In.Te.S.A. S.p.A.

Dostawca kwalifikowanych usług zaufania

Kodeks postępowania certyfikacyjnego w zakresie procedur zdalnego kwalifikowanego podpisu elektronicznego w usługach bankowych i finansowych

Kod dokumentu: MO_REMBAN

OID: 1.3.76.21.1.50.110

Sporządził: Antonio Raia

Zatwierdził: Franco Tafini

Data wydania: 1.07.2019 r.

Wersja: 04

Podpisał:
ANTONIO RAIA
Organizacja: IN.TE.S.A. S.p.A.

WERSJE

Nr wersji: 04		***Data przeglądu:***	***01.07.2019 r.***
Opis zmian:	Zmiana danych spółki i logo Aktualizacja definicji i odniesień prawnych Aktualizacja układu graficznego Wprowadzenie procedury podpisu dla klienta Prospect (I.2.3)		
Uzasadnienie:	Aktualizacja przepisów: rozporządzenie (UE) 910/2014 (eIDAS), dekret legislacyjny 179/2016 (RODO) Zmiany organizacyjne TSP Nowa procedura pozyskiwania klienta		
Nr wersji: 03		***Data przeglądu:***	***13.06.2012 r.***
Opis zmian:	Rozszerzenie zakresu kodeksu na usługi finansowe (Instytucje płatnicze), a nie tylko bankowe		
Uzasadnienie:	Aktualizacja		
Nr wersji: 02		***Data przeglądu:***	***02.04.2012 r.***
Opis zmian:	B.4.2. – Wprowadzenie systemu weryfikacji tożsamości posiadacza (odpowiedniej weryfikacji) bez jego fizycznej obecności. C.5. – Wprowadzenie sposobów weryfikacji tożsamości posiadacza (odpowiedniej weryfikacji). F.1.3. – Wprowadzenie standardowego ograniczenia w stosowaniu. G. – Wprowadzenie sposobu przesyłania potwierdzeń za pośrednictwem poczty elektronicznej.		
Uzasadnienie:	Aktualizacja		
Nr wersji: 01		***Data przeglądu:***	***01.11.2011 r.***
Opis zmian:	brak		
Uzasadnienie:	pierwsze wydanie		

Spis treści

Odniesienia prawne

Tekst jednolity – DPR 445/00 z późniejszymi zmianami i uzupełnieniami	Dekret Prezydenta Republiki nr 445 z dnia 28 grudnia 2000 r. „Tekst jednolity przepisów ustawowych i wykonawczych w sprawie dokumentacji administracyjnej". Określany dalej również jako „t.j.".
CAD – DLGS 82/05 z późniejszymi zmianami i uzupełnieniami	Dekret legislacyjny nr 82 z dnia 7 marca 2005 r. „Kodeks administracji cyfrowej". Określany dalej również jako „CAD".
DPCM 22/02/2013 „Nowe przepisy techniczne" z późniejszymi zmianami i uzupełnieniami	Rozporządzenie Prezesa Rady Ministrów z dnia 22 lutego 2013 r. „Przepisy techniczne dotyczące generowania, składania i weryfikacji zaawansowanych, kwalifikowanych i cyfrowych podpisów elektronicznych, zgodnie z art. 20 ust. 3, art. 24 ust. 4, art. 28 ust. 3, art. 32 ust. 3 lit. b), art. 35 ust. 2, art. 36 ust. 2 i art. 71" (CAD – przypis redakcji). Określane dalej również jako „DPCM".
Rozporządzenie (UE) nr 910/2014 (eIDAS) z późniejszymi zmianami i uzupełnieniami	Rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 910/2014 z dnia 23 lipca 2104 r. w sprawie identyfikacji elektronicznej i usług zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznym oraz uchylające dyrektywę 1999/93/WE. Określane dalej również jako „eIDAS".
RODO Rozporządzenie o ochronie danych osobowych z późniejszymi zmianami i uzupełnieniami	Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych). Określane dalej również jako „RODO".
POSTANOWIENIE nr 147/2019 z późniejszymi zmianami i uzupełnieniami	Wytyczne Agencji ds. Cyfryzacji Włoch wprowadzające zasady i zalecenia techniczne dotyczące generowania kwalifikowanych certyfikatów elektronicznych, kwalifikowanych podpisów i pieczęci elektronicznych oraz kwalifikowanych elektronicznych znaczników czasu. Określane dalej również jako „*POSTANOWIENIE*".

Definicje i skróty

AgID	Agencja ds. Cyfryzacji Włoch (wł. *Agenzia per l'Italia Digitale*, zwana wcześniej CNIPA i DigitPA) – www.agid.gov.it. Organ nadzoru w rozumieniu rozporządzenia (UE) nr 910/2014 (eIDAS). Określana dalej również jako „Agencja".
QTSP *(ang. Qualified Trust Service Provider).* *Akredytowany organ certyfikujący*	*Dostawca kwalifikowanych usług zaufania*. Osoba fizyczna lub prawna, która świadczy przynajmniej jedną kwalifikowaną usługę zaufania. Zwany wcześniej „akredytowanym organem certyfikującym" zgodnie z CAD. W niniejszym dokumencie w charakterze QTSP występuje spółka In.Te.S.A. S.p.A.
Kwalifikowana usługa zaufania	Usługa elektroniczna świadczona przez QTSP obejmująca elementy określone w art. 3 pkt 16) i 17) rozporządzenia (UE) nr 910/2014 (eIDAS). W niniejszym dokumencie w charakterze QTSP występuje spółka In.Te.S.A. S.p.A., która świadczy kwalifikowane usługi podpisu elektronicznego i elektronicznego znacznika czasu oraz inne powiązane z nimi usługi.
Kwalifikowany 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. Jest on wydawany przez kwalifikowanego dostawcę usług zaufania i spełnia wymogi określone w załączniku I do rozporządzenia (UE) nr 910/2014 (eIDAS).
Klucz prywatny	Element pary kluczy asymetrycznych używany przez posiadacza, za pomocą którego kwalifikowany podpis elektroniczny składany jest na dokumencie informatycznym.
Klucz publiczny	Element pary kluczy asymetrycznych przeznaczony do upublicznienia, za pomocą którego weryfikuje się podpis cyfrowy złożony na dokumencie informatycznym.
CRL	Lista unieważnionych certyfikatów (ang. *Certificate Revocation List*), tj. lista zawierająca unieważnione lub zawieszone certyfikaty, uznane przez wydający je organ certyfikujący za nieważne.
OCSP	Usługa weryfikacji ważności certyfikatu zgodnie z protokołem OCSP (ang. *Online Certificate Status Protocol*).
Dokument informatyczny	Dokument elektroniczny zawierający odwzorowanie istotnych prawnie aktów, faktów lub informacji w formie informatycznej.

KPE – kwalifikowany podpis elektroniczny *PC – podpis cyfrowy*	Podpis elektroniczny składany za pomocą kwalifikowanego urządzenia do składania podpisu elektronicznego, który opiera się na kwalifikowanym certyfikacie podpisu elektronicznego. We Włoszech jest on równoznaczny z *podpisem cyfrowym*, który w rozumieniu art. 1 ust. 1 lit. s) CAD oznacza: kwalifikowany podpis elektroniczny oparty na systemie wzajemnie powiązanych kluczy kryptograficznych, jednego publicznego i jednego prywatnego, który umożliwia posiadaczowi złożenie podpisu przy zapewnieniu autentyczności pochodzenia i integralności dokumentu elektronicznego lub zestawu dokumentów elektronicznych za pomocą klucza prywatnego, a odbiorcy ich weryfikację za pomocą klucza publicznego.
Zdalny podpis	Specjalna procedura kwalifikowanego podpisu elektronicznego lub podpisu cyfrowego, wygenerowanego na urządzeniu HSM, przechowywanym i zarządzanym przez akredytowany organ certyfikujący na jego odpowiedzialność, która pozwala zapewnić wyłączną kontrolę nad kluczami prywatnymi ich posiadaczom.
HSM (ang. Hardware Security Module)	Urządzenia, które służą do składania kwalifikowanego podpisu elektronicznego, pod warunkiem, że spełniają wymagania określone w załączniku II do rozporządzenia (UE) nr 910/2014. Zwane również „urządzeniami do podpisu".
Znacznik czasu (ang. Qualified Electronic Time Stamp)	*Kwalifikowany elektroniczny znacznik czasu* oznacza 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. Spełnia wymagania art. 42 rozporządzenia eIDAS.
Urząd certyfikacji (CA, ang. Certification Authority)	Organ wydający certyfikaty podpisu elektronicznego.
Punkt rejestracji (RA, ang. Registration Authority)	*Punkt rejestracji* oznacza podmiot, który w imieniu QTSP jest odpowiedzialny za rejestrację i weryfikację informacji (w szczególności tożsamości posiadacza) niezbędnych QTSP do wydania certyfikatu kwalifikowanego.
Rejestr certyfikatów	Jedna lub kilka połączonych baz danych prowadzonych przez organ certyfikujący, zawierających wszystkie wydane certyfikaty.
Wnioskodawca	Osoba fizyczna składająca wniosek o wydanie certyfikatu.
Posiadacz	Osoba fizyczna, której wydano kwalifikowany certyfikat i która jest upoważniona do jego używania w celu składania własnego podpisu cyfrowego.
Klient *Klient Prospect*	Klient (lub potencjalny klient, nazywany „klientem Prospect") Banku / Instytucji finansowej.
Odniesienie czasowe	Informacja zawierająca datę i godzinę przypisywaną do jednego lub kilku dokumentów informatycznych.
Urząd znakowania czasem (TSA, ang. Time Stamping Authority)	Organ wydający elektroniczne znaczniki czasu.

A. Wprowadzenie

Niniejszy dokument stanowi *Kodeks postępowania certyfikacyjnego w zakresie procedur zdalnego kwalifikowanego podpisu elektronicznego w usługach bankowych i finansowych* (zwany dalej *Kodeksem postępowania certyfikacyjnego*) dostawcy kwalifikowanych usług zaufania (QTSP) In.Te.S.A. S.p.A.

Treść niniejszego Kodeksu postępowania certyfikacyjnego jest zgodna z przepisami technicznymi zawartymi w rozporządzeniu Prezesa Rady Ministrów z dnia 22 lutego 2013 r. (zwanym dalej „DPCM") oraz dekrecie legislacyjnym nr 82 z dnia 7 marca 2005 r. wprowadzającym kodeks administracji cyfrowej z późniejszymi zmianami i uzupełnieniami (zwanym dalej „CAD") i spełnia wymogi rozporządzenia (UE) nr 910/2014 (zwanego dalej „eIDAS").

W sprawach nieregulowanych w niniejszym Kodeksie postępowania certyfikacyjnego mają zastosowanie właściwe obowiązujące lub przyszłe przepisy dotyczące konkretnego przypadku.

W niniejszym dokumencie określono zasady i procedury operacyjne dostawcy kwalifikowanych usług zaufania *In.Te.S.A. S.p.A.* (zwanego dalej „QTSP INTESA", „organem certyfikującym" lub „INTESA"), dotyczące wydawania kwalifikowanych certyfikatów, generowania i weryfikacji kwalifikowanego podpisu elektronicznego i postępowania związanego z usługą kwalifikowanego znacznika czasu zgodnie z obowiązującymi przepisami, w ramach projektów bankowych lub finansowych.

W tego rodzaju projektach instytucje bankowe i finansowe, świadczące usługi bankowości elektronicznej lub wykorzystujące aplikacje w oddziale, pełnią również rolę lokalnych punktów rejestracji (zwanych dalej „LRA", ang. Local Registration Authority) na rzecz QTSP INTESA. Takie instytucje bankowe lub finansowe są określane w dalszej części dokumentu również jako „Bank" lub „Instytucja płatnicza" (a także jako „Bank / Instytucja").

W tym kontekście posiadaczami kwalifikowanego certyfikatu są wyłącznie podmioty zidentyfikowane przez Bank / Instytucję, która na mocy specjalnego porozumienia zawartego z QTSP INTESA jest upoważniona do pełnienia funkcji punktu rejestracji (ang. *Registration Authority*).

Dlatego podkreśla się, że wszystkie procesy podpisywania dokumentów, o których mowa w niniejszym Kodeksie postępowania certyfikacyjnego, będą realizowane wyłącznie w ramach aplikacji bankowych lub finansowych.

Czynności opisane w niniejszym Kodeksie postępowania certyfikacyjnego są przeprowadzane zgodnie z rozporządzeniem (UE) nr 910/2014 (eIDAS).

A.1. Własność intelektualna

Niniejszy Kodeks postępowania certyfikacyjnego jest wyłączną własnością spółki In.Te.S.A. S.p.A., która jest właścicielem wszelkich związanych z nim praw własności intelektualnej.

Treść niniejszego dokumentu dotycząca prowadzenia działalności QTSP jest objęta prawami własności intelektualnej.

A.2. Zakres stosowania

Postanowienia niniejszego dokumentu dotyczą QTSP INTESA (tj. jego infrastruktury logistycznej i technicznej, a także personelu), posiadaczy wydanych przez niego certyfikatów oraz tych, którzy wykorzystują te certyfikaty do weryfikacji autentyczności i integralności dokumentów opatrzonych kwalifikowanym podpisem elektronicznym, w tym przy użyciu kwalifikowanych znaczników czasu wydanych przez QTSP INTESA, oraz Banku / Instytucji płatniczej występującej w charakterze lokalnego punktu rejestracji.

Korzystanie z kluczy i wydanych odnośnych certyfikatów podlega przepisom art. 5 ust. 4 DPCM, który stanowi, że klucze do składania i weryfikacji podpisów oraz powiązane usługi rozróżnia się według następujących typów:

a) klucze podpisu, przeznaczone do generowania i weryfikacji podpisów składanych na dokumentach lub z nimi powiązanych,
b) klucze certyfikacyjne, przeznaczone do generowania i weryfikacji podpisów używanych do podpisywania certyfikatów kwalifikowanych, informacji o ważności certyfikatu lub certyfikatów dotyczących kluczy elektronicznego znacznika czasu,
c) klucze znacznika czasu, przeznaczone do generowania i weryfikacji znaczników czasu.

B. Informacje ogólne

Celem niniejszego dokumentu jest ogólne określenie procedur i odnośnych zasad regulujących wydawanie kwalifikowanych certyfikatów przez QTSP INTESA.

Wspomniane zasady i procedury wynikają z przestrzegania właściwych obowiązujących przepisów, których stosowanie pozwala na umieszczenie INTESA na liście akredytowanych organów certyfikujących.

W związku z tym, w celu zapewnienia zgodności ze wspomnianymi przepisami, konieczne jest zaangażowanie innych podmiotów, określonych szczegółowo w dalszej części dokumentu.

B.1. Dane identyfikacyjne wersji Kodeksu postępowania certyfikacyjnego

Niniejszy dokument stanowi wersję nr 04 „Kodeksu postępowania certyfikacyjnego w zakresie procedur zdalnego kwalifikowanego podpisu elektronicznego w usługach bankowych i finansowych", wydanego zgodnie z art. 40 DPCM.

Identyfikator obiektu niniejszego dokumentu to: **1.3.76.21.1.50.110**.

Niniejszy Kodeks postępowania certyfikacyjnego jest opublikowany i udostępniony do wglądu w formie elektronicznej:

- w witrynie internetowej QTSP pod adresem: *https://www.intesa.it/e-trustcom/,*
- w witrynie internetowej Agencji ds. Cyfryzacji Włoch pod adresem: *www.agid.gov.it,*

- w witrynie internetowej Banku / Instytucji.

Uwaga: publikacja zaktualizowanych wersji niniejszego Kodeksu postępowania certyfikacyjnego wymaga uprzedniej zgody Agencji ds. Cyfryzacji Włoch.

B.2. Dane identyfikacyjne dostawcy kwalifikowanych usług zaufania – QTSP

Dostawcą kwalifikowanych usług zaufania (QTSP) jest spółka ***In.Te.S.A. S.p.A.***, której dane identyfikacyjne zostały podane poniżej.

Nazwa firmy	**In.Te.S.A. S.p.A.**
Adres siedziby	**Strada Pianezza, 289** **10151 Turyn**
Przedstawiciel ustawowy	**Pełnomocny członek zarządu**
Rejestr Przedsiębiorstw w Turynie	**Nr wpisu 1692/87**
NIP	**05262890014**
Nr telefonu (centrala)	**+39 011 19216111**
Strona internetowa	**www.intesa.it**
Adres poczty elektronicznej	**marketing@intesa.it**
Adres (URL) rejestru certyfikatów	**ldap://x500.e-trustcom.intesa.it**
Identyfikator obiektu ISO (OID)	**1.3.76.21.1**

Do pracowników odpowiedzialnych za działalność certyfikacyjną, zgodnie z art. 38 DPCM, należą pracownicy pełniący następujące funkcje:

a) kierownik ds. bezpieczeństwa,
b) kierownik ds. certyfikatów i znaczników czasu,
c) kierownik ds. obsługi technicznej systemów,
d) kierownik ds. systemów technicznych i logistycznych,
e) kierownik ds. kontroli i nadzoru (audytu).

Wszyscy pracownicy pełniący wyżej wymienione funkcje należą do organizacji QTSP INTESA.

B.3. Odpowiedzialność za Kodeks postępowania certyfikacyjnego

Odpowiedzialność za niniejszy Kodeks postępowania certyfikacyjnego spoczywa, zgodnie z art. 40 ust. 3 lit. c) DPCM, na urzędzie certyfikacji INTESA, który zajmuje się jego redakcją i publikacją.

Wszelkie uwagi lub wątpliwości można zgłaszać do INTESA, korzystając z następujących informacji kontaktowych:

adres poczty elektronicznej: *marketing@intesa.it*
numer telefonu: +39 011 19216111
usługa HelpDesk dla połączeń z Włoch 800 80 50 93
dla połączeń z zagranicy +39 02 871 193 396

B.4. Podmioty zaangażowane w procesy

W strukturze organizacyjnej QTSP można wyodrębnić podmioty biorące udział w procesach związanych z wydawaniem certyfikatów.

Podmioty te działają zgodnie z zasadami i procesami wdrażanymi przez QTSP, wykonując w ramach swoich kompetencji przypisane im czynności.

B.4.1. Urząd certyfikacji (CA)

INTESA, działając zgodnie z postanowieniami DPCM, CAD i eIDAS, świadczy usługi jako dostawca kwalifikowanych usług zaufania. Usługi te obejmują kwalifikowane usługi zaufania w zakresie składania, weryfikacji i walidacji podpisów elektronicznych, pieczęci elektronicznych lub elektronicznych znaczników czasu.

Dane identyfikacyjne QTSP INTESA zostały podane w poprzednim pkt *B.2*.

B.4.2. Lokalny punkt rejestracji (LRA)

W odniesieniu do konkretnego rodzaju świadczonych usług (zdalnego kwalifikowanego podpisu elektronicznego w ramach aplikacji bankowych i finansowych), opisanego w niniejszym Kodeksie postępowania certyfikacyjnego, QTSP INTESA deleguje wykonywanie funkcji punktu rejestracji Bankowi / Instytucji, które korzystają z usługi.

LRA zobowiązuje się do wykonywania następujących czynności:

- identyfikacji posiadacza,
- rejestracji posiadacza.

Bank / Instytucja, w ramach pełnienia funkcji punktu rejestracji, czuwa nad tym, aby weryfikacja tożsamości odbywała się zgodnie z obowiązującymi przepisami i postanowieniami niniejszego Kodeksu postępowania certyfikacyjnego. Bank / Instytucja może przeprowadzić identyfikację posiadacza (*odpowiednią weryfikację*), zgodnie z przepisami dotyczącymi przeciwdziałania praniu pieniędzy, również w przypadku gdy nie jest on fizycznie obecny w oddziale.

W takim przypadku Bank / Instytucja musi w każdym razie:

- potwierdzić tożsamość w oparciu o dokumenty, dane lub dodatkowe informacje, takie jak akty publiczne, pisma prywatne poświadczone urzędowo, certyfikaty używane do składania kwalifikowanego podpisu elektronicznego powiązanego z dokumentami informatycznymi, lub w oparciu o oświadczenie wydane przez włoski urząd konsularny,
- przyjąć dodatkowe środki służące weryfikacji dostarczonych dokumentów, takie jak np. poświadczenie instytucji kredytowej lub finansowej podlegającej dyrektywie,
- korzystać z dokumentacji potwierdzającej, że zaświadczenie o dostępności środków pochodzi z rachunku prowadzonego na nazwisko klienta.

C. Obowiązki

C.1. Obowiązki dostawcy kwalifikowanych usług zaufania (QTSP)

Dostawca kwalifikowanych usług zaufania (określany również jako „akredytowany organ certyfikujący"), w ramach prowadzenia swojej działalności, działa zgodnie z postanowieniami następujących aktów prawnych:

- dekretu legislacyjnego nr 82 z dnia 7 marca 2005 r. z późniejszymi zmianami,
- rozporządzenia Prezesa Rady Ministrów z dnia 22 lutego 2013 r.,
- rozporządzenia (UE) 2016/679 (RODO),
- rozporządzenia (UE) nr 910/2014 (eIDAS).

W szczególności QTSP:

- podejmuje wszelkie odpowiednie środki organizacyjne i techniczne służące uniknięciu szkód wobec innych podmiotów,
- postępuje zgodnie z przepisami technicznymi określonymi w DPCM z późniejszymi zmianami i uzupełnieniami,
- zapewnia zgodność własnego systemu jakości z normami ISO 9001,
- zapewnia zgodność urządzenia do generowania podpisów (HSM) z wymogami bezpieczeństwa przewidzianymi w art. 29 eIDAS,
- wydaje i upublicznia certyfikat kwalifikowany, o ile posiadacz nie wskazał inaczej, zgodnie z art. 32 CAD,
- przekazuje wnioskodawcom wyraźne i jasne informacje na temat procedury certyfikacji, niezbędnych wymogów technicznych, właściwości i ograniczeń w stosowaniu podpisów wydanych w oparciu o usługę certyfikacji,
- stosuje środki bezpieczeństwa w zakresie przetwarzania danych osobowych (RODO),
- nie zostaje depozytariuszem danych do składania podpisu posiadacza,
- przystępuje do opublikowania informacji o unieważnieniu lub zawieszeniu certyfikatu elektronicznego na wniosek posiadacza lub zainteresowanej strony trzeciej,

- zapewnia precyzyjne określenie daty i godziny wydania, unieważnienia i zawieszenia certyfikatów elektronicznych,
- przechowuje rejestr, w tym w formie elektronicznej, wszystkich informacji dotyczących certyfikatu kwalifikowanego przez okres 20 (dwudziestu) lat, w szczególności w celu dostarczenia dowodu certyfikacji w toku ewentualnego postępowania sądowego,
- zapewnia unikalność kodów identyfikacyjnych (mających wyłączne znaczenie dla QTSP), przypisywanych poszczególnym posiadaczom w obrębie jego użytkowników,
- przedstawia wszelkie informacje przydatne podmiotom wnioskującym o korzystanie z usług certyfikacyjnych na trwałych środkach komunikacji. Informacje te obejmują między innymi: dokładne warunki korzystania z certyfikatu, w tym wszelkie ograniczenia w stosowaniu, istnienie opcjonalnego systemu akredytacji oraz procedury reklamacji i rozstrzygania sporów. Powyższe informacje, które mogą być przekazane w formie elektronicznej, muszą zostać spisane jasnym językiem i dostarczone przed zawarciem umowy między wnioskodawcą a QTSP,
- stosuje niezawodne systemy zarządzania rejestrem certyfikatów w taki sposób, aby wyłącznie osoby upoważnione mogły dokonywać wpisów i wprowadzać zmiany, aby można było weryfikować autentyczność informacji, aby certyfikaty były udostępniane do wglądu publicznego tylko w przypadkach dozwolonych przez posiadacza certyfikatu, a także aby operator mógł dowiedzieć się o każdym zdarzeniu naruszającym wymogi bezpieczeństwa,
- rejestruje wydanie certyfikatów kwalifikowanych w dzienniku kontrolnym wraz z datą i godziną ich wygenerowania.

Zgodnie z art. 14 DPCM organ certyfikujący zobowiązany jest dostarczyć lub wskazać co najmniej jeden system umożliwiający weryfikację podpisów cyfrowych.

Ponadto QTSP:

- generuje certyfikat kwalifikowany dla każdego z kluczy zaawansowanego podpisu elektronicznego, używanego przez Agencję ds. Cyfryzacji Włoch do podpisywania publicznej listy organów certyfikujących i publikuje go w swoim rejestrze certyfikatów zgodnie z art. 42 DPCM,
- wskazuje system weryfikacji podpisu elektronicznego, o którym mowa w art. 10 DPCM,
- przechowuje podpisaną przez Agencję ds. Cyfryzacji Włoch listę certyfikatów odnoszących się do kluczy certyfikacyjnych, o której mowa w art. 43 DPCM, i udostępnia ją drogą elektroniczną zgodnie z art. 42 ust. 3 DPCM.

C.2. Obowiązki posiadacza

Posiadacz wnioskujący o wydanie kwalifikowanego certyfikatu dla usług opisanych w niniejszym Kodeksie postępowania certyfikacyjnego jest klientem Banku lub Instytucji płatniczej, które działają w charakterze punktu rejestracji.

Posiadacz otrzymuje kwalifikowany certyfikat zdalnego kwalifikowanego podpisu elektronicznego służący do podpisywania umów i dokumentów dotyczących produktów i/lub usług oferowanych przez Bank / Instytucję w sposób określony w pkt .

Posiadacz jest zobowiązany do odpowiedniego przechowywania informacji niezbędnych do korzystania z jego prywatnego klucza podpisu oraz do podjęcia wszelkich odpowiednich środków organizacyjnych i technicznych, służących uniknięciu szkód wobec innych podmiotów (art. 32 ust. 1 CAD).

Posiadacz klucza zobowiązany jest ponadto do:

- dostarczenia wszelkich informacji wymaganych przez QTSP, zapewniając ich wiarygodność na własną odpowiedzialność,
- złożenia wniosku o wydanie certyfikatu zgodnie z wytycznymi podanymi w niniejszym Kodeksie postępowania certyfikacyjnego,
- powiadomienia QTSP, w tym za pośrednictwem LRA, o wszelkich zmianach w informacjach podanych przy rejestracji: danych osobowych, miejscu zamieszkania, numerach telefonu, adresie e-mail itp.,
- przechowywania informacji umożliwiających posługiwanie się kluczem prywatnym z najwyższą dbałością i starannością,

- niezwłocznego zgłoszenia właściwym organom oraz Bankowi / Instytucji ewentualnej utraty lub kradzieży kodów i/lub urządzeń wskazanych w celu uzyskania dostępu do swoich kluczy do podpisu; w takim przypadku Bank / Instytucja natychmiast unieważnia certyfikat,
- złożenia ewentualnego wniosku o unieważnienie lub zawieszenie certyfikatu kwalifikowanego zgodnie z niniejszym Kodeksem postępowania certyfikacyjnego.

C.3. Obowiązki użytkowników certyfikatów

Użytkownikiem (ang. *Relying Party*) jest każda osoba, która otrzymuje dokument podpisany cyfrowo i, w celu weryfikacji jego ważności, korzysta z kwalifikowanego certyfikatu użytego przez posiadacza do podpisania tego dokumentu.

Weryfikację podpisu cyfrowego i późniejszą ekstrakcję podpisanych obiektów można przeprowadzić za pomocą dowolnego oprogramowania zdolnego do przetwarzania plików podpisanych zgodnie z rozporządzeniem eIDAS.

Osoby korzystające z kwalifikowanego certyfikatu do weryfikacji ważności dokumentu podpisanego cyfrowo są zobowiązane do:

- sprawdzenia ważności certyfikatu zawierającego klucz publiczny posiadacza, który podpisał wiadomość, zgodnie ze standardami obowiązującymi na dzień jego wydania,
- sprawdzenia stanu ważności certyfikatu przy użyciu protokołu OCSP lub przez skontrolowanie list unieważnionych certyfikatów,
- sprawdzenia ważności ścieżki certyfikacji w oparciu o publiczną listę QTSP,
- sprawdzenia istnienia ewentualnych ograniczeń w stosowaniu certyfikatu użytego przez posiadacza.

C.4. Obowiązki zainteresowanej strony trzeciej

Zainteresowaną osobą trzecią, w odniesieniu do usług określonych w niniejszym Kodeksie postępowania certyfikacyjnego, jest Bank lub Instytucja płatnicza. W związku z powyższym Bank / Instytucja, w charakterze zainteresowanej osoby trzeciej:

- weryfikuje spełnienie przez klienta wszystkich niezbędnych wymagań oraz upoważnia klienta do złożenia wniosku o wydanie kwalifikowanego certyfikatu zdalnego podpisu cyfrowego,
- udziela wsparcia posiadaczowi,
- wskazuje QTSP wszelkie dodatkowe ograniczenia w stosowaniu kwalifikowanego certyfikatu zdalnego podpisu cyfrowego poza tymi przewidzianymi w pkt *F.1.1*.

Bank / Instytucja, jako zainteresowana strona trzecia, może zatem wskazywać QTSP wszelkie ograniczenia w stosowaniu certyfikatu oraz wszelkie umocowania do reprezentacji, a także powiadamiać o zmianach w tym zakresie.

Tytułem przykładu wskazuje się następujące okoliczności:

- zmiana lub odwołanie umocowań do reprezentacji,
- zmiana funkcji lub stanowiska,
- ustanie stosunku zależności.

Otrzymany przez LRA wniosek zainteresowanej strony trzeciej o unieważnienie lub zawieszenie certyfikatu powinien być niezwłocznie przesłany do CA w przypadku gdy wymagania, na podstawie których wydano posiadaczowi kwalifikowany certyfikat podpisu elektronicznego, przestają być spełnione.

C.5. Obowiązki zewnętrznych punktów rejestracji (LRA)

Na potrzeby związane ze świadczeniem usług QTSP INTESA deleguje część swojej działalności związanej z prowadzeniem punktu rejestracji dodatkowym podmiotom (zwanym dalej „zewnętrznymi punktami rejestracji" lub „LRA") na terenie całego kraju.

QTSP In.Te.S.A. S.p.A. deleguje prowadzenie działalności w zakresie rejestracji Bankowi lub Instytucji płatniczej na podstawie specjalnej *umowy delegacji* podpisanej przez obie strony.

Do działań prowadzonych przez zewnętrzne punkty rejestracji należą w szczególności:

- pewna identyfikacja wnioskodawców (zwanych dalej „posiadaczami certyfikatu"),
- rejestracja wnioskodawców / posiadaczy,
- dostarczenie posiadaczowi urządzeń i/lub kodów umożliwiających mu dostęp do jego klucza do podpisu zgodnie z art. 8 i art. 10 ust. 2 DPCM,
- przesyłanie podpisanej dokumentacji do punktu rejestracji QTSP INTESA, o ile nie określono inaczej w umowie delegacji.

W umowie delegacji określone są obowiązki nałożone na Bank / Instytucję, której QTSP INTESA zleca prowadzenie działalności LRA, nad których wypełnieniem zobowiązany jest czuwać QTSP.

W szczególności od LRA wymaga się:

- zapewnienia zgodności prowadzonej działalności identyfikacyjnej z obowiązującymi przepisami (CAD z późniejszymi zmianami i uzupełnieniami, DPCM, eIDAS i przepisy dotyczące przeciwdziałania praniu pieniędzy),
- wykorzystywania i przetwarzania danych osobowych pozyskiwanych na etapie weryfikacji tożsamości zgodnie z RODO,
- udostępniania QTSP INTESA materiału zebranego podczas identyfikacji i rejestracji.

Identyfikacja (odpowiednia weryfikacja) może być przeprowadzona na następujące trzy sposoby:

- *kanoniczny*: wnioskodawca jest identyfikowany w oddziale Banku lub Instytucji płatniczej,
- *on demand*: przy otwieraniu nowego rachunku bieżącego wnioskodawca może poprosić o kontakt osobistego doradcy finansowego, który po umówieniu spotkania będzie wspierał klienta we wszystkich procedurach związanych z otwarciem rachunku bieżącego. Na tym etapie klient (po przeprowadzeniu identyfikacji i rejestracji) uzyska również pomoc przy składaniu wniosku o wydanie kwalifikowanego certyfikatu podpisu elektronicznego,
- *on-line*: jeżeli natomiast wnioskodawca wybierze metodę bezpośredniej subskrypcji i posiada już rachunek bieżący w innym banku na terenie kraju, może on zweryfikować swoją tożsamość w następujący sposób: – skorzystać z procedury SEPA (lub SDD – SEPA Direct Debit),

– wykonać przelew z ww. rachunku bieżącego prowadzonego w innym banku.

W ramach powyższych procedur LRA Banku lub Instytucji płatniczej uzyska wszystkie informacje wymagane przez prawo przy zapewnieniu pełnego bezpieczeństwa i prywatności.

D. Odpowiedzialność i ograniczenia w zakresie odszkodowania

D.1. Odpowiedzialność QTSP – Ograniczenia w zakresie odszkodowania

QTSP INTESA odpowiada wobec posiadaczy za wypełnienie wszystkich obowiązków wynikających z wykonywania czynności przewidzianych w DPCM, RODO, CAD i eIDAS (z późniejszymi zmianami i uzupełnieniami), jak opisano w pkt *C.1. Obowiązki dostawcy kwalifikowanych usług zaufania (QTSP)*.

INTESA, z wyjątkiem przypadków zamierzonego działania lub zaniedbania (art. 13 eIDAS), nie ponosi odpowiedzialności za konsekwencje wynikające z korzystania z certyfikatów w sposób inny niż określono w art. 5 DPCM, a w szczególności z nieprzestrzegania przez posiadacza i zainteresowaną stronę trzecią postanowień niniejszego Kodeksu postępowania certyfikacyjnego i/lub obowiązujących przepisów.

Podobnie, INTESA nie ponosi odpowiedzialności za konsekwencje wynikające z przyczyn od niego niezależnych, takich jak na przykład: klęski żywiołowe, awarie lub usterki techniczne i logistyczne pozostające poza jego kontrolą, interwencje organów oraz zamieszki lub działania wojenne dotykające między innymi lub wyłącznie podmioty, z działalności których INTESA korzysta w ramach świadczenia usług certyfikacyjnych.

QTSP INTESA nie ponosi odpowiedzialności za szkody wynikające z niewłaściwego korzystania z kwalifikowanego certyfikatu zdalnego podpisu cyfrowego w związku z ograniczeniem w stosowaniu określonym w pkt *F.1.1*.

Po zapoznaniu się z niniejszym Kodeksem postępowania certyfikacyjnego posiadacz powinien wdrożyć wszelkie środki należytej staranności, mające na celu uniknięcie szkód wobec osób trzecich związanych z niewłaściwym korzystaniem z materiałów dostarczonych przez akredytowany organ certyfikujący. W szczególności powinien on przechowywać z należytą starannością urządzenia OTP i tajne kody niezbędne do uzyskania dostępu do kluczy

podpisu.

D.2. Ubezpieczenie

QTSP INTESA jest beneficjentem umów ubezpieczenia obejmujących ryzyko związane z działalnością i ryzyko szkód wobec osób trzecich, których treść jest zgodna z wymogami niezbędnymi do prowadzenia danej działalności zawodowej.

Stosowne oświadczenie o zawarciu takiej umowy jest przesyłane do AgID.

E. Opłaty

Usługę świadczy swoim klientom Bank lub Instytucja płatnicza – opłaty za wydanie, odnowienie, unieważnienie i zawieszenie kwalifikowanego certyfikatu są określane w umowach zawieranych między klientem a Bankiem / Instytucją.

F. Sposoby identyfikacji i rejestracji użytkowników

F.1. Identyfikacja użytkowników

QTSP musi z całą pewnością zweryfikować tożsamość wnioskodawcy przy pierwszym wniosku o wydanie kwalifikowanego certyfikatu.

Powyższa czynność jest delegowana do Banku / Instytucji, działającej w charakterze LRA, i prowadzi do identyfikacji i rejestracji posiadacza zgodnie z obowiązującymi przepisami dotyczącymi przeciwdziałania praniu pieniędzy.

W przypadku późniejszego odnawiania certyfikatu kwalifikowanego przed utratą jego ważności ponowne przeprowadzenie tej czynności nie jest konieczne – posiadacz zawiadamia QTSP o wszelkich zmianach w danych rejestracyjnych za pośrednictwem Banku / Instytucji.

Dane rejestracyjne niezbędne do świadczenia usługi stanowiącej przedmiot niniejszego dokumentu obejmują:

- imię i nazwisko,
- datę urodzenia,
- miejsce urodzenia (miejscowość lub kraj w przypadku osób urodzonych za granicą),
- kod identyfikacji podatkowej,
- adres zamieszkania,
- adres korespondencyjny do korespondencji papierowej,
- numer telefonu komórkowego,
- adres poczty elektronicznej,
- rodzaj i numer okazanego dokumentu tożsamości,
- organ wydający dokument, datę i miejsce wydania oraz datę ważności.

Po zakończeniu tego etapu rejestracji posiadaczowi może zostać udostępnione do użytku urządzenie wyposażone w wyświetlacz, służące do generowania jednorazowych kodów liczbowych (ang. *One Time Password*, zwanych dalej „kodami OTP” lub „OTP”).

Jako alternatywę dla fizycznego tokena OTP Bank lub Instytucja płatnicza może wskazać posiadaczom, w jaki sposób aktywować system uwierzytelniania na poziomie oprogramowania dla urządzeń mobilnych (jeśli posiadacz posiada takie urządzenie i wybierze ten sposób uwierzytelniania jako preferowany ze względu na łatwość obsługi w porównaniu z korzystaniem z fizycznego tokena). Taki system na poziomie oprogramowania pozwoli na wygenerowanie OTP na urządzeniu mobilnym posiadacza, a tym samym będzie używany jako narzędzie uwierzytelniania w systemach zdalnego podpisu.

Posiadacz otrzyma, poza OTP, wszelkie niezbędne informacje oraz kod PIN służący do uzyskania bezpiecznego dostępu do usługi zdalnego podpisu udostępnianej przez Bank / Instytucję.

Ten sam PIN może służyć jako kod awaryjny (na przykład w przypadku zagubienia i/lub utraty tokena OTP lub urządzenia mobilnego) w celu pilnego zawieszenia swojego kwalifikowanego certyfikatu przez posiadacza (pkt *H.2.2*).

Posiadacz może w późniejszym czasie zmienić lub zaktualizować kod PIN, korzystając z usług udostępnionych przez Bank lub Instytucję płatniczą.

Na tym etapie posiadaczowi przekazywane są również informacje niezbędne do zmiany podanego wcześniej numeru telefonu komórkowego w dowolnym momencie.

Ponadto bezpośrednio w oddziale Banku / Instytucji lub w późniejszym czasie przy wykorzystaniu usług bankowości elektronicznej oferowanych przez Bank / Instytucję, ale w każdym razie przed złożeniem wniosku o wydanie kwalifikowanego certyfikatu, posiadacz powinien:

- zapoznać się z Kodeksem postępowania certyfikacyjnego QTSP INTESA,
- upoważnić Bank lub Instytucję płatniczą do przetwarzania swoich danych osobowych w celach związanych z wydaniem kwalifikowanego certyfikatu podpisu elektronicznego.

Powyższa dokumentacja, dotycząca rejestracji posiadaczy, przechowywana jest przez okres 20 (dwudziestu) lat od daty ważności certyfikatu.

F.1.1. Ograniczenia w stosowaniu

Kwalifikowany certyfikat podpisu elektronicznego, wydany w ramach usług opisanych w niniejszym Kodeksie postępowania certyfikacyjnego i świadczonych przez Bank / Instytucję, zawsze zawiera ograniczenie w stosowaniu.

Standardowa formuła ograniczenia ma następujące brzmienie:

Korzystanie z certyfikatu ograniczone jest do relacji z Nazwa Banku / Instytucji.

Szczególne ograniczenia w stosowaniu mogą być uzgodnione z Bankiem lub Instytucją płatniczą.
INTESA nie odpowiada za szkody wynikające z korzystania z kwalifikowanego certyfikatu w zakresie przekraczającym wprowadzone w nim ograniczenia lub wynikające z przekroczenia tych ograniczeń.

F.1.2. Tytuły i kwalifikacje zawodowe

W przypadku wymaganego wskazania kwalifikacji zawodowych (np. przynależności do izby zawodowej) w kwalifikowanym certyfikacie, wnioskodawca powinien przedłożyć odpowiednie dokumenty potwierdzające faktyczne istnienie takich kwalifikacji zawodowych lub równoważną dokumentację.

Kopia takiej dokumentacji przechowywana jest przez okres 20 (dwudziestu) lat od daty ważności certyfikatu.

Dokumentacja przedłożona na poparcie wniosku o umieszczenie tytułów lub kwalifikacji zawodowych w certyfikacie kwalifikowanym nie może być wydana wcześniej niż 10 (dziesięć) dni przed złożeniem wniosku o wydanie ww. certyfikatu.

INTESA nie odpowiada za szkody wynikające z niewłaściwego korzystania z kwalifikowanego certyfikatu zawierającego informacje dotyczące kwalifikacji zawodowych.

W przypadku podawania przez posiadacza danych w formie oświadczenia, INTESA nie ponosi żadnej odpowiedzialności, z wyjątkiem przypadków zamierzonego działania lub zaniedbania (art. 13 eIDAS), za wszelkie informacje podane w certyfikacie w oparciu o oświadczenie posiadacza.

F.1.3. Umocowania do reprezentacji

W przypadku wymaganego wskazania w kwalifikowanym certyfikacie informacji o umocowaniach do reprezentacji (np. przynależności do danej organizacji i pełnionej w niej funkcji, upoważnienia do działania w imieniu klienta itp.) wnioskodawca powinien przedłożyć odpowiednie dokumenty potwierdzające faktyczne istnienie takich umocowań do reprezentacji.

W odniesieniu do reprezentowania osób fizycznych wnioskodawca powinien przedłożyć poświadczoną kopię upoważnienia lub pełnomocnictwa notarialnego podpisaną przez osobę reprezentowaną wraz z zaświadczeniem o wyrażeniu przez tę osobę zgody na zawarcie informacji o funkcji w certyfikacie.

W przypadku, gdy wymagane jest wskazanie w certyfikacie funkcji związanej z reprezentowaniem organizacji lub instytucji prawa prywatnego, posiadacz powinien przedłożyć dokumentację potwierdzającą funkcję, która ma być zawarta w certyfikacie, oraz oświadczenie odnośnej organizacji lub instytucji upoważniające QTSP do umieszczenia informacji o określonej funkcji w certyfikacie. Oświadczenie to powinno być wydane nie wcześniej

niż 20 (dwadzieścia) dni przed złożeniem wniosku o wydanie certyfikatu kwalifikowanego.

Umieszczenie w kwalifikowanym certyfikacie informacji dotyczących wykonywania funkcji publicznych w instytucjach lub organizacjach prawa publicznego bądź umocowań do reprezentacji takich podmiotów podlega odrębnym ustaleniom umownym z tymi podmiotami. Ustalenia takie mogą obejmować funkcję pełnioną przez posiadacza w instytucji lub organizacji publicznej.

Przedłożona dokumentacja przechowywana jest przez okres 20 (dwudziestu) lat.

INTESA nie odpowiada za szkody wynikające z niewłaściwego korzystania z kwalifikowanego certyfikatu zawierającego informacje dotyczące umocowań do reprezentacji.

F.1.4. Korzystanie z pseudonimów

W szczególnych przypadkach posiadacz może złożyć wniosek o zawarcie w certyfikacie jego pseudonimu zamiast rzeczywistych danych.

Informacje dotyczące rzeczywistej tożsamości użytkownika przechowywane są przez 20 (dwadzieścia) lat.

F.2. Rejestracja użytkowników wnioskujących o wydanie certyfikatu

Po zakończeniu etapu identyfikacji dane posiadacza są rejestrowane w bazie danych urzędu certyfikacji.

Czynność tę można wykonać za pomocą oprogramowania, z którego można skorzystać bezpośrednio w aplikacjach udostępnionych przez Bank lub Instytucję płatniczą.

G. Generowanie kluczy certyfikacyjnych, kluczy znaczników czasu i kluczy podpisu

G.1. Generowanie kluczy certyfikacyjnych

Generowanie kluczy w urządzeniach do podpisu odbywa się w obecności kierownika ds. certyfikatów, zgodnie z art. 7 DPCM.

Powyższą czynność poprzedza inicjalizacja urządzeń do podpisu dla systemu generowania certyfikatów, którymi podpisywane są certyfikaty posiadaczy oraz certyfikaty dotyczące systemu znaczników czasu.

Wszystko to odbywa się w trybie podwójnej kontroli (ang. *dual control*), aby uniknąć działania niezgodnego z prawem.

Operacje następujące po wygenerowaniu par kluczy organu certyfikującego są możliwe wyłącznie za pośrednictwem określonych urządzeń autoryzujących (token usb) – uprzywilejowany dostęp do HSM jest możliwy wyłącznie przy użyciu kluczy zawartych w wymienionych wyżej urządzeniach autoryzujących.

W celu zapewnienia większego bezpieczeństwa klucze te są rozdzielone na różne urządzenia zgodnie z logiką typu „*x z y*", tak aby korzystanie z odpowiednich przywilejów było możliwe wyłącznie pod warunkiem jednoczesnej obecności co najmniej *x* części z *y* części klucza. Z tego względu są one przechowywane w specjalnych osobnych sejfach.

Długość kluczy certyfikacyjnych wynosi co najmniej 2048 bitów.

G.2. Generowanie kluczy systemu znaczników czasu

Klucze znaczników czasu generowane są zgodnie z art. 49 DPCM.

Długość kluczy systemu znaczników czasu wynosi co najmniej 2048 bitów.

G.3. Generowanie kluczy podpisu

Po zakończeniu etapu rejestracji, podczas którego dane posiadaczy zapisywane są w bazach danych organu certyfikującego, można przystąpić do wygenerowania kluczy podpisu.

Posiadacz może uruchomić procedurę prowadzącą do wygenerowania kluczy i uzyskania powiązanego z nimi certyfikatu podpisu w jeden ze sposobów określonych w pkt *I. Procedury operacyjne składania podpisu na dokumentach*. Pary kluczy podpisu tworzone są na bezpiecznych urządzeniach do podpisu (HSM - Hardware Security Module) spełniających wymagania określone w załączniku II do rozporządzenia eIDAS.

Długość kluczy podpisu wynosi co najmniej 2048 bitów.

H. Tryb wydawania certyfikatów

H.1. Procedura wydawania zaświadczeń certyfikacyjnych

W następstwie wygenerowania kluczy certyfikacyjnych, określonego w pkt *G.1*, generowane są certyfikaty kluczy publicznych, zgodnie z postanowieniami DPCM, podpisane odnośnymi kluczami prywatnymi i wpisane do rejestru certyfikatów zgodnie z odpowiednimi przepisami.

I Certyfikaty kluczy certyfikacyjnych wysyłane są do Agencji ds. Cyfryzacji Włoch za pośrednictwem systemu komunikacji, o którym mowa w art. 12 ust. 1 DPCM.

II Organ certyfikujący generuje certyfikat kwalifikowany dla każdego z kluczy kwalifikowanego podpisu elektronicznego używanego przez Agencję do podpisywania publicznej listy organów certyfikujących i publikuje go w swoim rejestrze certyfikatów. Organ certyfikujący jest zobowiązany do przechowywania podpisanej przez agencję listy certyfikatów odnoszących się do kluczy certyfikacyjnych i udostępniania jej drogą elektroniczną (art. 42 ust. 1 i 3 DPCM).

H.2. Procedura wydawania certyfikatów podpisu

INTESA wydaje certyfikaty w systemie zgodnym z art. 33 DPCM.

Po wygenerowaniu pary kluczy podpisu, określonym w pkt *G.3*, generowane jest żądanie wydania nowego certyfikatu w formacie *PKCSff10,* który dostarcza automatycznie dowód posiadania klucza prywatnego i umożliwia weryfikację prawidłowego działania pary kluczy.

Po wygenerowaniu kluczy żądanie wydania certyfikatu jest przesyłane niezwłocznie z aplikacji Banku / Instytucji do urzędu certyfikacji QTSP.

Wygenerowanie certyfikatów rejestrowane jest w dzienniku kontrolnym (art. 18 ust. 4 DPCM).

H.2.1. Informacje zawarte w certyfikatach podpisu

I Certyfikaty INTESA wydane w ramach niniejszego Kodeksu postępowania certyfikacyjnego, są certyfikatami kwalifikowanymi w rozumieniu rozporządzenia (UE) nr 910/2014 (eIDAS), w związku z czym zapewnia się ich interoperacyjność i uznawanie na szczeblu unijnym.

II Kwalifikowany certyfikat w sposób pewny określa organ certyfikujący, który go wydał i zawiera dane niezbędne do weryfikacji podpisu cyfrowego.

Każdy kwalifikowany certyfikat podpisu elektronicznego jest zgodny z rozporządzeniem eIDAS i postanowieniem AgID nr 147/2019 („Wytyczne Agencji ds. Cyfryzacji Włoch wprowadzające zasady i zalecenia techniczne dotyczące generowania certyfikatów").

Wszystkie kwalifikowane certyfikaty wydane w ramach usług określonych w niniejszym Kodeksie postępowania certyfikacyjnego zawierają ograniczenie w stosowaniu (pkt *F.1.1*).

H.2.2. Kod awaryjny

Zgodnie z art. 21 DPCM organ certyfikujący dostarcza *kod awaryjny* służący do złożenia wniosku o ***pilne zawieszenie*** certyfikatu.

W zastosowaniach opisanych w niniejszym Kodeksie postępowania certyfikacyjnego rolę kodu awaryjnego pełni kod PIN dostarczony posiadaczowi przy rejestracji.

I. Procedury operacyjne składania podpisu na dokumentach

Za pośrednictwem usług Banku lub Instytucji płatniczej QTSP INTESA udostępnia posiadaczom wszystkie elementy niezbędne do składania kwalifikowanych podpisów elektronicznych zgodnie z obowiązującymi przepisami.

Szczególny rodzaj usługi nie wymaga korzystania z aplikacji do składania podpisu instalowanej na własnym komputerze, ale z funkcji składania podpisu dostępnych w ramach usług bankowości elektronicznej Banku lub Instytucji płatniczej bądź bezpośrednio w oddziale Banku lub Instytucji płatniczej.

Kwalifikowane podpisy elektroniczne otrzymywane za pośrednictwem tych procedur są w pełni zgodne z przepisami art. 4 ust. 2 DPCM w odniesieniu do stosowanych algorytmów.

Ponadto dokumenty te, zgodnie z wymogami art. 4 ust. 3 DPCM, nie zawierają makropoleceń ani kodów wykonywalnych, które mogłyby uruchamiać funkcje prowadzące do zmiany informacji zawartych w dokumentach, bez wiedzy osoby składającej podpis.

Poniżej opisano dwie różne metody uwierzytelniania, które zgodnie z obowiązującymi przepisami umożliwiają posiadaczowi, po uprzedniej rejestracji, wygenerowanie kluczy podpisu i uzyskanie certyfikatu kwalifikowanego, a następnie użycie ich do składania kwalifikowanych podpisów elektronicznych.

Po złożeniu podpisu zostanie wysłany SMS ze stosownym potwierdzeniem. Alternatywnie, jeżeli posiadacz dysponuje smartfonem umożliwiającym odczytywanie korespondencji, potwierdzenia mogą być wysyłane, na wniosek posiadacza, za pośrednictwem poczty elektronicznej.

I.1. Uwierzytelnienie typu „Call Drop"

Ta metoda uwierzytelnienia wymaga, aby w celu potwierdzenia chęci złożenia podpisu na dokumencie, wcześniej zidentyfikowany użytkownik wykonał połączenie ze swojego telefonu komórkowego (z numeru podanego na etapie identyfikacji) na określony numer telefonu, podany w ramach usługi.

Po wykonaniu tego połączenia jest ono weryfikowane w celu upewnienia się, że zostało wykonane z numeru telefonu (ang. *Call Identifier*) powiązanego uprzednio z użytkownikiem na etapie rejestracji, i w przypadku pozytywnego wyniku weryfikacji, użytkownik uzyskuje autoryzację do złożenia kwalifikowanego podpisu elektronicznego.

W związku z tym, gdy posiadacz zamierza podpisać dokument, logując się w witrynie Banku / Instytucji, korzysta z uwierzytelniania dwuetapowego obejmującego wprowadzenie kodu PIN (informacji znanej wyłącznie użytkownikowi) oraz numeru telefonu (powiązanego z kartą SIM posiadaną wyłącznie przez użytkownika).

Ten typ uwierzytelniania nazywany jest również „*Call Drop*", ponieważ połączenie wykonywane przez posiadacza w celu dokonania uwierzytelnienia nie prowadzi do nawiązania żadnej rozmowy i po kilku sekundach zostaje przerwane.

Połączenie wykonywane przez posiadacza nie jest nigdy odbierane, w związku z czym nie ponosi on żadnych związanych z tym kosztów. Zaletami tej metody jest jej ekonomiczność i praktyczność, ponieważ nie wymaga korzystania z żadnego fizycznego urządzenia uwierzytelniającego i jest bardzo łatwa w użyciu.

W dalszej części dokumentu opisano powody, dla których ta metoda uwierzytelniania jest polecana w przypadkach, gdy posiadacz chce skorzystać z usługi w miejscach nienadzorowanych (zazwyczaj korzystając z bankowości elektronicznej Banku lub Instytucji płatniczej z własnego komputera), ale nie jest bardzo praktyczna, gdy posiadacz chce skorzystać z usługi w obecności zewnętrznego operatora, na przykład na stanowisku obsługiwanym przez kasjera Banku lub Instytucji płatniczej.

Dla tych ostatnich przypadków przewidziano rozwiązanie oparte na dynamicznym zarządzaniu numerami telefonów służących do ukończenia procesu uwierzytelniania w miejscach nazywanych miejscami nadzorowanymi.

I.1.1. Proces składania podpisu w miejscach nienadzorowanych (bankowość elektroniczna)

Po uzyskaniu niezbędnych kodów na etapie identyfikacji, posiadacz może w późniejszym czasie wystąpić o wydanie certyfikatu cyfrowego i złożyć podpis na dokumencie w niżej opisany sposób.

1. Posiadacz loguje się do aplikacji bankowej lub finansowej, używając swoich osobistych kodów dostępu do aplikacji.
2. Wybiera i weryfikuje dokument do podpisania.
3. Wprowadza swój kod PIN.
4. Po zweryfikowaniu kodu PIN, w celu potwierdzenia chęci podpisania dokumentu posiadacz powinien, w określonym czasie (nieprzekraczającym jednej minuty) i przy użyciu zarejestrowanego wcześniej telefonu komórkowego, niezwłocznie zadzwonić na numer telefonu, który pojawi się w międzyczasie na wyświetlaczu.
5. Po potwierdzeniu, że połączenie zostało wykonane z tego samego numeru, który został wcześniej zarejestrowany i powiązany z posiadaczem, system wykonuje operację podpisu i wysyła potwierdzenie jej pomyślnego zakończenia.

6. Jeżeli natomiast w ciągu określonego czasu system nie otrzyma połączenia telefonicznego na numer określony w pkt 4, operację uważa się za nieważną i zakończoną bez złożenia podpisu na dokumencie.

Jeżeli do podpisania jest więcej niż jeden dokument, posiadacz powinien powtórzyć kroki od 2 do 5 dla każdego dokumentu.

I.1.2. Proces składania podpisu w miejscach nadzorowanych (w oddziale banku lub instytucji finansowej)

Po uzyskaniu kwalifikowanego certyfikatu posiadacz może złożyć podpis na dokumencie.

Jak stwierdzono wcześniej, w oddziale banku lub instytucji, w obecności operatora, posiadacz może mieć trudność z wprowadzeniem osobistych i zastrzeżonych kodów, takich jak PIN.

Dlatego przewidziano alternatywne rozwiązanie, które jednocześnie zapewnia najwyższy poziom bezpieczeństwa:

1. Użytkownik udaje się do oddziału Banku / Instytucji (miejsca nadzorowanego) i jego tożsamość weryfikowana jest przez pracownika (np. kasjera) w tradycyjny sposób.
2. Po uzyskaniu wglądu do dokumentu do podpisania posiadacz może uruchomić procedurę składania podpisu.
3. Następnie na wyświetlaczu widocznym dla posiadacza pojawia się numer telefonu (wybrany losowo z obszernej puli dostępnych numerów) i jednocześnie uruchamia się odliczanie czasu.
4. W celu potwierdzenia chęci podpisania dokumentu posiadacz powinien, w określonym czasie (nieprzekraczającym jednej minuty), zadzwonić na numer, który pojawił się na wyświetlaczu (przy użyciu swojego telefonu komórkowego, który został wcześniej zarejestrowany).
5. Następnie system, po stwierdzeniu prawidłowości numeru dzwoniącego, wykonuje operację podpisu i wysyła SMS z potwierdzeniem jej zakończenia.
6. Jeżeli natomiast w ciągu określonego czasu system nie otrzyma połączenia telefonicznego na numer określony w pkt 3, operacja zostaje anulowana.

Jeżeli do podpisania jest więcej niż jeden dokument, posiadacz powinien powtórzyć kroki od 2 do 5 dla każdego dokumentu.

I.2. Uwierzytelnienie typu OTP Mobile

Poza uwierzytelnianiem typu Call Drop dostępna jest również alternatywna metoda uwierzytelniania o nazwie „OTP Mobile”.

W celu aktywowania tej metody posiadacz musi dysponować jednym ze smartfonów umieszczonych przez Bank / Instytucję na liście smartfonów obsługujących tę usługę.

Po przeprowadzeniu stosownej weryfikacji na etapie identyfikacji w oddziale Banku / Instytucji, w którym dokonano rejestracji, posiadacz otrzyma adres specjalnej strony internetowej w ramach witryny Banku lub Instytucji płatniczej, umożliwiającej pobranie na smartfon aplikacji o nazwie „OTP Mobile”, a także kod PIN.

Również w odniesieniu do tej drugiej metody uwierzytelniania poniżej opisano proces składania podpisu w zależności od miejsca (nienadzorowanego lub nadzorowanego).

I.2.1. Proces składania podpisu w miejscach nienadzorowanych (bankowość elektroniczna)

Po uzyskaniu swojego certyfikatu kwalifikowanego posiadacz może podpisać dokument, wykonując następujące kroki:

1. Posiadacz loguje się do aplikacji bankowej lub finansowej, używając swoich osobistych kodów dostępu do aplikacji.
2. Wybiera i weryfikuje dokument do podpisania.
3. Wprowadza swój kod PIN.
4. Uruchamia uprzednio pobraną na swój smartfon aplikację i uzyskuje kod OTP do wpisania po kodzie PIN.
5. Po potwierdzeniu prawidłowości wprowadzonych kodów PIN i OTP system wykonuje operację podpisu i wysyła potwierdzenie jej pomyślnego zakończenia.

Jeżeli do podpisania jest więcej niż jeden dokument, posiadacz powinien powtórzyć kroki od 2 do 5 dla każdego dokumentu.

I.2.2. Proces składania podpisu w miejscach nadzorowanych (w oddziale banku lub instytucji finansowej)

Również w tym przypadku przewidziano rozwiązanie, które nie wymaga wprowadzania przez posiadacza, w obecności pracowników Banku lub Instytucji płatniczych, swoich zastrzeżonych kodów, które mogłyby zostać wykorzystane na jego szkodę w sposób niezgodny z prawem.

Po uzyskaniu swojego certyfikatu kwalifikowanego posiadacz może podpisać dokument, postępując zgodnie z następującą procedurą:

1. Użytkownik udaje się do oddziału Banku lub Instytucji płatniczej (miejsca nadzorowanego) i jego tożsamość weryfikowana jest przez pracownika (np. kasjera) w tradycyjny sposób.
2. W momencie podpisu przed użytkownikiem włączany jest specjalny monitor wyposażony w kamerkę internetową.
3. Po uzyskaniu wglądu do dokumentu do podpisania, wyświetlanego na wspomnianym monitorze, posiadacz uruchamia na swoim smartfonie procedurę wygenerowania kodu OTP, który podawany jest również w formie kodu kreskowego.
4. Posiadacz może następnie zwrócić ekran swojego smartfona w kierunku kamerki internetowej w celu umożliwienia odczytania kodu OTP wygenerowanego w poprzednim kroku nr 3 i tym samym uruchomić procedurę składania podpisu.
5. Po złożeniu podpisu na dokumencie system natychmiast przesyła posiadaczowi SMS z potwierdzeniem.

W celu podpisania kilku dokumentów należy powtórzyć kroki od 2 do 5.

I.2.3. Proces składania podpisu dla klientów Prospect

Proces wydawania kwalifikowanego certyfikatu zdalnego podpisu może być obsługiwany również przez klienta Prospect podczas czynności Onboarding (pozyskiwanie klienta).

Proces ten jest kompatybilny z głównymi przeglądarkami (Chrome, Firefox, Edge, Safari) i nowszymi modelami urządzeń mobilnych Android i Apple.

Obejmuje on następujące etapy:

1. Po uruchomieniu procesu klient Prospect proszony jest o wprowadzenie swoich danych osobowych w celu zapewnienia jego późniejszej pewnej identyfikacji, po uprzednim podpisaniu zgody na przetwarzanie danych osobowych przez QTSP INTESA.
2. Bank lub Instytucja przesyła klientowi SMS zawierający kod OTP (ang. *One Time Password*) o

tymczasowej ważności – klient Prospect proszony jest o wprowadzenie tego kodu w celu weryfikacji rzeczywistej dostępności urządzenia mobilnego wskazanego na etapie wprowadzania danych.

3. Po zakończeniu weryfikacji określonej w poprzednim punkcie klient Prospect przekazuje Bankowi lub Instytucji dokumenty tożsamości – dane osobowe są wprowadzane przez klienta Prospect lub pozyskiwane z dokumentów przy użyciu systemu OCR.
4. Po zakończeniu rejestracji Bank przesyła klientowi Prospect dokumentację umowną, którą klient Prospect może podpisać przy użyciu kwalifikowanego certyfikatu zdalnego podpisu cyfrowego (ZPC) wydanego przez QTSP INTESA.
5. Klientowi Prospect, tak samo jak w procedurze opisanej dla bankowości elektronicznej, przedstawiona zostanie dokumentacja dotycząca wniosku o wydanie certyfikatu QTSP INTESA.
6. Klient zobowiązany jest potwierdzić zapoznanie się z tą dokumentacją, zaznaczając pola wyboru znajdujące się w dokumencie oraz składając podpis elektroniczny przy użyciu kodu OTP otrzymanego przez SMS od QTSP INTESA.
7. Kwalifikowany certyfikat może być wydany pod warunkiem pozytywnej weryfikacji wprowadzonego kodu OTP otrzymanego od QTSP INTESA; w przeciwnym razie konieczne będzie uzyskanie nowego OTP.
8. W każdym razie w chwili wygenerowania certyfikatu konieczne jest wprowadzenie kodu PIN, który będzie wymagany przy każdym użyciu certyfikatu podpisu.
9. Wydany certyfikat może być wykorzystany jedynie do podpisania oferty umownej, a nie żadnego innego dokumentu, dopóki Bank nie przeprowadzi wstępnych kontroli koniecznych do otwarcia rachunku bieżącego.
10. W przypadku pomyślnego zakończenia kontroli Banku i otwarcia rachunku bieżącego klient Prospect może używać wydanego certyfikatu w relacjach z Bankiem, w granicach określonych ograniczeń w stosowaniu. Natomiast w razie odmowy otwarcia rachunku bieżącego przez Bank, certyfikat ten jest unieważniany i jego dalsze używanie nie jest możliwe.
11. W obu przypadkach określonych w poprzednim punkcie klient Prospect informowany jest o wyniku kontroli i ewentualnym unieważnieniu certyfikatu.

I.3. Uwierzytelnienie przy użyciu tokena OTP

Wreszcie, dostępna jest również metoda uwierzytelniania związana z wykorzystaniem fizycznych tokenów OTP (bardzo powszechnych w usługach bankowych i finansowych).

Obecnie uwierzytelnianie przy użyciu fizycznego tokena OTP stosowane jest wyłącznie do logowania w miejscach nienadzorowanych (poza oddziałem, w usługach bankowości elektronicznej).

Posiadacz loguje się do aplikacji bankowej lub finansowej, używając swoich osobistych kodów dostępu do aplikacji, i w celu uruchomienia procedury podpisu wprowadza kody PIN i OTP generowane i wyświetlane w międzyczasie na wyświetlaczu tokena.

J. Procedury operacyjne weryfikacji podpisu

Dokumenty podpisywane przy wykorzystaniu sposobów określonych powyżej są dostępne wyłącznie w formacie PDF – format ten jest bowiem uznawany za łatwy w użyciu w ramach usług bankowych i finansowych. Podpisane dokumenty mogą być sprawnie zweryfikowane przy użyciu oprogramowania *Acrobat Reader DC*, które umożliwia weryfikację wszystkich rodzajów kwalifikowanego podpisu elektronicznego w formacie PDF złożonych w Unii Europejskiej zgodnie z rozporządzeniem eIDAS.

Program Acrobat Reader DC jest dostępny bezpłatnie do pobrania ze strony Adobe, *https://www.adobe.com/it/.*

K. Sposób unieważniania oraz zawieszania certyfikatów

Zgodnie z rozporządzeniem eIDAS informacje o statusie certyfikatu dostępne są przy użyciu protokołu OCSP pod adresem URL wskazanym w certyfikacie.

Unieważnienie i zawieszenie certyfikatu można również potwierdzić faktem ich umieszczenia na liście CRL (art. 22 DPCM). Profil listy CRL jest zgodny ze standardem RFC 3280. Lista ta, podpisana przez urząd certyfikacji wydający certyfikat, jest aktualizowana z określoną częstotliwością zgodną z obowiązującymi przepisami.

Lista CRL jest dostępna również w rejestrze certyfikatów.

W przypadku unieważnienia lub zawieszenia certyfikatu z inicjatywy organu certyfikującego lub zainteresowanej strony trzeciej (art. 23, 25, 27 i 29 DPCM) organ certyfikujący powiadamia o tym fakcie posiadacza, wskazując datę unieważnienia lub zawieszenia.

Na etapie składania wniosku zostanie określona data i godzina, wraz z którą certyfikat zostanie unieważniony (art. 24 ust. 1 DPCM).

K.1. Unieważnienie certyfikatu

Certyfikat może być unieważniony na wniosek posiadacza, zainteresowanej strony trzeciej lub urzędu certyfikacji (tj. QTSP).

Unieważniony certyfikat nie może być przywrócony.

K.1.1. Unieważnienie certyfikatu na wniosek posiadacza

Posiadacz może złożyć wniosek o unieważnienie certyfikatu, logując się do określonej sekcji udostępnionej w ramach usług Banku lub Instytucji płatniczej, bądź też kontaktując się bezpośrednio z biurem obsługi klienta Banku lub Instytucji płatniczej.

Po otrzymaniu zawiadomienia z Banku / Instytucji, która w międzyczasie przystępuje również do zablokowania kodów dostępu posiadacza, QTSP natychmiast unieważnia certyfikat.

K.1.2. Unieważnienie certyfikatu na wniosek zainteresowanej strony trzeciej

Bank lub Instytucja płatnicza może wystąpić o unieważnienie certyfikatu w charakterze zainteresowanej osoby trzeciej.

QTSP, po stwierdzeniu prawidłowości wniosku, powiadamia danego posiadacza o unieważnieniu certyfikatu za pomocą kanałów komunikacyjnych uzgodnionych z posiadaczem w momencie rejestracji lub zaktualizowanych i zgłoszonych QTSP w późniejszym czasie przez posiadacza, w tym za pośrednictwem LRA (pkt *C.2. Obowiązki posiadacza*).

K.1.3. Unieważnienie certyfikatu z inicjatywy organu certyfikującego

Organ certyfikujący, który zamierza unieważnić certyfikat kwalifikowany, zawiadamia o tym fakcie niezwłocznie, z wyjątkiem uzasadnionych pilnych przypadków, Bank / Instytucję (zainteresowaną stronę trzecią) za pośrednictwem poczty elektronicznej lub certyfikowanej poczty elektronicznej, jednocześnie przesyłając stosowną informację posiadaczowi na adres e-mail podany we wniosku o wydanie certyfikatu lub na adres zamieszkania, wskazując powód unieważnienia oraz datę i godzinę, wraz z którą certyfikat zostanie unieważniony.

K.1.4. Unieważnienie certyfikatu dotyczącego kluczy certyfikacyjnych

W przypadku:

- naruszenia klucza certyfikacyjnego,
- zaprzestania prowadzenia działalności,

organ certyfikujący unieważnia odnośne zaświadczenia certyfikacyjne i certyfikaty podpisu podpisane tym samym kluczem certyfikacyjnym.

W ciągu 24 godzin organ certyfikujący powiadamia o unieważnieniu certyfikatów Agencję ds. Cyfryzacji Włoch

oraz posiadaczy.

K.2. Zawieszenie certyfikatu

W odniesieniu do procedury zawieszania certyfikatów i powiadamiania o nim zastosowanie mają postanowienia dotyczące unieważniania certyfikatów określone w pkt *K.1*. Certyfikat zostaje zawieszony w razie konieczności przeprowadzenia dodatkowego dochodzenia mającego na celu potwierdzenie zasadności jego unieważnienia (na przykład w przypadkach, gdy istnieje obawa utraty / kradzieży tokena OTP, lub gdy konieczne jest przeprowadzenie kontroli w celu potwierdzenia rzeczywistego zaprzestania pełnienia przez posiadacza funkcji, w związku z którą certyfikat został wydany itp.).

Wniosek o zawieszenie mogą złożyć wszystkie podmioty przewidziane w art. 27, 28 i 29 DPCM (organ certyfikujący, posiadacz, zainteresowana osoba trzecia).

W przypadku braku pism ze strony posiadacza certyfikat zostanie automatycznie unieważniony po okresie zawieszenia wynoszącym 90 (dziewięćdziesiąt) dni, a w każdym razie przed upływem terminu ważności certyfikatu.

W każdym przypadku data rozpoczęcia okresu unieważnienia będzie zbieżna z datą rozpoczęcia okresu zawieszenia.

K.2.1. Zawieszenie certyfikatu na wniosek posiadacza

Posiadacz może złożyć wniosek o zawieszenie certyfikatu, logując się do określonej sekcji udostępnionej w ramach usług Banku lub Instytucji płatniczej, bądź też kontaktując się bezpośrednio z biurem obsługi klienta Banku lub Instytucji płatniczej.

Organ certyfikujący przystępuje do zawieszenia certyfikatu, o czym posiadacz jest informowany za pomocą określonych funkcji udostępnionych w ramach usług Banku lub Instytucji płatniczej.

Posiadacz może następnie zwrócić się o przywrócenie certyfikatu w sposób udostępniony przez Bank lub Instytucję płatniczą.

W przypadku braku dodatkowych pism zawieszony certyfikat zostanie automatycznie unieważniony po zakończeniu okresu zawieszenia, a data unieważnienia będzie zbieżna z datą rozpoczęcia okresu zawieszenia.

K.2.2. Zawieszenie certyfikatu na wniosek zainteresowanej strony trzeciej

Bank lub Instytucja płatnicza może wystąpić o zawieszenie certyfikatu w charakterze zainteresowanej osoby trzeciej.

Po stwierdzeniu prawidłowości wniosku organ certyfikujący niezwłocznie zawiesza certyfikat, o czym informuje zainteresowanych posiadaczy za pośrednictwem poczty elektronicznej lub komunikatu przesłanego w ramach usług udostępnianych przez Bank lub Instytucję płatniczą.

K.2.3. Zawieszenie certyfikatu z inicjatywy organu certyfikującego

Z wyjątkiem uzasadnionych pilnych przypadków, organ certyfikujący może zawiesić certyfikat, o czym informuje uprzednio posiadacza na adres e-mail podany we wniosku o wydanie certyfikatu na etapie rejestracji lub na adres zamieszkania, podając powód zawieszenia oraz datę i godzinę rozpoczęcia okresu zawieszenia.

Taką samą informację organ certyfikujący przesyła również do zainteresowanej strony trzeciej.

L. Sposoby zastępowania kluczy

L.1. Zastąpienie kwalifikowanych certyfikatów i kluczy posiadacza

Kwalifikowane certyfikaty podpisu elektronicznego wydane przez organ certyfikujący w ramach usług określonych w niniejszym Kodeksie postępowania certyfikacyjnego są ważne przez 36 (trzydzieści sześć) miesięcy od daty

wydania.

Po upływie tego terminu konieczne jest wygenerowane nowej pary kluczy podpisu oraz wydanie nowego certyfikatu.

W takim przypadku procedura wydawania nowego certyfikatu jest bardzo podobna do procedury wydawania pierwszego certyfikatu, z tą różnicą, że nie jest konieczna ponowna identyfikacja posiadacza.

L.2. Zastąpienie kluczy organu certyfikującego

L.2.1. Pilne zastąpienie kluczy certyfikacyjnych

Postępowanie na wypadek usterki urządzenia do podpisu (HSM) zawierającego klucze certyfikacyjne (CA i TSCA) lub awarii w centralnej siedzibie zostało opisane w sekcji *P Procedura zarządzania zdarzeniami awaryjnymi*.

L.2.2. Planowane zastąpienie kluczy certyfikacyjnych

Przy zachowaniu okresu zgodnego z obowiązującymi przepisami, przed wygaśnięciem certyfikatu odnoszącego się do par kluczy certyfikacyjnych (CA i TSCA), którymi posługują się systemy wydawania certyfikatów podpisu i certyfikatów TSA, organ certyfikujący przystąpi do procedury określonej w art. 30 DPCM.

L.3. Klucze systemu znakowania czasem (TSA)

Zgodnie z art. 49 ust. 2 DPCM, w celu ograniczenia liczby znaczników czasu generowanych za pomocą tej samej pary kluczy znaczników czasu, są one zastępowane w terminie 90 (dziewięćdziesięciu) dni od daty ich wydania. Jednocześnie wydawany jest certyfikat dotyczący nowej pary kluczy (bez unieważniania poprzedniego certyfikatu dotyczącego zastąpionej pary kluczy).

M. Rejestr certyfikatów

M.1. Sposób zarządzania rejestrem certyfikatów

W rejestrze certyfikatów INTESA publikuje:

1. certyfikaty kluczy podpisu i systemu znaczników czasu,
2. certyfikaty kluczy certyfikacyjnych (CA i TSCA),
3. certyfikaty wydane w następstwie zastąpienia kluczy certyfikacyjnych,
4. certyfikaty dla kluczy podpisu Agencji ds. Cyfryzacji Włoch (art. 42 ust. 1 DPCM),
5. listy unieważnionych i zawieszonych certyfikatów (CRL).

Czynności związane z rejestrem certyfikatów są wykonywane wyłącznie przez osoby do tego upoważnione, których liczba musi być odpowiednia, aby zapobiec bezprawnym działaniom możliwym ze strony małej grupy pracowników.

Organ certyfikujący przechowuje kopię referencyjną rejestru certyfikatów niedostępną z zewnątrz, która aktualizuje w czasie rzeczywistym kopię operacyjną, dostępną dla użytkowników przy użyciu protokołu LDAP.

Weryfikacja zgodności kopii referencyjnej z kopią operacyjną jest przeprowadzana systematycznie.

M.2. Dostęp logiczny do rejestru certyfikatów

Kopia referencyjna rejestru jest przechowywana w specjalnej sieci zabezpieczonej odpowiednimi urządzeniami, w związku z czym dostęp do niej jest możliwy wyłącznie z serwera wydawania certyfikatów, który rejestruje w nim wydane certyfikaty i listy CRL.

Kopie operacyjne są dostępne pod adresem ***ldap://x500.e-trustcom.intesa.it*** przy użyciu protokołu LDAP.

Organ certyfikujący zezwala na dostęp do list CRL za pośrednictwem protokołu http, pod adresem URL wskazanym

w certyfikacie w polu CDP (ang. *CRL Distribution Point*).

M.3. Fizyczny dostęp do pomieszczeń, w których znajdują się systemy służące do rejestru certyfikatów

Pracownicy upoważnieni do bezpośredniego zarządzania rejestrem certyfikatów mają dostęp do pomieszczenia, w którym zainstalowany jest system, i mogą w nim pracować, wyłącznie w trybie podwójnej kontroli (ang. *dual control*), aby uniknąć działania niezgodnego z prawem.

Pracownicy odpowiedzialni za zarządzanie systemami, zarządzanie siecią, konserwację itp. mają dostęp do pomieszczenia, w którym zainstalowany jest system, a w przypadku określonych pracowników – mogą w nim pracować, wyłącznie w obecności pracowników upoważnionych do zarządzania rejestrem certyfikatów zgodnie z procedurami opisanymi powyżej w odniesieniu do upoważnionych pracowników.

N. Sposoby ochrony danych osobowych

Środki ochrony danych osobowych są zgodne z przepisami rozporządzenia (UE) 2016/679 (RODO) z późniejszymi zmianami i uzupełnieniami.

O. Procedura zarządzania kopiami zapasowymi

Następujące bazy danych podlegają procedurze kopii zapasowych:

- REJESTR CERTYFIKATÓW, cyfrowa baza danych zawierająca elementy określone w pkt M.
- INFORMACJE OPERACYJNE, cyfrowa baza danych, w której zapisywane są wszystkie informacje otrzymane od posiadaczy w momencie rejestracji i składania wniosku o wydanie certyfikatu, a także wniosku o unieważnienie lub zawieszenie certyfikatu, z załączoną odnośną dokumentacją.
- DZIENNIK KONTROLNY, baza danych składająca się ze zbioru zapisów wykonywanych automatycznie przez systemy zainstalowane w lokalach urzędu certyfikacji QTSP (art. 36 DPCM).
- CYFROWA BAZA DANYCH ZNACZNIKÓW CZASU, zawiera znaczniki czasu wygenerowane przez system znakowania czasem (art. 53 ust. 1 DPCM).
- REJESTR OPERACYJNY ZDARZEŃ ZNAKOWANIA CZASEM, rejestr, w którym automatycznie zapisywane są zdarzenia dotyczące operacji znakowania czasem, dla których przewiduje się rejestrowanie wszelkich nieprawidłowości i prób naruszenia, które mogłyby wpływać na działanie systemu znakowania czasem (art. 52 DPCM).

Wszystkie wyżej wymienione kopie zapasowe przechowywane są zgodnie z obowiązującymi przepisami w tym zakresie.

P. Procedura zarządzania zdarzeniami awaryjnymi

QTSP INTESA dysponuje planem awaryjnym dotyczącym zarządzania zdarzeniami awaryjnymi, który obejmuje następujące etapy:

- postępowanie w sytuacji awaryjnej: na tym etapie zapewniona jest ciągłość dostępu do list CRL; ich wydanie może ulec opóźnieniu w związku z koniecznością aktywowania serwera kopii zapasowej CA, znajdującego się w pomieszczeniu kopii zapasowej,
- postępowanie w okresie przejściowym: na tym etapie zapewnione jest wydawanie certyfikatów i przywracanie dodatkowych rozwiązań w ramach odzyskiwania po awarii,
- powrót do normalnej sprawności: w tym samym miejscu lub w innym, ale ostatecznym miejscu.

Należy zaznaczyć, że istnienie replikacji kopii operacyjnej rejestru certyfikatów, zlokalizowanych w różnych

punktach, zapewnia możliwość dostępu do treści rejestru certyfikatów w przypadku przerwy w działaniu któregoś z punktów, w wersji aktualnej na moment przerwania działania.

W celu zapewnienia odpowiedniego zarządzania sytuacją awaryjną przewidziano replikację danych rejestru certyfikatów oraz danych systemu wydawania certyfikatów w pomieszczeniu kopii zapasowej, a także interwencję personelu w celu aktywacji funkcji wydawania list CRL w ciągu 24 godzin. Personel ten odbywa szkolenia nie tylko z zarządzania oprogramowaniem i sprzętem, ale również w zakresie postępowania w sytuacjach awaryjnych.

Papierowa kopia planu awaryjnego jest przechowywana we wszystkich siedzibach objętych zarządzaniem zdarzeniami awaryjnymi.

Q. Sposób umieszczania i określania odniesienia czasowego

Wszystkie maszyny systemu PKI organu certyfikującego są zsynchronizowane z włoskim głównym urzędem miar (I.N.RI.M. – wł. *Istituto Nazionale di Ricerca Metrologica* w Turynie (wcześniejsza nazwa *Istituto Elettrotecnico Nazionale Galileo Ferraris*). Funkcja ta jest realizowana przez specjalne oprogramowanie zainstalowane na każdym serwerze, które przez protokół NTP (Network Time Protocol) łączy się ze skonfigurowanym zdalnym serwerem.

Network Time Protocol (NTP) to jedna z najbardziej dokładnych i elastycznych metod przesyłania informacji o czasie i dacie przez internet. Umożliwia ona synchronizację komputerów połączonych za pośrednictwem sieci lokalnych, metropolitalnych, a nawet globalnych (internetu) za pomocą hierarchicznej struktury przypominającej piramidę.

I.N.RI.M zapewnia usługę synchronizacji systemów komputerowych podłączonych do internetu, opartą na dwóch serwerach podstawowych NTP zainstalowanych w sieci Laboratorium wzorcowych sygnałów czasu i częstotliwości. Są one synchronizowane, za pośrednictwem generatora kodu daty, przez atomowe wzorce cezowe używane do generowania włoskiej krajowej skali czasu UTC(IT). Różnica czasu między serwerami NTP I.N.RI.M a włoską skalą czasu jest utrzymywana pod kontrolą i zwykle wynosi mniej niż kilka milisekund. Osiągalna dokładność synchronizacji zależy od rodzaju sieci i odległości między serwerem NTP a maszyną, którą chce się zsynchronizować; typowe wartości odchylenia są mniejsze niż jedna milisekunda dla systemów należących do tej samej sieci i mogą sięgać kilkuset milisekund dla sieci zdalnych.

Oprogramowanie zainstalowane w lokalach organu certyfikującego łączy się ze zdalnym serwerem w regularnych odstępach czasu i po uzyskaniu aktualnej godziny koryguje zegar lokalnej maszyny za pomocą zaawansowanych algorytmów.

Odnośniki czasowe umieszczane przez aplikacje są ciągami znaków w formacie daty (DD/MM/RRRR gg:mm:ss), z dokładnością do sekundy, które przedstawiają czas lokalny, zgodnie z konfiguracją maszyny. Odniesienia te są zgodne z art. 51 DPCM.

Każdy zapis w dzienniku kontrolnym zawiera odniesienie czasowe, które ze względu na ww. sposób wygenerowania, jest wiążące również w stosunku do osób trzecich (art. 41 DPCM).

Q.1. Sposób składania wniosku o znacznik czasu i jego weryfikacji

Organ certyfikujący umieszcza znacznik czasu („kwalifikowany elektroniczny znacznik czasu” w rozumieniu rozporządzenia eIDAS) na wszystkich dokumentach podpisywanych przez posiadacza w ramach usług określonych w niniejszym Kodeksie postępowania certyfikacyjnego.

Umieszczenie tego znacznika jest procesem zintegrowanym z operacją składania podpisu i nie wymaga żadnego specjalnego działania ze strony posiadacza.

R. Czas realizacji i macierz RACI dot. wydawania certyfikatów

Poniżej przedstawiono tabelę dotyczącą czasu realizacji procesu w odniesieniu do zarządzania wnioskami o wydanie, unieważnienie, zawieszenie i przywrócenie certyfikatów.

Podmiot	Wniosek	Zaangażowany organ	Działanie zaangażowanego organu	Zaangażowany organ	Działanie zaangażowanego organu
Użytkownik, Wnioskodawca, Posiadacz certyfikatu	*Wniosek o wydanie certyfikatu do LRA*	*Bank / Instytucja (w charakterze) LRA*	*Po zweryfikowaniu tożsamości zleca CA publikację certyfikatu*	*Urząd certyfikacji*	*Rozpatrzenie wniosku o wydanie certyfikatu*
Użytkownik, Wnioskodawca, Posiadacz certyfikatu	*Wniosek o unieważnienie certyfikatu do RA lub LRA*	*Intesa (w charakterze) punktu rejestracji (RA) lub Bank / Instytucja (w charakterze LRA)*	*Po zweryfikowaniu tożsamości zleca CA unieważnienie certyfikatu*	*Urząd certyfikacji*	*Rozpatrzenie wniosku o unieważnienie certyfikatu*
Użytkownik, Wnioskodawca, Posiadacz certyfikatu	*Wniosek o zawieszenie certyfikatu do RA lub LRA*	*Intesa (w charakterze) punktu rejestracji (RA) lub Bank / Instytucja (w charakterze LRA)*	*Po zweryfikowaniu tożsamości zleca CA zawieszenie certyfikatu*	*Urząd certyfikacji*	*Rozpatrzenie wniosku o zawieszenie certyfikatu*
Użytkownik, Wnioskodawca, Posiadacz certyfikatu	*Wniosek o przywrócenie certyfikatu do RA lub LRA*	*Intesa (w charakterze) punktu rejestracji (RA) lub Bank / Instytucja (w charakterze LRA)*	*Po zweryfikowaniu tożsamości zleca CA przywrócenie certyfikatu*	*Urząd certyfikacji*	*Rozpatrzenie wniosku o przywrócenie certyfikatu*

Poniżej przedstawiono macierz RACI dotyczącą określania odpowiedzialności podmiotów zaangażowanych w wydawanie, unieważnianie, zawieszanie i przywracanie certyfikatów.

Zaangażowany podmiot	Odpowiedzialny	Rozliczany	Konsultujący	Informowany
Punkt rejestracji	***X***			
Lokalny punkt rejestracji	***X***			
Urząd certyfikacji		***X***		
Użytkownik, Wnioskodawca, Posiadacz certyfikatu			***X***	***X***

F. Odniesienia techniczne

ETSI-319.401	ETSI EN 319 401 v2.1.1 – Podpisy elektroniczne i infrastruktura (ESI); Ogólne wymagania polityki dla dostawców zaufanych usług
ETSI-319411-1	ETSI EN 319 411-1 V1.1.1 – Podpisy elektroniczne i infrastruktura (ESI); Wymagania polityki i bezpieczeństwa dla dostawców usług zaufania wydających certyfikaty Część 1: Wymagania ogólne
ETSI-319411-2	ETSI EN 319 411-2 V2.1.0 – Podpisy elektroniczne i infrastruktura (ESI); Wymagania polityki i bezpieczeństwa dla dostawców usług zaufania wydających certyfikaty Część 2: Wymagania dla dostawców usług zaufania wydających certyfikaty kwalifikowane UE
ETSI-319411-3	ETSI EN 319 411-3 V1.1.1 – Podpisy elektroniczne i infrastruktura (ESI); Wymagania polityki i bezpieczeństwa dla dostawców usług zaufania wydających certyfikaty Część 3: Wymagania polityki dla organów certyfikacji wydających certyfikaty kluczy publicznych
ETSI-319412-1	ETSI EN 319 412-1 V1.1.1 – Podpisy elektroniczne i infrastruktura (ESI); Profile certyfikatu; Część 1: Opis ogólny oraz ogólne struktury danych
ETSI-319412-2	ETSI EN 319 412-2 V2.1.1 – Podpisy elektroniczne i infrastruktura (ESI); Profile certyfikatu; Część 2: Profil certyfikatu dla certyfikatów wydawanych osobom fizycznym
ETSI-319412-5	ETSI EN 319 412-5 V2.1.1 – Podpisy elektroniczne i infrastruktura (ESI); Profile certyfikatu; Część 5: Deklaracje dla certyfikatów kwalifikowanych
Rec ITU-R	Zalecenie ITU-R TF.460-6, Dodatek 1 – Skale czasu.
RFC5905	Network Time Protocol (Protokół NTP)
ETSI-319.421	ETSI EN 319 421 v1.1.1 – Podpisy elektroniczne i infrastruktura (ESI); Wymagania polityki i bezpieczeństwa dla dostawców usług zaufania wydających znaczniki czasu
ETSI-319.422	ETSI EN 319 422 v1.1.1 – Podpisy elektroniczne i infrastruktura (ESI); Protokół znakowania czasem oraz profile tokena znacznika czasu
Rec ITU-R	Zalecenie ITU-R TF.460-6, Dodatek 1 – Skale czasu.
RFC5905	Network Time Protocol (Protokół NTP)

----- KONIEC DOKUMENTU ---------