NETHEOS CA

PKI Disclosure Statement

Version	Date	Description	Auteurs	Société
1.0	04/10/2024	Version initiale	FDV	Datasure

Etat du document - Classification	Référence
Finalisé – C1	OID : 1.3.6.1.4.1.55020.1.1.1.2

1 TSP Contact Info

Any request related to the service shall be sent to the following address. :

M. David EMO
Poste : Directeur technique
Adresse : NAMIRIAL, Les Centuries I, 93 place Pierre Duhem,
34000 Montpellier - France
Email : hello@netheos.com
Téléphone : (+33) 9 72 34 11 80

NAMIRIAL can also be contacted with the contact form available on the Internet website : https://www.namirial.com

2 Certificate type, validation procedures and usage

2.1 Certificates available

NAMIRIAL, with “NETHEOS” business trademark, issues qualified certificates according to European standard ETSI EN 319 411-2 and ANSSI procedure, and certificates related to other standards. Certificates are offered to the general public (private companies, public entities, professionals, private persons, etc.), at the conditions published on the CA website. All certificates are signed with at minimum a hashing function of SHA-256.

2.2 Certificates policy

2.3 Certificate usages

The certificate usage depends on the type of certificate

Case 1. LCP (signature certificate for PDF) 1.3.6.1.4.1.55020.1.1.2.4.5	The private key associated to the certificate allows to create Advanced Electronic Signature based on LCP certificate.
Case 2. NCP+ (signature certificate for PDF) 1.3.6.1.4.1.55020.1.1.2.4.1	The private key associated to the certificate, store in the certified HSM, allows to create Advanced Electronic Signature based on NCP+ certificate.
Case 3. LCP (signature certificate for hash signing) 1.3.6.1.4.1.55020.1.1.2.4.8	The private key associated to the certificate allows to create Advanced Electronic Signature based on LCP certificate.
Case 4. NCP+ (signature certificate for hash signing) 1.3.6.1.4.1.55020.1.1.2.4.7	The private key associated to the certificate, store in the certified HSM, allows to create Advanced Electronic Signature based on NCP+ certificate.
Case 5. NCP+ (seal certificate) 1.3.6.1.4.1.55020.1.1.2.4.3	The private key associated to the certificate, store in the certified HSM, allows to create Advanced Electronic Signature based on NCP+ certificate.
Case 6. NCP+ (seal certificate for hash signing) 1.3.6.1.4.1.55020.1.1.2.4.10	The private key associated to the certificate, store in the certified HSM, allows to create Advanced Electronic Signature based on NCP+ certificate.
Case 6. QCP-l (seal certificate) 1.3.6.1.4.1.55020.1.1.2.4.11	The private key associated to the certificate allows to create Advanced Electronic Signature based on qualified certificate.

2.4 Validation procedure

The validation procedure depends on the type of certificate

Case 1. LCP (signature certificate for PDF) 1.3.6.1.4.1.55020.1.1.2.4.5	Identification of the signatory with and ID document (national ID card, passport, residence permit).
Case 2. NCP+ (signature certificate for PDF) 1.3.6.1.4.1.55020.1.1.2.4.1	Identification of the signatory with and ID document (national ID card, passport, residence permit) and face-to-face process or face-to-face equivalent implementing an automated biometric verification system
Case 3. LCP (signature certificate for hash signing) 1.3.6.1.4.1.55020.1.1.2.4.8	Identification of the signatory with and ID document (national ID card, passport, residence permit).
Case 4. NCP+ (signature certificate for hash signing) 1.3.6.1.4.1.55020.1.1.2.4.7	Identification of the signatory with and ID document (national ID card, passport, residence permit) and face-to-face process or face-to-face equivalent implementing an automated biometric verification system
Case 5. NCP+ (seal certificate) 1.3.6.1.4.1.55020.1.1.2.4.3	Identification of the seal responsible with and ID document (national ID card, passport, residence permit) and face-to-face process or face-to-face equivalent implementing an automated biometric verification system. Identification of the legal representative with and ID document (national ID card, passport, residence permit) and identification of the legal person with authentic source, check of the link between legal representative and the legal person.
Case 6. NCP+ (seal certificate for hash signing) 1.3.6.1.4.1.55020.1.1.2.4.10	Identification of the seal responsible with and ID document (national ID card, passport, residence permit) and face-to-face process or face-to-face equivalent implementing an automated biometric verification system. Identification of the legal representative with and ID document (national ID card, passport, residence permit) and identification of the legal person with authentic source, check of the link between legal representative and the legal person.
Case 6. QCP-l (seal certificate) 1.3.6.1.4.1.55020.1.1.2.4.11	French PVID identification scheme

3 Reliance limits

Certificate and associated are limited to the usage specified in this PDS and in the CP/CPS.s
Audit logs related to the TSP, including registration information, are stored for 7 years after the expiration of the certificate, in application of ANSSI guidelines.

4 Subscriber obligations

The subscriber shall :

- Communicate exact and up-to-date information when requesting or renewing certificate;
- Respect key usages of the private key and corresponding certificate ;
- Notify the CA in case of change of the information within its certificate;
- Perform, without delay, a revocation request in case of compromise (or suspicion) of the private key or activation data.

Additional obligations applies for certain type of certificates.

Case 1. LCP (signature certificate for PDF) 1.3.6.1.4.1.55020.1.1.2.4.5	Non applicable. The security measure regarding the private key is covered by Netheos Signature service.
Case 2. NCP+ (signature certificate for PDF) 1.3.6.1.4.1.55020.1.1.2.4.1	Non applicable. The security measure regarding the private key is covered by Netheos Signature service.
Case 3. LCP (signature certificate for hash signing) 1.3.6.1.4.1.55020.1.1.2.4.8	Non applicable. The security measure regarding the private key is covered by Netheos Signature service.
Case 4. NCP+ (signature certificate for hash signing) 1.3.6.1.4.1.55020.1.1.2.4.7	Non applicable. The security measure regarding the private key is covered by Netheos Signature service.
Case 5. NCP+ (seal certificate) 1.3.6.1.4.1.55020.1.1.2.4.3	Non applicable. The security measure regarding the private key is covered by Netheos Signature service.
Case 6. NCP+ (seal certificate for hash signing) 1.3.6.1.4.1.55020.1.1.2.4.10	Non applicable. The security measure regarding the private key is covered by Netheos Signature service.
Case 6. QCP-l (seal certificate) 1.3.6.1.4.1.55020.1.1.2.4.11	Protect the private key with appropriate means, typically by ensure access control to the PKCS#12 signature file and by choosing a strong password in line with state of art.

5 Certificate status checking obligations of relying parties

It is recommended that relying parties, in addition to the validation of the signature, of the eSeal or of the TLS challenge protocol, verify the validity of the issued certificate. Data allowing to verify the validity are provided by Netheos.

Netheos provides :

- The complete certificat chain up to the root CA
- The list of revoked certificates (CRL). CRL are compliant with IETF RFC 5280 standard.

The publication service, under normal circumstances, is available 24/24 and 7/7 under SLA condition depicted in the CP/CPS.

The relying party using a certificate issued by Netheos shall also check that the certificate is appropriate for the usage intended, in particular, the relying party shall:

- Verify and respect the intended usage of the certificate,
- For each certificate of the chain of trust, for end-entity certificate until the Root CA, verify the electronic signature of the issuing CA and check the validity of the certificate (validity period, revocation status)
- Check and respect the relying parties obligation mentioned in this document and within the CP/CPS.

Technical verification can be done in an automated manner by standard tool such as Acrobat Reader™ or the SD-DSS Open-Source library (provided the EU Commission) or OpenSSL.

6 Limited warranty and disclaimer/Limitation of liability

6.1 Limitation of usage

Netheos does not check the compliancy of its services with the law and Regulation applicable to the subscriber. In particular, Netheos is not accredited to manage healthcare data or sensible data related to National Security. Netheos is not responsible for any usage of the service not in adequation with the applicable Law and Regulations.

6.2 Limit of responsibility

Netheos is not responsible in case of usage not compliant with the conditions expressed in this PDS, the Terms & conditions and the CP/CPS, or any of contractual document between Netheos and the subscriber. In particular, the responsability of Netheos is not engaged in case of divergence of the level provided by the service, as mentioned in the present document, Terms and Conditions and CP/CPS and the security needs expected by the subscriber or relying parties.

Netheos certificates issuance service is limited to the provisioning of a technical service to the subscribers and relying parties. Netheos responsibility cannot be engaged in case of illegal usage or in case of usage non compliance with applicable law and regulations.

Netheos is not responsible of any damage and consequence, direct and indirect, caused by the divulgation by the subscriber of its authentication means or activation data.

Netheos is not responsable for any indirect damage caused by the use of the service. In any case, the responsability is limited to the amount paid for the issuance of the certificate or for the creation of the eSignature or eSeal.

7 Applicable agreements, CPS, CP

The following Certificate policy are associated with the certificates

Case /type of certificate	OID	Applicable Standard / regulation
Case 1. LCP (signature certificate for PDF)	1.3.6.1.4.1.55020.1.1.2.4.5	ETSI 319 411-1 for LCP profile
Case 2. NCP+ (signature certificate for PDF)	1.3.6.1.4.1.55020.1.1.2.4.1.	ETSI 319 411-1 for NCP+ profile
Case 3. LCP (signature certificate for hash signing)	1.3.6.1.4.1.55020.1.1.2.4.8	ETSI 319 411-1 for LCP profile
Case 4. NCP+ (signature certificate for hash signing)	1.3.6.1.4.1.55020.1.1.2.4.7	ETSI 319 411-1 for NCP+ profile
Case 5. NCP+ (seal certificate)	1.3.6.1.4.1.55020.1.1.2.4.3	ETSI 319 411-1 for NCP+ profile
Case 6. NCP+ (seal certificate for hash signing)	1.3.6.1.4.1.55020.1.1.2.4.10	ETSI 319 411-1 for NCP+ profile
Case 6. QCP-l (seal certificate)	1.3.6.1.4.1.55020.1.1.2.4.11	ETSI 319 411-2 for QCP-l profile

8 Privacy policy

Namirial privacy policy is applicable

9 Refund policy

No refund policy is applicable

10 Applicable law, complaints and dispute resolution

Applicable law are the French Republic law and regulations.
In case of complaints and dispute, parties will try an amicable settlement before starting any suit.
The competent jurisdiction is the Commerce Judicial Court of Montpellier (France).

11 TSP and repository licenses, trust marks, and audit

The CA is regularly audited by an accredited body in accordance with standard EN 319 403 to ensure its compliance with the eIDAS Regulation and related standards.

_____