PDS

Informacje o infrastrukturze klucza publicznego

KOD DOKUMENTU	**ICERT-INDI-PDS**
WERSJA	**3.3**
DATA	**24.05.2022**

INFOCERT
TINEXTA GROUP

1. SPIS TREŚCI

2. Wprowadzenie

Niniejsze Informacje o infrastrukturze klucza publicznego (ang. *PKI-Disclosure-Statement*, PDS) spełniają wymagania w zakresie publikacji przewidziane w normie europejskiej ETSI EN 319 411-1 w odniesieniu do usług certyfikacyjnych świadczonych przez dostawcę kwalifikowanych usług zaufania InfoCert S.p.A. (zwanego dalej „**InfoCert**", „**QTSP**" lub „**CA**"), i mają na celu dostarczenie wnioskodawcy informacji technicznych niezbędnych do korzystania z tych usług.

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 jest dalej „**rozporządzeniem eIDAS**".

Niniejszy dokument wraz z regulaminem świadczenia usług stanowi integralną część dokumentacji umownej InfoCert.

Publikacja niniejszego PDS nie zastępuje publikacji Polityki certyfikacji i kodeksu postępowania certyfikacyjnego (CPS), który to dokument, zawierający bardziej szczegółowe informacje, jest dostępny na stronie internetowej InfoCert pod adresem:
https://www.firma.infocert.it/documentazione/.

3. Kontakt

Spółka InfoCert S.p.A. – NIP: IT 07945211006
Dostawca kwalifikowanych usług zaufania
Piazza Sallustio, 9
00187 Rzym, Włochy

Miejsce wykonywania działalności
Piazza Luigi da Porto 3
35131 Padwa, Włochy

Telefon: +39 06 836691 – Faks: +39 06 23328861
Infolinia w sprawie podpisu cyfrowego: patrz link https://help.infocert.it/contatti/
Strona www: http://www.firma.infocert.it/
E-mail: firma.digitale@legalmail.it
W celu złożenia wniosku o **unieważnienie** należy wypełnić odpowiedni formularz opublikowany na stronie internetowej InfoCert i przesłać go certyfikowaną pocztą elektroniczną (PEC), listem poleconym lub faksem z załączoną kserokopią ważnego dokumentu tożsamości. Wniosek o unieważnienie można złożyć również we właściwym punkcie rejestracji zgodnie z zasadami określonymi w regulaminie świadczenia usług. InfoCert zastrzega sobie prawo do dodatkowej weryfikacji tożsamości wnioskodawcy.

Wniosek o **zawieszenie** można złożyć bezpośrednio przez internet na stronie internetowej InfoCert, korzystając z tajnego kodu przypisanego w momencie rejestracji.

4. Rodzaje certyfikatów, ich walidacja i stosowanie

InfoCert wydaje kwalifikowane certyfikaty zgodnie z europejską normą **ETSI EN 319 411** i innymi powiązanymi normami; certyfikaty oferowane są ogółowi społeczeństwa (prywatnym firmom, instytucjom publicznym, osobom wykonującym wolny zawód, konsumentom itp.) na warunkach określonych w regulaminie opublikowanym na stronie internetowej QTSP lub punktów rejestracji (RA).

Algorytm używany do podpisywania certyfikatów może być wybrany spośród następujących:

- sha256WithRSAEncryption [iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) sha256WithRSAEncryption(11)]

- ecdsa-with-SHA256 [iso(1) member-body(2) us(840) ansi-x962(10045) signatures(4) ecdsa-with-SHA2(3) ecdsa-with-SHA256(2)]

• ecdsa-with-SHA384 [iso(1) member-body(2) us(840) ansi-x962(10045) signatures(4) ecdsa-with-SHA2(3) ecdsa-with-SHA384(3)]

• ecdsa-with-SHA512 [iso(1) member-body(2) us(840) ansi-x962(10045) signatures(4) ecdsa-with-SHA2(3) ecdsa-with-SHA512(4)].

Podpisy i certyfikaty można zweryfikować za pośrednictwem aplikacji **GoSign** do pobrania bezpłatnie ze strony internetowej InfoCert.

5. Ograniczenia w świadczeniu usług

InfoCert wydaje:

- **kwalifikowane certyfikaty dla osób fizycznych** do zaawansowanego lub kwalifikowanego podpisu elektronicznego,
- **kwalifikowane certyfikaty dla osób prawnych do elektronicznych pieczęci**, w tym w celu spełnienia wymagań PSD2.

Ponadto InfoCert świadczy usługi podpisu zdalnego na urządzeniach QSCD (Qualified Electronic Signature Creation Device), w ramach których generuje klucze i certyfikaty dla podpisującego i nimi zarządza.

Szczegółowe informacje i zasady zostały zawarte w politykach certyfikacji dostępnych pod adresem: *https://www.firma.infocert.it/documentazione*.

Okres ważności każdego certyfikatu jest wskazany w samym certyfikacie i może wynosić od jednej godziny do trzech lat i trzech miesięcy.

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

Dzienniki zdarzeń związanych z wydawaniem certyfikatów są przechowywane w odpowiednim systemie przechowywania dokumentów elektronicznych InfoCert przez nie mniej niż 20 (dwadzieścia) lat od daty wygaśnięcia

certyfikatu i nie więcej niż 23 (dwadzieścia trzy) lata od daty wydania certyfikatu.

6. Obowiązki posiadacza

Posiadacz powinien przestrzegać klauzul zawartych w CPS i regulaminie świadczenia usług, a w szczególności:

- przeczytać i zrozumieć dokumentację umowną oraz wszelkie dodatkowe dokumenty informacyjne;
- przejść procedury identyfikacji wdrożone przez urząd certyfikacji, zgodnie z opisem zawartym w CPS;
- przekazać informacje niezbędne do identyfikacji, uzupełnione, w stosownych przypadkach, o odpowiednią dokumentację;
- używać przydzielonej pary kluczy wyłącznie do celów i w sposób dopuszczony w CPS;
- 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;
- w okresie obowiązywania certyfikatu niezwłocznie informować CA lub RA w następujących przypadkach:
    - utrata, kradzież lub uszkodzenie swojego urządzenia do podpisu;
    - utrata wyłącznej kontroli nad swoim kluczem prywatnym, na przykład z powodu naruszenia danych aktywacyjnych (takich jak PIN) swojego urządzenia do podpisu;
    - nieprawidłowości lub zmiany w informacjach zawartych w certyfikacie;
- chronić poufność danych uwierzytelniających niezbędnych do korzystania z urządzeń lub usług służących do podpisu, nie przekazując ich ani nie ujawniając osobom trzecim i zachowując je pod swoją wyłączną kontrolą;
- niezwłocznie i definitywnie zaprzestać używania klucza w przypadku jego naruszenia, z wyjątkiem czynności odszyfrowania samego klucza;

- dopilnować, aby klucz prywatny nie był używany w przypadku poinformowania wnioskodawcy o unieważnieniu certyfikatu lub o naruszeniu CA.

Za zapewnienie i korzystanie z połączenia internetowego oraz wszystkich niezbędnych narzędzi (sprzętu i oprogramowania) odpowiada wnioskodawca.

7. Obowiązki wnioskodawcy, który nie jest tożsamy z posiadaczem

Wnioskodawca, który nie jest tożsamy z posiadaczem, powinien przestrzegać klauzul zawartych w CPS i regulaminie świadczenia usług, a w szczególności:

- read and understand the contract documentation and any additional informative documentation;
- przejść procedury identyfikacji wdrożone przez QTSP;
- provide all information necessary for the purposes of identification, accompanied, where required, by the appropriate documentation;
- in signing the request for registration and certification, accept the contractual conditions regulating the provision of the service, as stated in analog or electronic forms prepared by the CA;
- określić procedurę informatyczną, przy użyciu której zostaną przesłane dokumenty podlegające procedurze podpisu zdalnego i aktywacji kluczy do podpisu przez posiadacza, oraz poinformować o tej procedurze dostawcę usług zaufania (TSP);
- pokryć koszty usługi zdalnego podpisu oraz wskazać, w drodze określonych czynności i procedur, posiadaczy, którym mają być wydane certyfikaty;
- wskazać rodzaj systemu uwierzytelniania, jaki został wybrany w celu aktywacji procedury zdalnego podpisu;
- w przypadku zamiaru złożenia wniosku o unieważnienie lub zawieszenie certyfikatu posiadacza, podpisać odpowiedni formularz wniosku o unieważnienie lub zawieszenie certyfikatu, udostępniony przez QTSP;

- poinformować posiadacza o obowiązkach wynikających z certyfikatu, podać prawidłowe i zgodne z prawdą informacje o tożsamości posiadacza oraz przestrzegać procedur i wskazówek określonych przez QTSP lub RA;
- w przypadku posiadacza będącego osobą prawną, podać QTSP 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 wydania;
  - adres e-mail służący QTSP do przesyłania wiadomości wnioskodawcy;
  - nazwę posiadacza będącego osobą prawną;
  - NIP lub NTR (nr NIP lub numer w Rejestrze Przedsiębiorstw w przypadku podmiotów włoskich);
- w przypadku gdy klucze generowane są przez urządzenie będące w posiadaniu subskrybenta, wnioskodawca zobowiązany jest do przesłania odpowiedniego wniosku w formacie PKCS#10 podpisanego przez samego wnioskodawcę. W przypadku gdy urządzenie do podpisu nie zostanie udostępnione przez QTSP, wnioskodawca musi zapewnić, że urządzenie spełnia wymagania obowiązujących przepisów, przedstawiając odpowiednią dokumentację i podlegając okresowym audytom przeprowadzanym przez QTSP.

8. Status ważności certyfikatów

Wszystkie osoby polegające na informacjach zawartych w certyfikatach są zobowiązane do sprawdzenia, czy certyfikaty te nie zostały zawieszone ani unieważnione.

Weryfikację tę można przeprowadzić, korzystając z listy certyfikatów unieważnionych (CRL) opublikowanej przez CA pod adresem URL wskazanym

w certyfikacie lub za pośrednictwem usługi OCSP. Ważność certyfikatu można również sprawdzić przy użyciu produktu Dike GoSign, dostępnego do pobrania bezpłatnie ze strony internetowej InfoCert.

9. Ograniczona gwarancja i brak/ograniczenie odpowiedzialności

Kwalifikowane certyfikaty dostarczane są zgodnie z niniejszym dokumentem oraz regulaminem świadczenia usług. Wszelkie szczegółowe informacje techniczne podane są w CPS.

InfoCert ponosi odpowiedzialność za ewentualne szkody wyrządzone bezpośrednio i na skutek działań umyślnych lub z powodu niedbalstwa jakiejkolwiek osobie fizycznej lub prawnej w konsekwencji niedopełnienia 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 rezolucji Agencji ds. Cyfryzacji Włoch (AgID) nr 185/2017.

Poniesione koszty nie podlegają zwrotowi w przypadku, gdy niemożność skorzystania z usługi wynika 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.

10. Obowiązujące regulaminy, warunki i polityki certyfikacji

Regulaminy i warunki mające zastosowanie do usług QTSP oraz CPS opublikowane są na stronie internetowej InfoCert pod adresem: https://firma.infocert.it/documentazione.

11. Polityka prywatności

Dane dotyczące subskrybenta oraz wnioskodawcy, w posiadanie których wchodzi CA w związku z prowadzeniem swojej normalnej działalności, należy traktować jako 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*.

Dane osobowe przetwarzane są przez InfoCert zgodnie z zapisami włoskiego rozporządzenia z mocą ustawy 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 r.

12. Zasady zwrotu płatności

Posiadacz jest zobowiązany do poinformowania QTSP o swojej decyzji odstąpienia od umowy w drodze jednoznacznego oświadczenia przesłanego, przed upływem okresu przewidzianego na odstąpienie, certyfikowaną pocztą elektroniczną (PEC) na adres: *richieste.rimborso@legalmail.it* lub listem poleconym ze zwrotnym potwierdzeniem odbioru na adres: InfoCert S.p.A. – Direzione Generale e Amministrativa – Via Marco e Marcelliano, 45 00147 Roma. W tym celu może on skorzystać ze wzoru formularza odstąpienia

dostępnego na stronie internetowej InfoCert pod adresem: *https://www.InfoCert.it/pdf/Modulo-di-recesso-tipo.pdf*.

QTSP dokona zwrotu zrealizowanych płatności, po odjęciu kosztów zwrotu ewentualnego urządzenia do podpisu, które pokrywa posiadacz lub wnioskodawca. Zwrot płatności zostanie dokonany na konto bankowe użyte do początkowej transakcji, o ile posiadacz wyraźnie nie wskaże innego konta bankowego; w każdym przypadku posiadacz nie ponosi żadnych kosztów w związku ze zwrotem płatności.

13. Prawo właściwe dla reklamacji i rozstrzygania sporów

Świadczenie usług certyfikacji i znaczników czasu podlega prawu obowiązującemu we Włoszech. We wszystkich przypadkach nieuwzględnionych wyraźnie w niniejszym dokumencie zastosowanie ma włoski kodeks cywilny i inne obowiązujące akty prawne.
Wszelkie spory wynikające z interpretacji i wykonania niniejszej umowy lub z nią związane podlegają wyłącznej jurysdykcji właściwych sądów w Rzymie, o ile nie określono inaczej w regulaminie świadczenia usług.

W przypadku, gdy klientem jest konsument, ewentualne spory związane z umową zawartą przez konsumenta, rozstrzygane będą wyłącznie przez sąd właściwy dla miejsca jego stałego lub tymczasowego zamieszkania.

14. Archiwa, licencje i znaki towarowe, audyt

CA nie weryfikuje wykorzystania zarejestrowanych znaków towarowych, ale może odmówić wygenerowania lub zażądać unieważnienia certyfikatu będącego przedmiotem sporu.

Weryfikacja zgodności z rozporządzeniem (UE) nr 910/2014 z dnia 23 lipca 2014 r., zgodnie z normami ETSI EN 319 401, ETSI EN 319 411-1 i ETSI EN 319

411-2, została przeprowadzona przez CSQA Certificazioni S.r.l. według schematu oceny eIDAS określonego przez ACCREDIA zgodnie z normami ETSI EN 319 403 i ISO/IEC 17065: 2012.

InfoCert przedłożył raport z oceny zgodności Agencji ds. Cyfryzacji Włoch (AgID), która zatwierdziła umieszczenie InfoCert na liście zaufanych dostawców jako kwalifikowanego dostawcy usług zaufania zgodnie z rozporządzeniem (EU) nr 910/2014 z dnia 23 lipca 2014 r.

Włoska lista zaufanych CA dostępna jest na stronie internetowej Agencji ds. Cyfryzacji Włoch (AgID) pod adresem: *https://eidas.agid.gov.it/TL/TSL-IT.xml*