekcji strony internetowej CA. Okres zawieszenia jest wybierany przez podmiot wnioskujący, a jeżeli nie został on określony, certyfikat zostanie zawieszony do czasu wygaśnięcia certyfikatu, a następnie unieważniony. Zawieszenie certyfikatu upływa w ostatnim dniu wnioskowanego okresu zawieszenia.
Dla niektórych klientów, w oparciu o szczególne ustalenia umowne, udostępniona jest funkcja przywrócenia certyfikatu. W takim wypadku, certyfikat można przywrócić tylko wtedy, gdy nie upłynął jego termin ważności.

4.9.15.1 Zawieszenie certyfikatu wnioskowane przez posiadacza

Posiadacz zobowiązany jest do wnioskowania o zawieszenie certyfikatu w jednym z poniższych trybów:

korzystając z funkcji zawieszenia certyfikatu dostępnej na stronie internetowej CA, lub w przypadku certyfikatów do zdalnego składania podpisu, za pośrednictwem portalu MySign (jest to narzędzie udostępnione przez InfoCert do zarządzania certyfikatem do zdalnego składania podpisu), podając wymagane dane i wykorzystując kod awaryjny przekazany w momencie wystawiania certyfikatu, jeżeli jest znany;
korzystając (o ile jest dostępna) z funkcji zawieszenia certyfikatu przy użyciu OTP dostępnej na stronie internetowej podanej w dokumentacji umownej dostarczonej w chwili rejestracji; dzwoniąc do call center CA i podając wymagane informacje. W razie braku kodu awaryjnego i tylko w przypadku, gdy przyczyną wnioskowania o zawieszenie certyfikatu jest naruszenie poufności klucza, call center, po zweryfikowaniu numeru telefonu dzwoniącego, dokonuje natychmiastowego zawieszenia certyfikatu na okres 10 (dziesięciu) dni kalendarzowych w oczekiwaniu na pisemny wniosek posiadacza; w razie nieotrzymania w wyznaczonym terminie podpisanego wniosku, CA podejmuje działania zmierzające do przywrócenia

certyfikatu;
za pośrednictwem punktu rejestracji, który prosi o przekazanie niezbędnych danych oraz
dokumentów i przeprowadza wszelkie kontrole dotyczące tożsamości posiadacza; następnie,

zwraca się o zawieszenie certyfikatu do CA,
używając funkcji zawieszenia dostępnej na stronie internetowej RA umożliwiającej przejście do usług CMS.

Jeżeli certyfikat będący przedmiotem wniosku o zawieszenie zawiera informacje dotyczące roli posiadacza, CA podejmie kroki mające na celu poinformowanie o dokonaniu zawieszenia certyfikatu ewentualnej zainteresowanej strony trzeciej, z którą zostały zawarte określone porozumienia.

Jeżeli certyfikat będący przedmiotem wniosku o zawieszenie zawiera dane organizacji, CA podejmie kroki mające na celu poinformowanie tego podmiotu o dokonaniu zawieszenia.

Jeżeli umowa dotycząca certyfikatu będącego przedmiotem wniosku o zawieszenie przewiduje taką możliwość, CA poinformuje o dokonaniu zawieszenia również wnioskodawcę. Ze względu na sam charakter certyfikatu short-term, nie została przewidziana możliwość złożenia wniosku o zawieszenie przez posiadacza.

4.9.15.2 Zawieszenie wnioskowane przez wnioskodawcę lub zainteresowaną stronę trzecią

Wnioskodawca lub zainteresowana strona trzecia mogą zwrócić się o zawieszenie certyfikatu posiadacza, wypełniając odpowiedni formularz dostępny na stronie internetowej CA oraz w punktach RA, podając uzasadnienie swojego wniosku, a także załączając odpowiednią dokumentację, jeżeli istnieje, oraz podając dane posiadacza przekazane CA w momencie wystawienia certyfikatu.

CA weryfikuje autentyczność wniosku i informuje o tym fakcie posiadacza, korzystając ze sposobów komunikacji ustalonych w momencie składania wniosku o wydanie certyfikatu, a następnie dokonuje zawieszenia certyfikatu. Dodatkowe sposoby składania wniosku o zawieszenie certyfikatu przez wnioskodawcę lub zainteresowaną osobę trzecią mogą być określone w ewentualnych umowach zawartych przez wnioskodawcę lub zainteresowaną osobę trzecią i CA.

W przypadku wniosku o zawieszenie certyfikatów LongTerm i OneShot, z wyłączeniem certyfikatów short-term, wnioskodawca może zwrócić się o zawieszenie certyfikatu posiadacza poprzez uwierzytelnienie się w systemach udostępnionych przez CA, również przy użyciu usług aplikacyjnych, działając w sposób opisany w dokumentacji umownej. Ze względu na sam charakter certyfikatu short-term, nie została przewidziana możliwość złożenia wniosku o zawieszenie przez Wnioskodawcę.

4.9.15.3 Zawieszenie z inicjatywy CA

Z wyjątkiem pilnych przypadków, CA uprzedza posiadacza o zamiarze

zawieszenia certyfikatu, podając powód jego zawieszenia, datę rozpoczęcia okresu

zawieszenia i datę jego zakończenia. W każdym przypadku informacje te zostaną przekazane posiadaczowi w możliwie najkrótszym czasie.
Jeżeli certyfikat będący przedmiotem zawieszenia zawiera informacje dotyczące roli posiadacza, CA podejmie kroki mające na celu poinformowanie o dokonaniu zawieszenia certyfikatu ewentualnej zainteresowanej strony trzeciej, z którą zostały zawarte określone porozumienia. Jeżeli certyfikat będący przedmiotem zawieszenia zawiera dane organizacji, CA podejmie kroki mające na celu poinformowanie tego podmiotu o dokonaniu zawieszenia.
Jeżeli umowa dotycząca certyfikatu będącego przedmiotem zawieszenia przewiduje taką możliwość, CA poinformuje o dokonaniu zawieszenia również wnioskodawcę.

4.9.16 Ograniczenia czasowe dotyczące okresu zawieszenia certyfikatu

Okres zawieszenia jest wybierany przez podmiot wnioskujący i nie może być dłuższy niż okres ważności certyfikatu. Po upływie wnioskowanego okresu zawieszenia ważność certyfikatu zostanie przywrócona poprzez usunięcie certyfikatu z listy unieważnionych i zawieszonych certyfikatów (CRL). Przywrócenie certyfikatu nastąpi w ciągu 24 godzin po upływie okresu zawieszenia. Jeżeli dzień kończący okres zawieszenia zbiega się z dniem ustania ważności certyfikatu, zawieszenie zostanie przekształcone w unieważnienie obowiązujące od początku okresu zawieszenia.
Jeżeli umowa przewiduje taką możliwość, można zwrócić się o przywrócenie certyfikatu przed datą zakończenia okresu zawieszenia.
W przypadkach, gdy certyfikat został zawieszony poprzez CMS, można skorzystać z funkcji przywrócenia dostępnej na stronie internetowej umożliwiającej przejście do usług CMS.

4.10 Usługi dotyczące statusu certyfikatu

4.10.1 Cechy operacyjne

Informacje na temat statusu certyfikatów dostępne są za pośrednictwem listy CRL lub usługi OCSP. Numer seryjny unieważnionego certyfikatu pozostaje na liście CRL również po upływie okresu ważności certyfikatu, a przynajmniej do czasu ważności certyfikatu CA.
Informacje przekazywane przez usługę OCSP na temat certyfikatów są aktualizowane w czasie rzeczywistym.

4.10.2 Dostępność usługi

Usługa OCSP i lista CRL są dostępne 24 godziny na dobę przez 7 dni w tygodniu.

4.10.3 Cechy opcjonalne

Nie dotyczy

4.11 Rezygnacja z usług oferowanych przez CA

Stosunek prawny między posiadaczem i/lub wnioskodawcą a urzędem certyfikacji kończy się wraz z upływem okresu ważności certyfikatu lub z chwilą jego unieważnienia, z wyjątkiem szczególnych przypadków określonych w postanowieniach umowy.

4.12 Deponowanie klucza u osób trzecich i jego odzyskiwanie

Nie dotyczy

5 ŚRODKI BEZPIECZEŃSTWA I KONTROLI

TSP InfoCert stworzył szereg zabezpieczeń chroniących system informatyczny dostarczający usługi certyfikacji cyfrowej. Wdrożony system zabezpieczeń obejmuje trzy poziomy:

- poziom fizyczny, mający na celu zabezpieczenie środowiska, w którym TSP świadczy usługę,
- poziom proceduralny obejmujący kwestie typowo organizacyjne,
- poziom logiczny poprzez zastosowanie środków technologicznych z zakresu sprzętu i oprogramowania służących do rozwiązywania problemów i przeciwdziałania zagrożeniom związanym z rodzajem świadczonej usługi oraz używaną infrastrukturą.

Zadaniem powyższego systemu zabezpieczeń jest zapobieganie zagrożeniom wynikającym z awarii systemów, sieci i aplikacji, a także z nieupoważnionego przechwytywania lub modyfikacji danych.
Wyciąg z polityki bezpieczeństwa InfoCert udostępniany jest na wniosek, który należy wysłać na adres certyfikowanej poczty elektronicznej: infocert@legalmail.it.
Polityki bezpieczeństwa InfoCert są poddawane przeglądowi co najmniej raz w roku, a także są aktualizowane w razie jakichkolwiek istotnych zmian. Każdy przegląd jest widoczny w dokumencie, również wtedy, gdy nie było konieczne wprowadzanie jakichkolwiek zmian.

5.1 Bezpieczeństwo fizyczne

Wdrożone środki zapewniają odpowiednie gwarancje bezpieczeństwa w odniesieniu do następujących elementów:

- właściwości budynku i konstrukcji;
- czynne i bierne systemy antywłamaniowe;
- kontrola dostępów fizycznych;
- zasilanie elektryczne i klimatyzacja;
- ochrona przeciwpożarowa;
- ochrona przeciwpowodziowa;
- sposoby archiwizowania nośników magnetycznych;
- miejsca archiwizowania nośników magnetycznych.

5.1.1 Lokalizacja i rozwiązania konstrukcyjne

Główna siedziba Data Center InfoCert znajduje się w Padwie. Disaster Recovery

zlokalizowane jest w Modenie i jest połączone ze wspomnianym wyżej Data Center specjalnym nadmiarowym łączem opartym na dwóch odrębnych sieciach MPLS z prędkością transferu danych 40 Gb/s z możliwością upgrade'u do 100 Gb/s.

W obu miejscach wyodrębnione zostały pomieszczenia dysponujące najwyższym poziomem zabezpieczeń, zarówno fizycznych jak i logicznych, wśród których znajduje się certyfikowany sprzęt informatyczny stanowiący centralny ośrodek certyfikacji cyfrowej, sygnatur czasowych oraz zdalnego i automatycznego składania podpisów.

W przypadku usług w trybie ciągłości operacyjnej z wartościami RTO/RPO bliskimi zeru, niektóre komponenty usług CA dotyczące publikacji list CRL i usługi OCSP są hostowane w infrastrukturze chmurowej dostawców zewnętrznych, odpowiednio w Regionie Europa Frankfurt i w Regionie Europa Irlandia. Ponadto, w celu zagwarantowania ciągłości operacyjnej dla CA „InfoCert Qualified Electronic Signature CA 4" wykonuje się szyfrowaną kopię danych w chmurze w Regionie Europa Mediolan.

Dostawcy, z których korzysta InfoCert, posiadają certyfikaty zgodności z normami ISO/IEC 27001:2013 i ISO/IEC 9001:2015. Jeśli chodzi o infrastrukturę chmurową, dostawcy posiadają również certyfikaty 27017:2015, 27018:2019.

Rysunek 1 – sterRecovery

5.1.2 Dostęp fizyczny

Dostęp do Data Center regulowany jest procedurami bezpieczeństwa InfoCert. Wewnątrz Data Center znajduje się bunkier, w którym umieszczono systemy CA, dla których wymagany jest dodatkowy poziom zabezpieczeń.

5.1.3 Instalacja elektryczna i klimatyzacja

Siedziba w Padwie spełnia kryteria poziomu 3 zgodnie z normą ANSI TIA 942.

Pomieszczenia techniczne wyposażone są w system zasilania elektrycznego zaprojektowany w sposób, zapobiegający awariom i przede wszystkim przerwom w świadczeniu usług. Zasilanie systemów oparte jest na najnowocześniejszych rozwiązaniach technologicznych, zwiększających niezawodność i gwarantujących rezerwę mocy dla realizacji najbardziej kluczowych funkcji potrzebnych dla świadczonych usług.

Infrastruktura odpowiedzialna za zasilanie przewiduje:

- zasilacze bezprzerwowe prądu przemiennego wyposażone w akumulatory (UPS);
- dostępność napięcia przemiennego (220 – 380 V AC);
- szafy zasilane bezpiecznymi liniami zapewniającymi odpowiedni zapas mocy, o parametrach wynikających z uzgodnionego zapotrzebowania;
- generatory zasilania awaryjnego;
- system automatycznego przełączania i synchronizacji pracy poszczególnych generatorów, sieci i akumulatorów (STS).

Każda szafa sterująca zainstalowana w Data Center korzysta z dwóch linii elektrycznych, które zapewniają utrzymanie wysokiej dostępności (HA) w razie przerwy w działaniu jednej z dostępnych linii.

Działanie szafy sterującej jest zdalnie monitorowane. Prowadzone są również stałe kontrole stanu linii elektrycznej (ON/OFF) i pobieranej mocy (obciążenie żadnej z linii nie powinno przekraczać 50%).

Temperatura w pomieszczeniach technicznych utrzymywana jest zazwyczaj pomiędzy 20°C a 27°C, przy wilgotności względnej od 30 do 60%. Instalacje wyposażone są w skraplacze z zamkniętym systemem gromadzenia i odprowadzania kondensatu, którego praca kontrolowana jest przez sondy zalania. Cały system klimatyzacji wyposażony jest w generatory gwarantujące awaryjne zasilanie w przypadku braku dostaw energii elektrycznej. System chłodzenia szaf sterujących gwarantuje chłodzenie przy maksymalnym przewidzianym obciążeniu 10 kW dla szafy pojedynczej i 15 kW dla dwóch połączonych szaf.

5.1.4 Ochrona przeciwpowodziowa

Na obszarze, na którym zlokalizowana jest nieruchomość, nie występują zagrożenia środowiskowe wynikające z bliskości „niebezpiecznych” instalacji. W trakcie

projektowania budynku zostały podjęte odpowiednie kroki mające na celu odseparowanie potencjalnie niebezpiecznych pomieszczeń, takich jak pomieszczenia mieszczące agregat prądotwórczy lub instalację ciepłowniczą.
Pomieszczenia mieszczące sprzęt znajdują się na parterze budynku, na poziomie nieco wyższym

niż poziom drogi.

5.1.5 Ochrona przeciwpożarowa

W budynku Data Center znajduje się system wykrywania dymu sterowany przez adresowalną centralę analogową NOTIFIER z czujnikami optycznymi rozmieszczonymi w pomieszczeniach i w podwieszanym suficie oraz z czujnikami z systemem pobierania próbek powietrza zainstalowanymi pod podłogą i w przewodach wentylacyjnych.
System automatycznego wykrywania pożarów połączony jest z instalacją automatycznego gaszenia przy użyciu ekologicznych gazów gaśniczych ARGON IG-01. W momencie równoczesnego zadziałania dwóch czujników w tej samej strefie następuje użycie substancji gaszącej w danej strefie.
Dla każdej strefy pożarowej przewidziana jest jedna odrębna instalacja gaśnicza. Zgodnie z obowiązującymi przepisami ustawowymi i wykonawczymi, w obiekcie znajdują się również przenośne środki gaśnicze.

5.1.6 Nośniki pamięci

Jeśli chodzi o platformę storage, stosowane rozwiązanie zakłada stosowanie dla części NAS systemów NetApp (FAS 8060). Dla części SAN wdrożono natomiast infrastrukturę dla części data center opartej na technologiach Infinidat obejmujących 2 bloki InfiniBox generacji F4000 i F6000. W części CA insfrastruktura opiera się na technologii Pure Storage.

5.1.7 Utylizacja odpadów

InfoCert posiada certyfikowany system zarządzania środowiskiem według normy ISO 14001. Organizacja posiada wewnętrzne procedury bezpiecznego usuwania danych z urządzeń do przechowywania danych klasy Enterprise, korzystając z dostawców zapewniających ich usunięcie. Ponadto, stosuje cykl gospodarowania odpadami zgodny z obowiązującymi przepisami krajowymi obejmujący procedury gospodarowania odpadami i monitorowania cyklu życia odpadów i korzysta wyłącznie z dostawców uprawnionych do transportu i utylizacji odpadów.

5.1.8 Kopie zapasowe poza obiektem

W siedzibie Disaster Recovery odbywa się replikacja danych i wykonywana jest kopia zapasowa na pamięci zewnętrznej osób trzecich.

5.2 Kontrole proceduralne

5.2.1 Kluczowe role

Kluczowe role pełnią osoby spełniające niezbędne wymagania dotyczące doświadczenia, profesjonalizmu oraz przygotowania technicznego i prawniczego, które są stale weryfikowane w ramach prowadzonych ocen rocznych.
Lista nazwisk i schemat organizacyjny osób pełniących kluczowe role przekazana została do AgID przy okazji pierwszej akredytacji i jest stale aktualizowana, aby odzwierciedlała naturalne zmiany zachodzące w strukturze przedsiębiorstwa.

5.3 Kontrola personelu

5.3.1 Kwalifikacje, doświadczenie i wymagane pozwolenia

Po sporządzeniu rocznego planu zasobów ludzkich, kierownik funkcyjny lub kierownik jednostki organizacyjnej określa cechy i umiejętności osoby, którą chce wprowadzić do struktury (*job profile*). Następnie, wspólnie z osobą odpowiedzialną za rekrutację, uruchomiony zostaje proces poszukiwania i rekrutacji.

5.3.2 Procedury weryfikacji doświadczenia

Wybrani kandydaci biorą udział w procesie rekrutacji, uczestnicząc najpierw w rozmowie poznawczo-motywacyjnej z osobą odpowiedzialną za rekrutację, a następnie w rozmowie technicznej z kierownikiem funkcyjnym lub kierownikiem jednostki organizacyjnej, której celem jest zweryfikowanie umiejętności zadeklarowanych przez kandydata. Pozostałymi narzędziami kontrolnymi są ćwiczenia i testy.

5.3.3 Wymagania dotyczące szkoleń

W celu ochrony przed naruszeniem lub zakłóceniem bezpieczeństwa całego systemu lub przed podjęciem nieupoważnionych działań ze strony pojedynczych jednostek, zarządzanie operacyjne systemem powierzone jest różnym osobom, których zadania są rozdzielone i dokładnie zdefiniowane. Pracownik ds. projektowania i świadczenia usług certyfikacyjnych jest pracownikiem InfoCert i został wybrany na podstawie posiadanego doświadczenia w zakresie projektowania, realizacji i świadczenia usług informatycznych, a także dzięki cechom gwarantującym niezawodność i przestrzeganie zasad poufności. Działania szkoleniowe planowane są okresowo i mają na celu poszerzanie wiedzy na temat zadań powierzanych pracownikom. W szczególności, przed włączeniem pracownika do działań operacyjnych, przeprowadzane są szkolenia mające na celu przekazanie wiedzy (technicznej, organizacyjnej i proceduralnej) niezbędnej do wykonywania powierzonych mu zadań.

5.3.4 Częstotliwość przeprowadzania szkoleń

Na początku każdego roku przeprowadzana jest analiza potrzeb szkoleniowych, mająca na celu zdefiniowanie planu szkoleń do zrealizowania w ciągu roku. Analiza ta przebiega w następujący sposób:

- spotkanie z dyrekcją przedsiębiorstwa w celu zebrania danych dotyczących potrzeb szkoleniowych niezbędnych do osiągnięcia celów biznesowych;
- wywiady z kierownikami w celu ustalenia szczegółowych potrzeb szkoleniowych ich obszarów działania;
- przekazanie zebranych danych dyrekcji przedsiębiorstwa w celu zamknięcia i zatwierdzenia planu szkoleń.

Do lutego uzgodniony w ten sposób plan szkoleń zostaje podany do wiadomości pracownikom.

5.3.5 Częstotliwość rotacji w zmianowym systemie pracy

Obecność w miejscu pracy lub praca w systemie elastycznym (smart working) jest wymagana w przedziale godzinowym od 8.00 do 19.00, od poniedziałku do piątku.
Obecność pracowników w pomieszczeniach produkcyjnych w okresie nocnym i w święta jest zagwarantowana na podstawie zmianowego planu dostępności pracowników przygotowywanego co miesiąc przez kierownika jednostki organizacyjnej, co najmniej z dziesięciodniowym wyprzedzeniem (10). W zależności od potrzeb interwencje mogą być prowadzone zdalnie (zdalna interwencja) lub wymagają dostępu do placówek.
Pod warunkiem spełnienia niezbędnych wymagań technicznych i zawodowych, przedsiębiorstwo zapewnia wprowadzanie do planu dostępności jak największej liczby pracowników, przyznając pierwszeństwo tym, którzy o to wnioskują.

5.3.6 Sankcje z tytułu nieuprawnionych działań

Procedura nakładania sankcji na pracowników jest uregulowana w dokumencie „CCNL Metalmeccanici e installazione impianti industria privata”
[Włoski układ zbiorowy dla pracowników branży obróbki metalu i montażu linii w przemyśle prywatnym].

5.3.7 Nadzorowanie pracowników kontraktowych

Dostęp dla pracowników kontraktowych jest regulowany specjalną polityką przedsiębiorstwa.

5.3.8 Dokumentacja, którą personel zobowiązany jest dostarczyć

W momencie zatrudnienia pracownik zobowiązany jest dostarczyć kopię ważnego dokumentu tożsamości, kopię ważnej karty ubezpieczenia zdrowotnego oraz zdjęcie do karty

dostępu do pomieszczeń. Następnie musi podpisać zgodę na przetwarzanie danych osobowych i zobowiązanie do nierozpowszechniania poufnych informacji i/lub dokumentów. Na koniec musi zapoznać się z Kodeksem etycznym i Netykietą InfoCert.

5.4 Prowadzenie dziennika kontrolnego

Zdarzenia związane z zarządzaniem CA i cyklem życia certyfikatu gromadzone są w dzienniku kontrolnym zgodnie z postanowieniami rozporządzenia i przepisami technicznymi [5].

5.4.1 Rodzaje rejestrowanych zdarzeń

Rejestracji podlegają zdarzenia dotyczące bezpieczeństwa, uruchamiania i wyłączania, awarii systemu i sprzętu, działania zapory sieciowej i routerów, a także prób uzyskania dostępu do systemu PKI. Gromadzone są wszystkie dane i dokumenty wykorzystywane na etapie identyfikacji oraz przyjmowania wniosku składanego przez wnioskodawcę: kopia dokumentu tożsamości, dokumentacja umowna, wyciąg z rejestru przedsiębiorców itd.
Rejestracji podlegają zdarzenia związane z rejestracją i cyklem życia certyfikatów: wnioski o wydanie i odnowienie, dokonane rejestracje certyfikatu, generowanie, przekazywanie oraz ewentualne decyzje o unieważnieniu lub zawieszeniu certyfikatu.
Rejestracji podlegają wszystkie zdarzenia związane z personalizacją urządzeń do składania podpisu.
Rejestracji podlegają wszystkie fizyczne dostępy do ściśle zabezpieczonych pomieszczeń, w których znajdują się maszyny CA.
Rejestracji podlegają wszystkie dostępy logiczne do aplikacji CA.
Każde zdarzenie zapisywane jest z datą oraz godziną jego wystąpienia w systemie.

5.4.2 Częstotliwość przetwarzania i zapisywania dziennika kontrolnego

Przetwarzanie i grupowanie danych, a także ich zapisywanie w serwisie przechowywania danych InfoCert spełniającego normy odbywa się raz w miesiącu.

5.4.3 Okres przechowywania dziennika kontrolnego

Dziennik kontrolny przechowywany jest przez CA przez co najmniej 20 lat. Dzienniki dotyczące cyklu życia certyfikatu są przechowywane przez co najmniej 20 lat od wygaśnięcia certyfikatu, do maksymalnie 23 lat od daty wydania certyfikatu.

5.4.4 Zabezpieczenie dziennika kontrolnego

Zabezpieczenie dziennika kontrolnego gwarantuje serwis przechowywania danych InfoCert spełniający wymogi dokumentów informatycznych.

5.4.5 Procedury tworzenia kopii zapasowych dziennika kontrolnego

Serwis przechowywania danych InfoCert spełniający wymogi dokumentów informatycznych wdraża politykę i procedurę tworzenia kopii zapasowych (backup), zgodnie z instrukcją bezpieczeństwa przewidzianą dla powyższego systemu.

5.4.6 Procedura zapisywania dziennika kontrolnego

Gromadzenie dzienników zdarzeń następuje automatycznie, a ich zapisywanie odbywa się na zasadach przewidzianych przez serwis przechowywania danych InfoCert spełniający normy i opisany w instrukcji bezpieczeństwa powyższego systemu.

5.4.7 Zawiadomienia w przypadku stwierdzenia podatności systemu na zagrożenia

Nie dotyczy

5.4.8 Ocena podatności na zagrożenia

InfoCert okresowo przeprowadza ocenę podatności systemu na zagrożenia (vulnerability assessment) oraz testy penetracyjne (penetration test). Następnie, w zależności od wyników, wdraża wszelkie środki zaradcze w celu zabezpieczenia aplikacji.

5.5 Archiwizacja protokołów

5.5.1 Rodzaje archiwizowanych protokołów

Dla najważniejszych zdarzeń danego urzędu certyfikacji sporządza się i archiwizuje odpowiednie protokoły. Protokoły przechowywane są przez urząd certyfikacji przez 20 lat za pomocą serwisu przechowywania danych InfoCert spełniającego wymogi dokumentów informatycznych.

5.5.2 Zabezpieczenie protokołów

Zabezpieczenie protokołów gwarantuje serwis przechowywania danych InfoCert spełniający wymogi dokumentów informatycznych.

5.5.3 Procedury tworzenia kopii zapasowych protokołów

Serwis przechowywania danych InfoCert spełniający wymogi dokumentów informatycznych wdraża politykę i procedurę tworzenia kopii zapasowych (backup), zgodnie z instrukcją bezpieczeństwa przewidzianą dla powyższych usług.

5.5.4 Wymagania dotyczące sygnatur czasowych protokołów

Nie dotyczy

5.5.5 System zapisywania archiwów

Gromadzenie protokołów następuje automatycznie, a ich zapisywanie odbywa się na zasadach przewidzianych przez serwis przechowywania danych InfoCert spełniający wymogi dokumentów informatycznych i opisany w instrukcji bezpieczeństwa.

5.5.6 Procedury dostępu do informacji zawartych w archiwach oraz ich weryfikacji

Wszystkie dane są przechowywane za pomocą serwisu przechowywania danych InfoCert spełniającego wymogi dokumentów informatycznych, który przewiduje wyrywkowe kontrole stanu systemu i integralności danych. Dane są udostępniane zgodnie z postanowieniami przepisów.

5.6 Wymiana prywatnego klucza CA

CA przeprowadza procedury okresowej wymiany prywatnego klucza wykorzystywanego do podpisywania certyfikatów w sposób umożliwiający posiadaczowi używanie posiadanego certyfikatu do czasu jego wygaśnięcia. Każda wymiana spowoduje zmianę niniejszego Podręcznika obsługi oraz konieczność przekazania odpowiedniej informacji organowi nadzoru (AgID).

5.7 Naruszenie prywatnego klucza CA i disaster recovery

5.7.1 Procedury zarządzania incydentami

CA opisał procedury zarządzania incydentami w ramach systemu SZBI certyfikowanego zgodnie z normą ISO 27001. Każdy ewentualny incydent niezwłocznie po jego wykryciu jest poddawany dokładnej analizie i określa się działania naprawcze, a kierownik serwisu sporządza stosowny protokół. Protokół jest podpisany elektronicznie i jedna jego kopia jest przesyłana również do AgID, wraz z informacją o działaniach interwencyjnych mających na celu wyeliminowanie prawdopodobnych przyczyn wystąpienia incydentu, jeżeli znajduje się pod kontrolą InfoCert, zgodnie z art. 19 rozporządzenia eIDAS.

5.7.2 Uszkodzenie sprzętu, oprogramowania lub danych

W przypadku awarii bezpiecznego urządzenia do składania podpisu HSM zawierającego klucze certyfikacyjne, należy użyć zapasowej kopii klucza, odpowiednio zapisanej i przechowywanej, bez konieczności unieważnienia odpowiadającego mu certyfikatu CA.
Oprogramowanie i dane są przedmiotem regularnie wykonywanych kopii zapasowych, zgodnie z obowiązującymi procedurami wewnętrznymi.

5.7.3 Procedury w razie naruszenia prywatnego klucza CA

Naruszenie klucza certyfikacyjnego uważa się za zdarzenie szczególnie krytyczne, ponieważ prowadzi do utraty ważności wystawionych certyfikatów podpisanych z użyciem tego klucza. Należy zatem zwrócić szczególną uwagę na zabezpieczenie klucza certyfikacyjnego, a także na wszelkie czynności w zakresie rozwijania i konserwacji systemu, które mogą mieć na niego wpływ.
Mimo że jest to rzadki przypadek, InfoCert opracował szczegółową procedurę, którą należy zastosować w ramach systemu SZBI certyfikowanego zgodnie z normą ISO 27001, informując o tym CAB. Po stwierdzeniu naruszenia prywatnego klucza CA InfoCert niezwłocznie:

- informuje włoski organ nadzoru AgID w celu usunięcia klucza z TSL oraz CAB,
- zawiadamia RA oraz klientów, niezależnie od tego, czy są posiadaczami certyfikatu, czy wnioskodawcami, przekazując informację bezpośrednio, o ile to możliwe, i umieszczając komunikat na stronie internetowej InfoCert,
- unieważnia certyfikaty, których dotyczy naruszenie, ewentualnie dokonuje wydania i akredytacji nowego root CA oraz w wiarygodny sposób przekazuje informacje o statusie unieważnienia certyfikatów.

5.7.4 Świadczenie usług CA w przypadku katastrof

InfoCert wdrożył niezbędne procedury mające na celu zagwarantowanie ciągłości usług również w sytuacjach wysoce krytycznych lub w przypadku katastrof.

5.8 Zaprzestanie świadczenia usług przez CA lub RA

W przypadku zaprzestania prowadzenia działalności certyfikacyjnej, InfoCert poinformuje o tym organ nadzoru (AgID) oraz jednostkę oceniającą zgodność (CAB) co najmniej z trzymiesięcznym (3) wyprzedzeniem, wskazując ewentualnie podmiot certyfikujący, który go zastąpi, i który będzie depozytariuszem rejestru certyfikatów oraz stosownej dokumentacji. Z takim samym okresem wyprzedzenia InfoCert poinformuje o zaprzestaniu prowadzenia działalności wszystkich posiadaczy wydanych

przez niego certyfikatów. W informacji tej, w razie braku wskazania zastępczego podmiotu certyfikującego, zostanie wyraźnie podane, że wszystkie certyfikaty, które będą ważne w momencie zaprzestania prowadzenia działalności przez CA, zostaną unieważnione.

W razie zaprzestania prowadzenia działalności przez CA informacja o unieważnieniu zostanie przekazana poprzez wydanie ostatniej listy CA zgodnej z wymogami normy ETSI 319 411-1.

Dodatkowe informacje znajdują się w dokumencie TSP „Termination Plan dei Servizi di Certificazione Digitale, Validazione Temporale e Convalida firme" [Plan zakończenia usług certyfikacji cyfrowej, znaczników czasu i walidacji podpisów], który jest dostępny w jednostce certyfikującej.

6 KONTROLE BEZPIECZEŃSTWA TECHNOLOGICZNEGO

6.1 Instalacja i generowanie pary kluczy certyfikacyjnych

W celu prowadzenia swojej działalności urząd certyfikacji musi wygenerować parę kluczy certyfikacyjnych do podpisywania certyfikatów posiadaczy.
Klucze generowane są tylko przez personel wyraźnie wyznaczony do tego zadania. Generowanie kluczy i podpisów odbywa się w ramach dedykowanych modułów kryptograficznych, certyfikowanych zgodnie z obowiązującymi przepisami.
Ochronę kluczy prywatnych CA zapewnia moduł kryptograficzny do generowania i używania danego klucza. Klucz prywatny może być generowany tylko w obecności jednocześnie dwóch operatorów wyznaczonych do generowania. Generowanie kluczy odbywa się w obecności kierownika ds. usług certyfikacyjnych.
Klucze prywatne CA są duplikowane wyłącznie w celu ich odzyskania po uszkodzeniu bezpiecznego urządzenia do składania podpisu, zgodnie z kontrolowaną procedurą, która przewiduje podział klucza i kontekstu na wiele urządzeń, zgodnie z kryteriami bezpieczeństwa urządzenia HSM.
Moduł kryptograficzny używany do generowania kluczy i do składania podpisu spełnia wymagania, które zapewniają:

- zgodność pary z wymogami ustanowionymi przez stosowane algorytmy generowania i weryfikacji;
- równe prawdopodobieństwo wygenerowania wszystkich możliwych par;
- identyfikację podmiotu uruchamiającego procedurę generowania;
- generowanie podpisu wewnątrz urządzenia w sposób uniemożliwiający przechwycenie wartości użytego prywatnego klucza.

6.1.1 Generowanie pary kluczy posiadacza

Klucze asymetryczne generowane są w bezpiecznym urządzeniu do składania podpisu SSCD lub QSCD a także typu HSM z wykorzystaniem natywnych funkcji oferowanych przez te urządzenia.
W przypadku, gdy urządzenie nie zostanie udostępnione przez CA, wnioskodawca musi zapewnić, że urządzenie spełnia wymagania obowiązujących przepisów,

przedstawiając stosowną dokumentację i poddając się okresowym audytom. W przypadku HSM, InfoCert zastrzega sobie prawo przewodniczenia Key Ceremony.

6.1.2 Dostarczanie klucza prywatnego wnioskodawcy

Klucz prywatny znajduje się w urządzeniu kryptograficznym, niezależnie od tego, czy jest to SSCD czy QSCD. Dla certyfikatów do zdalnego i automatycznego składania podpisu urządzeniem kryptograficznym jest zawsze HSM. Wraz z dostarczeniem urządzenia kryptograficznego posiadaczowi wchodzi on w pełne posiadanie klucza prywatnego, z którego może korzystać wyłącznie za pomocą kodu PIN, który udostępniany jest do jego wyłącznej wiadomości.
W przypadku procesu rejestracji przeprowadzanego w obecności posiadacza urządzenie dostarczane jest natychmiast po wygenerowaniu kluczy.
Jeżeli proces rejestracji nie jest przeprowadzany w obecności posiadacza, urządzenie dostarczane jest zgodnie z procedurami określonymi w umowie, dbając zawsze przekazywanie urządzenia i informacji na temat jego używania różnymi kanałami, czyli dostarczanie ich posiadaczowi w dwóch różnych momentach czasowych. W niektórych przypadkach urządzenia mogą być już dostępne dla posiadacza, ponieważ zostały wcześniej dostarczone zgodnie z bezpiecznymi procedurami i po uprzedniej identyfikacji podmiotu.

6.1.3 Dostarczanie klucza publicznego CA

Nie dotyczy

6.1.4 Dostarczanie klucza publicznego użytkownikom

Na wniosek wnioskodawcy jest on również publikowany w rejestrze publicznym, z którego może zostać pobrany przez użytkownika,
przy czym nie dotyczy to certyfikatów LongTerm i OneShot.

6.1.5 Algorytm i długość kluczy

Para kryptograficznych kluczy certyfikacyjnych generowana jest w wyżej wymienionym urządzeniu kryptograficznym.
Kluczami root CA, które podpisują wydawane nowe certyfikaty, mogą być:

- klucze asymetryczne RSA o długości nie mniejszej niż 4096 bitów;
- klucze asymetryczne EC na jednej z krzywych eliptycznych przewidzianych w dokumencie ETSI TS 119 312 – Cryptographic Suites o długości nie mniejszej niż 256 bitów.

Kluczami podmiotu mogą być:

- klucze asymetryczne RSA o długości nie mniejszej niż 2048 bitów;

- klucze asymetryczne EC na jednej z krzywych eliptycznych przewidzianych w dokumencie ETSI TS 119 312 – Cryptographic Suites o długości nie mniejszej niż 256 bitów.

6.1.6 Kontrola jakości i generowanie klucza publicznego

Używane urządzenia są certyfikowane zgodnie z wysokimi standardami bezpieczeństwa (patrz pkt 6.2.1) i zapewniają, że klucz publiczny jest poprawny i losowy. Przed wydaniem certyfikatu CA sprawdza, czy klucz publiczny nie został już użyty.

6.1.7 Cel użycia klucza

6.1.7.1 Użycie klucza CA

Klucz CA jest używany wyłącznie do podpisywania certyfikatów posiadaczy, list certyfikatów unieważnionych i certyfikatów OCSP. Rozszerzenie KeyUsage certyfikatu CA zawiera podpis certyfikatów (keyCertSign) podpis listy CRL (cRLSign).
Odpowiedzi OCSP są podpisywane za pomocą stosownych certyfikatów z extKeyUsage o wartości ocspSigning.

6.1.7.2 Użycie klucza posiadacza

Cel użycia klucza posiadacza określony jest przez rozszerzenie KeyUsage, zgodnie z definicją zawartą w standardzie X.509. Większość certyfikatów opisanych w niniejszej Polityce zawiera tylko KeyUsage „niezaprzeczalność". Dozwolone są wyjątki zidentyfikowane określonymi OID, aby umożliwić również dwa cele: „niezaprzeczalność" i „podpis cyfrowy" i trzy cele: „niezaprzeczalność", „podpis cyfrowy" i „szyfrowanie klucza". Ten ostatni typ jest używany na przykład w hiszpańskich organach administracji publicznej zgodnie z odniesieniami prawnymi [17], [18], [19].

6.2 Ochrona klucza prywatnego i kontrole techniczne modułu kryptograficznego

6.2.1 Kontrole i standardy modułu kryptograficznego

Moduły kryptograficzne używane przez InfoCert dla kluczy certyfikacyjnych (CA) i respondera OCSP posiadają w Europie zatwierdzenie FIPS 140 Level 3 oraz Common Criteria (CC) Information Technology Security Evaluation Assurance Level (EAL) EAL 4 + Type 3 (EAL 4 Augmented by AVA_VLA.4 and AVA_MSU.3).
Karty elektroniczne używane przez InfoCert posiadają certyfikację jako urządzenia kwalifikowane (QSCD) zgodnie z rozporządzeniem eIDAS.
Moduły kryptograficzne używane przez InfoCert dla kluczy podpisu zdalnego i automatycznego posiadacza znajdują się na liście notyfikowanych QSCD zgodnie z

treścią art. 3 rozporządzenia eIDAS 910/2014.

6.2.2 Kontrola klucza prywatnego CA przez kilka osób

Dostęp do urządzeń zawierających klucze certyfikacyjne odbywa się tylko w obecności dwóch osób uwierzytelnionych w tym samym czasie.

6.2.3 Deponowanie klucza prywatnego CA u osób trzecich

Nie dotyczy

6.2.4 Kopia zapasowa prywatnego klucza CA

Kopia zapasowa kluczy przechowywana jest w sejfie, do którego dostęp mają wyłącznie osoby, które nie mają dostępu do urządzeń HSM. Ewentualne przywrócenie kopii zapasowej wymaga zatem obecności zarówno personelu mającego dostęp do urządzeń, jak i pracowników, którzy mają dostęp do sejfu.

6.2.5 Archiwizacja klucza prywatnego CA

Nie dotyczy

6.2.6 Przeniesienie klucza prywatnego z modułu lub na moduł kryptograficzny

Nie dotyczy

6.2.7 Zapisywanie klucza prywatnego na module kryptograficznym

Klucz certyfikacyjny jest generowany i zapisywany w bezpiecznym miejscu urządzenia kryptograficznego obsługiwanego przez podmiot certyfikujący, które uniemożliwia jego eksport. Ponadto, w przypadku złamania zabezpieczeń, system operacyjny urządzenia powoduje blokadę urządzenia lub sprawia, że jest ono nieczytelne.

6.2.8 Metoda aktywacji klucza prywatnego

Prywatny klucz certyfikacyjny jest aktywowany przez oprogramowanie CA w trybie dual control, czyli w obecności dwóch osób pełniących określone role i w obecności kierownika ds. usług certyfikacyjnych.
Podmiot lub wnioskodawca w imieniu osoby prawnej jest odpowiedzialny za zabezpieczenie własnego klucza prywatnego za pomocą mocnego hasła, aby zapobiec jego nieuprawnionemu użyciu. Aby aktywować klucz prywatny, posiadacz musi

dokonać uwierzytelnienia.

6.2.9 Metoda dezaktywacji klucza prywatnego

Nie dotyczy

6.2.10 Metoda niszczenia klucza prywatnego CA

Wyznaczony do tej roli personel InfoCert zajmuje się zniszczeniem klucza prywatnego po wygaśnięciu lub unieważnieniu certyfikatu, zgodnie z procedurami bezpieczeństwa określonymi w polityce bezpieczeństwa i w specyfikacjach producenta urządzenia.

6.2.11 Klasyfikacja modułów kryptograficznych

Nie dotyczy

6.3 Inne aspekty zarządzania kluczami

Nie dotyczy

6.3.1 Archiwizacja klucza publicznego

Nie dotyczy

6.3.2 Okres ważności certyfikatu i pary kluczy

Okres ważności certyfikatu określa się na podstawie:

- stanu technologii;
- aktualnego stanu wiedzy kryptograficznej;
- zamierzonego wykorzystania samego certyfikatu.

Okres ważności certyfikatu jest w nim wyrażony w sposób wskazany w punkcie 3.3.3. Obecnie certyfikat CA jest ważny przez maksymalnie 16 (szesnaście) lat, a certyfikaty wydawane osobom fizycznym lub prawnym ważne są nie dłużej niż 63 (sześćdziesiąt trzy) miesiące z uwzględnieniem solidności użytych algorytmów.

6.4 Dane aktywujące klucz prywatny

Odsyła się do punktów 4.3.3 i 6.3.

6.5 Kontrole bezpieczeństwa informatycznego

6.5.1 Szczególne wymagania dotyczące bezpieczeństwa komputerów

Systemy operacyjne urządzeń przetwarzających, wykorzystywanych w działalności certyfikacyjnej do generowania kluczy, generowania certyfikatów i zarządzania rejestrem certyfikatów, są zabezpieczone (hardening), tzn. są skonfigurowane w taki sposób, aby zminimalizować wpływ ewentualnej podatności na zagrożenia poprzez wyeliminowanie wszystkich funkcji, które nie są niezbędne do działania i zarządzania CA.

Dostęp administratorów systemu, wyznaczonych w tym celu zgodnie z obowiązującymi przepisami prawa, odbywa się poprzez aplikację root on demand, która umożliwia korzystanie z uprawnień użytkownika root dopiero po indywidualnym uwierzytelnieniu. Dostępy są śledzone, rejestrowane i przechowywane przez 12 (dwanaście) miesięcy.

6.6 Działania dotyczące systemów zarządzania

InfoCert przywiązuje strategiczne znaczenie do bezpiecznego przetwarzania informacji i uznaje potrzebę ciągłego rozwijania, utrzymywania, kontrolowania i doskonalenia systemu zarządzania bezpieczeństwem informacji (SZBI) zgodnie z normą ISO/IEC 27001 dla działań EA:33-35.
SZBI przewiduje następujące procedury i kontrole:

- zarządzanie aktywami;
- kontrola dostępu;
- bezpieczeństwo fizyczne i środowiskowe;
- bezpieczeństwo działań operacyjnych;
- bezpieczeństwo komunikacji;
- pozyskiwanie, rozwój i utrzymanie systemów;
- zarządzanie incydentami;
- ciągłość działania.

Wszystkie procedury są zatwierdzane przez właściwych kierowników i udostępniane wewnętrznie w systemie zarządzania dokumentami InfoCert.

6.7 Kontrole bezpieczeństwa sieci

InfoCert opracował dla usługi certyfikacyjnej infrastrukturę bezpieczeństwa sieciowego, opartą na wykorzystaniu mechanizmów zapory sieciowej i protokołu SSL, w celu stworzenia bezpiecznego kanału pomiędzy punktami rejestracji a systemem

certyfikacji, a także pomiędzy systemem a administratorami lub operatorami.

Systemy i sieci InfoCert połączone są z Internetem w sposób kontrolowany przez systemy zapory sieciowej, które umożliwiają podział połączenia na obszary stopniowo zwiększającego się bezpieczeństwa: sieć Internet, sieci DMZ (Demilitarized Zone) lub sieci obwodowe, sieci wewnętrzne. Cały przepływ danych między różnymi obszarami podlega akceptacji ze strony zapory sieciowej w oparciu o zestaw ustalonych zasad. Reguły zdefiniowane na zaporach sieciowych są zaprojektowane zgodnie z zasadami „default deny" (to, co nie jest wyraźnie dozwolone, jest domyślnie zabronione, co oznacza, że zasady te dopuszczają tylko to, co jest ściśle niezbędne dla prawidłowego funkcjonowania aplikacji) i „defense in depth" (kolejne poziomy obrony są zorganizowane najpierw na poziomie sieci, poprzez kolejne zapory sieciowe, a na koniec przez zastosowanie hardeningu).

6.8 System znaczników czasu

InfoCert oferuje usługę kwalifikowanych znaczników czasu. Informacje na temat znaczników czasu znajdują się w Polityce certyfikacji ICERT-INDI-TSA dostępnej na stronie internetowej InfoCert.

7 FORMAT CERTYFIKATU, LISTY CRL I OCSP

7.1 Format certyfikatu

Certyfikat zawiera informacje określone we wniosku o wydanie certyfikatu.
Format wydanego certyfikatu jest zgodny z rozporządzeniem eIDAS [1] i z decyzją nr 147/2019 [13]; w ten sposób zagwarantowana jest pełna czytelność i weryfikowalność w kontekście europejskich przepisów i jednostek certyfikujących.
InfoCert wykorzystuje standard ITU X.509 wersja 3 dla całej struktury PKI.
W Aneksie A podano kody źródłowe certyfikatów root i certyfikatów posiadaczy będących osobami fizycznymi i prawnymi.

7.1.1 Numer wersji

Wszystkie certyfikaty wydane przez InfoCert są zgodne z X.509 wersja 3.

7.1.2 Rozszerzenia certyfikatu

Certyfikaty kwalifikowane charakteryzują się rozszerzeniami zawartymi w qcStatement punkt 3.2.6 normy IETF RFC 3739. Ich stosowanie reguluje norma ETSI 319 412-5. W celu uzyskania informacji o rozszerzeniach certyfikatu patrz Aneks A.

7.1.3 OID algorytmu podpisu

Do podpisywani certyfikatów można wybrać jeden z następujących algorytmów:

- sha256WithRSAEncryption [iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) sha256WithRSAEncryption(11)]
- ecdsa-with-SHA256 [iso(1) member-body(2) us(840) ansi-x962(10045) signatures(4) ecdsa-with-SHA2(3) ecdsa-with-SHA256(2)]
- ecdsa-with-SHA384 [iso(1) member-body(2) us(840) ansi-x962(10045) signatures(4) ecdsa-with-SHA2(3) ecdsa-with-SHA384(3)]
- ecdsa-with-SHA512 [iso(1) member-body(2) us(840) ansi-x962(10045) signatures(4) ecdsa-with-SHA2(3) ecdsa-with-SHA512(4)].

7.1.4 Formy nazw

Każdy certyfikat zawiera unikalny numer seryjny w obrębie CA, który go wydał.

7.1.5 Restrykcje dotyczące nazw

W tym zakresie patrz punkt 3.1.

7.1.6 OID certyfikatu

W tym zakresie patrz punkt 1.2.

7.2 Format listy CRL

Do celów tworzenia list unieważnionych certyfikatów CRL InfoCert używa profilu RFC5280 „Internet X.509 Public Key Infrastructure Certificate Revocation List (CRL)" i dodaje do podstawowego formatu rozszerzenia zdefiniowane w RFC 5280: „Authority Key Identifier", „CRL Number", „Issuing Distribution Point" i „expiredCertsOnCRL"

7.2.1 Numer wersji

Wszystkie listy CRL wydawane przez InfoCert są zgodne z X.509 wersja 2.

7.2.2 Rozszerzenia listy CRL

W celu uzyskania informacji na temat listy CRL patrz Aneks A.

7.3 Format OCSP

Aby umożliwić określenie statusu unieważnienia certyfikatu bez konieczności wnioskowania o dostęp do listy CRL, InfoCert udostępnia usługi OCSP zgodne z profilem RFC6960 „X.509 Internet Public Key Infrastructure Online Certificate Status Protocol – OCSP". Protokół ten podaje dane, które powinny być wymieniane przez aplikację, która chce zweryfikować status certyfikatu i usługi OCSP.

7.3.1 Numer wersji

Protokół OCSP używany przez InfoCert jest zgodny z wersją 1 normy RFC6960.

7.3.2 Rozszerzenia OCSP

W celu uzyskania informacji na temat OCSP patrz Aneks A.

8 KONTROLE I OCENY ZGODNOŚCI

W celu uzyskania kwalifikacji kwalifikowanych i niekwalifikowanych dostawców usług zaufania, zgodnie z rozporządzeniem eIDAS należy przeprowadzić procedurę przewidzianą w art. 21 tego rozporządzenia.
InfoCert złożył do AgID odpowiedni wniosek o uzyskanie statusu „kwalifikowanego dostawcy usług zaufania", załączając raport z oceny zgodności z rozporządzeniem (Conformity Assessment Report – CAR) wydany przez jednostkę oceniającą upoważnioną przez właściwy organ krajowy (CAB), którym we Włoszech jest ACCREDIA.

8.1 Częstotliwość lub okoliczności oceny zgodności

Ocena zgodności powtarzana jest co dwa lata, lecz co roku CAB przeprowadza audyt w ramach nadzoru.

8.2 Tożsamość i kwalifikacje audytora

Audyt przeprowadza:

Nazwa firmy: CSQA Certification S.r.l. Siedziba statutowa: Via S. Gaetano n. 74, 36016 Thiene (VI)
Numer telefonu: +39 0445 313011
Numer wpisu do Rejestru Przedsiębiorstw: Kod identyfikacji podatkowej 02603680246 Nr w Rejestrze Przedsiębiorstw VI: 02603680246 / Nr w REA [Repertorium gospodarczo-administracyjne]: 258305
Numer VAT: 02603680246
Strona internetowa: http://www.csqa.it

8.3 Związek InfoCert z CAB

InfoCert świadczy usługi jako kwalifikowany dostawca usług zaufania zgodnie z rozporządzeniem (UE) nr 910/2014 del 23/07/2014, na podstawie oceny zgodności przeprowadzonej przez Conformity Assessment Body CSQA Certificazioni S.r.l., w rozumieniu powyższego rozporządzenia i normy ETSI EN 319 401, według schematu oceny eIDAS określonego przez ACCREDIA na podstawie norm ETSI EN 319_403 i UNI CEI EN ISO/IEC 17065:2012.

8.4 Aspekty będące przedmiotem oceny

CAB powinna dokonać oceny zgodności przyjętych procedur,

organizacji CA, organizacji roli, szkolenia personelu i dokumentacji umownej w odniesieniu do Podręcznika obsługi, rozporządzenia i mających zastosowanie przepisów.

8.5 Działania podejmowane w przypadku niezgodności

W przypadku niezgodności CAB podejmie decyzję, czy pomimo tego przesłać raport do AgID,
czy też zastrzec sobie prawo do ponownego przeprowadzenia audytu po usunięciu niezgodności. InfoCert zobowiązuje się do niezwłocznego usunięcia wszelkich niezgodności, wdrażając wszelkie niezbędne działania naprawcze i dostosowawcze.

9 POZOSTAŁE ASPEKTY PRAWNE I BIZNESOWE

9.1 Opłaty

9.1.1 Opłaty za wydanie i odnowienie certyfikatów oraz ponowne wystawienie certyfikatów z nowymi kluczami

W przypadku certyfikatów LongTerm lub OneShot, zwykle koszty wydania certyfikatu ponosi bezpośredni klient InfoCert a nie posiadacz, na podstawie opłat określonych w umowie o świadczenie usług zawartej przez klienta i InfoCert.
W pozostałych przypadkach opłaty są dostępne na stronach internetowych: https://www.firma.infocert.it/ i http://ecommerce.infocert.it lub w punktach rejestracji. CA może zawierać porozumienia handlowe z RA i/lub klientami zawierające inne opłaty.

9.1.2 Opłaty za dostęp do certyfikatów

Dostęp do publicznego rejestru opublikowanych certyfikatów jest nieograniczony i wolny od opłat.

9.1.3 Opłaty za dostęp do informacji dotyczących statusu zawieszenia i unieważnienia certyfikatów

Dostęp do listy certyfikatów unieważnionych lub zawieszonych jest nieograniczony i wolny od opłat.

9.1.4 Opłaty za inne usługi

Opłaty są dostępne na stronach internetowych: https://www.firma.infocert.it/ i http://ecommerce.infocert.it lub w punktach rejestracji.
CA może zawierać porozumienia handlowe z RA i/lub klientami zawierające inne opłaty.

9.1.5 Polityka dotycząca zwrotów poniesionych kosztów

W przypadku nabycia usługi przez posiadacza, którego na podstawie przepisów można

uznać za konsumenta, ma prawo odstąpić od umowy w terminie 14 dni od daty zawarcia umowy, otrzymując zwrot uiszczonej kwoty. Instrukcje dotyczące możliwości skorzystania z prawa do odstąpienia od umowy oraz wniosek o zwrot poniesionych kosztów dostępne są na stronie internetowej https://help.infocert.it/ lub w RA.

9.2 Odpowiedzialność finansowa

9.2.1 Ochrona ubezpieczeniowa

TSP InfoCert zawarł stosowną umowę ubezpieczeniową obejmującą ryzyko związane z prowadzoną działalnością oraz ewentualne szkody wyrządzone osobom trzecim zawierającą następujące maksymalne sumy odszkodowania:

- 10 000 000 euro za pojedyncze zdarzenie;
- 10 000 000 euro rocznie.

9.2.2 Pozostałe działania

Nie dotyczy

9.2.3 Gwarancja lub ochrona ubezpieczeniowa podmiotów końcowych

Patrz punkt 9.2.1.

9.3 Poufność informacji biznesowych

9.3.1 Zakres stosowania zasad dotyczących informacji poufnych

W ramach działalności będącej przedmiotem niniejszego Podręcznika obsługi nie przewiduje się zarządzania
informacjami poufnymi.

9.3.2 Informacje, dla których nie znajdują zastosowania zasady dotyczące informacji poufnych

Nie dotyczy

9.3.3 Odpowiedzialność za ochronę informacji poufnych

Nie dotyczy

9.4 Ochrona danych osobowych

Informacje dotyczące posiadacza i wnioskodawcy, w posiadanie których CA wejdzie w

związku z prowadzeniem swojej normalnej działalności, o ile nie uzyskano wyraźnej zgody, należy traktować jako poufne i niepodlegające publikacji, z wyjątkiem informacji wyraźnie przeznaczonych do użytku publicznego (jak klucz publiczny, certyfikat, jeśli jest wnioskowany przez posiadacza, data unieważnienia i data zawieszenia certyfikatu). W szczególności, dane osobowe przetwarzane są przez InfoCert zgodnie z zapisami [włoskiego] Kodeksu

administracji cyfrowej, [włoskiego] dekretu ustawodawczego nr 196 z dnia 30 czerwca 2003 roku oraz rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 roku w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych, w pełni obowiązującego od dnia 25 maja 2018 roku [4].

9.4.1 Program dotyczący ochrony danych osobowych

InfoCert stosuje szereg zasad, za pośrednictwem których wdraża i włącza ochronę danych osobowych do swojego systemu zarządzania bezpieczeństwem informacji zgodnie z normą ISO 27001, w oparciu o proces ciągłego doskonalenia.

9.4.2 Dane przetwarzane jako dane osobowe

Przetwarzaniu w sposób przewidziany dla danych osobowych podlegają dane odpowiadające definicji zawartej w obowiązujących przepisach [4]. Za dane osobowe uznaje się zatem wszelkie informacje dotyczące osoby fizycznej, zidentyfikowanej lub możliwej do zidentyfikowania, również pośrednio, poprzez odniesienie do jakiejkolwiek innej informacji, w tym do osobistego numeru identyfikacyjnego.

9.4.3 Dane nieuznawane za dane osobowe

Dane przeznaczone do upublicznienia przez dział techniczny CA, czyli klucz publiczny, certyfikat (jeśli wnioskowany przez posiadacza) oraz data unieważnienia i zawieszenia certyfikatu, nie są uznawane za dane osobowe.

9.4.4 Administrator danych osobowych

InfoCert S.p.A.
Piazza Sallustion n. 9
00147 Rzym
richieste.privacy@legalmail.it

9.4.5 Polityka prywatności i zgoda na przetwarzanie danych osobowych

Polityka prywatności dostępna jest na stronie internetowej www.infocert.it. Przed rozpoczęciem jakiegokolwiek procesu przetwarzania danych osobowych InfoCert uzyskuje w razie potrzeby zgodę na przetwarzanie tych danych, na zasadach i w formie przewidzianej w przepisach prawa [4]. Szczegółowe informacje mogą znajdować się na stronie internetowej klienta, który w razie potrzeby może uzyskać

zgodę na przetwarzanie tych danych w imieniu InfoCert.

9.4.6 Udostępnianie danych na wniosek organów władzy

Udostępnianie danych na wniosek organów władzy jest obowiązkowe i następuje na zasadach każdorazowo ustalanych przez dany organ.

9.4.7 Inne powody udostępniania danych

Nie przewidziano.

9.5 Własność intelektualna

Prawa autorskie do niniejszego dokumentu przysługują InfoCert. Wszelkie prawa zastrzeżone.

9.6 Prawo do reprezentowania i gwarancje

InfoCert ponosi odpowiedzialność za przestrzeganie procedur ustalonych w swojej własnej polityce dotyczącej bezpieczeństwa informacji, również wtedy, gdy niektóre zadania są przekazane innemu podmiotowi, zgodnie z art. 2.4.1. Załącznika do rozporządzenia wykonawczego Komisji (UE) 2015/1502.
W tym ostatnim przypadku, prawo do reprezentowania realizowane jest na podstawie pełnomocnictwa udzielonego przez InfoCert punktowi rejestracji (RA), w którym określony jest zakres odpowiedzialności i obowiązki stron. W szczególności, punkt rejestracji zobowiązany jest do wykonania czynności rejestracyjnych zgodnie z obowiązującymi przepisami prawa, a także zgodnie z procedurami opisanymi w Polityce, ze szczególnym uwzględnieniem obowiązku wiarygodnej identyfikacji osób podpisujących wniosek o wydanie cyfrowego certyfikatu, a także do przekazywania wyników tych czynności do InfoCert.
Posiadacz jest odpowiedzialny za prawdziwość danych przekazanych we wniosku o rejestrację i wydanie certyfikatu. Jeżeli w momencie identyfikacji posiadacz, również poprzez użycie nieprawdziwych dokumentów osobistych, zataił swoją prawdziwą tożsamość lub podał się za inny podmiot, lub też podjął jakiekolwiek działania naruszające proces identyfikacji i dane zawarte w certyfikacie, będzie odpowiedzialny za wszelkie szkody poniesione przez podmiot certyfikujący i/lub osoby trzecie wynikające z nieprecyzyjności informacji zawartych w certyfikacie i będzie zobowiązany do zaspokojenia ewentualnych roszczeń odszkodowawczych, zwalniając z tego obowiązku podmiot certyfikujący.
Ponadto, posiadacz i wnioskodawca są odpowiedzialni za szkody poniesione przez podmiot certyfikujący i/lub osoby trzecie w razie opóźnienia uruchomienia przez nich

procedur, o których mowa w punkcie 4.9 niniejszego Podręcznika obsługi (unieważnienie i zawieszenie certyfikatu).

9.7 Ograniczenia gwarancji

Podmiot certyfikujący nie udziela żadnej gwarancji na (i) prawidłowe działanie oraz bezpieczeństwo sprzętu komputerowego i oprogramowania używanych przez posiadacza; (ii) używanie prywatnego klucza, bezpiecznego urządzenia do składania podpisu, jeśli występuje, i/lub certyfikatu podpisu do celów innych niż cele przewidziane w obowiązujących przepisach prawa i w niniejszej Polityce; (iii) prawidłowe i nieprzerwane działanie krajowych lub międzynarodowych linii elektrycznych i telefonicznych; (iv) ważność i znaczenie, również dowodowe, certyfikatu podpisu lub wszelkich wiadomości, aktów lub dokumentów związanych z nim lub utworzonych za pośrednictwem kluczy, do których odnosi się certyfikat, z zastrzeżeniem skuteczności prawnej kwalifikowanego podpisu elektronicznego równoważnej podpisowi własnoręcznemu, na mocy art. 25 rozporządzenia (UE) nr 910/2014; (v) poufność i/lub integralność wszelkich wiadomości, aktów lub dokumentów związanych z certyfikatem lub utworzonych za pośrednictwem kluczy, do których odnosi się certyfikat (w tym sensie, że ewentualne naruszenie poufności lub integralności certyfikatu zwykle stwierdzane jest przez posiadacza lub odbiorcę przy pomocy odpowiednich procedur weryfikacyjnych).
InfoCert udziela gwarancji wyłącznie na działanie usług na poziomie, o którym mowa w punkcie 9.15 Podręcznika obsługi.

9.8 Ograniczenia odpowiedzialności

InfoCert nie ma żadnych zobowiązań z tytułu nadzoru treści, rodzaju lub elektronicznego formatu dokumentów i/lub, ewentualnie, identyfikatorów *hash* przesyłanych w ramach procedury informatycznej wskazanej przez wnioskodawcę lub posiadacza, nie ponosi też odpowiedzialności za ich ważność oraz możliwość ich powiązania z rzeczywistą wolą posiadacza.
Z wyjątkiem przypadków działania umyślnego lub zaniedbania, InfoCert nie ponosi odpowiedzialności za szkody bezpośrednie i pośrednie poniesione przez posiadaczy i/lub osoby trzecie w wyniku zastosowania lub niezastosowania certyfikatów podpisu wystawionych na podstawie postanowień niniejszego Podręcznika obsługi i Ogólnych warunków świadczenia usług certyfikacyjnych.
InfoCert nie ponosi odpowiedzialności za jakiekolwiek szkody bezpośrednie i/lub pośrednie wynikające z co najmniej jednego z następujących zdarzeń: (i) utrata narzędzi do identyfikacji i uwierzytelniania, (ii) ich niewłaściwe przechowywanie, (iii) ich niewłaściwe zastosowanie, i/lub (iv) nieprzestrzeganie powyższych postanowień przez posiadacza.
Ponadto, InfoCert na etapie sporządzania umowy na usługi certyfikacyjne, a także w trakcie jej realizacji, nie odpowiada za ewentualne szkody i/lub opóźnienia wynikające z nieprawidłowego działania lub blokady systemu informatycznego i sieci internetowej.
Z wyjątkiem przypadków działania umyślnego lub zaniedbania, InfoCert nie ponosi

kosztów ani odpowiedzialności za szkody, bezpośrednie lub pośrednie, niezależnie od ich natury lub wagi, poniesione przez posiadacza, wnioskodawcę i/lub osoby trzecie w wyniku ingerencji lub interwencji w usługę lub sprzęt, podjętych przez osoby trzecie nieupoważnione przez InfoCert.

9.9 Odszkodowanie

InfoCert ponosi odpowiedzialność za ewentualne szkody wyrządzone, na skutek działań umyślnych lub zaniedbania, bezpośrednio jakiejkolwiek osobie fizycznej lub prawnej, w związku z niewypełnieniem przez InfoCert obowiązków, o których mowa w rozporządzeniu Parlamentu Europejskiego i Rady (UE) nr 910/2014 z dnia 23 lipca 2014 roku, oraz z powodu niepodjęcia przez InfoCert wszelkich niezbędnych środków, mających na celu zapobieganie powstaniu szkody.

W przypadku, o którym mowa w poprzednim punkcie, wnioskodawcy lub posiadaczowi przysługiwać będzie prawo do odszkodowania za szkody poniesione bezpośrednio w wyniku działań, o których mowa w poprzednim punkcie, w wysokości w żadnym przypadku nieprzekraczającej maksymalnych sum odszkodowania przewidzianych za pojedyncze zdarzenie lub rocznie, zgodnie z art. 3 ust. 7 regulaminu załączonego do decyzji nr 185/2017.

Nie można ubiegać się o zwrot poniesionych kosztów w przypadku, gdy brak możliwości korzystania z usługi wynika z niewłaściwej eksploatacji usługi certyfikacji lub z winy operatora sieci telekomunikacyjnej lub też z powodów losowych, działania siły wyższej lub przyczyn w każdym razie niezależnych od InfoCert, takich jak na przykład strajki, rozruchy, trzęsienia ziemi, akty terroryzmu, zamieszki, zorganizowane akty sabotażu, zdarzenia chemiczne i/lub bakteriologiczne, wojny, powodzie, środki podejmowane przez właściwe organy lub nieodpowiedniość struktur, sprzętu komputerowego i/lub oprogramowania używanych przez wnioskodawcę.

9.10 Zakończenie stosunku umownego i rozwiązanie umowy

9.10.1 Zakończenie stosunku umownego

W chwili zakończenia stosunku umownego między CA a posiadaczem, między CA a RA oraz między CA a wnioskodawcą, certyfikat zostanie unieważniony. Certyfikat jest ważny przez okres równy okresowi ważności certyfikatu podpisu podanemu w polu „termin ważności” (*validity*)” certyfikatu.
Przed upływem ważności certyfikatu posiadacz może zwrócić się o jego odnowienie, z tymi samymi kluczami lub dokonując ponownej certyfikacji z nowymi kluczami, zgodnie z procedurą opisaną w niniejszej Polityce. Odnowienie powoduje przedłużenie umowy certyfikacyjnej do daty ważności lub unieważnienia odnowionego certyfikatu oraz konieczność uregulowania opłat z tytułu świadczonej usługi. Nie można odnowić certyfikatu, którego termin ważności już upłynął, ani certyfikatu unieważnionego.

9.10.2 Rozwiązanie umowy

Umowa ulega rozwiązaniu z mocy prawa, z równoczesnym zaprzestaniem świadczenia usług certyfikacyjnych oraz unieważnieniem

wystawionego certyfikatu w przypadku niespełnienia warunków każdorazowo wskazanych w umowie świadczenia usługi. Umowa ulega rozwiązaniu z mocy prawa również wtedy, gdy jedna ze stron poinformuje drugą stronę, za pośrednictwem certyfikowanej poczty elektronicznej lub listem poleconym z potwierdzeniem odbioru, o zamiarze skorzystania z niniejszej klauzuli.
We wszystkich przypadkach rozwiązania umowy, zapisy umowy pozostają wiążące do momentu jej rozwiązania.
Posiadacz przyjmuje do wiadomości, że w przypadku rozwiązania umowy, niezależnie od powodów rozwiązania, nie będzie możliwe dalsze korzystanie z usług.

9.10.3 Skutki rozwiązania umowy

Rozwiązanie umowy powoduje natychmiastowe unieważnienie certyfikatu.

9.10.4 Oficjalne kanały komunikacyjne

Patrz kanały komunikacyjne opisane w punkcie 1.5.1.

9.10.5 Aktualizacje Podręcznika obsługi

CA zastrzega sobie prawo do wprowadzania zmian do niniejszego dokumentu wynikających ze względu na wymogi techniczne lub zmiany w procedurach dokonane zarówno w związku ze zmianami obowiązujących przepisów ustawowych lub wykonawczych, jak również w celu optymalizacji cyklu pracy. Każda nowa wersja Podręcznika obsługi anuluje i zastępuje poprzednie wersje, które jednak nadal mają zastosowanie dla certyfikatów wydanych w okresie ich obowiązywania, do wygaśnięcia pierwszego terminu ważności tych certyfikatów.
Zmiany, które nie mają znaczącego wpływu na użytkowników, wiążą się z publikacją nowego wydania tej samej wersji dokumentu, natomiast zmiany o znaczącym wpływie na użytkowników (jak np. zmiany dotyczące procedur działania) wiążą się z publikacją nowej wersji dokumentu. W każdym z przypadków Podręcznik obsługi jest niezwłocznie publikowany i udostępniany zgodnie z przewidzianymi zasadami. O każdej zmianie technicznej lub proceduralnej wprowadzonej do niniejszego Podręcznika obsługi niezwłocznie informuje się RA.
Jeśli wprowadzone zmiany są znaczące, CA musi poddać się audytowi prowadzonemu przez akredytowaną jednostkę CAB, przedstawić organowi nadzoru (AgID) raport z oceny zgodności (*CAR – Conformity Assessment Report*) i Podręcznik obsługi oraz poczekać na zgodę na ich opublikowanie.

9.10.6 Historia zmian

Wersja/wydanie	**4.11**
nr:	
Data wersji/wydania:	15.05.2024
Opis zmian:	pkt 1.2, 4.1.1: Doprecyzowano poprzez dodanie strony internetowej instytucji pkt 1.3.1: Zweryfikowano dane na temat firmy pkt 1.3.2.1: Wprowadzono doprecyzowania pkt 1.5.1, 4.9.3: Usunięto numer faksu z danych kontaktowych i zweryfikowano dane kontaktowe pkt 1.5.2, 9.10.7: Zaktualizowano nazwy obszarów przedsiębiorstwa pkt 1.6.1 i 1.6.2: Dodano definicję . klienta, ujednolicono definicje i skróty pkt 2.3.1, 2.3.2: Doprecyzowano adres publikacji pkt 3.1.3: Zweryfikowano politykę przechowywania pkt 3.2.2: Doprecyzowano korzystanie z wiarygodnych baz danych pkt 3.2.3: Doprecyzowano tryby potwierdzania tożsamości pkt 4.5.3: Zweryfikowano ograniczenia stosowania pkt 4.9.3 i 4.9.5: Doprecyzowano unieważnienie pkt 5.1.1: Zweryfikowano opis pkt 5.1.3: Zaktualizowano certyfikację obiektu pkt 5.1.7 i 5.1.8: Zweryfikowano opis pkt 6.2.1: Zweryfikowano opis pkt 6.6: Zweryfikowano opis pkt 8.3: Zweryfikowano opis pkt 9.2.1: Zweryfikowano opis pkt 9.4: Wprowadzono doprecyzowania pkt 9.4.4: Dokonano aktualizacji pkt 9.4.5: Zweryfikowano opis pkt 9.10.2: Zweryfikowano opis pkt 9.12: Zweryfikowano opis Weryfikacja ogólna z korektą błędów ortograficznych i gramatycznych, dokonano przeformułowań i doprecyzowań
Uzasadnienie:	Przegląd ogólny

Wersja/wydanie nr:	**4.10**
Data	20.09.2023

Wersja/wydanie:	
Opis zmian:	Wyjaśnienia dotyczące SelfQ i Re-key
Uzasadnienie:	Żądania przeformułowania ze strony AgID

Wersja/wydanie nr:	**4.9**
Data wersji/wydania:	29.05.2023
Opis zmian:	pkt 3.2.3, 3.2.3.5 Nowy tryb potwierdzania tożsamości
Uzasadnienie:	Nowy tryb potwierdzania tożsamości

Wersja/wydanie nr:	**4.8**
Data wersji/wydania:	18.04.2023
Opis zmian:	Zmiana logo InfoCert i formatowania pkt 1.2 Dodano nowe OID pkt 1.2, 3.1.1, 3.1.5, 3.2.4, 7.1, 9.15 Dodano odniesienie do Decyzji AgID nr 147/2019 pkt 3.3, 4.6, 4.7, 9.1, 9.10 Doprecyzowano odnawianie i ponowną certyfikację kluczy pkt 3.2.3.1, 3.2.3.5 Dodano doprecyzowania pkt 5.1.1, 5.1.3, 5.1.5 Zweryfikowano aspekty instrumentu pkt 5.4.2 Zweryfikowano opis pkt 5.6 Skorygowano opis pkt 5.8 Zmieniono terminy wypowiedzenia w przypadku rozwiązania umowy pkt 6.1.7.2 Zmieniono dozwolone KeyUsage pkt Aneks A Zaktualizowano format CRL i OCSP
Uzasadnienie:	Przegląd ogólny rebrandingu

Wersja/wydanie nr:	**4.7**
Data wersji/wydania:	17.03.2022
Opis zmian:	pkt 1.2 Zweryfikowano opisy w tabeli OID pkt 1.6.1 Zweryfikowano definicje LongTerm i OneShot oraz wprowadzono certyfikaty short-term pkt 3.1.1 Odstępstwo od RFC 5280 z powodu długości niektórych pól subjectDN pkt 3.1.5 Wprowadzono kod LEI w certyfikatach dla osoby prawnej pkt 3.2.5 Skorygowano odniesienia do punktów dokumentu pkt 3.2.3 Dodano „Potwierdzanie tożsamości zgodnie z trybem 7 – ContoID” pkt 4.5.1 Zweryfikowano opis pkt 4.5.3 Zweryfikowano opis i dodano ograniczenie stosowania dla certyfikatów dla osoby prawnej z kodem LEI dla PoC pkt 4.9.3 Doprecyzowano certyfikaty short-term pkt 4.9.5 Przeformułowano terminy rozpatrzenia wniosku o unieważnienie pkt 4.9.9 Doprecyzowano zgodność między OCSP i listą CRL pkt 4.9.15 Doprecyzowano certyfikaty short-term pkt 5 Częstotliwość weryfikacji polityki bezpieczeństwa pkt 5.4.3 Doprecyzowano okres przechowywania pkt 5.4.4. 5.5 Zaktualizowano opis pkt 6.1.2 Zweryfikowano opis pkt 6.4 Skorygowano odniesienie do punktu dokumentu pkt Aneks A Uproszczono opis rozszerzeń certyfikatu Formatowanie w celu zapewnienia dostępności dokumentu
Uzasadnienie:	Przegląd ogólny Zmiana formatowania

Wersja/wydanie nr:	**4.6**
Data wersji/wydania:	10.09.2021

Opis zmian:	pkt 1.5.1 Zaktualizowano dane kontaktowe
Uzasadnienie:	Zmiana danych kontaktowych

Wersja/wydanie nr:	**4.5**
Data wersji/wydania:	18.05.2021
Opis zmian:	pkt 3.1.1 Dodano szczegółowe informacje na temat stosowania decyzji AgID pkt3.1.6 Dodano doprecyzowania dotyczące korzystania ze znaków towarowych zarejestrowanych pkt3.2.3, 3.2.3, 3.2.4, 3.2.5 Zweryfikowano organizację punktów pkt3.2.3 Dodano odniesienie do „CPS Addendum – Akceptowalne dokumenty tożsamości” pkt 3.2.3.3 Doprecyzowano korzystanie z trybu SignID pkt 4.2.1, 4.2.2, 4.2.3 Zweryfikowano organizację punktów pkt 4.3.1 Zaktualizowano opis pkt 4.5.3 Dodano odniesienie do ograniczeń stosowania dla certyfikatów hiszpańskich pkt 4.9, 5.8 Wprowadzono wyjaśnienie na temat informacji o statusie unieważnienia certyfikatów pkt 4.9.15.1 Zaktualizowano opis pkt 5.1.1 Zaktualizowano kwestie technologiczne pkt 5.3.5 Zaktualizowano opis pkt 5.3.7 Zaktualizowano opis pkt 5.8 Zweryfikowano opis pkt 5.5.6 Zweryfikowano opis pkt 6.1.5 i 7.1.3 Zaktualizowano algorytmy i długość kluczy pkt 6.1.7 Zaktualizowano opis pkt 6.1.7.2 Dodano wyjątek w celu użycia klucza prywatnego pkt 9.15 Dodano odnośne prawo w kontekście Hiszpanii i „CPS Addendum – Akceptowalne dokumenty tożsamości” pkt Aneks A Dodano nowy root CA pkt Aneks B Zaktualizowano nazwę handlową oprogramowania weryfikacyjnego

	pkt Aneks C Wprowadzono certyfikat kwalifikowany obywatela Hiszpanii Wprowadzono korekty formalne, zaktualizowano definicje, skróty, odniesienia
Uzasadnienie:	Nowy root CA Przegląd ogólny

Wersja/wydanie nr:	**4.4**
Data wersji/wydania:	10.02.2021
Opis zmian:	pkt 4.2.1 Zaktualizowano obowiązkowy i jednoznaczny charakter adresu e-mail i numeru telefonu pkt 4.2.2 Tryb dostarczania drogą elektroniczną szyfrowanej koperty jako tryb domyślny pkt 4.9.13 Dodano możliwość zawieszenia zapobiegawczego według uznania CA
Uzasadnienie:	Wniosek AgID

Wersja/wydanie nr:	**4.3**
Data wersji/wydania:	15.06.2020
Opis zmian:	pkt 3.2.3 Zaktualizowano listę trybów potwierdzania tożsamości pkt 3.2.3.4 Potwierdzenie tożsamości przez ramy interoperacyjności węzła eIDAS pkt 3.2.3.5 Rozróżnienie między video z udziałem operatora i bez udziału operatora z przelewem wzmacniającym pkt 3.2.3.6 eDocID – Potwierdzenie tożsamości przy użyciu elektronicznych dokumentów tożsamości pkt 4.5.3 Zaktualizowano punkt poprzez wprowadzenie ograniczeń stosowania dla trybów potwierdzania tożsamości autID i eDocID pkt4.9.15 i pkt4.9.16 Wyjaśnienia dotyczące okresu zawieszenia

Uzasadnienie:	Rozszerzenie trybu potwierdzania tożsamości Wyjaśnienia i korekta literówek

Wersja/wydanie nr:	4.2
Data wersji/wydania:	24.03.2020
Opis zmian:	pkt 5.1.1 Zaktualizowano kwestie technologiczne i odniesienia do usług hostowanych w chmurze AWS pkt 5.1.6 Zaktualizowano kwestie technologiczne nośników pamięci pkt Aneks A – wprowadzono nowy root CA Electronic Signature Qualified Root „InfoCert Qualified Electronic Signature CA 4”
Uzasadnienie:	Nowy root CA

Wersja/wydanie nr:	4.1
Data wersji/wydania:	10.10.2019
Opis zmian:	pkt 3.1.5 Dodano możliwość używania unikalnego identyfikatora zgodnie z treścią dokumentu eIDAS eID Profile di EiDAS cooperation network
Uzasadnienie:	-

Wersja/wydanie nr:	4.0 (wersja nigdy nieopublikowana, aktualizacje przeniesione do pkt 4.1)
Data wersji/wydania:	14.06.2019
Opis zmian:	Wprowadzono korekty formalne, zaktualizowano definicje, skróty, odniesienia pkt 1.2 Zaktualizowano wersję dokumentu, opis OID agIDcert pkt 1.3.5 Zaktualizowano dla osoby nieletniej pkt 1.6.1 Wprowadzono definicje certyfikatów OneShot, certyfikatów LongTerm i domeny informatycznej pkt 2.2.3 Zaktualizowano punkty dystrybucji listy CRL pkt 3.1.1 Zaktualizowano według decyzji AgID nr 121/2019 pkt 3.1.5 Zaktualizowano według decyzji AgID nr 121/2019

	pkt 3.2.6 Wprowadzono bardziej precyzyjny opis pkt 4.3.1.5 Wprowadzono opis certyfikatów wystawianych do celów testowych pkt 4.5.3 Dodano ograniczenie stosowania dla wydania z SPID i Zaktualizowano opis limitu kwotowego pkt 4.9.2 Wprowadzono bardziej precyzyjny opis pkt 5.1.1 Wprowadzono wyjaśnienie na temat siedziby Data Center pkt 5.3.7 Wypełniono opis dostępów fizycznych pkt 5.4.1 Dodano opis dziennika dostępów fizycznych i logicznych Połączono następujące punkty z dwóch Podręczników obsługi: • pkt 2.2.2 Publikacja certyfikatów • pkt 3.1.3 Anonimowość i pseudonimizacja wnioskodawców • pkt 3.2.3.4 Potwierdzanie tożsamości zgodnie z trybem 4 – AUTID • pkt 4.1.1 Kto może wnioskować o wydanie certyfikatu? • pkt 4.3.2 Zawiadomienie wnioskodawców o wystawieniu certyfikatu • pkt 4.4.2 Publikacja certyfikatu przez urząd certyfikacji • pkt 4.5.1 Korzystanie z prywatnego klucza i certyfikatu przez posiadacza • pkt 4.6.1 Przyczyny odnowienia • pkt 4.9.3 Procedury wnioskowania o unieważnienie certyfikatu • pkt 4.9.15 Procedury wnioskowania o zawieszenie certyfikatu • pkt 6.1.1 Generowanie pary kluczy posiadacza • pkt 6.1.2 Dostarczanie klucza prywatnego wnioskodawcy • pkt 6.1.4 Dostarczanie klucza publicznego użytkownikom • pkt 6.2.7 Zapisywanie klucza prywatnego na module kryptograficznym • pkt 9.1.1 Opłaty za wydanie i odnowienie certyfikatów • pkt 9.4.5 Polityka prywatności i zgoda na przetwarzanie danych osobowych • pkt 9.10.2 Rozwiązanie umowy
Uzasadnienie:	Fuzja ICERT-INDI-MO, wersja 3.5 z dnia 30.11.2018 r. i ICERT-INDI-MO-ENT, wersja 3.5 z dnia 30.11.2018 r. Zaktualizowano według decyzji AgID nr 121/2019. Wprowadzono wyjaśnienia.

Wersja/wydanie nr:	**3.5**
Data	30.11.2018

Wersja/wydanie:	
Opis zmian:	pkt 1.2 Zaktualizowano OID i opis pkt 1.3 Zaktualizowano nazwę grupy pkt 3.2.6 Identyfikacja osoby prawnej PSP w ramach PSD2 pkt 4.2.1.2 Informacje o osobie prawnej w ramach PSD2 pkt 4.9 Wniosek o unieważnienie ze strony NCA dla PSD2 Korekty literówek
Uzasadnienie:	Wystawianie certyfikatów podpisu QSealC zgodnie z dyrektywą PSD2 Zmiana nazwy firmy TecnoInvestimenti

Wersja/wydanie nr:	**3.4**
Data wersji/wydania:	20.06.2018
Opis zmian:	pkt 1.5.1 Zmieniono numer call center pkt 9.2.1 Zaktualizowano maksymalne sumy odszkodowania ubezpieczenia
Uzasadnienie:	-

Wersja/wydanie nr:	**3.3**
Data wersji/wydania:	04.09.2918
Opis zmian:	Rozdz. 1 Poprawiono „podpis elektroniczny” na „podpis elektroniczny kwalifikowany”. Wprowadzono kilka korekt terminologicznych dla lepszego zrozumienia treści, dodano kilka definicji terminów użytych w dokumencie pkt 3.1.5 Przeredagowano częściowo punkt w celu lepszego zrozumienia treści pkt 3.2.3 Przeredagowano częściowo tabelę i podpunkty dla większej jasności treści i kontekstualizacji w zakresie rynków europejskich. Rozszerzono tryb 4 AutID na środki identyfikacji elektronicznej państw członkowskich. Zdefiniowano specjalny dokument z rodzajami akceptowanych dokumentów i środków identyfikacji

	elektronicznej

	pkt 4.2 Przeredagowano częściowo punkt dla lepszego zrozumienia treści i kontekstualizacji w zakresie rynków europejskich pkt 4.2.2 Dodatkowe systemy uwierzytelniania pkt 4.3.3.2 Możliwość wystawienia już aktywnego certyfikatu pkt 4.5.3 Wprowadzono dodatkowe ograniczenie stosowania pkt 4.9.15 i 4.9.16 Zawieszenie i przywrócenie certyfikatu poprzez CMS pkt 9.4 Dodano odniesienia do RODO pkt 9.6, pkt 9.7, pkt 9.8, pkt 9.9, pkt 9.10 Przeredagowano częściowo punkty w celu lepszej kontekstualizacji Certyfikaty użytkownika: Dodano certyfikaty dla osoby prawnej w QSCD, poprawiono niektóre błędy
Uzasadnienie:	-

Wersja/wydanie nr:	**3.2**
Data wersji/wydania:	02.05.2017
Opis zmian:	Dodano informację dotyczącą CA „Infocert Firma Qualificata 2” Dodano kilka OID dotyczących CA „Infocert Firma Qualificata 2” Skorygkowano formę i ortografię
Uzasadnienie:	

Wersja/wydanie nr:	**3.1**
Data wersji/wydania:	27.01.2017
Opis zmian:	pkt 3.2.3 Usunięto wszystkie odniesienia do systemu SPID jako narzędzia uwierzytelniającego do celów identyfikacji pkt 3.2.3.1 Uszczegółowiono potwierdzanie tożsamości przez pracodawcę pkt 4.8.12 Opisano sposób przywracania zawieszonego certyfikatu

Uzasadnienie:	-

Wersja/wydanie nr:	**3.0**
Data wersji/wydania:	12.12.2016
Opis zmian:	Nie dotyczy
Uzasadnienie:	nowe wydanie dokumentu

9.10.7 Procedury dotyczące aktualizacji

Procedury dotyczące aktualizacji Podręcznika obsługi są analogiczne do procedur jego redagowania. Zmiany wprowadzane są w porozumieniu z kierownikiem ds. usług certyfikacyjnych, kierownikiem ds. bezpieczeństwa, kierownikiem ds. ochrony danych osobowych, kierownikiem ds. prawnych i kierownikiem odpowiedzialnym za kwestie regulacyjne, a następnie zatwierdzane przez organ zarządzający firmy.

9.10.8 Terminy i sposób publikacji

Podręcznik obsługi udostępniany jest:

- w wersji elektronicznej na stronie internetowej TSP (adres: http://www.firma.infocert.it/doc/manuali.htm);
- w wersji elektronicznej na powszechnie dostępnej liście podmiotów certyfikujących prowadzonej przez AgID;
- w wersji papierowej na wniosek składany w punktach rejestracyjnych lub w przypadku użytkowników końcowych – w momencie bezpośredniego kontaktu.

9.10.9 Przypadki, w których OID wymaga zmiany

Nie dotyczy

9.11 Rozstrzyganie sporów

Patrz zapisy umowne szczegółowo regulujące zasady rozstrzygania sporów.

9.12 Sąd właściwy

Patrz zapisy umowne szczegółowo regulujące kwestię sądu właściwego.

9.13 Prawo właściwe

Prawem właściwym dla niniejszego Podręcznika obsługi jest prawo włoskie.
Poniżej znajduje się niewyczerpujący wykaz podstawowych odniesień do obowiązujących przepisów prawnych:

[1] Rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 910/2014 z dnia 23 lipca 2014 r. w sprawie identyfikacji elektronicznej i usług zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznym oraz uchylające dyrektywę 1999/93/WE (zwane również *Rozporządzeniem eIDAS*).
[2] [włoski] Dekret ustawodawczy nr 82 z dnia 7 marca 2005 r. ([włoski] Dziennik Ustaw nr 112 z dnia 16 maja 2005 r.) – Kodeks administracji cyfrowej (oznaczony również skrótem „CAD") z późn. zm. i uzup.
[3] brak
[4] [włoski] Dekret ustawodawczy nr 196 z dnia 30 czerwca 2003 r. ([włoski] Dziennik Ustaw nr 174 z dnia 29 lipca 2003 r.) – Kodeks ochrony danych osobowych z późn. zm. i uzup. oraz rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych (obowiązujące od 25 maja 2018 r.).
[5] brak
[6] brak
[7] Dyrektywa Parlamentu Europejskiego i Rady (UE) nr 2011/83/WE z dnia 25 października 2011 r. w sprawie praw konsumentów oraz odnośne krajowe przepisy transponujące.
[8] Wstępna kontrola 24 września 2015 r. [4367555] Przetwarzanie danych osobowych w ramach „Procesu wydawania dokumentów na podstawie identyfikacji z użyciem kamery internetowej" dla kwalifikowanego podpisu elektronicznego lub cyfrowego.
[9] Uchwała CNIPA (włoskie Krajowe Centrum Informatyczne Administracji Publicznej) nr 45 z dnia 21 maja 2009 r., z późniejszymi
zmianami (z dnia 5 lipca 2019 r. zastąpiona przez [13]).
[10] Decyzja AgID nr 189/2017
[11] Dyrektywa Parlamentu Europejskiego i Rady (UE) 2015/2366 z dnia 25 listopada 2015 r. znana jako Payment Services Directive – PSD2 (dyrektywa o usługach płatniczych).
[12] Rozporządzenie delegowane Komisji (UE) 2018/389 z dnia 27 listopada 2017 r. uzupełniające dyrektywę Parlamentu Europejskiego i Rady (UE) 2015/2366 w odniesieniu do regulacyjnych standardów technicznych dotyczących silnego uwierzytelniania klienta i wspólnych i bezpiecznych otwartych standardów komunikacji.
[13] Decyzja AgID nr 121/2019 wer. 1.1 (zastępuje decyzję CNIPA nr 45/2009) z późniejszymi sprostowaniami w drodze decyzji nr 147/2019.

[14] CPS Addendum – Akceptowalne dokumenty tożsamości.
[15] [hiszpańska] Ustawa 6/2020 z dnia 11 listopada, regulująca niektóre aspekty zaufanych usług elektronicznych.
[16] [hiszpańskie] Rozporządzenie królewskie 4/2010 z dnia 8 stycznia, regulujący Krajowy system interoperacyjności w dziedzinie administracji elektronicznej.
[17] [hiszpańska] Ustawa 39/2015 z dnia 1 października o powszechnym postępowaniu administracyjnym przed organami administracji publicznej.

[18] [hiszpańska] Ustawa 40/2015 z dnia 1 października o systemie prawnym sektora publicznego.
[19] [hiszpańskie] Rozporządzenie królewskie 203/2021 z dnia 30 marca zatwierdzające Rozporządzenie w sprawie działania i funkcjonowania sektora publicznego za pośrednictwem środków elektronicznych.

Ponadto zastosowanie znajdują wszystkie okólniki oraz uchwały organu nadzoru [10], a także akty wykonawcze, o których mowa w rozporządzeniu eIDAS [1].

9.14 Postanowienia różne

Patrz zapisy umowne regulujące wszelkie inne postanowienia niezawarte w niniejszym Podręczniku obsługi.

9.15 Inne postanowienia

Godziny świadczenia usługi, z zastrzeżeniem innych postanowień umownych:

Usługa	Godziny
Dostęp do publicznego archiwum certyfikatów (obejmuje certyfikaty, listy CRL i OCSP).	Od 0:00 do 24:00 7 dni w tygodniu (minimalna dostępność 99%)
Wniosek o unieważnienie i zawieszenie certyfikatów.	Od 0:00 do 24:00 7 dni w tygodniu (minimalna dostępność 99%)
Pozostałe czynności: rejestracja, generowanie, publikowanie, odnowienie[11].	Od 9:00 do 17:00 od poniedziałku do piątku, z wyjątkiem dni ustawowo wolnych od pracy Od 9:00 do 13:00 sobota
Wniosek o wydanie i/lub weryfikacja znacznika czasu.	24 h przez 7 dni w tygodniu (minimalna dostępność 99%)

[10] Dostępne na stronie https://www.agid.gov.it/index.php/it/piattaforme/firma-elettronica-qualificata.
[11] Proces rejestracji prowadzony jest w punktach rejestracji, których godziny otwarcia mogą różnić się między sobą. W każdym przypadku InfoCert zapewnia możliwość korzystania z oferowanej przez siebie usługi w podanych wyżej godzinach.

ANEKS A

Electronic Signature Qualified Root „InfoCert Firma Qualificata 2”

```
 0 1318: SEQUENCE {
 4 1038:   SEQUENCE {
 8  3:     [0] {
10  1:       INTEGER 2
      :     }
13  1:     INTEGER 1
16 13:     SEQUENCE {
18  9:       OBJECT IDENTIFIER
      :       sha256WithRSAEncryption (1 2 840 113549 1 1 11)
29  0:       NULL
      :     }
31 133:    SEQUENCE {
34 11:       SET {
36  9:         SEQUENCE {
38  3:           OBJECT IDENTIFIER countryName (2 5 4 6)
43  2:           PrintableString 'IT'
      :         }
      :       }
47 21:       SET {
49 19:         SEQUENCE {
51  3:           OBJECT IDENTIFIER organizationName (2 5 4 10)
56 12:           UTF8String 'INFOCERT SPA'
      :         }
      :       }
70 34:       SET {
72 32:         SEQUENCE {
74  3:           OBJECT IDENTIFIER organizationalUnitName (2 5 4 11)
79 25:           UTF8String 'Certificatore Accreditato'
      :         }
      :       }
106 20:      SET {
108 18:        SEQUENCE {
110  3:          OBJECT IDENTIFIER serialNumber (2 5 4 5)
115 11:          PrintableString '07945211006'
      :         }
      :       }
128 37:      SET {
130 35:        SEQUENCE {
132  3:          OBJECT IDENTIFIER commonName (2 5 4 3)
137 28:          UTF8String 'InfoCert Firma Qualificata 2'
      :         }
      :       }
      :     }
167 30:    SEQUENCE {
169 13:      UTCTime 19/04/2013 14:26:15 GMT
184 13:      UTCTime 19/04/2029 15:26:15 GMT
      :     }
199 133:   SEQUENCE {
202 11:      SET {
204  9:       SEQUENCE {
206  3:         OBJECT IDENTIFIER countryName (2 5 4 6)
211  2:         PrintableString 'IT'
      :         }
      :       }
```

```
215 21:       SET {
217 19:         SEQUENCE {
```

```
219  3:           OBJECT IDENTIFIER organizationName (2 5 4 10)
224 12:           UTF8String 'INFOCERT SPA'
      :         }
      :       }
238 34:       SET {
240 32:         SEQUENCE {
242  3:           OBJECT IDENTIFIER organizationalUnitName (2 5 4 11)
247 25:           UTF8String 'Certificatore Accreditato'
      :         }
      :       }
274 20:       SET {
276 18:         SEQUENCE {
278  3:           OBJECT IDENTIFIER serialNumber (2 5 4 5)
283 11:           PrintableString '07945211006'
      :         }
      :       }
296 37:       SET {
298 35:         SEQUENCE {
300  3:           OBJECT IDENTIFIER commonName (2 5 4 3)
305 28:           UTF8String 'InfoCert Firma Qualificata 2'
      :         }
      :       }
      :     }
335 290:    SEQUENCE {
339 13:       SEQUENCE {
341  9:         OBJECT IDENTIFIER rsaEncryption (1 2 840 113549 1 1 1)
352  0:         NULL
      :       }
354 271:      BIT STRING, encapsulates {
359 266:        SEQUENCE {
363 257:          INTEGER
      :           00 C5 A1 6E 5E 03 49 37 01 C5 3E FE FD AE 29 C9
      :           44 84 6A F1 5E 5A 8E 52 9B 40 40 92 D2 8F 2B 0F
      :           EC 86 8A 2A D1 B1 21 E5 FC 1C D6 AF C5 16 83 90
      :           B9 10 34 49 6A 97 EB 78 1A 02 0F C8 99 38 97 31
      :           DB 1F BD 9C D4 BB 36 48 7D 3A 5F BB 82 A3 98 86
      :           44 7D FE 15 4D 52 71 B7 2B CE F8 80 3C 1F B2 7A
      :           A5 19 D5 C2 A4 1B 2C 86 43 5C 01 B2 8A F1 A5 11
      :           14 79 A8 E4 5B 6C 2C 0E 26 3F 0D 8C 9E 4C 6D 48
      :               [ Another 129 bytes skipped ]
624 3:            INTEGER 65537
      :         }
      :       }
      :     }
629 413:    [3] {
633 409:      SEQUENCE {
637 15:       SEQUENCE {
639  3:         OBJECT IDENTIFIER basicConstraints (2 5 29 19)
644  1:         BOOLEAN TRUE
647  5:         OCTET STRING, encapsulates {
649  3:           SEQUENCE {
651  1:             BOOLEAN TRUE
      :           }
      :         }
      :       }
654 88:       SEQUENCE {
656  3:         OBJECT IDENTIFIER certificatePolicies (2 5 29 32)
661 81:         OCTET STRING, encapsulates {
663 79:           SEQUENCE {
665 77:             SEQUENCE {
667  4:               OBJECT IDENTIFIER anyPolicy (2 5 29 32 0)
673 69:               SEQUENCE {
675 67:                 SEQUENCE {
```

```
677  8:                 OBJECT IDENTIFIER cps (1 3 6 1 5 5 7 2 1)
687 55:                 IA5String
     :                 'http://www.firma.infocert.it/documentazione/manu'
     :                 'ali.php'
     :                   }
     :                 }
     :               }
     :             }
     :           }
     :         }
744 37:       SEQUENCE {
746  3:         OBJECT IDENTIFIER issuerAltName (2 5 29 18)
751 30:         OCTET STRING, encapsulates {
753 28:           SEQUENCE {
755 26:             [1] 'firma.digitale@infocert.it'
     :           }
     :         }
     :       }
783 213:      SEQUENCE {
786  3:       OBJECT IDENTIFIER cRLDistributionPoints (2 5 29 31)
791 205:       OCTET STRING, encapsulates {
794 202:         SEQUENCE {
797 199:           SEQUENCE {
800 196:             [0] {
803 193:               [0] {
806 42:                 [6]
     :                 'http://crl.infocert.it/crls/firma2/ARL.crl'
850 146:                [6]
     :                 'ldap://ldap.infocert.it/cn%3DInfoCert%20Firma%20'
     :                 'Qualificata%202,ou%3DCertificatore%20Accreditato'
     :                 ',o%3DINFOCERT%20SPA,c%3DIT?authorityRevocationLi'
     :                 'st'
     :                   }
     :                 }
     :               }
     :             }
     :           }
     :         }
999 14:       SEQUENCE {
1001  3:       OBJECT IDENTIFIER keyUsage (2 5 29 15)
1006  1:       BOOLEAN TRUE
1009  4:       OCTET STRING, encapsulates {
1011  2:         BIT STRING 1 unused bit
     :           '1100000'B
     :         }
     :       }
1015 29:      SEQUENCE {
1017  3:       OBJECT IDENTIFIER subjectKeyIdentifier (2 5 29 14)
1022 22:       OCTET STRING, encapsulates {
1024 20:         OCTET STRING
     :           93 DD 21 FC 03 D0 15 0A 72 AD A3 CC D5 9A 09 9D
     :           38 8B 9D E9
     :         }
     :       }
     :     }
     :   }
1046  13: SEQUENCE {
1048   9:   OBJECT IDENTIFIER sha256WithRSAEncryption (1 2 840 113549 1 1
           11)
1059.  0:   NULL
     :   }
1061. 257: BIT STRING
```

```
    :    69 82 8F 17 A0 84 16 FE AF 6D 35 03 F0 66 47 5D
    :    FD B0 1F 80 B8 9B A2 5B DB 93 B6 53 B2 25 65 56
    :    FD F9 05 BF 6B 84 CE 7C 48 A3 F5 5D AF 5C DB A0
    :    9F F3 2E 33 86 8A 65 55 B8 5F 29 11 95 08 B8 F5
    :    BB 51 17 74 F8 42 51 06 FC 59 67 0C D0 0C 8B 39
    :    78 F7 AA 16 CC 87 BE D4 2F 42 BD 79 A4 6B C1 30
    :    04 35 B9 78 DC 9C BA E4 73 C7 B9 B3 67 93 D5 3D
    :          [ Another 128 bytes skipped ]
    : }
```

Electronic Signature Qualified Root ”InfoCert Qualified Electronic Signature CA 3”

```
  0 1881: SEQUENCE {
  4 1345:   SEQUENCE {
  8  3:     [0] {
 10  1:       INTEGER 2
     :     }
 13  1:     INTEGER 1
 16 13:     SEQUENCE {
 18  9:       OBJECT IDENTIFIER
     :       sha256WithRSAEncryption (1 2 840 113549 1 1 11)
 29  0:       NULL
     :     }
 31 165:    SEQUENCE {
 34 11:       SET {
 36  9:         SEQUENCE {
 38  3:           OBJECT IDENTIFIER countryName (2 5 4 6)
 43  2:           PrintableString 'IT'
     :         }
     :       }
 47 24:       SET {
 49 22:         SEQUENCE {
 51  3:           OBJECT IDENTIFIER organizationName (2 5 4 10)
 56 15:           UTF8String 'InfoCert S.p.A.'
     :         }
     :       }
 73 41:       SET {
 75 39:         SEQUENCE {
 77  3:           OBJECT IDENTIFIER organizationalUnitName (2 5 4 11)
 82 32:           UTF8String 'Qualified Trust Service Provider'
     :         }
     :       }
116 26:       SET {
118 24:         SEQUENCE {
120  3:           OBJECT IDENTIFIER '2 5 4 97'
125 17:           UTF8String 'VATIT-07945211006'
     :         }
     :       }
144 53:       SET {
146 51:         SEQUENCE {
148  3:           OBJECT IDENTIFIER commonName (2 5 4 3)
153 44:           UTF8String
     :           'InfoCert Qualified Electronic Signature CA 3'
     :         }
     :       }
     :     }
199 30:     SEQUENCE {
201 13:       UTCTime 12/12/2016 16:34:43 GMT
```

```
216 13:       UTCTime 12/12/2032 17:34:43 GMT
      :     }
231 165:    SEQUENCE {
234 11:      SET {
236  9:       SEQUENCE {
238  3:        OBJECT IDENTIFIER countryName (2 5 4 6)
243  2:        PrintableString 'IT'
      :       }
      :      }
247 24:      SET {
249 22:       SEQUENCE {
251  3:        OBJECT IDENTIFIER organizationName (2 5 4 10)
256 15:        UTF8String 'InfoCert S.p.A.'
      :       }
      :      }
273 41:      SET {
275 39:       SEQUENCE {
277  3:        OBJECT IDENTIFIER organizationalUnitName (2 5 4 11)
282 32:        UTF8String 'Qualified Trust Service Provider'
      :       }
      :      }
316 26:      SET {
318 24:       SEQUENCE {
320  3:        OBJECT IDENTIFIER '2 5 4 97'
325 17:        UTF8String 'VATIT-07945211006'
      :       }
      :      }
344 53:      SET {
346 51:       SEQUENCE {
348  3:        OBJECT IDENTIFIER commonName (2 5 4 3)
353 44:        UTF8String
      :         'InfoCert Qualified Electronic Signature CA 3'
      :       }
      :      }
      :     }
399 546:    SEQUENCE {
403 13:      SEQUENCE {
405  9:       OBJECT IDENTIFIER rsaEncryption (1 2 840 113549 1 1 1)
416  0:       NULL
      :      }
418 527:     BIT STRING, encapsulates {
423 522:      SEQUENCE {
427 513:       INTEGER
      :         00 B7 C1 D3 BF 11 CB A8 28 B6 91 DD E1 11 85 9F
      :         9D 9A 51 25 B3 B2 BC B2 AE AD DF 3E 5D 9F 5A A0
      :         F9 E4 64 C8 34 40 DA AB 7A EC 98 62 05 38 EC 91
      :         EA 84 F9 07 E6 58 DE 58 34 A0 EB 0D 11 19 50 BA
      :         E9 C0 13 C7 60 08 DB E5 AE 00 50 E9 7C 10 16 09
      :         9E 4D F4 EC 7B 14 99 6F D0 A4 67 68 CD 7D 88 1E
      :         D1 3E DA 25 BC 3C 66 61 8D B6 5D D6 F8 CF BA 7A
      :         55 96 86 62 CC 3F 9D D1 B0 2B 58 03 A7 21 49 BC
      :             [ Another 385 bytes skipped ]
944 3:        INTEGER 65537
      :       }
      :      }
      :     }
949 400:    [3] {
953 396:     SEQUENCE {
957  15:      SEQUENCE {
959   3:       OBJECT IDENTIFIER basicConstraints (2 5 29
               19)
964   1:       BOOLEAN TRUE
967   5:       OCTET STRING, encapsulates {
```

```
969  3:          SEQUENCE {
```

```
 971  1:             BOOLEAN TRUE
      :           }
      :         }
      :       }
 974 88:       SEQUENCE {
 976  3:        OBJECT IDENTIFIER certificatePolicies (2 5 29 32)
 981 81:        OCTET STRING, encapsulates {
 983 79:         SEQUENCE {
 985 77:          SEQUENCE {
 987  4:           OBJECT IDENTIFIER anyPolicy (2 5 29 32 0)
 993 69:           SEQUENCE {
 995 67:            SEQUENCE {
 997  8:             OBJECT IDENTIFIER cps (1 3 6 1 5 5 7 2 1)
1007 55:               IA5String
      :             'http://www.firma.infocert.it/documentazione/manu'
      :             'ali.php'
      :            }
      :           }
      :          }
      :         }
      :       }
1064 239:     SEQUENCE {
1067  3:      OBJECT IDENTIFIER cRLDistributionPoints (2 5 29 31)
1072 231:      OCTET STRING, encapsulates {
1075 228:       SEQUENCE {
1078 225:        SEQUENCE {
1081 222:         [0] {
1084 219:          [0] {
1087 37:           [6] 'http://crl.infocert.it/ca3/qc/ARL.crl'
1126 177:           [6]
      :           'ldap://ldap.infocert.it/cn%3DInfoCert%20Qualifie'
      :           'd%20Electronic%20Signature%20CA%203,ou%3DQualifi'
      :           'ed%20Trust%20Service%20Provider,o%3DINFOCERT%20S'
      :           'PA,c%3DIT?authorityRevocationList'
      :          }
      :         }
      :        }
      :       }
      :      }
1306 14:     SEQUENCE {
1308  3:      OBJECT IDENTIFIER keyUsage (2 5 29 15)
1313  1:      BOOLEAN TRUE
1316  4:      OCTET STRING, encapsulates {
1318  2:       BIT STRING 1 unused bit
      :       '1100000'B
      :      }
      :     }
1322 29:     SEQUENCE {
1324  3:      OBJECT IDENTIFIER subjectKeyIdentifier (2 5 29 14)
1329 22:       OCTET STRING, encapsulates {
1331 20:        OCTET STRING
      :       9B 3B 1B 18 6A 3E A2 04 03 F4 D7 99 10 CF 97 11
      :       4C F1 AA DE
      :      }
      :     }
      :    }
      :   }
1353 13: SEQUENCE {
1355  9:    OBJECT IDENTIFIER sha256WithRSAEncryption (1 2 840 113549 1 1 11)
1366  0:    NULL
```

```
      :    }
1368 513: BIT STRING
      :    54 49 DC F3 76 1F BF 5D 33 B7 78 3A 26 72 4B 2B
      :    50 79 22 70 4A 7E DA EB 8F 26 3C 7F 8D CB 08 8E
      :    96 A6 EB 00 93 5D 82 1D 48 C8 E0 FF C6 1D 69 32
      :    3F E8 F3 FC 7A C7 9C 33 4B 19 FA 13 37 01 7F 54
      :    12 49 A3 51 19 6C 3B 0C 50 F1 D2 97 83 7B CF 4F
      :    58 F4 82 27 98 FB C7 11 97 B8 D7 FC 73 F2 96 41
      :    D1 13 25 07 5A 77 B1 E4 BE 6C 0E BD FA D8 CA 58
      :    5B DC 4B 08 4F EC CC 9F CD E9 E8 9E 7D 43 27 4D
      :          [ Another 384 bytes skipped ]
      : }
```

Electronic Signature Qualified Root „InfoCert Qualified Electronic Signature CA 4”

```
  0 1693: SEQUENCE {
  4 1157: SEQUENCE {
  8  3:     [0] {
 10  1:       INTEGER 2
      :     }
 13  1:     INTEGER 1
 16 13:     SEQUENCE {
 18  9:       OBJECT IDENTIFIER
      :       sha256WithRSAEncryption (1 2 840 113549 1 1 11)
 29  0:       NULL
      :     }
 31 165:    SEQUENCE {
 34 11:       SET {
 36  9:         SEQUENCE {
 38  3:           OBJECT IDENTIFIER countryName (2 5 4 6)
 43  2:           PrintableString 'IT'
      :         }
      :       }
 47 24:       SET {
 49 22:         SEQUENCE {
 51  3:           OBJECT IDENTIFIER organizationName (2 5 4 10)
 56 15:           UTF8String 'InfoCert S.p.A.'
      :         }
      :       }
 73 41:       SET {
 75 39:         SEQUENCE {
 77  3:           OBJECT IDENTIFIER organizationalUnitName (2 5 4 11)
 82 32:           UTF8String 'Qualified Trust Service Provider'
      :         }
      :       }
116 26:       SET {
118 24:         SEQUENCE {
120  3:           OBJECT IDENTIFIER '2 5 4 97'
125 17:           UTF8String 'VATIT-07945211006'
      :         }
      :       }
144 53:       SET {
146 51:         SEQUENCE {
148  3:           OBJECT IDENTIFIER commonName (2 5 4 3)
153 44:           UTF8String
      :           'InfoCert Qualified Electronic Signature CA 4'
```

: }

```
    :       }
    :     }
199  30:   SEQUENCE {
201  13:     UTCTime 23/03/2020 09:21:16 GMT
216  13:     UTCTime 23/03/2036 10:21:16 GMT
    :     }
231 165:   SEQUENCE {
234 11:     SET {
236  9:       SEQUENCE {
238  3:         OBJECT IDENTIFIER countryName (2 5 4 6)
243  2:         PrintableString 'IT'
    :       }
    :     }
247 24:     SET {
249 22:       SEQUENCE {
251  3:         OBJECT IDENTIFIER organizationName (2 5 4 10)
256 15:         UTF8String 'InfoCert S.p.A.'
    :       }
    :     }
273 41:     SET {
275 39:       SEQUENCE {
277  3:         OBJECT IDENTIFIER organizationalUnitName (2 5 4 11)
282 32:         UTF8String 'Qualified Trust Service Provider'
    :       }
    :     }
316 26:     SET {
318 24:       SEQUENCE {
320  3:         OBJECT IDENTIFIER '2 5 4 97'
325 17:         UTF8String 'VATIT-07945211006'
    :       }
    :     }
344 53:     SET {
346 51:       SEQUENCE {
348  3:         OBJECT IDENTIFIER commonName (2 5 4 3)
353 44:         UTF8String
    :           'InfoCert Qualified Electronic Signature CA 4'
    :       }
    :     }
    :   }
399 546:   SEQUENCE {
403  13:     SEQUENCE {
405   9:       OBJECT IDENTIFIER rsaEncryption (1 2 840 113549 1 1
    :         1)
416   0:       NULL
    :     }
418 527:     BIT STRING, encapsulates {
423 522:       SEQUENCE {
427 513:         INTEGER
    :           00 B3 F6 00 3B 90 01 2E AC 2A 26 9E CB 03 0C 02
    :           E3 8A C3 14 FE F6 22 6B 6B B5 31 8E 44 8B 01 C2
    :           80 46 B8 E9 3B A6 84 84 4A AB 45 D4 60 D5 67 AF
    :           9D 57 BA DC EC AE AE AF 4F DD 71 4C 63 9E E2 81
    :           AF 71 16 A6 D2 4A C7 EE 7B EB 2B A4 18 14 6E 35
    :           C8 33 C6 BF AD 43 F9 10 90 97 73 A0 5C 87 B0 19
    :           5E 1E 87 E7 45 70 BE 68 19 EB 53 34 56 15 A5 D4
    :           84 57 6A AA 69 25 F0 48 1C 3A 59 B6 2B EF D9 68
    :           E3 CA 7D E6 39 30 BC BE 38 55 6A 08 D9 F7 B5 37
    :           8A ED B6 15 25 D3 E8 95 B3 3B 3F 7D B4 4F C0 EB
    :           D5 44 D4 A0 7E 93 4A 37 84 8D 2D 3B A2 77 44 48
    :           BC 29 F0 AE 98 85 0A 04 BE DD 3E 4A 73 BA 09 9A
    :           F9 9C DE B8 29 0D A2 E9 70 01 68 37 CB 53 36 80
    :           7B 04 C3 71 64 FE 20 91 B2 37 A1 B5 C7 B9 15 68
    :           C8 22 C5 C2 D8 DC 5D 7C F6 92 E7 D6 12 4B AA C6
```

: 61 A9 C8 F3 FE E6 6C 89 8E A5 28 8A 20 7D D1 1F

```
    :           A8 D4 34 A2 C0 24 E5 07 BB E3 1F AF 07 5C 46 AB
    :           1C 05 52 92 7B FE C4 C4 BD 87 66 FE 2F 4D F3 D9
    :           20 08 45 81 6E A0 03 A3 6E F7 38 DB A0 76 DD 8C
    :           D1 1F 0A E8 6E DB 6F 55 F0 EE 19 6D E7 AA 63 5C
    :           32 03 43 D1 F5 6C 08 16 93 DC 2D 00 B7 38 30 2F
    :           92 56 02 69 BA 0C 9E E2 B9 31 29 DB 2D 29 27 BF
    :           B1 94 9D 36 EE 2E 6F 2D E6 E8 43 17 93 E1 79 EB
    :           76 03 EB 30 7D 39 01 B0 6E 92 51 8D 1B 75 A3 7C
    :           E6 07 F2 24 96 DA 91 A6 5A AC 14 14 2D 8C 79 9C
    :           F4 CD 5A 78 A6 6A B2 7A 6D 2D 5C 78 91 D6 F6 D1
    :           0D 6E 24 4B A6 81 35 4C 58 E8 CA 21 B5 FA 7F 6C
    :           9A 03 45 51 DA F8 C8 17 2E 6B 95 3D F3 29 C7 DF
    :           80 AC 6D 59 B8 B9 6C 85 9F 9E EC CC 54 76 B4 94
    :           0A 0C 12 93 19 14 B2 E3 87 1D 9C 25 78 4C 9E 75
    :           70 B0 37 5F A9 EF EC 86 FD F8 5A 9B 5F A7 E6 85
    :           9E 5E DD 4A 98 58 86 8C 61 73 1D FF F0 C2 36 98
    :           99
944  3:         INTEGER 65537
    :       }
    :      }
    :     }
949 213:    [3] {
952 210:     SEQUENCE {
955  15:      SEQUENCE {
957   3:       OBJECT IDENTIFIER basicConstraints (2 5 29 19)
962   1:       BOOLEAN TRUE
965   5:       OCTET STRING, encapsulates {
967   3:        SEQUENCE {
969   1:         BOOLEAN TRUE
    :         }
    :        }
    :       }
972  88:      SEQUENCE {
974   3:       OBJECT IDENTIFIER certificatePolicies (2 5 29 32)
979  81:       OCTET STRING, encapsulates {
981  79:        SEQUENCE {
983  77:         SEQUENCE {
985   4:          OBJECT IDENTIFIER anyPolicy (2 5 29 32 0)
991  69:          SEQUENCE {
993  67:           SEQUENCE {
995   8:            OBJECT IDENTIFIER cps (1 3 6 1 5 5 7 2 1)
1005  55:             IA5String
    :             'http://www.firma.infocert.it/documentazione/manu'
    :             'ali.php'
    :            }
    :           }
    :          }
    :         }
    :        }
1062  54:      SEQUENCE {
1064   3:       OBJECT IDENTIFIER cRLDistributionPoints (2 5 29 31)
1069  47:       OCTET STRING, encapsulates {
1071  45:        SEQUENCE {
1073  43:         SEQUENCE {
1075  41:          [0] {
1077  39:           [0] {
1079  37:            [6] 'http://crl.ca4.infocert.it/qc/ARL.crl'
    :           }
    :          }
    :         }
    :        }
    :       }
```

```
    :         }
1118 14:        SEQUENCE {
1120  3:          OBJECT IDENTIFIER keyUsage (2 5 29 15)
1125  1:          BOOLEAN TRUE
1128  4:          OCTET STRING, encapsulates {
1130  2:            BIT STRING 1 unused bit
    :             '1100000'B
    :           }
    :         }
1134 29:        SEQUENCE {
1136  3:          OBJECT IDENTIFIER subjectKeyIdentifier (2 5 29 14)
1141 22:          OCTET STRING, encapsulates {
1143 20:            OCTET STRING
    :             5D 7C 6B 61 E8 AC 90 EB 5E C9 D7 BE B4 E3 34 2E
    :             5C 2B 1C DF
    :           }
    :         }
    :       }
    :     }
    :   }
1165   13: SEQUENCE {
1167    9:   OBJECT IDENTIFIER sha256WithRSAEncryption (1 2 840 113549 1 1
          11)
1178.   0:   NULL
        :   }
1180. 513: BIT STRING
        :   80 F2 2D 1C 50 0B 6C 38 DE 22 99 D7 69 5B 92 95
        :   99 AE FD FD 7A 3A 4D 06 D0 01 E3 CE 56 DC AF 5B
        :   A6 23 EB CD 35 DB 11 C0 72 27 79 E6 7B 91 E6 4F
        :   D5 77 D6 68 E3 D2 48 B3 E9 49 D6 5B D4 57 3F E0
        :   9E 46 E4 0E F4 CF 66 E6 28 6A 91 F1 BE 3F 42 44
        :   0E 75 EB A8 1A D4 24 2C 65 36 9B D5 1E 82 2B 45
        :   29 18 3A CC 91 51 66 69 7D FE 6E E2 63 94 DA E1
        :   E9 82 AE 9B CE 5E B9 7B 7C E3 08 97 94 DB 57 C9
        :   EC D1 9A 71 2B DE 25 2B 85 77 2B 7F 99 97 16 4D
        :   7B 84 A9 DF DA 75 C6 62 8B 3B 65 B3 C3 D7 5C 42
        :   BA AB FB CE 2D 6B AA B6 EB 6E AD EA 84 52 F1 0F
        :   C8 E0 64 9C A1 07 94 9E CF E0 22 E2 D1 3D 71 DD
        :   B5 90 6B D5 69 5E 86 7A BF 4D 6C 50 B5 EC CF 8F
        :   E4 15 DE 37 C8 5F CE 7A 8A 3E 52 C1 DE AB CF 08
        :   1B E9 8D 1D A0 14 8C A7 67 C0 77 3F A4 55 1C F3
        :   7A E9 CE 7D C1 99 BE D0 32 37 81 F9 39 95 AF 46
        :   EE B8 B3 22 16 9C AA 1D A2 EA F2 B1 67 93 3B 4B
        :   2F 71 80 91 5B CE 7F 0D EF F2 BD 31 73 C2 2A 8F
        :   E3 F1 B3 99 F0 97 10 4F DE 15 C9 B5 89 ED A7 14
        :   0B 57 96 70 AF 76 D2 F0 F9 5E 35 19 5E 4D 67 7F
        :   1E 23 D3 FA F6 6E CA DF B1 60 DE 35 38 81 08 21
        :   FF 7E 4E 06 3C 8E 75 55 78 AC 55 F0 73 40 84 D2
        :   76 97 FE 1E FE 42 E7 9D F3 69 5B BD 45 09 89 AF
        :   C9 11 A6 12 E0 E6 BB 34 87 51 21 78 38 FA 4B DA
        :   B9 57 6C 3A 85 65 01 DB 7D 27 64 89 C3 83 DD 44
        :   0B BF 91 46 EC 94 88 0A DB 7D 4F BD 79 5D 5E 2C
        :   07 D0 5D E0 87 6B 3E 68 4F 79 CA DF 1F 15 89 60
        :   C2 09 B9 4A 5F D6 D3 38 B0 F8 9A 4F 26 A4 34 D6
        :   62 9E 2A 7C 50 BF 43 7E AE F0 5C 31 F2 99 BE DD
        :   6B 97 12 E6 42 94 45 44 19 C0 01 33 E4 C8 FA 0B
        :   E2 BB D1 F2 A3 25 4A B8 58 12 C3 2A E9 BD 9C FF
        :   8D 31 41 5C 8D DC 55 9B B3 DB 9A 64 A0 56 14 8A
        :
```

Electronic Signature Qualified Root „InfoCert Qualified Electronic Signature EC CA 4”

```
  0 872: SEQUENCE {
  4 751:   SEQUENCE {
  8   3:     [0] {
 10   1:       INTEGER 2
      :     }
 13  20:     INTEGER 0D 32 E7 F4 61 63 3C 34 DE 12 56 26 8E 51 91 97 08 F2 91 EF E3 5
 10:       SEQUENCE {E
 37   8:     OBJECT
IDENTIFIER ecdsaWithSHA384 (1 2 840 10045 4 3 3)
      :     }
 47 168:   SEQUENCE {
 50  11:     SET {
 52   9:       SEQUENCE
 54   3:       {
 59   2:         OBJECT IDENTIFIER countryName (2 5 4
      :           6) PrintableString 'IT'
      :       }}
 63  24:
 65  22:     SET {
 67   3:       SEQUENCE
 72  15:       {
      :         OBJECT IDENTIFIER organizationName (2 5 4 10)
      :       }     UTF8String 'InfoCert S.p.A.'
 89  41:     }
 91  39:
 93   3:     SET {
 98  32:       SEQUENCE
      :       {
      :       }   OBJECT IDENTIFIER organizationalUnitName (2 5 4 11)
132  26:         UTF8String 'Qualified Trust Service Provider'
134  24:     }
136   3:
               SET {
                 SEQUENCE
                 {
                  OBJECT IDENTIFIER '2 5 4 97'
141  17:          UTF8String 'VATIT-07945211006'
      :         }
      :       }
160  56:     SET {
162  54:       SEQUENCE
164   3:       {
169  47:         OBJECT IDENTIFIER commonName (2 5 4 3)
      :           UTF8String
      :         'InfoCert Qualified Electronic Signature EC CA 4'
      :       }}
      :
218  30:   }
           SEQUENCE {
220  13:     UTCTime 07/06/2021 08:43:18 GMT
235  13:     UTCTime 07/06/2036 09:43:18 GMT
      :     }
250 168:   SEQUENCE {
253  11:     SET {
255   9:       SEQUENCE {
```

```
257 3:           OBJECT IDENTIFIER countryName (2 5 4 6)
262 2:           PrintableString 'IT'
     :         }
     :       }
266 24:      SET {
268 22:        SEQUENCE {
```

```
270 3:           OBJECT IDENTIFIER organizationName (2 5 4 10)
275 15:          UTF8String 'InfoCert S.p.A.'
    :         }
    :       }
292 41:       SET {
294 39:         SEQUENCE {
296 3:           OBJECT IDENTIFIER organizationalUnitName (2 5 4 11)
301 32:          UTF8String 'Qualified Trust Service Provider'
    :         }
    :       }
335 26:       SET {
337 24:         SEQUENCE {
339 3:           OBJECT IDENTIFIER '2 5 4 97'
344 17:          UTF8String 'VATIT-07945211006'
    :         }
    :       }
363 56:       SET {
365 54:         SEQUENCE {
367 3:           OBJECT IDENTIFIER commonName (2 5 4 3)
372 47:          UTF8String
    :          'InfoCert Qualified Electronic Signature EC CA 4'
    :         }
    :       }
    :     }
421 118:    SEQUENCE {
423 16:       SEQUENCE {
425 7:         OBJECT IDENTIFIER ecPublicKey (1 2 840 10045 2 1)
434 5:         OBJECT IDENTIFIER secp384r1 (1 3 132 0 34)
    :       }
441 98:       BIT STRING
    :       04 5A 3E C7 0A 5F EB BB 35 7B 85 FF B8 3C AD 7C
    :       D6 06 9B D0 A1 F9 6A E5 7F 95 9B D3 BE 74 E8 64
    :       D0 01 7F F2 B9 ED FF 8B 0C 97 66 6C 28 AC 26 20
    :       B1 28 96 F7 11 12 15 05 B9 94 75 FB CA 95 19 D0
    :       45 57 CD 7B 0E 7E DB A2 89 25 F1 F8 5A 4F 0B 59
    :       CF 9A 8C 68 9E C8 2E 69 56 94 5E 90 83 6F 9D 64
    :       FD
    :     }
541 215:    [3] {
544 212:      SEQUENCE {
547 15:         SEQUENCE {
549 3:           OBJECT IDENTIFIER basicConstraints (2 5 29 19)
554 1:           BOOLEAN TRUE
557 5:           OCTET STRING, encapsulates {
559 3:             SEQUENCE {
561 1:               BOOLEAN TRUE
    :             }
    :           }
    :         }
564 88:         SEQUENCE {
566 3:           OBJECT IDENTIFIER certificatePolicies (2 5 29 32)
571 81:          OCTET STRING, encapsulates {
573 79:            SEQUENCE {
575 77:              SEQUENCE {
577 4:                OBJECT IDENTIFIER anyPolicy (2 5 29 32 0)
583 69:               SEQUENCE {
585 67:                 SEQUENCE {
587 8:                   OBJECT IDENTIFIER cps (1 3 6 1 5 5 7 2 1)
597 55:                  IA5String
    :                'http://www.firma.infocert.it/documentazione/manu'
    :                'ali.php'
    :                 }
    :                }
```

```
    :             }
    :           }
    :         }
    :       }
654 56:       SEQUENCE {
656 3:         OBJECT IDENTIFIER cRLDistributionPoints (2 5 29 31)
661 49:        OCTET STRING, encapsulates {
663 47:          SEQUENCE {
665 45:            SEQUENCE {
667 43:              [0] {
669 41:                [0] {
671 39:                  [6] 'http://crl.ca4.infocert.it/qcec/ARL.crl'
    :                }
    :              }
    :            }
    :          }
    :        }
712 14:       SEQUENCE {
714 3:         OBJECT IDENTIFIER keyUsage (2 5 29 15)
719 1:         BOOLEAN TRUE
722 4:         OCTET STRING, encapsulates {
724 2:           BIT STRING 1 unused bit
    :           '1100000'B
    :         }
    :       }
728 29:       SEQUENCE {
730 3:         OBJECT IDENTIFIER subjectKeyIdentifier (2 5 29 14)
735 22:        OCTET STRING, encapsulates {
737 20:          OCTET STRING
    :           8C DF 7C B8 F0 94 15 36 0B 7F DF 81 71 F5 DB 41
    :           5D 3B FD FC
    :         }
    :       }
    :     }
    :   }
759 10: SEQUENCE {
761 8:    OBJECT IDENTIFIER ecdsaWithSHA384 (1 2 840 10045 4 3 3)
    :   }
771 103: BIT STRING, encapsulates {
774 100:   SEQUENCE {
776 48:     INTEGER
    :       7C AF 22 1A 96 90 7C 55 72 88 49 DC B4 03 B6 7B
    :       E4 5F B2 2A CB 78 33 CC D6 EC 38 10 86 F4 21 41
    :       39 7B 78 EA 3D 59 10 BA BA 8C 30 E5 D6 09 2D FC
826 48:     INTEGER
    :       23 5D F8 C0 B2 26 9C D8 0D DA 64 EB 88 50 AB F2
    :       44 8F 85 BE 9A 59 7A C1 35 7A 66 4D 54 96 B1 60
    :       14 9A 2A C5 8D 63 93 A7 7B 14 78 8E AF 53 03 E3
    :     }
    :   }
    : }
```

Rozszerzenia certyfikatu

Rozszerzenia zawarte w wydanych certyfikatach i ich zawartość znajdują się w poniższym wykazie:

VERSION: zawiera wartość 3, jak opisano w punkcie 7.1.1 **SERIAL NUMBER**: przypisany automatycznie przez wydający CA **INNER SIGNATURE**: pkt 7.1.3

ISSUER: zawiera następujące pola z wartością DN jednego z wydających CA, zgodnie z treścią punktu Aneks A:

CountryName
OrganizationName
OrganizationalUnitName
OrganizationIdentifier
CommonName

VALIDITY: maksymalnie 63 (sześćdziesiąt trzy) miesiące, zawiera następujące pola:

NotBefore
NotAfter

SUBJECT: zawiera informacje dotyczące posiadacza będącego osobą fizyczną lub osobą prawną, może zawierać następujące pola, które ulegają zmianom w zależności od rodzaju certyfikatu, dodatkowe szczegóły znajdują się w punkcie 3.1:

W przypadku certyfikatu wydawanego osobie fizycznej:

CountryName: kod kraju na podstawie normy ISO 3166.

OrganizationName: w przypadku, gdy posiadacz jest osobą fizyczną związaną z organizacją, pole posiadacza certyfikatu może identyfikować tę organizację za pomocą atrybutów: OrganizationName i OrganizationIdentifier

OrganizationalUnitName: jeśli istnieją atrybuty dotyczące organizacji, pole to zawiera dodatkowe informacje o organizacji i może pojawić się nie więcej niż 4 (cztery) razy

OrganizationIdentifier: patrz definicja OrganizationName, kod identyfikacyjny

organizacji, z którą związany jest posiadacz, może mieć postać określoną w punkcie 5.1.4 normy ETSI EN 319 412-1 (np. „VATIT-TaxIdentificationNumber”, „NTRIT-IdentifierNationalTradeRegister)

GivenName: Imię posiadacza

Surname: Nazwisko posiadacza

SerialNumber: kod identyfikacyjny posiadacza; może mieć postać określoną w punkcie 5.1.3 normy ETSI EN 319 412-1 i w punkcie 3.1.5 niniejszego Podręcznika obsługi

Title: szczególne kwalifikacje lub rola podmiotu, patrz pkt 3.2.4. niniejszego Podręcznika obsługi

LocalityName

DNQualifier: unikalny kod identyfikacyjny w obrębie CA przypisany do posiadacza

Pseudonym: zawiera pseudonim posiadacza, jeżeli występują GivenName i Surname, ta wartość nie może występować.

CommonName: nazwisko posiadacza będącego osobą fizyczną

W przypadku certyfikatu wydawanego osobie prawnej:

CountryName: kod kraju na podstawie normy ISO 3166.

OrganizationName: zarejestrowana nazwa posiadacza będącego osobą prawną

OrganizationIdentifier: identyfikator organizacji posiadacza, może mieć postać określoną w punkcie 5.1.4 normy ETSI EN 319 412-1 i w punkcie 3.1.5 niniejszego Podręcznika obsługi

CommonName: nazwisko posiadacza będącego

osobą prawną StateOrProvinceName

LocalityName

PUBLIC KEY: pkt 6.1.5

EXTENSIONS:

AuthorityKeyIdentifier: pozwala zidentyfikować klucz publiczny odpowiadający kluczowi prywatnemu używanemu do podpisania certyfikatu

KeyUsage: rozszerzenie oznaczone jako krytyczne, które określa cel klucza zawartego w certyfikacie i spełnia zalecenia norm ETSI EN 319 412–2 i ETSI EN 319 412–3

CRLDistributionPoints: zawiera adresy URL publikacji list CRL, patrz pkt 2.2.3

AuthorityInformationAccess: zawiera informacje umożliwiające dostęp do usług wydającego CA, takich jak adres URL usługi OCSP do walidacji online (patrz pkt 7.3) i adres URL publikacji certyfikatu CA.

SubjectKeyIdentifier: zawiera identyfikator klucza publicznego certyfikatu

SubjectDirectoryAttributes: może występować i może zawierać dodatkowe atrybuty związane z posiadaczem:

DateOfBirth

SubjectAlternativeName: zawiera adresy e-mail, nazwy DNS, adresy IP i URI związane z posiadaczem certyfikatu

RFC822Name: adres e-mail posiadacza

CertificatePolicies: zawiera jedno lub większą liczbę kryteriów złożonych z jednego OID i kwalifikatory opcjonalne wskazujące polityki, na podstawie których certyfikat został wydany, oraz cele, do których może być on używany, patrz pkt 1.2, 4.5.3, zawiera ponadto adres publikacji niniejszego Podręcznika obsługi (CPS).

qcStatements: (*Qualified Certificate Statements*) zawierają rozszerzenie do włączenia oświadczeń wskazujących szczególne właściwości certyfikatu:

QcCompliance (0.4.0.1862.1.1): zawiera deklarację zgodności z prawodawstwem europejskim pkt 9.15 i występuje we wszystkich certyfikatach wystawionych zgodnie z niniejszym Podręcznikiem obsługi.

QcEuLimitValue (0.4.0.1862.1.2): jeśli zostało to przewidziane zawiera kwotę i walutę zgodnie

z treścią punktu 4.5.3

QcEURetentionPeriod (0.4.0.1862.1.3): zawiera wartość 20, rozumianą jako liczba lat przechowywania danych, zgodnie z treścią punktów 3.1.3, 4.9, 5.4.3, 5.5.1

QcSSCD (0.4.0.1862.1.4): jeżeli występuje, oświadcza, że klucz prywatny związany z kluczem publicznym zawartym w certyfikacie znajduje się w Qualified Signature/Seal Creation Device (QSCD) patrz pkt 1.2

QcEuPDS (0.4.0.1862.1.5): zawiera adres URL publikacji PKI Disclosure Statements (PDS)

QcType (0.4.0.1862.1.6): zawiera jedną z następujących wartości w zależności od celu, do którego certyfikat został wystawiony:
id-etsi-qct-esign
id-etsi-qct-eseal

pkixQCSyntax-v2 (1.3.6.1.5.5.7.0.18.11.2): jeżeli istnieje, zawiera semantykę według atrybutów i nazw zawartych w polach i w rozszerzeniach certyfikatu, jak określono w RFC3739:
id-etsi-qcs-semanticsId-Natural (0.4.0.194121.1.1)
id-etsi-qcs-SemanticsId-Legal (0.4.0.194121.1.2)

SIGNATURE: pkt 7.1.3

Rozszerzenia QCStatement dla QSealC PSD2

ETSI extensions: etsi-psd2-qcStatement (QcType)::= 0.4.0.19495.2	*SEQUENCE{* *rolesOfPSP RolesOfPSP,* *nCAName NCAName, nCAId* *NCAId }*
RolesOfPSP	*SEQUENCE{* *roleOfPspOid RoleOfPspOid, roleOfPspName* *RoleOfPspName }*
RoleOfPspOid	itu-t(0) identified-organization(4) etsi(0) psd2(19495) id-roles(1) 1 itu-t(0) identified-organization(4) etsi(0) psd2(19495) id-roles(1) 2 itu-t(0) identified-organization(4) etsi(0) psd2(19495) id-roles(1) 3 itu-t(0) identified-organization(4) etsi(0) psd2(19495) id-roles(1) 4
RoleOfPspName	PSP_AS PSP_PI PSP_AI PSP_IC
NCAName	*plain text name in English of the NCA*
NCAId	• *2 character ISO 3166 country code representing the NCA country;* • *hyphen-minus "-" (0x2D (ASCII), U+002D (UTF-8)); and* • *2-8 character NCA identifier without country code (A-Z uppercase only, no separator).*

Format list CRL i OCSP

Rozszerzenie	Wartość

Issuer Signature Algorithm	W zależności od klucza certyfikatu root CA wybranego spośród sha256WithRSAEncryption [iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) sha256WithRSAEncryption(11)] ecdsa-with-SHA256 [iso(1) member-body(2) us(840) ansi-

	x962(10045) signatures(4) ecdsa-with-SHA2(3) ecdsa-with-SHA256(2)] ecdsa-with-SHA384 [iso(1) member-body(2) us(840) ansi-x962(10045) signatures(4) ecdsa-with-SHA2(3) ecdsa-with-SHA384(3)] ecdsa-with-SHA512 [iso(1) member-body(2) us(840) ansi-x962(10045) signatures(4) ecdsa-with-SHA2(3) ecdsa-with-SHA512(4)]
Issuer Distinguished Name	InfoCert
thisUpdate	Data w formacie UTC
nextUpdate	Data następnej listy CRL w formacie UTC
Revoked Certificates List	Lista unieważnionych certyfikatów z numerem seryjnym i datą unieważnienia lub zawieszenia
Issuer's Signature	Podpis CA

Wartości i rozszerzenia dla list CRL i OCSP

Listy CRL mają następujące rozszerzenia

Extension	Value
Authority Key Identifier	Wartość odcisku 160-bit SHA-1 di issuerPublicKey
CRL number	Unikalny numer listy CRL przyznany przez CA
ExpiredCertsOnCRL	Data w formacie GeneralizedTime, po upływie której przeterminowane certyfikaty przechowywane są na liście CRL. Ustawiona wartość odpowiada dacie wystawienia CA
Issuing Distribution Point	Wyznacza miejsce dystrybucji list CRL oraz cel: wskazuje, czy lista CRL została wygenerowana tylko dla certyfikatów CA, czy dla certyfikatów podmiotu (end-entity)
Invalidity Date	Data w formacie UTC oznaczająca datę, od której uznaje się, że certyfikat jest nieważny

Żądanie OCSP zawiera następujące pola:

Field	Value

Hash Algorithm	sha-1 [1 3 14 3 2 26] OR sha-256 [2 16 840 1 101 3 4 2 1] OR sha-384 [2 16 840 1 101 3 4 2 2] OR sha-512 [2 16 840 1 101 3 4 2 3]
Issuer Name Hash	Hash DN podmiotu wystawiającego
Issuer Key Hash	Hash publicznego klucza podmiotu wystawiającego.
Serial Number	Numer seryjny certyfikatu

Odpowiedź OCSP zawiera następujące pola:

Field	Value
Response Status	Status odpowiedzi OCSP
Response Type	id-pkix-ocsp-basic [1 3 6 1 5 5 7 48 1 1]
Responder ID	Subject DN certyfikatu podpisującego odpowiedź OCSP
Produced at	Data w formacie GeneralizedTime, w której została wygenerowana odpowiedź OCSP
Hash Algorithm	sha-1 [1 3 14 3 2 26] OR sha-256 [2 16 840 1 101 3 4 2 1] OR sha-384 [2 16 840 1 101 3 4 2 2] OR sha-512 [2 16 840 1 101 3 4 2 3]
Issuer Name Hash	Hash Distinguished Name podmiotu wystawiającego
Issuer Key Hash	Hash publicznego klucza podmiotu wystawiającego
Serial Number	Numer seryjny certyfikatu
thisUpdate	Data weryfikacji statusu certyfikatu w formacie GeneralizedTime
nextUpdate	Data, w której możliwa jest aktualizacja statusu certyfikatu
Issuer Signature Algorithm	W zależności od klucza certyfikatu OCSP Responder wybranego spośród sha256WithRSAEncryption [iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) sha256WithRSAEncryption(11)] ecdsa-with-SHA256 [iso(1) member-body(2) us(840) ansi-x962(10045) signatures(4) ecdsa-with-SHA2(3) ecdsa-with-SHA256(2)] ecdsa-with-SHA384 [iso(1) member-body(2) us(840) ansi-x962(10045) signatures(4) ecdsa-with-SHA2(3) ecdsa-with-

	SHA384(3)] ecdsa-with-SHA512 [iso(1) member-body(2) us(840) ansi-x962(10045) signatures(4) ecdsa-with-SHA2(3) ecdsa-with-SHA512(4)]
Issuer's Signature	[OCSP response Signature]
Issuer certificate	[OCSP response signing certificate]

Żądanie OCSP może zawierać następujące rozszerzenia:

Extension	Value
nonce	Dowolny numer tylko do jednorazowego użytku. Kryptograficznie łączy żądanie z odpowiedzią na nie, aby zapobiec atakom przez ponawianie. W przypadku żądania numer ten zawarty jest w requestExtensions, natomiast w przypadku odpowiedzi może być zawarty w responseExtensions.

Aneks B

Narzędzia i zasady składania oraz weryfikacji podpisu cyfrowego

InfoCert udostępnia darmowy produkt (zwany „GoSign”) ,
który posiadacze certyfikatu mogą pobrać ze strony www.firma.infocert.it i który umożliwia:

- cyfrowe podpisywanie dokumentów wszystkim posiadaczom posiadającym certyfikat wystawiony przez InfoCert;
- weryfikację podpisu złożonego pod dokumentami podpisanymi cyfrowo zgodnie ze wzorami ustalonymi w aktach wykonawczych do rozporządzenia.

Środowiska, w których działa GoSign, oraz wymagania dotyczące sprzętu i oprogramowania, a także wszelkie instrukcje dotyczące procedury instalowania produktu dostępne są na powyższej stronie internetowej. Instrukcje dotyczące korzystania z produktu zawarte są w samym produkcie i można się z nimi zapoznać przy użyciu funkcji pomocy. Produkt GoSign może służyć do podpisywania każdego rodzaju pliku. Możliwość wyświetlania pliku zależy od dostępności odpowiedniego oprogramowania do wizualizacji na stanowisku pracy użytkownika.
InfoCert może udostępnić, za opłatą i zgodnie z ustaleniami w porozumieniach handlowych każdorazowo zawieranych z RA, wnioskodawcami, posiadaczami lub użytkownikami, dodatkowe produkty lub usługi w zakresie składania i/lub weryfikowania podpisu. Dokumenty elektroniczne podpisywane przy pomocy certyfikatów wystawianych przez InfoCert mogą być weryfikowane również przy użyciu innych narzędzi, które obsługują przewidziane formaty podpisów. InfoCert nie bierze odpowiedzialności za narzędzia, o których mowa powyżej.
Na przykład dokumenty podpisane z wykorzystaniem certyfikatów wystawionych w świetle niniejszego CPS w formacie PAdES, można zweryfikować również za pomocą Adobe Reader®.

Aneks C

Niniejszy aneks zawiera listę i cechy certyfikatów kwalifikowanych dla Hiszpanii.
Obecnie jedynym przetwarzanym certyfikatem jest certyfikat kwalifikowany obywatela hiszpańskiego określający tożsamość osoby fizycznej, która go podpisała i działa na własny rachunek.
Ogólnie rzecz biorąc, hiszpańskie organy administracji publicznej wymagają, aby certyfikaty były wydawane dla następujących zastosowań:

- Uwierzytelnianie w oparciu o certyfikaty X.509v3;
- Podpis cyfrowy, zaawansowany lub kwalifikowany, w oparciu o certyfikaty X.509v3;
- Kryptografia asymetryczna lub mieszana w oparciu o certyfikaty X.509v3.

Odniesienia do obowiązujących hiszpańskich przepisów prawnych znajdują się w punktach od [15] do [19].

Polityka dla certyfikatu kwalifikowanego obywatela Hiszpanii na urządzeniu kwalifikowanym jest następująca:

Opis	OID
Podręcznik obsługi dla certyfikatu kwalifikowanego obywatela Hiszpanii wystawionego osobie fizycznej i kluczy na urządzeniu kwalifikowanym (SSCD)	**1.3.76.36.1.1.10.16.1.1.1** zgodna z polityką QCP-n- qscd 0.4.0.194112.1.2

Certyfikat kwalifikowany obywatela Hiszpanii będącego osobą fizyczną w QSCD
Wystawionego przez root CA „InfoCert Qualified Electronic Signature CA 4”

Field	Value
ISSUER:	
Country Name:	IT
Organization Name:	InfoCert S.p.A.
Organizational Unit Name:	Qualified Trust Service Provider
Organization Identifier:	VATIT-07945211006

Common Name:	InfoCert Qualified Electronic Signature CA 4
SUBJECT:	
Country Name:	*CountryCode (ISO 3166) (mandatory)* ***(*)***
GivenName:	*Name (mandatory)*
Surname:	*Surname**s** (mandatory)*
SerialNumber:	*as defined in clause 5.1.3 of ETSI EN 319 412-1 (i.e. "**TINES**-NIF or NIE", "**PASES-**PassportNumber", "**IDCES-**DNI or TIE CardNumber") (mandatory)*
DNQualifier	*Holder's identification code assigned by the Certification Authority, unique within the Certification Authority itself (mandatory)*
Common Name	*<DNI or NIE of the subject> + "" + <Name of the subject> <First Surname of the subject> (mandatory)*
Subject Alternative Name	
RFC822Name	*certificate holder e-mail*
Directory Name	*(mandatory)*
	*Certificate holder **name** (mandatory) (OID 1.3.6.1.4.1.17326.30.7)*
	*Certificate holder **First Surname** (mandatory) (OID 1.3.6.1.4.1.17326.30.8)*
	*Certificate holder **Second Surname** (mandatory) (OID 1.3.6.1.4.1.17326.30.9)*
	*Certificate **Description** (mandatory) (OID 1.3.6.1.4.1.17326.30.10) ("CERTIFICADO ELECTRONICO CUALIFICADO DE CIUDADANO")*
User Notice	*Certificado cualificado de Ciudadano. Consulte las condiciones de uso en http://www.firma.infocert.it/documentazione/manuali.php (mandatory)*

(*): it contains the country consistent with the legal Jurisidction under which the certificate is issued

Ostrzeżenie

Niektóre formaty pozwalają wprowadzić do dokumentu wykonywalny kod (makro lub polecenia), bez naruszania jego struktury binarnej i umożliwiający aktywację funkcji, które mogą zmienić akty, fakty lub dane zawarte w tym dokumencie. Podpis cyfrowy złożony w plikach zawierających takie elementy nie ma skutków, o których mowa w art. 25 ust. 2 rozporządzenia [1], czyli nie może być uważany za równoważny podpisowi własnoręcznemu. W gestii posiadacza jest upewnienie się, za pośrednictwem funkcji właściwych dla danego produktu, że dokument nie zawiera takiego kodu wykonywalnego.