

Autoritatea de Certificare

Declarația de Transparență a PKI (Infrastructura de Cheie Publică)

Categorie	Politica generală TPS	ID Document	NAMTSP-PDS-RO	Namirial S.p.A.
Întocmită de	Simone Baldini	Nivel de clasificare	Document Public	Reprezentant legal
Verificată de	Giuseppe Benedetti	Versiunea	1.1	Davide Ceccucci
Aprobată de	Davide Ceccucci	Data emiterii	14/06/2018	_____



Namirial S.p.A.

Registered office, management and administration 60019 Senigallia (AN) - via Caduti sul Lavoro, 4
Tax Code/Company Register of Ancona n. 02046570426 - VAT no. IT02046570426 Share Capital € 6.500.000,00 fully paid-up
Tel. 07163494 s.a. - Fax 199.418016 - info@namirial.com - www.namirial.com



– Această pagină a fost lăsată goală în mod intenționat –



CUPRINS

Cuprins.....	3
ISTORICUL MODIFICĂRILOR	4
REFERINȚE.....	5
1 INTRODUCERE	7
2 INFORMAȚIILE DE CONTACT ALE AUTORITĂȚII DE CERTIFICARE (AC)	7
3 TIPURI DE CERTIFICATE, PROCEDURI DE VALIDARE ȘI UTILIZARE	7
4 LIMITE DE ÎNTREBUINȚARE.....	8
5 OBLIGAȚIILE SEMNATARILOR.....	8
6 OBLIGAȚIA UTILIZATORULUI DE VERIFICARE A STATUSULUI CERTIFICATULUI	9
7 GARANȚIA LIMITATĂ ȘI DECLINAREA / LIMITAREA RĂSPUNDERII.....	9
8 ACORDURI APLICABILE, CPP, PC	9
9 POLITICA DE CONFIDENȚIALITATE	9
10 POLITICA DE RAMBURSARE	9
11 LEGEA APLICABILĂ, SOLUȚIONAREA RECLAMAȚIILOR ȘI A DISPUTELOR	10
12 LICENȚELE TSP (ALE FURNIZORULUI DE SERVICII DE ÎNCREDERE) ȘI ALE DEPOZITARULUI, MĂRCILE DE ÎNCREDERE ȘI AUDITUL.....	10



ISTORICUL MODIFICĂRILOR

VERSIUNEA	1.1
Date	14/06/2018
Motivul	Revizie
Modificări	§9 adăugat la Regulamentul (UE) 2016/679

VERSIUNEA	1.0
Date	26/05/2017
Motivul	Prima versiune a documentului
Modificări	---



REFERINȚE

NUMĂR	DESCRIERE
[I]	Decretul Președintelui Republicii (DPR) din 28 decembrie 2000 nr. 445 " Textul unic al dispozițiilor legislative și de reglementare în materie de documentație administrativă" publicat în Suplementul ordinar al Monitorului oficial nr. 42 din 20 februarie 2001
[II]	Decretul Președintelui Consiliului (DPCM) din 22 februarie 2013 " Regulile tehnice în materie de generare, depunere și verificare a semnăturilor electronice avansate, calificate și digitale, în temeiul articolelor 20, alineat 3, 24, alineat 4, 28, alineat 3, 32, alineat 3, litera b) , 35, alineat 2, 36, alineat 2 și 71".
[III]	Regulamentul (UE) 2016/679 al Parlamentului European și al Consiliului din 27 aprilie 2016 privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și privind libera circulație a acestor date și de abrogare a Directivei 95 / 46 / CE.
[IV]	Decretul legislativ (CAD) din 7 martie 2005, nr. 82 " Codul Administrației digitale ", publicat în Monitorul Oficial nr.112 din 16 mai 2005 cu modificările și completările stabilite de Decretul legislativ din 26 august 2016, nr. 179.
[V]	Regulamentul UE nr.910/2014 al Parlamentului European și Consiliului din 23 iulie 2014 privind identificarea electronică și serviciile de încredere pentru tranzacțiile electronice pe piața internă și de abrogare a Directivei 1999/93/CE
[VI]	DECIZIA DE PUNERE ÎN APLICARE (UE) 2016/650 A COMISIEI din 25 aprilie 2016 de stabilire a standardelor pentru evaluarea securității dispozitivelor de creare a semnăturilor și a sigiliilor calificate în temeiul articolului 30 alineatul (3) și al articolului 39 alineatul (2) din Regulamentul (UE) nr. 910/2014 al Parlamentului European și al Consiliului privind identificarea electronică și serviciile de încredere pentru tranzacțiile electronice pe piața internă
[VII]	DECIZIA DE PUNERE ÎN APLICARE (UE) 2015/1505 A COMISIEI din 8 septembrie 2015 de stabilire a specificațiilor tehnice și a formatelor pentru listele sigure în temeiul articolului 22 alineatul 5 din Regulamentul (UE) nr. 910/2014 al Parlamentului European și al Consiliului privind identificarea electronică și serviciile de încredere pentru tranzacțiile electronice pe piața internă.
[VIII]	REGULAMENTUL DE PUNERE ÎN APLICARE (UE) 2015/1501 AL COMISIEI din 8 septembrie 2015 privind cadrul de interoperabilitate prevăzut la articolul 12, alineatul 8 din Regulamentul (UE) nr. 910/2014 al Parlamentului European și al Consiliului privind identificarea electronică și serviciile de încredere pentru tranzacțiile electronice pe piața internă
[IX]	ETSI EN 319 411-1 - Semnături electronice și infrastructuri (ESI); Cerințe privind politica și de securitate pentru furnizorii de servicii de încredere care eliberează certificate; Partea 1: Cerințe generale
[X]	ETSI EN 319 411-2 - Semnături electronice și infrastructuri (ESI); Cerințe privind politica și de securitate pentru furnizorii de servicii de încredere care eliberează certificate; Partea a 2-a: Cerințe pentru furnizorii de servicii de încredere care eliberează certificate calificate UE
[XI]	ETSI EN 319 412-1 - Semnături electronice și infrastructuri (ESI); Profiluri de Certificate; Partea 1: Prezentare generală și structuri comune de date
[XII]	ISO EN UNI 9001:2008 – Sistemul calității
[XIII]	ISO / IEC 29115: 2013 Tehnologia informației - Tehnici de securitate - Cadrul de asigurare a autentificării entităților
[XIV]	Decizia CNIPA nr. 45/2009 cu modificările și completările ulterioare
[XV]	ETSI EN 319 401 V2.1.1 (2016-02) Semnături electronice și Infrastructuri (ESI); Cerințe privind politica generală a Furnizorilor de Servicii De încredere
[XVI]	ISMS-DOC-A16 – Procedura de raportare a atentatelor care pun în pericol securitatea – V1 Final
[XVII]	20170428-NAM_CA_Structura_Organizativa_v3.0



NUMĂR	DESCRIERE
[XVIII]	Manualul operațional. Servicii de Certificare și de Marcare Temporară
[XIX]	IISMS-DOC-08-Regulamentul de siguranță a informațiilor societăților
[XX]	HR001 Profilul Furnizorului de Servicii de Încredere
[XXI]	Manualul de guvernanță ISMS
[XXII]	ISMS-DOC-06 - Manualul de management și control al riscului informațiilor
[XXIII]	Politica de continuitate a afacerilor ISMS-DOC-A17
[XXIV]	Politica de gestionare a incidentelor ISMS-DOC-A16
[XXV]	ISMS-FORM-08-Evaluarea riscurilor și planul de măsuri -V1 Final
[XXVI]	Propunere pentru Articolul 19 Raportarea incidentelor - Anexa A
[XXVII]	Declarația privind practicile serviciilor de încredere
[XXVIII]	ISMS-DOC-08 - Politica operațională de securitate a informațiilor.23.02.2017-V1
[XXIX]	Semnătură Electronică Calificată la distanță – Cerere de autorizare pentru utilizarea aparatelor Thales în conformitate cu art. 35, alineat 5 din CAD



1 INTRODUCERE

Acest document este Declarația de Transparență a PKI, conform cerințelor standardului european ETSI EN 319 411-1, referitoare la serviciul de certificare oferit de furnizorul de servicii de încredere Namirial S.p.A..

În cele ce urmează, serviciul de certificare este denumit "serviciul AC" (al Autorității de certificare). REGULAMENTUL (UE) NR. 910/2014 AL PARLAMENTULUI EUROPEAN ȘI AL CONSILIULUI din 23 iulie 2014 privind "identificarea electronică și serviciile de încredere pentru tranzacțiile electronice pe piața internă și de abrogare a Directivei 1999/93 / CE" este denumit "Regulamentul eIDAS".

Acest document nu înlocuiește Termenii și condițiile serviciului AC, nici Codul de Practici și Proceduri (CPP) publicate pe site-ul AC (vezi mai jos).

2 INFORMAȚIILE DE CONTACT ALE AUTORITĂȚII DE CERTIFICARE (AC)

AC poate fi contactată la următoarea adresă:

VIA CADUTI SUL LAVORO, 4
60019 - SENIGALLIA (AN)
TEL: 071.63494
FAX: 071.60910

Site web: [https:// http://www.namirialtsp.com](https://http://www.namirialtsp.com)

Info mail: firmacerta@namirial.com

Tel. +39 071.63494

Fax +39 071.60910

Pentru orice întrebări referitoare la această Declarație de Transparență PKI sau la alte documente ale Autorității de Certificare a Namirial S.p.A., vă rugăm să trimiteți un e-mail la firmacerta@sicurezzapostale.it.

Pentru a solicita revocarea unui certificat, urmați procedura on-line descrisă în CPP (necesită acreditările furnizate la data emiterii certificatului). Alternativ, contactați echipa de asistență pentru clienți a Namirial S.p.A la numărul de fax +39.071.60910 sau trimiteți un e-mail la firmacerta@namirial.com. Pentru informații suplimentare, consultați CPP-ul publicat pe site-ul Autorității de Certificare.

3 TIPURI DE CERTIFICATE, PROCEDURI DE VALIDARE ȘI UTILIZARE

Namirial S.p.A. eliberează certificate calificate în conformitate cu standardele europene ETSI EN 319 411, EN 319 412 și cu alte standarde conexe. Certificatele sunt oferite publicului larg (companii private, entități publice, profesioniști, persoane private etc.), în condițiile publicate pe site-ul Web al Autorității de Certificare.

Toate certificatele sunt semnate cu funcția "hashing" SHA-256. Pentru informații suplimentare despre politicile acceptate privind certificatele (de exemplu, OID-urile respective (identificatoarele de obiect) și alte caracteristici), consultați documentația publicată pe site-ul Autorității de Certificare la adresa <https://docs.namirialtsp.com/>.

Certificatele emise de CA cu privire la SA Namirial sunt publicate pe site-ul Autorității de Certificare și pe site-ul AgID (Agenzia per l'Italia Digitale) la adresa www.agid.gov.it (a se vedea Lista furnizorilor de servicii de încredere).

Pentru a permite validarea certificatelor, Autoritatea de Certificare pune la dispoziție atât Lista Certificatelor Revocate (CRL), cât și un serviciu de verificare a statusului online, pe baza standardul OCSP. Adresele URL ale ambelor sunt incluse în toate certificatele, respectiv în extensiile CRLDistributionPoints și AuthorityInformationAccess.



4 LIMITE DE ÎNTREBUIŢARE

CertIFICATELE sunt eliberate pentru semnături electronice și sigilii electronice avansate și calificate.

Limitările privind utilizarea certificatelor pot fi specificate chiar în cadrul certificatelor, în atributul UserNotice (Informare pentru Utilizatori) al extensiei CertificatePolicies (Politicele Certificatului).

Limitările privind valoarea tranzacțiilor în care poate fi utilizat certificatul pot fi specificate în certificate, în extensia certificatului qCStatements, cu ajutorul elementului QcEuLimitValue.

Toate înregistrările referitoare la durata de valabilitate a certificatelor, precum și toate jurnalele de audit ale serviciului CA, vor fi păstrate de Namirial S.p.A. timp de 20 de ani.

5 OBLIGAȚIILE SEMNATARILOR

Semnatarul certificatului trebuie:

- să furnizeze informații complete, corecte și veridice către Autoritatea de Certificare la momentul solicitării certificatului;
- să utilizeze cheile sale private doar în scopurile și modalitățile permise de CPP;
- să adopte măsuri adecvate pentru a preîntâmpina utilizarea neautorizată a cheilor sale private;
- (pentru certificatele care necesită utilizarea unui aparat de semnătură electronică) dacă își generează singur cheia privată, aceasta trebuie să fie generată într-un aparat de semnătură electronică aprobat de Autoritatea de Certificare;
- până la data expirării certificatului, să informeze imediat Autoritatea de Certificare în următoarele cazuri:
 - o dacă aparatul de semnătură electronică se pierde, este furat sau se deteriorează;
 - o dacă a pierdut controlul exclusiv al cheii private, de ex. din cauza compromiterii datelor de activare (de exemplu, codul PIN) ale aparatului său de semnătură electronică;
 - o dacă unele informații conținute în certificatul său sunt inexacte sau nu mai sunt valabile;
- în cazul compromiterii cheii sale private (de exemplu, din cauza pierderii sau divulgării persoanelor neautorizate a codului PIN al aparatului său de semnătură electronică), încetați imediat să utilizați o astfel de cheie privată și asigurați-vă că aceasta nu va mai fi utilizată.

Pentru informații suplimentare, vă rugăm să consultați CPP.



6 OBLIGAȚIA UTILIZATORULUI DE VERIFICARE A STATUSULUI CERTIFICATULUI

Toți cei care se bazează pe informațiile conținute în certificate (pe scurt, "Utilizatorii") trebuie să verifice dacă certificatele nu sunt suspendate sau anulate. Această verificare poate fi efectuată consultând Lista Certificatelor Revocate (CRL) publicate de Autoritatea de Certificare sau prin interogarea serviciului OCSP furnizat de Autoritatea de Certificare, la adresele (URL-urile) conținute în certificatul propriu-zis.

7 GARANȚIA LIMITATĂ ȘI DECLINAREA / LIMITAREA RĂSPUNDERII

Pentru limitările privind garanția și limitarea răspunderii, consultați Termenii și condițiile serviciului Autorității de Certificare calificate, publicat pe site-ul web Namirial la adresa <https://docs.namirialtsp.com/>.

8 ACORDURI APLICABILE, CPP, PC

Acordurile și condițiile care se aplică serviciului Autoritatea de Certificare se găsesc în următoarele documente, publicate pe site-ul Namirial S.p.A., la <https://docs.namirialtsp.com/>:

- Codul de Practici și Proceduri (CPP) al Autorității de Certificare calificate
- Termenii și condițiile generale ale Autorității de Certificare calificate

Politicile de certificare (PC) acceptate sunt descrise în CPP; a se vedea și secțiunea 3 de mai sus.

9 POLITICA DE CONFIDENȚIALITATE

Namirial respectă Regulamentul UE nr. 679/2016 și recomandările și prevederile Autorității italiene pentru Protecția Datelor. Pentru informații suplimentare, consultați Termenii și condițiile generale ale Autorității de certificate calificate, publicate pe site-ul web Namirial S.p.A. la <https://docs.namirialtsp.com/>.

Toate înregistrările referitoare la certificatele calificate emise de Namirial S.p.A. (de exemplu, dovezi ale identității semnatarilor, cereri de emitere a certificatelor, inclusiv acceptarea Termenilor și condițiilor, solicitări de revocare a certificatelor etc.) sunt păstrate de către Namirial S.p.A. pe o perioadă de 20 ani.

10 POLITICA DE RAMBURSARE

Pentru politica de rambursare, consultați Termenii și condițiile generale ale Autorității de certificare calificate publicate pe site-ul web al Namirial S.p.A. la adresa <https://docs.namirialtsp.com/>.



11 LEGEA APLICABILĂ, SOLUȚIONAREA RECLAMAȚIILOR ȘI A DISPUTELOR

Serviciul Autorității de certificare furnizat de Namirial S.p.A se supune legislației italiene și europene. Aplicabilitatea, executarea, interpretarea și validitatea CPP sunt reglementate de legislația italiană și de legile europene direct aplicabile, indiferent de contract sau de altă alegere a dispozițiilor legale și fără necesitatea de a stabili un punct comercial de contact în Italia. Această alegere este menită să asigure uniformitatea procedurilor și interpretărilor pentru toți utilizatorii, indiferent de locul în care locuiesc sau în care folosesc serviciul.

Pentru toate disputele legale legate de serviciul Autorității de certificare Namirial SpA, în cazul în care Namirial SpA este reclamantă sau pârâtă, Instanța de judecată din Ancona are competență exclusivă, cu excluderea oricărei alte instanțe de judecată și excluzând orice ipoteză în care legea prevede instanța de judecată cu competențe în ceea ce privește Consumatorul.

12 LICENȚELE TSP (ALE FURNIZORULUI DE SERVICII DE ÎNCREDERE) ȘI ALE DEPOZITARULUI, MĂRCILE DE ÎNCREDERE ȘI AUDITUL

Începând cu 3 noiembrie 2010, Namirial S.p.A. este un Furnizor de Servicii de certificare (Autoritate de certificare) înscris în registrul public al Autorităților de Certificare acreditate, deținut de Agenzia per Italia Digitale (AgID).

Începând cu 1 iulie 2016, Namirial S.p.A. este furnizor de servicii de certificare și de servicii electronice de marcaje temporale conform Regulamentului eIDAS și, prin urmare, a fost înscrisă în Lista furnizorilor de servicii de încredere (TSL) din Italia publicată de AgID. Serviciul Autorității de Certificare Namirial S.p.A. este supus evaluării conformității la fiecare doi ani, în conformitate cu normele europene ETSI EN 319 411-1 și ETSI 319 411-2, de către un auditor independent, calificat și acreditat, conform cerințelor Regulamentului eIDAS