Disposable Signature Certificates

Operating Manual Addendum

Category	**Certification Authority**	Docuement ID	**NAM-MO-FDMT-ADD-DISP-ENG**	**Namirial S.p.A.**
Written by	**Simone Baldini**	Confidentiality note	**Public Document**	Legal Representative
Verified by	**Giuseppe Benedetti**	Version	**1.3**	**Davide Ceccucci**
Approved by	**Davide Ceccucci**	Issuance date	**01/10/2018**	CECCUCCI DAV 2018.10.03 10:32:05 CN=CECCUCCI DAVIDE C=IT O=NAMIRIAL S.p.A. 2.5.4.97=VATIT-02046570 RSA/2048 bits

Namirial S.p.A.

Registered office, management and administration 60019 Senigallia (AN) - via Caduti sul Lavoro, 4
Tax Code/REG. REGISTER OF COMPANIES OF ANCONA no. 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

– This page is intentionally left blank –

INDEX

HISTORY OF CHANGES

VERSION	**1.3**
Date	01/10/2018
Reason	Fourth issue
Changes	Added the definition for "Long-lived Disposable" certificates.

VERSION	Errore. Nome della proprietà del documento sconosciuto.
Date	28/06/2018
Reason	Third issue
Changes	New usage-restriction added.

VERSION	**1.1**
Date	26/01/2018
Reason	Second issue
Changes	New usage-restriction added.

VERSION	**1.0**
Date	03/05/2016
Reason	First issue
Changes	Operating Manual to request, issue and use a Digital Signature accompanied by "Disposable" certificates.

REFERENCES

NUMBER	DESCRIPTION
[I]	Legislative decree No.159 dated April 4, 2006 Supplementary and corrective provisions to Legislative Decree No. 82 dated March 7, 2005, including the code of digital administration.
[II]	DPCM 12/10/2007 Postponement of the deadline authorizing self-certification of compliance with safety requirements as per Article 13, paragraph 4, of the Prime Minister's Decree published on the Official Gazette No. 13 dated October 30, 2003
[III]	Legislative decree No.82 dated March 7, 2005 Digital Administration Code (CAD)
[IV]	CNIPA/CR/48 Authority for Informatics in the Public Administration (CNIPA) memorandum dated September 6, 2005 Procedure to submit an application for registration in the list of Public Certification Authorities, as per Article 28, paragraph 1 of Presidential Decree No. 445 dated December 28, 2000.
[V]	DPCM 22/02/2013 Technical rules regarding the generation, affixing and verification of: electronic advanced, qualified and digital signatures.
[VI]	Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)
[VII]	Presidential Decree No. 445 dated December 28, 2000. Consolidation Act of legislative and regulatory provisions regarding administrative documentation.
[VIII]	CNIPA Resolution No. 45 dated May 21, 2009 and subsequent amendments. This resolution repealed: CNIPA Resolution No. 4 dated February 17, 2005 n. 4- CNIPA Resolution No. 34 dated May 18, 2006 Rules for the recognition and verification of electronic document.
[IX]	CNIPA limitations of use on CQ. Limitations of use guaranteed to users in accordance with Article 12, paragraph 6, letter c) of the CNIPA Resolution No. 45 dated May 21, 2009
[X]	RFC 3647 Certificate Policy and Certification Practices Framework
[XI]	RFC 5280 Internet X.509 Public Key Infrastructure - Certificate and CRL Profile
[XII]	ETSI TS 101 456 Policy requirements for certification authorities issuing qualified certificates
[XIII]	ETSI TS 101 862 Qualified Certificate profile
[XIV]	ETSI TS 102 023 Policy requirements for time-stamping authorities
[XV]	ITU-T X.509 ISO/IEC 9594-8 Information Technology – Open Systems Interconnection – The Directory: Authentication Framework
[XVI]	DigitPA – Commissioner Determination No. 69/2010. Resolution amendment No. 45 dated May 21, 2009 issued by CNIPA containing "Rules for the recognition and verification of electronic document", published on December 3, 2009 on the Official Gazette of the Republic of Italy - General Series - No. 282.
[XVII]	CAD 30/12/2010 No.235 Amendments and supplements to Legislative Decree No. 82 dated March 7, 2005 including the Code on Digital Administration, in accordance with Article 33 of the Law No. 69 dated June 18, 2009.
[XVIII]	Legislative Decree 231/2007 "Application of the directive 2005/60/EC concerning the prevention of the financial system use for money laundering purposes for money originating from criminal activities and financing to terrorism as well as directive 2006/70/EC that specifies its implementation measures".
[XIX]	Legislative Decree No. 83 dated June 22, 2012. Urgent measures for the building and transport infrastructure. Article 22 of the DigitPA and the Agency for the spreading of innovation technology have been deleted. The two agencies were joined into the Agency for Digital Italy.

[XX]	RFC 2560 X.509 Internet Public Key Infrastructure Online Certificate Status Protocol – OCSP.
[XXI]	RFC 3161 Internet X.509 Public key infrastructure Time Stamp Protocol (TSP) PKIW Working Group IETF - August 2001.
[XXII]	Decree of the Ministry of Interior, the Minister for Innovation and technologies, and the Minister of Economy and Finance dated December 09, 2004. Technical and safety requirements related to the technologies and materials used in the manufacturing of National Services Card "published on the Official Gazette No. 296, dated December 18, 2004.
[XXIII]	Directive 2005/60/EC issued by the European Parliament and Council dated October 26, 2005, on preventing the use of the financial system for the purpose of money laundering and terrorist financing
[XXIV]	Directive 2006/70/EC dated August 1, 2006 containing implementing measures for the Directive 2005/60/EC of the European Parliament and Council regarding the definition of "persons politically exposed " and the technical criteria for simplified procedures for the adequate verification of the clientèle and for exemption in case of financial activity conducted on an occasional or very limited basis
[XXV]	Directive (EU) 2015/849 of the European Parliament and of the Council dated May 20, 2015, concerning the prevention of use of the financial system for money laundering or terrorist financing, amending (EU) Regulations No. 648/2012 of the European Parliament and Council and repealing Directive 2005/60/EC of the European Parliament and Council and Commission Directive 2006/70/EC.
[XXVI]	Regulation (EU) no 910/2014 of the European Parliament and of the Council of 23 july 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC

Table 1: Regulation and Technical References

INDEX OF TABLES

1 INTRODUCTION

1.1 PURPOSE AND APPLICATION

This document is an **Addendum to the Operating Manual for Digital Certification Services issued by Namirial S.p.A.** and it has the purpose of describing the rules and operating procedures adopted by the Certification Authority to issue qualified "Disposable" digital certificates. The feature of said qualified certificates is to have a short validity and/or usage, no longer than 60 (sixty) minutes from the time of issuance.

1.2 DEFINITIONS AND ACRONYMS USED IN THE DOCUMENT

TERM OR ACRONYM	MEANING
AgID	Agency for Digital Italy [XIX].
Time-stamping authority	It is the software/hardware system managed by the Certification Authority that provides the time-stamping service.
Digital Certificate Qualified Certificate	It is an electronic document certifying, by digital signature, the association between a public key and the identity of a subject (natural person). See [I] Art.28
Certification Authority	It is the public or private agency authorized to issue digital certificates by using the certification procedure meeting the international standards and in compliance with Italian and European regulations.
Private Key	It is the cryptographic key used in an asymmetric encryption system; each private key is associated with a public key, and it is in possession only of the holder who uses it to digitally sign documents.
Public key	It is the encryption key used in an asymmetric encryption system; each public key is associated with a private key, and it is used to check the digital signature affixed on an electronic document by the holder of the asymmetric key.
CIE	Electronic Identity Card. In Italy, the paper version of the identity card is meant to be replaced by this document.
CNS	National Service Card
Co-interested and Co-signer	Refer to LRA
CRL - List of suspended and revoked certificates	It is a list of certificates that have been "voided" by the certification authority before their due date. Revocation makes the certificates "void" forever. Suspension makes the certificates "void" for a specific period of time.
CRS	Regional Service Card
CUC	It is the Certified Univocal Code and it is shown on the Registration Request and it is included in the certificate. It uniquely identifies the certificate issued by the Certification authority.

TERM OR ACRONYM	MEANING
CUT	It is the Holder's Univocal Code and it is shown on the Registration Request.
Recipient	It is the person to whom the document is intended and/or evidence of a digitally signed IT document.
Disposable	Qualified Signature Certificate with a short validity period (e.g. 60 minutes)
Secure Device for Creation of the Signature	Hardware device capable to effectively protect the secrecy of the private key.
GdC - Control Journal	The Control Journal is the set of registrations, automatically or manually carried out, of the events established by the Basic Technical rules.
IUT	Holder's Univocal Identification Number, different for each certificate issued.
IR	It is a subject belonging to a Third Party Company, which may at a later date sign an agreement between the Certification authority and the Third Party Company. The latter includes the staff, which is identified as Registration Representative (IR) and must operate according to procedures established and contained in the MO regarding the identification stages of the natural person to whom the digital signature belongs.
LRA	It is the natural or legal person authorized by the Certification authority to carry out operations needed to issue Certificates, according to the procedures identified and described in this Manual. The agency must have previously signed service agreements with the Certification authority. LRA may rely on RAO for operations of identification, registration and issuance.
Timestamp	It is the time of reference that allows time-stamping.
Operating Manual	It is the public document filed at AgID that defines the procedures applied by the Certification authority in carrying out its activities.
OID [Object Identifier]	It is a sequence of numbers, registered under the ISO/IEC 6523 standard, which identifies a particular object within a hierarchy.
OCSP [Online Certificate Status Protocol]	It is a protocol that allows verifying the validity of a certificate in real-time.
Organization	It is an organized group of users (e.g. agencies, companies, corporations, professional boards, associations, etc.) that entered into agreements with the Certification authority to issue digital signature certificates to their employees and/or associates.
OTP	One-Time-Password. Numerical code generated by a physical device used to carry out a two-factor authentication.
PIN [Personal Identification Number]	Code associated to a signature secure device, used by the Holder to access the device functions.
RA	Registration Authority, subject performing the identification of those who request qualified certificates under the procedures established by the Certification authority.
RAO	It is a subject expressly appointed by the Certification authority to carry out, on behalf of the latter, operations of identification and registration of the Holder, as well as to issue the Certificates. Such subject must belong to a LRA.
Contact Person	It is the natural person responsible for the preparation of all documents necessary for the life cycle of the signature and the one maintaining contact with the Certification authority.
Certificates Register	It is the list of certificates issued by the Certifying Authority. The list includes all revoked and suspended certificates, accessible telematically.

TERM OR ACRONYM	MEANING
Revocation of certificate	It is the operation by which the Certification authority voids the validity of the certificate before its natural due date, from an established moment, not retroactive, onwards.
Applicant	It is the subject requesting the Certification authority to issue the qualified certificates. If the subject is different from the Identity Certificate Holder of the Applicant it will be included into the Organization field of the X.509 certificate.
RSA	Asymmetric encryption algorithm, based on public and private keys.
SHA-1 [Secure Hash Algorithm]	Cryptographic algorithm that generates a 160-bit digital fingerprint.
SHA-256 [Secure Hash Algorithm]	Cryptographic algorithm that generates a 256-bit digital fingerprint.
SBA - Biometric Authentication System	Correlation between a natural person and his/her physiological and/or behavioral characteristics
Suspension of certificate	It is the operation by which the Certification authority suspends the validity of the certificate before its natural due date, for a specific period of time that is not retroactive.
Interested Party	It is the natural or legal person that gives consent, in accordance with the regulations, to issue qualified certificates in which belonging to an Organization or any powers of representation or titles and positions held is shown. It has the right/duty to request the revocation or suspension of the Certificate in the event that the requirements on which the certificate was issued have been changed.
Holder	It is the natural person, identified by the Certification authority, to whom the digital signature belongs.
X.509	It is a standard ITU-T for infrastructures with public key (PKI).

Table 1: Definitions and Acronyms

2 THE CERTIFICATION AUTHORITY

2.1 CERTIFICATION AUTHORITY IDENTIFICATION DATA

In accordance with [III] and subsequent amendments, Namirial S.p.A is the Accredited Certification Authority which issues, publishes in the register and revokes Qualified Certificates (or Subscription Certificates) and CNS, in accordance with current technical regulations. The Certification authority is identified as shown in the following table.

Corporate name:	NAMIRIAL S.p.A.
Registered office:	VIA CADUTI SUL LAVORO, 4 60019 - SENIGALLIA (AN) TEL: 071.63494 FAX: 071.60910
Location of Office Providing the Service:	VIA CADUTI SUL LAVORO, 4 60019 - SENIGALLIA (AN) TEL: 071.63494 FAX: 071.60910
VAT Number	IT02046570426
Registration at the Business Registry	of Ancona
Economic and Administrative Index (REA)	02046570426
Share Capital:	€ 6,500,000 fully paid up
Service Website Address:	http://www.firmacerta.it
Portal URL address for the Holder:	https://cms.firmacerta.it/areaPrivata
Certification Authority Website Address:	http://www.namirial.com
Certified Email Address (PEC):	firmacerta@sicurezzapostale.it
Certification Authority Email:	firmacerta@namirial.com

Table 2: Certification authority identification data

2.2 SUMMARY DESCRIPTION OF NAMIRIAL S.P.A.

Namirial S.p.A. is an IT and web engineering company operating in the Information Technology sector specialized in producing software for the new and increasing needs to adapt the Italian manufacturing sector facing highly competitive and globalized economic scenarios. Within a national economic structure characterized for the most part by the activity of small and medium businesses, it was deemed essential to develop solutions and software services accessible also via Internet and capable to provide solutions to emerging technological and modern issues in a professional manner while maintaining cost-efficiency. The company has is head office in a modern facility of more than two thousand square meters, where it features an Internet Data Center equipped with all the required security systems needed to ensure the inviolability of the data and to support users in need of hosting services, housing services and in general server farm services.

Namirial S.p.A. è:	
	A Qualified Certification Authority accredited by AgID (former DigitPA) and authorized to issue qualified certificates in accordance with Regulation (EU) no 910/2014 of the European Parliament and of the Council of 23 july 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC, as well as CNS certificates and Time-Stamps.
	Certified Email (PEC) Manager since 26/02/2007, accredited by AgID (former DigitPA) and authorized to manage Certified Email **boxes and domains**.
	SPID Identity Provider, since 13/04/2017, AgID approved (as for BVI certiifcate #IT273825), under: - Commission Implementing Regulation (EU) 2015/1502 - Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 eIDAS.
	Long Data Preservation Service Provider, since 13/03/2015, AgID approved (as for BVI certiifcate #IT277150), under: - DPCM 3 Dec 2013; - Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 eIDAS.
	Certified ISO 9001:2015. Namirial was awarded certificate No. 223776 issued by **Bureau Veritas Italia S.p.A.**
	Certified ISO/IEC 27001:2013. Namirial was awarded certificate No. IND12.2513U issued by **Bureau Veritas Italia S.p.A.**
	Adobe Certified. Since June 2013 Namirial is a **member of AATL** (Adobe Approved Trust List).

Table 3: Namirial S.p.A. certifications

2.3 CONTACTS AND HELPDESK

In order to receive information about Namirial S.p.A. products and Certification services, please use the following contact details:

- Phone: (+39) 071 63494
- e-mail : commerciale@firmacerta.it
- Web: http://www.firmacerta.it

To receive technical information and assistance on the service, use the following contact details:

- Phone: (+39) 071 63494
- e-mail : helpdesk@firmacerta.it
- Web: http://www.firmacerta.it

The service is available on weekdays from 9:00 a.m. to 1:00 p.m. and from 2:00 p.m. to 7:00 p.m.

2.4 DOCUMENT VERSION

This document named "**NAM-FDMT-MO-ADD-DISP-ENG**" is identified by a revision number and issue date shown on all pages. The document introduction also shows the history of revisions carried out. At least once a year, the Certification Authority performs a compliance check on the certification service delivery process and, where necessary, it updates this document also taking into account the development of the applicable regulatory and technological standards.

2.5 PUBLICATION OF DOCUMENT

This document and any other documents issued for particular topics and in special cases, such as the Operating Manual, are kept at the Certification authority's office but they are filed at AgID and are available, electronically, at the following web addresses (under Article 40 paragraph 2 of [V]): http://www.firmacerta.it/manuali-MO. This URL is also shown in the cSPuri field of the "Certificate Policies" extension for qualified certificates, Time-stamping and OCSP servers.
This document is published in PDF format, signed to ensure its origin and integrity.

2.6 DOCUMENT MANAGER

The responsibility of this Addendum to the Operating Manual falls on the Certification Authority as "Manager of the temporal certification and validation service" (Article 40 paragraph 3 letter c) of [V]), which is responsible for its preparation, publication and update. Notifications concerning this document must be sent to the attention of the aforementioned Manager at the following addresses:

- Phone: (+39) 071 63494
- e-mail : firmacerta@namirial.com
- fax: (+39) 071 60910

3 GENERAL RULES

3.1 PARTIES INVOLVED IN THE PROCESSES

The parties mentioned in this document are:

- The Certification Authority
- The Registration Authority (RA)
- The Local Registration Authority (LRA)
- The Registration Authority's Operator (RAO)
- The Party in charge of the Registration (IR)
- The Holder
- The Interested Third Party

3.2 OBLIGATIONS OF THE CERTIFICATION AUTHORITY, HOLDER AND PARTIES REQUESTING THE SIGNATURE VERIFICATION

3.2.1 CERTIFICATION AUTHORITY'S OBLIGATIONS

Namirial S.p.A., the Certification authority:

1. meets the requirements of the current legislation on Digital Signature [III], [V], [VIII], [XVII] and subsequent amendments;
2. identifies with certainty the person applying for certification;
3. makes sure of the authenticity of the application for certification;
4. issues and manages a qualified certificate only in the cases allowed by the certificate holder according to procedures and cases established by Article 32, paragraph 3, letter b) of [III], in accordance with [VI], and subsequent amendments;
5. provides or specifies to the Holder the security signature devices used for the issuing of qualified certificate, for the generation of the key, the preservation of the private key and signature operations necessary to protect the private key and data for the creation of the signature of the Holder according to secure criteria in compliance with the current legislation and latest scientific and technological knowledge;
6. notifies in advance to the Holder, in a complete and clear fashion, concerning the certification process and the requirements needed to access it, the characteristics and limitations of use of signatures issued on the basis of the certification service.
7. is not the depositary of the data, in their entirety, for the creation of the Holder signature;
8. does not copy or duplicate the private signature keys of the subject to whom the certification authority provides the certification service;
9. ensures the accurate identification of the date and time of issue, the due date, cancellation and suspension of qualified certificates;
10. records on the control journal the issuing of qualified certificates, specifying the date and time of generation; the time of generation of the certificate is certified by a time reference;
11. keeps a record, including electronically, of all the information related to the qualified certificate from the time of its issuance to at least 20 (twenty) years, also to provide evidence of certification for any legal proceedings;

12. makes available electronically a copy of the lists, signed by AgID, of the certificates related to the certification keys referred to in [V];
13. provides at least a system that allows the Holder to verify the qualified signature;
14. adopts secure measures for the processing of personal data, in accordance with[VI].

3.2.2 HOLDER'S OBLIGATIONS

The Holder of qualified certificates has the obligation to:

1. read carefully this document before requesting a qualified certificate and comply with its applicable requirements;
2. provide all the information required by the Certification Authority guaranteeing the reliability of such data under its own responsibility;
3. keep exclusively and preserve with the utmost care the OTP device that may be provided;
4. not to use the qualified signature for functions and purposes other than those for which it was issued;
5. adopt the measures established by this manual in order not to affix qualified signatures on documents containing macro instructions or executable codes that may change the acts or facts that are represented and that would therefore void the effectiveness of the signature;
6. adopt appropriate security measures (e.g. Anti-virus/anti-malware) in order to prevent the fraudulent use of the signature devices.

3.2.3 OBLIGATIONS OF PARTIES REQUESTING THE VERIFICATION OF SIGNATURES

Those who verify digital signatures generated with keys certified by NAMIRIAL are required to verify:

1. that the certificate of the Holder was issued by an accredited Certification authority
2. the authenticity of the certificate containing the public key of the document's signer;
3. the absence of the certificate from the Revocation and Suspension Certificate List (CRL)
4. the existence of and compliance with any limitations of use for the certificate used by the holder;
5. the integrity of the document received through a verification software in compliance with the current legislation.

The interested Third Party is required to:

1. collect, upon explicit consent of the applicants, the data required for registration in the form specified by the Certification authority;
2. request the revocation and suspension of the certificates according to the procedures specified in this document whenever the conditions under which the certificate was issued to the holder are not met (halt of business activities, change of tasks, suspensions, etc.).
3. promptly notify to the certification authority any change in the circumstances specified at the time of issuance of the relevant certificate for the purposes of its use;
4. submit the request for revocation or suspension to the Certification authority along with signature and motivation, specifying the effective date (and term in case of suspension).

3.2.4 LOCAL REGISTRATION AUTHORITY'S OBLIGATION (LRA)

The LRA is required to:

1. notify in advance to the Holder, in a complete and clear fashion, concerning the certification process and the requirements needed to access it, the characteristics and limitations of use of signatures issued on the basis of the certification service.
2. inform the Holder about the obligations assumed by the latter concerning the preservation with utmost diligence of the OTP device that may be provided;
3. request, when required and before issuing the certificate, the proof of possession of the private key and verify the correctness of the key pair;
4. inform the Holder about the security measures adopted for the processing of personal data, in accordance with [VI];
5. identify with certainty the person applying for certification;
6. ensure the authenticity of the application for certification;
7. notify to the Certification Authority all data and documents obtained during the Holder identification process and required by the Certification Authority to promptly activate the issuing of the certificate;
8. verify and submit to the Certification authority the revocation/suspension requests requested by the Holder at the LRA;
9. strictly follow the rules issued by the Certification Authority and described in this document and, where appropriate, in the Operating Manual.
10. When he is a Co-Interested and Co-Signer, for application of the Long-Lived Disposable remote signature procedure, described in this Manual, he is obliged to respect the additional restrictions set forth in §4.1.1

The Certification Authority, without prejudice to the right for compensation, is the one and only responsible entity towards third parties for the activity carried out by the LRA.
The Certification Authority periodically verifies compliance with the procedures adopted by the LRA and what is specified in this document. In any case, upon simple request of the Certification authority, the LRA is required to send to the Certification Authority all the documentation in its own possession related to each request for the issuance of signature certificates originating from each Holder.

3.3 LIABILITY AND INDEMNIFICATION LIMITATIONS

3.3.1 CERTIFICATION AUTHORITY'S LIMITED LIABILITY

The Certification authority is responsible towards the Holders for the fulfillment of the legal obligations resulting from the activities referred to in [III], [IV], [V], [VI], [VII], [VIII], [XVII] and subsequent amendments and integrations.
The Certification Authority does not assume any responsibility:

- for the misuse of the issued certificates;
- for any consequences resulting from ignorance or non-compliance, by the Holder, with the procedures and operating methods specified in this document;
- for non-fulfillment of its obligations due to causes not attributable to it;

3.3.2 LIMITATIONS AND INDEMNITIES

According to Article 57, paragraph 2 of [V], the Certification Authority has entered into an insurance policy agreement to cover the risks related to the activity and damages towards all the parties involved (Holders, Interested Third Parties, Recipients) not exceeding the maximum amounts specified below: € 150,000 per individual accident for a total of € 1,500,000 per insurance year for all financial losses resulting from any claims for compensation made against the Certification Authority for all combined insurance coverages.

3.4 PERSONAL DATA PROTECTION

The policies for data access are in compliance with the minimum-security measures for the processing of personal data established by [VI] in particular, they allow:

- the appropriate procedures to appoint the person in charge of the processing;
- the identification of the data supervisor and persons in charge;
- the assignment of identification codes;
- the protection of computer terminals.

The information regarding the Holder and the interested Third Party of which the Certification Authority becomes aware during the activity should be considered, unless specific consent is provided, confidential and non-publishable with the exception of those cases specifically intended for public use (Public Key, Certificate, Suspension, Revocation, etc.) in accordance with the current legislation and with the consent provided by the Holder.

3.5 RATES

The service rates are published on the website www.firmacerta.it under the Shop section or available at the LRA Registration Offices.

4 POLICIES, LIMITATIONS OF USE AND MANAGEMENT OF CERTIFICATES

4.1 CERTIFICATE POLICY

The Certification Authority uses the following Object Identifier (OID):

1.3.6.1.4.1.36203	NAMIRIAL S.p.A.
1.3.6.1.4.1.36203.1	CA Qualified Signature
1.3.6.1.4.1.36203.1.1	CA Policy Qualified Signature

Table 4: Policy OID

Certificates issued in accordance with the rules of this document are identified by the following Object Identifier (OID):

1.3.6.1.4.1.36203.1.1.6	The policy for qualified certificates associated with a secure device for creating the signature through a Disposable remote procedure.
1.3.6.1.4.1.36203.1.1.7	The policy for qualified certificates associated with a secure device for creating the signature through a Long-Lived Disposable remote procedure.

Table 5: Specified Policy OID for Disposable and Long-Lived Disposable certificates

4.1.1 LONG-LIVED DISPOSABLE PROFILE

The Long-Lived Disposable certificate profile allows to manage the Qualified Certificate issuance in restricted use-cases restricted to closed-group users contexts, where digital signatures do not produce any legal effect if the verification of the certificate holder identity is not completed with a positive result.
A typical use case is when the document to be signed is a contract that needs to be executed by two or more parties and it does not carry any legal effect until all parties have signed it.

This kind of certificate, as for the provisions included in the communication AgID 0016101.07-06-2016, provided that certain domain's constraints do exist as well as restricted scopes of usage, allows the use of the digital signature before having completed the certificate holder identification process, under the following conditions:

RESTRICTION	RESPONSIBILITY
1. The process is related exclusively to remote signature systems;	Certification Autority
2. The use of digital signature must take place in a closed user environment	Certification Autority
3. The qualified certificate shall include specific usage restriction related to the relationship scope between the certificate holder and the co-interested party/co-signer. (see § 4.2);	Certification Autority

RESTRICTION	RESPONSIBILITY
4. The certificate must be clearly distinguishable from those issued with more traditional procedures. The qualified certificate shall include a specific OID, which is defined in the operating manual, describing this particular process and its restricted scope (§ 4.1);	Certification Autority
5. Tighten application limits must exist. The application that requires remote signature must limit the possible subscription objects to the documents proposed by the co-interested and co-signer. The documents to be signed must be legally imperfect. It means that as long as both the signature of the co-interested and co-signer are missing the document has no legal effect. For example, contracts for joining a service	Co-interested and Co-Signer
6. In the event that the Holder Identity verification takes place through a physical meeting between the holder and the responsibility for the identity verification, the latter must be the personal of the Certification Authority or the person delegated by him, but not any agent belonging to the co-interested and co-signer if different from the Certification Authority	Certification Autority
7. The co-interested and co-signer can carry out the verification of the identity on behalf of the Certification Authority, through audio-video sessions, through the procedures indicated by the Certification Authority and approved by AgID, or as an application of the local regulation implementing the identity verification referred to the Anti Money Laudering regulation in force, where applicable. In case, in the context of the verification pursuant to the AML local regulaiton, the bank transfer is used, it must be verified that this bank transfer originates from a bank account made out exclusively to the certificate holder;	Co-interested and Co-Signer
8. Upon the holder's signature is applyed, the Certification Authority is required and committed to not apply the timestamp.	Certification Autority
9. Upon signing the holder's signature, the Co-Interested and Co-signer is required and committed to not apply the timestamp.	Co-interested and Co-Signer
10. The timestamp shall be necessarily applied after the signature of the co-interester and co-signer in order to obtain a signed document which carries full legal effect;	Co-interested and Co-Signer
11. As long as the signatures and timestamp, referred in the previous point 10, are not applied, the document which is signed just by the holder must not be provided to anyone and, if the verification of the holder's identity has not been successfully completed, the signed document shall be destroyed by keeping audit trail log events .	Co-interested and Co-Signer

Table 6: Long-Lived Disposable issuing conditions

As a further safety measure aimed to reducing the end user's exposure to the risk of using their digital signature, the Long-Lived Disposable certificate can be used only within 60 minutes starting from the issue time.

4.2 LIMITATIONS OF USE

Without prejudice to the responsibility of the ***Certification Authority*** referred to in [III] (article 30 paragraph 1 letter a), it is the responsibility of the ***Holder*** to verify compliance with the limitations of use included in the certificate.
The request to include other specific limitations of use, the text of which may not exceed 200 characters, will be assessed by the **Certification Authority** for its legal, technical and interoperability aspects and priced accordingly.
In view of the aforementioned limitations, the ***Certification Authority*** adopts the limitations of use specified by the users, in accordance with Article 12, paragraph 6, letter c) of the Resolution [VIII] and subsequent amendments, and includes, on request of the Holder or the legal person requesting the certificate, at least the following **limitations of use**:

- I titolari fanno uso del certificato solo per le finalità di lavoro per le quali esso è rilasciato. / The certificate holder must use the certificate only for the purposes for which it is issued.
- L'utilizzo del certificato è limitato ai rapporti con *(indicare il soggetto)*. / The certificate may be used only for relations with the *(declare the subject)*.
- Valido solo per la sottoscrizione di polizze assicurative, escluse polizze vita caso morte/The certificate may be used only to sign insurance contract, excluded the ones for whole life insurance
- Valido solo per la sottoscrizione di contratti di telefonia mobile/ The certificate may be used only to sign mobile phone contracts

Please note that the subject specified in the above limitation of use must be intended as the legal person, acting as the interested third party and/or LRA.

4.3 INFORMATION CONTAINED IN THE DISPOSABLE CERTIFICATES

All certificates issued comply with ISO 9594-8-2001 standards, current regulations and, in particular, with what is specified by Resolution [VIII] and subsequent amendments. Consequently, their interoperability is guaranteed in the context of activity of the Italian accredited certification authorities.

4.4 CERTIFICATE REGISTER

The certificate register contains:

- all the certificates issued by the Certification Authority;
- The list of suspended and revoked certificates (CRL).

4.4.1 ACCESS TO THE CERTIFICATE REGISTER

The reference copy of the certificate register is accessible only from the certificate generation system. The publication of the information on operational copies of the certificate register is only allowed to the Certification Authority. Such information is publicly accessible only in read-only mode and through the http protocol. To avoid having CRLs that are too large, at the time of issue of each certificate, the Certification Authority associates to the latter a specific CRL whose full downloading address is included in the CRL Distribution Point extension. The CRLs related to the qualified and authentication certificates are distinguished by a progressive number, positioned before the file extension. Suspended or revoked certificates are included and published in the CRL itself, already described in the Operating Manual and published on: http://crl.firmacerta.it/FirmaCertaQualificata1.crl.
Upon the issuance of the revocation list, the Certification Authority guarantees the publication of all CRLs needed to cover all the certificates issued until then by the Certification Authority. Certificates and partitioned CRLs are issued in compliance with the RFC 5280 technical specification, with particular reference to the extensions necessary to the CRL partitioning described herein. According to Article 42, paragraph 3 of [V] the Certification Authority also makes accessible at the following URL the copy of the list, signed by the Agency, of the certificates related to the certification keys referred to in Article 43, paragraph 1, letter e) of [V]:

https://cms.firmacerta.it/certificatori/certificatori.zip.p7m

4.4.2 CERTIFICATE REGISTER MANAGEMENT

The reference copy of the certificates register is managed by the certification authority; it is not accessible from the outside and contains all the qualified certificates and revocation lists issued by the certification authority. All operations that change data within the register are automatically included in the Control Journal. The register is updated upon issuing qualified certificates and upon publication of the revocation list (CRL). The certificate revocation lists (CRL) are publicly accessible in read-only mode and contain the revoked or suspended signed certificates. The publication of the revocation lists is updated in synchrony with every update of the certificate register that are revoked or suspended.

5 OPERATIONS

This section describes the procedures with which the Certification Authority operates and in particular the organization and roles of the staff responsible for the certification service, the procedures to request the certificate, the identification of the applicant and the communication procedures with the applicant for the certificate, that is the certificate Holder.

5.1 IDENTIFICATION AND REGISTRATION PROCEDURES

The requesting Holder may be identified:

- by authorized personnel of the Certification authority or by the LRA registration offices;
- by the Contact Person of the Interested Third Party who signed an Agreement;
- through its electronic identity associated with a digital signature certificate, a CNS or CIE, that is SPID (Public Digital Identity System) credentials of level 3 issued by Namirial;
- through the recognition already carried out by a financial broker or other party exercising financial activity;
- through the credentials issued for a previous Disposable certificate;

The next paragraphs show in details the aforementioned procedures.

5.1.1 IDENTIFICATION THROUGH AUTHORIZED PERSONNEL OF THE CERTIFICATION AUTHORITY OR THE LRA REGISTRATION OFFICES

The requesting Holder may be identified by visiting the Certification Authority office (or a LRA registration office) accompanied by a valid identity document or an equivalent identification document according to article 35 of [VII]. The Holder may also be identified electronically through the "FACE/VISI" remote identification system of the Certification Authority or equivalent system; to this end, it is necessary that the Holder is in possession of a personal computer, a webcam connected to it and a working PC audio system or a smartphone, tablet, or other computing devices with equivalent features.
In order to ensure the protection and management of the personal data, in full compliance with Legislative Decree 196/2003, any applicant will be provided in advance with the privacy policy statement and will be required to consent to the video recording and data processing by the persons appointed by the Certification Authority. Each applicant will also be informed about the fact that for security reasons the video call (video/voice) will be recorded and kept in accordance with the provisions of article 32, paragraph 3, letter j) of the CAD and that in case of false statements, false documents, use or presentation of false documents or documents containing data no longer valid, will be subjected to the criminal penalties established by article 76 of the [VII].
Only after the applicant consent to the video conference, the recording may be started and begin with the repetition of the request of consent process.
The specific telematics procedures of identification and recording designed by the Certification Authority and implemented by its appointed staff on that occasion are not made public for security reasons.
In detail, the recording data, consisting of video and audio files and metadata structured in electronic format, are stored in a protected form for twenty years at the Certification authority offices. This procedure complies with the requirements of Article 32, paragraph 3, letter a) of the CAD.

The person performing the identification verifies the Holder's identity by checking a valid identification document containing a recent and recognizable photograph of the holder, the related written signature and stamp, issued by a State administration or recognized by it. By way of example, a list of accepted documents is shown below:

a) Identity card;
b) Passport;
c) Driver's License;
d) Boating License;
e) Pension plan booklet;
f) Official qualification certificate for operation of heating plants;
g) Firearms license

It is the right of the person performing the identification to exclude the admissibility of the document used by the Holder if it is deemed unsuitable to provide unambiguous identification.
Such person performing the identification concludes the process by recording the details of the submitted document. Then information such as the validity period, the issuing Agency, the type of document, etc. are collected.

5.1.2 IDENTIFICATION BY THE CONTACT PERSON OF THE INTERESTED THIRD PARTY WHO SIGNED AN AGREEMENT;

The Interested Third Party, in the person of the Contact Person:

- structures the list of Holders subjected to certification by enclosing the necessary information for the registration (personal data, details of identification document, type of product requested, any role performed, any limitation of use, etc.).
- notifies such list to the Certification Authority by using procedures that guarantee their authenticity, origin and integrity;
- It undertakes to obtain acceptance and confirmation by the Holders that they want to proceed with the issuing of the certificate.

5.1.3 IDENTIFICATION THROUGH ONE'S OWN DIGITAL IDENTITY ASSOCIATED WITH A DIGITAL SIGNATURE CERTIFICATE, A CNS OR CIE, THAT IS LEVEL 3 SPID(PUBLIC DIGITAL IDENTITY SYSTEM) CREDENTIALS.

With this method, the Certification Authority bases itself on the recognition already carried out by Namirial or by other accredited subjects. The Holder must be in possession of credentials or electronic instruments suitable to an unambiguous identification.

5.1.3.1 AUTHENTICATION VIA DIGITAL SIGNATURE

This procedure requires that the Applicant fills out the application form needed for the issuance of a digital signature (NAM_CA02 or derivatives), signs it through a qualified electronic signature and submits the signed document to the system. An automated procedure performs the following verifications:

- Signature validity;
- Matching between the person who signed the form and the Applicant;
- that a copy of the same request document has not already been used to obtain another digital signature certificate.

5.1.3.2 AUTHENTICATION VIA LEVEL 3 SPID(PUBLIC DIGITAL IDENTITY SYSTEM)

This procedure requires that the applicant is in possession of credential of Level 3 SPID and that connects to a portal of the Certification Authority or its LRA, which acts as a SPID Service Provider. The access to the functionality of the certificate request, or to the private area that allows its use, takes place using level 3 authentication after the prior use of SPID credentials issued by the Certification authority.
In this way the registration portal obtains the necessary information in the form of SAML messages originating from the SPID Identity Provider that issued the credentials used for the authentication.

5.1.3.3 AUTHENTICATION BY CNS OR CIE

This procedure requires that the applicant is in possession and that makes use of the following cards:

- CNS;
- CRS;
- CIE or equivalent document in the country of origin of the applicant.

After inserting the card PIN, the Applicant performs authentication on the Certification Authority portal. The system retrieves the personal data information included in the digital certificate and associates them with those related to the signed certificate subject matter of the request.

5.1.4 IDENTIFICATION THROUGH THE RECOGNITION ALREADY CARRIED OUT BY A FINANCIAL BROKER OR OTHER PARTY PERFORMING FINANCIAL ACTIVITY.

According to this method, the Certification Authority makes use of the recognition already carried out by a financial broker or other party performing financial activities, which, under the anti-money laundering regulations from time to time in force, is obligated to identify its customers.
The data used for the recognition of the Applicant are issued by the financial party in accordance with specific national regulation according to the Directives [XXIII], [XXIV] and [XXV].

5.1.5 IDENTIFICATION THROUGH THE CREDENTIALS ISSUED FOR THE ISSUANCE OF A PREVIOUS DISPOSABLE CERTIFICATE.

According to this method, the Certification Authority bases itself on the identification already carried out on occasion of issue of a previous Disposable certificate. The Applicant already in possession of credentials is authenticated through the Certification Authority portal or LRA and calls for the issuance of a new Disposable certificate, after confirming or updating the registration data. For issuing the certificate it is necessary that the Holder enters a One-Time-Password sent to his OTP device and the LRA or the Third Concerned Party gives permission to proceed.

5.1.6 APPLICANT REGISTRATION AND ISSUANCE OF CERTIFICATE

The Disposable certificates are issued to be used simultaneously by remote signature applications.
The issuance of Disposable Certificates to natural persons takes place after the Applicant is identified by one of the parties listed in paragraph 5.1. The procedures for the Applicant registration and issuance of the certificate require:

a) that the Applicant is unambiguously identified with one of the procedures described in the previous paragraphs.

b) that the Applicant has read the information referred to in Article 13 of [VI];

c) that the Applicant has given consent to the video recording and data processing, in the case of electronic identification;

d) that the Applicant has communicated its mobile phone number to be used for sending the OTP via SMS.

e) that the Applicant has read and understood the General Terms and Conditions and this Operating Manual Addendum;

f) that the Applicant has expressed the will to obtain the issuance of a Disposable certificate upon confirmation and acceptance of the application for registration, attested by appropriate electronic proof proving their truthfulness and availability at the Certification Authority or LRA location.

The Certification authority or LRA, once completed the identification stage, performs the Applicant registration through the web portal of the digital certification service, or through the provided web-services. The Certification authority subsequently issues a qualified Disposable certificate.
The Certification authority reserves the right to check the authenticity of the provided documentation.
The Applicant upon issuance of the certificate becomes the Holder.

5.2 PROCEDURES TO GENERATE THE KEYS, TO ISSUE CERTIFICATES AND TO USE THE SIGNATURE KEYS

The generation of the asymmetric pair of keys (public and private) is performed by devices and procedures that ensure, based on the current status of scientific and technological knowledge, the uniqueness and strength of the generated keys, as well as the secrecy of the private key. The key generation system ensures:

- compliance of the pair of keys with the requirements established by the generation and verification algorithms used;
- the generation of equi-probability of all possible pairs;
- the identification of the subject activating the generation procedure.

The keys belonging to one of the types listed in article 5, paragraph 4, of [V] are generated (articles 6 and 7), kept (article 8) and used (article 11, paragraph 1) within the same electronic device having the security features referred to in article 12 of [V]. The keys have the characteristics established by articles 4 and 5 of [V].
The key generation takes places within an HSM with OCSI certification or equivalent certification.

5.2.1 CRYPTOGRAPHIC ALGORITHMS AND LENGTH OF THE KEYS

According to Article 3 of [VIII] and subsequent amendments:

- The RSA algorithm (Rivest-Shamir-Adleman) is used in the signing operation;
- The keys used by the Certification Authority for certified signatories have a 2048 bit length;

5.2.2 PROCEDURE TO GENERATE AND PROTECT THE SIGNATURE KEYS

Once completed the recording process, during which the data of the Holders are stored in the Certification authority archives (or LRA), it is possible to generate the signature keys which are generated by the Certification authority. The keys are generated in accordance with [V], Article 6, paragraphs 2, and 7, paragraph 3. The signature devices used comply with the safety requirements established by [V], Article 12, paragraph 1.

5.2.3 REPLACEMENT OF THE CERTIFICATION KEYS

The replacement of the certification keys takes place in compliance with article 30 of [V].
The "Root" certificate of the CA used by the Certification authority to sign qualified Certificates of the Holder lasts 20 years and is replaced at least every 13 years to ensure the usability of all certificates issued until their natural expiration.

5.2.4 HASH FUNCTIONS

The hash SHA-256 function is used for impression-generation. The SHA-1 algorithm is supported only in signature verification mode within the limits of Article 27 paragraph 4 and Article 29 of [VIII] and subsequent amendments.

5.2.5 ISSUANCE OF DISPOSABLE CERTIFICATES

The issuance of certificates for Remote qualified signature applications of a Disposable type (with HSM at the Certification authority) takes place in compliance with Articles 11, 12 and 13 of [V], using a multi-stage articulated process and based on secure communication channels. The Disposable signature certificates are issued in the active state.

5.3 REVOCATION AND SUSPENSION OF A QUALIFIED CERTIFICATE

Despite the limited period of validity of the Disposable certificate, where applicable, the procedures described in the Certification Authority's Operating Manual remain valid.

5.3.1 SUSPENSION PROCEDURE OF THE DISPOSABLE CERTIFICATE

The suspension of the certificate may be carried out directly by the Holder through specific functionalities accessible online through the Certification Authority's portal.
The suspension functionality, operating with the same mechanisms, will be made available to the Holder also through third party portals, such as those of the LRA or the Interested Third Party.

5.4 INSTRUMENTS AND PROCEDURES FOR AFFIXING THE SIGNATURE

To affix remotely the signature, it will be possible to use online applications and operating through services provided by the Certification Authority or the LRA. In the latter case, the Certification Authority makes sure that the system managed by the LRA ensures the exclusive knowledge of the data for the signature creation by the Holders thanks to appropriate security requirements.
The Certification Authority makes available web services to allow the integration with applications requiring signature services. It is understood that the documents to be signed are normally formed by said applications, depending on the specific needs.
The signing request originating from the user, given the short duration of Disposable certificates may be authenticated through either the credential component known to the Holder (OTP), or through a Biometric Authentication System (SBA).
If a SBA is used, upon registration, a set of one or more physiological and/or behavioral characteristics solely attributable to the holder is associated with the Holder, such as: the characteristics of handwritten signatures, the ear shape, the face physiognomy, fingerprints, iris color and size, the hand shape, the hand palm, vascularization, the voice print, the style of typing on the keyboard or body movements.
In the authentication stage, the correspondence with parameters detected during the recording stage will be checked to proceed with the signature.