Podręcznik Obsługi

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

InfoCert
GRUPPO TECNOINVESTIMENTI

SPIS TREŚCI

SPIS ILUSTRACJI

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 Polityką certyfikacji i kodeksem postępowania certyfikacyjnego dla **dostawcy usług zaufania InfoCert** (*Trust Service Provider*), który, w ramach swoich usług zaufania, świadczy również usługi kwalifikowanego podpisu elektronicznego. Polityka ta zawiera zasady i praktyki stosowane w procesie identyfikacji i wydawania certyfikatu kwalifikowanego, przyjęte środki bezpieczeństwa, obowiązki, gwarancje i zakresy odpowiedzialności oraz, ogólnie, wszystko, 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 została na standardach 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.

1.2 Nazwa i identyfikacja dokumentu

Dokument ten nosi nazwę „Dostawca usług zaufania InfoCert – Polityka certyfikacji i kodeks postępowania certyfikacyjnego" i oznakowany został kodem dokumentu: **ICERT-INDI-MO**. Wersja i poziom wydania widoczne są w nagłówku każdej strony.

Wersja 3.0 niniejszego dokumentu stanowi kontynuację i zastępuje poprzednie polityki certyfikacji o kodach:

- ICERT-INDI-MO, wersja 2.12 z dnia 3.11.2016 r. dotycząca wydawania kwalifikowanych certyfikatów dla osób fizycznych;
- ICERT-INDI-MO-CMS, wersja 1.3 z dnia 25.03.2016 r. dotycząca wydawania kwalifikowanych certyfikatów dla osób fizycznych za pośrednictwem systemu CMS;

opisując w jednym dokumencie zasady i procedury zarządzania certyfikatami kwalifikowanymi zgodnie z rozporządzeniem eIDAS [1].

Do dokumentu przypisane są opisane poniżej identyfikatory obiektu (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:

Polityka certyfikacji 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
Polityka certyfikacji 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
Polityka certyfikacji dla certyfikatu kwalifikowanego wydawanego osobie prawnej również na urządzeniu (SSCD)	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:

Polityka certyfikacji 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
Polityka certyfikacji dla certyfikatu kwalifikowanego wydawanego osobie fizycznej do automatycznego zdalnego podpisu na urządzeniu (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
Polityka certyfikacji dla certyfikatu kwalifikowanego wydawanego osobie fizycznej do zdalnego podpisu na urządzeniu (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
Polityka certyfikacji dla certyfikatu kwalifikowanego wydawanego osobie fizycznej za pośrednictwem systemu CMS na urządzeniu (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
Polityka certyfikacji dla certyfikatu kwalifikowanego wydawanego osobie prawnej na urządzeniu (QSCD)	1.3.76.36.1.1.46 zgodna z polityką QCP-l-qscd 0.4.0.194112.1.3

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 niniejszej Polityki.
Dokument ten jest publikowany w formie elektronicznej na stronie internetowej dostawcy usług zaufania pod adresem: http://www.firma.infocert.it, w zakładce „Dokumentacja”.

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 (**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 włoskim kodeksem administracji cyfrowej [2].

Pełne dane organizacji pełniącej funkcję CA są następujące:

Nazwa firmy	InfoCert – spółka akcyjna Spółka podlegająca zarządowi i koordynacji Tecnoinvestimenti S.p.A.
Siedziba statutowa	Piazza Sallustio nr 9, 00187, Roma (RM)
Siedziba operacyjna	Via Marco e Marcelliano nr 45, 00147, Roma (RM)
Przedstawiciel prawny	Danilo Cattaneo Jako pełnomocny członek zarządu
Numer telefonu	06 836691
Numer wpisu do Rejestru Przedsiębiorstw	Kod identyfikacji podatkowej 07945211006
Numer NIP	07945211006
Strona internetowa	https://www.infocert.it

1.3.2 Registration authority – punkt rejestracji (RA)

Punkty rejestracji (RA, ang. *Registration Authority***)** 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 takie jest 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, zwane „Konwencją RAO", 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** działają na podstawie instrukcji otrzymanych od RA, któremu podlegają i którego zadaniem jest nadzorowanie poprawności stosowanych procedur.

1.3.3 posiadacz

posiadaczem jest osoba fizyczna lub prawna będąca posiadaczem certyfikatu kwalifikowanego, do którego wprowadzane są podstawowe dane identyfikacyjne. W niektórych częściach niniejszej Polityki i 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 obecnym kwalifikowanym podpisie elektronicznym) w celu 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, ponosząc wszelkie odnośne koszty, której przysługuje prawo do zawieszenia lub unieważnienia 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.

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, aby zagwarantować ich zgodność z wymogami ustanowionymi 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.

1.4 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 certyfikat należy.

CA InfoCert udostępnia do weryfikacji podpisów produkt opisany w 0. 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 Polityką

1.5.1 Kontakt

InfoCert jest odpowiedzialny za opracowanie, publikację i aktualizację niniejszego dokumentu. Pytania, reklamacje, uwagi i prośby o udzielenie wyjaśnień dotyczące niniejszej Polityki 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 nr 3
35131 Padova (Padwa)
Telefon: 06 836691
Fax: 049 0978914
Call center: 06 54641489
Strona internetowa: https://www.firma.infocert.it
e-mail: firma.digitale@legalmail.it

posiadacz lub wnioskodawca mogą żądać wydania kopii dokumentacji ich dotyczącej 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 Polityki

Niniejszy dokument jest weryfikowany przez kierownika ds. bezpieczeństwa i polityk, kierownika ds. ochrony danych osobowych, kierownika ds. usług certyfikacyjnych, Biuro Prawne i Dział Doradztwa oraz zatwierdzany przez zarząd przedsiębiorstwa.

1.5.3 Procedury zatwierdzania

Polityka jest sporządzana i zatwierdzana zgodnie z procedurami systemu zarządzania jakością w przedsiębiorstwie wg normy ISO 9001:2008.
Co najmniej raz w roku dostawca usług zaufania sprawdza zgodność niniejszej Polityki z własnym procesem świadczenia usług certyfikacyjnych.

1.6 Definicje i skróty

1.6.1 Definicje

Poniżej podano definicje terminów stosowanych w niniejszych dokumencie. W celu zrozumienia znaczenia terminów zdefiniowanych w rozporządzeniu eIDAS [1] i 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, standardach 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 zgodnie z obowiązującymi przepisami prawa.
CAB – Conformity Assessment Body (jednostka oceniająca zgodność)	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.
CAR – Conformity Assessment Report (raport z oceny zgodności)	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 posiadaczów lub wnioskodawców.
Certyfikat podpisu elektronicznego	Poświadczenie elektroniczne, które przyporządkowuje dane służące do walidacji podpisu elektronicznego do osoby fizycznej i potwierdza co najmniej imię i nazwisko lub pseudonim 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]).
Klucz certyfikacyjny lub klucz root	Para kluczy kryptograficznych używanych przez CA do podpisywania certyfikatów i list unieważnionych lub zawieszonych certyfikatów.
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]).
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 służące do walidacji	Dane używane do walidacji podpisu elektronicznego (patrz eIDAS [1]).
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	Skonfigurowane oprogramowanie lub skonfigurowany sprzęt, które wykorzystuje się do składania podpisu elektronicznego (patrz eIDAS [1]).
Kwalifikowane urządzenie do składania podpisu elektronicznego (SSCD – secure system creation device, lub QSCD)	Urządzenie do składania podpisu elektronicznego, które spełnia wymogi określone w załączniku II rozporządzenia eIDAS (patrz eIDAS [1]). Litera Q oznacza, że urządzenie jest kwalifikowane.
Dokument elektroniczny	Każda treść przechowywana w postaci elektronicznej, w szczególności tekst lub nagranie dźwiękowe, wizualne lub audiowizualne (patrz eIDAS [1]).
Podpis automatyczny	Szczególna procedura informatyczna podpisu elektronicznego, przeprowadzana po uprzedniej autoryzacji podpisującego, który zachowuje wyłączną kontrolę nad własnymi kluczami do podpisu, w przypadku braku terminowego i ciągłego nadzorowania z jego strony.
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 posiadaczowi za pomocą klucza prywatnego oraz odbiorcy za pomocą klucza publicznego, odpowiednio, ujawnienie i weryfikację pochodzenia i 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 w postaci elektronicznej, 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

	pozwala zapewnić wyłączną kontrolę kluczy prywatnych przez ich posiadaczy (patrz rozporządzenie DPCM [5]).
Podpisujący	Osoba fizyczna, która składa podpis elektroniczny (patrz eIDAS [1]).
Dziennik kontrolny	Dziennik kontrolny zawiera zbiór zapisów, wykonywanych automatycznie lub ręcznie, dotyczących zdarzeń przewidzianych w przepisach technicznych[5].
Identyfikacja elektroniczna	Proces używania danych w postaci elektronicznej identyfikujących osobę, unikalnie reprezentujących osobę fizyczną lub prawną, lub osobę fizyczną reprezentującą osobę prawną (patrz eIDAS [1]).
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, jeśli jest trwała, lub zawieszeniem, jeśli jest tymczasowa. W przypadku unieważnienia lub zawieszenia certyfikatu, jego numer seryjny jest dodawany do listy CRL, która jest następnie publikowana w rejestrze publicznym.
Polityka certyfikacji i kodeks postępowania certyfikacyjnego [certificate practice statement]	Dokument Polityka certyfikacji i kodeks postępowania certyfikacyjnego (zwany również „Polityką") definiuje procedury, które CA stosuje przy świadczeniu usługi. Podczas opracowywania Polityki 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.
OTP – One Time Password	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 przynajmniej jedną usługę zaufania, jako kwalifikowany lub niekwalifikowany dostawca usług zaufania (patrz eIDAS [1]).
Kwalifikowany dostawca usług zaufania	Dostawca usług zaufania, który świadczy przynajmniej jedną kwalifikowaną usługę zaufania i któremu status kwalifikowany nadał organ nadzoru (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]	Rejestr publiczny jest 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 przerywa ważność certyfikatu przed upływem jego naturalnej daty ważności.
Rola	Termin „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: a) tworzenie, weryfikację i walidację podpisów elektronicznych, pieczęci elektronicznych lub elektronicznych znaczników czasu, usług rejestrowanego doręczenia elektronicznego oraz certyfikatów powiązanych z tymi usługami; lub b) tworzenie, weryfikację i walidację certyfikatów uwierzytelniania witryn internetowych; lub c) 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]).
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 czasie (patrz eIDAS [1]).
Kwalifikowany elektroniczny znacznik czasu	Elektroniczny znacznik czasu spełniający wymogi art. 42 rozporządzenia eIDAS (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	
AgID	Agencja ds. Cyfryzacji Włoch – organ nadzoru nad dostawcami usług zaufania
CA	Certification Authority – urząd certyfikacji
CAB	Conformity Assessment Body – jednostka oceniająca zgodność
CAD	Włoski kodeks administracji cyfrowej
CAR	Conformity Assessment Report – raport z oceny zgodności
CC	Common Criteria
CIE	Elektroniczny dowód osobisty
CMS	Card Management System
CNS – TS-CNS	Krajowa karta usług Karta ubezpieczenia zdrowotnego – krajowa karta usług
CRL	Certificate Revocation List
DMZ	Demilitarized Zone

DN	Distinguish Name
EAL	Evaluation Assurance Level
eID	Electronic Identity
eIDAS	Electronic Identification and Signature Regulation
ERC	Emergency Request Code
ETSI	European Telecommunications Standards Institute
FIPS	Federal Information Processing Standard
HSM	Hardware Secure Module – 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	Operator punktu rejestracji
ISO	International Organization for Standardization – ISO, założona w 1946 roku, jest międzynarodową organizacją złożoną z krajowych organów normalizacyjnych
ITU	International Telecommunication Union – założona w 1865 r., jest międzynarodową organizacją zajmującą się ustanawianiem standardów w telekomunikacji
IUT	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
NTR Code	National Trade Register Code
OID	Object Identifier – składa się z sekwencji liczb, zarejestrowanej zgodnie z procedurą określoną w ISO/IEC 6523, która identyfikuje określony obiekt w zakresie hierarchii
OTP	OneTime Password
PEC	Certyfikowana poczta elektroniczna
PIN	Personal Identification Number – kod przypisany do bezpiecznego urządzenia do składania podpisu, używany przez posiadacza w celu uzyskania dostępu do funkcji danego urządzenia
PKCS	Public-Key Cryptography Standards
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
RA	Registration Authority – punkt rejestracji
RFC	Request for Comment – dokument zawierający informacje lub specyfikacje dotyczące nowych badań, innowacji i metodologii w

	dziedzinie IT, przekazany przez autorów do oceny społecznej
RSA	Pochodzi od inicjałów wynalazców algorytmu: River, Shamir, Adleman
SZBI	System zarządzania bezpieczeństwem informacji
SPID	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
URL	Uniform Resource Locator
VAT Code	Value Added Tax Code
X.500	Standard ITU-T dla usług LDAP i directory
X.509	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, 7 dni w tygodniu.

2.2 Publikacja informacji dotyczących certyfikacji

2.2.1 Publikacja Polityki

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

2.2.2 Publikacja certyfikatów

posiadacz lub wnioskujący reprezentujący osobę prawną może złożyć wniosek o upublicznienie własnego certyfikatu, przesyłając odpowiedni formularz (dostępny na stronie internetowej www.firma.infocert.it), podpisany cyfrowo kluczem odpowiadającym certyfikatowi, o którego publikację wnioskuje. Wniosek należy wysłać pocztą elektroniczną na adres richiesta.pubblicazione@cert.legalmail.it zgodnie z procedurą opisaną na stronie internetowej.

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 pod adresem: ldap://ldap.infocert.it lub za pośrednictwem protokołu HTTP pod adresem http://crl.infocert.it. Dostęp do tych list można uzyskać za pomocą oprogramowania dostarczonego przez CA i/lub korzystając z funkcji obecnych w produktach dostępnych na rynku, które obsługują protokół LDAP i/lub HTTP.

Oprócz wyżej wskazanych metod 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 Polityki

Polityka publikowana jest 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 Politykę oraz poczekać na pozwolenie na publikację.

2.3.2 Częstotliwość publikacji list certyfikatów unieważnionych i zawieszonych

Listy CRL są publikowane co godzinę.

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 Nadawanie nazw

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 normami ETSI dotyczącymi wydawania certyfikatów kwalifikowanych oraz zgodnie z przepisami DPCM.

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 3.2.3.1) posiadacz ma prawo do zażądania od CA, aby certyfikat zawierał pseudonim zamiast rzeczywistych danych. Ponieważ certyfikat jest kwalifikowany, CA będzie przechowywać informacje na temat rzeczywistej tożsamości osoby przez dwadzieścia (20) lat po wydaniu certyfikatu.

3.1.4 Zasady interpretacji rodzajów nazw

InfoCert spełnia wymagania standardu X.500.

3.1.5 Jednoznaczność nazw

Aby zapewnić jednoznaczną identyfikację posiadacza, certyfikat musi zawierać imię i nazwisko oraz unikalny kod identyfikacyjny, tj. TIN – Tax Identification Number. TIN może zostać nadany 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, wykorzystywanego w procedurach rozpoznawania.

W przypadku osoby prawnej, w celu zapewnienia jednoznacznej identyfikacji posiadacza, w certyfikacie należy podać nazwę organizacji i unikalny kod identyfikacyjny:

- NIP lub numer w Rejestrze Przedsiębiorstw w przypadku włoskich osób prawnych,
- NIP (Value Added Tax Code) lub NTR (National Trade Register) w przypadku innych osób prawnych.

3.1.6 Uznawanie, 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.

CA nie weryfikuje wykorzystania znaków towarowych i może 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, w tym za pośrednictwem punktu rejestracji lub jego operatora, w drodze weryfikacji jego tożsamości 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 pod wnioskiem o certyfikat za pomocą klucza prywatnego odpowiadającego kluczowi publicznemu, który ma być certyfikowany.

3.2.2 Uwierzytelnienie tożsamości organizacji

Nie dotyczy

3.2.3 Identyfikacja osoby fizycznej

Bez uszczerbku dla odpowiedzialności CA, tożsamość posiadacza może zostać ustalona przez podmioty upoważnione do rozpoznawania, z wykorzystaniem następujących procedur:

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	Nie dotyczy

	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 wykonawczymi.	
3 SignID	● Urząd certyfikacji (CA) ● Punkt rejestracji (RA) ● Operator punktu rejestracji	Stosowanie 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
5 VideoID	● Urząd certyfikacji (CA) ● Punkt rejestracji (RA) ● Operator punktu rejestracji	Nie dotyczy

3.2.3.1 Rozpoznawanie wykonywane zgodnie z trybem 1 - LiveID

Tryb identyfikacji **LiveID** przewiduje osobiste spotkanie pełnoletniego posiadacza z jednym z podmiotów upoważnionych do rozpoznawania.
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[1].
W celu zagwarantowania jednoznacznej identyfikacji posiadacza i jego nazwy, musi on również posiadać unikalny kod identyfikacyjny, o którym mowa w pkt. 3.1.5. Podmiot uprawniony do rozpoznawania może zażądać okazania dokumentacji potwierdzającej posiadanie takiego unikalnego kodu identyfikacyjnego.
Punkty rejestracji działające za granicą, lub które w każdym razie identyfikują posiadaczów zamieszkujących 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.
Identyfikacji może również dokonać funkcjonariusz publiczny, zgodnie z przepisami regulującymi jego działalność. posiadacz wypełnia wniosek o wydanie certyfikatu i podpisuje go przed funkcjonariuszem publicznym, podpis zgodnie z obowiązującymi przepisami. Wniosek jest następnie składany do CA w jednym ze związanych umową punktów rejestracji.
Identyfikacja przeprowadzona przez pracodawcę w celu zawarcia umowy o pracę uznawana jest przez CA za ważną zgodnie z opisanym poniżej trybem rozpoznawania, po sprawdzeniu procedur operacyjnych w zakresie identyfikacji i uwierzytelniania. Podobnie uznawana jest za ważną, zgodnie z opisanym poniżej trybem rozpoznawania, identyfikacja przeprowadzona przez pracodawcę w

[1] 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.

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[2]. Wydane w ten sposób certyfikaty mogą być wykorzystywane wyłącznie do celów pracy, do 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 Rozpoznawanie wykonywane 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.
W kontekście włoskiego ustawodawstwa posiadacz podaje dane wykorzystywane do rozpoznawania w myśl dekretu legislacyjnego 231/2007 z późniejszymi zmianami i uzupełnieniami, zgodnie z którym klienci zobowiązani są do dostarczenia – na własną odpowiedzialność – wszelkich aktualnych informacji niezbędnych do zapewniania, aby adresaci obowiązków wywiązali się z obowiązków w zakresie identyfikacji klientów.
Ten tryb identyfikacji przewiduje udzielenie przez CA umocowania z prawem do reprezentacji podmiotowi podlegającemu obowiązkowi, który występuje zatem w charakterze punktu rejestracji. Dane identyfikacyjne posiadacza zebrane w momencie rozpoznania są zazwyczaj przechowywane przez CA w formie elektronicznej i mogą być również przechowywane w formie analogowej.

3.2.3.3 Rozpoznawanie wykonywane zgodnie z trybem 3 - SignID

W **trybie 3 – SignID** CA InfoCert opiera się na rozpoznaniu przeprowadzonym 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.

3.2.3.4 Rozpoznawanie wykonywane zgodnie z trybem 4 – AUTID

W **trybie 4 – AutID** CA opiera się na istniejącym środku identyfikacji elektronicznej:

- 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;

[2] CA przed udzieleniem umocowania przeprowadza dokładną ocenę bezpieczeństwa procedur identyfikacji pracownika oraz sposobu przydzielania narzędzi identyfikacji osobistej oraz zarządzania nimi w systemach informatycznych, do których pracownik (lub agent, lub emerytowany pracownik) ma dostęp w celu wnioskowania do CA o wydanie certyfikatu podpisu cyfrowego. Takie przypadki będą zgłaszane organowi nadzoru.

- 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.

Środki identyfikacji elektronicznej wykorzystywane przez CA i RA wymienione są na liście opublikowanej na stronie internetowej CA i zgłoszonej do AgID.
W kontekście włoskiego ustawodawstwa są to środki identyfikacji elektronicznej takie jak CNS (krajowa karta usług) lub TS-CNS (karta ubezpieczenia zdrowotnego – krajowa karta usług), CIE (elektroniczny dowód osobisty) oraz tożsamości wydane w kontekście systemu SPID.

W takich przypadkach dane rejestracyjne przechowywane są wyłącznie w formacie elektronicznym.

3.2.3.5 Rozpoznawanie wykonywane 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.
Odpowiednio przeszkolony operator punktu rejestracji weryfikuje tożsamość posiadacza lub wnioskodawcy w oparciu o jeden lub kilka ważnych dokumentów identyfikacyjnych z aktualnym i rozpoznawalnym zdjęciem, znajdujących się na liście akceptowanych dokumentów opublikowanej na stronie internetowej CA[3].

RA działające za granicą, lub w każdym razie identyfikujące posiadaczów zamieszkujących za granicą, mogą zostać upoważnione przez InfoCert do akceptowania dokumentów tożsamości wydanych przez organy państw należących do Unii Europejskiej, po uprzednim przeanalizowaniu dokumentów i ich obiektywnych cech gwarantujących pewność tożsamości i bezpieczeństwo w procesie wydawania dokumentów przez organy wydające, a także po przeprowadzeniu specjalnego szkolenia[4].
Operator punktu rejestracji może wykluczyć dopuszczalność dokumentu używanego przez posiadacza lub wnioskodawcę, jeżeli uzna, że dokument ten nie posiada wymienionych cech. Dane rejestracyjne, składające się z plików audio-video i ustrukturyzowanych metadanych w formacie elektronicznym, przechowywane są w bezpiecznej formie.

3.2.4 Identyfikacja osoby prawnej

Wniosek o wydanie certyfikatu dla osoby prawnej powinien zostać złożony przez osobę fizyczną, zidentyfikowaną w jednym z wyżej opisanych trybów (patrz pkt. 3.2.3).
Należy również przedłożyć dokumentację dotyczącą osoby prawnej oraz dokumentację potwierdzającą uprawnienia do złożenia wniosku w imieniu osoby prawnej.

[3] 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. Z uwagi na bezpieczeństwo i procedury dotyczące zwalczania nadużyć finansowych rodzaj dokumentów akceptowanych w tym trybie jest ograniczony do najbardziej powszechnych dokumentów tożsamości

[4] Takie przypadki będą zgłaszane organowi nadzoru.

3.2.5 Niezweryfikowane informacje dotyczące posiadacza lub wnioskodawcy

posiadacz może uzyskać, bezpośrednio lub za zgodą zainteresowanej strony trzeciej, włączenie do certyfikatu 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 uchwały nr 45 [9].

posiadacz zobowiązany jest przedstawić odpowiednie oświadczenie wykazujące rzeczywiste istnienie danej roli, w tym w drodze samocertyfikacji[5]. CA nie ponosi żadnej odpowiedzialności, z wyjątkiem przypadków zamierzonego działania lub niedbalstwa, za włączenie do certyfikatu informacji poświadczonych przez posiadacza w drodze samocertyfikacji.

Nazwa przedsiębiorstwa lub nazwa i kod identyfikacyjny **organizacji** zostaną natomiast wskazane w certyfikacie, jeśli upoważniła ona do wydanie certyfikatu posiadaczowi, nawet bez wyraźnego wskazania roli. W takim przypadku CA sprawdza formalną prawidłowość dokumentacji przedłożonej przez posiadacza. Wniosek o wydanie certyfikatu ze wskazaniem roli i/lub organizacji może złożyć wyłącznie organizacja posiadająca kod identyfikacji podatkowej lub NIP (VAT Code).

3.2.6 Walidacja wniosku

CA lub RA weryfikują informacje wymagane do celów identyfikacji, określone w punktach 3.2.3 i 3.2.4, oraz walidują wniosek.

3.3 Identyfikacja i uwierzytelnianie w celu odnowienia kluczy i certyfikatów

3.3.1 Identyfikacja i uwierzytelnianie w celu odnowienia kluczy i certyfikatów

Niniejszy punkt opisuje procedury stosowane do uwierzytelniania i identyfikacji posiadacza w przypadku odnowienia kwalifikowanego certyfikatu podpisu.

Certyfikat zawiera wskazanie okresu ważności w polu „termin ważności" (*validity*) z atrybutami „ważny od" (*not before*) i „ważny do" (*not after*). Poza tym zakresem dat, obejmującym godziny, minuty i sekundy, certyfikat jest 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 jest możliwe jego odnowienie, lecz wymagane jest jego nowe wydanie.

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

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 zamieszczenie 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 pkt. 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 wydawania certyfikatu lub za pomocą innego systemu uwierzytelniania opisanego w dokumentacji umownej dostarczonej w momencie rejestracji.

W przypadku wniosku składanego w punkcie rejestracji uwierzytelnienie posiadacza przeprowadza się zgodnie z procedurami 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, który wnosi 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 4.9.3.2 lub 4.9.15.2. CA zastrzega sobie prawo do określenia dodatkowych sposobów składania wniosku o unieważnienie lub zawieszenie certyfikatu przez wnioskodawcę lub zainteresowaną stronę trzecią w odpowiednich porozumieniach zawieranych z wnioskodawcą lub zainteresowaną stroną trzecią.

4 WYMAGANIA FUNKCJONALNE

4.1 Wnoszenie o wydanie certyfikatu

4.1.1 Kto może wnosić o wydanie certyfikatu?

O wydanie certyfikatu kwalifikowanego dla osoby fizycznej może wnosić:

- posiadacz,
  - zwracając się w tym celu bezpośrednio do CA za pośrednictwem strony www.firma.infocert.it, lub
  - zwracając się do punktu rejestracji;
- wnioskodawca w imieniu posiadacza,
  - zwracając się w tym celu bezpośrednio do CA za pośrednictwem strony www.firma.infocert.it, lub zawierając z CA odpowiednie porozumienie handlowe;
  - zwracając się do punktu rejestracji;

O wydanie certyfikatu kwalifikowanego dla osoby prawnej może wnosić:

- wnioskodawca reprezentujący osobę prawną,
  - zwracając się w tym celu bezpośrednio do CA za pośrednictwem strony www.firma.infocert.it, lub zawierając z CA odpowiednie porozumienie handlowe;
  - zwracając się do punktów rejestracji powołanych do 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. Czynności te niekoniecznie muszą odbywać się w tej kolejności.

Poszczególni uczestnicy procesu rejestracji 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 wnosi o wydanie kwalifikowanego certyfikatu;
- wnioskodawca (jeśli występuje) ma obowiązek poinformować posiadacza, w imieniu którego wnosi o wydanie certyfikatu, o obowiązkach z niego wynikających, dostarczyć prawidłowe oraz prawdziwe informacje dot. jego tożsamości, a także realizować procedury oraz wykonywać instrukcje CA i/lub RA;

- punkt rejestracji, jeśli występuje, w tym za pośrednictwem operatora punktu rejestracji, ma obowiązek jednoznacznie zidentyfikować posiadacza oraz wnioskodawcę, poinformować poszczególne podmioty o obowiązkach wynikających z posiadania certyfikatu, a także dokładnie realizować procedury wyznaczone przez CA;
- urząd certyfikacji jako ostatni jest odpowiedzialny za zidentyfikowanie posiadacza, a także za pozytywne zakończenie procesu rejestracji certyfikatu.

Gdy posiadaczem jest osoba prawna, a klucze generowane są przez urządzenie będące w jego posiadaniu, wnioskodawca zobowiązany jest do przesłania wniosku także w formacie PKCS#10 podpisanego przez samego wnioskodawcę.

4.2 Przetwarzanie wniosków

By uzyskać certyfikat podpisu, posiadacz i/lub wnioskodawca musi:

- zapoznać się z dokumentacją umowną oraz wszelką dokumentacją dodatkową;
- przejść procedury identyfikacji wdrożone przez urząd certyfikacji, zgodnie z opisem zawartym w niniejszym punkcie;
- przekazać informacje niezbędne do identyfikacji, uzupełnione – tam, gdzie jest to wymagane – 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 Informacje, które posiadacz zobowiązany jest dostarczyć

4.2.1.1 Osoba fizyczna

W związku z wnioskiem o wydanie kwalifikowanego certyfikatu podpisu, posiadacz lub wnioskodawca wnioskujący o wydanie certyfikatu dla osoby fizycznej, zobowiązany jest podać poniższe informacje:

- nazwisko i imię;
- datę i miejsce urodzenia;
- kod TIN (we Włoszech kod identyfikacji podatkowej) lub, w przypadku jego braku, inny analogiczny kod identyfikujący osobę, jak np. numer dokumentu tożsamości;
- dane dokumentu tożsamości podanego do identyfikacji, tj. rodzaj, numer, nazwę organu wydającego oraz datę jego wystawienia;
- przynajmniej jedną z poniższych informacji kontaktowych służących CA do przesyłania wiadomości posiadaczowi:
  - adres zamieszkania;
  - adres e-mail;
- numer telefonu komórkowego do przesyłania haseł OTP, jeśli to właśnie ta technologia miałaby być stosowana.

Opcjonalnie posiadacz (lub wnioskodawca) może podać także inną nazwę, pod którą jest powszechnie znany, a która to nazwa zostanie wprowadzona do odpowiedniego pola o nazwie commonName (nazwa powszechnie znana) w SubjectDN certyfikatu. W przypadku gdy nie podano

dodatkowej nazwy posiadacza lub wnioskodawcy 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, będący w osobie jej prawnym przedstawicielem lub osobą fizyczną działającą na podstawie odpowiedniego pełnomocnictwa, musi dostarczyć następujące informacje:

- nazwisko i imię wnioskodawcy;
- kod TIN lub inny analogiczny kod identyfikujący wnioskodawcę (we Włoszech kod identyfikacji podatkowej);
- dane dokumentu tożsamości podanego w celu identyfikacji wnioskodawcy, tj. rodzaj, numer, nazwę organu wydającego oraz datę jego wydania;
- adres e-mail służący CA do przesyłania wiadomości wnioskodawcy;
- nazwę posiadacza będącego osobą prawną;
- VAT lub też NTR (nr NIP lub numer w Rejestrze Przedsiębiorstw w przypadku podmiotów włoskich).

Opcjonalnie wnioskodawca może podać inną nazwę, pod którą podmiot prawny jest powszechnie znany, a która to nazwa zostanie wprowadzona do odpowiedniego pola o nazwie commonName (nazwa powszechnie znana) w SubjectDN certyfikatu.
Gdyby osoba prawna chciała uzyskać certyfikat dla własnych par kluczy, wnioskodawca zobowiązany jest do dostarczeni pliku w formacie PKCS#10 zawierającego wniosek podpisany przez wnioskodawcę.
Przekazane informacje zapisywane są w archiwach CA (etap rejestracji) i stanowić będą podstawę do wygenerowania certyfikatu kwalifikowanego.

4.2.2 Przeprowadzanie identyfikacji i uwierzytelniania

W początkowej fazie rejestracji oraz przyjmowania wniosku o rejestrację i wydanie certyfikatu posiadaczowi lub wnioskodawcy, będącemu prawnym przedstawicielem osoby prawnej, przekazane zostają kody bezpieczeństwa umożliwiające aktywację urządzenia do składania podpisu lub uruchomienie procedury podpisu, jeśli ta następuje zdalnie, i/lub złożenie ewentualnego wniosku o zawieszenie certyfikatu (kod ERC lub inny analogiczny, jeśli tak przewidują zapisy umowy). Kody bezpieczeństwa dostarczane są w zaciemnionej kopercie lub, jeśli następuje to drogą elektroniczną, w zaszyfrowanych plikach.
CA może postanowić, aby posiadacz lub wnioskodawca będący prawnym przedstawicielem osoby prawnej sam wybierał kod PIN potrzebny do podpisu. W takich przypadkach obowiązek zapamiętania PIN-u leży po stronie posiadacza lub wnioskodawcy.
CA może także postanowić o stosowaniu certyfikatu podpisu w procedurze zdalnej za pośrednictwem systemu uwierzytelniania oferowanego przez RA, którego poziom bezpieczeństwa jest co najmniej średni, lub który jest oferowany w ramach certyfikacji bezpiecznego urządzenia do składania podpisu, po wcześniejszym przeanalizowaniu jego cech.

4.2.3 Przyjęcie lub odrzucenie wniosku o wydanie certyfikatu

Po wstępnej rejestracji CA lub RA może odmówić wydania certyfikatu podpisu w przypadku stwierdzenia braku lub niekompletności informacji, negatywnego wyniku kontroli spójności

przekazanych informacji lub kontroli pod kątem zwalczania nadużyć finansowych, wątpliwości co do tożsamości posiadacza lub wnioskodawcy itd.

4.2.4 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 zostaje wygenerowana 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 weryfikuje ważność podpisu na PKCS#10 oraz prawo podmiotu do przesłania wniosku, a także generuje certyfikat kwalifikowany, który następnie zostaje przesłany bezpiecznym kanałem do urządzenia.

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 zostaje wygenerowana przez RA bezpośrednio na HSM; to oznacza, iż RA przesyła do CA wniosek o wydanie certyfikatu klucza publicznego w formacie PKCS#10, podpisany elektronicznie przy użyciu specjalnie do tego celu wygenerowanego kwalifikowanego certyfikatu podpisu dla procedury automatycznej.

CA weryfikuje ważność podpisu na PKCS#10 oraz prawo podmiotu do przesłania wniosku, a także generuje certyfikat kwalifikowany, który następnie zostaje zapisany w HSM.

4.3.1.3 Wystawienie certyfikatu przy użyciu systemu Card Management System

Para kluczy kryptograficznych zostaje wygenerowana 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 weryfikuje ważność podpisu na PKCS#10 oraz prawo podmiotu do przesłania wniosku, a także generuje certyfikat kwalifikowany, który następnie zostaje przesłany bezpiecznym kanałem do urządzenia.

4.3.1.4 Wystawienie certyfikatu dla osoby prawnej

Para kluczy kryptograficznych zostaje wygenerowana przez RA bezpośrednio na HSM; to oznacza, iż RA przesyła do CA wniosek o wydanie certyfikatu klucza publicznego w formacie PKCS#10, podpisany elektronicznie przy użyciu specjalnie do tego celu wygenerowanego kwalifikowanego certyfikatu podpisu dla procedury automatycznej.

CA weryfikuje ważność podpisu na PKCS#10 oraz prawo podmiotu do przesłania wniosku, a także generuje certyfikat kwalifikowany, który następnie zostaje zapisany w HSM.

W przypadku, gdy para kluczy generowana jest w sprzętowym module bezpieczeństwa HSM posiadacza, posiadacz zobowiązany jest do przesłania podpisanego PKCS#10, a CA, po zweryfikowaniu ważności podpisu na PKCS#10 oraz prawa podmiotu do przesłania wniosku, generuje certyfikat kwalifikowany, który następnie zostaje zapisany w HSM.

4.3.2 Zawiadomienie wnioskodawców o wystawieniu certyfikatu

W przypadku certyfikatu wystawianego na urządzeniu kryptograficznym posiadacz (lub wnioskodawca) nie potrzebuje specjalnego zawiadomienia, ponieważ certyfikat dostępny jest na otrzymanym przez niego urządzeniu. W pozostałych przypadkach zawiadomienie zostaje przesłane na adres mailowy podany w chwili rejestracji.

4.3.3 Aktywacja

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

Po otrzymaniu urządzenia posiadacz, wykorzystując otrzymane poufnie kody aktywacyjne, a także stosowne oprogramowanie udostępnione przez CA, przechodzi do aktywacji urządzenia, wybierając równocześnie PIN podpisu oraz zastrzeżony limit bezpieczeństwa, których to przechowywanie oraz ochrona leży wyłącznie w gestii posiadacza.

4.3.3.2 Aktywacja urządzenia do zdalnego składania podpisu (HSM)

posiadacz, a w przypadku osób prawnych wnioskodawca, którego dostęp do portali CA został uwierzytelniony przy użyciu otrzymanych poufnie kodów aktywacyjnych, wybiera PIN podpisu oraz zastrzeżony limit bezpieczeństwa, których to przechowywanie oraz ochrona leży wyłącznie w gestii samego posiadacza, co zostaje potwierdzone wprowadzeniem OneTime Password otrzymanym SMS-em lub też wygenerowanym przez token lub aplikację token-app przypisaną do certyfikatu.
W niektórych przypadkach wystawiony certyfikat jest już aktywny i gotowy do użycia.

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 certyfikacyjnej, certyfikat zostaje wprowadzony do odpowiedniego rejestru certyfikatów, bez podawania go do publicznej wiadomości. Podmiot zainteresowany jego upublicznieniem może się o to zwrócić, podejmując kroki opisane w pkt. 0. Wniosek zostanie przetworzony w ciągu 3 dni roboczych.

4.4.3 Zawiadomienie wnioskodawców o upublicznieniu certyfikatu

Nie dotyczy

4.5 Korzystanie z pary kluczy oraz certyfikatu

4.5.1 Korzystanie z prywatnego klucza oraz certyfikatu przez posiadacza

posiadacz zobowiązany jest do bezpiecznego przechowywania urządzenia do składania podpisu lub innych narzędzi uwierzytelniających zdalny podpis; zobowiązany jest także do przechowywania informacji umożliwiających użycie prywatnego klucza z dala od samego urządzenia. Musi on zachować w tajemnicy oraz chronić przed dostępem osób trzecich kod awaryjny służący zawieszeniu certyfikatu; wolno mu korzystać z certyfikatu tylko do celów opisanych w Polityce oraz zgodnie z obowiązującymi, krajowymi oraz międzynarodowymi, przepisami prawa.
Nie wolno składać podpisów elektronicznych, korzystając z prywatnych kluczy, dla których unieważniono lub zawieszono certyfikat, ani też składać podpisów elektronicznych, korzystając z certyfikatu wydanego przez CA, któremu cofnięto uprawnienia.

4.5.2 Korzystanie z publicznego klucza oraz certyfikatu przez użytkowników końcowych

Użytkownik końcowy musi zapoznać się z zakresem stosowania certyfikatu opisanym w Polityce oraz w samym certyfikacie. Zobowiązany jest także do zweryfikowania ważności certyfikatu przez skorzystaniem z zawartego w nim klucza publicznego, a także do zweryfikowania, czy dany certyfikat nie został zawieszony lub unieważniony, kontrolując w tym celu zapisy odpowiednich rejestrów; zobowiązany jest także do zweryfikowania istnienia oraz zakresu ewentualnych ograniczeń w stosowaniu pary kluczy, uprawnień do reprezentacji oraz uprawnień zawodowych.

4.5.3 Ograniczenia w stosowaniu oraz limity kwotowe

Kwalifikowane certyfikaty do składania podpisów w procedurze automatycznej zawierają ograniczenia w ich stosowaniu ustalone przez organy nadzoru, jako dodatkowe Certificate Policy,

oznaczone poniższymi OID:

1.3.76.36.1.1.24.1	Niniejszy certyfikat jest ważny jedynie dla podpisów składanych w procedurze automatycznej. Niniejsza deklaracja stanowi dowód zastosowania tejże procedury dla podpisanych dokumentów.
1.3.76.36.1.1.24.2	The certificate may be used only for automatic procedure signature purposes
1.3.76.36.1.1.23	Posiadacze certyfikatu korzystają z certyfikatu tylko do celów służbowych, dla których dany certyfikat został wystawiony. The certificate holder must use the certificate only for the purposes for which it is issued.
1.3.76.36.1.1.25	„Korzystanie z certyfikatu ograniczone jest do kontaktów z" w dalszej części nazwa podmiotu, w kontaktach z którym certyfikat może być stosowany. "The certificate may be used only for relations with the" followed by the name of the subject with which the certificate can be used.

Certyfikaty wystawione na podstawie identyfikacji typu 4-AutID, z wykorzystaniem tożsamości cyfrowych SPID, zawierają następujące ograniczenie ich stosowania:

- Certyfikat wystawiony za pomocą danych do logowania SPID nie może być stosowany do wnioskowania o cyfrowe tożsamości. Certificate issued through SPID digital identity, not usable to require digital identity

Ponadto posiadacz lub wnioskodawca mają prawo zwrócić się do urzędu certyfikacji o wprowadzenie indywidualnych ograniczeń stosowania certyfikatu. Wniosek o wprowadzenie innych, szczególnych ograniczeń w stosowaniu certyfikatu analizowany jest przez CA pod kątem prawnym, technicznym oraz ze względu na ich interoperacyjność, a następnie rozpatrywany zgodnie z przeprowadzoną analizą.

posiadacz ma prawo zwrócić się do CA także o wprowadzenie limitów kwotowych odnoszących się do wartości aktów jednostronnych oraz umów, do których certyfikat może być stosowany. Podane wartości należy wyrazić pełnymi dodatnimi kwotami, bez miejsc po przecinku.

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.

Z zastrzeżeniem odpowiedzialności CA, o której mowa w CAD (art. 30), za zweryfikowanie ograniczeń dot. korzystania z certyfikatu oraz limitów kwotowych z nim związanych odpowiedzialny jest użytkownik.

4.6 Odnowienie certyfikatu

4.6.1 Przyczyny odnowienia

Odnowienie certyfikatu umożliwia otrzymanie nowego certyfikatu podpisu do podpisywania dokumentów oraz zawierania transakcji.

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 dany certyfikat nie został unieważniony oraz pod warunkiem, iż wszystkie informacje podane w momencie jego poprzedniego wystawiania są wciąż aktualne. Odnowienie certyfikatu nie jest możliwe po upływie terminu jego ważności; w takiej sytuacji konieczne jest złożenie wniosku o wydanie nowego certyfikatu.
Procedura odnowienia certyfikatu stosowana jest wyłącznie dla certyfikatów wystawianych przez InfoCert.
Odnowienie certyfikatu stosowanego do podpisu automatycznego nie jest możliwe; w takiej sytuacji konieczne jest złożenie wniosku o wydanie nowego certyfikatu.
Odnowienie certyfikatu wystawionego dla osoby prawnej nie jest możliwe; w takiej sytuacji konieczne jest złożenie wniosku o wydanie nowego certyfikatu.

4.6.3 Przetwarzanie wniosku o odnowienie certyfikatu

Odnowienie certyfikatu następuje przy użyciu funkcji udostępnionej przez CA w ramach kontaktów handlowych oraz na warunkach wynikających z umowy z posiadaczem oraz RA (jeśli dotyczy).

4.7 Ponowne wystawienie certyfikatu

Nie dotyczy

4.8 Zmiany certyfikatu

Nie dotyczy

4.9 Unieważnienie oraz zawieszenie certyfikatu

Unieważnienie lub zawieszenie certyfikatu powoduje wygaśnięcie ustalonego terminu ważności certyfikatu oraz sprawia, iż nieważne stają się podpisy złożone po opublikowaniu informacji o jego unieważnieniu. Unieważnione lub zawieszone certyfikaty wpisywane są na listę unieważnionych i zawieszonych certyfikatów (CRL) podpisaną przez CA, który je wystawił, oraz publikowaną w rejestrze certyfikatów z wcześniej ustaloną częstotliwością. W szczególnych okolicznościach CA może nalegać na nieplanowane opublikowanie CRL. Unieważnienie lub zawieszenie certyfikatu staje się skuteczne w chwili opublikowania listy, tj. z datą rejestracji zdarzenia w dzienniku kontrolnym prowadzonym przez urząd certyfikacjidany Certification Authority.

4.9.1 Przyczyny unieważnienia

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

1. naruszony został prywatny klucz, tj. wystąpił jeden z poniższych przypadków:
   - zagubione zostało bezpieczne urządzenie do składania podpisu zawierające klucz;
   - naruszona została poufność klucza lub jego kodu aktywacyjnego (PIN) lub też, w przypadku certyfikatów do podpisu zdalnego, zostało naruszone lub zgubione urządzenie OTP;
   - miało miejsce 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 dot. roli, w zakresie powodującym, iż powyższe dane przestały być poprawne i/lub prawdziwe;
4. zakończeniu uległy stosunki między posiadaczem a CA lub między wnioskodawcą a CA;
5. doszło do istotnego naruszenia niniejszej Polityki.

4.9.2 Kto może zwrócić się o unieważnienie certyfikatu?

O unieważnienie certyfikatu, z jakiegokolwiek powodu i w jakimkolwiek momencie, może zwrócić się sam posiadacz. Ponadto wniosek o unieważnienie certyfikatu może złożyć także wnioskodawca, z powodów oraz w trybie ustalonym w niniejszej Polityce. Certyfikat może zostać unieważniony również z urzędu przez CA.

4.9.3 Procedury dot. wnioskowania o unieważnienie certyfikatu

Wniosek o unieważnienie należy złożyć na zasadach przewidzianych dla podmiotu, który go składa.

4.9.3.1 Unieważnienie wnioskowane przez posiadacza

posiadacz zobowiązany jest do podpisania wniosku o unieważnienie z wykorzystaniem formularza dostępnego na stronie internetowej InfoCert, przekazując go do RA lub przesyłając bezpośrednio do CA listem poleconym, certyfikowaną pocztą elektroniczną lub faksem, wraz z fotokopią ważnego dokumentu tożsamości.

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

Jeśli certyfikat będący przedmiotem wniosku o unieważnienie zawiera informacje dot. roli posiadacza, CA podejmie kroki mające na celu poinformowanie o dokonaniu unieważnienia certyfikatu ewentualnej zainteresowanej strony trzeciej, na zasadach określonych w zawartych z tą stroną porozumieniach. Jeśli certyfikat będący przedmiotem wniosku o unieważnienie zawiera dane organizacji, CA podejmie kroki mające na celu poinformowanie tego podmiotu o dokonaniu unieważnienia.

4.9.3.2 Unieważnienie wnioskowane przez wnioskodawcę lub zainteresowaną stronę trzecią

Wnioskodawca może zwrócić się o unieważnienie certyfikatu posiadacza, wypełniając odpowiedni

formularz dostępny na stronie internetowej CA oraz w placówkach RA, podając uzasadnienie swojego wniosku, a także załączając odpowiednią dokumentację (jeśli istnieje) oraz podając dane posiadacza przekazane CA w momencie wystawiania certyfikatu. Wniosek należy złożyć pisemnie.

CA lub RA weryfikuje autentyczność wniosku, tak aby CA mogło podjąć kroki zmierzające do unieważnienia certyfikatu, a następnie poinformować o tym fakcie posiadacza, korzystając w tym celu z narzędzi komunikacji ustalonych w chwili wnoszenia o wydanie certyfikatu.

Dodatkowe zasady dot. wniosku o unieważnienie certyfikatu składanego przez wnioskodawcę lub zainteresowaną stronę trzecią będzie można ustalić w ramach ewentualnych dodatkowych porozumień zawieranych z CA.

4.9.3.3 Unieważnienie certyfikatu z inicjatywy urzędu certyfikacji

W przypadku zaistnienia takiej konieczności CA ma prawo unieważnić certyfikat, uprzedzając o tym fakcie posiadacza, podając uzasadnienie unieważnienia, a także datę i godzinę, kiedy to nastąpi.

Jeśli certyfikat będący przedmiotem unieważnienia zawiera informacje dot. roli posiadacza, CA podejmie kroki mające na celu poinformowanie o dokonaniu unieważnienia certyfikatu ewentualną zainteresowaną stronę trzecią, na zasadach określonych w zawartych z tą stroną porozumieniach. Jeśli certyfikat będący przedmiotem wniosku o unieważnienie zawiera dane organizacji, CA podejmie kroki mające na celu poinformowanie tego podmiotu o dokonaniu unieważnienia.

4.9.4 Okres karencji dla wniosku o unieważnienie

Okres karencji listy CRL obejmuje czas pomiędzy opublikowaniem przez CA kolejnej listy CRL, a terminem obowiązywania tej bieżącej. W celu uniknięcia utrudnień dla którejkolwiek ze stron, okres ten jest dłuższy od czasu, jaki CA potrzebuje na wygenerowanie oraz opublikowanie nowej listy CRL. W ten sposób bieżąca CRL obowiązuje przynajmniej do chwili zastąpienia jej przez nową CRL.

4.9.5 Maksymalny czas przetwarzania wniosku o unieważnienie certyfikatu

Wniosek zostaje przetworzony w ciągu godziny, chyba że istnieje konieczność przeprowadzenia dodatkowych kontroli jego autentyczności. Jeśli wniosek zostaje prawidłowo uwierzytelniony, zostaje on natychmiast przetworzony. W przeciwnym razie podjęte zostają kroki zmierzające do zawieszania certyfikatu w oczekiwaniu na wynik dodatkowych kontroli dot. autentyczności otrzymanego wniosku.

4.9.6 Wymagania dot. 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 oraz publikowaną w publicznym rejestrze. CRL publikowana jest regularnie co godzinę (emisja zwyczajna). W szczególnych przypadkach CA może nalegać na nieplanowane opublikowanie CRL (natychmiastowa nadzwyczajna emisja), np. gdy unieważnienie

lub zawieszenie certyfikatu następuje w wyniku podejrzenia naruszenia tajemnicy prywatnego klucza (natychmiastowe unieważnienie lub zawieszenie). CRL publikowana jest zawsze w całości. Za moment publikacji listy CRL uznaje się datę podawaną przez system Time Stamping Authority InfoCert. Taki zapis zostaje umieszczony w dzienniku kontrolnym. Każdy element listy CRL zawiera datę i godzinę unieważnienia lub zawieszenia podane w odpowiednim rozszerzeniu. CA – w celu odciążenia sieci – zastrzega sobie prawo do odrębnego publikowania innych list CRL stanowiących podzbiory głównej listy. Uzyskanie listy CRL i zapoznanie się z nią leży w gestii użytkowników. Lista CRL, z którą należy się zapoznać w związku z konkretnym certyfikatem, wskazana jest w, samym certyfikacie zgodnie z obowiązującymi przepisami prawa.

4.9.8 Maksymalne opóźnienie CRL

Czas oczekiwania pomiędzy złożeniem wniosku o unieważnienie lub zawieszenie certyfikatu a jego realizacją poprzez opublikowanie certyfikatu na liście CRL wynosi maksymalnie 1 godzinę.

4.9.9 Kontrola online statusu wniosku o unieważnienie certyfikatu

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

4.9.10 Wymagania dla kontroli online

Patrz załącznik B

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. złożony został wniosek o unieważnienie certyfikatu bez możliwości zweryfikowania w szybkim czasie jego autentyczności;
2. posiadacz, wnioskodawca lub zainteresowana strona trzecia, RA lub CA weszli w posiadanie elementów rodzących wątpliwości dot. ważności certyfikatu;
3. pojawiły się wątpliwości dot. bezpieczeństwa urządzenia OTP (jeśli dotyczy);
4. konieczne jest tymczasowe przerwanie ważności certyfikatu.

W powyższych przypadkach wnioskuje się o zawieszenie certyfikatu, podając czas, na jaki ma on zostać zawieszony. Po upływie okresu zawieszenia nastąpi albo ostateczne unieważnienie certyfikatu albo przywrócenie jego ważności.

4.9.14 Kto może zwrócić się o zawieszenie certyfikatu?

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

4.9.15 Procedury dot. wnioskowania o zawieszenie certyfikatu

Wniosek o zawieszenie należy złożyć na zasadach przewidzianych dla podmiotu, który go składa. Zawieszenie certyfikatu jest zawsze ograniczone w czasie. Zawieszenie upływa o godzinie 24:00:00 ostatniego dnia wnioskowanego okresu.

4.9.15.1 Zawieszenie certyfikatu wnioskowane przez posiadacza

posiadacz zobowiązany jest do złożenia wniosku o zawieszenie w jednym z poniższych trybów:

1. korzystając z funkcji zawieszenia certyfikatu dostępnej na stronie internetowej CA, wypełniając dane oraz wykorzystując kod awaryjny podany w momencie wystawiania certyfikatu;
2. korzystając z funkcji zawieszenia certyfikatu przy użyciu OTP dostępnej na stronie internetowej podanej w dokumentacji umownej dostarczonej w chwili rejestracji (jeśli dostępna);
3. dzwoniąc do call center danego CA i podając wymagane informacje. W przypadku braku kodu awaryjnego oraz tylko wówczas, gdy przyczyną wnioskowania o zawieszenie certyfikatu jest naruszenie tajemnicy klucza, call center – zweryfikowawszy numer telefonu osoby dzwoniącej – 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;
4. za pośrednictwem punktu rejestracji, który prosi o podanie wymaganych danych oraz przeprowadza niezbędne kontrole, na koniec zwracając się o zawieszenie certyfikatu do CA. posiadacz zobowiązany jest do podpisania wniosku o zawieszenie certyfikatu oraz o dostarczenie go do placówki RA lub przesłanie go bezpośrednio do CA listem zwykłym, certyfikowaną pocztą elektroniczną lub faksem, wraz z fotokopią ważnego dokumentu tożsamości;
5. korzystając z funkcji zawieszenia dostępnej na stronie internetowej RA, stanowiącej interfejs z usługami CMS.

Jeśli certyfikat będący przedmiotem wniosku o zawieszenie zawiera informacje dot. roli posiadacza, CA podejmie kroki mające na celu poinformowanie o zawieszeniu certyfikatu ewentualnej zainteresowanej strony trzeciej, na zasadach określonych w zawartych z tą stroną porozumieniach. Jeśli certyfikat będący przedmiotem wniosku o zawieszenie certyfikatu zawiera dane organizacji, CA podejmie kroki mające na celu poinformowanie tego podmiotu o dokonanym zawieszeniu.

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 placówkach RA, podając uzasadnienie swojego wniosku, a także załączając odpowiednią dokumentację (jeśli istnieje) oraz podając dane posiadacza przekazane CA w chwili wystawiania certyfikatu.

CA weryfikuje autentyczność wniosku oraz informuje o tym fakcie posiadacza, korzystając z narzędzi komunikacji podanych w chwili składania wniosku o wydanie certyfikatu, a następnie przystępuje do jego zawieszenia. Dodatkowe zasady dot. wniosku o zawieszenie certyfikatu składanego przez wnioskodawcę lub zainteresowaną stronę trzecią będzie można ustalić w ramach ewentualnych dodatkowych porozumień z CA.

4.9.15.3 Zawieszenie z inicjatywy CA

CA, z wyjątkiem pilnych przypadków, uprzedza posiadacza o zamiarze zawieszenia certyfikatu, podając powód jego zawieszenia, a także datę rozpoczęcia okresu zawieszenia oraz datę jego zakończenia. W każdym przypadku informacje dot. okresu zawieszenia zostają przekazane posiadaczowi w możliwie najkrótszym czasie.
Jeśli certyfikat będący przedmiotem zawieszenia zawiera informacje dot. roli posiadacza, CA podejmie kroki mające na celu poinformowanie o zawieszeniu certyfikatu ewentualnej zainteresowanej strony trzeciej, na zasadach określonych w zawartych z tą stroną porozumieniach.
Jeśli certyfikat będący przedmiotem zawieszenia zawiera dane organizacji, CA podejmie kroki mające na celu poinformowanie tego podmiotu o dokonanym zawieszeniu.

4.9.16 Ograniczenia czasowe dot. okresu zawieszenia certyfikatu

Po upływie wnioskowanego okresu zawieszenia ważność certyfikatu zostaje przywrócona poprzez usunięcie certyfikatu z listy unieważnionych i zawieszonych certyfikatów (CRL). Przywrócenie certyfikatu następuje w ciągu 24 godzin po upływie okresu zawieszenia. Jeśli dzień kończący okres zawieszenia zbiega się z dniem ustania ważności certyfikatu lub z dniem następującym po tym dniu, zawieszenie zostaje przekształcone w unieważnienie obowiązujące od początku okresu zawieszenia.

Możliwe jest zwrócenie się o przywrócenie certyfikatu przed datą zakończenia okresu jego zawieszenia, przesyłając w tym celu podpisany formularz, dostępny na stronie internetowej InfoCert, wraz z kopią dokumentu tożsamości. Wniosek ten może zostać przesłany certyfikowaną pocztą elektroniczną lub faksem.

Jeśli certyfikat został zawieszony przy użyciu CMS, można go przywrócić za pomocą funkcji dostępnej na stronie internetowej stanowiącej interfejs z usługami CMS

4.10 Usługi dot. statusu certyfikatu

4.10.1 Cechy funkcjonowania

Informacje na temat statusu certyfikatu dostępne są za pośrednictwem listy CRL lub usługi OCSP. Numer seryjny unieważnionego certyfikatu pozostaje na liście CRL także po zakończeniu okresu ważności certyfikatu, a przynajmniej do czasu ważności certyfikatu CA.
Informacje przekazywane przez usługę OCSP dot. certyfikatów są aktualizowane zgodnie z treścią ostatniej opublikowanej listy CRL.

4.10.2 Dostępność usługi

Usługa OCSP oraz listy CRL dostępne są 24 h na dobę przez 7 dni w tygodniu.

4.10.3 Cechy opcjonalne

Nie dotyczy

4.11 Rezygnacja z usług oferowanych przez CA

Stosunek prawny pomiędzy posiadaczem i/lub wnioskodawcą a urzędem certyfikacji kończy się w chwili zakończenia okresu ważności certyfikatu lub w chwili jego unieważnienia, z wyjątkiem szczególnych przypadków wynikających z zapisów umowy.

4.12 Deponowanie i odtwarzanie klucza

Nie dotyczy

5 ŚRODKI BEZPIECZEŃSTWA I KONTROLI

TSP InfoCert zrealizował serię zabezpieczeń chroniących system informatyczny dostarczający usługi cyfrowej certyfikacji. Wdrożony system zabezpieczeń obejmuje 3 poziomy:

- poziom fizyczny, mający na celu zabezpieczenie środowiska, w którym CA świadczy usługę;
- poziom proceduralny dot. kwestii typowo organizacyjnych;
- poziom logiczny dot. zastosowania sprzętu i oprogramowania służącego rozwiązywaniu problemów i przeciwdziałaniu zagrożeniom związanym z rodzajem świadczonej usługi oraz wykorzystywaną infrastrukturą.

Wspomniany system bezpieczeństwa ma za zadanie unikanie zagrożeń wynikających z awarii systemów, sieci oraz aplikacji, a także z nieupoważnionego przechwytywania lub modyfikacji danych.

Wyciąg z polityki bezpieczeństwa stosowanej przez InfoCert udostępniany jest na wniosek, który należy wysłać na adres certyfikowanej poczty elektronicznej infocert@legalmail.it.

5.1 Bezpieczeństwo fizyczne

Zastosowane środki bezpieczeństwa obejmują swoim zakresem:

- właściwości budynku oraz konstrukcji;
- czynne i bierne systemy antywłamaniowe;
- kontrolę dostępów fizycznych;
- zasilanie elektryczne oraz klimatyzację;
- ochronę przeciwpożarową;
- ochronę przeciwpowodziową,
- sposoby archiwizowania nośników magnetycznych;
- miejsca archiwizowania nośników magnetycznych.

5.1.1 Lokalizacja oraz rozwiązania konstrukcyjne

Data Center InfoCert znajduje się w siedzibie w Padwie. Disaster Recovery zlokalizowane jest w Modenie i jest połączone ze wspomnianym wyżej Data Center InfoCert specjalnym nadmiarowym łączem opartym na dwóch odrębnych sieciach MPLS z prędkością transferu danych 10 Gbit/s z możliwością upgrade'u do 100 Gbit/s.

W obu miejscach wyodrębnione zostały pomieszczenia dysponujące najwyższym poziomem zabezpieczeń, fizycznych i logicznych, wewnątrz których znajduje się certyfikowany sprzęt informatyczny stanowiący serce cyfrowej certyfikacji, czasowego znakowania oraz zdalnego i automatycznego podpisu.

KOD DOKUMENTU	ICERT-INDI-MO
WERSJA	3.4
DATA	20.06.2018 r.

Ilustracja 1 – lokalizacja Data Center InfoCert oraz siedziba DisasterRecovery

5.1.2 Dostęp fizyczny

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

5.1.3 Instalacja elektryczna i klimatyzacja

Budynek, w którym mieści się Data Center InfoCert w Padwie, pomimo braku certyfikatu, spełnia kryteria wymagane dla Data Center z certyfikatem Tier III.

Pomieszczenia techniczne wyposażone są w system zasilania elektrycznego zaprojektowany tak, by zapobiegać awariom, a przede wszystkim przerwom w świadczeniu usług. Zasilanie systemów oparte jest na najnowocześniejszych rozwiązaniach technologicznych, zwiększających niezawodność oraz gwarantujących rezerwę mocy dla realizacji najbardziej kluczowych funkcji pełnionych w związku ze świadczonymi usługami.

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 oraz synchronizacji pracy poszczególnych generatorów, sieci oraz akumulatorów (STS).

Każda szafa sterująca zainstalowana w Data Center korzysta z dwóch linii elektrycznych, zapewniających utrzymanie wysokiej dostępności (HA) w przypadku przerwy w działaniu jednej z linii.

Praca szafy sterującej jest zdalnie monitorowana; prowadzone są także stałe kontrole stanu linii elektrycznej (on/off), a także pobieranej mocy (obciążenie żadnej z linii nie powinno przekraczać 50%).

Temperatura w pomieszczeniach technicznych utrzymywana jest pomiędzy 20°C a 27°C, przy wilgotności względnej od 30 do 60%. Instalacje wyposażone są w skraplacze z zamkniętym systemem zbierania 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 obciążeniu 10 kW dla szafy pojedynczej oraz maksymalnie 15 kW przy dwóch połączonych szafach.

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, tj. pomieszczeń mieszczących 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, którego pracą kieruje centrala analogowa adresowalna NOTIFIER z czujnikami optycznymi rozmieszczonymi w pomieszczeniach i w podwieszanym suficie oraz czujniki z systemem pobierania próbek powietrza zainstalowane pod podłogą oraz w przewodach wentylacyjnych.
System automatycznego wykrywania pożarów połączony jest z instalacją automatycznego gaszenia przy użyciu ekologicznych gazów gaśniczych NAFS125 i PF23, a w niektórych pomieszczeniach, z systemami gaszenia aerozolem.
Użycie substancji gaszącej w danej strefie następuje w momencie równoczesnego zadziałania dwóch detektorów.
Dla każdej strefy pożarowej przewidziana jest jedna instalacja gaszenia.
Zgodnie z obowiązującymi przepisami prawa w obiekcie znajdują się także przenośne urządzenia gaśnicze.

Przewody powietrza pierwotnego służące pomieszczeniom ze sprzętem wyposażone są, zgodnie z podziałem na strefy pożarowe, w klapy przeciwpożarowe uruchamiane przez system automatycznego wykrywania pożarów.

5.1.6 Nośniki pamięci

Jeśli chodzi o platformę storage, wybrane rozwiązanie zakłada stosowanie dla części NAS systemów NetApp (FAS 8060). Dla części SAN wdrożono natomiast infrastrukturę opartą na technologiach EMC2 obejmujących VNX 7600, VNX 5200 i XtremIO i zarządzanych przez warstwę wirtualizacji storage VPLEX. Zarządzanie tą infrastrukturą odbywa się za pośrednictwem ViPR.

5.1.7 Utylizacja odpadów

InfoCert posiada certyfikat ISO 14001 zakładający zrównoważone zarządzanie środowiskiem w ramach własnego cyklu produkcyjnego, w tym segregację odpadów oraz ich zrównoważoną utylizację. Jeśli chodzi o odpady elektroniczne, wszystkie urządzenia przed likwidacją zostają oczyszczone zgodnie z przewidzianymi procedurami lub też przekazane w tym celu do autoryzowanych firm dezynfekcyjnych.

5.1.8 Off-site backup

Off-site backup wykonywany jest w siedzibie Disaster Recovery, przy użyciu EMC Data Domain 4200, na którym główny Data Domain siedziby w Padwie tworzy zapasowe kopie danych.

5.2 Kontrole proceduralne

5.2.1 Kluczowe role

Kluczowe role pełnią osoby spełniające niezbędne wymagania dot. doświadczenia, profesjonalizmu oraz przygotowania technicznego i prawniczego, które to cechy są stale weryfikowane w ramach prowadzonych ocen rocznych.
Lista nazwisk wraz ze schematem organizacyjnym osób pełniących kluczowe role przekazana została do AgID przy okazji pierwszej akredytacji i jest stale aktualizowana, tak by odzwierciedlała naturalne zmiany zachodzące w strukturze przedsiębiorstwa.

5.3 Kontrola personelu

5.3.1 Kwalifikacje, doświadczenie oraz wymagane zezwolenia

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

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 oraz testy.

5.3.3 Wymagania dot. przygotowania

W celu ochrony przed naruszeniem lub zakłóceniem bezpieczeństwa całego systemu lub też przed podjęciem nieupoważnionych działań ze strony pojedynczych jednostek, zarządzanie operacyjne systemem powierzone zostaje różnym osobom, których zadania są rozdzielone oraz dokładnie zdefiniowane. Pracownik ds. projektowania oraz świadczenia usług certyfikacyjnych jest pracownikiem InfoCert i został wybrany na podstawie posiadanego doświadczenia w zakresie projektowania, realizacji oraz świadczenia usług informatycznych, a także dzięki cechom gwarantującym niezawodność oraz przestrzeganie zasad poufności. Działania szkoleniowe planowane są okresowo i mają na celu poszerzanie wiedzy na temat powierzanych pracownikom zadań. 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 przeprowadzanych 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 w celu zebrania danych dot. potrzeb szkoleniowych niezbędnych do osiągnięcia celów biznesowych;
- wywiady z kierownikami w celu ustalenia szczegółowych potrzeb szkoleniowych dot. ich obszarów działania;
- przekazanie zebranych danych dyrekcji przedsiębiorstwa w celu zamknięcia oraz przyjęcia planu szkoleń.

Do lutego uzgodniony w ten sposób plan szkoleń zostaje upubliczniony.

5.3.5 Częstotliwość rotacji w zmianowym systemie pracy

Obecność w miejscu pracy regulowana jest na podstawie zmianowego planu pracy, który co miesiąc przygotowywany jest przez kierownika jednostki organizacyjnej, z wyprzedzeniem przynajmniej 10 dni. Każda zmiana trwa 8 godzin roboczych.
Pod warunkiem posiadania przez pracowników niezbędnego przygotowania technicznego oraz zawodowego, przedsiębiorstwo stara się stosować rotację zmianową jak największej liczby pracowników, dając pierwszeństwo tym, którzy się o to zwracają.

Nie przewiduje się obecności w miejscu pracy w godzinach nocnych. Zmiany wymagające obecności w miejscu pracy odbywają się w godzinach od 07:00 do 21:00 od poniedziałku do piątku oraz od 07:00 do 12:00 w soboty.

5.3.6 Sankcje z tytułu nieuprawnionych działań

Procedura nakładania sankcji na pracowników uregulowana jest w dokumencie „CCNL [włoski układ zbiorowy] Pracownicy przemysłu obróbki metalu oraz montażu linii w przemyśle prywatnym".

5.3.7 Nadzorowanie pracowników kontraktowych

Nie dotyczy

5.3.8 Informacje, które 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 zobowiązany jest do podpisania zgody na przetwarzanie danych osobowych oraz zobowiązania do nierozpowszechniania poufnych informacji i/lub dokumentów. Na koniec musi zapoznać się z Kodeksem etycznym oraz Netykietą InfoCert.

5.4 Prowadzenie dziennika kontrolnego

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

5.4.1 Rodzaje rejestrowanych zdarzeń

Rejestracji podlegają zdarzenia dot. bezpieczeństwa, uruchamiania oraz wygaszania, awarii systemu oraz sprzętu, działania firewalla oraz routerów, a także prób włamania się do systemu PKI.
Gromadzone są wszystkie dane oraz 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 oraz cyklem życia certyfikatów: wnioski o wydanie i odnowienie, dokonane rejestracje, generowanie, przekazywanie oraz ewentualne decyzje o unieważnieniu lub zawieszeniu certyfikatu.
Rejestracji podlegają także wszystkie zdarzenia związane z personalizacją urządzeń do składania podpisu.
Każde zdarzenie zapisywane jest z datą oraz godziną jego wystąpienia (zgodnie ze wskazaniami systemu).

5.4.2 Częstotliwość przetwarzania oraz zapisywania dziennika kontrolnego

Przetwarzanie oraz grupowanie danych, a także ich zapisywanie w systemie przechowywania, zgodnie z regulacjami InfoCert, następuje raz w miesiącu.

5.4.3 Okres przechowywania dziennika kontrolnego

Dziennik kontrolny przechowywany jest przez CA przez 20 lat.

5.4.4 Zabezpieczenie dziennika kontrolnego

Za zabezpieczenie dziennika kontrolnego odpowiada system przechowywania dokumentów elektronicznych InfoCert, posiadający akredytację AgID, zgodnie z obowiązującymi przepisami.

5.4.5 Procedury backupu dziennika kontrolnego

System przechowywania dokumentów elektronicznych wdraża zasady oraz procedurę dotyczącą tworzenia kopii zapasowej (backup), zgodnie z instrukcją bezpieczeństwa przewidzianą dla systemu.

5.4.6 Procedury zapisywania dziennika kontrolnego

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

5.4.7 Zawiadomienia w przypadku stwierdzenia luk w zabezpieczeniu systemu

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, podejmuje działania w celu lepszego zabezpieczenia aplikacji.

5.5 Archiwizacja protokołów

5.5.1 Rodzaje archiwizowanych protokołów

Dla najważniejszych zdarzeń danego urzędu certyfikacji sporządza się oraz archiwizuje odpowiednie protokoły. Protokoły te przechowywane są przez urząd certyfikacji przez 20 lat w systemie przechowywania dokumentów InfoCert.

5.5.2 Zabezpieczenie protokołów

Zabezpieczenie protokołów zapewnia system przechowywania dokumentów InfoCert, posiadający akredytację organu nadzoru (AgID).

5.5.3 Procedury backupu protokołów

System przechowywania, zgodny z obowiązującymi przepisami, wdraża zasady oraz procedurę dotyczącą tworzenia kopii zapasowej (backup), zgodnie z instrukcją bezpieczeństwa przewidzianą dla systemu.

5.5.4 Wymaganie znakowania czasem protokołów

Nie dotyczy

5.5.5 System zapisywania archiwów

Gromadzenie protokołów następuje automatycznie, a ich zapisywanie odbywa się na zasadach przewidzianych przez system przechowywania danych spełniający normy InfoCert, opisanych w instrukcji bezpieczeństwa tego systemu.

5.5.6 Procedury dostępu do informacji zawartych w archiwach oraz ich weryfikacji

Istnieją procedury oraz automatyczne systemy, których zadaniem jest kontrola stanu systemu certyfikacji oraz wewnętrznej infrastruktury technicznej CA.

5.6 Wymiana prywatnego klucza CA

CA przeprowadza procedury okresowej wymiany prywatnego klucza wykorzystywanego do podpisywania certyfikatów w sposób umożliwiający posiadaczowi używanie posiadanego certyfikatu aż do momentu jego odnowienia. Każda wymiana powodować będzie zmianę niniejszej Polityki oraz konieczność przekazania odpowiedniej informacji organowi nadzoru (AgID).

5.7 Naruszenie prywatnego klucza CA oraz disaster recovery

5.7.1 Procedury zarządzania incydentami

CA opisał procedury zarządzania incydentami w ramach SZBI zgodnego z ISO 27000. Niezwłocznie po stwierdzeniu każdego ewentualnego incydentu poddaje się go dokładnej analizie i określa się działania naprawcze, a kierownik ds. usług sporządza odnośny protokół. Elektronicznie podpisany protokół przesłany zostaje do systemu przechowywania InfoCert. Jedną jego kopię otrzymuje także AgID, wraz z informacją o działaniach interwencyjnych mających na celu wyeliminowanie prawdopodobnych przyczyn wystąpienia incydentu, jeśli – zgodnie z art. 19 rozporządzenia – znajduje się on pod kontrolą InfoCert.

5.7.2 Uszkodzenie sprzętu, oprogramowania lub danych

W przypadku awarii bezpiecznego urządzenia do składania podpisu HSM zawierającego klucze certyfikacyjne, należy sięgnąć po zapasową kopię klucza, odpowiednio zapisaną oraz przechowywaną, bez konieczności unieważnienia odpowiadającego mu certyfikatu CA.

Oprogramowanie oraz dane są przedmiotem regularnie wykonywanego backupu, zgodnie z obowiązującymi procedurami wewnętrznymi.

5.7.3 Procedury w razie naruszenia prywatnego klucza CA

Naruszenie klucza certyfikacyjnego stanowi szczególnie krytyczne zdarzenie, jako że powoduje utratę ważności wystawionych certyfikatów podpisanych z użyciem tego klucza. Należy więc zwrócić szczególną uwagę na ochronę klucza certyfikacyjnego, a także na wszelkie czynności w zakresie rozwijania i utrzymywania systemu, mogące mieć na niego wpływ.
InfoCert opisał procedurę, którą należy zastosować w przypadku naruszenia klucza, w ramach SZBI zgodnego z ISO 27000, informując o fakcie jej wdrożenia także organ nadzoru AgID oraz CAB.

5.7.4 Świadczenie usług CA w przypadku katastrof

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

5.8 Zaprzestanie świadczenia usług przez CA lub RA

W przypadku chęci zaprzestania prowadzenia działalności certyfikacyjnej InfoCert poinformuje o tym fakcie organ nadzoru (AgID) oraz jednostkę oceniającą zgodność (CAB) z co najmniej 6-miesięcznym wyprzedzeniem. Może on także wskazać inny podmiot certyfikujący, który go zastąpi, oraz który stanie się depozytariuszem rejestru certyfikatów oraz związanej z tym dokumentacji. Z takim samym okresem wyprzedzenia InfoCert poinformuje o chęci zaprzestania prowadzenia działalności także wszystkich posiadaczy wydanych przez siebie certyfikatów. W informacji tej, w przypadku braku wskazania zastępczego podmiotu certyfikującego, zostanie wyraźnie podane, iż wszystkie certyfikaty pozostające ważne w momencie zaprzestania prowadzenia działalności przez CA, zostaną unieważnione.

6 KONTROLE BEZPIECZEŃSTWA TECHNOLOGICZNEGO

6.1 Instalacja i generowanie pary kluczy certyfikacyjnych

W celu prowadzenia działalności urząd certyfikacji musi wygenerować parę kluczy certyfikacyjnych do podpisywania certyfikatów posiadaczów.

Klucze generowane są tylko przez personel wyraźnie wyznaczony do tej funkcji. Generowanie kluczy i podpisów odbywa się w ramach dedykowanych modułów kryptograficznych, certyfikowanych zgodnie z obowiązującymi przepisami.

Ochrona kluczy prywatnych CA przeprowadzana jest przez moduł kryptograficzny generowania i użycia tego samego klucza. Klucz prywatny może być generowany tylko przy jednoczesnej obecności dwóch operatorów wyznaczonych do generowania. Generowanie kluczy odbywa się w obecności kierownika ds. usług certyfikacyjnych.

Klucze prywatne CA duplikowane są, 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 składania podpisu spełnia wymagania pozwalające zapewnić:

- zgodność pary z wymaganiami ustanowionymi przez stosowane algorytmy generowania i weryfikacji;
- jednakowe prawdopodobieństwo wygenerowania wszystkich możliwych par;
- identyfikację podmiotu uruchamiającego procedurę generowania;
- generowanie podpisu wewnątrz urządzenia w taki sposób, aby nie było możliwe przechwycenie wartości użytego klucza prywatnego.

6.1.1 Generowanie pary kluczy posiadacza

Klucze asymetryczne generowane są w bezpiecznym urządzeniu do składania podpisu SSCD lub QSCD 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 odpowiednią dokumentację i podlegając okresowym audytom.

6.1.2 Dostarczanie klucza prywatnego wnioskodawcy

Klucz prywatny znajduje się w urządzeniu kryptograficznym, niezależnie od tego, czy jest to SSCD czy QSCD. 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, z zapewnieniem transportu urządzenia i informacji dotyczących jego użytkowania różnymi kanałami, co znaczy, że elementy te dostarczane są posiadaczowi w dwóch różnych momentach czasowych.

6.1.3 Dostarczanie klucza publicznego CA

Nie dotyczy

6.1.4 Dostarczanie klucza publicznego użytkownikom

Klucz publiczny zawarty jest w certyfikacie wydanym wyłącznie wnioskodawcy. Na wniosek wnioskodawcy zostanie on również opublikowany w rejestrze publicznym, z którego może zostać pobrany przez użytkownika.

6.1.5 Algorytm i długość kluczy

Para kluczy kryptograficznych generowana jest w ww. sprzętowym urządzeniu kryptograficznym. Algorytm asymetryczny RSA używany jest z kluczami o długości nie mniejszej, niż 4096 bitów.
Dla kluczy posiadacza stosowany algorytm asymetrycznego szyfrowania jest algorytmem RSA, a długość kluczy jest nie mniejsza, niż 2048 bitów.

6.1.6 Kontrola jakości i generowanie klucza publicznego

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

6.1.7 Cel użycia klucza

Cel użycia klucza prywatnego określony jest przez rozszerzenie KeyUsage, zgodnie z definicją w standardzie X.509. Dla certyfikatów opisanych w niniejszej Polityce jedynym dozwolonym zastosowaniem jest „niezaprzeczalność”, tzn. mogą być one używane tylko do podpisywania.

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 zatwierdzenie Common Criteria (CC) Information Technology Security Evaluation Assurance Level EAL 4+ Type 3 (EAL 4 Augmented by AVA_VLA.4 and AVA_MSU.3) lub EAL5 Augmented by ALC_DVS.2, AVA_VAN.5.
Moduły kryptograficzne używane przez InfoCert dla kluczy podpisu zdalnego i automatycznego posiadacza posiadają zatwierdzenie FIPS 140 Level 3 i Common Criteria (CC) Information Technology Evaluation Assurance Level EAL 4.

6.2.2 Kontrola klucza prywatnego CA przez kilka osób

Dostęp do urządzeń zawierających klucze certyfikacyjne możliwy jest tylko w przypadku obecności dwóch osób uwierzytelnionych w tym samym czasie.

6.2.3 Deponowanie klucza prywatnego CA u stron trzecich

Nie dotyczy

6.2.4 Tworzenie kopii zapasowej klucza prywatnego 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 tego, który ma 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 generowany jest i przechowywany w bezpiecznym miejscu urządzenia kryptograficznego, które uniemożliwia jego eksport. Ponadto system operacyjny urządzenia w przypadku złamania zabezpieczeń powoduje blokadę lub brak czytelności urządzenia.

6.2.8 Metoda aktywacji klucza prywatnego

Prywatny klucz certyfikacyjny aktywowany jest przez oprogramowanie CA w trybie *dual control*, tj. w obecności dwóch osób pełniących określone role i w obecności kierownika ds. usług certyfikacyjnych.
Podmiot lub wnioskodawca reprezentujący osobę prawną jest odpowiedzialny za ochronę 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 jest odpowiedzialny za zniszczenie klucza prywatnego po wygaśnięciu lub unieważnieniu certyfikatu, zgodnie z procedurami bezpieczeństwa określonymi w polityce bezpieczeństwa i specyfikacjami 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 wyraża się w nim w sposób wskazany w pkt. 3.3.1.

Obecnie certyfikat CA ważny jest przez 16 lat, a certyfikaty wydawane osobom fizycznym lub prawnym ważne są nie dłużej, niż 3 lata.

6.4 Dane aktywujące klucz prywatny

Odsyła się do punktów 4.2 i 6.3.

6.5 Kontrole bezpieczeństwa informatycznego

6.5.1 Szczególne wymogi 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 ewentualnych luk 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 miesięcy.

6.6 Działania dotyczące systemów zarządzania

InfoCert przywiązuje najwyższą wagę do bezpiecznego przetwarzania informacji i uznaje potrzebę ciągłego rozwijania, utrzymywania, kontrolowania i doskonalenia systemu zarządzania bezpieczeństwem informacji (SZBI) zgodnie z ISO/IEC 27001.
InfoCert posiada certyfikat ISO/IEC 27001:2005 od marca 2011 roku dla działań EA:33-35. W marcu 2015 roku otrzymał certyfikat w zakresie nowej wersji normy ISO/IEC 27001:2013.
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 zatwierdzane są przez właściwych kierowników i udostępniane wewnętrznie w systemie zarządzania dokumentami InfoCert.

6.7 Kontrole bezpieczeństwa sieci

InfoCert zaprojektował 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 firewall, które pozwalają na podział połączenia na obszary stopniowo zwiększającego się bezpieczeństwa: sieć Internet, sieci DMZ (Demilitarized Zone) lub sieci obwodowe, sieci wewnętrzne. Cały przepływ danych pomiędzy różnymi obszarami podlega akceptacji przez zaporę sieciową w oparciu o zestaw ustalonych zasad. Reguły zdefiniowane na zaporach sieciowych zaprojektowane są zgodnie z zasadami „default deny” (co nie jest wyraźnie dozwolone, jest domyślnie zabronione, co oznacza, że zasady te pozwolą tylko na to, co jest ściśle niezbędne do 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 na stronie internetowej dostawcy usług zaufania 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 i uchwałą CNIPA [9]; 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 0 podano kody źródłowe certyfikatów root i certyfikatów posiadaczów 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 certyfikatów

Certyfikaty kwalifikowane charakteryzują się rozszerzeniami zawartymi w qcStatement clause 3.2.6 IETF RFC 3739. Ich stosowanie reguluje norma ETSI 319 412-5.
W celu uzyskania informacji o rozszerzeniach patrz 0.

7.1.3 OID algorytmu podpisu

Certyfikaty podpisywane są następującym algorytmem:
sha256WithRSAEncryption[iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 11].

7.1.4 Formy nazw

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

7.1.5 Restrykcje dotyczące nazw

Patrz punkt 3.1.

7.1.6 OID certyfikatu

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 list CRL

Aby uzyskać informacje na temat rozszerzeń list CRL, patrz 0.

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 mają 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 RFC6960.

7.3.2 Rozszerzenia OCSP

Aby uzyskać informacje na temat rozszerzeń OCSP, patrz 0.

8 KONTROLE I OCENY ZGODNOŚCI

W celu uzyskania kwalifikacji kwalifikowanych i niekwalifikowanych dostawców usług zaufania, zgodnie z rozporządzeniem eIDAS konieczne jest przeprowadzenie procedury przewidzianej 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 zgodność (CAB) upoważnioną przez właściwy organ krajowy, którą we Włoszech jest ACCREDIA.
InfoCert świadczy usługi jako dostawca kwalifikowanych usług zaufania zgodnie z rozporządzeniem (UE) nr 910/2014 z dnia 23.07.2014 r., na podstawie oceny zgodności przeprowadzonej przez jednostkę oceniającą zgodność CSQA Certificazioni S.r.l., w myśl powyższego rozporządzenia oraz normy ETSI EN 319 401, zgodnie ze schematem oceny eIDAS, określonym przez ACCREDIA w odniesieniu do norm ETSI EN 319_403 i UNI CEI EN ISO/IEC 17065:2012.

8.1 Częstotliwość lub okoliczności oceny zgodności

Ocena zgodności powtarzana jest co dwa lata, ale każdego roku CAB przeprowadza audyt nadzoru.

8.2 Tożsamość i kwalifikacje audytora

Audyt przeprowadza:

Nazwa firmy	CSQA Certification S.r.l.
Siedziba statutowa	Via S. Gaetano nr 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 NIP	02603680246
Strona internetowa	http://www.csqa.it

8.3 Związek InfoCert z CAB

InfoCert i CSQA nie są powiązane żadnymi wspólnymi interesami finansowymi ani relacjami biznesowymi.
W obiektywnej ocenie CSQA brak jest bieżących relacji biznesowych lub partnerskich, które mogłyby działać na korzyść lub na niekorzyść InfoCert.

8.4 Aspekty objęte audytem

CAB dokona oceny zgodności przyjętych procedur, organizacji CA, organizacji roli, szkolenia personelu i dokumentacji umownej w odniesieniu do Polityki, 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 oraz odnowienie certyfikatów

Tabela opłat dostępna jest na stronach https://www.firma.infocert.it/ oraz http://ecommerce.infocert.it lub w punktach rejestracji (RA). CA może zawierać odrębne porozumienia handlowe z RA i/lub wnioskodawcami, 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 dot. statusu zawieszenia oraz unieważnienia certyfikatów

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

9.1.4 Opłaty za inne usługi

Tabela opłat dostępna jest na stronach https://www.firma.infocert.it/ oraz http://ecommerce.infocert.it lub w punktach rejestracji (RA).

CA może zawierać odrębne porozumienia handlowe z RA i/lub wnioskodawcami, zawierające inne opłaty.

9.1.5 Polityka dot. zwrotów poniesionych kosztów

W przypadku nabycia usługi przez konsumenta, Podmiot posiadacz ma prawo odstąpić od umowy w terminie 14 dni od daty zawarcia umowy, otrzymując zwrot uiszczonej kwoty. Instrukcje dot. możliwości skorzystania z prawa do odstąpienia od umowy oraz wniosek o zwrot poniesionych kosztów dostępne są na stronie https://help.infocert.it/ lub w punktach rejestracji (RA).

9.2 Odpowiedzialność finansowa

9.2.1 Ochrona ubezpieczeniowa

TSP InfoCert zawarł umowę ubezpieczeniową obejmującą ryzyko związane z prowadzoną działalnością oraz ewentualne szkody wyrządzone osobom trzecim, której treść została uzgodniona oraz przyjęta przez AgID, zawierającą następujące maksymalne sumy odszkodowania:

- 10 000 000 euro za pojedyncze zdarzenie;
- 10 000 000 euro w agregacie rocznym.

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 dot. informacji poufnych

W ramach działalności będącej przedmiotem niniejszej Polityki nie przewiduje się zarządzania informacjami poufnymi.

9.3.2 Informacje, dla których nie znajdują zastosowania zasady dot. informacji poufnych

Nie dotyczy

9.3.3 Odpowiedzialność za ochronę informacji poufnych

Nie dotyczy

9.4 Ochrona danych

Informacje dotyczące posiadacza oraz wnioskodawcy, w posiadanie których wchodzi CA w związku z prowadzeniem swojej normalnej działalności, należy traktować za poufne i niedopuszczone do ujawniania (chyba że uzyskano wyraźną zgodę), z wyjątkiem tych jednoznacznie przeznaczonych do użytku publicznego, takich jak klucz publiczny, certyfikat (jeśli wnioskowany przez posiadacza) oraz data unieważnienia i zawieszenia certyfikatu. To oznacza, iż dane osobowe przetwarzane są przez InfoCert zgodnie z zapisami [włoskiego] dekretu legislacyjnego nr 196 z dnia 30 czerwca 2003 r. oraz rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych, w pełni obowiązującego od dnia 25 maja 2018 roku [4].

9.4.1 Program dot. ochrony danych

InfoCert stosuje szereg zasad, za pośrednictwem których wdraża i integruje system ochrony danych osobowych w ramach własnego systemu zarządzania bezpieczeństwem informacji zgodnie z ISO 270001, w oparciu o zasadę stałego 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], zgodnie z którą za dane osobowe uznaje się wszelkie informacje dot. osoby fizycznej, zidentyfikowanej lub możliwej do zidentyfikowania, także pośrednio, poprzez odniesienie do jakiejkolwiek innej informacji, w tym do numeru identyfikacyjnego osoby.

9.4.3 Dane nieuznawane za dane osobowe

Dane przeznaczone do upublicznienia przez dział techniczny CA, tj. 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.
Siedziba operacyjna
Via Marco e Marcelliano 45
00147 Roma
richieste.privacy@legalmail.it

9.4.5 Informacje na temat ochrony danych oraz zgoda na przetwarzanie danych osobowych

Polityka prywatności dostępna jest na stronie www.infocert.it.
Przed rozpoczęciem jakiegokolwiek procesu przetwarzania danych osobowych InfoCert uzyskuje zgodę na przetwarzanie tychże danych, na zasadach oraz w formie przewidzianej obowiązującymi przepisami prawa [4].

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

Brak.

9.5 Własność intelektualna

Prawa autorskie do niniejszego dokumentu przysługują InfoCert S.p.A. Wszelkie prawa zastrzeżone.

9.6 Prawo do reprezentowania oraz gwarancje

InfoCert odpowiada za przestrzeganie procedur zapisanych we własnej polityce bezpieczeństwa informacji, także wtedy, gdy realizacja niektórych jego zadań przekazana jest innemu podmiotowi, zgodnie z art. 2.4.1. załącznika do rozporządzenia wykonawczego Komisji (UE) 2015/1502.
W takim przypadku prawo do reprezentowania realizowane jest na podstawie pełnomocnictwa udzielonego przez InfoCert punktowi rejestracji (RA), w którym określony zostaje zakres odpowiedzialności oraz obowiązki stron. W szczególności punkt rejestracji zobowiązany jest do przeprowadzania działań rejestracyjnych zgodnie z obowiązującymi przepisami prawa, a także zgodnie z procedurami opisanymi w Polityce, ze szczególnym uwzględnieniem obowiązku identyfikacji osób podpisujących wniosek o wydanie cyfrowego certyfikatu, a także do przekazywania odnośnych danych do InfoCert.
Posiadacz odpowiedzialny jest za prawdziwość danych przekazywanych we wniosku o rejestrację i wydanie certyfikatu. W przypadku gdy w chwili identyfikacji posiadacz ukryje swoją prawdziwą tożsamość lub poda się za inny podmiot, w tym przez użycie nieprawdziwych dokumentów osobistych, lub też podejmie jakiekolwiek działania naruszające proces identyfikacji oraz fałszujące dane zawarte w certyfikacie, będzie on odpowiedzialny za wszelkie szkody poniesione przez podmiot certyfikujący i/lub osoby trzecie wynikające z nieprecyzyjności informacji zawartych w certyfikacie i będzie miał obowiązek zaspokojenia ewentualnych roszczeń odszkodowawczych, zwalniając z tego obowiązku podmiot certyfikujący.
Ponadto posiadacz oraz wnioskodawca odpowiedzialni są za szkody poniesione przez podmiot certyfikujący i/lub osoby trzecie, wynikające z opóźnienia uruchomienia przez nich procedur, o których mowa w punkcie 4.9. niniejszej Polityki (unieważnienie i zawieszenie certyfikatu).

9.7 Ograniczenia gwarancji

Podmiot certyfikujący nie udziela żadnej gwarancji na: prawidłowe działanie oraz bezpieczeństwo sprzętu komputerowego oraz oprogramowania używanych przez posiadacza; wykorzystywanie prywatnego klucza, bezpiecznego urządzenia do składania podpisu (jeśli występuje) i/lub certyfikatu podpisu do celów innych niż te przewidziane w obowiązujących przepisach prawa oraz w niniejszej Polityce; prawidłowe i nieprzerwane działanie krajowych lub międzynarodowych linii elektrycznych i telefonicznych; ważność i znaczenie, w tym znaczenie dowodowe, certyfikatu podpisu lub wszelkich wiadomości, aktów lub dokumentów związanych z nim za pośrednictwem kluczy, do których odnosi się certyfikat, z zastrzeżeniem skuteczności prawnej kwalifikowanego podpisu elektronicznego równoważnej podpisowi własnoręcznemu, zgodnie z art. 25 rozporządzenia (UE) nr 910/2014; poufność i/lub integralność wszelkich wiadomości, aktów lub dokumentów związanych z nim za pośrednictwem kluczy, do których odnosi się certyfikat (w tym sensie, iż ewentualne naruszenie poufności lub integralności zwykle stwierdzane jest przez posiadacza lub odbiorcę przy pomocy odpowiednich procedur weryfikacyjnych).
Podmiot certyfikujący udziela gwarancji wyłącznie na działanie usług na poziomie, o którym mowa w punkcie 9.17 Polityki.

9.8 Ograniczenia odpowiedzialności

Na Podmiocie certyfikującym nie ciąży żaden obowiązek nadzoru nad treścią, rodzajem lub elektronicznym formatem dokumentów i/lub, ewentualnie, identyfikatorów *hash* przesyłanych w ramach procedury informatycznej wskazanej przez wnioskodawcę lub posiadacza, ani też odpowiedzialność za ich ważność oraz możliwość ich powiązania z rzeczywistą wolą posiadacza.
Z wyjątkiem przypadków działania umyślnego lub niedbalstwa, podmiot certyfikujący nie ponosi odpowiedzialności za szkody bezpośrednie i pośrednie poniesione przez posiadaczy i/lub osoby trzecie w konsekwencji zastosowania lub niezastosowania certyfikatów podpisu wystawionych na podstawie zapisów zawartych w niniejszej Polityce oraz w Ogólnych warunkach świadczenia usług certyfikacyjnych.
InfoCert nie ponosi odpowiedzialności za jakiekolwiek szkody bezpośrednie i/lub pośrednie wynikające z co najmniej jednego z następujących zdarzeń: utraty narzędzi identyfikacji i uwierzytelniania, ich niewłaściwego przechowywania, ich niewłaściwego zastosowania, i/lub nieprzestrzegania ww. zapisów przez posiadacza.
Ponadto podmiot certyfikujący, już 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 oraz sieci internetowej.
Z wyjątkiem przypadków działania umyślnego lub niedbalstwa, 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 mających za przedmiot 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 z powodu niedbalstwa, bezpośrednio jakiejkolwiek osobie fizycznej lub prawnej, w konsekwencji niedopełnienia przez InfoCert obowiązków, o których mowa w rozporządzeniu Parlamentu Europejskiego i Rady (UE) nr 910/2014 z dnia 23 lipca 2014 r., oraz braku podjęcia przez InfoCert wszelkich możliwych kroków, mających na celu niedoprowadzenie do powstania szkody.

W ww. przypadku wnioskodawcy lub posiadaczowi przysługiwać będzie prawo do odszkodowania za szkody poniesione bezpośrednio w konsekwencji ww. działań, w wysokości w żadnym przypadku nieprzekraczającej maksymalnych sum odszkodowania, za pojedyncze zdarzenie lub w agregacie rocznym, zgodnie z art. 3 ust. 7 regulaminu załączonego do decyzji nr 185/2017.

Niemożliwym będzie ubieganie się o zwrot poniesionych kosztów w przypadku, gdy niemożność skorzystania z usługi wynikać będzie z niewłaściwej jej eksploatacji lub z problemów związanych z siecią telekomunikacyjną, lub też z powodów losowych, z działania siły wyższej lub z przyczyn niezależnych od InfoCert, takich jak na przykład strajki, protesty, trzęsienia ziemi, akty terroryzmu, zamieszki, zorganizowane akty sabotażu, zdarzenia chemiczne i/lub bakteriologiczne, wojny,

powodzie, decyzje właściwych władz lub nieodpowiedniość struktur, sprzętu komputerowego i/lub oprogramowania stosowanego przez wnioskodawcę.

9.10 Zakończenie stosunku umownego oraz rozwiązanie umowy

9.10.1 Zakończenie stosunku umownego

W chwili zakończenia stosunku umownego pomiędzy CA a posiadaczem, pomiędzy CA a RA oraz pomiędzy CA a wnioskodawcą, certyfikat zostanie unieważniony. Umowa certyfikacyjna pomiędzy podmiotem certyfikującym a posiadaczem zawierana jest na czas równy okresowi ważności certyfikatu podpisu podanemu w polu „termin ważności" (*validity*).
Przed upływem ważności certyfikatu jego posiadacz może zwrócić się o jego odnowienie, 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 oraz unieważnieniem wystawionego certyfikatu, w przypadku niespełnienia przez posiadacza i/lub wnioskodawcę warunków umowy, o których mowa w art. 3 (Odpowiedzialność posiadacza oraz wnioskodawcy), art. 4.6 (Własność intelektualna), art. 8 (Obowiązki posiadacza), art. 11 (Opłaty), art. 12.3 (dot. obowiązku zawiadamiania o przypadkach oraz przyczynach zawieszenia oraz unieważnienia certyfikatu), a także – jeśli dotyczy – art. 45 (Dodatkowe obowiązki posiadacza i wnioskodawcy) oraz art. 47 (Dodatkowe obowiązki posiadacza), jak również zapisów niniejszej Polityki. Umowa ulega rozwiązaniu z mocy prawa również wtedy, gdy jedna ze stron poinformuje drugą stronę, za pośrednictwem certyfikowanej poczty elektronicznej lub listem poleconym ze zwrotnym potwierdzeniem odbioru, o zamiarze skorzystania z niniejszej klauzuli.
W przypadku, gdy posiadaczem certyfikatu jest konsument, ewentualne spory o charakterze cywilnym związane z umową zawartą przez konsumenta, rozstrzygane będą wyłącznie przez sąd właściwy dla miejsca jego stałego lub tymczasowego zamieszkania.
Konsument może na zasadzie dobrowolności skorzystać z pozasądowych metod rozstrzygania sporów, o których mowa we włoskim kodeksie konsumenta oraz w innych, właściwych dla charakteru sprawy, obowiązujących przepisach prawa.
Ponadto informuje się, iż zgodnie z rozporządzeniem (UE) nr 524/2013, w celu rozstrzygania sporów związanych z umowami online oraz usługami oferowanymi online, istnieje możliwość skorzystania z procedury internetowego rozstrzygania sporów (ODR), wprowadzonej przez Komisję Europejską i dostępnej pod adresem: https://webgate.ec.europa.eu/odr/ .
Podmiotowi certyfikującemu przysługuje prawo odstąpienia od umowy na usługi certyfikacyjne, i wynikającego z niego unieważnienia certyfikatu, w każdym czasie, z zachowaniem 30-dniowego okresu wypowiedzenia.
W każdym przypadku niewypełnienia podjętych zobowiązań przez posiadacza lub wnioskodawcę podmiot certyfikujący ma prawo zawiesić świadczenie usług, w tym poprzez zawieszenie certyfikatu.
W szczególności, w przypadku nieuiszczenia opłat za usługi InfoCert będzie miał prawo rozwiązać

umowę z wnioskodawcą oraz posiadaczem w każdym momencie jej obowiązywania, bez zachowania okresu wypowiedzenia oraz ponoszenia jakichkolwiek opłat z tego tytułu.
Odstąpienie od umowy przez posiadacza lub unieważnienie certyfikatu nie zwalnia z obowiązku uiszczenia opłaty za usługi, a w przypadku jej wcześniejszego uiszczenia, zostaje ona w całości zatrzymana przez InfoCert, także z tytułu samego odstąpienia.
W każdym przypadku rozwiązania umowy, odstąpienia od niej lub jej wygaśnięcia, zapisy umowy pozostają wiążące aż do momentu rozwiązania, odstąpienia lub wygaśnięcia.
Posiadacz uznaje fakt, iż w przypadku wygaśnięcia umowy, niezależnie od powodów wygaśnięcia, nie będzie możliwe dalsze korzystanie z usług.

9.10.3 Skutki rozwiązania umowy

Rozwiązanie umowy powoduje natychmiastowe unieważnienie certyfikatu.

9.11 Oficjalne kanały komunikacyjne

Patrz kanały komunikacyjne opisane w punkcie 1.5.1.

9.12 Aktualizacje Polityki

CA zastrzega sobie prawo do wprowadzania zmian do niniejszego dokumentu wynikających z potrzeb technicznych lub ze zmian proceduralnych, zarówno spowodowanych zmianami obowiązujących przepisów prawa lub rozporządzeń, jak i mających na celu optymalizację pracy. Każda nowa wersja Polityki anuluje i zastępuje poprzednie, które jednak znajdują zastosowanie dla certyfikatów wydanych w okresie ich obowiązywania, do wygaśnięcia pierwszego terminu ważności tych certyfikatów.

Zmiany niemające znaczącego wpływu dla użytkowników wiążą się z publikacją nowego wydania tej samej wersji dokumentu, natomiast zmiany o znaczącym wpływie dla użytkowników (jak np. zmiany dotyczące procedur działania) wiążą się z publikacją nowej wersji dokumentu. W każdym z przypadków Polityka jest niezwłocznie publikowana oraz udostępniana na wcześniej ustalonych zasadach. O każdej zmianie technicznej lub proceduralnej wprowadzonej do niniejszej Polityki niezwłocznie informuje się punkty rejestracji (RA).
Jeśli wprowadzone zmiany są znaczące, CA zobowiązany jest poddać je audytowi ze strony akredytowanej jednostki CAB, przedstawić organowi nadzoru (AgID) raport z oceny zgodności (*CAR – Conformity Assessment Report*) i Politykę, oraz poczekać na zgodę na ich opublikowanie.

9.12.1 Historia zmian

Wersja/wydanie nr:	3.4
Data wersji/wydania:	20.06.2018 r.

Opis zmian:	Pkt. 1.5.1 Zmiana numeru call center. Pkt. 9.2.1 Aktualizacja maksymalnych sum ubezpieczenia.
Uzasadnienie:	-

Wersja/wydanie nr:	3.3
Data wersji/wydania:	04.09.2918 r.
Opis zmian:	Rozdz. 1 Zmiana „podpisu cyfrowego” na „kwalifikowany podpis elektroniczny”. Wprowadzenie kilku zmian terminologicznych, mających na celu lepsze zrozumienie tekstu, a także dodanie kilku definicji terminów użytych w dokumencie. Pkt. 3.1.5 Ponowne częściowe zredagowanie punktu w celu jego lepszego zrozumienia. Pkt. 3.2.3 Ponowne zredagowanie tabeli oraz podpunktów w celu ich lepszego zrozumienia oraz nadania kontekstu odpowiedniego dla rynków europejskich. Rozszerzenie trybu 4 AutID na narzędzia identyfikacji elektronicznej stosowane w państwach członkowskich. Zdefiniowanie specjalnego dokumentu zawierającego rodzaje dokumentów oraz akceptowane narzędzia identyfikacji elektronicznej. Pkt. 4.2 Ponowne częściowe zredagowanie punktu w celu jego lepszego zrozumienia oraz nadania kontekstu odpowiedniego dla rynków europejskich. Pkt. 4.2.2 Dodatkowe systemy uwierzytelniania. Pkt. 4.3.3.2 Możliwość wystawiania już aktywnego certyfikatu. Pkt. 4.5.3 Wprowadzenie dodatkowego ograniczenia dot. stosowania. Pkt. 4.9.15 i 4.9.16 Zawieszenie oraz przywrócenie przy pomocy CMS. Pkt. 9.4 Dodanie odniesień do GDPR. Pkt. 9.6, pkt. 9.7, pkt. 9.8, pkt. 9.9, pkt. 9.10 Ponowne zredagowanie punktów w celu nadania im lepszego kontekstu. Certyfikaty użytkownika: dodanie certyfikatów dla osoby prawnej na urządzeniu QSCD, poprawienie kilku błędów.
Uzasadnienie:	-

Wersja/wydanie nr:	3.2
Data wersji/wydania:	02.05.2017 r.
Opis zmian:	Dodanie informacji dot. CA „Infocert Podpis Kwalifikowany 2” Dodanie kilku OID dot. CA „Infocert Podpis Kwalifikowany 2” Poprawienie formy i pisowni
Uzasadnienie:	

Wersja/wydanie nr:	3.1
Data wersji/wydania:	27.01.2017 r.
Opis zmian:	Pkt. 3.2.3 Wyeliminowanie wszystkich odniesień do systemu SPID jako narzędzia uwierzytelniającego do celów identyfikacji. Pkt. 3.2.3.1 Uszczegółowienie rozpoznania przez pracodawcę. Pkt. 4.8.12 Opisanie sposobu przywracania zawieszonego certyfikatu.
Uzasadnienie:	-

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

9.12.2 Procedury dot. aktualizacji

Procedury dot. 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, Biurem Prawnym oraz Działem Doradczym, a następnie przyjmowane przez organ zarządzający.

9.12.3 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 włoską Agencję ds. Cyfryzacji Włoch (AgID);
- w wersji papierowej na wniosek składany w urzędach rejestracyjnych, a w przypadku użytkowników końcowych – w momencie bezpośredniego kontaktu.

9.12.4 Przypadki, w których OID wymaga zmiany

Nie dotyczy

9.13 Rozstrzyganie sporów

Patrz zapisy umowne szczegółowo regulujące zasady rozstrzygania sporów.

9.14 Właściwość sądu

W przypadku konsumentów właściwym sądem jest sąd miasta, w których konsument posiada stałe miejsce zamieszkania. Dla podmiotów innych niż konsumenci właściwym sądem jest Sąd w Rzymie. W ramach odrębnych porozumień zawieranych pomiędzy CA i RA, pomiędzy CA i Wnioskodawcą lub pomiędzy CA i Podmiotem możliwe jest wyznaczenie innego właściwego sądu.

9.15 Właściwość prawa

Prawem właściwym dla niniejszego Podręcznika obsługi jest prawo włoskie.

Poniżej wykaz niektórych podstawowych, mających zastosowanie, odniesień normatywnych:

[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] Dekret legislacyjny nr 82 z dnia 7 marca 2005 r. ([włoski] Dziennik Ustaw nr 112 z dnia 16 maja 2005 r.) – Kodeks administracji cyfrowej (oznaczany również skrótem „CAD") z późn. zm. i uzup.

[3] *brak*

[4] Dekret legislacyjny 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.

[10] Postanowienie AgID nr 189/2017.

Ponadto zastosowanie znajdują wszystkie okólniki oraz uchwały organu nadzoru[6], a także akty wykonawcze, o których mowa w rozporządzeniu eIDAS [1].

9.16 Inne postanowienia

Inne postanowienia niezawarte w niniejszej Polityce określone są w umowie regulujące świadczenie usług.

9.17 Pozostałe postanowienia

Godziny świadczenia usługi (z zastrzeżeniem innych postanowień umownych):

Usługa	Godziny
Dostęp do publicznego archiwum certyfikatów (obejmuje certyfikaty oraz listy unieważnionych certyfikatów [CRL]).	Od 0:00 do 24:00 7 dni w tygodniu
Unieważnienie oraz zawieszenie certyfikatów.	Od 0:00 do 24:00 7 dni w tygodniu
Pozostałe czynności: rejestracja, generowanie, publikowanie, odnowienie[7].	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 95%)

[6] Dostępne na stronie http://www.agid.gov.it/agenda-digitale/infrastrutture-architetture/firme-elettroniche.

[7] Proces rejestracji prowadzony jest w placówkach rejestracyjnych, których godziny otwarcia mogą różnić się między sobą. W każdym przypadku InfoCert zapewnia możliwość korzystania z oferowanej przez siebie usługi w godzinach podanych wyżej.

Appendice A Root CA

Załącznik A

Electronic Signature Qualified Root ”InfoCert Podpis Kwalifikowany 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
         :     96 1D 20 03 BC 24 21 EB F5 D4 D3 FE 4A 72 E4 06
         :     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 ]
        :   }
```

Certyfikat kwalifikowany dla osoby fizycznej z identyfikatorami oraz kluczami semantycznymi na urządzeniu QSCD

Field	Value
VERSION:	3
SERIAL:	Allocated automatically by the Issuing CA
INNER SIGNATURE:	
ALG. ID:	id-sha256-with-rsa-encryption
PARAMETER:	0
ISSUER:	
Country Name:	IT
Organization Name:	InfoCert S.p.A.
Organizational Unit Name:	ified Trust Service Provider
Organization Identifier:	T-07945211006
Common Name:	InfoCert Qualified Electronic Signature CA 3
VALIDITY:	max 39 month
Not Before:	
Not After:	
SUBJECT:	
Country Name:	*CountryCode (ISO 3166) (mandatory)(*****)*
Organization Name:	*(conditioned presence)* ***(***)***

Organizational Unit	*(conditioned presence) (****)*

Organization Identifier:	*(conditioned presence)* ***(***)*** *as defined in clause 5.1.4 of ETSI EN 319 412-1 (i.e. "***VATIT-***TaxIdentificationNumber", "***NTRIT-***IdentifierNationalTradeRegister")*
GivenName:	*Name (conditioned presence)* ***(*)***
Surname:	*Surname (conditioned presence)* ***(*)***
SerialNumber:	*(conditioned presence)* ***(**)*** *as defined in clause 5.1.3 of ETSI EN 319 412-1 (i.e. "***TINIT***-Codicefiscale", "***PASIT-***PassportNumber", "***IDCIT-***IdentityCardNumber")*

Title	*Holder's specific qualification (optional)*
Locality	*(conditioned presence)* ***(****)***
DNQualifier	*Holder's identification code assigned by the Certification Authority, unique within the Certification Authority itself (mandatory)*

Pseudonym:	*(conditioned presence)* ***(*)***
Common Name	*name of the subject (recommended)*
PUBLIC KEY:	(key size is 2048 bits or higher)
ALGORITHM:	
ALG. ID:	id-rsa-encryption
PARAMETER:	0
MODULUS:	
EXPONENT:	
EXTENSIONS:	

Authority Key Identifier:	key identifier (sha1 160 bit) of Issuer Public Key
Key Usage*:	Non-Repudiation (critical)
CRL Distribution Points:	
Distribution Point 1:	
Uniform Resource ID1:	
http://crl.infocert.it/ca3/qc/CRLxx.crl	
Uniform Resource ID2:	
ldap://ldap.infocert.it/cn%3DInfoCert%20Qualified%20Electronic%20Signature%20CA%203%20CRLxx,ou%3DQualified%20Trust%20Service%20Provider,o%3DINFOCERT%20SPA,c%3DIT?certificateRevocationList	
Authority Information Access	
Access Method	1.3.6.1.5.5.7.48.1
Alternative Name	http://ocsp.qc.ca3.infocert.it
Access Method	1.3.6.1.5.5.7.48.2
Alternative Name	http://cert.infocert.it/ca3/qc/CA.crt
Subject Key Identifier:	key identifier (sha1 (160 bit) of public key)
SubjectDirectoryAttributes	
DateOfBirth	
Subject Alternative Name	
RFC822Name	*certificate holder e-mail*
Certificate Policies:	
Policy 1:	
Policy ID:	0.4.0.194112.1.2
Policy 2:	
Policy ID:	• 1.3.76.36.1.1.61 • 1.3.76.36.1.1.62 • 1.3.76.36.1.1.63 • 1.3.76.36.1.1.66
Policy Qualifier ID:	cps (id-qt-cps)
CPS uri:	http://www.firma.infocert.it/documentazione/manuali.php
ETSI extensions: qcStatement-1 (QcCompliance) ::= 0.4.0.1862.1.1	
ETSI extensions: qcStatement-2 (QcEuLimitValue) ::= 0.4.0.1862.1.2	*(optional)*

ETSI extensions: QCStatement-3 (QcEURetentionPeriod)::= 0.4.0.1862.1.3	20
ETSI extensions: qcStatement-4 (QcSSCD)::= 0.4.0.1862.1.4	
ETSI extensions: qcStatement-5 (QcEuPDS)::= 0.4.0.1862.1.5	*PDS URL and LANGUAGE*
ETSI extensions: qcStatement-6 (QcType)::= 0.4.0.1862.1.6	id-etsi-qct-esign
RFC3739 extensions: qcStatement-2 (pkixQCSyntax-v2)::= 1.3.6.1.5.5.7.0.18.11.2	id-etsi-qcs-semanticsId-Natural (0.4.0.194121.1.1) *(mandatory)* id-etsi-qcs-SemanticsId-Legal (0.4.0.194121.1.2) *(optional)*
SIGNATURE:	
ALG. ID:	id-sha256-with-rsa-encryption
PARAMETER:	0
VALUE:	Ca Signature
***(*)**: the pseudonym attribute shall not be present if the givenName and surname attributes are present*	
***(**)**: if givenName and surname or pseudonym attributes are not sufficient to ensure Subject name uniqueness within the context of the issuer, then the serialNumber attribute shall be present*	
***(***):** when a natural person subject is associated with an organization, the subject attributes may also identify such organization using attributes such as organizationName and organizationIdentifier*	
***(****):** if the organization attribute is present, contains more information about the organization itself. This attribute may appear, at most, four times.*	
***(*****):** if the organization attribute is present, contains the conuntry where the organization is based, otherwise the country where the subject lives*	
NB: xx = partitioned revocation list progressive numbering	

Certyfikat kwalifikowany dla osoby fizycznej BEZ identyfikatorów i kluczy semantycznych na urządzeniu QSCD, wystawiony przez root CA „InfoCert Qualified Electronic Signature CA 3"

Field	Value
VERSION:	3
SERIAL:	Allocated automatically by the Issuing CA
INNER SIGNATURE:	
ALG. ID:	id-sha256-with-rsa-encryption
PARAMETER:	0
ISSUER:	
Country Name:	IT
Organization Name:	InfoCert S.p.A.
Organizational Unit Name:	ified Trust Service Provider
Organization Identifier:	T-07945211006
Common Name:	InfoCert Qualified Electronic Signature CA 3
VALIDITY:	max 39 month
Not Before:	
Not After:	
SUBJECT:	
Country Name:	*CountryCode (ISO 3166) (mandatory)(*****)*
Organization Name:	*(conditioned presence)* ***(***)***
Organization Identifier:	*(conditioned presence)* ***(***)***
Organizational Unit	*(conditioned presence) (****)*
GivenName:	*Name (conditioned presence)* ***(*)***
Surname:	*Surname (conditioned presence)* ***(*)***
SerialNumber:	*(conditioned presence)* ***(**)***
Title	*Holder's specific qualification (optional)*
Locality	*(conditioned presence)* ***(****)***
DNQualifier	*Holder's identification code assigned by the Certification Authority, unique within the Certification Authority itself (mandatory)*
Pseudonym:	*(conditioned presence)* ***(*)***
Common Name	*name of the subject (recommended)*
PUBLIC KEY:	(key size is 2048 bits or higher)
ALGORITHM:	
ALG. ID:	id-rsa-encryption
PARAMETER:	0
MODULUS:	
EXPONENT:	
EXTENSIONS:	
Authority Key Identifier:	key identifier (sha1 160 bit) of Issuer Public Key
Key Usage*:	Non-Repudiation (critical)
CRL Distribution Points:	
Distribution Point 1:	

Uniform Resource ID1:	
http://crl.infocert.it/ca3/qc/CRLxx.crl	
Uniform Resource ID2:	
ldap://ldap.infocert.it/cn%3DInfoCert%20Qualified%20Electronic%20Signature%20CA%203%20CRLxx,ou%3DQualified%20Trust%20Service%20Provider,o%3DINFOCERT%20SPA,c%3DIT?certificateRevocationList	
Authority Information Access	
Access Method	1.3.6.1.5.5.7.48.1
Alternative Name	http://ocsp.qc.ca3.infocert.it
Access Method	1.3.6.1.5.5.7.48.2
Alternative Name	http://cert.infocert.it/ca3/qc/CA.crt
Subject Key Identifier:	key identifier (sha1 (160 bit) of public key)
SubjectDirectoryAttributes	
DateOfBirth	
Subject Alternative Name	
RFC822Name	*certificate holder e-mail*
Certificate Policies:	
Policy 1:	
Policy ID:	0.4.0.194112.1.2
Policy 2:	
Policy ID:	• 1.3.76.36.1.1.61 • 1.3.76.36.1.1.62 • 1.3.76.36.1.1.63 • 1.3.76.36.1.1.66
Policy Qualifier ID:	cps (id-qt-cps)
CPS uri:	http://www.firma.infocert.it/documentazione/manuali.php
ETSI extensions: qcStatement-1 (QcCompliance) ::= 0.4.0.1862.1.1	
ETSI extensions: qcStatement-2 (QcEuLimitValue) ::= 0.4.0.1862.1.2	*(optional)*
ETSI extensions: QCStatement-3 (QcEURetentionPeriod)::= 0.4.0.1862.1.3	20
ETSI extensions: qcStatement-4 (QcSSCD)::= 0.4.0.1862.1.4	

ETSI extensions: qcStatement-5 (QcEuPDS)::= 0.4.0.1862.1.5	*PDS URL and LANGUAGE*
ETSI extensions: qcStatement-6 (QcType)::= 0.4.0.1862.1.6	id-etsi-qct-esign
SIGNATURE:	
ALG. ID:	id-sha256-with-rsa-encryption
PARAMETER:	0
VALUE:	Ca Signature
***(*)**: the pseudonym attribute shall not be present if the givenName and surname attributes are present*	
***(**)**: if givenName and surname or pseudonym attributes are not sufficient to ensure Subject name uniqueness within the context of the issuer, then the serialNumber attribute shall be present*	
***(***):** when a natural person subject is associated with an organization, the subject attributes may also identify such organization using attributes such as organizationName and organizationIdentifier*	
***(****):** if the organization attribute is present, contains more information about the organization itself. This attribute may appear, at most, four times.*	
***(*****):** if the organization attribute is present, contains the conuntry where the organization is based, otherwise the country where the subject live*	
NB: xx = partitioned revocation list progressive numbering	

Certyfikat kwalifikowany dla osoby fizycznej BEZ identyfikatorów i kluczy semantycznych na urządzeniu QSCD, wystawiony przez root CA „InfoCert Podpis Kwalifikowany 2"

Field	Value
VERSION:	3
SERIAL:	Allocated automatically by the Issuing CA
INNER SIGNATURE:	
ALG. ID:	id-sha256-with-rsa-encryption
PARAMETER:	0
ISSUER:	
Country Name:	IT
Organization Name:	INFOCERT SPA
Organizational Unit Name:	ficatore Accreditato
serialNumber	5211006
Common Name:	InfoCert Firma Qualificata 2
VALIDITY:	max 39 month
Not Before:	
Not After:	
SUBJECT:	
Country Name:	*CountryCode (ISO 3166) (mandatory) (*****)*
Organization Name:	*(conditioned presence)* ***(***)***
Organization Identifier:	*(conditioned presence)* ***(***)***
Organizational Unit	*(conditioned presence) (****)*
GivenName:	*Name (conditioned presence)* ***(*)***
Surname:	*Surname (conditioned presence)* ***(*)***
SerialNumber:	*(conditioned presence)* ***(**)***
Title	*Holder's specific qualification (optional)*
Locality	*(conditioned presence)* ***(****)***
DNQualifier	Holder's identification code assigned by the Certification Authority, unique within the Certification Authority itself (mandatory)
Pseudonym:	*(conditioned presence)* ***(*)***
Common Name	*name of the subject (recommended)*
PUBLIC KEY:	(key size is 2048 bits or higher)
ALGORITHM:	
ALG. ID:	id-rsa-encryption
PARAMETER:	0
MODULUS:	
EXPONENT:	
EXTENSIONS:	
Authority Key Identifier:	key identifier (sha1 160 bit) of Issuer Public Key
Key Usage*:	Non-Repudiation (critical)
CRL Distribution Points:	
Distribution Point 1:	
Uniform Resource ID1:	
http://crl.infocert.it/crls/firma2/CRLxx.crl	

Uniform Resource ID2:	
URI = ldap://ldap.infocert.it/cn%3DInfoCert%20Firma%20Qualificata%202%20CRL05,ou%3DCertificatore%20Accreditato,o%3DINFOCERT%20SPA,c%3DIT?certificateRevocationList	
Authority Information Access	
Access Method	1.3.6.1.5.5.7.48.1
Alternative Name	http://ocsp.sc.infocert.it/
Access Method	1.3.6.1.5.5.7.48.2
Alternative Name	http://cert.infocert.it/ca2/firma2/CA.crt
Subject Key Identifier:	key identifier (sha1 (160 bit) of public key)
SubjectDirectoryAttributes	
DateOfBirth	
Subject Alternative Name	
RFC822Name	*certificate holder e-mail*
Certificate Policies:	
Policy 1:	
Policy ID:	0.4.0.194112.1.2
Policy 2:	
Policy ID:	• 1.3.76.36.1.1.1 (firma qualificata) • 1.3.76.36.1.1.2 (firma qualificata automatica) • 1.3.76.36.1.1.22 (firma qualificata remota) • 1.3.76.36.1.1.32 (firma qualificata CMS)
Policy Qualifier ID:	cps (id-qt-cps)
CPS uri:	http://www.firma.infocert.it/documentazione/manuali.php
ETSI extensions: qcStatement-1 (QcCompliance) ::= 0.4.0.1862.1.1	
ETSI extensions: qcStatement-2 (QcEuLimitValue) ::= 0.4.0.1862.1.2	*(optional)*
ETSI extensions: QCStatement-3 (QcEURetentionPeriod)::= 0.4.0.1862.1.3	20
ETSI extensions: qcStatement-4 (QcSSCD)::= 0.4.0.1862.1.4	

ETSI extensions: qcStatement-5 (QcEuPDS)::= 0.4.0.1862.1.5	*PDS URL and LANGUAGE*
ETSI extensions: qcStatement-6 (QcType)::= 0.4.0.1862.1.6	id-etsi-qct-esign
SIGNATURE:	
ALG. ID:	id-sha256-with-rsa-encryption
PARAMETER:	0
VALUE:	Ca Signature
***(*)**: the pseudonym attribute shall not be present if the givenName and surname attributes are present*	
***(**)**: if givenName and surname or pseudonym attributes are not sufficient to ensure Subject name uniqueness within the context of the issuer, then the serialNumber attribute shall be present*	
***(***):** when a natural person subject is associated with an organization, the subject attributes may also identify such organization using attributes such as organizationName and organizationIdentifier*	
***(****):** if the organization attribute is present, contains more information about the organization itself. This attribute may appear, at most, four times.*	
***(*****):** if the organization attribute is present, contains the conuntry where the organization is based, otherwise the country where the subject live*	
NB: xx = partitioned revocation list progressive numbering	

Certyfikat kwalifikowany dla osoby fizycznej z identyfikatorami oraz kluczami semantycznymi

Field	Value
VERSION:	3
SERIAL:	Allocated automatically by the Issuing CA
INNER SIGNATURE:	
ALG. ID:	id-sha256-with-rsa-encryption
PARAMETER:	0
ISSUER:	
Country Name:	IT
Organization Name:	InfoCert S.p.A.
Organizational Unit Name:	ified Trust Service Provider
Organization Identifier:	T-07945211006
Common Name:	InfoCert Qualified Electronic Signature CA 3
VALIDITY:	max 39 month
Not Before:	
Not After:	
SUBJECT:	
Country Name:	*CountryCode (ISO 3166) (mandatory) (*****)*
Organization Name:	*(conditioned presence) **(***)***
Organization Identifier:	*(conditioned presence) **(***)** as defined in clause 5.1.4 of ETSI EN 319 412-1 (i.e. "**VATIT-***TaxIdentificationNumber*", "**NTRIT-***IdentifierNationalTradeRegister*")*
Organizational Unit	*(conditioned presence) (****)*
GivenName:	*Name (conditioned presence) **(*)***

Surname:	*Surname (conditioned presence) **(*)***
SerialNumber:	*(conditioned presence) **(**)** as defined in clause 5.1.3 of ETSI EN 319 412-1 (i.e. "**TINI**T-Codicefiscale", "**PASIT-**PassportNumber", "**IDCIT-**IdentityCardNumber")*
Title	*Holder's specific qualification (optional)*
Locality	*(conditioned presence) **(****)***
DNQualifier	Holder's identification code assigned by the Certification Authority, unique within the Certification Authority itself (mandatory)
Pseudonym:	*(conditioned presence) **(*)***
Common Name	*name of the subject (recommended)*
PUBLIC KEY:	(key size is 2048 bits or higher)
ALGORITHM:	
ALG. ID:	id-rsa-encryption
PARAMETER:	0
MODULUS:	
EXPONENT:	
EXTENSIONS:	
Authority Key Identifier:	key identifier (sha1 160 bit) of Issuer Public Key
Key Usage*:	Non-Repudiation (critical)
CRL Distribution Points:	
Distribution Point 1:	
Uniform Resource ID1:	
http://crl.infocert.it/ca3/qc/CRLxx.crl	
Uniform Resource ID2:	
ldap://ldap.infocert.it/cn%3DInfoCert%20Qualified%20Electronic%20Signature%20CA%203%20CRLxx,ou%3DQualified%20Trust%20Service%20Provider,o%3DINFOCERT%20SPA,c%3DIT?certificateRevocationList	
Authority Information Access	
Access Method	1.3.6.1.5.5.7.48.1
Alternative Name	http://ocsp.qc.ca3.infocert.it
Access Method	1.3.6.1.5.5.7.48.2
Alternative Name	http://cert.infocert.it/ca3/qc/CA.crt
Subject Key Identifier:	key identifier (sha1 (160 bit) of public key)
SubjectDirectoryAttributes	
DateOfBirth	
Subject Alternative Name	
RFC822Name	*certificate holder e-mail*
Certificate Policies:	
Policy 1:	
Policy ID:	0.4.0.194112.1.0
Policy 2:	

Policy ID:	1.3.76.36.1.1.48
Policy Qualifier ID:	cps (id-qt-cps)
CPS uri:	http://www.firma.infocert.it/documentazione/manuali.php
ETSI extensions: qcStatement-1 (QcCompliance) ::= 0.4.0.1862.1.1	
ETSI extensions: qcStatement-2 (QcEuLimitValue) ::= 0.4.0.1862.1.2	*(optional)*
ETSI extensions: QCStatement-3 (QcEURetentionPeriod)::= 0.4.0.1862.1.3	20
ETSI extensions: qcStatement-5 (QcEuPDS)::= 0.4.0.1862.1.5	*PDS URL and LANGUAGE*
ETSI extensions: qcStatement-6 (QcType)::= 0.4.0.1862.1.6	id-etsi-qct-esign
RFC3739 extensions: qcStatement-2 (pkixQCSyntax-v2)::= 1.3.6.1.5.5.7.0.18.11.2	id-etsi-qcs-semanticsId-Natural (0.4.0.194121.1.1) *(mandatory)* id-etsi-qcs-SemanticsId-Legal (0.4.0.194121.1.2) *(optional)*
SIGNATURE:	
ALG. ID:	id-sha256-with-rsa-encryption
PARAMETER:	0
VALUE:	Ca Signature

(*): the pseudonym attribute shall not be present if the givenName and surname attributes are present

(**): if givenName and surname or pseudonym attributes are not sufficient to ensure Subject name uniqueness within the context of the issuer, then the serialNumber attribute shall be present

(***): when a natural person subject is associated with an organization, the subject attributes may also identify such organization using attributes such as organizationName and organizationIdentifier

(****): if the organization attribute is present, contains more information about the organization itself. This attribute may appear, at most, four times.

(*****): if the organization attribute is present, contains the conuntry where the organization is based, otherwise the country where the subject live

NB: xx = partitioned revocation list progressive numbering

Certyfikat kwalifikowany dla osoby fizycznej BEZ identyfikatorów i kluczy semantycznych

Field	Value
VERSION:	3
SERIAL:	Allocated automatically by the Issuing CA
INNER SIGNATURE:	
ALG. ID:	id-sha256-with-rsa-encryption
PARAMETER:	0
ISSUER:	
Country Name:	IT
Organization Name:	InfoCert S.p.A.
Organizational Unit Name:	ified Trust Service Provider
Organization Identifier:	T-07945211006
Common Name:	InfoCert Qualified Electronic Signature CA 3
VALIDITY:	max 39 month
Not Before:	
Not After:	
SUBJECT:	
Country Name:	*CountryCode (ISO 3166) (mandatory) (*****)*
Organization Name:	*(conditioned presence)* ***(***)***
Organization Identifier:	*(conditioned presence)* ***(***)***
Organizational Unit	*(conditioned presence) (****)*
GivenName:	*Name (conditioned presence)* ***(*)***
Surname:	*Surname (conditioned presence)* ***(*)***
SerialNumber:	*(conditioned presence)* ***(**)***
Title	*Holder's specific qualification (optional)*
Locality	*(conditioned presence)* ***(****)***
DNQualifier	Holder's identification code assigned by the Certification Authority, unique within the Certification Authority itself (mandatory)
Pseudonym:	*(conditioned presence)* ***(*)***
Common Name	*name of the subject (recommended)*
PUBLIC KEY:	(key size is 2048 bits or higher)
ALGORITHM:	
ALG. ID:	id-rsa-encryption
PARAMETER:	0
MODULUS:	
EXPONENT:	
EXTENSIONS:	
Authority Key Identifier:	key identifier (sha1 160 bit) of Issuer Public Key
Key Usage*:	Non-Repudiation (critical)
CRL Distribution Points:	
Distribution Point 1:	
Uniform Resource ID1:	
http://crl.infocert.it/ca3/qc/CRLxx.crl	
Uniform Resource ID2:	

ldap://ldap.infocert.it/cn%3DInfoCert%20Qualified%20Electronic%20Signature%20CA%203%20CRLxx,ou%3DQualified%20Trust%20Service%20Provider,o%3DINFOCERT%20SPA,c%3DIT?certificateRevocationList	
Authority Information Access	
Access Method	1.3.6.1.5.5.7.48.1
Alternative Name	http://ocsp.qc.ca3.infocert.it
Access Method	1.3.6.1.5.5.7.48.2
Alternative Name	http://cert.infocert.it/ca3/qc/CA.crt
Subject Key Identifier:	key identifier (sha1 (160 bit) of public key)
SubjectDirectoryAttributes	
DateOfBirth	
Subject Alternative Name	
RFC822Name	*certificate holder e-mail*
Certificate Policies:	
Policy 1:	
Policy ID:	0.4.0.194112.1.0
Policy 2:	
Policy ID:	1.3.76.36.1.1.48
Policy Qualifier ID:	cps (id-qt-cps)
CPS uri:	http://www.firma.infocert.it/documentazione/manuali.php
ETSI extensions: qcStatement-1 (QcCompliance) ::= 0.4.0.1862.1.1	
ETSI extensions: qcStatement-2 (QcEuLimitValue) ::= 0.4.0.1862.1.2	*(optional)*
ETSI extensions: QCStatement-3 (QcEURetentionPeriod)::= 0.4.0.1862.1.3	20
ETSI extensions: qcStatement-5 (QcEuPDS)::= 0.4.0.1862.1.5	*PDS URL and LANGUAGE*
ETSI extensions: qcStatement-6 (QcType)::= 0.4.0.1862.1.6	id-etsi-qct-esign
SIGNATURE:	
ALG. ID:	id-sha256-with-rsa-encryption

PARAMETER:	0
VALUE:	Ca Signature
(*): the pseudonym attribute shall not be present if the givenName and surname attributes are present	
(**): if givenName and surname or pseudonym attributes are not sufficient to ensure Subject name uniqueness within the context of the issuer, then the serialNumber attribute shall be present	
(***): when a natural person subject is associated with an organization, the subject attributes may also identify such organization using attributes such as organizationName and organizationIdentifier	
(****): if the organization attribute is present, contains more information about the organization itself. This attribute may appear, at most, four times.	
(*****): if the organization attribute is present, contains the conuntry where the organization is based, otherwise the country where the subject live	
NB: xx = partitioned revocation list progressive numbering	

Certyfikat kwalifikowany dla osoby prawnej z identyfikatorami oraz kluczami semantycznymi

Field	Value
VERSION:	3
SERIAL:	Allocated automatically by the Issuing CA
INNER SIGNATURE:	
ALG. ID:	id-sha256-with-rsa-encryption
PARAMETER:	0
ISSUER:	
Country Name:	IT
Organization Name:	InfoCert S.p.A.
Organizational Unit Name:	ified Trust Service Provider
Organization Identifier:	T-07945211006
Common Name:	InfoCert Qualified Electronic Signature CA 3
VALIDITY:	max 3 years
Not Before:	
Not After:	
SUBJECT:	
Country Name:	*CountryCode (ISO 3166) (mandatory)*
Organization Name:	*full registered name of the subject (legal person) (mandatory)*
Organization Identifier:	*as defined in clause 5.1.4 of ETSI EN 319 412-1 (i.e. "***VATIT-***TaxIdentificationNumber", "***NTRIT-***IdentifierNationalTradeRegister") (mandatory)*
Common Name	*name of the subject (legal person) (mandatory)*
PUBLIC KEY:	(key size is 2048 bits or higher)
ALGORITHM:	
ALG. ID:	id-rsa-encryption
PARAMETER:	0
MODULUS:	
EXPONENT:	
EXTENSIONS:	
Authority Key Identifier:	key identifier (sha1 160 bit) of Issuer Public Key

Key Usage*:	Non-Repudiation (critical)
CRL Distribution Points:	
Distribution Point 1:	
Uniform Resource ID1:	
http://crl.infocert.it/ca3/qc/CRLxx.crl	
Uniform Resource ID2:	
ldap://ldap.infocert.it/cn%3DInfoCert%20Qualified%20Electronic%20Signature%20CA%203%20CRLxx,ou%3DQualified%20Trust%20Service%20Provider,o%3DINFOCERT%20SPA,c%3DIT?certificateRevocationList	
Authority Information Access	
Access Method	1.3.6.1.5.5.7.48.1
Alternative Name	http://ocsp.qc.ca3.infocert.it
Access Method	1.3.6.1.5.5.7.48.2
Alternative Name	http://cert.infocert.it/ca3/qc/CA.crt
Subject Key Identifier:	key identifier (sha1 (160 bit) of public key)
SubjectDirectoryAttributes	
DateOfBirth	
Subject Alternative Name	
RFC822Name	*certificate holder e-mail*
Certificate Policies:	
Policy 1:	
Policy ID:	0.4.0.194112.1.1
Policy 2:	
Policy ID:	1.3.76.36.1.1.47
Policy Qualifier ID:	cps (id-qt-cps)
CPS uri:	http://www.firma.infocert.it/documentazione/manuali.php
ETSI extensions: qcStatement-1 (QcCompliance) ::= 0.4.0.1862.1.1	
ETSI extensions: qcStatement-2 (QcEuLimitValue) ::= 0.4.0.1862.1.2	*(optional)*
ETSI extensions: QCStatement-3 (QcEURetentionPeriod)::= 0.4.0.1862.1.3	20

ETSI extensions: qcStatement-5 (QcEuPDS)::= 0.4.0.1862.1.5	*PDS URL and LANGUAGE*
ETSI extensions: qcStatement-6 (QcType)::= 0.4.0.1862.1.6	id-etsi-qct-eseal
RFC3739 extensions: qcStatement-2 (pkixQCSyntax-v2)::= 1.3.6.1.5.5.7.0.18.11.2	id-etsi-qcs-SemanticsId-Legal (0.4.0.194121.1.2) *(mandatory)*
SIGNATURE:	
ALG. ID:	id-sha256-with-rsa-encryption
PARAMETER:	0
VALUE:	Ca Signature
NB: xx = partitioned revocation list progressive numbering	

Certyfikat kwalifikowany dla osoby prawnej BEZ identyfikatorów i kluczy semantycznych

Field	Value
VERSION:	3
SERIAL:	Allocated automatically by the Issuing CA
INNER SIGNATURE:	
ALG. ID:	id-sha256-with-rsa-encryption
PARAMETER:	0
ISSUER:	
Country Name:	IT
Organization Name:	InfoCert S.p.A.
Organizational Unit Name:	ified Trust Service Provider
Organization Identifier:	T-07945211006
Common Name:	InfoCert Qualified Electronic Signature CA 3
VALIDITY:	max 3 years
Not Before:	
Not After:	
SUBJECT:	
Country Name:	*CountryCode (ISO 3166) (mandatory)*
Organization Name:	*full registered name of the subject (legal person) (mandatory)*
Organization Identifier:	*identification of the subject organization different from the organization name (mandatory)*
Common Name	*name of the subject (legal person) (mandatory)*
PUBLIC KEY:	(key size is 2048 bits or higher)
ALGORITHM:	
ALG. ID:	id-rsa-encryption
PARAMETER:	0
MODULUS:	
EXPONENT:	
EXTENSIONS:	
Authority Key Identifier:	key identifier (sha1 160 bit) of Issuer Public Key
Key Usage*:	Non-Repudiation (critical)
CRL Distribution Points:	
Distribution Point 1:	
Uniform Resource ID1:	
http://crl.infocert.it/ca3/qc/CRLxx.crl	
Uniform Resource ID2:	
ldap://ldap.infocert.it/cn%3DInfoCert%20Qualified%20Electronic%20Signature%20CA%203%20CRLxx,ou%3DQualified%20Trust%20Service%20Provider,o%3DINFOCERT%20SPA,c%3DIT?certificateRevocationList	
Authority Information Access	
Access Method	1.3.6.1.5.5.7.48.1
Alternative Name	http://ocsp.qc.ca3.infocert.it

Access Method	1.3.6.1.5.5.7.48.2
Alternative Name	http://cert.infocert.it/ca3/qc/CA.crt
Subject Key Identifier:	key identifier (sha1 (160 bit) of public key)
SubjectDirectoryAttributes	
DateOfBirth	
Subject Alternative Name	
RFC822Name	*certificate holder e-mail*
Certificate Policies:	
Policy 1:	
Policy ID:	0.4.0.194112.1.1
Policy 2:	
Policy ID:	1.3.76.36.1.1.47
Policy Qualifier ID:	cps (id-qt-cps)
CPS uri:	http://www.firma.infocert.it/documentazione/manuali.php
ETSI extensions: qcStatement-1 (QcCompliance) ::= 0.4.0.1862.1.1	
ETSI extensions: qcStatement-2 (QcEuLimitValue) ::= 0.4.0.1862.1.2	*(optional)*
ETSI extensions: QCStatement-3 (QcEURetentionPeriod)::= 0.4.0.1862.1.3	20
ETSI extensions: qcStatement-5 (QcEuPDS)::= 0.4.0.1862.1.5	*PDS URL and LANGUAGE*
ETSI extensions: qcStatement-6 (QcType)::= 0.4.0.1862.1.6	id-etsi-qct-eseal
SIGNATURE:	
ALG. ID:	id-sha256-with-rsa-encryption
PARAMETER:	0
VALUE:	Ca Signature
NB: xx = partitioned revocation list progressive numbering	

Certyfikat kwalifikowany dla osoby prawnej z identyfikatorami oraz kluczami semantycznymi na urządzeniu QSCD

Field	Value
VERSION:	3
SERIAL:	Allocated automatically by the Issuing CA
INNER SIGNATURE:	
ALG. ID:	id-sha256-with-rsa-encryption
PARAMETER:	0
ISSUER:	
Country Name:	IT
Organization Name:	InfoCert S.p.A.
Organizational Unit Name:	ified Trust Service Provider
Organization Identifier:	T-07945211006
Common Name:	InfoCert Qualified Electronic Signature CA 3
VALIDITY:	max 3 years
Not Before:	
Not After:	
SUBJECT:	
Country Name:	*CountryCode (ISO 3166) (mandatory)*
Organization Name:	*full registered name of the subject (legal person) (mandatory)*
Organization Identifier:	*as defined in clause 5.1.4 of ETSI EN 319 412-1 (i.e. "**VATIT-**TaxIdentificationNumber", "**NTRIT-**IdentifierNationalTradeRegister") (mandatory)*
Common Name	*name of the subject (legal person) (mandatory)*
PUBLIC KEY:	(key size is 2048 bits or higher)
ALGORITHM:	
ALG. ID:	id-rsa-encryption
PARAMETER:	0
MODULUS:	
EXPONENT:	
EXTENSIONS:	
Authority Key Identifier:	key identifier (sha1 160 bit) of Issuer Public Key
Key Usage*:	Non-Repudiation (critical)
CRL Distribution Points:	
Distribution Point 1:	
Uniform Resource ID1:	
http://crl.infocert.it/ca3/qc/CRLxx.crl	
Uniform Resource ID2:	
ldap://ldap.infocert.it/cn%3DInfoCert%20Qualified%20Electronic%20Signature%20CA%203%20CRLxx,ou%3DQualified%20Trust%20Service%20Provider,o%3DINFOCERT%20SPA,c%3DIT?certificateRevocationList	
Authority Information Access	
Access Method	1.3.6.1.5.5.7.48.1

Alternative Name	http://ocsp.qc.ca3.infocert.it
Access Method	1.3.6.1.5.5.7.48.2
Alternative Name	http://cert.infocert.it/ca3/qc/CA.crt
Subject Key Identifier:	key identifier (sha1 (160 bit) of public key)
SubjectDirectoryAttributes	
DateOfBirth	
Subject Alternative Name	
RFC822Name	*certificate holder e-mail*
Certificate Policies:	
Policy 1:	
Policy ID:	0.4.0.194112.1.1
Policy 2:	
Policy ID:	1.3.76.36.1.1.46
Policy Qualifier ID:	cps (id-qt-cps)
CPS uri:	http://www.firma.infocert.it/documentazione/manuali.php
ETSI extensions: qcStatement-1 (QcCompliance) ::= 0.4.0.1862.1.1	
ETSI extensions: qcStatement-2 (QcEuLimitValue) ::= 0.4.0.1862.1.2	*(optional)*
ETSI extensions: QCStatement-3 (QcEURetentionPeriod)::= 0.4.0.1862.1.3	20
ETSI extensions: qcStatement-4 (QcSSCD)::= 0.4.0.1862.1.4	
ETSI extensions: qcStatement-5 (QcEuPDS)::= 0.4.0.1862.1.5	*PDS URL and LANGUAGE*
ETSI extensions: qcStatement-6 (QcType)::= 0.4.0.1862.1.6	id-etsi-qct-eseal
RFC3739 extensions: qcStatement-2 (pkixQCSyntax-v2)::= 1.3.6.1.5.5.7.0.18.11.2	id-etsi-qcs-SemanticsId-Legal (0.4.0.194121.1.2) *(mandatory)*
SIGNATURE:	
ALG. ID:	id-sha256-with-rsa-encryption

PARAMETER:	0
VALUE:	Ca Signature
NB: xx = partitioned revocation list progressive numbering	

Certyfikat kwalifikowany dla osoby prawnej BEZ identyfikatorów i kluczy semantycznych na urządzeniu QSCD

Field	Value
VERSION:	3
SERIAL:	Allocated automatically by the Issuing CA
INNER SIGNATURE:	
ALG. ID:	id-sha256-with-rsa-encryption
PARAMETER:	0
ISSUER:	
Country Name:	IT
Organization Name:	InfoCert S.p.A.
Organizational Unit Name:	ified Trust Service Provider
Organization Identifier:	T-07945211006
Common Name:	InfoCert Qualified Electronic Signature CA 3
VALIDITY:	max 3 years
Not Before:	
Not After:	
SUBJECT:	
Country Name:	*CountryCode (ISO 3166) (mandatory)*
Organization Name:	*full registered name of the subject (legal person) (mandatory)*
Organization Identifier:	*identification of the subject organization different from the organization name (mandatory)*
Common Name	*name of the subject (legal person) (mandatory)*
PUBLIC KEY:	(key size is 2048 bits or higher)
ALGORITHM:	
ALG. ID:	id-rsa-encryption
PARAMETER:	0
MODULUS:	
EXPONENT:	
EXTENSIONS:	
Authority Key Identifier:	key identifier (sha1 160 bit) of Issuer Public Key
Key Usage*:	Non-Repudiation (critical)
CRL Distribution Points:	
Distribution Point 1:	
Uniform Resource ID1:	
http://crl.infocert.it/ca3/qc/CRLxx.crl	
Uniform Resource ID2:	
ldap://ldap.infocert.it/cn%3DInfoCert%20Qualified%20Electronic%20Signature%20CA%203%20CRLxx,ou%3DQualified%20Trust%20Service%20Provider,o%3DINFOCERT%20SPA,c%3DIT?certificateRevocationList	
Authority Information Access	
Access Method	1.3.6.1.5.5.7.48.1
Alternative Name	http://ocsp.qc.ca3.infocert.it

Access Method	1.3.6.1.5.5.7.48.2
Alternative Name	http://cert.infocert.it/ca3/qc/CA.crt
Subject Key Identifier:	key identifier (sha1 (160 bit) of public key)
SubjectDirectoryAttributes	
DateOfBirth	
Subject Alternative Name	
RFC822Name	*certificate holder e-mail*
Certificate Policies:	
Policy 1:	
Policy ID:	0.4.0.194112.1.1
Policy 2:	
Policy ID:	1.3.76.36.1.1.46
Policy Qualifier ID:	cps (id-qt-cps)
CPS uri:	http://www.firma.infocert.it/documentazione/manuali.php
ETSI extensions: qcStatement-1 (QcCompliance) ::= 0.4.0.1862.1.1	
ETSI extensions: qcStatement-2 (QcEuLimitValue) ::= 0.4.0.1862.1.2	*(optional)*
ETSI extensions: QCStatement-3 (QcEURetentionPeriod)::= 0.4.0.1862.1.3	20
ETSI extensions: qcStatement-4 (QcSSCD)::= 0.4.0.1862.1.4	
ETSI extensions: qcStatement-5 (QcEuPDS)::= 0.4.0.1862.1.5	*PDS URL and LANGUAGE*
ETSI extensions: qcStatement-6 (QcType)::= 0.4.0.1862.1.6	id-etsi-qct-eseal
SIGNATURE:	
ALG. ID:	id-sha256-with-rsa-encryption
PARAMETER:	0
VALUE:	Ca Signature
NB: xx = partitioned revocation list progressive numbering	

Format list CRL oraz OCSP

Rozszerzenie	Wartość
Issuer Signature Algorithm	sha-256WithRSAEncryption [1 2 840 113549 1 1 11]
Issuer Distinguished Name	InfoCert
thisUpdate	Data w formacie UTC
nextUpdate	Data następnej listy CRL In format
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 oraz protokołów OCSP

Listy CRL mają następujące rozszerzenia

Extension	Value
Authority Key Identifier	Wartość odcisku 160-bit SHA-1 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: informuje, 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 certyfikat przestaje być ważny

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]
Issuer Name Hash	Hash DN (Distinguished Name) 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 wygenerowania odpowiedzi OCSP
Hash Algorithm	sha-1 [1 3 14 3 2 26] OR sha-256 [2 16 840 1 101 3 4 2 1]

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	sha-256WithRSAEncryption [1 2 840 113549 1 1 11]
Issuer's Signature	[OCSP response Signature]
Issuer certificate	[OCSP response signing certificate]

Żądanie OCSP może zawierać następujące rozszerzenia:

Extension	Value
nonce	Dowolny numer jednorazowego użytku. Kryptograficznie łączy żądanie z odpowiedzią w celu niedopuszczenia do ataków przez ponawianie. W przypadku żądania numer ten zawarty jest w requestExtensions, natomiast w przypadku odpowiedzi może być zawarty w responseExtensions.

Appendice B Narzędzia i zasady składania oraz weryfikacji podpisu cyfrowego

InfoCert udostępnia darmowy produkt o nazwie „Dike”, który posiadacze certyfikatu mogą pobrać ze strony www.firma.infocert.it, umożliwiający:

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

Środowiska, w których pracuje Dike, oraz wymagania dot. sprzętu i oprogramowania, a także wszelkie instrukcje dot. procedury instalowania produktu dostępne są na ww. stronie internetowej. Instrukcje dot. korzystania z produktu zawarte są w samym produkcie i można z nich skorzystać przy użyciu funkcji pomocy. Produkt Dike może służyć do podpisywania każdego rodzaju pliku. Możliwość wizualizacji pliku zależy od dostępności odpowiedniego oprogramowania do wizualizacji na stanowisku pracy użytkownika.

InfoCert może udostępnić, za odpowiednią opłatą i zgodnie z ustaleniami w odrębnych porozumieniach handlowych zawartych z punktami rejestracji (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 także przy użyciu innych narzędzi, obsługujące uzgodnione wcześniej formaty podpisów. InfoCert nie bierze odpowiedzialności za narzędzia, o których mowa powyżej.

Np. dokumenty podpisane z wykorzystaniem certyfikatów wystawionych w świetle niniejszej Polityki, w formacie PAdES, można zweryfikować także za pomocą Adobe Reader®.

Ostrzeżenie

Niektóre formaty pozwalają wprowadzić do dokumentu wykonywalny kod (makro lub polecenie), bez naruszania jego struktury binarnej, umożliwiający aktywację funkcji zmieniających informacje zawarte w tym dokumencie. Podpis cyfrowy złożony w plikach zawierających wspomniane elementy nie ma skutków, o których mowa w art. 25 ust. 2 rozporządzenia [1], tj. nie jest równoważny podpisowi własnoręcznemu. W gestii posiadacza certyfikatu jest upewnienie się, za pośrednictwem funkcji właściwych dla danego produktu, że dokument nie zawiera takiego kodu wykonywalnego.